SonicWall™
Secure Mobile Access 8.6

Administration Guide

SMA 200/400
SRA 1600/4600
SMA 500v Virtual Appliance

SONICWALL™

Copyright © 2017 SonicWall Inc. All rights reserved.

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

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

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

Legend

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

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

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

SonicWall SMA Administration Guide
Updated - September 2017
Software Version - 8.6
232-003817-00 Rev B

Contents

Part 1. Introduction

Part 2. Configuring Secure Mobile Access

Part 3. Configuring Services & Clients

Part 4. Configuring Users & Logs

Part 1

Introduction

- About This Guide
- Secure Mobile Access Overview

1

About This Guide

This *SonicWall Inc. Secure Mobile Access Administration Guide* provides network administrators with a high-level overview of Secure Mobile Access (SMA) technology, including activation, configuration, and administration of SonicWall Inc. SMA/SRA appliances using the Secure Mobile Access management interface.

Refer to SMA Documentation for the latest version of this guide as well as other SonicWall Inc. product and services documentation.

Guide Conventions

The following conventions are used in this guide:

Conventions used in this guide

Convention	Use
Bold	Highlights field, button, and tab names. Also highlights window, dialog box, and screen names. 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.

2

Secure Mobile Access Overview

This section provides an overview of the Secure Mobile Access (SMA) technology, concepts, basic navigational elements and standard deployment guidelines.

Topics:

Overview of SMA/SRA Hardware and Components

The SMA and SRA appliances provide organizations with a simple, secure and clientless method of access to applications and network resources specifically for remote and mobile employees. Organizations can use SMA 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.

This section contains the following subsections:

SMA Software Components

SMA/SRA appliances provide clientless identity-based secure remote access to the protected internal network. Using the Virtual Office environment, SMA/SRA appliances 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 Citrix or Microsoft Terminal Servers.

Although SMA protocols are described as clientless, the typical SMA portal combines Web, Java, and ActiveX components that are downloaded from the portal transparently, allowing users to connect to a remote network without needing to manually install and configure a VPN client application. In addition, SMA 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 SMA web-based management interface provides an end-to-end SMA solution. This interface can configure SMA users, access policies, authentication methods, user bookmarks for network resources, and system settings.

For clients, web-based SMA 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 version 2 (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 SMA network extension client, NetExtender, is available through the SMA Web portal through 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. 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. 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 and VNC applets support MS JVM in Internet Explorer, and run on other browsers with SUN JRE 1.6.0_10 or higher.

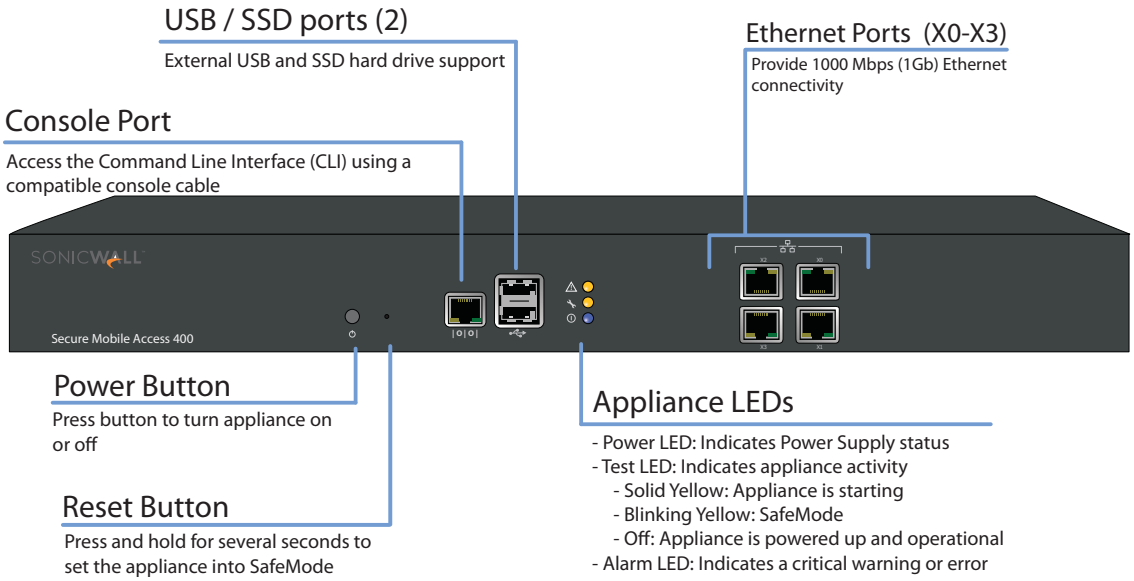
SMA Hardware Components

See the following sections for descriptions of the hardware components on SMA appliances:

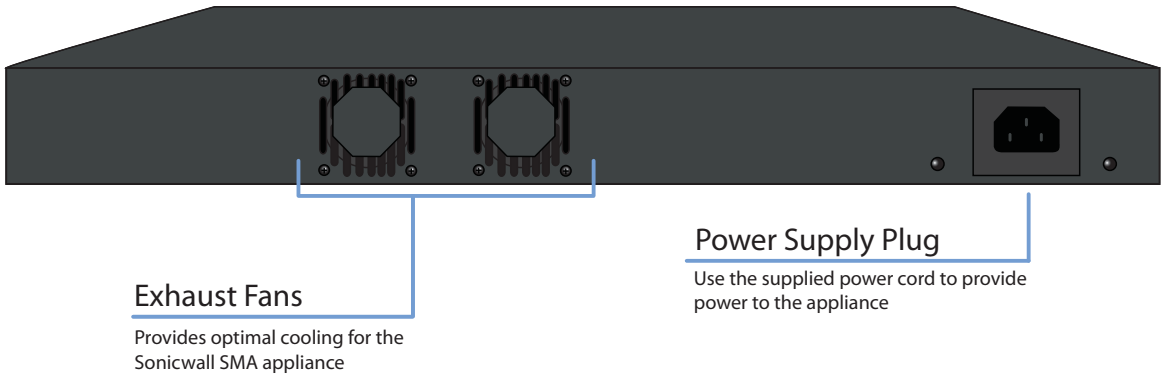
- SMA 400 Front and Back Panels Overview on page 16
- SMA 200 Front and Back Panels Overview on page 17

SMA 400 Front and Back Panels Overview

Front Panel



Rear Panel



SMA 400 Front Panel Features

Front Panel Feature	Description
Console Port	RJ-45 port, provides access to console messages with serial connection (115200 Baud). Provides access to command line interface (for future use).
USB/SSD Ports	Provides access to external USB and SSD hard drive support.
Reset Button	Provides access to SafeMode.
Power LED	Indicates the SMA 400 is powered on.
Test LED	Indicates the SMA 400 is in test mode.
Alarm LED	Indicates a critical error or failure.

SMA 400 Front Panel Features (Continued)

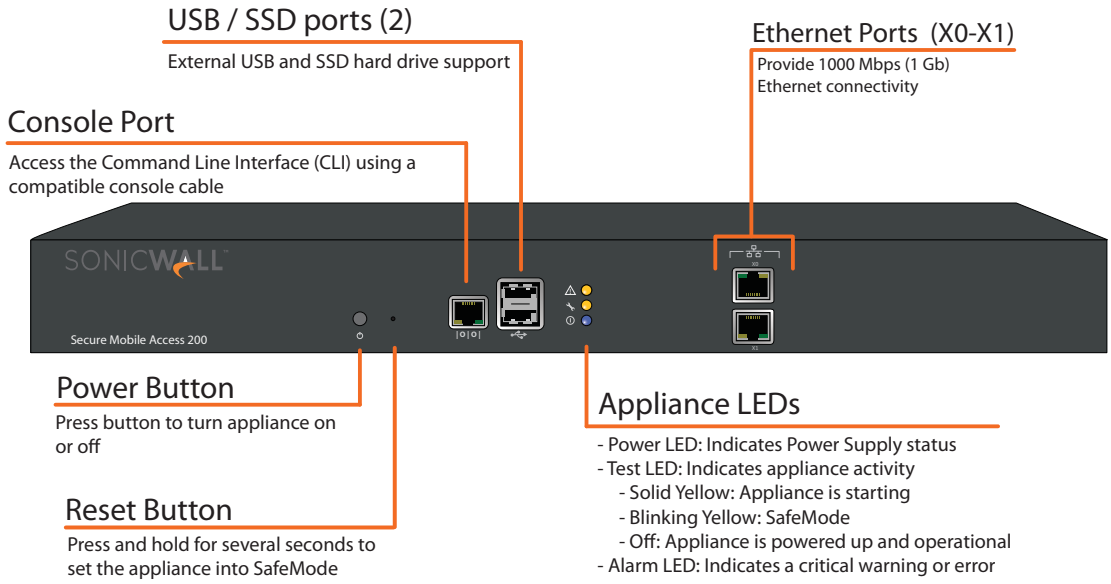
Front Panel Feature	Description
X3	Provides access to the X3 interface and to SMA resources.
X2	Provides access to the X2 interface and to SMA resources.
X1	Provides access to the X1 interface and to SMA resources.
X0	Default management port. Provides connectivity between the SMA 400 and your gateway.

SMA 400 Back Panel Features

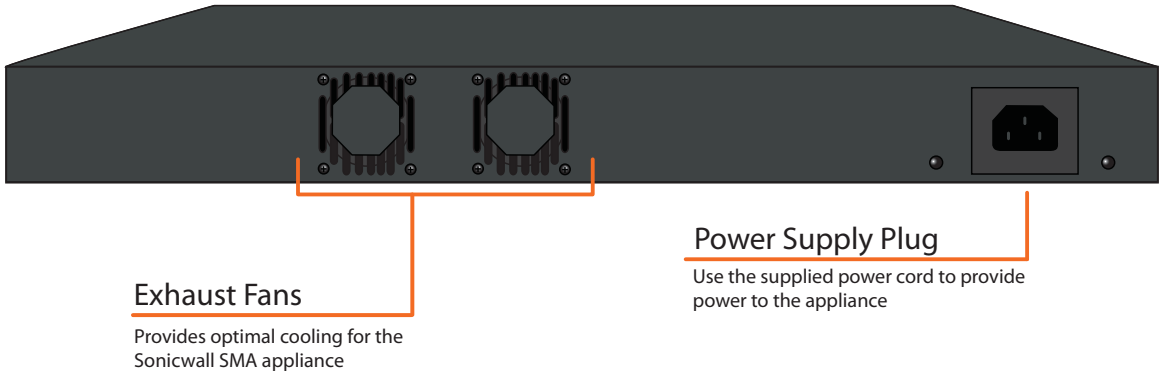
Back Panel Feature	Description
Exhaust fans	Provides optimal cooling for the SMA 400 appliance.
Power supply plug	Provides power connection using supplied power cord.

SMA 200 Front and Back Panels Overview

Front Panel



Rear Panel



SMA 200 Front Panel Features

Front Panel Feature	Description
Console Port	RJ-45 port, provides access to console messages with serial connection (115200 Baud). Provides access to command line interface.
USB/SSD Ports	Provides access to external USB and SSD hard drive support.
Reset Button	Provides access to SafeMode.
Power LED	Indicates the SMA 200 is powered on.
Test LED	Indicates the SMA 200 is in test mode.
Alarm LED	Indicates a critical error or failure.
X1	Provides access to the X1 interface and to SMA resources.
X0	Default management port. Provides connectivity between the SMA 200 and your gateway.

SMA 200 Back Panel Features

Back Panel Feature	Description
Exhaust fans	Provides optimal cooling for the SMA 200 appliance.
Power supply plug	Provides power connection using supplied power cord.

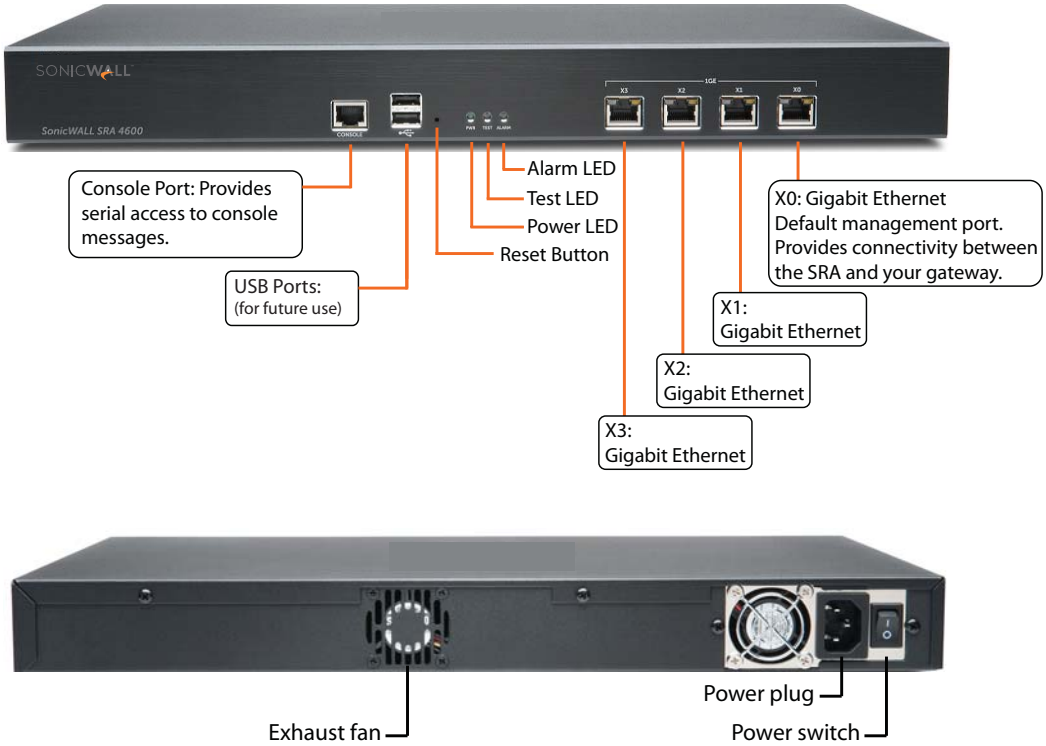
SRA Hardware Components

See the following sections for descriptions of the hardware components on SRA appliances:

- SRA 4600 Front and Back Panels Overview on page 19
- SRA 1600 Front and Back Panels Overview on page 20

SRA 4600 Front and Back Panels Overview

SRA 4600 Front and Back Panels



SRA 4600 Front Panel Features

Front Panel Feature	Description
Console Port	RJ-45 port, provides access to console messages with serial connection (115200 Baud). Provides access to command line interface (for future use).
USB Ports	Provides access to USB interface (for future use).
Reset Button	Provides access to SafeMode.
Power LED	Indicates the SRA 4600 is powered on.
Test LED	Indicates the SRA 4600 is in test mode.
Alarm LED	Indicates a critical error or failure.
X3	Provides access to the X3 interface and to SRA resources.
X2	Provides access to the X2 interface and to SRA resources.
X1	Provides access to the X1 interface and to SRA resources.
X0	Default management port. Provides connectivity between the SRA 4600 and your gateway.

SRA 4600 Back Panel Features

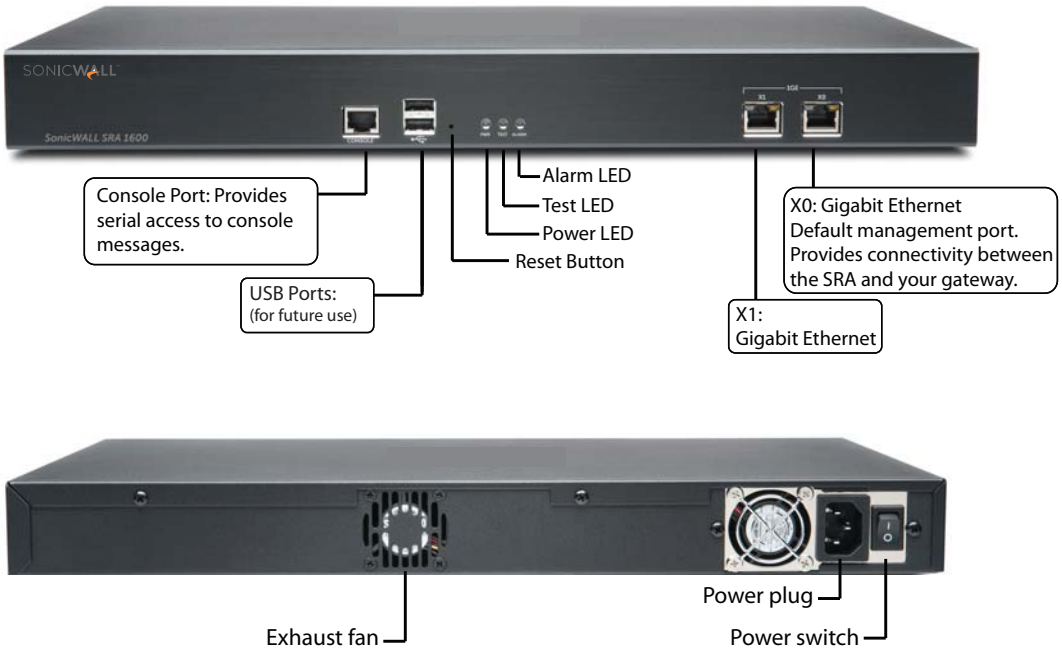
Back Panel Feature	Description
Exhaust fan	Provides optimal cooling for the SRA 4600 appliance.

SRA 4600 Back Panel Features (Continued)

Back Panel Feature	Description
Power plug	Provides power connection using supplied power cord.
Power switch	Powers the SRA 4600 on and off.

SRA 1600 Front and Back Panels Overview

SRA 1600 Front and Back Panels



SRA 1600 Front Panel Features

Front Panel Feature	Description
Console Port	RJ-45 port, provides access to console messages with serial connection (115200 Baud). Provides access to command line interface (for future use).
USB Ports	Provides access to USB interface (for future use).
Reset Button	Provides access to SafeMode.
Power LED	Indicates the SRA 1600 is powered on.
Test LED	Indicates the SRA 1600 is in test mode.
Alarm LED	Indicates a critical error or failure.
X1	Provides access to the X1 interface and to SRA resources.
X0	Default management port. Provides connectivity between the SRA 1600 and your gateway.

SRA 1600 Back Panel Features

Back Panel Feature	Description
Exhaust fan	Provides optimal cooling for the SRA 1600 appliance.
Power plug	Provides power connection using supplied power cord.
Power switch	Powers the SRA 1600 on and off.

SMA 500v Virtual Appliance

The SMA 500v Virtual Appliance is a virtual machine that runs the SMA software on a VMware platform. All software components, features, and functionality described in this guide are supported by the SMA 500v Virtual Appliance, except High Availability and SSL Off-loading.

Deploying SMA as a virtual appliance allows leveraging of shared computing resources to optimize utilization, easy migration and reduced capital costs. The SMA 500v Virtual Appliance provides the following benefits:

- Cost savings:
  - Multiple virtual machines can run on a single server, reducing hardware costs, power consumption, and maintenance costs.
  - Microsoft Windows Server is not required, eliminating the cost of the Windows license.
- Operational ease:
  - In a virtual environment, it is easy to commission new servers or decommission old ones, or to bring servers up or down.
  - Installation is accomplished by importing a file into the virtual environment, with no need to run an installer.
- Security:
  - The SMA 500v Virtual Appliance provides the same hardened operating system that comes with the SMA/SRA hardware appliances.

The elements of basic VMware structure must be implemented prior to deploying the SMA 500v Virtual Appliance. For detailed information about deploying the SMA 500v Virtual Appliance, see the *SonicWall Inc. SMA 500v Virtual Appliance Getting Started Guide*, available at: SMA Documentation

Concepts for Secure Mobile Access

This section provides an overview of the following key concepts that the administrator should be familiar with when using the SMA/SRA appliance and SMA 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 SMA/SRA appliance, the appliance sends the user its own encryption information, including an SSL certificate with a public encryption key.

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.

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 SMA/SRA appliance provides customers with cost-effective alternatives to deploying parallel remote-access infrastructures.

SSL Handshake Procedure

The following procedure is an example of the standard steps required to establish an SSL session between a user and an SMA/SRA gateway using the Secure Mobile Access web-based management interface:

1 When a user attempts to connect to the SMA/SRA appliance, the user's Web browser sends information about the types of encryption supported by the browser to the appliance.

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

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

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 SMA/SRA gateway.

5 The SMA/SRA gateway uses the pre-master key to create a master key and sends the new master key to the user's Web browser.

6 The browser and the SMA/SRA gateway use the master key and the agreed upon encryption algorithm to establish an SSL connection. From this point on, the user and the SMA/SRA gateway encrypts and decrypts data using the same encryption key. This is called symmetric encryption.

7 After the SSL connection is established, the SMA/SRA gateway encrypts and sends the Web browser the SMA/SRA gateway login page.

8 The user submits their user name, password, and domain name.

9 If the user's domain name requires authentication through a RADIUS, LDAP, or Active Directory Server, the SMA/SRA gateway forwards the user's information to the appropriate server for authentication.

10 After being authenticated, the user can access the Secure Mobile Access 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.

IPv6 supports stateful address configuration that 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.

Secure Mobile Access 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.
- **SSHv2 Bookmark** – Define an 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.

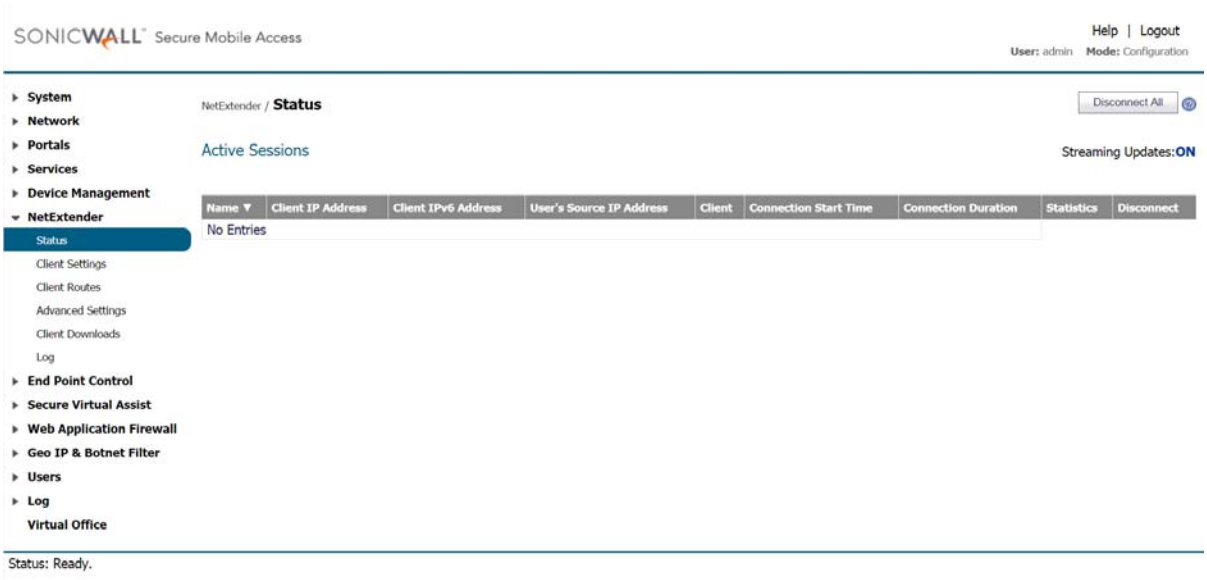
NOTE: IPv6 is not supported for File Shares (CIFS).

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 SMA/SRA appliance if the client machine supports IPv6 and an IPv6 address pool is configured on the SMA/SRA appliance. NetExtender supports IPv6 client connections from Windows systems running Vista or newer, and from Linux clients.



Secure 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.

Portals Overview

Secure Mobile Access provides a mechanism called Virtual Office that is a web-based *portal* interface that provides clients with easy access to internal resources in your organization. Components such as NetExtender, Secure 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 SMA/SRA appliance 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

SMA/SRA appliances allow you to configure multiple portals, each with their own title, banner, login message, logo and set of available resources. Each portal also enables you to set individual Virtual Hosts/Domain Names 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** window. For information on configuring portals, refer to Portals > Portals on page 142.

Domains Overview

A domain in the Secure Mobile Access environment is a mechanism that enables authentication of users attempting to access the network being serviced by the SMA/SRA appliance. Domain types include the Secure Mobile Access internal LocalDomain, and the external platforms Microsoft Active Directory, LDAP, and RADIUS. Often, only one domain suffices to provide authentication to your organization, although a larger organization might require distributed domains to handle multiple nodes or collections of users attempting to access applications through the portal.

Application Offloading and HTTP(S) Bookmarks Overview

SMA/SRA appliances use HTTP(S) bookmarks and application offloading to provide access to web-based applications running on servers within the intranet. This includes SharePoint 2007 and the enhanced versions of commonly-used Web mail interfaces, such as Microsoft OWA Premium and Domino Web Access 8.0.1, 8.5.1, and 8.5.2. SharePoint 2010 is supported with application offloading, but not with HTTP(S) bookmarks. SharePoint 2013 is supported with application offloading. Note that third-party modules that are not proxy friendly might not be supported by SharePoint.

Both application offloading and HTTP(S) bookmarks use an HTTP(S) reverse proxy. A reverse proxy is a proxy server that is deployed between a remote user outside an intranet and a target Web server within the intranet. The reverse proxy intercepts and forwards packets that originate from outside the intranet. An HTTP(S) reverse proxy specifically intercepts HTTP(S) requests and responses.

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 might 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 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 offloaded application portal must be configured as a virtual host with a suitable Secure Mobile Access 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 offloaded application 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.

Benefits of HTTP(S) Bookmarks

By using HTTP(S) bookmarks, users can access the full-featured versions of SharePoint 2007, Microsoft OWA Premium, and Domino Web Access 8.0.1, 8.5.1, and 8.5.2 Web mail interfaces. These interfaces are easier to use and provide more enhanced features than their basic counterparts.

Benefits of Application Offloading

An offloaded Web application has the following advantages over configuring the Web application as an HTTP(S) bookmark in Secure Mobile Access:

- No URL rewriting is necessary, thereby improving throughput significantly.
- The functionality of the original Web application is retained almost completely, while an HTTP(S) bookmark is a best-effort solution.
- Application offloading extends Secure Mobile Access 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 SSL acceleration of the SMA/SRA 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.
- To authenticate ActiveSync Application Offloading technology that delivers Web applications using Virtual Hosting and Reverse Proxy. ActiveSync authentication does not require URL rewriting in order to deliver the Web applications seamlessly. As an example, the ActiveSync protocol is used by a mobile phone's email client to synchronize with an Exchange server, as explained in ActiveSync Authentication on page 30.

Supported Platforms

Appliance Platforms

Application Offloading and HTTP(S) bookmarks are supported on all the SMA/SRA appliances that support the Secure Mobile Access 8.6 release:

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

HTTP Versions

HTTP(S) bookmarks and application offloading portals support both HTTP/1.0 and HTTP/1.1.

Certain performance optimization features, such as caching, compression, SSL hardware acceleration, HTTP connection persistence, TCP connection multiplexing and transfer-chunk encoding for proxies are automatically enabled depending on the usage.

Applications

SharePoint 2010 and **SharePoint 2013** are supported with application offloading, but not with HTTP(S) bookmarks. The following features have been tested and verified as working well on the indicated browsers:

Supported SharePoint features

SharePoint Features	Browsers
Add Announcement	Internet Explorer 9
Delete Announcement	Firefox 16.0 and later
Download Document	Chrome 22.0 and later
Add Document	
Delete Document	
Add New Item	
Delete Item	

The following Web applications have been tested and verified to work with HTTP(S) bookmarks and as offloaded applications:

- Microsoft Outlook Web Access 2013

  Microsoft Outlook Web Access 2010

  Microsoft Outlook Web Access 2007

  NOTE: Outlook Web Access is supported on the SMA 400/200, SRA 4600/1600, and the SMA 500v Virtual Appliance platforms.

- Windows SharePoint 2013 (supported only using App Offloading)

  Windows SharePoint 2007 (supported only using App Offloading)

  Windows SharePoint Services 3.0

  NOTE: The integrated client features of SharePoint are not supported.

- Lotus Domino Web Access 8.0.1

  Lotus Domino Web Access 8.5.1

  Lotus Domino Web Access 8.5.2

  NOTE: Domino Web Access is supported on the SMA 400/200, SRA 4600/1600, and the SMA 500v Virtual Appliance platforms.

- Novell Groupwise Web Access 7.0
- ActiveSync with Microsoft Exchange 2010
- ActiveSync with Microsoft Exchange 2007
- ActiveSync with Microsoft Exchange 2003

  Exchange ActiveSync is supported on the following:

  - Apple iPhone
  - Apple iPad
  - Android 2.3.x (Gingerbread), 4.0.x (ICS) and 4.1 (Jelly Bean) based phones

  NOTE: Application Offloading supports authentication for ActiveSync. ActiveSync is a protocol used by a mobile phone's email client to synchronize with an Exchange server. The Administrator can create an offloading portal and set the application server host to the backend Exchange server. Then, a user can use the new virtual host name in a mobile phone's email client, and synchronize with the backend Exchange server through the SMA/SRA appliance.

Authentication Schemes

The following authentication schemes are supported for use with application offloading and HTTP(S) bookmarks:

- **Basic** – Collects credentials in the form of a username and password.
- **Forms-based authentication** – Uses a Web form to collect credentials.

Software Prerequisites

The following end-user requirements must be met in order to access the complete set of application offloading and HTTP(S) bookmarks features:

- Internet Explorer 9.0 or newer

- Windows 10 and Windows 7

NOTE:

- The maximum number of users supported is limited by the number of applications being accessed and the volume of application traffic being sent.
- Feature support varies based on your hardware and installation, see the respective sections for more detailed information about specific application support.

TIP: If you are using the correct Web browser and operating system, and a supported application does not work, delete the browser session cookies, close and reopen all instances of your browser, clear the browser cache, and then try again.

Supported Application Deployment Considerations

Be aware of these installation and general feature caveats when using application offloading and HTTP(S) bookmarks with the following software applications:

- SharePoint
    - SharePoint 2013 and SharePoint 2010 are supported with application offloading, but not with HTTP(S) bookmarks.
- Outlook Anywhere
    - SMA/SRAs with Application Offloading.
    - Outlook Anywhere uses Microsoft's MS-RPCH proprietary protocol that could conflict with normal HTTP(S) protocol.

Application Offloading is only supported on SharePoint 2013 and with any application using HTTP/HTTPS. Secure Mobile Access has limited support for applications using Web services and no support for non-HTTP protocols wrapped within HTTP.

The application should not contain hard-coded self-referencing URLs. If these are present, the Application Offloading proxy must rewrite the URLs. Because Web site development does not usually conform to HTML standards, the proxy can only do a best-effort translation when rewriting these URLs. Specifying hard-coded, self-referencing URLs is not recommended when developing a Web site because content developers must modify the Web pages whenever the hosting server is moved to a different IP or hostname.

For example, if the backend application has a hard-coded IP address and scheme within URLs as follows, Application Offloading must rewrite the URL.

```
<a href="http://1.1.1.1/doAction.cgi?test=foo">
```

This can be done by enabling the **Enable URL Rewriting for self-referenced URLs** setting for the Application Offloading Portal, but all the URLs might not be rewritten, depending on how the Web application has been developed. (This limitation is usually the same for other vendors employing reverse proxy mode.)

Cross Domain Single Sign-On

External Website Bookmarks can be created for application offloading portals to achieve a single point of access for users. This allows users to automatically log in to application offloading portals after logging into the main portal.

To use Cross Domain Single Sign-on (SSO):

1. Create two or more portals with the same shared domain (from Virtual Host Domain name) and that need authentication. One portal should be a regular portal. These portals are also in the same SMA/SRA

appliance's domain so that a user can log in to both of them with the same credentials. Adding Portals on page 143 explains how to create a portal.

2 Log in to the portal and create a bookmark, as explained in Adding or Editing User Bookmarks on page 374.

3 Set the service to **External Web Site**, as explained in External Web Site on page 386.

4 Enable **Automatically log in** for the bookmark that enables Cross Domain SSO for this bookmark.

5 Specify a Host that is a portal with the same shared domain name.

6 Save the bookmark and launch it. The new portal is logged in automatically without any credential.

The shared domain names do not need to be identical; a sub-domain also works. For example, one portal is a regular portal whose virtual host domain name is "www.example.com" and its shared domain name is ".example.com." The other portal's virtual host domain name is "intranet.eng.example.com" and the shared domain name is ".eng.example.com." If a bookmark to xyz.eng.example.com is created in the www.example.com portal, Cross Domain SSO works because ".eng.example.com" is a sub-domain of ".example.com."

ActiveSync Authentication

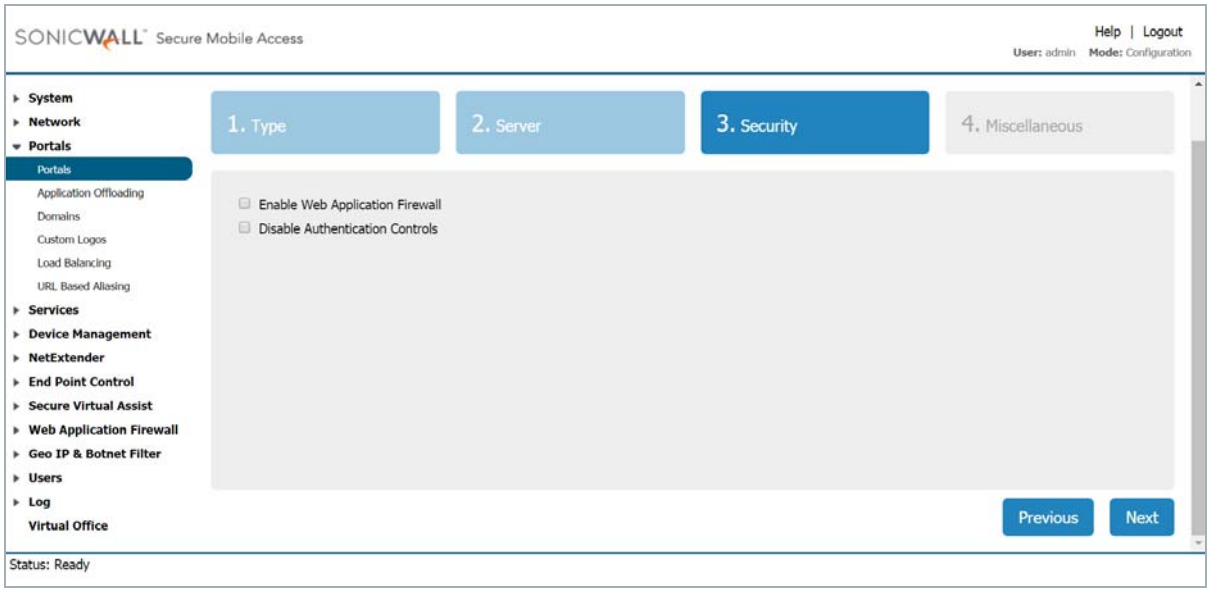
Application Offloading now supports authentication for ActiveSync. Application Offloading technology delivers Web applications using Virtual Hosting and Reverse Proxy. Users still need to authenticate with the SMA/SRA appliance before accessing the backend Web application. However, the proxy avoids URL rewriting in order to deliver the Web applications seamlessly.

ActiveSync is a protocol used by a mobile phone's email client to synchronize with an Exchange server. The Administrator can create an offloading portal and set the application server host to the backend Exchange server. Then, a user can use the new virtual host name in a mobile phone's email client, and synchronize with the backend Exchange server through the SMA/SRA appliance.

NOTE: On iPhones/iPads running versions earlier than iOS 6.1.2, initial account synchronization might fail if a calendar contains a recurring invite.

NOTE: To provide better protection for the Exchange Server, anonymous ActiveSync access will not be supported in the future.

ActiveSync is managed through the **Portals > Offload Web Application > Offloading > Security Settings** page:



To configure ActiveSync authentication, clear **Disable Authentication Controls** to display the authentication fields. Select **Enable ActiveSync authentication** and then type the default domain name. The default domain name cannot be used when the domain name is set in the email client's setting.

ActiveSync Log Entries

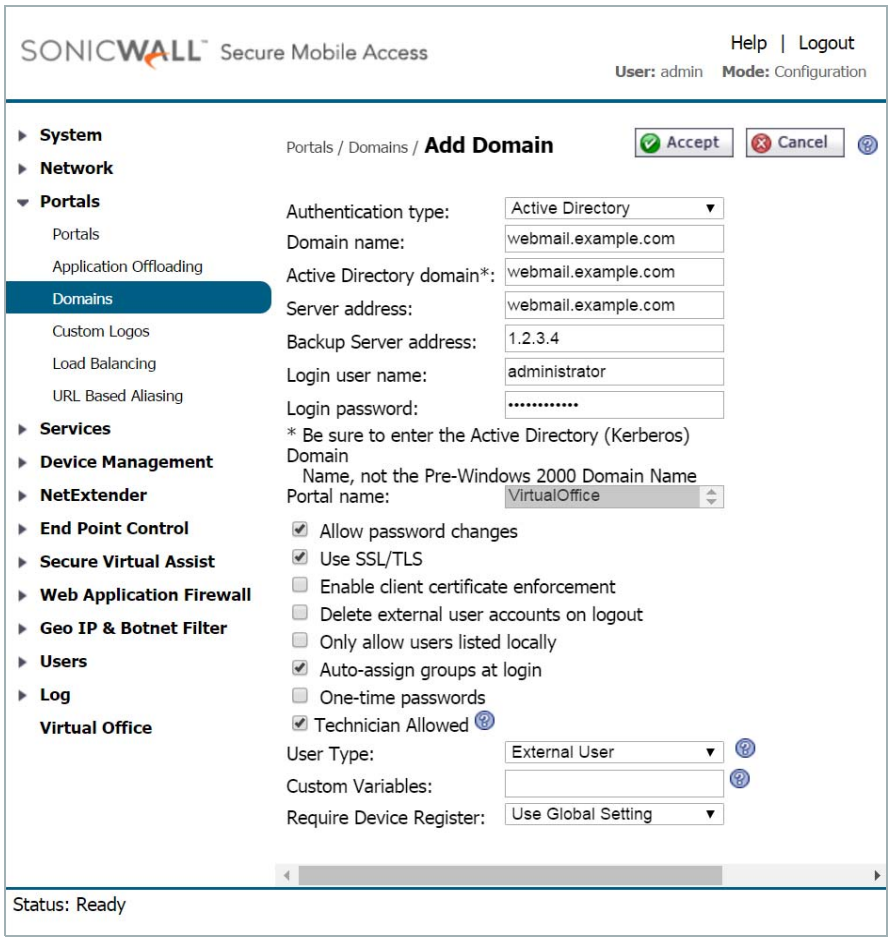
The **Log > View** page is updated when a Web application is offloaded. Most mobile systems (iPhone, Android, and so on) support ActiveSync. These log entries identify when the client began to use ActiveSync through the offloading portal. The ActiveSync message identifies the device ID (ActiveSync: Device ID is…) for an ActiveSync request unless a client sets up the account and the request does not contain a device ID.

NOTE: A user's credential in the Exchange server must be the same as the one in the SMA/SRA appliance. Many authentication types are available for each domain in the appliance. If using the Local User Database, make sure the user name and password is the same as the one for the Exchange server. Fortunately, other authentication types like Active Directory can share credentials for both the Exchange server and SMA/SRA appliance. However, authentication using authentication types that share credentials might take longer and the first ActiveSync request can time out. After authentication succeeds, a session is created and other requests are not necessary to be authenticated again.

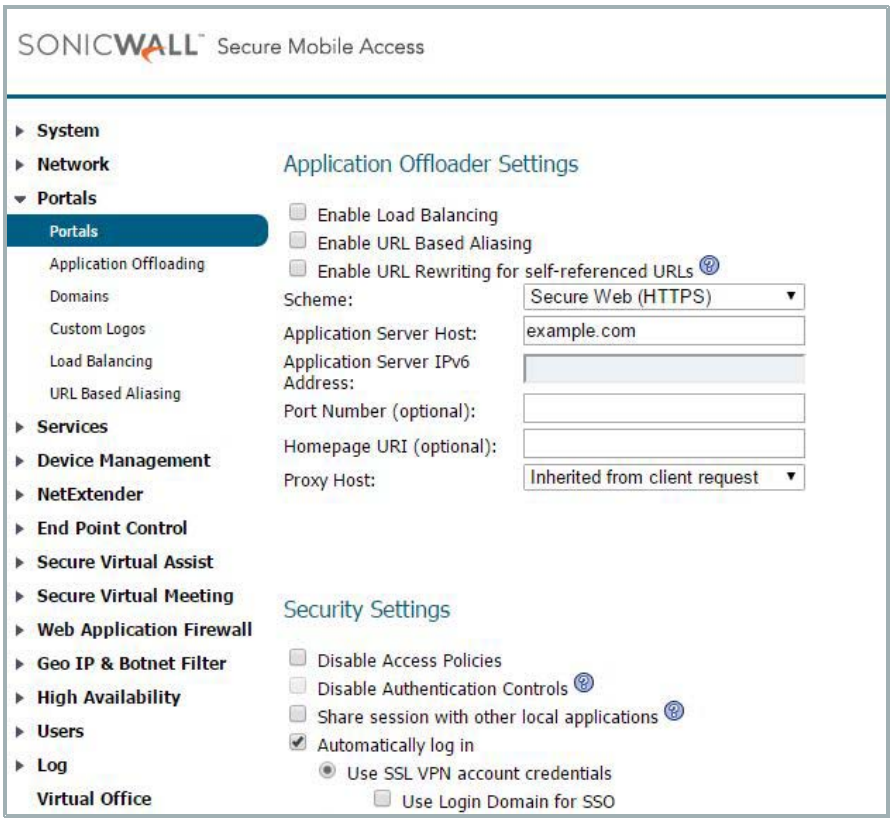
Configuring a Portal to Check Email From an Android Device

The following example shows how to set up ActiveSync to check emails from an Android device. Be sure to replace entries shown in the examples with entries for your environment, and be careful to input the correct password. Otherwise, the account is blocked.

1 Create a **Domain name** of webmail.example.com. Set the **Active Directory domain** and **Server address** to webmail.example.com. Set the **Portal name** to VirtualOffice.



2 In the Secure Mobile Access management interface, scroll down to the relevant section and create an offloading portal with the name **sales**.



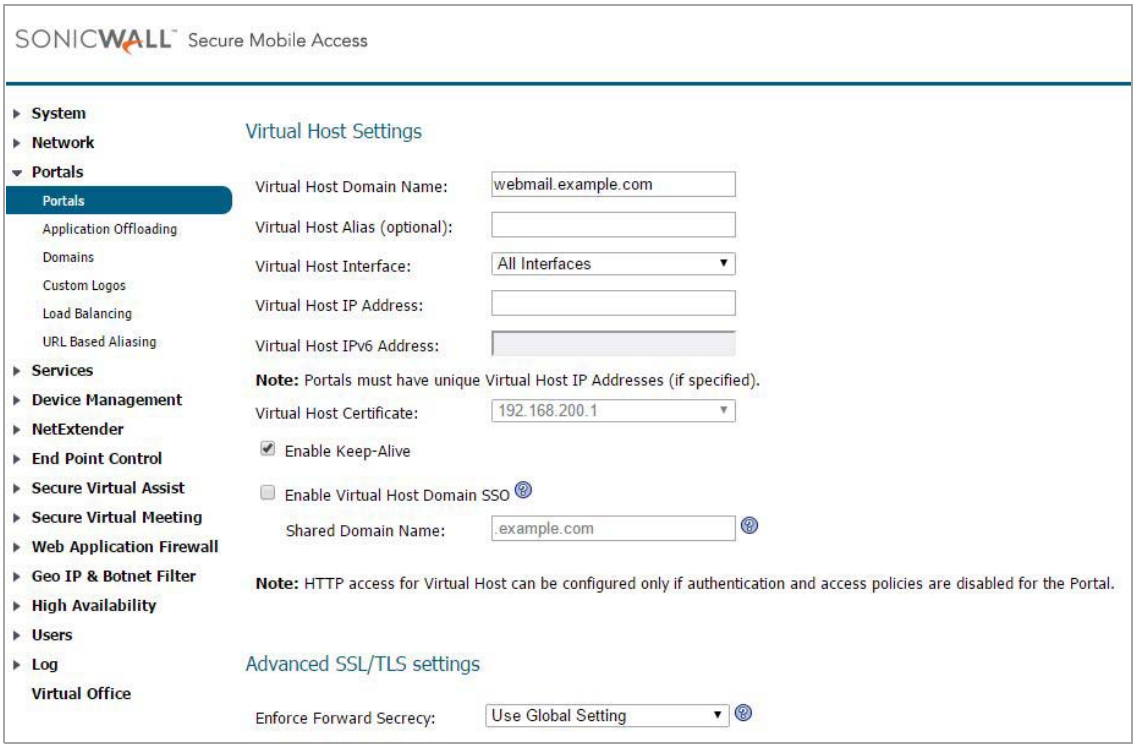
3 Set the **Scheme** to **Secure Web (HTTPS).**

4 Set the **Application Server Host** to your Exchange server, for example *webmail.example.com*.

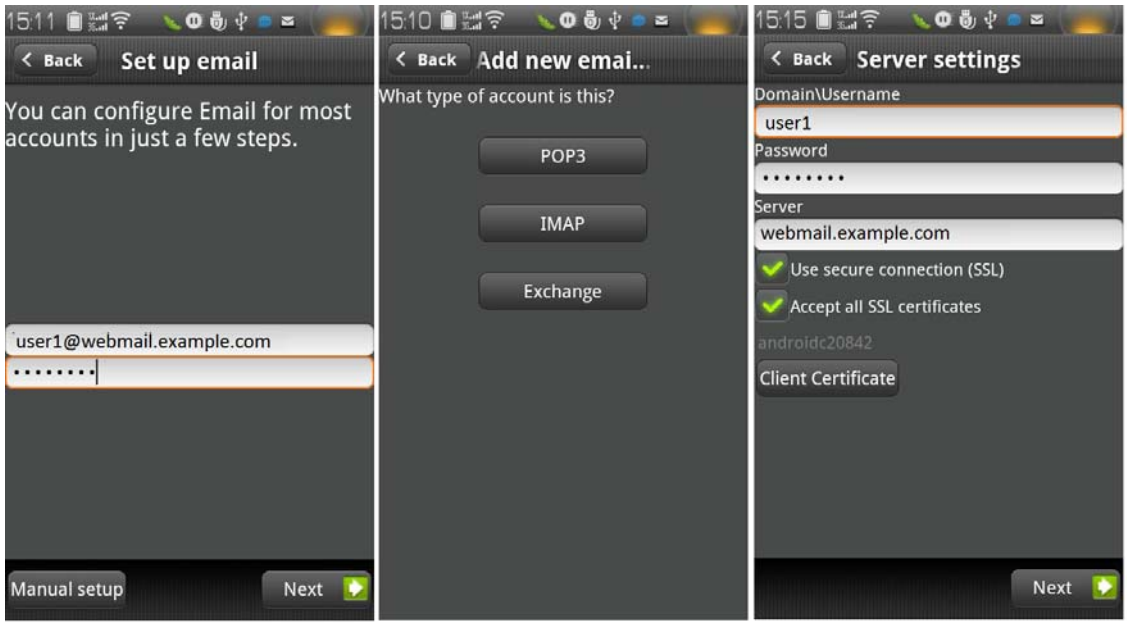
5 Set the virtual host name, for example, *webmail.example.com*. The virtual host name should be resolved by the DNS server. Otherwise, modify the hosts file in the Android phone.

6 Select **Enable Email Clients Authentication**. Leave the default domain name blank or input **webmail.example.com.**

7 Click the **Virtual Host** tab.



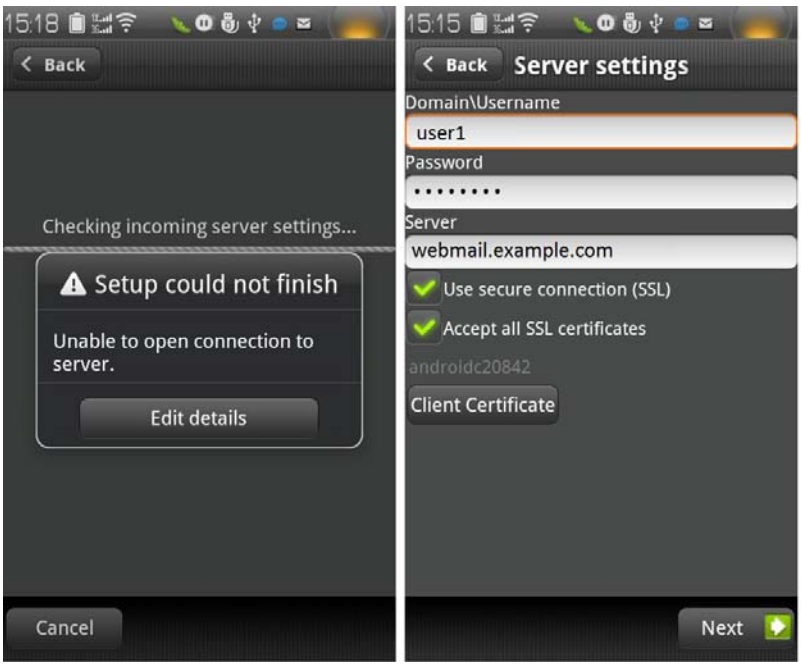
8 Turn on the Android phone, open the Email application, and type your email address and password. Click **Next**.



9 Choose **Exchange.**

10 Input your **Domain\Username**, **Password**, and **Server**. No domain name is displayed, so use the default domain name specified in the offloading portal's setting. Select **Accept all SSL certificates** and click **Next.**

11 If the AD authentication times out, the **Setup could not finish** message is displayed. Wait about 20 seconds and try again. You can also check the Secure Mobile Access log to see if the user logged in successfully. You might not encounter this problem if the AD authentication is fast.



12 When the authentication finishes, a security warning appears. Click **OK** to continue, modify your account settings, and click **Next**.

13 Try to send and receive emails, and ensure that ActiveSync entries are included in the Secure Mobile Access log.

Network Resources Overview

Network Resources are the granular components of a trusted network that can be accessed using the SMA/SRA appliance. 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 the SMA/SRA appliance:

HTTP (Web) and Secure HTTPS (Web)

The SMA/SRA 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 SMA/SRA appliance using HTTPS and requests a URL. The URL is then retrieved over HTTP by the SMA/SRA appliance. The URL is transformed as needed, and returned encrypted to the remote user.

The Secure Mobile Access 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, Windows SharePoint 2007, Novell Groupwise Web Access 7.0, or Domino Web Access 8.0.1, 8.5.1, and 8.5.2 with HTTP(S) reverse proxy support. Reverse-proxy bookmarks also support the HTTP 1.1 protocol and connection persistence.

HTTPS bookmarks on SMA 400 and SRA 4600 appliances support keys of up to 2048 bits.

HTTP(S) caching is supported on the SMA/SRA 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 SMA/SRA 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 SMA/SRA appliance and is cleared for access by the access policies. However, Secure Mobile Access optimizes traffic to the backend Web server 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 SMA/SRA 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 appliance saves bandwidth and results in higher throughput. Furthermore, only compressed content is cached, saving nearly 40-50 percent of the required memory. Note that gzip compression is not available on the local (clear text side) of the SMA/SRA appliance, or for HTTPS requests from the remote client.

Telnet

Java is being deprecated. Going forward, use HTML5 bookmarks. 8.6 utilizes HTML5 by default.

To enable Java for legacy support, call SonicWall Customer Support for assistance. Note that Java will not be supported in the future.

Telnet client is delivered through the remote user's Web browser. The remote user can specify the IP address of any accessible Telnet server and the SMA/SRA appliance makes 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. Telnet also supports HTML5 and Smart Access selection.

SSHv2

Java is being deprecated. Going forward, use HTML5 bookmarks. 8.6 utilizes HTML5 by default.

To enable Java for legacy support, call SonicWall Customer Support for assistance. Note that Java will not be supported in the future.

SSH clients delivered through the remote user's Web browser. The remote user can specify the IP address of any accessible SSH server and the SMA/SRA appliance makes a connection to the server. Communication between the user over SSL and the server is proxied using natively encrypted SSH. 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. SSHv2 also supports HTML5 and Smart Access selection.

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 SMA/SRA appliance. The remote user communicates with the SMA/SRA appliance by HTTPS and requests a URL that is retrieved over HTTP by the SMA/SRA appliance, 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 might be required. FTP also supports HTML5 and Smart Access selection.

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 and VNC are supported on Windows, Linux, and Mac operating systems. 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. RDP and VNC also supports HTML5 and Smart Access selection. The RDP and VNC clients are automatically delivered to authorized remote users through their Web browser in the following formats:

- **VNC** - 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 7 Support

The SMA/SRA appliance supports connections with RDP 7 clients and supports the RDP 7 feature set. RDP 7 is available on following operating systems:

- Windows Server 2016
- Windows Server 2012
- Windows 10
- Windows 7
- Windows Vista SP2
- Windows Vista SP1

RDP 6 Support

The SMA/SRA appliance supports connections with RDP 6.1 and RDP 6 clients, and supports the RDP 5 feature set plus four RDP 6 features.

RDC 6.1 is included with the following operating systems:

- Windows 7
- Windows Server 2008
- Windows Vista Service Pack 1 (SP1)

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 Adding or Editing User Bookmarks on page 374.

NOTE: RDP 6 and RDP 7 end client systems must have the client installed on their system. The SMA/SRA appliance does not provision the mstsc client and utilizes the locally installed client for those connections.

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 Native** – Uses the native 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 HTML5** – Uses the HTML5-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

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

Application Support Table

Application	Supports SSO	Global/Group/ User Policies	Bookmark Policies
Terminal Services (RDP - Native)	Yes	Yes	Yes
Terminal Services (RDP - HTML5)	Yes	Yes	Yes
Virtual Network Computing (VNC - HTML5)	Yes	Yes	Yes
File Transfer Protocol (FTP)	Yes	Yes	Yes
Telnet	Yes	Yes	Yes
Telnet (HTML5)	Yes	Yes	Yes
Secure Shell (SSH)	Yes	Yes	Yes
Web (HTTP)	Yes	Yes	Yes
Secure Web (HTTPS)	Yes	Yes	Yes
File Shares (CIFS)	Yes	Yes	Yes
Citrix Portal (Citrix)	No	Yes	Yes

Microsoft Outlook Web Access

Secure Mobile Access includes reverse proxy application support for all versions of OWA 2013, 2010, and 2007.

Microsoft OWA Premium mode is a Web client for Microsoft Outlook 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. Secure Mobile Access HTTP(S) reverse proxy supports Microsoft OWA Premium.

See Creating Unique Access Policies for AD Groups on page 474 for a use case involving configuring group-based access policies for multiple Active Directory groups needing access to Outlook Web Access.

Windows SharePoint Services

The Secure Mobile Access reverse proxy application support for Windows SharePoint 2007 and Windows SharePoint Services 3.0 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

Lotus Domino Web Access

The SMA/SRA appliance reverse proxy application supports for Domino Web Access 8.0.1, 8.5.1, and 8.5.2 includes the following features:

Lotus Domino web access: Supported features

8.5.1 and 8.5.2 Features	8.0.1 Features
Full Mode:	
Email	Email
Calendar	Calendar
Contacts	Contacts
To Do	To Do
Notebook	Notebook
Lite Mode:	
Email	Email
Calendar	Calendar
Contacts	
Ultra Lite Mode:	
Inbox	
Sent	
All Docs	
Day At a Glance	
Contacts	
Trash	

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 Receiver clients for ActiveX and Java are supported, as well as the earlier XenApp and ICA clients. In previous versions of Citrix, the Citrix ICA Client was renamed as the Citrix XenApp plug-in.

Secure Mobile Access supports Citrix XenApp Server 7.6, 6.5, XenApp Server 6.0, and XenApp Server 5.0.

Secure Mobile Access supports Citrix Receiver for Windows 4.2, 4.1, 4.0(Online Plug-in 14.2, 14.1, 14.0); Java client version 10.1.006 or higher.

NOTE: Citrix Java Bookmarks are no longer officially supported by SonicWall Inc. because Citrix has ended support for the Java Receiver. SonicWall Inc. recommends using the HTML5 or ActiveX access methods for Citrix Bookmarks.

SNMP Overview

SMA/SRA appliances support Simple Network Management Protocol (SNMP) that 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 SMA/SRA appliance to enable it to resolve host names with IP addresses. The Secure Mobile Access 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 SMA/SRA appliance to reach remote IP networks through the designated default gateway. The gateway is typically the upstream firewall to which the SMA/SRA 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.

NetExtender Overview

This section provides an overview to the NetExtender feature.

Topics:

For information on using NetExtender, refer to the NetExtender > Status on page 242 or refer to the *Secure Mobile Access User's Guide*.

What is NetExtender?

SonicWall Inc. NetExtender is a transparent software application for Windows 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.

NetExtender capabilities include the SonicWall Inc. Mobile Connect app for Mac, Apple iPhone, iPad, and iPod Touch. Mobile Connect enables secure, mobile connections to private networks protected by SonicWall Inc. security appliances. For information about installing and using SonicWall Inc. Mobile Connect, see the *SonicWall Inc. Mobile Connect User's Guide*.

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 Firefox. On Linux 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

Secure Mobile Access 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. 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 first uninstalls the old NetExtender and installs the new version.

After 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.

NetExtender can establish a VPN session before the user logs into the Windows domain. For Windows Vista or later, users can click **Switch User** on the Windows login screen and click the blue computer icon that appears at the right bottom of the screen to view the dialup connection list, and then can select NetExtender to connect.

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.

NetExtender is compatible with the following SonicWall Inc. appliances:

- SMA 400/200
- SRA 4600/1600
- SMA 500v Virtual Appliance
- NSA, TZ, and SuperMassive 9000 series (with an SSL VPN license)

NetExtender is also backward compatible with older SRA 1200/4200 and SSL-VPN 2000/4000 appliances for connectivity.

NetExtender is officially supported on the following client platforms:

- Fedora 14+
- Ubuntu 11.04+
- OpenSUSE 10.3+
- Windows 10, Windows 7, Windows 2012, Windows Server 2008 R2.

NetExtender might work properly on other Linux distributions, but they are not officially supported by SonicWall Inc..

NOTE: The Mobile Connect application is now available for iOS 4.3 or higher and Android 4.0 or higher.

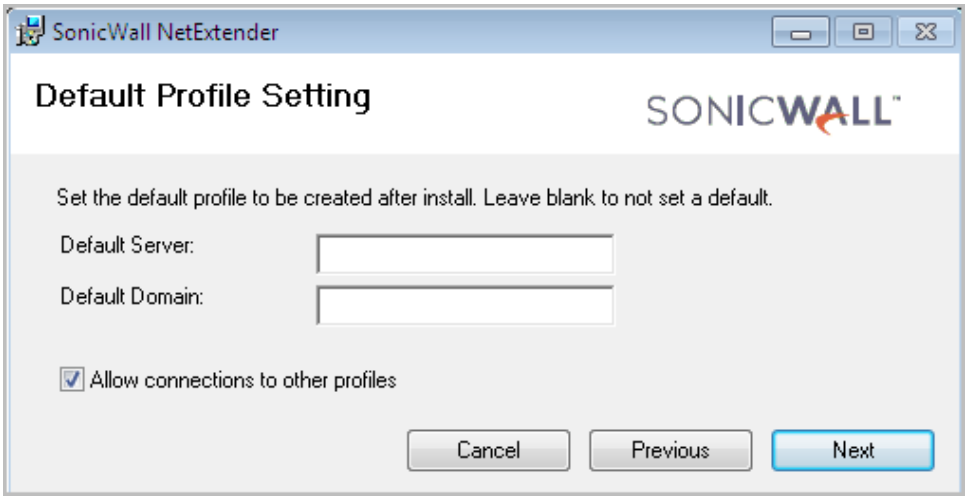
Pre-filling the Server and Domain Fields while Installing NetExtender through Microsoft Installer

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

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

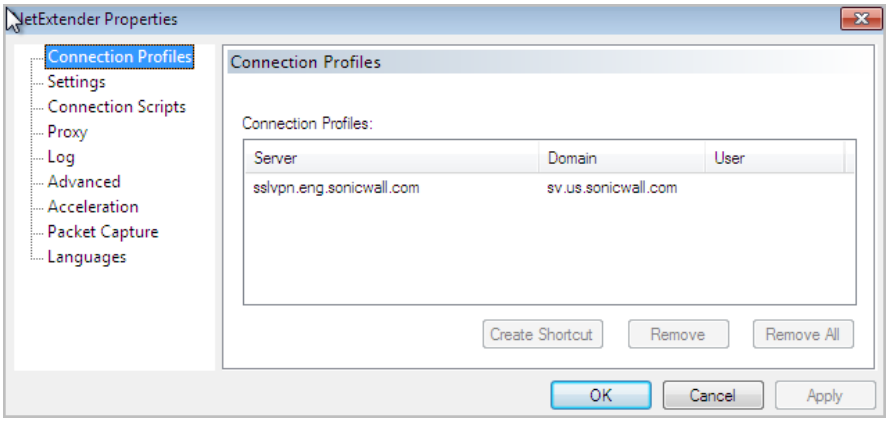
1 On the **Default Profile Setting** page, enter the IP address of the **Default Server** in the appropriate field and the location of the **Default Domain** in the second field.

NOTE: You must use the Microsoft Installer for this page to appear.



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

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



Multiple Ranges and Routes

Multiple range and route support for NetExtender on SMA/SRA appliances 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. The following sections describe the multiple range and route enhancements:

- IP Address User Segmentation on page 44
- Client Routes on page 45

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 SMA/SRA appliance assigns IP addresses. When assigning an IP address to a NetExtender client, the SMA/SRA 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, and so on). This segmentation is controlled by **Add Global NetExtender Client routes** and **Add Group NetExtender Client routes**.

NetExtender with External Authentication Methods

Networks that use an external authentication server are not configured with local usernames on the SMA/SRA appliance. In such cases, when a user is successfully authenticated, a local user account is created when the **Add Global NetExtender Client routes** and **Add Group NetExtender Client routes** settings are enabled.

Point to Point Server IP Address

In Secure Mobile Access, 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 are used for NetExtender clients.

Connection Scripts

SMA/SRA appliances provide 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 Secure Mobile Access 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:

Tunnel All mode: Routes to be added to 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 Secure Mobile Access 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 Secure Mobile Access tunnel.

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

Proxy Configuration

SMA/SRA appliances support 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)) that can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, 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 prompts 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 SMA/SRA server directly. The proxy server then forwards traffic to the SMA/SRA 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.

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

Two RADIUS servers can be used for two-factor authentication, allowing users to be authenticated through the Web portal or with an Secure Mobile Access client such as NetExtender or Secure Virtual Assist.

NOTE: Single sign-on (SSO) in SMA/SRA appliances do not support two-factor authentication.

See the following sections:

- Benefits of Two-Factor Authentication on page 47
- How Does Two-Factor Authentication Work? on page 47
- Supported Two-Factor Authentication Providers on page 47

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, or two separate RADIUS authentication servers.

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 or password

When two RADIUS servers are used, the second stage PIN or password can be sent to the user through SMS or email. NetExtender login and Secure Virtual Assist both provide extra challenge(s) for entering it.

When a third-party authentication service is used, it consists of two components:

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

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 dual RADIUS servers solution, the RSA SecureID solution, and the 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 not supported on all hardware platforms and is supported through RADIUS only.

VASCO

VASCO is a public company that provides user authentication products. VASCO utilizes Digipass tokens to authenticate through a VASCO IdentiKey server. VASCO is supported on all SMA/SRA platforms.

VASCO Data Security delivers reliable authentication through the use of One Time Password technology. VASCO IdentiKey combined with SMA/SRA and firewall VPN appliances creates an open-market approach delivered through VASCO IdentiKey technology.

VASCO IdentiKey allows users to utilize the VASCO DIGIPASS concept that uses One Time Passwords that are assigned for time segments that provide easy and secure remote access. The One Time Password within the

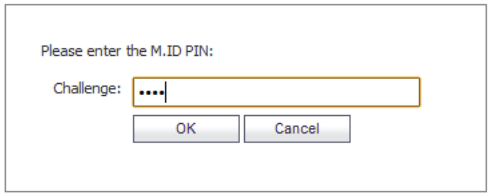
authentication request is verified on the VASCO IdentiKey. After verification, a RADIUS access-accept message is sent to the SMA/SRA server for authentication.

Two-Factor Authentication Login Processes

This section provides examples of the two-factor authentication login prompts when using Web login and NetExtender.

With Web login, the **Username** and **Password** fields are used to enter the first-stage credentials.

When prompting the user to input the challenge code, the message “Please enter the M.ID PIN:” is the reply message from the RADIUS server in this example; different RADIUS servers can have different reply message formats.

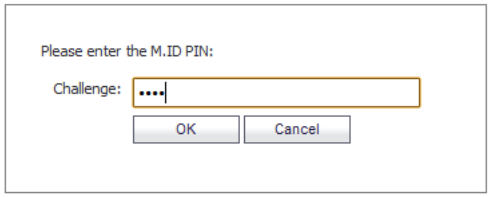


Some RADIUS servers might require the user to respond to several challenges to complete the authentication. In this example, the M.ID server asks the user to supply two challenges. The following passcode can be received through email or cellphone (if SMS is configured).

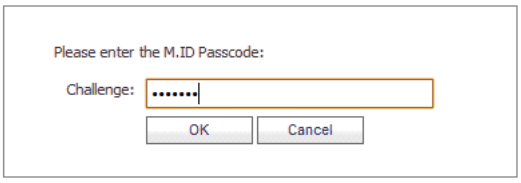
When using two-factor authentication with the NetExtender Windows client, the login process through the client is very similar to logging in through the Web page.

Initially, the **Username** and **Password** fields are used to enter the first-stage credentials.

This is followed by the PIN challenge.



Last, the Passcode challenge is displayed.



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?

The Secure Mobile Access 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 Secure Mobile Access 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 Secure Mobile Access users.

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

Benefits of One Time Passwords

The Secure Mobile Access 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 Secure Mobile Access administrator before completing the Secure Mobile Access 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 One Time Password Feature Work?

The Secure Mobile Access 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 Secure Mobile Access 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.

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 that take precedence over those auto-configured by a domain policy and over AD/LDAP settings.

In order to use the Secure Mobile Access One Time Password feature, the administrator must configure valid mail server settings in the **Log > Settings** page of the Secure Mobile Access 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 One Time Passwords are in an external domain (such as SMS addresses or external webmail addresses), you might need to configure your SMTP server to allow relaying from the SMA/SRA appliance to the external domain.

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 Secure Mobile Access interface. After login, users receive a message that a temporary password has been sent to a pre-defined email account. The user must log in to the external email account and retrieve the one-time password, then type or paste it into the appropriate field in the Secure Mobile Access login interface. Any user requests prior to entering the correct one-time password re-directs 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 **Cancel** in the Secure Mobile Access interface, or it is automatically deleted when the user fails to login within that user’s timeout policy period.

Configuring One Time Passwords for SMS-Capable Phones

Secure Mobile Access One Time Passwords can be configured to be sent by email directly to SMS-capable phones. Contact your cell phone service provider for further information about enabling SMS (Short Message Service).

The following 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@text.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 the Using SMS Email Formats on page 515 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 can vary. You might need additional service or information from your provider before using SMS. Contact the SMS provider directly to verify these formats and for further information on SMS services, options, and capabilities.

To configure the SMA/SRA appliance to send one-time passwords to an SMS email address, follow the procedure described in Editing User Settings on page 360, 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, log in to the Secure Mobile Access Virtual Office user interface using the credentials for that account.

If you are able to successfully log in 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, log in 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.

End Point Control Overview

This section provides an introduction to the End Point Control feature. This section contains the following topics:

What is End Point Control?

In traditional VPN solutions, accessing your network from an untrusted site like an employee-owned computer or a kiosk at an airport or hotel increases the risk to your network resources. EPC provides secure access from any Web-enabled system, including devices in untrusted environments.

Benefits of End Point Control

The SMA/SRA appliance supports End Point Control (EPC) that provides the following benefits:

- Verifies that the user's environment is secure before establishing a connection.
- Protects sensitive data and
- Ensures that your network is not compromised when accessed from devices in untrusted environments.
- Protects the network from threats originating from client devices participating in the SMA/SRA.

How Does End Point Control Work?

The SMA/SRA appliance provides end point security controls by completing host integrity checking and security protection mechanisms before a tunnel session is begun. Host integrity checks help ensure that the client system is in compliance with your organization's security policy. SonicWall end point security controls are tightly integrated with access control to analyze the Windows client system and apply access controls based on the results.

End Point Control is supported on Mac iOS and Android mobile devices using Mobile Connect, allowing device profiles to be created for these devices. This provides security protection from threats against client devices and protection to the SMA/SRA appliance from threats originating from client devices logged in to the appliance. For more information on Mobile Connect, refer to the *Mobile Connect User Guides*.

Configuring End Point Control

To configure End Point Control (EPC), complete the following tasks:

1. Configure Device Profiles that allow or deny user authentication based on various global, group, or user attributes. See End Point Control > Device Profiles on page 260.
2. Add and configure groups and users to allow or deny End Point Control profiles. See Edit EPC Settings on page 433.
3. Configure users to inherit their group profiles. See Edit EPC Settings on page 433.
4. Enable End Point Control. See End Point Control > Status on page 266.
5. Connect to NetExtender and monitor the End Point Control log. See End Point Control > Log on page 267.

Secure Virtual Assist Overview

NOTE: Secure Virtual Assist is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

This section provides an introduction to the Secure Virtual Assist feature. This section contains the following topics:

What is Secure Virtual Assist?

NOTE: Secure Virtual Assist is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

Secure Virtual Assist is an easy to use tool that allows Secure Mobile Access 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. Secure Virtual Assist creates a simple to deploy, easy to use remote support solution.

Benefits of Secure Virtual Assist

NOTE: Secure Virtual Assist is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

Secure Virtual Assist provides the following benefits:

- **Simplified and effective customer support** - Support staff can use Secure 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** - Secure 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 Secure 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 SMA/SRA appliance and tokenless two-factor authentication can be utilized.
- **Secure connections** - 256-bit AES SSL encryption of the data by the SMA/SRA 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 Secure Virtual Access functionality, support staff can access their personal systems located outside the LAN of the SMA/SRA appliance.

How Does Secure Virtual Assist Work?

NOTE: Secure Virtual Assist is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

The following sections describe how the Secure Virtual Assist feature works:

- Basic Operation on page 54
- Remote File Transfer on page 55
- Chat Feature on page 55

- Email Invitation on page 55
- Secure Virtual Access on page 55

Basic Operation

NOTE: Secure Virtual Assist is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

Secure Virtual Assist is a lightweight, thin client that installs automatically using Java from the Secure Mobile Access Virtual Office without requiring the installation of any external software. For computers that do not support Java, Secure Virtual Assist can be manually installed by downloading an executable file from the Virtual Office.

For basic screen sharing support, administrative privileges are not required to run Secure Virtual Assist. For full installation of the client, administrative rights might be necessary, but full installation is not necessary to use the service.

When a user requests service as a customer, Secure Virtual Assist should not be run while connected to the system through RDP for Windows 7 and Windows Vista platforms. Secure 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 Secure 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 Secure Virtual Assist session consists of the following sequence of events:

1. The technician launches Secure Virtual Assist from the Secure Mobile Access Virtual Office.
2. The technician monitors the Assistance Queue for customers requesting assistance.
3. The customer requests assistance by one of the following methods:
    - Logs into the Secure Mobile Access Virtual Office and clicks on the Secure Virtual Assist link.
    - Receives an email invitation from the technician and clicks on the link to launch Secure Virtual Assist.
    - Navigate directly to the URL of the Secure Virtual Assist home page that is provided by the technician.
4. The Secure Virtual Assist application installs and runs on the customer's browser.
5. The customer appears in the Secure Virtual Assist Assistance Queue.
6. The technician clicks on the customer's name and launches a Secure 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 Secure 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 does.
9. If at anytime the customer wants to end the session, they can take control and click **End Virtual Assist** in the bottom right corner of the screen.
10. When the session ends, the customer resumes sole control of the computer.

Remote File Transfer

NOTE: Secure Virtual Assist is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

Secure 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 Secure Virtual Assist window. The File Transfer feature supports the upload and download of multiple files.

Chat Feature

NOTE: Secure Virtual Assist is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

Secure 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 **Chat** in the Secure Virtual Assist taskbar.

Email Invitation

NOTE: Secure Virtual Assist is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

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

Secure Virtual Access

NOTE: Secure Virtual Assist is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

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

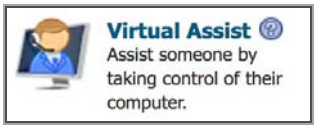
Installing and using Secure Virtual Access requires administrative privileges.

Launching a Secure Virtual Assist Technician Session

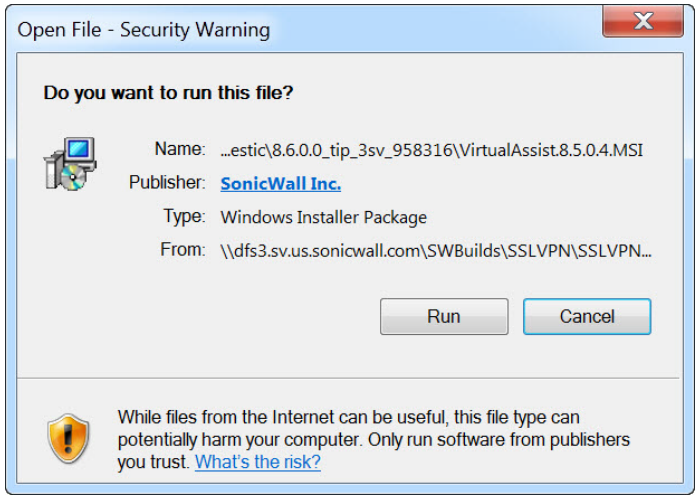
NOTE: Secure Virtual Assist is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

To launch a Secure Virtual Assist session as a technician:

1. Log in to the Secure Mobile Access Virtual Office. If you are already logged in to the Secure Mobile Access management interface, click **Virtual Office**.
2. Click on **Secure Virtual Assist**.



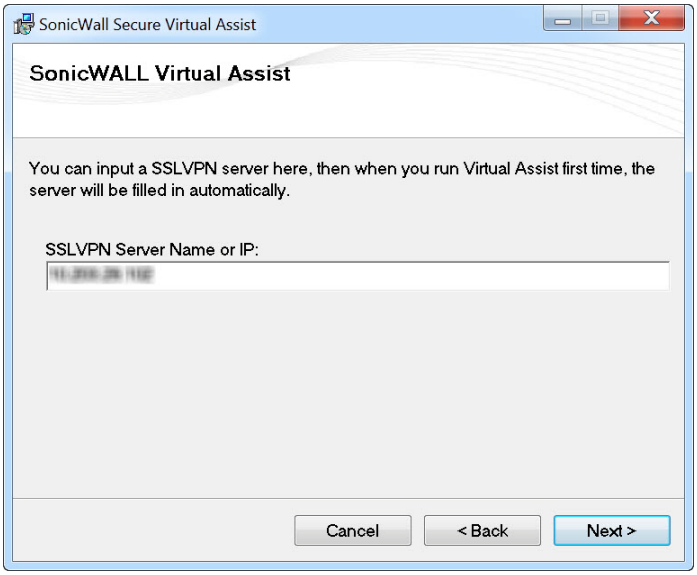
3 If the Virtual Assist plug-in is not installed, the File Download window displays, and Secure Virtual Assist attempts to automatically install. Click **Run** to launch the program directly, or click **Save** to save the installer file to your computer, and then manually launch it.



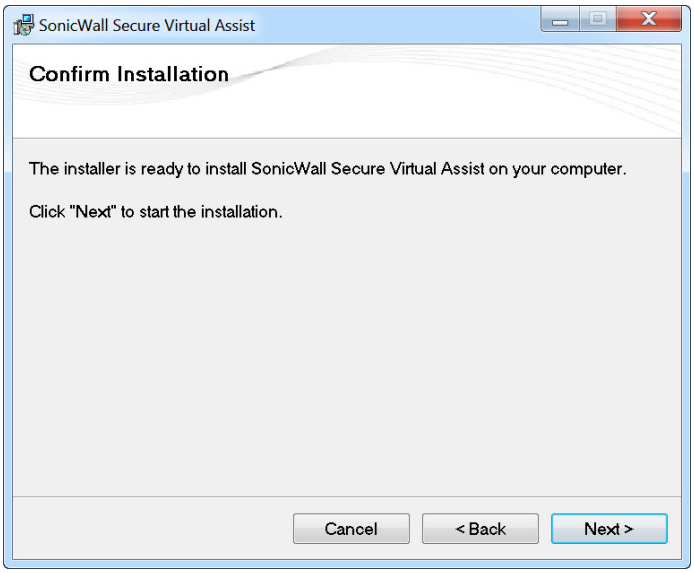
When downloading through IPv6, the File Download window displays IPv6 information.

4 A pop-up wizard asks if you would like to install Secure Virtual Assist as a standalone client. Click **Next** to begin the installation.

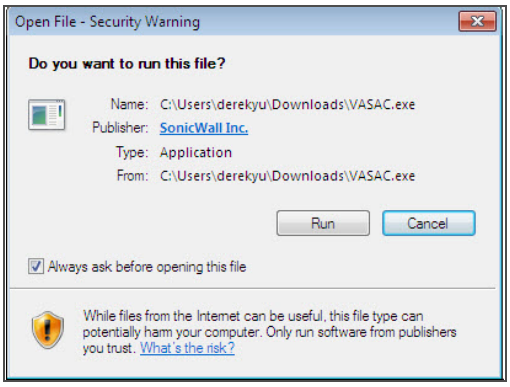
5 Enter an **SSLVPN Server Name or IP** in the space provided and click **Next**.



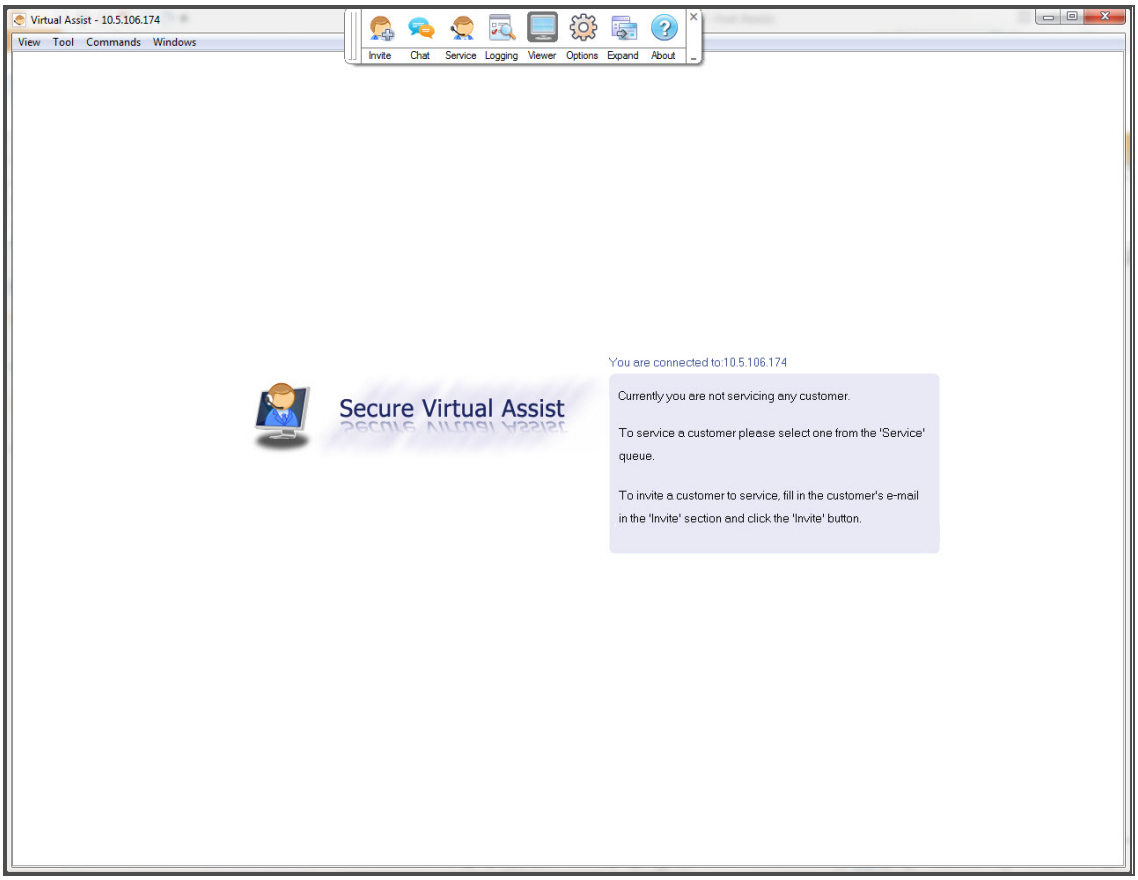
6 When you see the confirmation screen, the installer is ready to install SonicWall Inc. Secure Virtual Assist on your computer. Click **Next** to begin the installation.



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



8 The Secure Virtual Assist standalone application launches.



9 The technician is now ready to assist customers.

Performing Secure Virtual Assist Technician Tasks

NOTE: Secure Virtual Assist is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

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

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

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

- Inviting Customers by Email on page 58
- Assisting Customers on page 59
- Using the Secure Virtual Assist Taskbar on page 59
- Controlling the Secure Virtual Assist Display on page 61
- Request Full Control on page 61

Inviting Customers by Email

To invite a customer to a Secure Virtual Assist session by email:

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

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

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

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

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

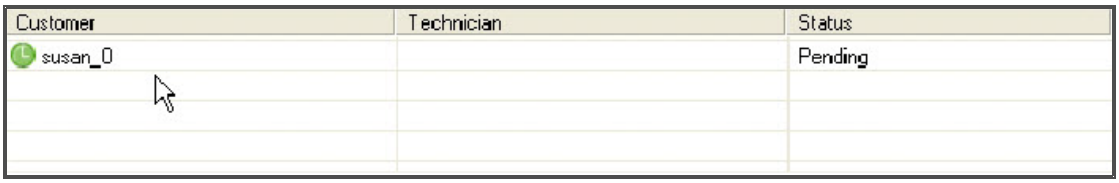
5 Click **Invite**. The customer receives an email with an HTML link to launch Secure Virtual Assist.

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

Assisting Customers

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

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



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

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

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

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

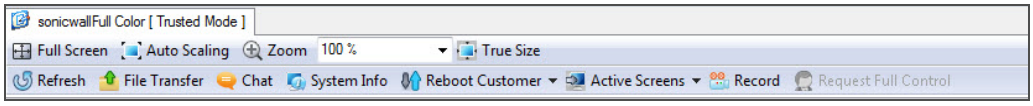
The customer has the following options during a Secure Virtual Assist session, each enabled after clicking the corresponding button.

- **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.

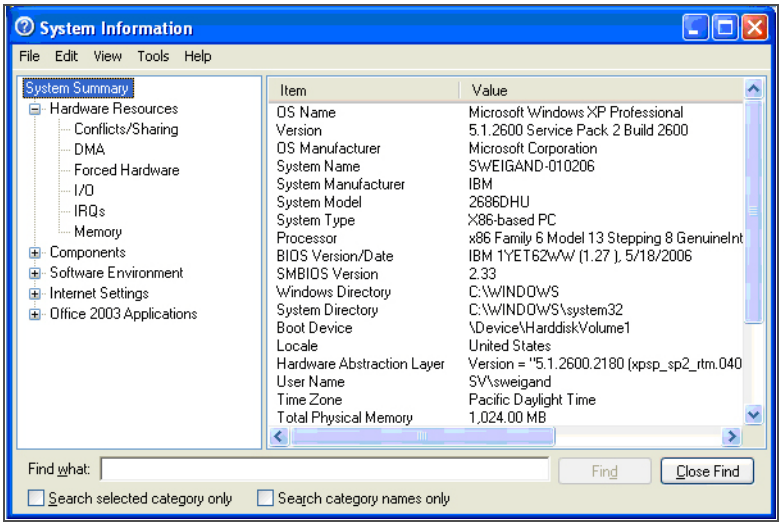
Using the Secure Virtual Assist Taskbar

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

In Windows, the taskbar contains the following buttons:

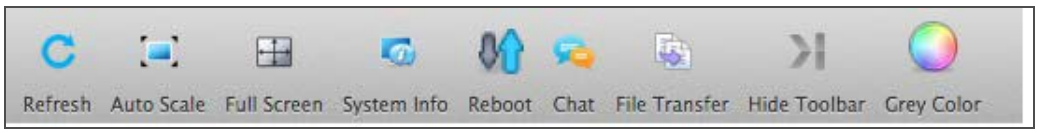


- **Full Screen** - Adjusts the screen to fill the entire window.
- **Auto Scaling** - Adjusts the screen to fit the window size.
- **Zoom** - Zooms the display to one of several presets or allows you enter a specific value.
- **True Size** - Zooms to 100 percent.
- **Refresh** - Refreshes the display of the customer's computer.
- **File Transfer** - Launches a window to transfer files to and from the customer's computer. see Using the Secure Virtual Assist File Transfer on page 62 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 Secure 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 is warned about and given the opportunity to deny the reboot.
- **Active Screens -** Switches to a second monitor if the customer's computer has more than one monitor configured.

In MacOS, the taskbar contains the following buttons:



- **Refresh** - Refreshes the display of the customer's computer.
- **System Info** -Displays detailed information about the customer's computer similar to that shown for a Windows computer.
- **Reboot** - Reboot the customer's computer. Unless you have Requested full control, the customer is warned about and given the opportunity to deny the reboot.

- **Chat** - Launches the text chat window to communicate with the customer. The technician can also use the dedicated chat window in the bottom left window of the Secure Virtual Assist application.
- **File Transfer** - Launches a window to transfer files to and from the customer's computer. see Using the Secure Virtual Assist File Transfer on page 62 for more information.
- **Hide Toolbar** - Hides the taskbar from view.
- **Gray Color** - Displays everything in grey monochrome

Controlling the Secure Virtual Assist Display

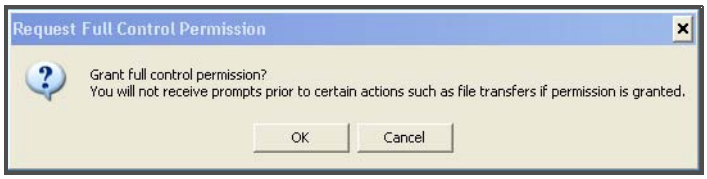
- **Full Screen** - Hides all of the Secure Virtual Assist toolbars and displays the customer's desktop on the technician's entire screen with the Secure Virtual Assist taskbar in the top left corner.

  If the Secure Virtual Assist taskbar does not 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 Secure Virtual Assist window.
- **Zoom** - Zooms the display to one of several presets or allows you enter a specific value.
- **True Size** - Zooms to 100 percent.

NOTE: A number of these options can be configured from the drop-down menus at the top of the Secure Virtual Assist application.

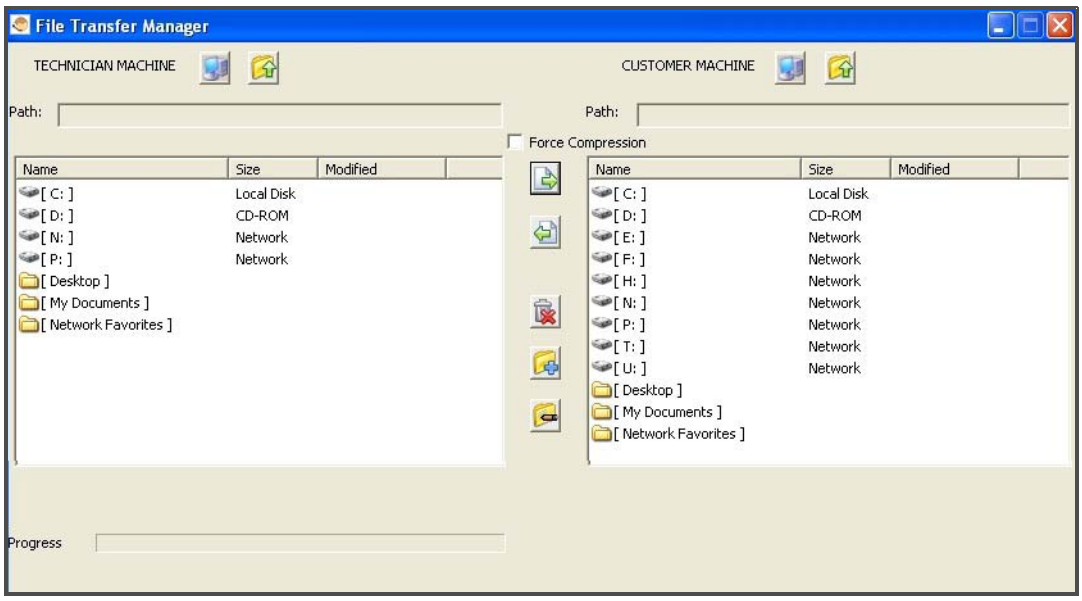
Request Full Control

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 appears on the customer's desktop.



Using the Secure Virtual Assist File Transfer

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



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

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

  NOTE: When deleting or 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 **Exit** to cancel a transfer in progress.

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

Enabling a System for Secure Virtual Access

NOTE: Secure Virtual Access is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

If Secure Virtual Access has been enabled on the Virtual Assist tab on the **Portals > Portals** page of the Secure Mobile Access management interface, users should see a link on the portal to set-up a system for Secure Virtual Access. To enable Secure Virtual Access within the Secure Mobile Access management interface, see Configuring Per-Portal Virtual Assist Settings on page 151.

To configure Secure Virtual Access on a system:

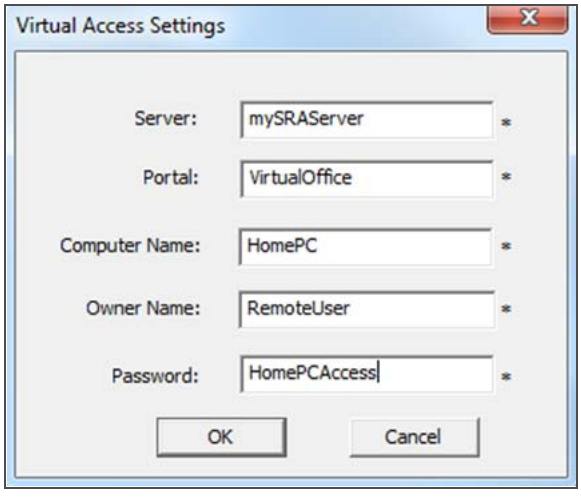
1 Log in to the portal through the system you wish to configure for Secure Virtual Access and click the **Virtual Access** link.

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

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

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

- **Server:** This should be the name or IP address of the appliance the technician normally accesses the Virtual Office from outside the management interface (Do not include “https://”).
- **Portal:** The name of the portal the technician would normally log in to.
- **Computer Name:** This is an identifier for the system to help differentiate between other systems that might 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.



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 **Secure Virtual Assist > Status** page within the management interface. Upon double-clicking the system listing, the

technician is prompted to provide the password established during system set-up to gain Secure Virtual Access to the system.

Ending Secure Virtual Access Mode

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

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

NOTE: For tasks and information on using Secure Virtual Assist as an end-user, refer to the *Secure Mobile Access User's Guide*.

Secure Virtual Meeting Overview

NOTE: Secure Virtual Meeting is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

This section provides an introduction to the Secure Virtual Meeting feature. This section contains the following topics:

What is Secure Virtual Meeting?

NOTE: Secure Virtual Meeting is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

Secure Virtual Meeting is a web-based management interface for the SMA 400, SRA 4600, and SMA 500v Virtual Appliance. Secure Virtual Meeting allows multiple users to view a desktop and interactively participate in a meeting from virtually anywhere with an Internet connection. Secure Virtual Meeting is similar to the one-to-one desktop sharing provided by Virtual Assist except multiple users can share a desktop.

Benefits of Secure Virtual Meeting

NOTE: Secure Virtual Meeting is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

Secure Virtual Meeting provides the following benefits:

- **Secure connections** - 256-bit AES SSL encryption of the data by the SMA/SRA appliance provides a secure environment for the data and assists in the effort to be compliant with regulations like Sarbanes-Oxley and HIPAA.
- **Time and cost savings** - Secure Virtual Meeting eliminates the need to visit customer sites and reduces the average time-to-resolution of support calls.
- **Educational tool** - Trainers and support staff can use Secure Virtual Meeting to remotely show customers how to use programs and tools.
- **Configurable environment with multiple functions** - Meeting parameters can be configured for specific meetings, in addition to meeting configurations that apply to all virtual meetings.

- **Meeting functions** - Meeting attendees can complete several functions, such as polling meeting attendees, text chatting, and switching who shares their desktop or controls the meeting.

User Roles

NOTE: Secure Virtual Meeting is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

Secure Virtual Meeting has several user roles:

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

    Only the Host can control the Host System, unless the Host grants permission when a Participant requests control. The Host can also give control to any Participant by selecting the Participant from the Meeting Members list. Only one Participant can control the Host System at any one time. When a Participant takes control of the Host System, he loses control as soon as the Host moves his mouse pointer on the screen. The meeting control permission state is visible to all Participants while in the lobby.
- **Participant** (User with credentials to join the meeting) - A Participant must enter a meeting code before they can join a meeting. The code required to join the meeting is determined by the Coordinator prior to the meeting. After joining a meeting, the Participant can view the shared desktop and chat with another attendee privately or type a message in the Chat window that is visible to all attendees. A Participant becomes the Assistant if selected by the Coordinator or by an Assistant who has the required privilege.
- **View-only Participant** (User with limited meeting capabilities) - The Coordinator can designate any Participant as a View-only Participant. A View-only Participant cannot be assigned any privileges nor become an Assistant or Host.

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

How Does a Secure Virtual Meeting Work?

NOTE: Secure Virtual Meeting is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

See the following sections:

- Configuring Secure Virtual Meeting on page 66
- Performing Coordinator Tasks on page 66
- Performing Participant Tasks on page 68

Configuring Secure Virtual Meeting

NOTE: Secure Virtual Meeting is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

Secure Virtual Meeting configuration and management tasks are done through the Secure Mobile Access web-based management interface and consist of the following:

- Status
- Settings
- Log
- Licensing

These tasks are explained in detail in Secure Virtual Meeting Overview on page 64 and the Secure Virtual Meeting Feature Module.

Performing Coordinator Tasks

NOTE: Secure Virtual Meeting is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

The Virtual Meeting Coordinator completes the following tasks:

Virtual Meeting Coordinator tasks

Coordinator Tasks	Description
Logging In	Log in from a Virtual Meeting client using Secure Mobile Access credentials.
Setting Up a Meeting	Set up a meeting by scheduling a time and creating a meeting code that allows meeting members to join the meeting.
Performing Lobby Functions	Access various meeting functions in the lobby before or during a meeting. See Performing Lobby Functions on page 67.
Controlling Roles	Control what meeting members can do and appoint an Assistant to help facilitate the meeting.
Revising Meeting Settings	Set up a proxy or modify login profiles for meetings.
Logging Actions and Messages	Review a log of actions that occurred and view any warning or error message details that might require attention.
Using the Control Menu During a Meeting	Access functions available while a meeting is active. See Using the Control Menu during a Meeting on page 67.
Creating Email Invites	Invite meeting members through email before or during a meeting.
Polling	Create a poll for attendees to participate in.

Virtual Meeting Coordinator tasks (Continued)

Coordinator Tasks	Description
Viewing Polling Feedback	View the feedback submitted for a poll.
Text Chatting	Chat with everyone or specific individuals in a meeting.

Performing Lobby Functions

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

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

Clicking **Stop Meeting** stops the meeting. Only the Coordinator and Assistant can end the meeting.

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

Clicking **Invite** sends an email invitation to Participants. Only the Coordinator and Assistant can invite Participants.

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

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

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

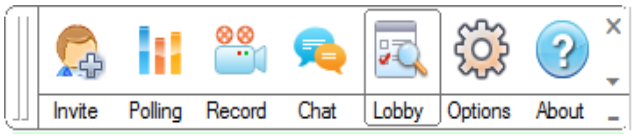
Clicking **Start Sharing** shares the Host desktop with all Participants in the meeting. Sharing is only available during a meeting.

Clicking **Stop Sharing** stops sharing the Host System desktop. Only the Host can stop sharing and only while in the sharing state (after Start Sharing has been selected).

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

Using the Control Menu during a Meeting

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



Invite is available for the Coordinator or Assistants with invite permission. It opens the invite dialog if the lobby is not open.

Polling is available for the Coordinator or Assistants with polling permission. It opens the polling dialog.

Chat is available for all Participants, including View-only Participants. It opens a chat dialog if the lobby is not open.

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

 **Options** opens the Meeting Settings window and is available for all Participants.

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

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

Performing Participant Tasks

NOTE: Secure Virtual Meeting is being deprecated. For legacy support, call SonicWall Customer Support for assistance.

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

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

Web Application Firewall Overview

This section provides an introduction to the Web Application Firewall feature. This section contains the following topics:

What is Web Application Firewall?

Web Application Firewall is subscription-based software that runs on the SMA/SRA appliance and protects Web applications running on servers behind the appliance. Web Application Firewall also provides real-time protection for resources such as HTTP(S) bookmarks, Citrix bookmarks, offloaded Web applications, and the Secure Mobile Access management interface and user portal that run on the SMA/SRA 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. Secure Mobile Access Web Application Firewall protects against these top ten, defined as follows:

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.
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 that then forces the victim's browser to do 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 complete unauthorized operations by accessing those URLs directly.

Slowloris Protection

In addition to the top ten threats listed previously, 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. After the attack stops or the session is closed, the Web server logs can 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 How Does Web Application Firewall Work? on page 71.

Offloaded Web Application Protection

Web Application Firewall can also protect an offloaded Web application that is a special purpose portal created to provide seamless access to a Web application running on a server behind the SMA/SRA 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 Inc. advanced authentication features such as One Time Password, Two-factor Authentication, and Single Sign-On apply to the offloaded host.

Application Profiling

Application Profiling (Phase 1) allows the administrator to generate custom rules in an automated manner based on a trusted set of inputs. This is a highly effective method of providing security to Web applications because it develops a profile of what inputs are acceptable by the application. Everything else is denied, providing positive security enforcement. This results in fewer false positives than generic signatures that adopt a negative security model. When the administrator places the device in learning mode in a staging environment, the SMA/SRA appliance learns valid inputs for each URL accessed by the trusted users. At any point during or after the learning process, the custom rules can be generated based on the “learned” profiles.

Rate Limiting for Custom Rules

You can track the rate at which a custom rule, or rule chain, is being matched. This is extremely useful to block dictionary attacks or brute force attacks. The action for the rule chain is triggered only if the rule chain is matched as many times as configured.

Cookie Tampering Protection

Cookie Tampering Protection is an important item in the Payment Card Industry Data Security Standard (PCI DSS) section 6.6 requirements and part of the Web Application Firewall evaluation criteria that offers strict security for cookies set by the backend Web servers. Various techniques such as encryption and message digest are used to prevent cookie tampering. See Configuring Cookie Tampering Protection Settings on page 295 for additional information.

Credit Card and Social Security Number Protection

Credit Card/SSN protection is a Data Loss Prevention technique that ensures that sensitive information, such as credit card numbers and Social Security numbers are not leaked within Web pages. After such leakage is detected, the administrator can choose to mask these numbers partially or wholly, present a configurable error page, or simply log the event. See Configuring Information Disclosure Protection on page 297 for additional information.

Web Site Cloaking

Web Site Cloaking prevents guessing the Web server implementation and exploiting its vulnerabilities. See Configuring Web Site Cloaking on page 296 for additional information.

PDF Reporting for WAF Monitoring and PCI DSS 6.5 and 6.6 Compliance

PDF reporting is introduced for Web Application Firewall Monitoring and PCI DSS 6.5 and 6.6 Compliance. You can generate the reports on the **Web Application Firewall > Status** page. The time line for generating the data published in the reports is configurable on the **Web Application Firewall > Monitoring** page.

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. Secure Mobile Access uses SSL encryption to encrypt data between the Web Application Firewall and the client. Secure Mobile Access 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 because of 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 SMA/SRA appliance.

Deploying Web Application Firewall at the SMA/SRA 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 that improves the proxy performance and functionality.

There are several benefits of integrating Web Application Firewall with SMA/SRA appliances. Firstly, identity-based policy controls are core to Web Application Firewall and this is easily achievable using Secure Mobile Access technology. Secondly, there are lower latencies because of the existing hardware-based SSL offloading. Most importantly, SMA/SRA 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 an SMA/SRA appliance provides a convenient, cost-effective solution.

Web Application Firewall is easy to configure in the Secure Mobile Access management interface. The administrator can configure Web Application Firewall settings globally, by attack priority, and on a per-signature basis. After custom configuration settings or exclusions are in place, you can disable Web Application Firewall without losing the configuration, allowing you to complete 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 Secure Mobile Access management interface. Web Application Firewall can be configured to log or block detected attacks arriving from the Internet.

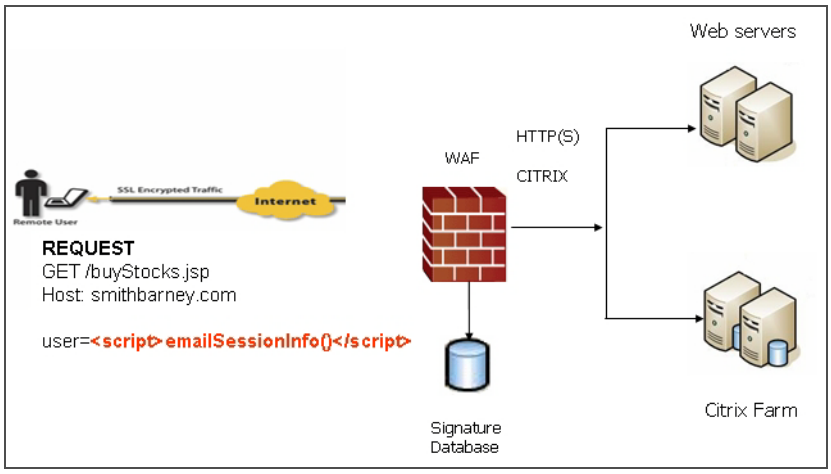
The following sections describe how Web Application Firewall and SMA/SRA appliances prevent attacks such as Slowloris or those listed in the OWASP top ten, how Web Application Firewall protects against information disclosure, and how other features work:

- How are Signatures Used to Prevent Attacks? on page 72
- How is Cross-Site Request Forgery Prevented? on page 74
- How is Information Disclosure Prevented? on page 74
- How are Broken Authentication Attacks Prevented? on page 75
- How are Insecure Storage and Communications Prevented? on page 75

How are Signatures Used to Prevent Attacks?

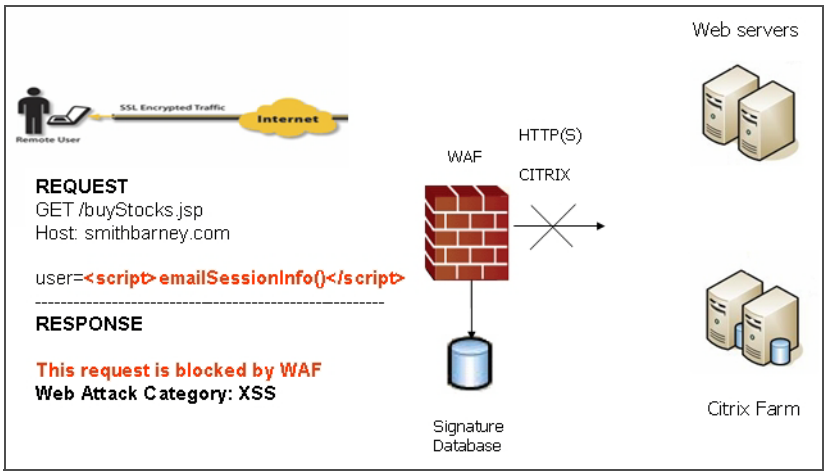
For Cross Site Scripting, Injection Flaws, Malicious File Execution, and Insecure Direct Object Reference vulnerabilities, the Web Application Firewall feature uses a black list of signatures that are known to make Web applications vulnerable. New updates to these signatures are periodically downloaded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

How signatures are used to prevent attacks



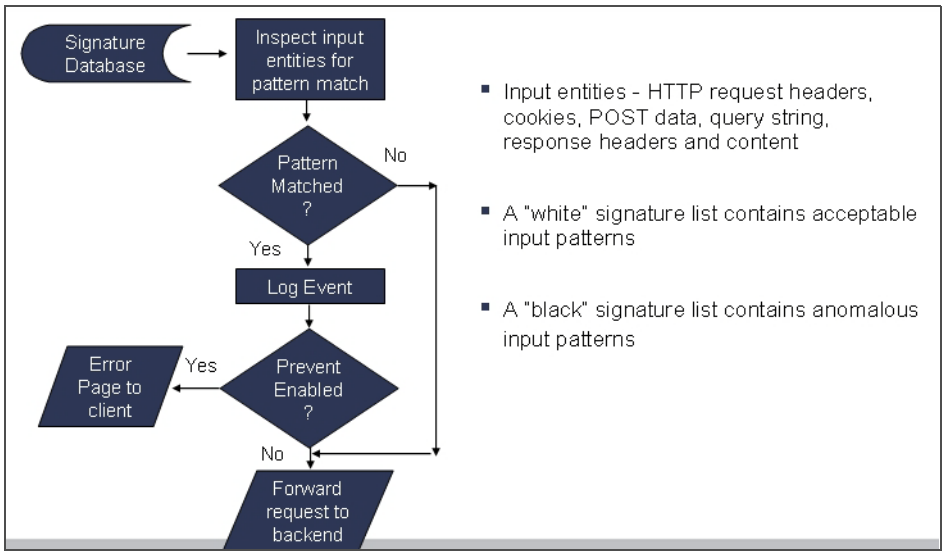
When input arrives from the Internet, Web Application Firewall inspects HTTP/HTTPS request headers, cookies, POST data, query strings, response headers, and content. It compares the input to both a black list and a white list of signatures. If pattern matching succeeds for any signature, the event is 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.

What happens when no signature is matched



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

Web Application Firewall process



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

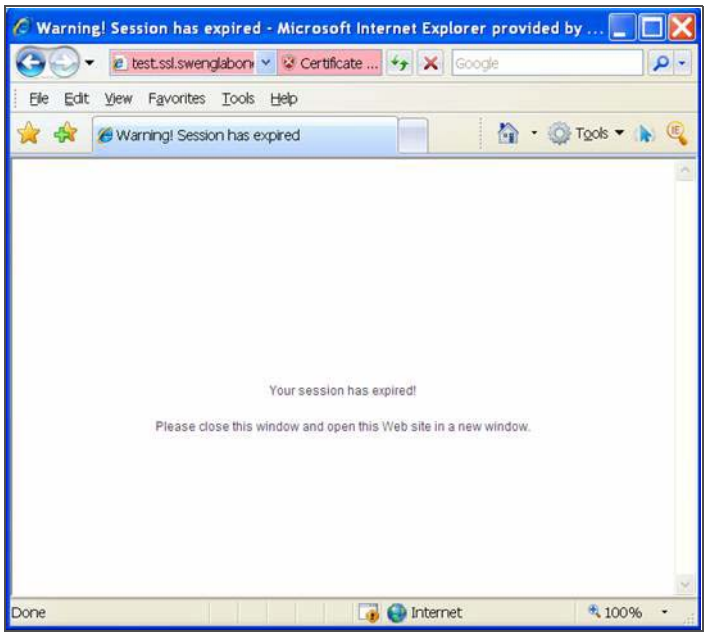
This page is customizable under **Web Application Firewall > Settings** in the Secure Mobile Access management interface. Some administrators might want to customize the HTML contents of this page. Others might not want to present a user friendly page for security reasons. Instead, they might prefer 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 can 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 done for Application Offloading.

If authentication is enforced for the portal, then the user is redirected to the login page for the portal.



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.

Web Application Firewall protects against inadvertent disclosure of credit card and Social Security numbers (SSN) in HTML Web pages.

NOTE: Only text or HTML pages, and only the first 512K bytes are inspected for credit card or SSN disclosure.

Web Application Firewall can identify credit card and SSN numbers in various formats. For example, a SSN can be specified as XXX XX XXXX or XXX-XX-XXXX. Web Application Firewall attempts to eliminate false-positives by

filtering out formats that do not conform to the credit card or SSN specification. For example, credit cards follow the Luhn's algorithm to determine if an n-digit number could be a credit card number or not.

The administrator can set an appropriate action, such as detect (log), prevent, or just mask the digits that can reveal the user identity. Masking can be done fully or partially, and you can select any of the following characters for masking: #, *, -, x, X, ., !, $, and ?. The resulting masked number is similar to the appearance of credit card numbers printed on an invoice.

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. Secure Mobile Access 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 in to 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. Secure Mobile Access also supports HTTPS with the backend Web server.

How is Access to Restricted URLs Prevented?

Secure Mobile Access 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 an SMA/SRA security appliance, that limits, buffers, or proxies HTTP requests. Web Application Firewall uses a rate-limiter to thwart Slowloris HTTP Denial of Service attacks.

What Type of PCI Compliance Reports Are Available?

Payment Card Industry Data Security Standard (PCI DSS) 6.5 (Version 2.0) and PCI DSS 6.6 (Version 1.2) are covered in PCI reporting. The administrator can configure Web Application Firewall to satisfy these PCI requirements.

You can generate and download the PCI report file on the **Web Application Firewall > Status** page.

NOTE: This is not an official PCI Compliance report. It is for your self-assessment only.

In the report cover, the following information is displayed:

- The model, serial number, and firmware version of the appliance
- The user name of the person who downloaded the report, displayed as the author of the report
- Time when the report was generated

The following is an example:

Model: SRA 4200
Serial Number: 0017C552EE24
Firmware Version: SonicOS SSL-VPN 6.0.0.0-11sv
Author: admin
Time: 2012/04/03 12:24:37

Two tables are dynamically generated in the PCI compliance report to display the status of each PCI requirement. The format of the table is shown in the example that follows:

PCI DSS 6.5 Compliance Report

PCI DSS 6.5 Requirements	Status	Comments
1. Injection flaws, particularly SQLinjection. Also consider OS CommandInjection, LDAP and XPath injectionflaws as well as other injection flaws.	Partially Satisfied	Please update your WAF signatures.

The first column describes the PCI requirement.

The second column displays the status of the PCI requirement under current Web Application Firewall settings. There are four possible values for the status, distinguished by color.

- Satisfied (Green)
- Partially Satisfied (Orange)
- Unsatisfied (Red)
- Unable to determine (Black)

The third column provides comments and details explaining the status rating. If the status is Satisfied, no comments are provided.

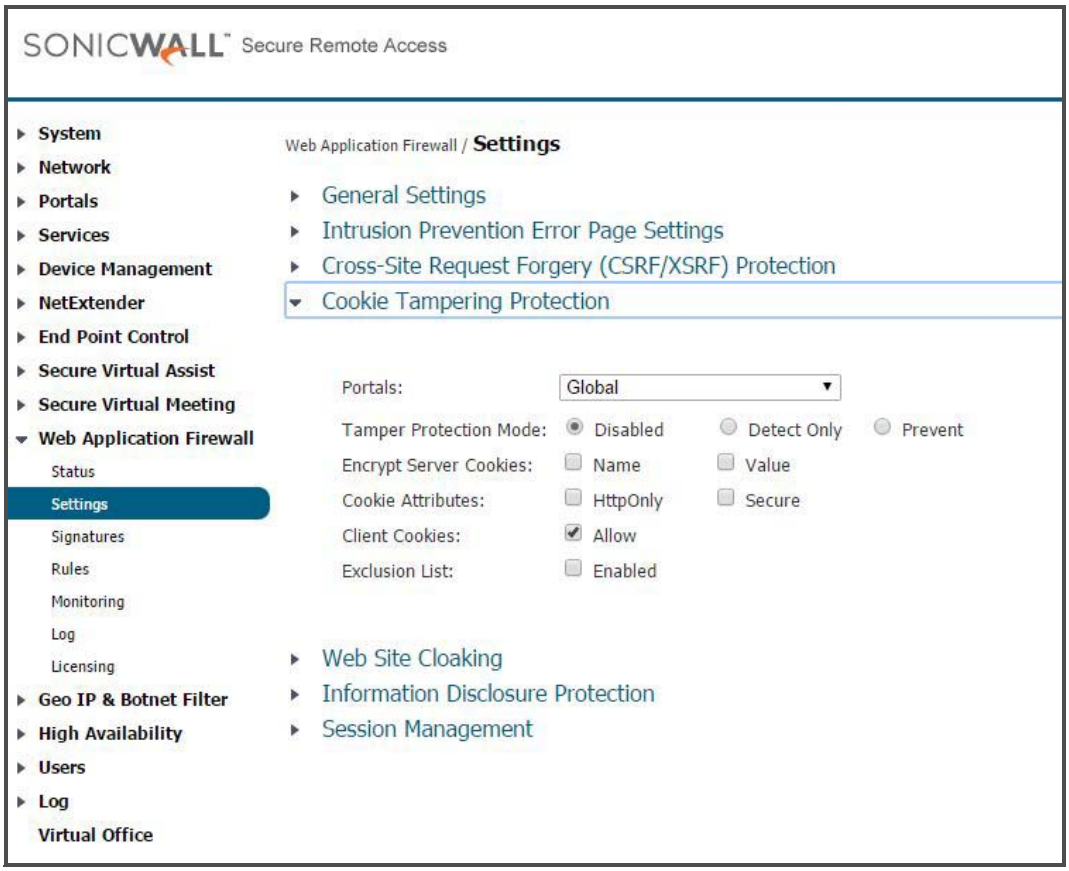
How Does Cookie Tampering Protection Work?

SMA/SRA appliances protect important server-side cookies from tampering.

There are two kinds of cookies:

- **Server-Side Cookies** – These cookies are generated by backend Web servers. They are important and have to be protected. They have optional attributes like Path, Domain, Secure, and HttpOnly.
- **Client-Side Cookies** – These cookies are created by client side scripts in user browsers. They are not safe, and can be easily tampered with.

This feature is found on the **Web Application Firewall > Settings** page.



This page contains the following options:

Portals – A list of all application offloading portals. Each portal has its own settings. The item **Global** is the default setting for all portals.

Tamper Protection Mode – Three modes are available:

- **Prevent** – Strip all the tampered cookies and log them.
- **Detect only** – Log the tampered cookies only.
- **Inherit Global** – Use the global setting for this portal.

Encrypt Server Cookies – Choose to encrypt name and value separately. This affects client-side script behavior because it makes cookie names or values unreadable. Only server-side cookies are encrypted by these options.

Cookie Attributes – The attributes *HttpOnly* and *Secure* are appended to server-side cookies if they are enabled.

The attribute *HttpOnly* prevents the client-side scripts from accessing the cookies that is important in mitigating attacks such as Cross Site Scripting and session hijacking. The attribute *Secure* ensures that the cookies are transported only in HTTPS connections. Both together add a strong layer of security for the server-side cookies.

NOTE: By default, the attribute Secure is always appended to an HTTP connection even if Cookie Tampering Protection is disabled. This behavior is a configurable option, and can be turned off.

Allow Client Cookies – The Allow Client Cookies option is enabled by default. In Strict mode, the Allow Client Cookies option is disabled. When disabled, client-side cookies are not allowed to be sent to the backend systems. This option does not affect server-side cookies.

Exclusion List – If the Exclusion List is enabled and contains a cookie, the cookie is passed as usual and is not protected. You can exclude server-side cookies and client-side cookies.

Exclusion list items are case sensitive, and in the format 'CookieName@CookiePath.' Cookies with the same name and different paths are treated as different cookies. 'CookiePath' can be left empty to represent any path.

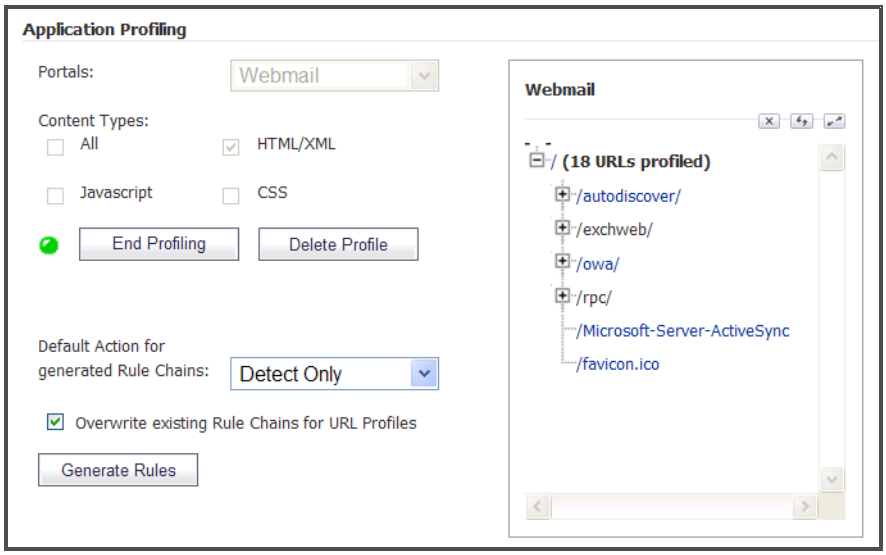
Import Global – Application Offloading portals can import the Global exclusion list.

How Does Application Profiling Work?

The administrator can configure application profiling on the **Web Application Firewall > Rules** page. Application profiling is completed independently for each portal and can profile multiple applications simultaneously.

After selecting the portal, you can select the type of application content that you want to profile. You can choose **HTML/XML**, **JavaScript**, **CSS**, or **All** that includes all content types such as images, HTML, and CSS. HTML/XML content is the most important from a security standpoint, because it typically covers the more sensitive Web transactions. This content type is selected by default.

Then the SMA/SRA appliance is placed in learning mode by clicking **Begin Profiling** (the button then changes to **End Profiling**). The profiling should be done while trusted users are using applications in an appropriate way. The Secure Mobile Access records inputs and stores them as URL profiles. The URL profiles are listed as a tree structure on the **Web Application Firewall > Rules** page in the Application Profiling section.



Only the URLs presented as hyperlinks are accessible URLs on the backend server. You can click on the hyperlink to edit the learned values for that URL if the values are not accurate. You can then generate rules to use the modified URL profile.

The SMA/SRA appliance learns the following HTTP Parameters:

- Response Status Code
- Post Data Length – The Post Data Length is estimated by learning the value in the Content-Length header. The maximum size is set to the power of two that is closest to and higher than this value. This accommodates the amount of memory that could have been allocated by the backend application. For example, for a Content Length of 65, the next power of two greater than 65 is 128. This is the limit configured in the URL profile. If the administrator determines that this is not accurate, the value can be modified appropriately.
- Request Parameters – This is the list of parameters that a particular URL can accept.

When an adequate amount of input has been learned, you can click **End Profiling** and are ready to generate the rules from the learned input. You can set one of the following as a default action for the generated rule chains:

- **Disabled** – The generated rules are disabled rather than active.
- **Detect Only** – Content triggering the generated rule are detected and logged.
- **Prevent** – Content triggering the generated rule are blocked and logged.

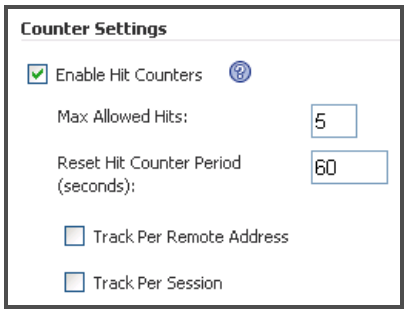
If a rule chain has already been generated from a URL profile in the past, then the rule chain are overwritten only when **Overwrite existing Rule Chains for URL Profiles** is selected. When you click **Generate Rules**, the rules are generated from the URL profiles. If a URL profile has been modified, those changes are incorporated.

How Does Rate Limiting for Custom Rules Work?

The administrator can configure rate limiting when adding or editing a rule chain from the **Web Application Firewall > Rules** page. When rate limiting is enabled for a rule chain, the action for the rule chain is triggered only when the number of matches within a configured time period is above the configured threshold.

This type of protection is useful in preventing Brute Force and Dictionary attacks. An example rule chain with a Rule Chain ID of 15002 is available in the Secure Mobile Access management interface for administrators to use as reference.

The associated fields are exposed when **Enable Hit Counters** is selected at the bottom of the **New Rule Chain** or **Edit Rule Chain** screen.



After a rule chain is matched, Web Application Firewall keeps an internal counter to track how many times the rule chain is matched. The **Max Allowed Hits** field contains the number of matches that must occur before the rule chain action is triggered. If the rule chain is not matched for the number of seconds configured in the **Reset Hit Counter Period** field, then the counter is reset to zero.

Rate limiting can be enforced per remote IP address or per user session or both. **Track Per Remote Address** enables rate limiting based on the attacker's remote IP address.

Track Per Session enables rate limiting based on the attacker's browser session. This method sets a cookie for each browser session. Tracking by user session is not as effective as tracking by remote IP if the attacker initiates a new user session for each attack.

The **Track Per Remote Address** option uses the remote address as seen by the SMA/SRA appliance. In the case where the attack uses multiple clients from behind a firewall that is configured with NAT, the different clients effectively send packets with the same source IP address and is counted together.

Navigating the Management Interface

The following sections describe how to navigate the Secure Mobile Access management interface:

Browser Requirements

The following sections describe the browser requirements for the Secure Mobile Access management interface.

Topics:

Browser Requirements for the Administrator

The following Web browsers and operating systems support the Secure Mobile Access web-based management interface and the user portal, **Virtual Office**.

Secure Mobile Access Administrator Browser Requirements

Browser	Operating System	
Internet Explorer 9	• Windows 7	
Internet Explorer 10	• Windows 10	
Internet Explorer 11	• Windows 10	
Mozilla Firefox (latest version)	• Windows Vista • Windows 10 • Windows 7	• Linux • MacOS X
Google Chrome	• Windows Vista • Windows 10 • Windows 7	• Linux • MacOS X

To configure an SMA/SRA appliance using the Secure Mobile Access web-based management interface, an administrator must use a Web browser with Java, JavaScript, ActiveX, cookies, pop-ups, TLS 1.0, TLS 1.1, and TLS 1.2 enabled. Java is only required for various aspects of the Secure Mobile Access Virtual Office, not the Secure Mobile Access management interface.

Browser Requirements for the End User

The following is a list of Web browser and operating system support for various Secure Mobile Access protocols including NetExtender and various Application Proxy elements. Minimum browser version requirements are shown for Windows, Windows Vista, Windows 7, Linux, and MacOS.

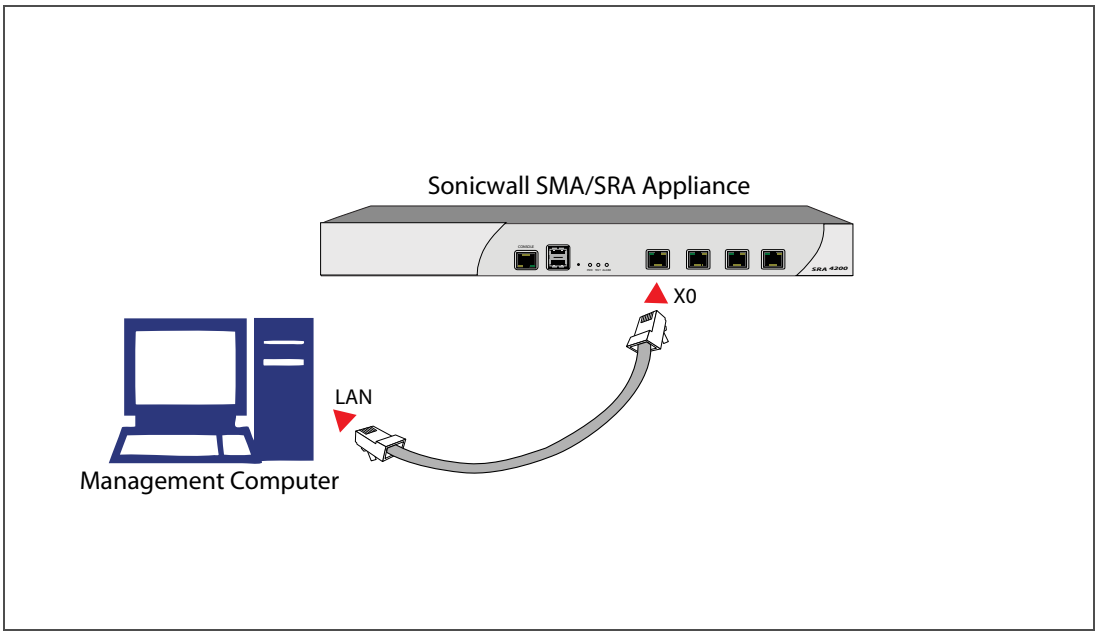
The following table provides specific browser requirements for the Secure Mobile Access End User Interface:

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

Management Interface Introduction

The following is an overview of basic setup tasks that connect you to the Secure Mobile Access web-based management interface of the SMA/SRA appliance. For more detailed information on establishing a management session and basic setup tasks, refer to the Getting Started Guide for your platform. To access the Secure Mobile Access web-based management interface of the SonicWall SMA/SRA appliance:

1 Connect one end of a CAT-6 cable into the **X0** port of your SMA/SRA appliance. Connect the other end of the cable into the computer you are using to manage the SMA/SRA appliance.



2 Set the computer you use to manage your SMA/SRA 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 Getting Started Guide for your model.

NOTE: For configuring the SMA/SRA appliance using the Secure Mobile Access web-based management interface, a Web browser supporting Java and HTTP uploads, such as Internet Explorer 9 or higher, Firefox 16.0 or higher, or Chrome 22.0 or higher is recommended. Users need to use IE 9 or higher, supporting JavaScript, Java, cookies, SSL and ActiveX in order to take advantage of the full suite of Secure Mobile Access applications.

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

4 A security warning can appear. Click **Yes** to continue.

5 The **Secure Mobile Access 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 **Login**.

NOTE: The number and duration of login attempts can be controlled by the use of the Secure Mobile Access auto-lockout feature. For information on configuring the auto-lockout feature, refer to Configuring Login Security on page 116.

When you have successfully logged in, you 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 done 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**, **Secure 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.

Help in the upper right corner of the management interface opens a separate browser window that displays Secure Mobile Access Help.

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

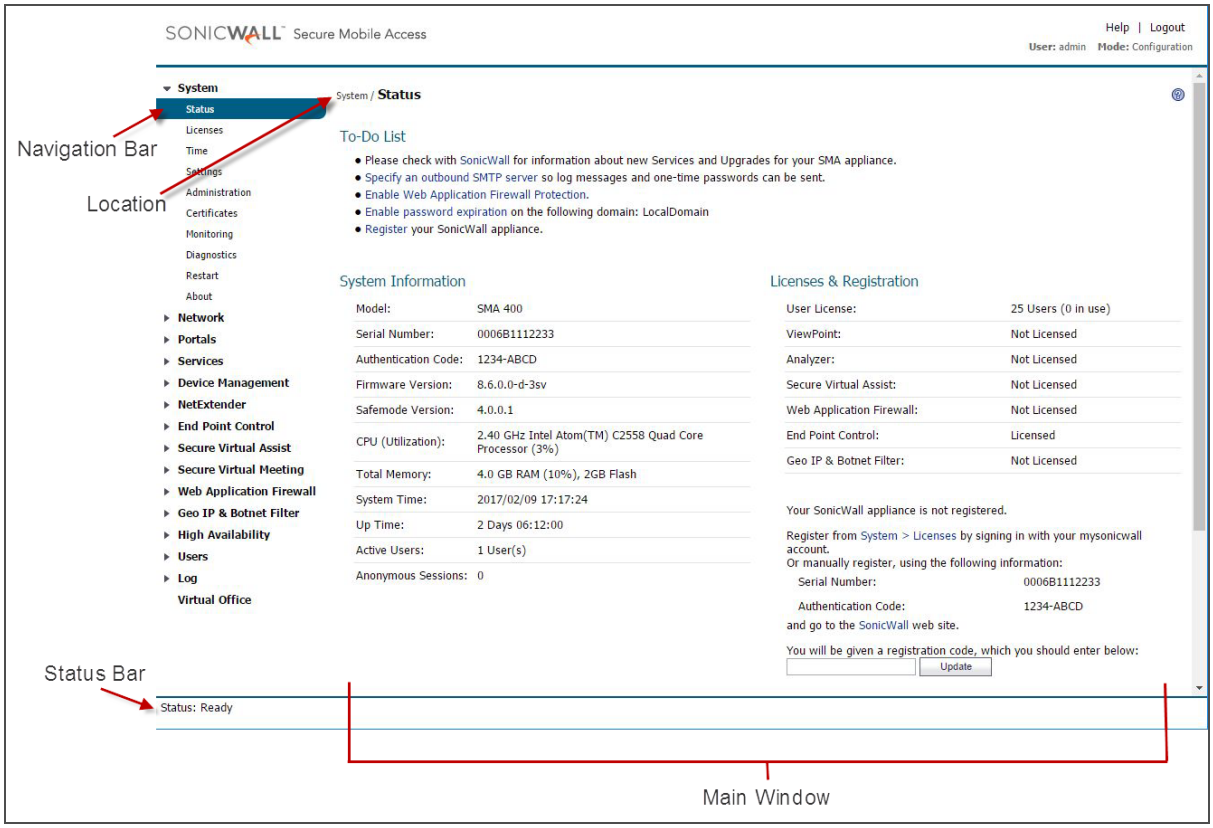
Navigating the Management Interface

The Secure Mobile Access web-based management interface allows the administrator to configure the SMA/SRA appliance. The Secure Mobile Access management interface contains top level, read-only windows and configuration windows:

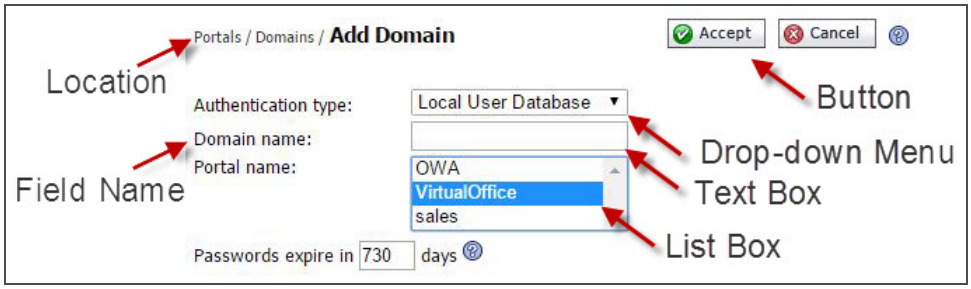
- **Windows** - Displays information in a read-only format.
- **Configuration windows** - Enables administrator interaction to add and change values that characterize objects. For example, IP addresses, names, and authentication types.

The following figures show sample windows in the Secure Mobile Access web-based management interface. Note the various elements of a standard Secure Mobile Access interface window.

System > Status Page



The following is a sample configuration window:



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

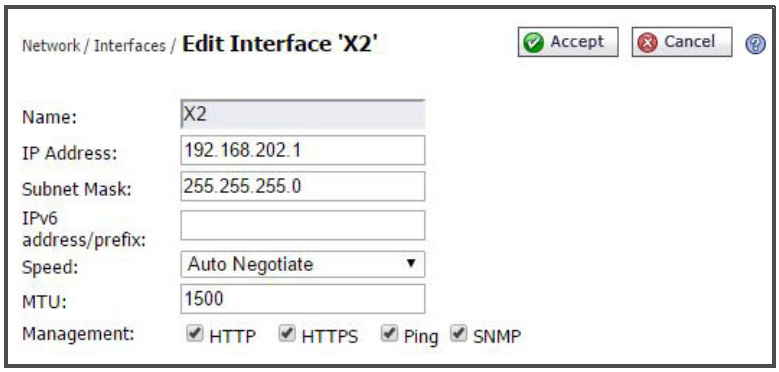
Status Bar

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

Accepting Changes

Click **Accept** 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 within the Secure Mobile Access management interface, **Accept** is still available at the top right corner of the window.



Navigating Tables

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

Log > View

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 SMA/SRA appliance.

NOTE: Restarting takes approximately two minutes and causes all users to be disconnected.

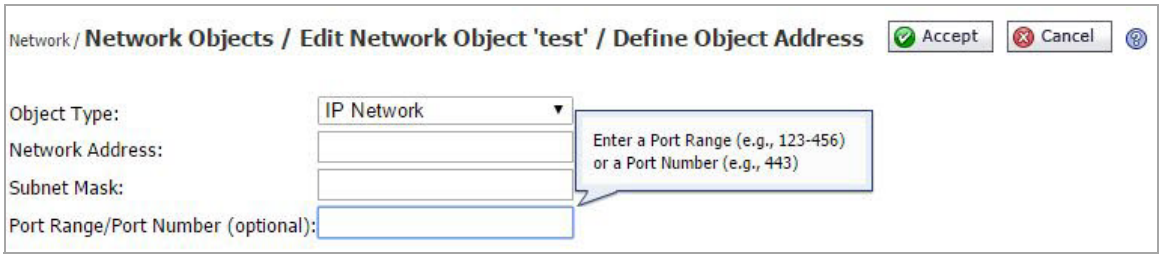
Common Icons in the Management Interface

The following icons are used throughout the Secure Mobile Access 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 Secure Mobile Access management interface display popup tooltips with configuration information when the mouse cursor hovers over a check box, text field, or radio button. Some fields have a Help icon that provides a tooltip stating related requirements.



Getting Help

Help in the upper right corner of the Secure Mobile Access management interface opens a separate Web browser that displays the main Secure Mobile Access Help.

SMA/SRA appliances also include 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 SMA/SRA appliance online Help requires an active Internet connection.

Logging Out

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

When you click **Logout**, you are logged out of the Secure Mobile Access management interface and the Web browser is closed.

Navigation Bar

The Secure Mobile Access navigation bar is located on the left side of the Secure Mobile Access 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**, **Services**, **NetExtender**, **End Point Control**, **Secure Virtual Assist**, **Secure Virtual Meeting**, **Web Application Firewall**, **High Availability**, **Users**, **Log**, and **Virtual Office**.

Deployment Guidelines

This sections provides information about deployment guidelines for the SMA/SRA 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.

Concurrent tunnels supported based on appliance

Appliance Model	Maximum Concurrent Tunnels Supported	Recommended Number of Concurrent Tunnels
SMA 400	250	125
SMA 200	50	50
SRA 4600	500	100
SRA 1600	50	25
SMA 500v Virtual Appliance	50	50

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 SMA/SRA appliance.

Supported application and resource types

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

NetExtender	• Any TCP/IP based application including:
	  • Email access through native clients residing on the user's laptop (Microsoft Outlook, Lotus Notes, and so on.)
	  • 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 other SonicWall Inc. Products

The SMA/SRA appliance integrates with other SonicWall Inc. products, complementing the SonicWall Inc. NSA, SuperMassive (9000 Series) and TZ Series product lines. Incoming HTTPS traffic is redirected by a SonicWall Inc. firewall appliance to the SMA/SRA appliance. The SMA/SRA 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

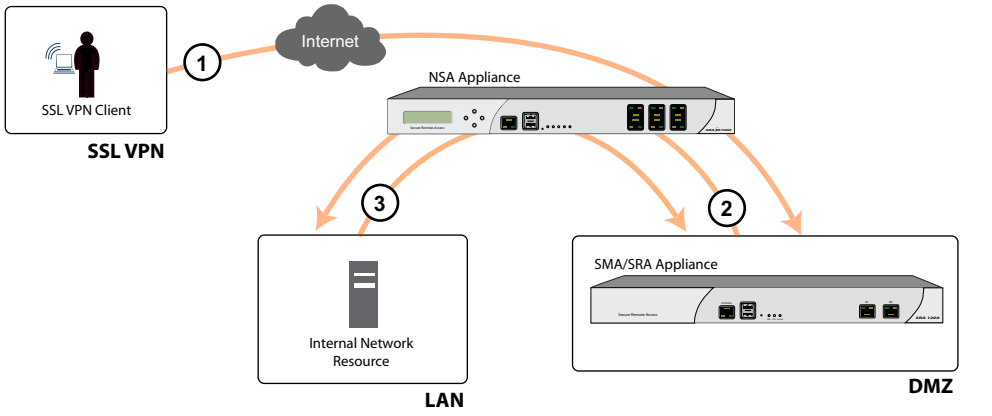
The SMA/SRA appliance is commonly deployed in tandem in one-armed mode over the DMZ or Opt interface on an accompanying gateway appliance, for example, a SonicWall Inc. network security appliance, such as a NSA 4600.

This method of deployment offers additional layers of security control plus the ability to use SonicWall Inc.'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. SonicWall Inc. recommends one-armed mode deployments over two-armed for the ease-of-deployment and for use in conjunction with UTM GAV/IPS for clean VPN.

As shown in the following figure, in one-armed mode the primary interface (X0) on the SMA/SRA appliance connects to an available segment on the gateway device. The encrypted user session is passed through the gateway to the SMA/SRA appliance (step 1). The SMA/SRA appliance decrypts the session and determines the requested resource. The Secure Mobile Access 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 SMA/SRA appliance through the gateway (step 3) where it is encrypted and returned to the client.

Sequence of Events in Initial Connection



1. X0 interface connects to available segment on gateway. Encrypted session passes to the SMA/SRA appliance.
2. SMA/SRA traffic traverses the gateway to reach internal network resource
3. The internal network resource returns content to the SMA/SRA appliance through the gateway.

For information about configuring the SMA/SRA appliance to work with third-party gateways, refer to Configuring the SMA/SRA Appliance with a Third-Party Gateway on page 454.

Two-armed Deployment

The SMA/SRA appliances also support two-armed deployment scenarios, using one external (DMZ or WAN side) interface and one internal (LAN) interface. However, two-armed mode introduces routing issues that need to be considered before deployment. The SMA/SRA appliance does not route packets across interfaces, as there are IP tables rules preventing that, and therefore cannot be used as a router or default gateway. Any other machines connected to an internal interface of the SMA/SRA appliance in two-armed mode would need to access the Internet or other network resources (DNS, NTP) through a different gateway.

If you have an internal router as well as an Internet router, you can use a two-armed deployment to leverage your internal router to access your internal resources.

Sample Scenario: Company A has resources and a number of subnets on their internal network, and they already have a robust routing system in place. With two-armed deployment of the SMA/SRA appliance, client requests destined for internal resources on the corporate network can be delivered to an internal router.

Part 2

Configuring Secure Mobile Access

- System Configuration
- Network Configuration
- Portals Configuration

3

System Configuration

This section provides information and configuration tasks specific to the **System** pages in the Secure Mobile Access web-based management interface, including registering your SMA/SRA appliance, setting the date and time, configuring system settings, system administration and system certificates.

Topics:

System > Status

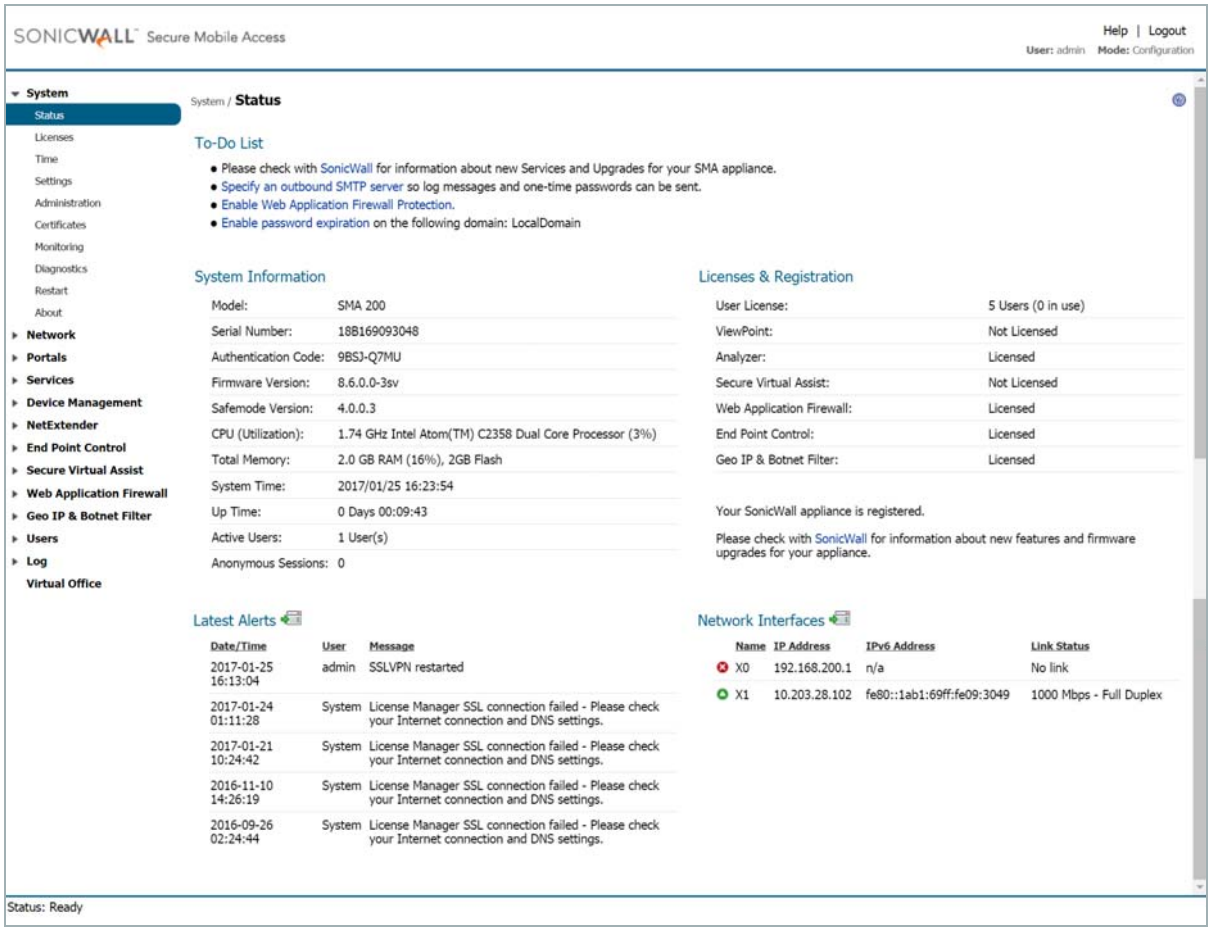
This section provides an overview of the **System > Status** page and a description of the configuration tasks available on this page.

System > Status Overview

The **System > Status** page provides the administrator with current system status for the SMA/SRA appliance, including information and links to help manage the SMA/SRA appliance and SonicWall Inc. Security Services

licenses. This section provides information about the page display and instructions to complete the configuration tasks on the **System > Status** page.

System > Status Page



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

- System Messages on page 91
- System Information on page 92
- Latest Alerts on page 92
- Licenses & Registration on page 92
- Network Interfaces on page 93

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 SMA/SRA appliance. The following information is displayed in this section:

System Information

Field	Description
Model	The type of SMA/SRA appliance.
Serial Number	The serial number or the MAC address of the SMA/SRA appliance.
Authentication Code	The alphanumeric code used to authenticate the SMA/SRA appliance on the registration database at <https://www.MySonicWall.com>.
Firmware Version	The firmware version loaded on the SMA/SRA appliance.
ROM Version	Indicates the ROM version. The ROM code controls low-level functionality of the appliance.
CPU (Utilization)	The type of the SMA/SRA appliance processor and the average CPU usage over the last 5 minutes.
Total Memory	The amount of RAM and Flash memory on the appliance.
System Time	The current date and time.
Up Time	The number of days, hours, minutes, and seconds, that the SMA/SRA appliance has been active since its most recent restart.
Active Users	The number of users who are currently logged into the Secure Mobile Access management interface of the SMA/SRA 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 SMA/SRA appliance. The status of your Analyzer, ViewPoint, Secure Virtual Assist, Spike License, Stateful High Availability (SMA 400, SRA 4600 only), 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 Registering Your SMA/SRA Appliance with System Status on page 93.

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 Inc. server, see Registering the SMA/SRA Appliance with System > Licenses on page 97.

Network Interfaces

The Network Interfaces section provides the administrator with a list of SMA/SRA appliance 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 Configuring Network Interfaces on page 95.

Registering Your SMA/SRA Appliance with System Status

Register with MySonicWall to get the most out of your SMA/SRA appliance. Complete the steps in the following sections to register.

Before You Register

Verify that the time, DNS, and default route settings on your SMA/SRA appliance are correct before you register your appliance. These settings are generally configured during the initial SMA/SRA appliance 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 Setting the Time on page 104, Configuring DNS Settings on page 133 and Configuring a Default Route for the SMA/SRA Appliance on page 136.

NOTE: You need a MySonicWall account to register the SonicWall SMA/SRA appliance.

Creating a MySonicWall Account from System > Licenses

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

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.

3 Follow the instructions to activate your MySonicWall account.

Registering with MySonicWall

There are two ways to register your SMA/SRA appliance:

- Log in to your MySonicWall account directly from a browser or click the **SonicWall Inc.** 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 Registering the SMA/SRA Appliance with System > Licenses on page 97.

To register your SMA/SRA appliance:

1. If you are not logged into the Secure Mobile Access management interface, log in with the username ***admin*** and the administrative password you set during initial setup of your SMA/SRA appliance (the default is *password*). For information about configuring the administrative password, refer to the Getting Started Guide for your appliance model.
2. If the **System > Status** page is not automatically displayed in the Secure Mobile Access management interface, click **System** in the left-navigation menu, and then click **Status**.
3. Record your **Serial Number** and **Authentication Code** from the **Licenses & Registration** section.
4. Do one of the following to access the MySonicWall Web page:
   - Click the **SonicWall Inc.** 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.

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.

6. Navigate to **Products** in the left navigation bar.
7. Enter your **Serial Number** and **Authentication Code** in the appropriate fields.
8. Enter a descriptive name for your SMA/SRA appliance in the **Friendly Name** field.
9. Select the product group for this appliance, if any, from the **Product Group** drop-down list.

10 Click **Register**.

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**.

12 On the **System > Status** page of the Secure Mobile Access 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 SMA/SRA appliance can 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 that can also be accessed from the navigation bar. From the **Network > Interfaces** page, a SMA/SRA 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 SMA/SRA 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 Network > Interfaces on page 129.

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:

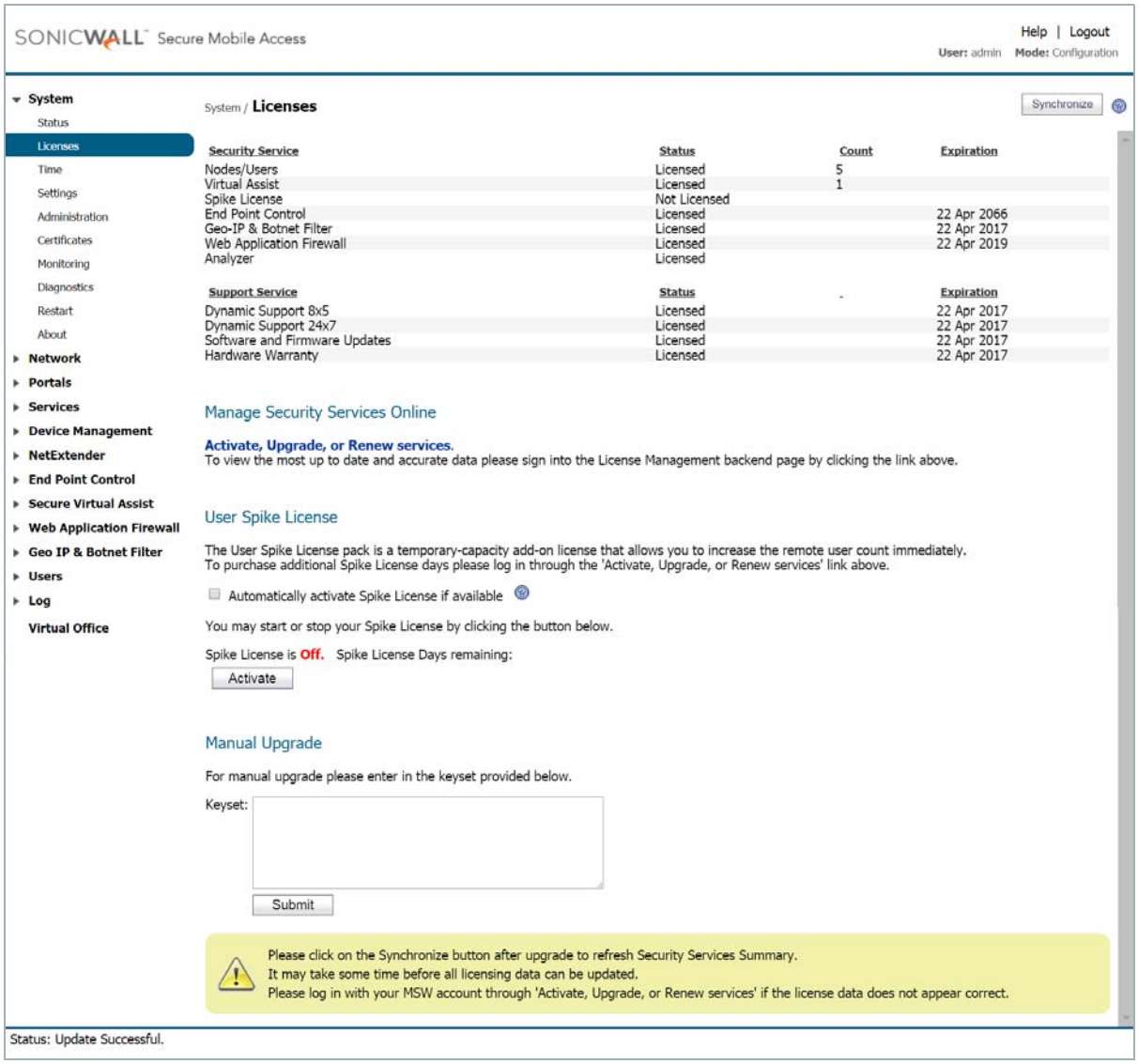
System > Licenses Overview

Services upgrade licensing and related functionality is provided by the License Manager that runs on the SMA/SRA appliance. The License Manager communicates periodically (hourly) with the SonicWall Inc. 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.

The **System > Licenses** page provides a link to activate, upgrade, or renew SonicWall Inc. Security Services licenses. From this page in the Secure Mobile Access management interface, you can manage all the SonicWall Inc. Security Services licenses for your SMA/SRA appliance.

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 SMA/SRA appliance.

The **Security Service** column lists all the available SonicWall Inc. Security Services and upgrades available for the security appliance. The **Status** column indicates if the security service is activated (Licensed), available for activation (Not Licensed, or for Spike License, Inactive), or no longer active (Expired). ViewPoint, Secure Virtual Assist, Spike License, Stateful High Availability (only on SMA 400, SRA 4600), and Web Application Firewall are licensed separately as upgrades.

The number of nodes (computer or other device connected to your appliance with an IP address) or users allowed by the license is displayed in the **Count** column. This number refers to the maximum number of simultaneous connections to the SMA/SRA appliance.

The **Expiration** column displays the expiration date for any licensed service that is time-based. For a Spike License, the Expiration column shows the number of days that the Spike License can be active before it expires. The days do not have to be consecutive.

The information listed in the **Security Services Summary** table is updated from the SonicWall Inc. licensing server every time the SMA/SRA appliance automatically synchronizes with it (hourly), or you can click **Synchronize** to synchronize immediately.

NOTE: If the licenses do not update after a synchronize, you might need to restart your SMA/SRA appliance. DNS must be configured properly and the appliance should be able to reach the sonicwall.com domain.

Manage Security Services Online

You can log in 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.

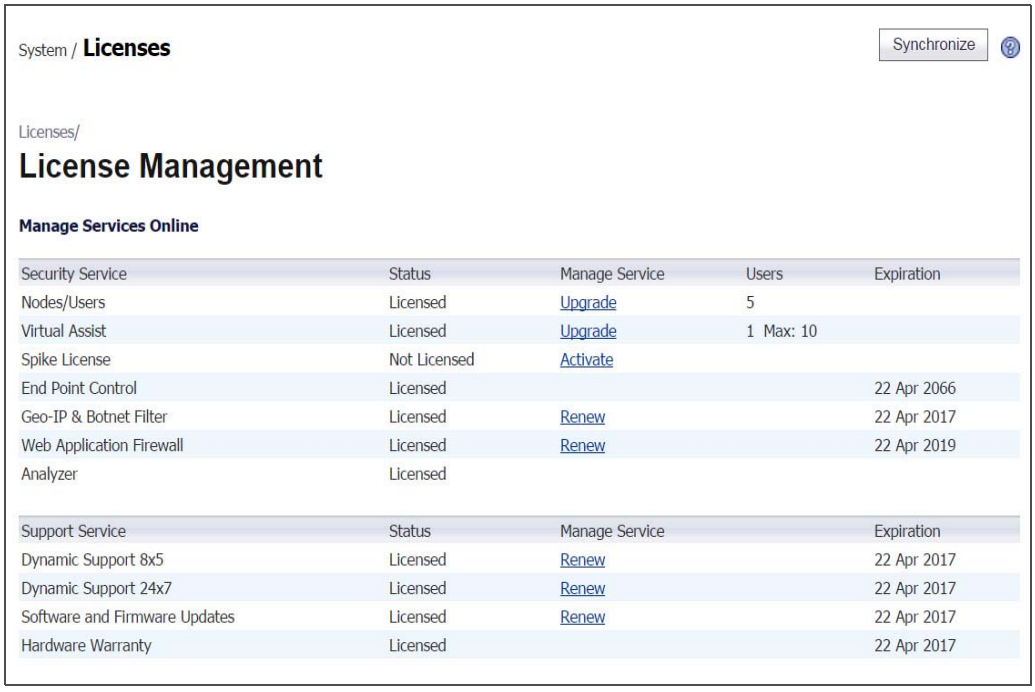
Registering the SMA/SRA Appliance with System > Licenses

On a new SMA/SRA appliance or after upgrading your firmware from an earlier release, you can register your appliance from the **System > Licenses** page.

To register your appliance from the System > Licenses page:

1 Log in to the **System > Licenses** page. Click "A**ctivate, Upgrade, or Renew services**." Enter your MySonicWall user name and password into the fields and then click **Submit**.

2 The License Management page is displayed.



Security Service	Status	Manage Service	Users	Expiration
Nodes/Users	Licensed	Upgrade	5	
Virtual Assist	Licensed	Upgrade	1 Max: 10	
Spike License	Not Licensed	Activate		
End Point Control	Licensed			22 Apr 2066
Geo-IP & Botnet Filter	Licensed	Renew		22 Apr 2017
Web Application Firewall	Licensed	Renew		22 Apr 2019
Analyzer	Licensed			

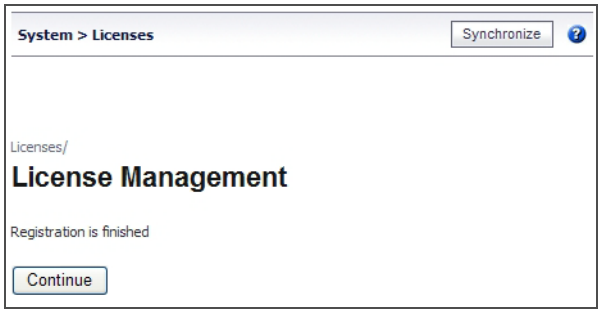
Support Service	Status	Manage Service	Expiration
Dynamic Support 8x5	Licensed	Renew	22 Apr 2017
Dynamic Support 24x7	Licensed	Renew	22 Apr 2017
Software and Firmware Updates	Licensed	Renew	22 Apr 2017
Hardware Warranty	Licensed		22 Apr 2017

3 Click **Activate**, **Upgrade**, or **Renew** on your existing license.

4 Enter your license key in the spaces provided.

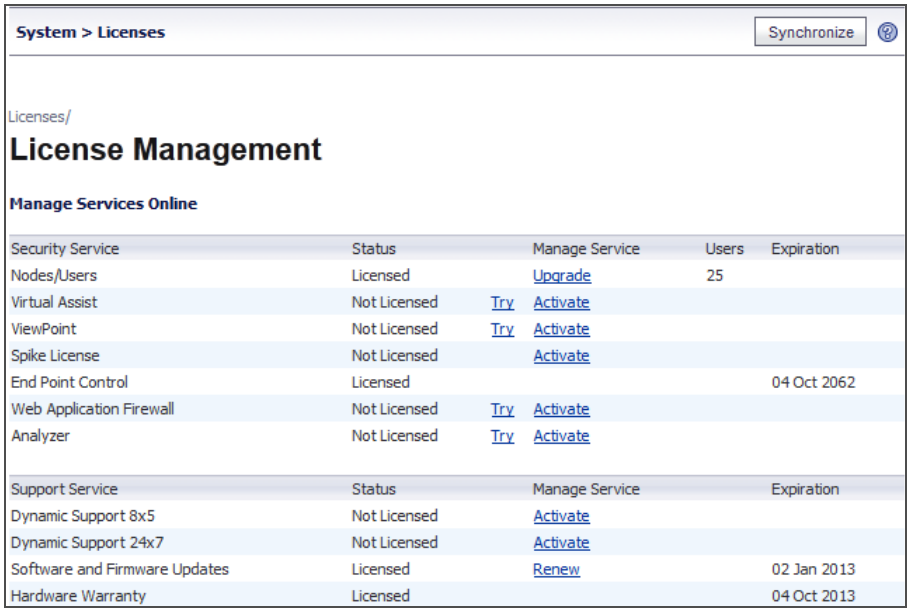
5 Click **Submit**.

6 The display changes to inform you that your SMA/SRA appliance is registered.



7 Click **Continue**.

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

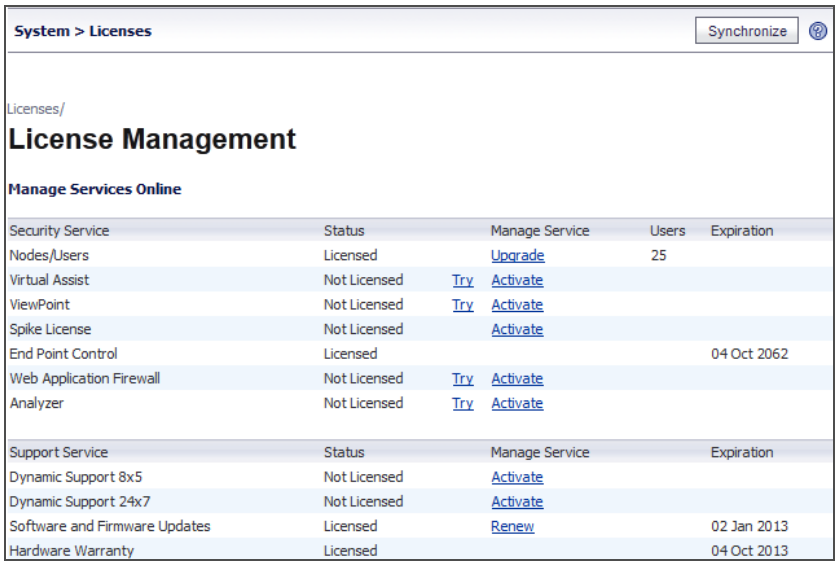


NOTE: After registration, some network environments require the SMA/SRA appliance to be offline so that it is unable to connect to the SonicWall Inc. licensing server. In this mode, the appliance still honors the valid licenses; however, timed-based licenses might not be valid.

Activating or Upgrading Licenses

After your SMA/SRA appliance is registered, you can activate licenses for Secure Virtual Assist (includes Secure Virtual Meeting), Analyzer/ViewPoint, End Point Control, Spike License, and Web Application Firewall, and for SMA 400 and SRA 4600, Stateful High Availability on the **System > Licenses** page. Secure Virtual Assist, Analyzer/ViewPoint, and Web Application Firewall also offer a free trial. You can also upgrade a license from this page. 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 a reseller before you can activate or upgrade. You will receive an activation key to enter into the License Manager page.

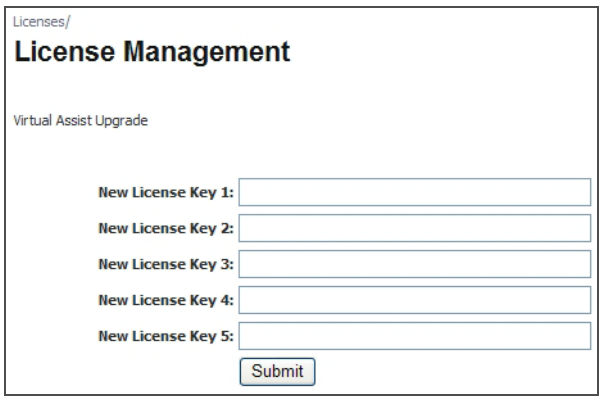


NOTE: Services displayed on the **System > Licenses** page vary, depending on the appliance.

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

1. On the **System > Licenses** page, click **Activate, Upgrade, or Renew services**. The License Management page is displayed.
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. The services can have a **Try** link, an **Activate** link, or an **Upgrade** link.
3. To activate a free 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 Inc. product subscription at any time during or after the trial. Click **Continue**, and follow the setup instructions.
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**.

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**.



6 After completing the activation or upgrading process, click **Synchronize** to update the appliance license status from the SonicWall Inc. licensing server. Rebooting the appliance also updates the license status.

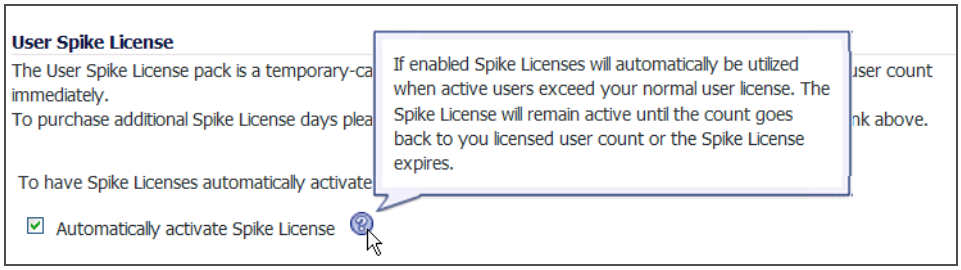
Using a Spike License

A Spike License enables you to temporarily increase the number of remote users your appliance or SMA 500v Virtual Appliance can support if there is a sudden spike in remote access needs, such as during a period of severe weather or during a business event for remote participants. Licensed separately, this feature helps you accommodate spikes in remote access traffic during planned or unplanned events.

When you buy a Spike License, it is valid for a given number of users and days (total number of users supported when the Spike License is activated, not the number in addition to your base license number). You can suspend and resume the use of the license as needed.

More than one Spike Licenses can be uploaded to your appliance, but only one can be active at a time.

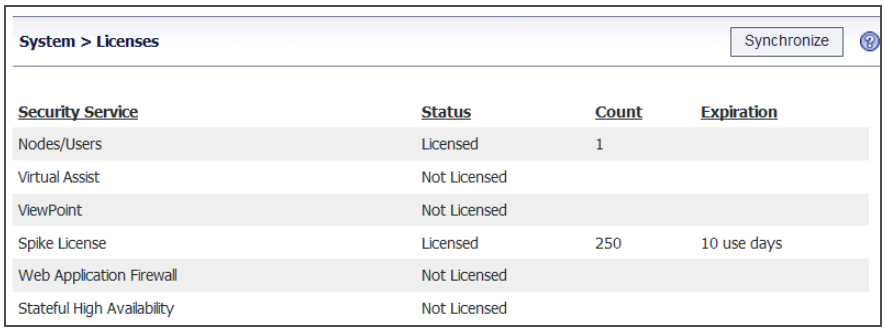
An option is available to automatically enable and disable the license depending on the number of user connections. Select **Automatically activate Spike License** to enable it. If this option is enabled, the Spike License is automatically activated when the number of connected users exceeds your normal user license. The Spike License stays active until either the number of users decreases back to your normal licensed amount or the Spike License expires.



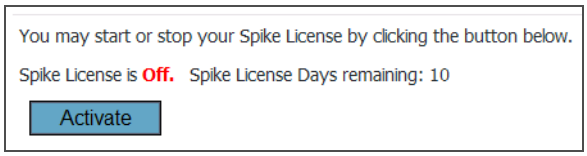
To activate or stop a Spike License:

1 Purchase your Spike License from MySonicWall and import it to the appliance, as described in Activating or Upgrading Licenses on page 99. After licensing, the status is updated to *Licensed*, and the total users

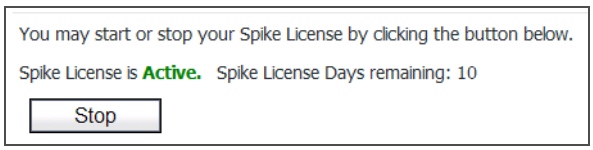
supported and number of usage days remaining in the Spike License are shown on the **System > Licenses** page.



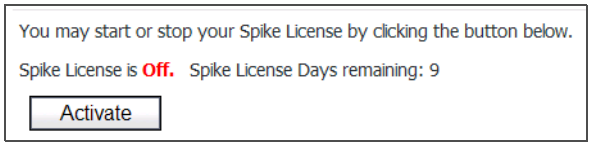
2 After reloading the page, the Spike License is listed as *Off* on the **System > Licenses** page.



3 When you need to accommodate more users, click **Activate**. The status changes to *Active*.



4 To stop an active Spike License, click **Stop**. The status goes back to *Off*, and the number of days remaining is updated.

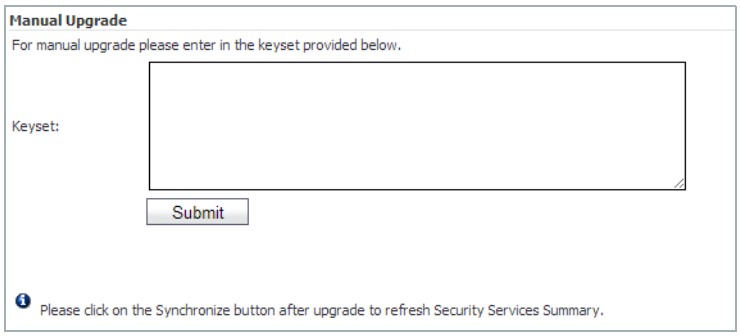


NOTE: Whenever you activate and then stop a Spike License, the number of days for which it is valid decreases by one, even if fewer than 24 hours have elapsed. If it remains active for several days, a day is subtracted after each 24 hour period.

Manual Upgrade

To manually upgrade the your Security Services, scroll down to the Manual Upgrade section of the **System** > **Licences** page. You will need the Keyset for the service(s) you wish to upgrade. Enter the **Keyset** in the available

field, then click **Submit**. Click **Synchronize** at the top of the page to refresh the Security Services Summary. You should now see the upgraded license in the Security Services Summary.



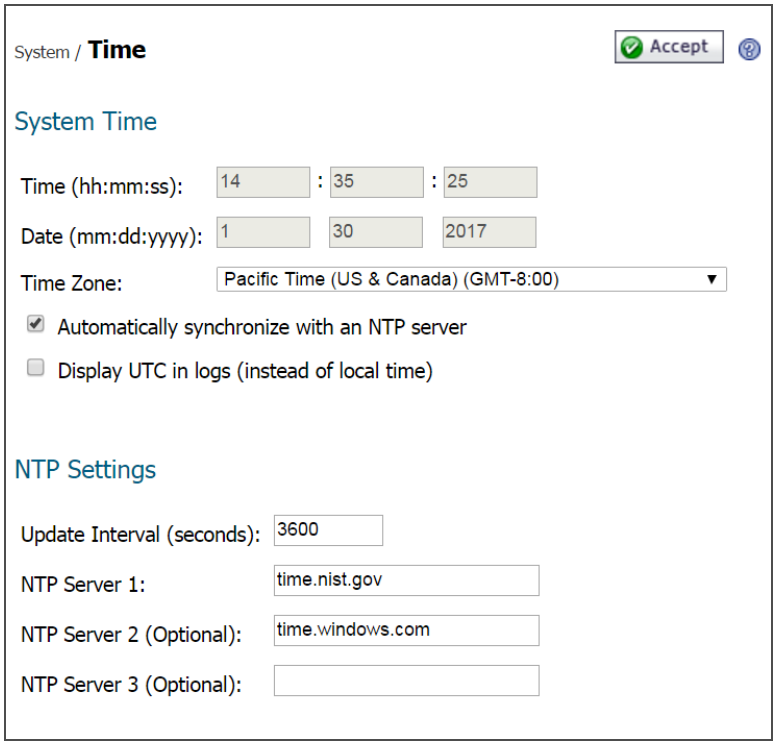
System > Time

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 SMA/SRA appliance system time, date and time zone, and to set the SMA/SRA appliance to synchronize with one or more NTP servers.

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 SMA/SRA appliance must have the correct time and date configured.

To configure the time and date settings:

1. Select your time zone in the **Time Zone** drop-down list.
2. The current time, in 24-hour time format, appears in the **Time (hh:mm:ss)** field and the current date appears in the **Date (mm:dd:yyyy)** field.

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 check box next to **Automatically synchronize with an NTP server** is selected, you cannot manually enter the time and date. To manually enter the time and date, clear the check box.

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

Enabling Network Time Protocol

If you enable Network Time Protocol (NTP), then the NTP time settings overrides the manually configured time settings. The NTP time settings are 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):

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

2 Select **Automatically synchronize with an NTP server**.

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 selects the default update interval, 3600 seconds.

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

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

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.

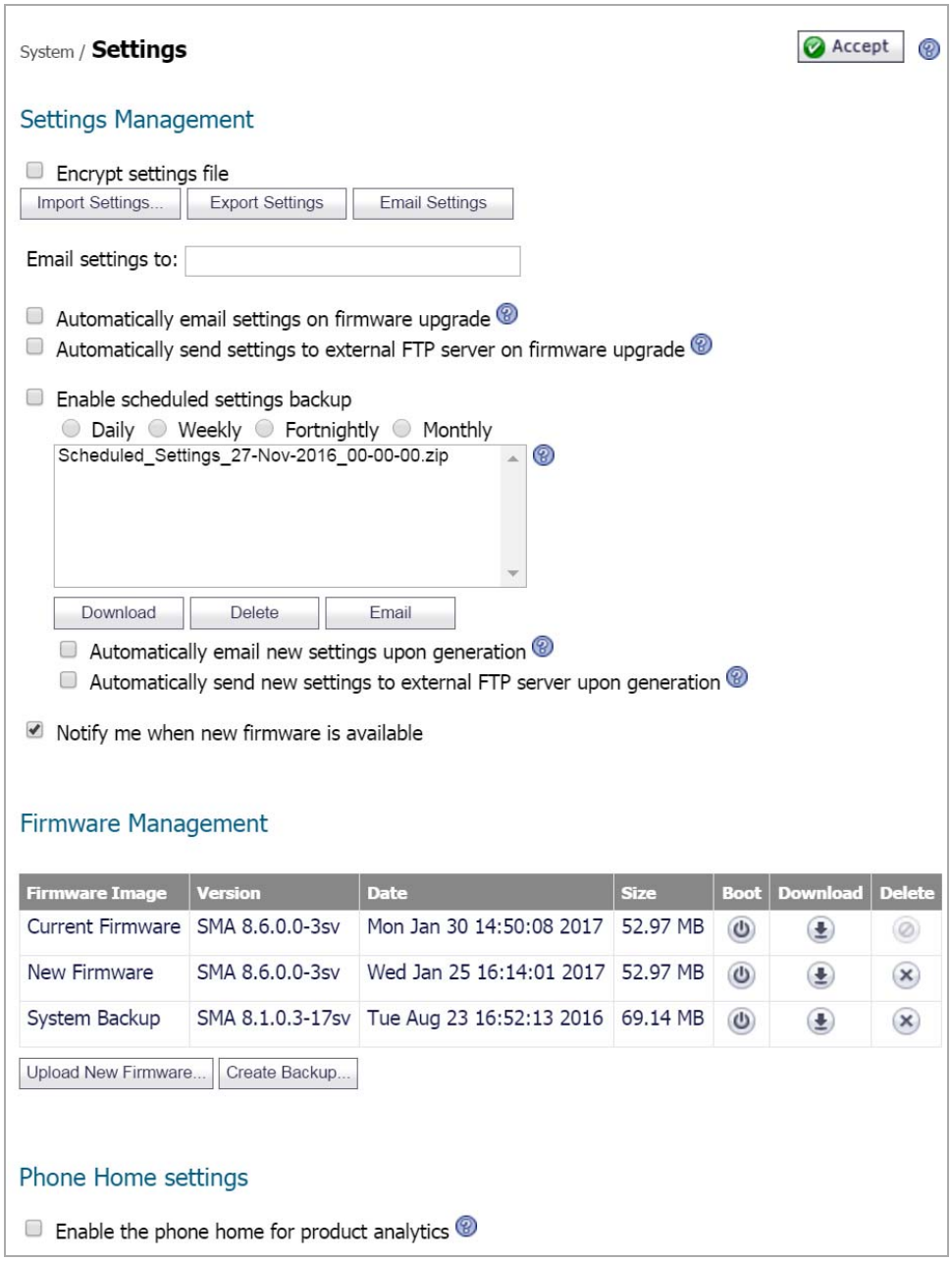
- System > Settings Overview on page 105
- Managing Configuration Files on page 107
- Managing Firmware on page 110

System > Settings Overview

The **System** > **Settings** page allows the administrator to import and export the settings of the SMA/SRA appliance. Options to automatically send your settings to an external FTP server after a firmware upgrade and upon generation are included. SMA already had a period backup of the appliance settings, but these options provide a new method for backup.

On a physical appliance, the **System** > **Settings** page provides a way to upload new firmware, and to boot either the current firmware, newly uploaded firmware, or backup firmware.

System > Settings Page - Physical Appliance



Configure the FTP server on the **System > Administration** page to automatically send new settings to the external FTP server. Refer to the Configuring External FTP/TFTP Server Settings on page 118.

On an SMA 500v Virtual Appliance, the **System** > **Settings** page allows for settings management, but does not provide any firmware management, because the SMA 500v Virtual Appliance is itself a software image.

Settings

The Settings page provides buttons to import and export settings along with email settings, and allows the administrator to encrypt the settings files. There is also an option to be notified when new firmware becomes available.

Firmware Management

The Firmware Management section allows the administrator to control the firmware that is running on the SMA/SRA 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.

Phone Home Settings

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

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

Managing Configuration Files

SMA/SRA appliances allow you to save and import file sets that hold the SMA/SRA configuration settings. These file sets can be saved and uploaded through the **System > Settings** page in the Secure Mobile Access management interface.

These tasks are described in the following sections:

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 **Encrypt settings file** in the **System > Settings** page.

Importing a Configuration File

You can import the configuration settings that you previously exported to a backup configuration file.

To import a configuration file:

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

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

> **NOTE:** Because of feature differences between some platforms, importing settings from the SMA 200 to the SMA 400 and vice versa or the SRA 1600 to the SRA 4600 and vice versa is not fully supported. In addition, importing Virtual Machine settings to any other platform is not fully supported. If you import settings between these platforms, be sure to verify settings were imported correctly.

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.

4 Click **Upload**. Secure Mobile Access imports the settings from the file and configures the appliance with those settings.

> **NOTE:** Make sure you are ready to reconfigure your system. After you import the file, the system overwrites the existing settings immediately.

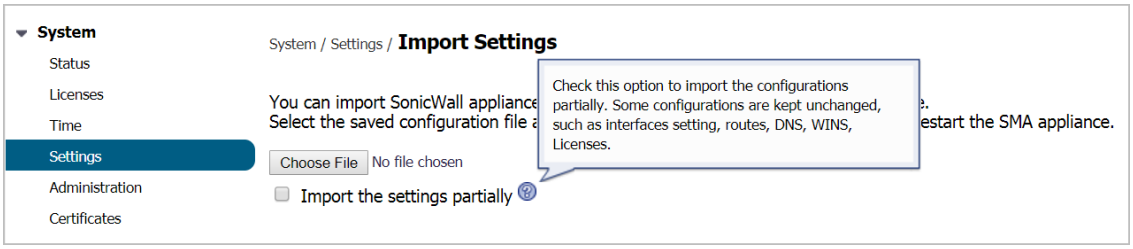
5 After the file has been imported, restart the appliance to make the changes permanent.

Importing Partial Configurations

This feature allows you to import settings on partial configurations while leaving some configurations unchanged; including interface settings, route settings, DNS settings, WINS settings, and Licenses.

To import the settings partially,

1 Navigate to **System > Settings > Import Settings**. The **Import Settings** page appears.



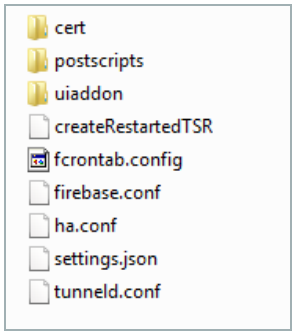
2 Choose the configuration file you would like to upload, and click **Import the settings partially**.

3 Click **Accept**.

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 can 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 shown in the following figure.

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.
- **settings.json** file – Contains user, group, domain and portal settings.
- **fcrontab.config** file – Only generated when the Schedule TSR is enabled.

To export a backup configuration file:

1. Navigate to the **System > Settings** page.
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.
3. Select the option to **Save** the file.
4. Choose the location to save the configuration file. The file is named **sslvpnSettings-serialnumber.zip** by default, but it can be renamed.
5. Click **Save** to save the configuration file.

Emailing Configuration Settings

You can email the current settings, auto-generated settings on upgrade, and scheduled settings to an email address as another way to back up your system. Specify an email address in the **Email Settings to** field. Then, click **Email Settings**.

You can also have the email settings sent automatically upon every firmware upgrade. Select the Automatically email settings on firmware upgrade check box. The **Mail Server** and **Mail From Address** values must be configured for automated email delivery. See Log > Settings on page 437 for more information.

Enabling Scheduled Backups

You can set scheduled backups for your current settings by selecting **Enable scheduled settings backup**. Then, specify the frequency of back ups to be scheduled. You can specify for the back ups to occur Daily, Weekly, Fortnightly, or Monthly.

Emailing New Settings

You can select **Automatically email new settings upon generation** to have emails sent to you of the newest settings after they are generated.

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 on page 110
- Creating a Backup on page 110
- Downloading Firmware on page 110
- Booting a Firmware Image on page 110
- Uploading New Firmware on page 111

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 **Notify me when new firmware is available**.

Creating a Backup

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

Downloading Firmware

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

Booting a Firmware Image

You can boot up (restart) the appliance with any firmware image that appears in the Firmware Management table on the **System > Settings** page. You have the choice of keeping current configuration settings or reverting to factory default settings.

To boot a firmware image:

1. Click the boot icon  in the row for the Firmware Image version that you want to run on the SMA/SRA appliance.
2. To reboot the image with factory default settings, select **Boot with factory default settings**. If this option is not selected, current configuration settings are kept.

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

Uploading New Firmware

To upload new firmware:

1 Log in to MySonicWall.

2 Download the latest Secure Mobile Access firmware version.

3 In the Secure Mobile Access management interface, navigate to the **System > Settings** page.

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

5 Click **Browse**.

6 Select the downloaded Secure Mobile Access firmware. It should have a .sig file extension.

7 Click **Open**.

8 Click **Accept**. Wait for the firmware to upload and be written to the disk.

9 The **System** > **Settings** page displays the firmware table, with the uploaded firmware listed in it. Click the Boot icon in the **Uploaded Firmware** row to boot the new firmware with existing settings.

Managing Language Settings

SMA/SRA appliances allow you to import and apply new language packs to the firmware. The language packs are stored on the back end server. The Secure Mobile Access firmware is scheduled to check the back end server every hour for updates to existing or new language packs.

These tasks are described in the following sections:

- Downloading a language pack on page 111
- Importing a language pack on page 112
- Selecting a language on page 112
- Querying for new languages on page 112

Downloading a language pack

The Language Settings section displays the newest language pack(s) available. Log in to MySonicWall to download the language pack to your local system, or click the link for the language you want to download to be automatically directed to MySonicWall.

Importing a language pack

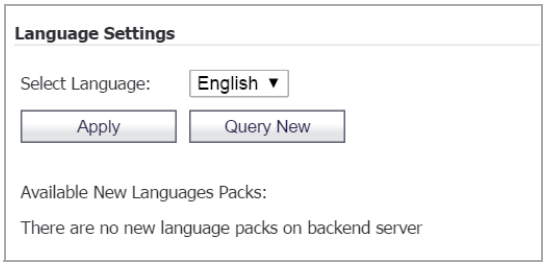
After you have downloaded a new language pack from MySonicWall, you can import it to your Secure Mobile Access firmware. Click **Import**. Then, click **Choose File** to select the language file to import. Click **Open**.

Selecting a language

The **Select Language** drop-down menu has the available languages downloaded to the back end server of the SMA/SRA appliance. The default language is English. Select the language from the drop-down menu, then click **Apply**. This process can take a few minutes.

Querying for new languages

To manually query available language packs on the back end server, click **Query Now**. If there are any new language packs available, they are listed under “Available New Language Packs.”



System > Administration

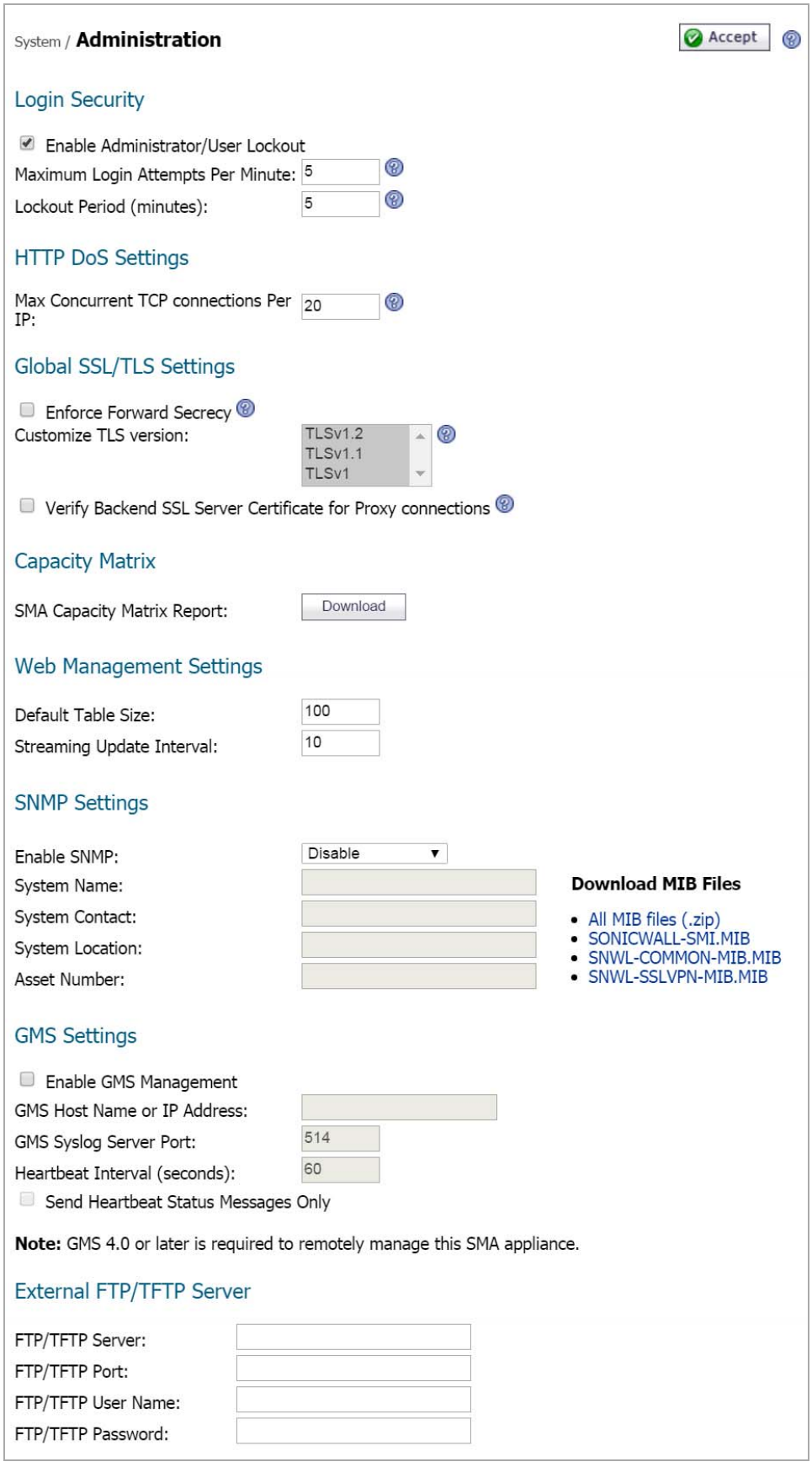
This section provides an overview of the **System > Administration** page and a description of the configuration tasks available on this page.

System > Administration Overview

This section provides the administrator with information about and instructions to complete the configuration tasks on the **System > Administration** page. The **System > Administration** page allows the administrator to configure login security, Web management settings, SNMP settings, and GMS settings.

See the following sections:

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.

HTTP DOS Settings

The HTTP DOS Settings section is used to configure the maximum concurrent TCP connections (20-100, default 20) a client can open with the Secure Mobile Access web server.

Global SSL/TSL Settings

The Global SSL/TLS settings section allows the administrator to configure Secure Sockets Layer (SSL) and Transport Layer Security (TSL) settings globally from the **System > Administration** page.

Configure the following settings:

- **Enforce Forward Secrecy** — Enable this option to allow current information to be kept in secrecy, even if the private key is compromised in the future. Note that browsers that do not support Forward Secrecy might not be able to connect to the SMA/SRA appliance. The performance of this feature can decline depending on the ciphers that the client browser supports.
- **Verify Backend SSL Server Certificate for Proxy connections** — When this option is enabled, the connection is dropped if the backend SSL/TLS server certificate is not trusted. The verification depth is 10. Alert level log messages are also generated when this option is enabled.

Capacity Matrix

The Secure Mobile Access Capacity Matrix Report is a downloadable .PDF file that allows you to view the total number of various connections, interfaces, portals, domains, groups, users, and so on, available for your specific SMA/SRA appliance model. Click **Download** to have the report downloaded to your local system.

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 Secure Mobile Access management interface.

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

- Secure **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 one second, the default is 10 seconds, and the maximum is 99,999.

SNMP Settings

The SNMP Settings section allows the administrator to enable SNMP and specify SNMP settings for the appliance. A list of downloaded MIBs is displayed to the right of the fields. MIBs can be downloaded from MySonicWall.

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).

Configuring Login Security

SMA/SRA appliance 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:

1. Navigate to **System > Administration**.
2. Select **Enable Administrator/User Lockout**.
3. In the **Maximum Login Attempts Per Minute** field, type the number of maximum login attempts allowed before a user is locked out. The default is five attempts. The maximum is 99 attempts.
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 five minutes. The maximum is 9999 minutes.
5. Click **Accept** to save your changes.

Configuring HTTP DOS Settings

HTTP DPS setting is used to configure the maximum concurrent TCP connections per IP address. Complete the following steps to change the maximum number of connections at any one time:

1. Navigate to **System > Administration**.
2. In the **Max Concurrent TCP connections Per IP** field, type the maximum number of concurrent TCP connections a client can open with the Secure Mobile Access web server. The default is 20 and the maximum is 100 connections.

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 Secure Mobile Access management interface.

To set the table page size and streaming update interval:

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

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

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

Configuring SNMP Settings

To configure the SNMP Settings fields:

1 Navigate to **System > Administration**.

2 Select **Enable SNMP**.

3 Type the name (FQDN) of the system into the **System Name** field.

4 Type the email address of the system contact into the **System Contact** field.

5 Type the city or other identifying location of the system into the **System Location** field.

6 Type the asset number of the system into the **Asset** field. The asset number is defined by the administrator.

7 Type the public community name into the **Get Community Name** field. This name is used in SNMP GET requests.

8 Click **Accept** to save your changes.

Enabling GMS Management

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

To enable GMS management of your SMA/SRA appliance, complete the following steps:

1 Navigate to **System > Administration**.

2 Select **Enable GMS Management**.

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

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.

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).

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

External FTP/TFTP Server

The External FTP/TFTP Server section allows you to configure an external FTP server to backup your settings and diagnostic data.

Configuring External FTP/TFTP Server Settings

To configure the External FTP/TFTP Server field:

1 Navigate to **System > Administration | External FTP/TFTP Server**.

2 Type the FTP/TFTP server address, port, user name, and password into the corresponding fields.

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

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.

System > Certificates Page

See the following sections:

- Server Certificates on page 119
- Additional CA Certificates on page 119

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 SMA/SRA appliance. The appliance 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 SMA/SRA appliance, not by a real CA), and there could 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.

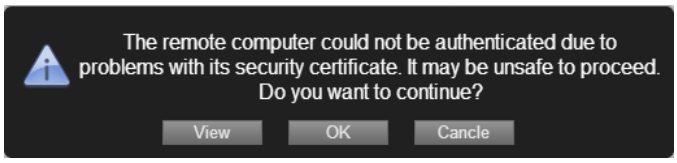
The imported additional certificates only take effect after restarting the SMA/SRA appliance.

Certificate Management

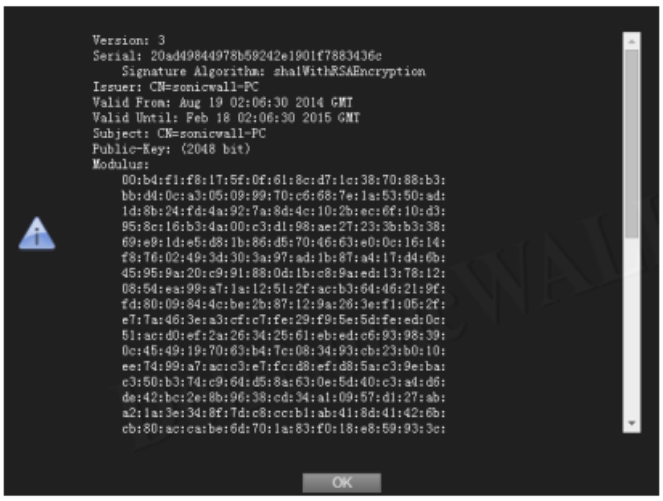
The SMA/SRA appliance comes with a pre-installed self-signed X509 certificate for SSL functions. A self-signed certificate provides all the same functions as a certificate obtained through a well-known certificate authority (CA), but presents an “untrusted root CA certificate” security warning to users until the self-signed certificate is imported into their trusted root store. This import procedure can be completed by the user by clicking **Import Certificate** 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).

Virtual Assist verifies the server certificate that provides a safer environment for the appliance. If the certificate is not issued by an authorized organization, an alert message is displayed to notify the user of the risk.



View - Click for detailed information about the server certificate. Information displays, as shown in the following image:



OK - Click to accept the certificate and launch the connection.

Cancel - Click to end the connection.

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 SMA/SRA appliance.

To generate a certificate signing request:

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

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

3 Fill in the fields in the dialog box and click **Accept**.

> **NOTE:** The Subject Alternative Name (SAN)/Unified Communications Certificate (UCC) can be included in the request.

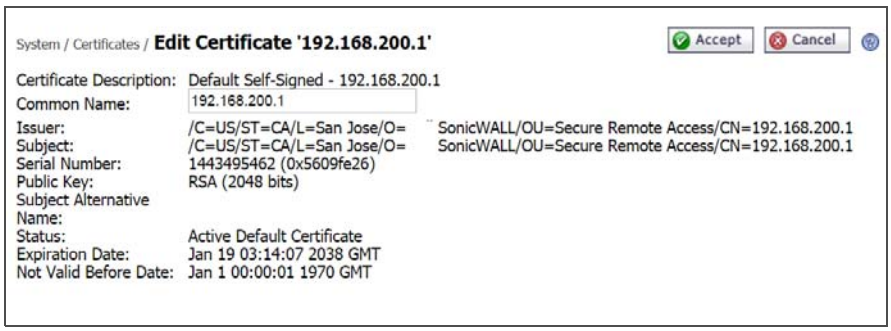
4 If all information is entered correctly, a **csr.zip** file is created. Save this .zip file to disk. You need to provide the contents of the server.csr file, found within this zip file, to the CA.

Viewing and Editing Certificate Information

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

To view certificate and issuer information and edit the Common Name in the certificate:

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



2 From the **Edit Certificate** window, you can view the issuer and certificate subject information.

3 On self-signed certificates, type in the Web server host name or IP address in the **Common Name** field.

4 Click **Accept** to submit the changes.

You can also delete an expired or incorrect certificate. Delete the certificate by clicking **Delete** 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:

1. Navigate to the **System** > **Certificates** page.
2. Click **Import Certificate**. The Import Certificate dialog box is displayed.
3. Click **Browse**.
4. Locate the server certificate. If uploading from a PKCS #12 file, select the .p12 or .pfx file from your disk or network drive. If uploading a zipped file containing the private key and certificate select the .zip file from your disk or network drive. Any filename is 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 is not uploaded.
5. Click **Upload**.

   After the certificate has been uploaded, the certificate is displayed in the Certificates list in the **System > Certificates** page.

NOTE: Private keys might 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:

1. Navigate to the **System > Certificates** page.
2. Click **Import CA Certificate** in the Additional CA Certificates section. The Import Certificate dialog box is displayed.
3. Click **Browse**.
4. Locate the PEM-encoded, DER-encoded, or PKCS #7 CA certificate file on your disk or network drive and select it. Any filename is accepted.
5. Click **Upload**.

   After the certificate has been uploaded, the CA certificate is displayed in the Additional CA Certificates list in the **System > Certificates** page.
6. To add the new CA certificate to the Web server's active CA certificate list, the Web server must be restarted. Restart the SMA/SRA 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

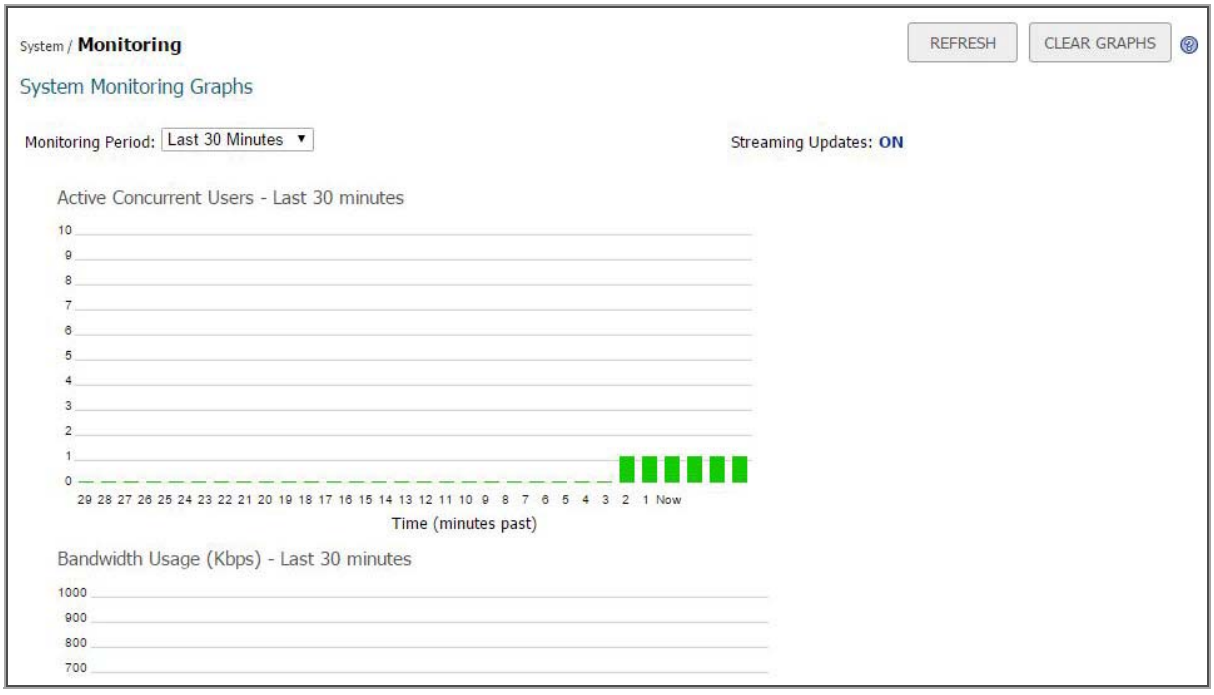
The SMA/SRA appliance provides configurable monitoring tools that enable you to view usage and capacity data for your appliance. The **System > Monitoring** page provides the administrator with four monitoring graphs:

- 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.

The following Figure shows the **System > Monitoring** page.

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.

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 **Refresh** at the top right corner of the **System > Monitoring** page.

System > Diagnostics

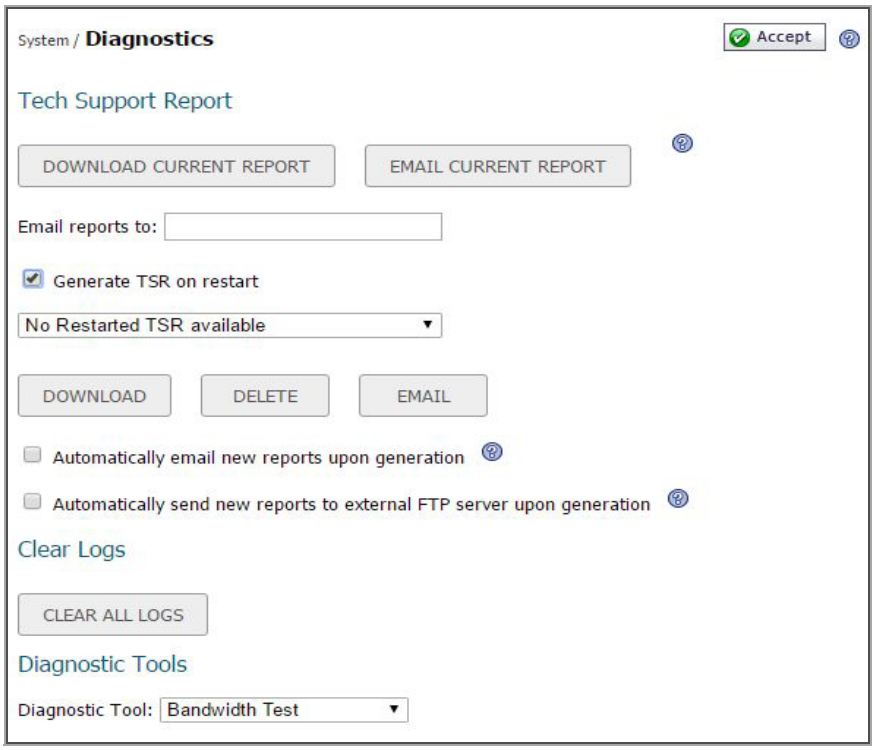
This section provides an overview of the **System > Diagnostics** page and a description of the configuration tasks available on this page.

- System > Diagnostics Overview on page 125
- Downloading & Generating the Tech Support Report on page 125
- Performing Diagnostic Tests on page 126

System > Diagnostics Overview

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

System > Diagnostics Page



Options to automatically send the TSR to an external FTP server after a restart and upon generation are included. Configure the FTP server in the **System > Administration** page to automatically send the TSR to an external FTP server. See Configuring External FTP/TFTP Server Settings on page 118 for more information.

Downloading & Generating the Tech Support Report

Downloading a Tech Support Report records system information and settings that are useful to SonicWall Inc. Technical Support when analyzing system behavior. The following options are available for Tech Support Reports:

- **Download Current Report**—Clicking this button prompts a Windows pop-up to 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 SMA/SRA appliance.
- **Email Current Report**— Click to email the TSR report to the Email address specified in the **Email Reports to** field.
- **Generate TSR on Restart**—Enable this option by selecting the check box. When enabled, the SMA/SRA appliance generates a new TSR upon every restart of the appliance. The latest report generated from an appliance restart is available in the drop-down list, prefaced with “Restarted_TSR_.”
    - **Download**—This button allows you to download the latest Restarted Tech Support Report to your local system.
    - **Delete**—This button allows you to delete the latest Restarted Tech Support Report.

- **Email**—Click this button to email the latest Restarted Tech Support Report to the values specified in the **Mail Server** field on the **Log** > **Settings** page.
- **Automatically email new reports upon generation**—Select this check box to enable automatic emailing of the latest Restarted Tech Support Report. You must specify the **Mail Server** and **Mail From Address** fields on the **Log** > **Settings** page for automated email delivery.

- **Enable scheduled TSR generation**—Click the check box to enable scheduled Tech Support Reports. After enabled, you can either have them generated **Hourly** or **Daily**. Note that a maximum of 12 TSRs are stored, with a total file size not exceeding 50 MB. Scheduled Tech Support Reports are mostly used for diagnostics or troubleshooting purposes by a SonicWall Inc. technician, if needed.

  NOTE: Scheduled TSR is disabled by default. You must enable the feature on the **<SSLVPN>/cgi-bin/diag** page first.

  - **Download**—This button allows you to download the latest scheduled Tech Support Reports to your local system.
  - **Delete**—This button allows you to delete the latest scheduled Tech Support Reports.
  - **Email**—Click this button to email the latest scheduled Tech Support Reports to the values specified in the **Mail Server** field on the **Log** > **Settings** page.
  - **Automatically email new reports upon generation**—Select this check box to enable automatic emailing of the latest scheduled Tech Support Reports. You must specify the **Mail Server** and **Mail From Address** fields on the **Log** > **Settings** page for automated email delivery.

Performing Diagnostic Tests

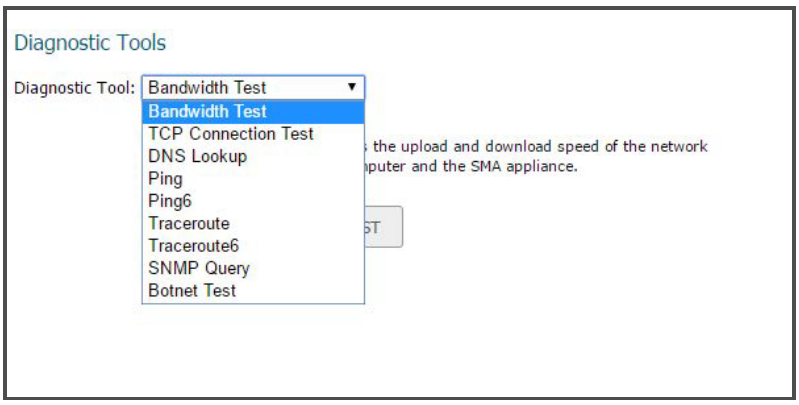
Diagnostic tools allows the administrator to test SMA/SRA connectivity by performing a ping, TCP connection test, DNS lookup, or Traceroute for a specific IP address or Web site. You can also do a bandwidth test between the SMA/SRA appliance and your local computer, or do an SNMP query to display information about the appliance.

You can do standard network diagnostic tests on the SMA/SRA appliance in the **System > Diagnostics** page.

To run a diagnostic test:

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

2 In the **Diagnostic Tool** drop-down list, select **Bandwidth Test**, **TCP Connection Test**, **DNS Lookup**, **Ping**, **Ping6**, **Traceroute**, **Traceroute6**, **SNMP Query**, or **Botnet Test**.



The following Table describes the diagnostic tools and functions.

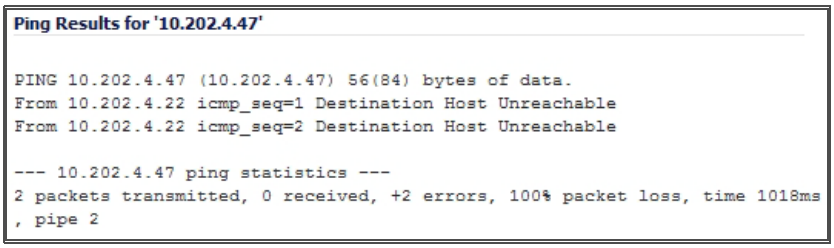
Diagnostic tools and their functions

Diagnostic Tool	Function
Bandwidth Test	Measures the upload and download speed of the network connection between your computer and the SMA/SRA appliance.
TCP Connection Test	Tests the connectivity of a port that is specified by appending a colon and port number to the host name or IP address (for example, 10.9.9.19:83 or www.myhost.com:83. If no port is specified, port 80 is tested.
DNS Lookup	Translates a DNS name to an IP address and vice versa.
Ping	Tests the connection to a host or IP address.
Ping6	Tests the connection to an IPv6 address or domain. Ping6 is meant for use with IPv6 addresses and networks.
Traceroute	Identifies the route and number of hops needed to connect to a host or IP address.
Traceroute6	Identifies the route and number of hops needed to connect to an IPv6 address or domain. Traceroute 6 is meant for use with IPv6 addresses and networks.
SNMP Query	Looks up SNMP information from the selected MIB. SNMP must be enabled (**System > Administration** page) before a query can be completed. In the **SNMP MIB** drop-down list, select the MIB for which to display the values. The SNWL-SSLVPN-MIB is the Secure Mobile Access specific MIB that shows device statistics and licensing information. The SNWL-COMMON-MIB is a file common to all SonicWall Inc. products and shows product name, serial, firmware, ROM version, and asset number (user defined). The rest of the MIBs are standard SNMP MIBs including SNMPv2-MIB and All SNMP MIB-2, or you can select ALL MIBs.
Botnet Test	Identifies whether an IP address is a Botnet IP address.

3 If prompted for additional information like a Host or IP Address, type the requested information.

4 Click **Enter**.

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 on page 128
- Restarting the SMA/SRA Appliance on page 128

System > Restart Overview

The **System > Restart** page allows the administrator to restart the SMA/SRA appliance.

A warning is displayed that restarting takes one or two minutes and causes all current users to be disconnected.

Restarting the SMA/SRA Appliance

To restart the SMA/SRA appliance, complete the following steps:

1. Navigate to **System > Restart**.
2. Click **Restart**.
3. In the confirmation dialog box, click **OK**.

NOTE: Restarting takes approximately two minutes and causes all users to be disconnected.

System > About

The **System** > **About** page provides the End-User License Agreement for using the SMA/SRA appliance. Click **Download** for SonicWall Inc. copyright Information. For more information regarding the End-User License Agreement, refer to https://www.sonicwall.com/legal/.

4

Network Configuration

This section provides information and configuration tasks specific to the **Network** pages on the Secure Mobile Access web-based management interface. Network tasks for the SMA/SRA appliance include configuring network interfaces, DNS settings, routes, and host resolution.

Topics:

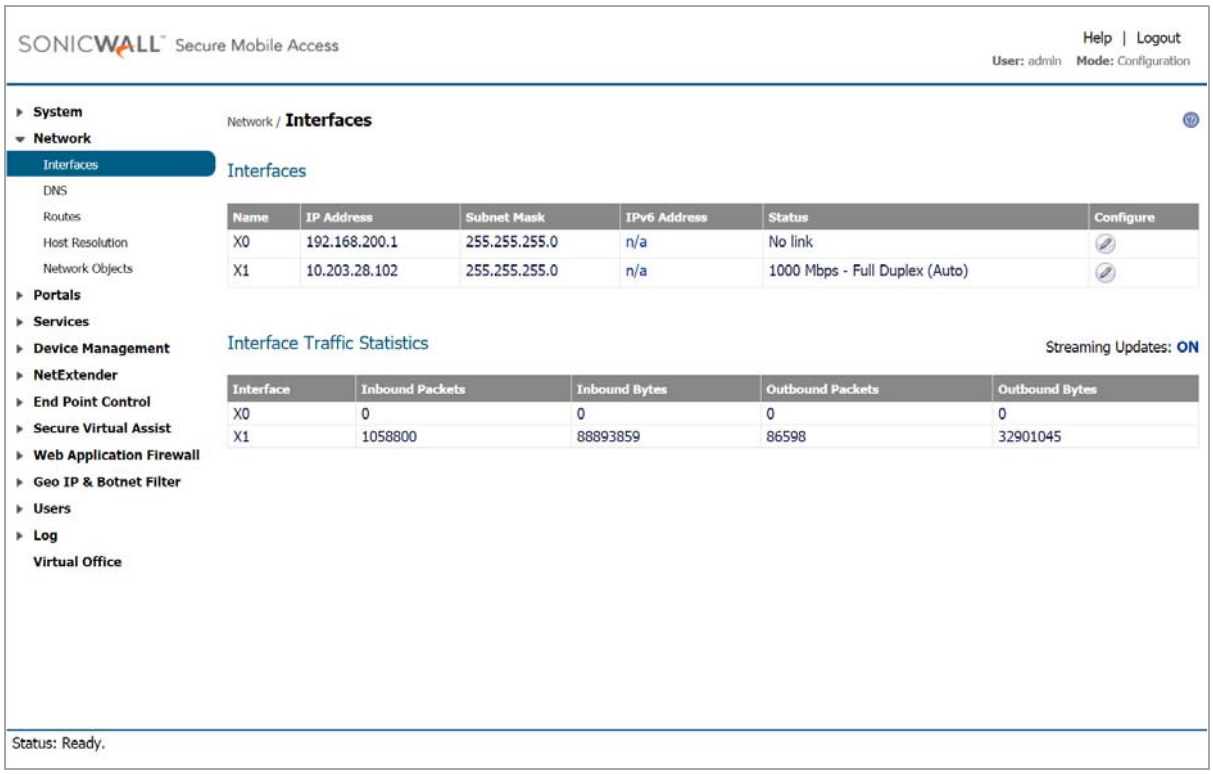
Network > Interfaces

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 SMA/SRA appliance.

Network > Interfaces Page



Configuring Network Interfaces

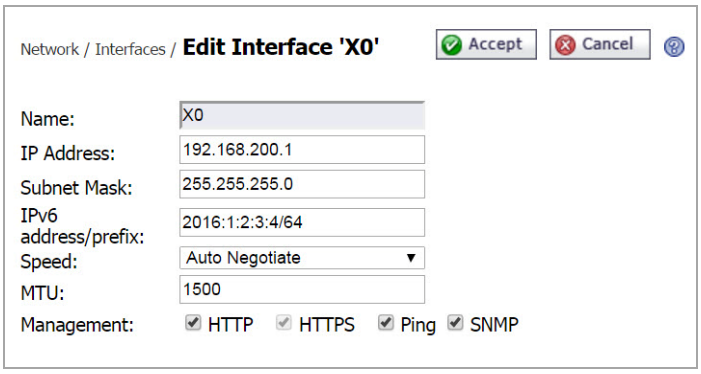
The **Network > Interfaces** page allows the administrator to view and configure the IP address, subnet mask, speed, and management settings of the X0, X1, X2, X3, and where available, the X4 and X5 interfaces on the SMA/SRA appliance. For a port on your SMA/SRA appliance to communicate with a firewall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

NOTE: If the Secure Mobile Access management interface IP address changes, the Secure Mobile Access services are automatically restarted. This interrupts any existing user sessions, and users need to reconnect to continue using the SMA/SRA appliance.

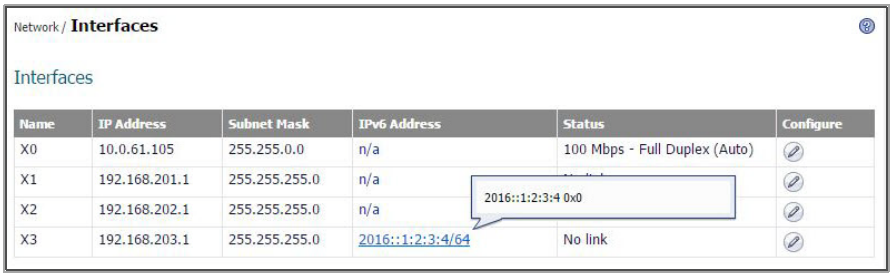
To configure these settings for an interface on the SMA/SRA appliance:

1. Navigate to the **Network > Interfaces** page and click the configure icon next to the interface you want to configure.
2. In the **Edit Interfaces** dialog box on the SMA/SRA appliance, type an unused static IP address in the **IP Address** field. This IP address should reside within the local subnet to which your SMA/SRA appliance is connected.

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



4 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.



5 In the **Speed** drop-down list, **Auto Negotiate** is selected by default to allow the SMA/SRA 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:

- 1000 Mbps - Full Duplex
- 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 Inc. security appliance as well.

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

7 Click **Accept**.

Network > DNS

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

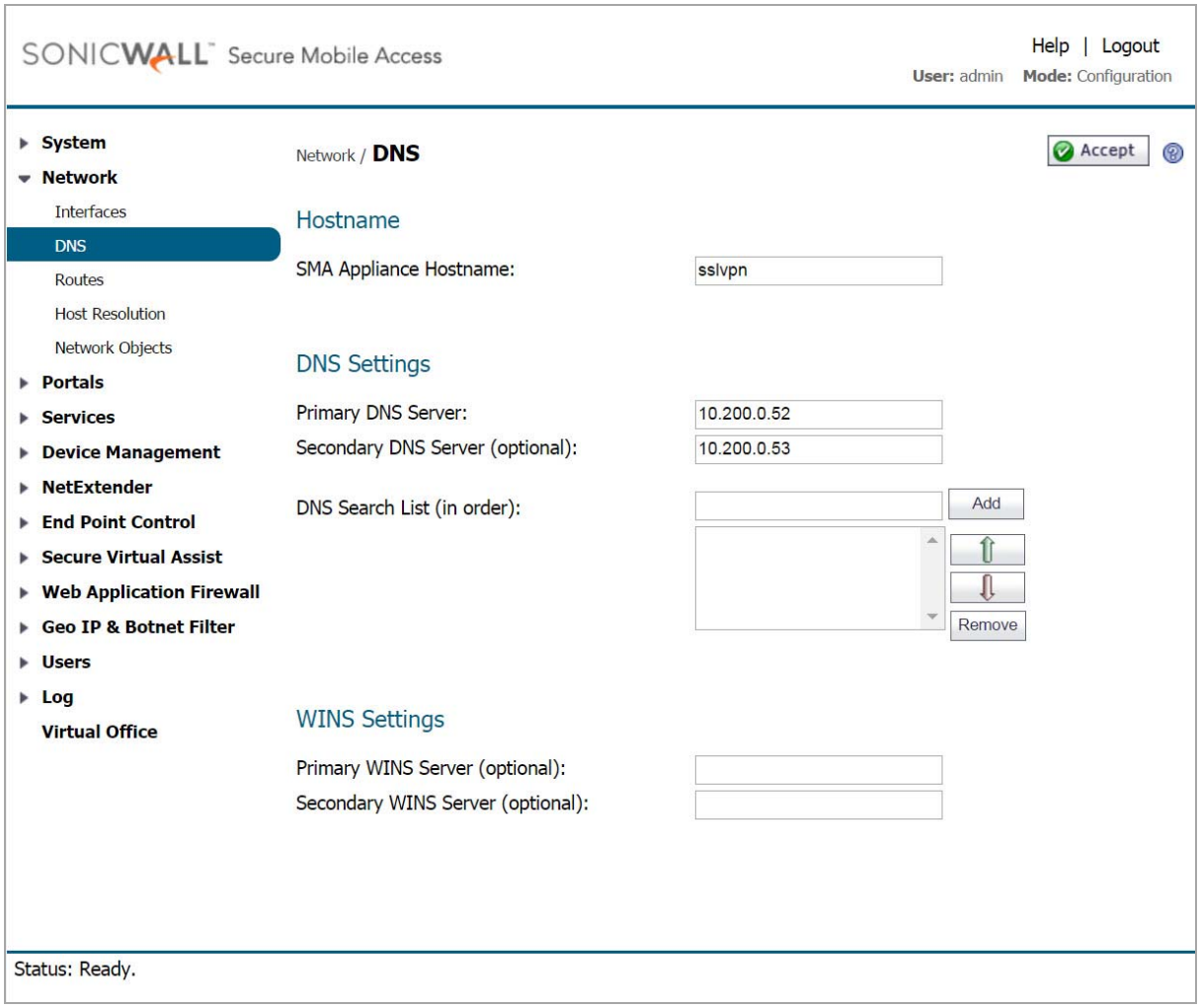
- Network > DNS Overview on page 132
- Configuring Hostname Settings on page 133

- Configuring DNS Settings on page 133
- Configuring WINS Settings on page 134

Network > DNS Overview

The **Network > DNS** page allows the administrator to set the SMA/SRA appliance hostname, DNS settings and WINS settings.

Network > DNS Page



The hostname section allows the administrator to specify the SMA/SRA gateway hostname.

DNS Settings

The DNS settings section allows the administrator to specify a **Primary DNS Server, Secondary DNS Server** (optional) and **DNS Domain** (optional). The Primary DNS Server is required.

For SMA/SRA appliances supporting connections from Apple iPhones, iPads, or other iOS devices using SonicWall Inc. Mobile Connect, the **DNS Domain** is a required field. This DNS domain is set on the VPN interface of the iPhone/iPad after the device makes a connection to the appliance. When the mobile device user accesses a URL, iOS determines if the domain matches the VPN interface's domain, and if so, uses the VPN interface's

DNS server to resolve the hostname lookup. Otherwise, the Wi-Fi or 3G/4G DNS server is used that cannot resolve hosts within the company intranet.

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:

1. Navigate to the **Network > DNS** page.
2. In the Hostname region, type a hostname for the SMA/SRA appliance in the **SMA Gateway Hostname** field.
3. Click **Accept**.

Configuring DNS Settings

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

To configure a DNS server:

1. Navigate to the **Network > DNS** page.
2. In the DNS Settings region, type the address of the primary DNS server in the **Primary DNS Server** field.
3. An optional secondary address can be provided in the **Secondary DNS Server (optional)** field.
4. Optionally, use the **DNS Search List** field to create a pool of domain names:
    a. Type the domain suffix in the **Domain Search List** and click **Add**. The suffix is appended with the host name to make a Fully Qualified Domain Name (FQDN) that is used in host resolution.
    b. To remove a DNS suffix, select the domain suffix from the list and click **Remove**.
    c. Use the up and down arrow keys to arrange the DNS domain suffixes in the order that is used to resolve host names.

    For example, your host name is SonicPRS and the usa.n.sonicwall.com and rsc.sonicwall.com DNS suffixes are added to the search list. The first suffix is appended to SonicPRS to make the FQDN (SonicPRS.usa.n.sonicwall.com) that is used in name resolution. If the name is not resolved, the next suffix in the search list is used (SonicPRS.rsc.sonicwall.com).This process continues until the name is resolved or all suffixes have been tried.
5. Click **Accept**.
6. Restart the appliance to ensure new DNS settings take effect.

Configuring WINS Settings

WINS settings are optional. The SMA/SRA 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:

1. Navigate to the **Network > DNS** page.
2. In the WINS Settings region, type a primary WINS address in the **Primary WINS Server (optional) field**.
3. In the WINS settings region, type a secondary WINS address in the **Secondary WINS Server (optional)** field.
4. Click **Accept**.

Network > Routes

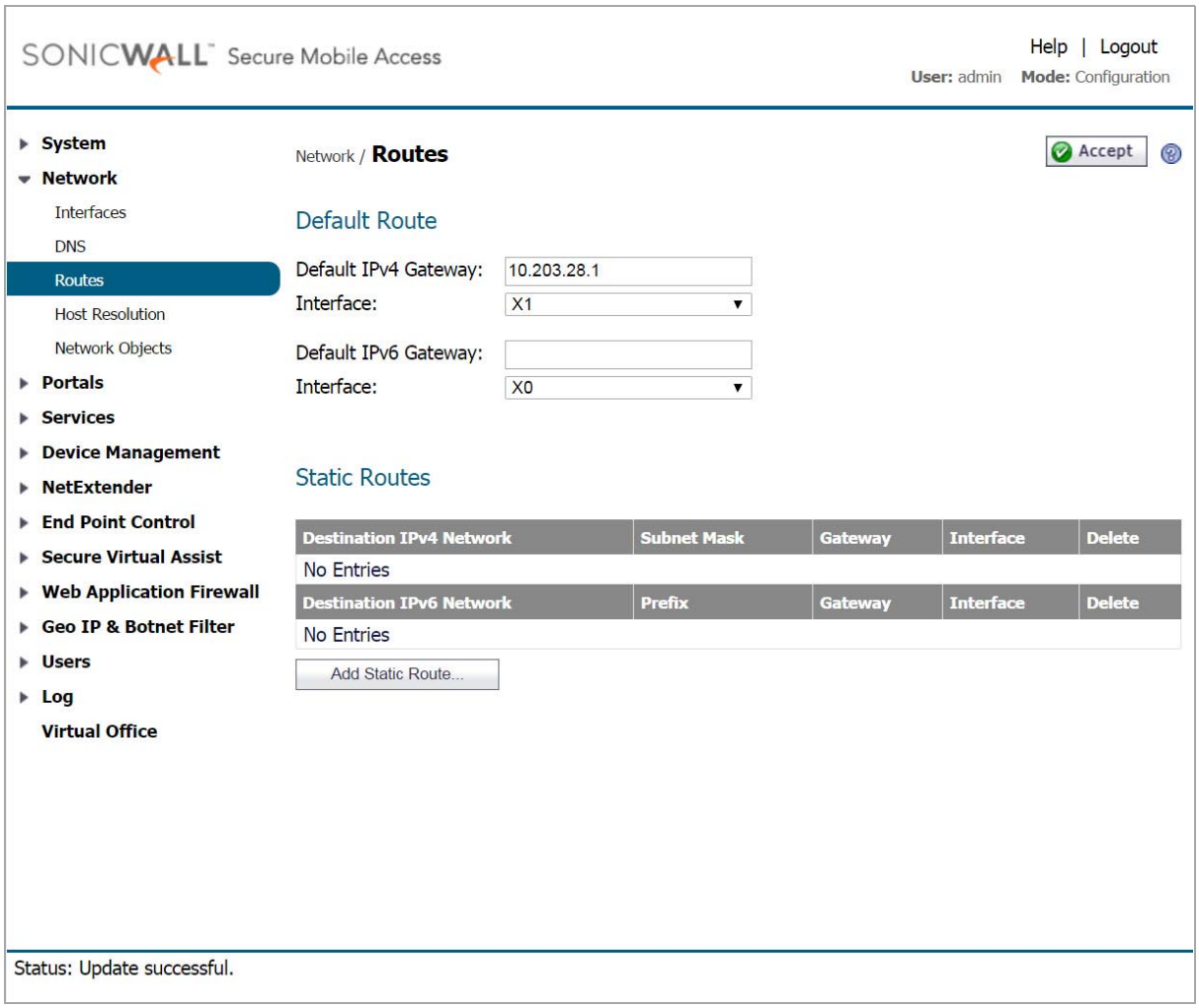
This section provides an overview of the **Network > Routes** page and a description of the configuration tasks available on this page.

- Network > Routes Overview on page 134
- Configuring a Default Route for the SMA/SRA Appliance on page 136
- Configuring Static Routes for the Appliance on page 136

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 Getting Started Guide for your appliance model.

Network > Routes Page

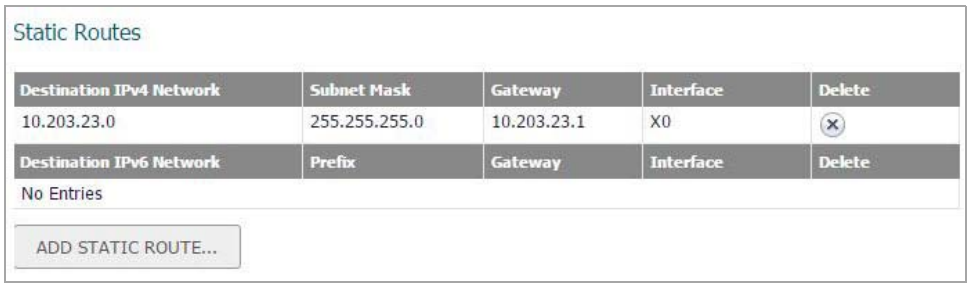


Default Route

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 gateway and interface. 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.



Configuring a Default Route for the SMA/SRA Appliance

You must configure a default gateway on your SMA/SRA 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 is the LAN IP address of the firewall interface to which the SMA/SRA appliance is connected. This is the default route for the appliance.

To configure the default route:

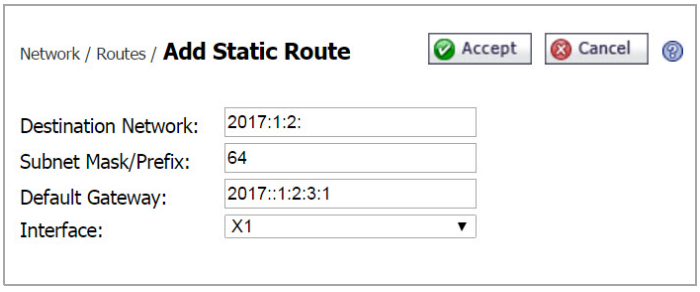
1. Navigate to the **Network > Routes** page.
2. In the **Default IPv4 Gateway** field, type the IP address of the firewall or other gateway device through which the SMA/SRA appliance connects to the network. This address acts as the default route for the appliance.
3. In the **Interface** drop-down list, select the interface that serves as the IPv4 connecting interface to the network. In most cases, the interface is X0.
4. In the **Default IPv6 Gateway** field, type the IPv6 address of the firewall or other gateway device through which the SMA/SRA appliance connects to the network. This address acts as the default IPv6 route for the appliance.
5. In the **Interface** drop-down list, select the interface that serves as the IPv6 connecting interface to the network.
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 SMA/SRA 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, complete the following steps:

1. Navigate to the **Network > Routes** page and click **Add Static Route..**.
2. In the **Add Static Route** dialog box, type the subnet or host to which the static route is 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, **2017:1:2::**).



3. In the **Subnet Mask/Prefix** field, enter the number of bits used for the prefix.
4. In the **Default Gateway** field, type the IP address of the gateway device that connects the appliance to the network.You can enter an IPv6 address.

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

6 Click **Accept**.

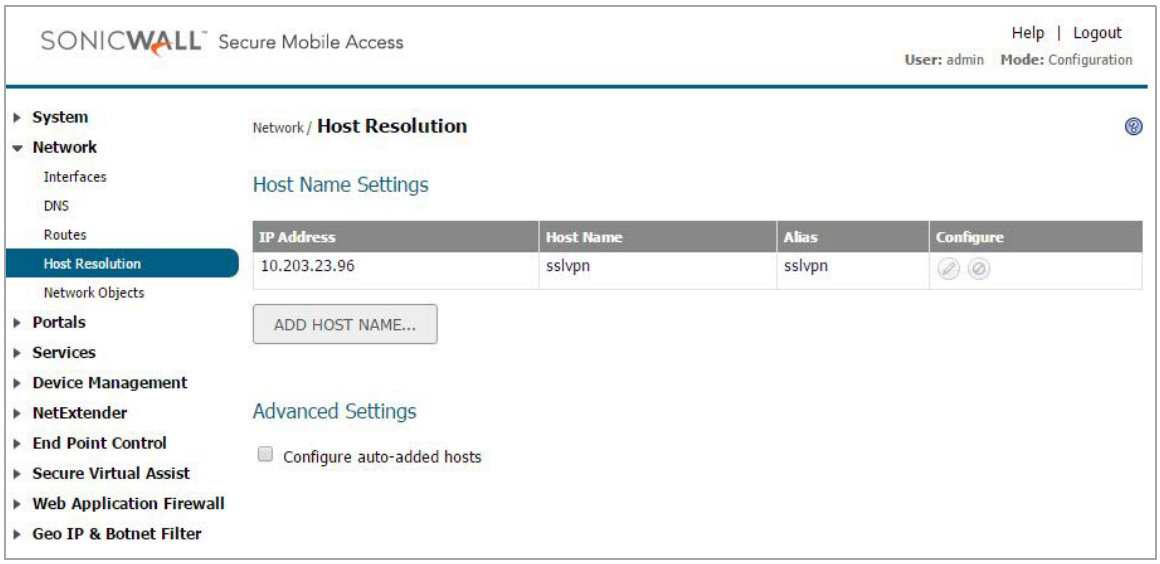
Network > Host Resolution

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.

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 SMA/SRA appliance itself. Do not delete it.

The SMA/SRA 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:

1. Navigate to the **Network > Host Resolution** page. The **Network** > **Host Resolution** page is displayed.
2. Click **Add Host Name**.
3. In the **Add Host Name** window, in the **IP Address** field, type the IP address that maps to the hostname.
4. In the **Host Name** field, type the hostname that you want to map to the specified IP address.
5. Optionally, in the **Alias** field, type a string that is the alias for the hostname.
6. Click **Add**. The **Host Resolution** page now displays the new host name.
7. Optionally select **Configure auto-added hosts** 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 on page 138
- Adding Network Objects on page 139
- Editing Network Objects on page 139

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.

You can create IPv6 network objects using IPv6 object types and addresses.

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 & Mobile Connect

- Terminal Services (RDP)
- 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.

Adding Network Objects

To add a network object:

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

2 Click **Add Network Object...** The **Add Network Object** screen is displayed.

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

> **NOTE:** To edit an existing network object, select **Configure** next to the object you want to edit. A new network object with the same name as an existing network object does not replace or modify an existing network object.

4 Click on the **Service** list and select a service type: Web (HTTP), Secure Web (HTTPS), NetExtender, Terminal Services (RDP), Virtual Network Computing (HTML5), File Transfer Protocol, Telnet, Telnet (HTML5), Secure Shell Version 1 (SSHv1), Secure Shell Version 2 (SSHv2), File Shares (CIFS), or Citrix Portal.

5 Click **Accept**. The **Edit Network Object** screen is displayed, showing the network object name and the service associated with it. To complete the object by adding addresses mapped to the network object, see Editing Network Objects on page 139.

Editing Network Objects

To edit a network object, complete the following steps:

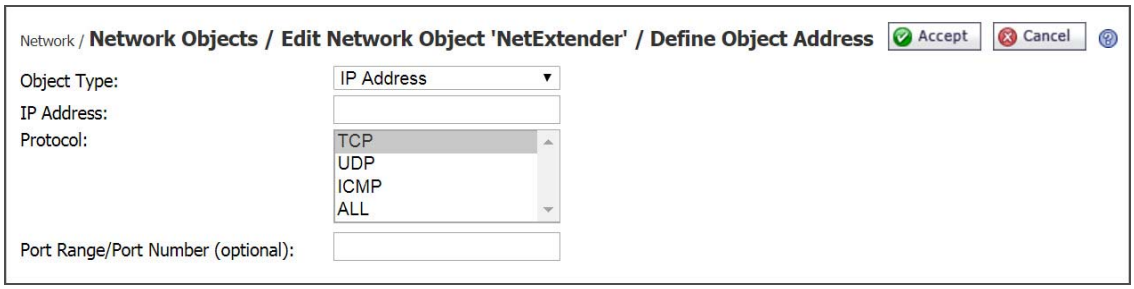
1 To edit an existing network object, navigate to the **Network** > **Network Objects** page and click the Configure icon or click the **Incomplete** link for the object you wish to edit. The **Edit Network Object** screen is displayed.

If you just created a network object, the **Edit Network Object** screen is displayed as soon as you clicked **Accept**.

The **Edit Network Object** shows 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.

2 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 **Done** if finished.

3 To add or edit **Object Type** and **IP Address** values for this Network Object, click **Add**. The **Define Object Address** page is displayed.



4 Select the desired **Protocol**. The available value options in the Protocol field include: **TCP**, **UDP**, **ICMP**, and **ALL**. You can select multiple items among **TCP**, **UDP** and **ICMP**. However, when **ALL** is selected, all others options are deselected.

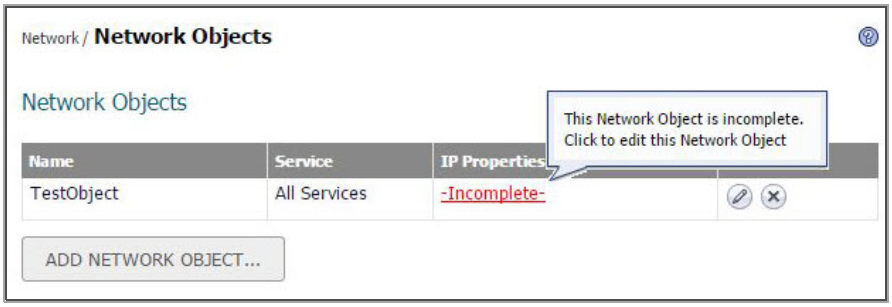
NOTE: The protocol setting only appears when the Service is set to "NetExtender & Mobile Connect" or "All Services."

5 Click **Accept** to add the Object Address to the Network Objects.

6 When finished adding addresses, click **Done** in the Edit Network Object screen.

7 The **Network** > **Network Objects** page is displayed with the new network object in the **Network Objects** list.

8 If the object is not fully defined with at least one IP address or network range, the status **Incomplete** displays. Click the **Incomplete** link or the Configure icon to edit the network object again, and then click **Add** to add Type and Address values for this network object. The **Define Object Address** page is displayed.



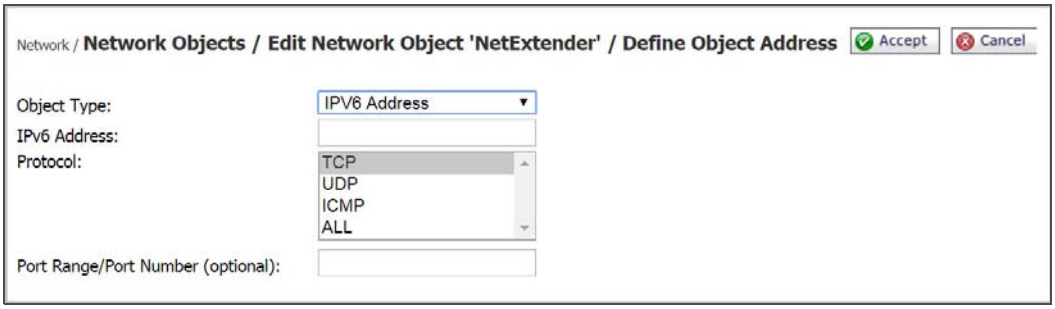
NOTE: Policies cannot be created for incomplete network objects.

Defining an Object Address

1 In the **Define Object Address** page, click on the **Object Type** drop-down list and select an object type. The four object types are:

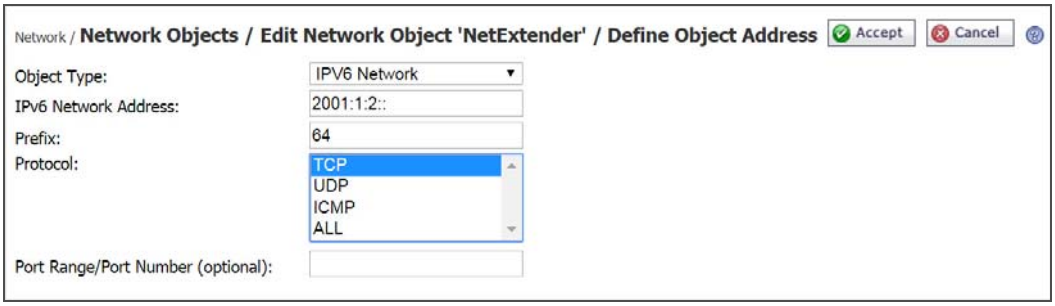
- **IP Address** - A single IP address.

- **IP Network** - 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.



2 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.



3 When finished adding addresses, click **Done** in the Edit Network Object dialog box.

5

Portals Configuration

This section provides information and configuration tasks specific to the **Portals** pages on the Secure Mobile Access web-based management interface, including configuring portals, assigning portals, and defining authentication domains, such as RADIUS, LDAP, and Active Directory.

Topics:

Portals > Portals

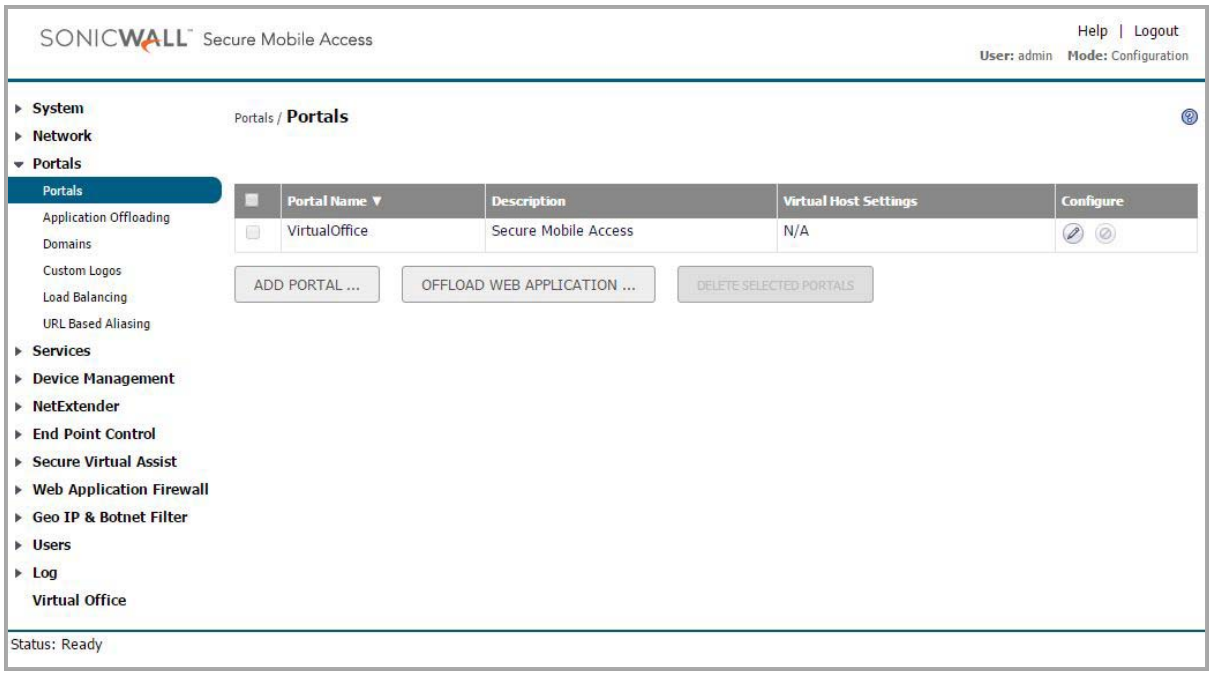
This section provides an overview of the **Portals > Portals** page and a description of the configuration tasks available on this page.

For information about Application Offloading and **Offload Web Application**, see Portals > Application Offloading on page 158.

Portals > Portals Overview

The **Portals > Portals** page allows the administrator to configure a custom portal for the Secure Mobile Access portal login page as well as the portal home page.

Portals > Portals page



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, login uniqueness, and client source uniqueness.

Additional Information About the Portal Home Page

For most Secure Mobile Access 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:

- 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 is displayed following all other content on the home page. You can also add HTML tags and JavaScript to the **Home Page Message** field.
- Because the uploaded HTML file is displayed after other content, do not include <head> or <body> tags in the file.

Adding Portals

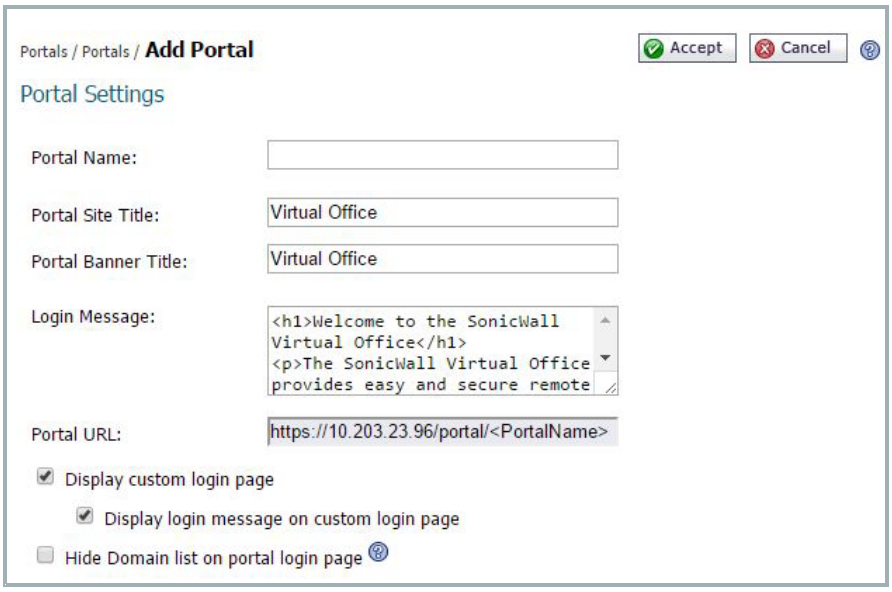
The administrator can customize a portal that appears as a customized landing page to users when they are redirected to the SMA/SRA appliance for authentication.

The network administrator might 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:

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



The following Table provides a description of the fields you can configure in the **General** section. Refer to Configuring General Portal Settings on page 145 for the specific steps required to configure a custom portal.

General Section 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 appears on the Web browser title bar of users access this portal.
Portal Banner Title	The welcome text that appears on top of the portal screen.
Login Message	Optional text that appears on the portal login page above the authentication area.
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 login page for this portal.
Display login message on custom login page	Displays the text specified in the Login Message text box.
Hide Domain list on portal login page	If enabled, this option replaces the Domain list box on the login page to a text box. The user can then type in the correct domain name. This option is only enabled for portal login through Web.
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.
Enable ActiveX Web cache cleaner	Loads an ActiveX control (browser support required) that cleans up all session content after the Secure Mobile Access session is closed.

General Section Fields (Continued)

Field	Description
Enforce login uniqueness	If enforced, login uniqueness restricts each account to one session at a time. Select to **Automatically logout existing session** or **Confirm logout of existing session** as the preferred Enforcement Method. If not enforced, each account can have multiple simultaneous sessions.
Enforce client source uniqueness	If enforced, client source uniqueness prevents multiple connections from a user with the same client source address when connecting with a SonicWall Inc. client (NetExtender, Mobile Connect, Virtual Assist, and so on). This prevents a user from consuming multiple licenses when a user reconnects after an unexpected network interruption.
Small Logo	Specify the link for the small logo. The recommended size is 128 x 128.
Medium Logo	Specify the link for the medium logo. The recommended size is 270 x 270.
Wide Logo	Specify the link for the wide logo. The recommended size is 558 x 270.
Large Logo	Specify the link for the large logo. The recommended size is 558 x 558.
Background Color	Specify the background color for Live Tile. The default setting is #0085C3.
Site Name	Specify the display name for the bookmark. The default setting is your portal name.

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 in the General section for a new portal:

1. Navigate to the **Portals > Portals** page.
2. Click **Add Portal** or Configure next to the portal you want to configure. The **Add Portal** or **Edit Portal** screen displays.
3. In the General section, enter a descriptive name for the portal in the **Portal Name** field. This name is part of the path of the Secure Mobile Access portal URL. For example, if your Secure Mobile Access portal is hosted at **https://vpn.company.com**, and you created a portal named “sales,” then users are 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 is truncated before the first non-alphanumeric character.

4. Enter the title for the Web browser window in the **Portal Site Title** field.
5. To display a banner message to users before they log in to the portal, enter the banner title text in the **Portal Banner Title** field.
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.
7. The **Portal URL** field is automatically populated based on your SMA/SRA appliance network address and Portal Name.

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

> **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 in Adding a Custom Portal Logo on page 156.

9 Select **Enable HTTP meta tags for cache control** 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 SMA 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.

10 Select **Enable ActiveX Web cache cleaner** to load an ActiveX cache control when users log in to the SMA/SRA appliance. The Web cache cleaner prompts 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 do not support ActiveX.

11 See Enforcing Login Uniqueness on page 146.

12 See Enforcing Client Source Uniqueness on page 146.

13 Specify the link(s) for the **Small** / **Medium** / **Wide** / **Large** Logo to be used with Live Tile.

14 Specify the **Background Color** for Live Tile. If no value is specified, the default color is #0085C3.

15 Specify the **Site Name** to be displayed for Live Tile. If no value is specified, the default is the Portal Name.

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:

1 Navigate to **Portals > Portals.**

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

3 Select **Enforce login uniqueness**.

4 Click **Accept**.

Enforcing Client Source Uniqueness

Client source uniqueness, when enforced, prevents multiple connections from a user with the same client source address when connecting with a SonicWall Inc. client (NetExtender, Mobile Connect, Virtual Assist, and so on). This prevents a user from consuming multiple licenses when a user reconnects after an unexpected network interruption.

For example, a user on an unreliable network is disconnected because of a network issue. If login uniqueness is NOT enabled, the user session on the appliance stays active for this type of disconnect until the timeout value is reached. The user reconnects and consumes a second license with the potential of consuming more licenses before the timeout disconnects them.

To enforce client source uniqueness:

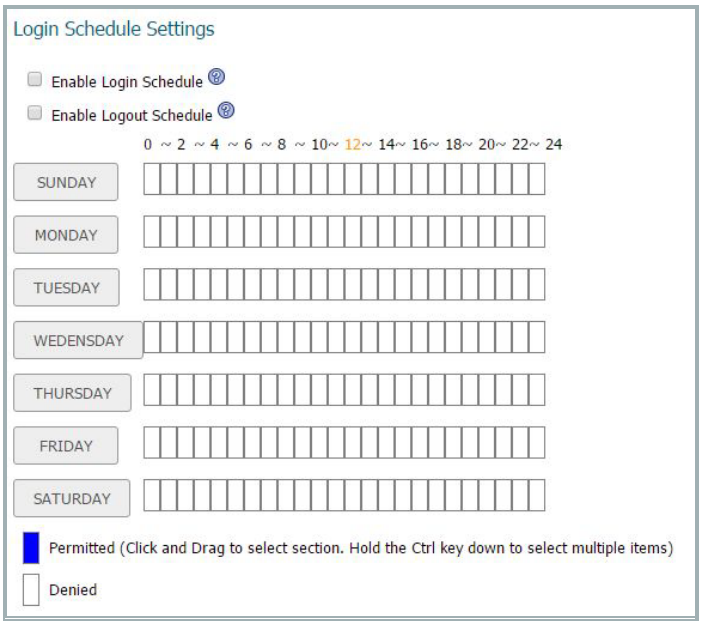
1. Navigate to **Portals > Portals.**
2. For an existing portal, click the configure icon next to the portal you want to configure. Or, for a new portal, click **Add Portal**.
3. Select **Enforce client source uniqueness**.
4. Click **Accept**.

Configuring Login Schedules

The login schedules section allows you to restrict access to a portal based on the time specified.

To enable login schedules:

1. Navigate to **Portals** > **Portals**.
2. Select the existing portal you want to configure.
3. Go to the **Login Schedule** section. The Login Schedule displays.



4. Click **Enable Login Schedule**.
5. Set the login schedule by clicking the time slot on the day you wish to permit or deny access. To select multiple items, hold the Ctrl key down. You can also click **Day** to select the whole day.
6. Click **Accept** to save changes made to the login schedule.

Configuring the Home Page

The home page is an optional starting page for the Secure Mobile Access appliance portal. The home page enables you to create a custom page that mobile users see when they log in to 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 Secure Mobile Access-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.

See also:

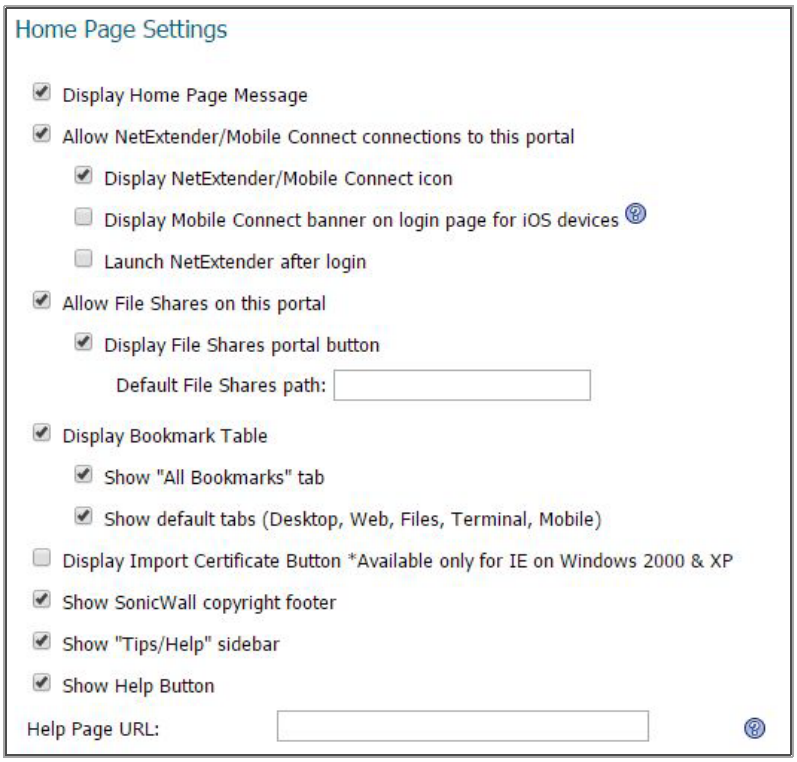
- Enabling NetExtender to Launch Automatically in the User Portal on page 150
- File Sharing Using “Applet as Default” on page 150

To configure the home page:

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

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

3 Go to the **Home Page** section.



The following table provides a description of the configurable options in the Home Page section.

Home Page Section Fields

Field	Description
Display Home Page Message	Displays the customized home page message after a user successfully authenticates to the SMA/SRA appliance.
Allow NetExtender/Mobile Connect connections to this portal	If selected, activates the following two check box options. If not selected, NetExtender and Mobile Connect are not available on the portal.
Display NetExtender/Mobile Connect Icon	Displays the icon to NetExtender or Mobile Connect, allowing users to install and invoke the clientless NetExtender virtual adapter, or the Mobile Connect application for mobile devices.

Home Page Section Fields (Continued)

Field	Description
Display Mobile Connect banner on login page for iOS devices	Displays the Mobile Connect banner on the login page for devices running iOS 6 or higher.
Launch NetExtender after login	Launches NetExtender automatically after a user successfully authenticates to the SMA/SRA appliance. See Enabling NetExtender to Launch Automatically in the User Portal on page 150.
Allow File Shares on this portal	If selected, activates the following two check box options. If not selected, File Shares are not accessible from the portal.
Display File Shares portal button	Provide a button to link to the File Shares (Windows CIFS/SMB) Web interface according to their domain permissions. See File Sharing Using "Applet as Default" on page 150
Use Applet for portal button	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.
Default File Shares path	Specify the specific file share path when allowing file shares on the portal. If nothing is specified, the file share provides a link for the user to find all available domains. The file share also lists all available file share bookmarks for the user to launch.
Display Bookmark Table	If selected, activates the following two check box options. If not selected, Bookmarks are not available from the portal.
Show "All Bookmarks" tab	Displays the tab containing administrator-provided bookmarks and allows users to define their own bookmarks to network resources.
Show default tabs (Desktop, Web, Files, Terminal)	Displays the default bookmark tabs.
Display Import Certificate Button	Displays a button that allows users to permanently import the SSL security certificate.
Show SonicWall Inc. copyright footer	Displays SonicWall Inc. 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 **Legacy Look & Feel** is selected on the General tab.
Show Help Button	Displays the **Help** button.
Help Page URL	Specify the URL for the Help Page. Leave this field blank to use the default SonicWall Inc. Help Page.
Show Options Button	If selected, displays the **Options** button.
Home Page Message	Optional text that can be displayed on the home page after successful user authentication.

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 disables access to the DFS file shares from other domains. The SMA/SRA appliance is not a domain member and cannot connect to the DFS file shares. DFS file shares on a stand-alone root are not affected by this Microsoft restriction.
- Some ActiveX applications, such as the ActiveX Terminal Services RDP client, only works 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 SMA/SRA appliance, then you can select **Display Import self-signed certificate links** 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 **Display Import self-signed certificate links**.

4 Click **Accept** 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:

1 Navigate to **Portals > Portals**

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

3 Click the **Home Page** section.

4 To prevent users from accessing NetExtender through this portal, clear **Allow NetExtender connections to this portal**. Because Mobile Connect acts as a NetExtender client when connecting, clearing this check box also prevents Mobile Connect users on this portal.

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

6 Click **Accept**.

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:

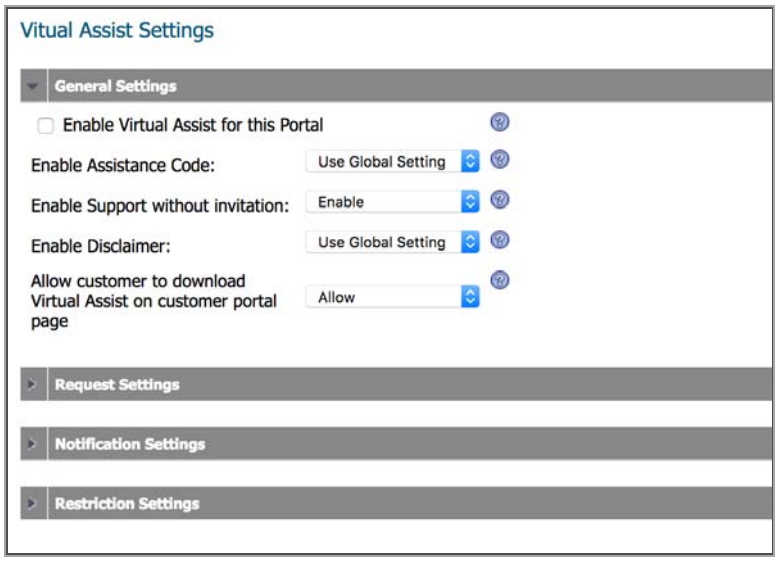
- Overwriting of existing files
- Uploading directories
- Drag-and-drop capability
- Multiple file selection
- Contextual click capability
- Sortable file listings
- Ability to navigate directly to folders by entering path
- Back and forward buttons with a drop-down history menu
- Properties window displays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

To use the Java File Shares Applet on this portal:

1. Navigate to **Portals > Portals**.
2. Click **Add Portal** or **Configure** next to the portal you want to configure. The **Add Portal** or **Edit Portal** screen displays.
3. Click the **Home Page** section.
4. Select **Display File Shares portal button**.
5. Select **Use Applet for portal button**.
6. Click **Accept** to save changes.

Configuring Per-Portal Virtual Assist Settings

The administrator can enable Secure Virtual Assist on a per-portal basis.



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

To configure the Virtual Assist settings for a portal:

1. Navigate to **Portals > Portals**.
2. Click **Add Portal** or **Configure** next to the portal you want to configure. The **Add Portal** or **Edit Portal** screen displays.
3. Go to the **Virtual Assist** section.
4. To allow Virtual Assist on this portal, select **Enable Virtual Assist for this Portal**.
5. Select **Display Technician Button**. If this box is not selected, **Virtual Assist** is hidden and technicians are required to login directly through a downloaded client.
6. Select **Display Request Help Button** to allow users to request assistance through the portal.
7. Select **Enable Virtual Access Mode** to allow Secure Virtual Access connections to be made to this portal. This must be enabled per-portal for Secure Virtual Access to function. If this box is selected, you can then select **Display Virtual Access Setup Link** to display the corresponding link on the portal. For more information on Secure Virtual Access functionality, see Enabling a System for Secure Virtual Access on page 63.

8 Use the **Run Virtual Assist without installation** feature to allow users to launch Virtual Assist without installing it on the client machine. This feature can be enabled globally or per portal. Select one of the following from the drop-down list:

- Select **Use Global Setting** to apply the global setting to this portal.
- Select **Enable** for this portal to launch Virtual Assist from the web without installing it, no matter what is selected for the global setting.
- Select **Disable** for this portal to install Virtual Assist when accessing it from the web, no matter what is selected for the global setting.

9 Use the **Wake customer on LAN** feature to allow Technicians to wake a client running Virtual Assist on the LAN if both are in the same subnet. The client can be woken when powered off, in the Sleep state, or in the Hibernate state. This feature can be enabled globally or per portal.

- Select **Use Global Setting** to apply the global setting to this portal.
- Select **Enable** this feature, no matter what is selected for the global setting.
- Select **Disable** this feature, no matter what is selected for the global setting.

NOTE: To use Wake Client, this feature must be configured on the client machine, as explained in the *Secure Mobile Access User Guide*.

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

11 Check **Enable Assistance Code** to require a user to enter the designated code before requesting assisting. Checking this check box displays an **Assistance Code** field, where you specify the code users must enter.

12 See Secure Virtual Assist > Settings on page 270 for information about all other configuration settings in the Virtual Assist section.

13 Expand each section of the page to configure the related options.

14 Click **Accept** to save changes.

Configuring Virtual Meeting Settings

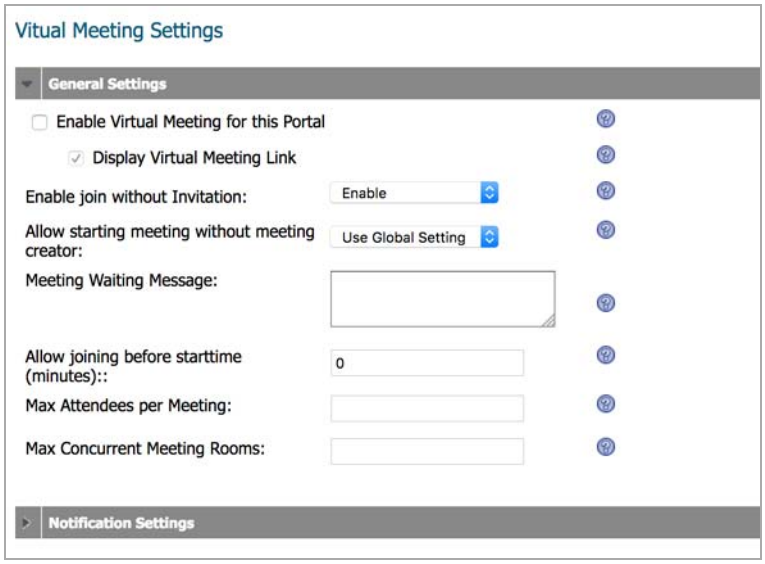
The Virtual Meeting section allows you to configure Virtual Meeting settings for the portal. There is a General Settings section and a Notification Settings section that can both be configured.

To configure Virtual Meeting Settings:

1 Navigate to **Portals > Portals**.

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

3 Go to the **Virtual Meeting** section.



4 Navigate to the **General Settings** section.

5 To allow Virtual Meeting control for users logging in through this portal, select **Enable Virtual Meeting for this Portal**.

With the Virtual Meeting for this Portal option enabled, select **Display Virtual Meeting Link** to have the Virtual Meeting icon link for a download or install.

6 To allow participants to join a meeting without an invite from the coordinator, select to Use Global Setting, Enable, or Disable in the **Enable join without Invitation** field. If this option is disabled, participants can only join a meeting by invite from a meeting creator.

7 To allow a participant to act as the meeting coordinator if the coordinator is not present at the beginning of a meeting, select to Use Global Setting, Enable, or Disable in the **Allow starting meeting without meeting creator** field.

8 Create a default message to display when the meeting has not started in the **Meeting Waiting Message** field. If this field is left blank, Virtual Meeting uses the global setting for this option.

9 Set the Allow joining before start time with a value in minutes. This is the time before a scheduled meeting start time that participants are allowed to join the meeting. After a participant is in the meeting lobby, a license is considered in use. Set this field to 0 to allow an unrestricted amount of time to join the meeting. If this field is left blank, Virtual Meeting uses the global setting for this option.

10 Set the maximum number of concurrent systems for a meeting in the **Max Attendees per Meeting** field. Set this field to 0 to allow an unrestricted amount of meeting attendees. If this field is left blank, Virtual Meeting uses the global setting for this option.

11 Set the maximum concurrent active meetings at a time for this appliance in the **Max Concurrent Meeting Room field**. Set this field to 0 to allow an unrestricted amount of meeting rooms. If this field is left blank, Virtual Meeting uses the global setting for this option.

12 Next, navigate to the **Notification Settings** section.

13 In the **Subject of Invitation** field, specify the subject for the email invitation to Virtual Meeting. The following variables can be used for this field:

- %COORDINATOR% - Coordinator Name
- %MEETINGNAME% - Meeting Name
- %MEETINGCODE% - Meeting Code

- %STARTTIME% - The start date and time of the meeting
- %ENDTIME% - The end date and time of the meeting
- %MEETINGDESCRIPTION% - A description of the meeting

Note that variables are case-sensitive. If this field is left blank, Virtual Meeting uses the global setting for this option.

14 In the **Invitation Message** field, specify the body of the invitation to Virtual Meeting. The following variables can be used for this field:

- %COORDINATOR% - Coordinator Name
- %MEETINGNAME% - Meeting Name
- %MEETINGCODE% - Meeting Code
- %STARTTIME% - The start date and time of the meeting
- %ENDTIME% - The end date and time of the meeting
- %MEETINGDESCRIPTION% - A description of the meeting

Note that variables are case-sensitive. If this field is left blank, Virtual Meeting uses the global setting for this option.

15 Click **Accept** to save changes.

Configuring Virtual Host Settings

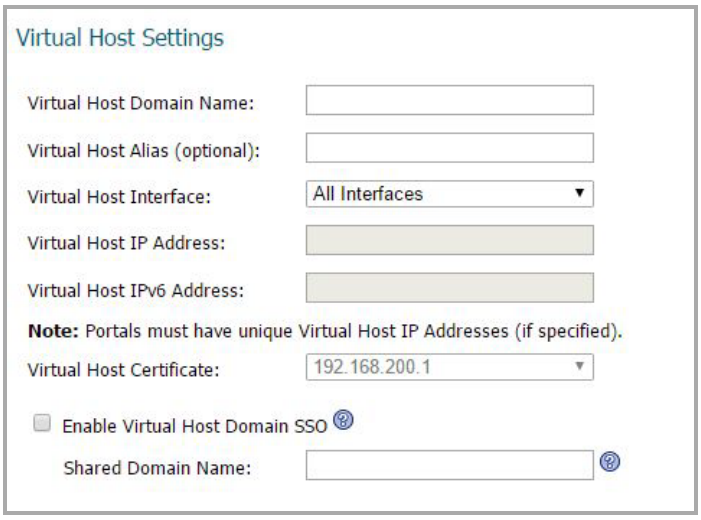
Creating a virtual host allows users to log in using a different hostname than your default URL. For example, sales members can access **https://sales.company.com** instead of the default domain, **https://vpn.company.com** that you use for administration. The Portal URL (for example, **https://vpn.company.com/portal/sales**) still exists 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.

To create a Virtual Host Domain Name:

1 Navigate to **Portals > Portals**.

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

3 Go to the **Virtual Host** section.



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

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

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

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.

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 use 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 SMA/SRA appliance.

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. 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

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.

Unless you have a certificate for each virtual host domain name, or if you have purchased a *.domain SSL certificate, your users might see a **Certificate host name mismatch** warning when they log in to the Secure Mobile Access Virtual Office portal. The certificate hostname mismatch affects the login page, NetExtender, and Secure Virtual Access/Assist/Meeting clients; Other Secure Mobile Access client applications are not affected by a hostname mismatch.

To achieve a single point of access for users, configure External Website Bookmarks for application offloading portals by selecting **Enable Virtual Host Domain SSO** to enable cross domain Single Sign-On (SSO). Cross Domain SSO shares the credentials for all portals in the same shared domain. Enabling Virtual Host Domain SSO automatically sets the Shared Domain Name one level up from the Virtual Host Domain name and displays it in the **Shared Domain Name** field. For example, the Shared Domain Name is example.com if the Virtual Host Domain is webmail.example.com.

NOTE: In previous releases, users had to log in twice – once for the regular portal and once for the application offloading portal after External Website Bookmark redirection. The Cross Domain SSO feature allows users after logging into the main portal to automatically log in to application offloading portals or Web sites that share the same Virtual Host Domain.

9 Under the **Advanced SSL/TLS settings** section, the Enforce Forward Secrecy field allows you to: **Use Global Setting**, **Enable**, or **Disable** the feature. Enable this option to allow current information to be kept in secrecy, even if the private key is compromised in the future. Note that browsers that do not support Forward Secrecy might not be able to connect to the SMA/SRA appliance. The performance of this feature can decline depending on the ciphers that the client browser supports.

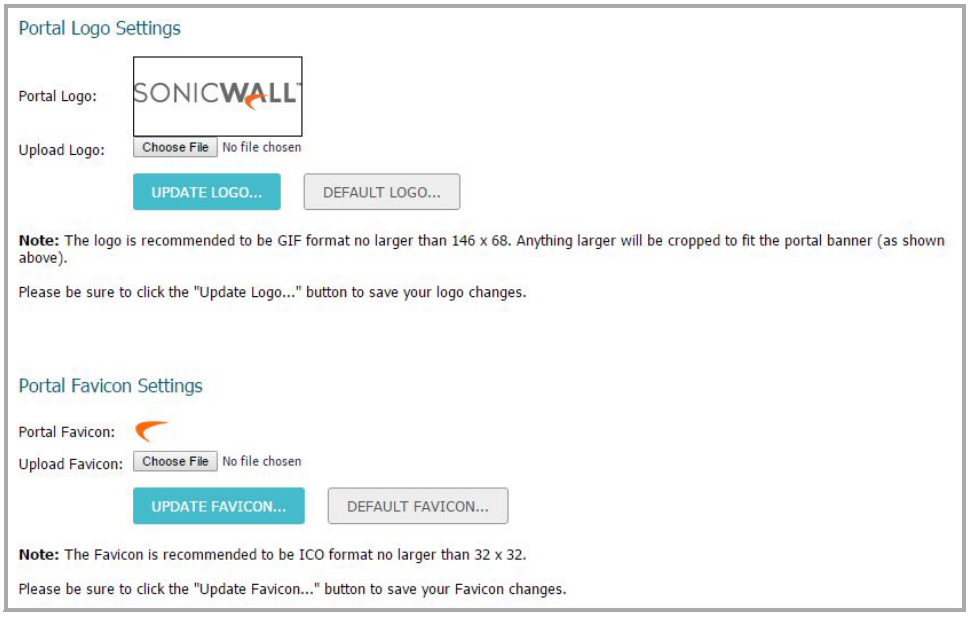
10 **Verify Backend SSL Server Certificate for Proxy connections** — When this option is enabled, the connection is dropped if the backend SSL/TLS server certificate is not trusted. The verification depth is 10. Alert level log messages are also generated when this option is enabled.

11 Enable **Force SSL/TLS version for Proxy connections** to enable communication between the Virtual Host and the Backend Server.

Adding a Custom Portal Logo

The Custom Logo Settings section allows the administrator to upload a custom portal logo and to toggle between the default SonicWall Inc. logo and a custom uploaded logo. You can also upload a custom portal favicon in this section. You must add the portal before you can upload a custom logo or custom favicon. In the Add Portal screen, the Logo section does not have an option to upload a custom logo or custom favicon.

NOTE: A Logo or Favicon can also be customized for OWA access.



To add a custom portal logo:

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

2 Go to the **Logo** section.

3 Click **Choose File** by the **Upload Logo** field. The file browser window displays.

4 Select an appropriate-sized .gif format logo in the file browser and click **Open**.

> **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 is 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.

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

6 Click **Update Logo** to transfer the logo to the SMA/SRA appliance.

7 Click **Default Logo** to revert to the default SonicWall Inc. logo.

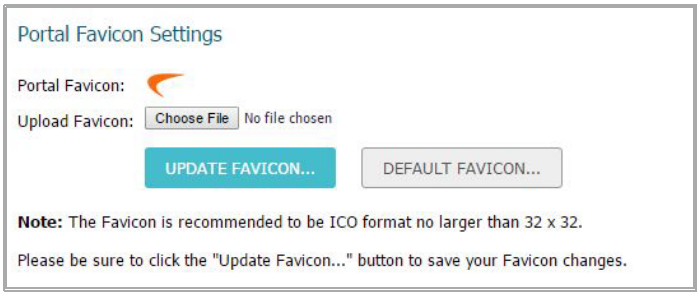
8 Click **Accept** to save changes.

To add a custom favicon:

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

2 Go to the **Logo** section. Navigate to the **Portal Favicon Settings** section.

3 Click **Choose File** by the **Upload Favicon** field. The file browser window displays.



4 Select an appropriate-sized ICO format favicon in the file browser and click **Open**.

> **NOTE:** The custom favicon logo must be in ICO format. The custom favicon size must not be larger than 32x32 pixels.

5 Click **Update Favicon** to transfer the favicon to the SMA/SRA appliance.

6 Click **Default Favicon** to revert to the default SonicWall Inc. favicon.

7 If authentication control of the portal is disabled, **Reuse Favicon to Offload Server** is available. Enabling this option allows the favicon of the backend server to display in the client browser.

8 Click **Accept** to save changes.

NOTE: Favicon behavior can differ in each browser, especially when the favicon is cached. Sometimes a refresh or cleaning of the cache is needed to display the favicon properly.

Portals > Application Offloading

The **Portals > Application Offloading** page in the Secure Mobile Access 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 **Offload Web Application** to configure an offloaded application.

See the following sections:

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 might 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 Inc. 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 Secure Mobile Access 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 Secure Mobile Access:

- 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 Secure Mobile Access 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 SMA/SRA 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.

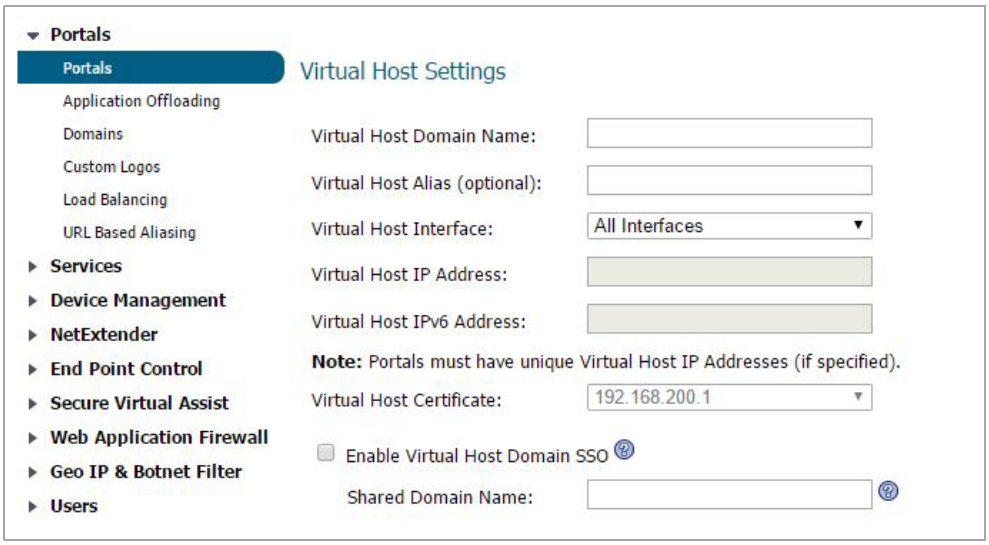
NOTE:

- The maximum number of users supported is limited by the number of applications being accessed and the volume of application traffic being sent.
- The Application Offloading feature does not work well when the application refers to resources within the same host using absolute URLs. In this case, you might need to convert an absolute URL reference to its relative form.
- Further information about configuring specific backend Web applications is available in the *Secure Mobile Access Application Offloading and HTTP(S) Bookmarks* feature module, available under **Support** on www.sonicwall.com.

Configuring an HTTP/HTTPS Application Offloading Portal

To offload a Web application and create a portal for it:

1 Navigate to **Portals > Portals** and go to the **Virtual Host** section. The Virtual Host Settings screen opens. This allows you to access the Portal directly.



2 Enter a descriptive name in the **Virtual Host Domain Name** field.

3 On the **Offloading** tab, select **Enable Load Balancing** for load balancing among offloaded application servers.

4 Select one of the following from the **Scheme** drop-down list:

- **Web (HTTP)** – access the Web application using HTTP (default scheme)
- **Secure Web (HTTPS)** – access the Web application using HTTPS
- **Auto (HTTP/HTTPS)** – allows the user to determine the actual scheme used to talk to the backend server when accessing an offloading portal. Access is still under the control of the access policy.

  When using the Auto scheme, users can type http://www.example.virtual.host.com or https://www.example.virtual.host.com in browser's address bar to test this feature. Even scheme set to Auto, it's still under the control of the access policy.

△ **CAUTION: It is the Administrator's responsibility to configure the correct scheme used to talk to the backend server. Auto (HTTP/HTTPS) Scheme can operate only if HTTP access is enabled for the Virtual Host (under the Virtual Host tab) and authentication is disabled (under the Offloading tab) that can be insecure. Therefore, you are prompted to click OK to enable HTTP for Virtual Host.**

- **Generic (SSL Offloading)** – use SSL offloading to access custom SSL applications (non-HTTP(S) applications)

  For more information about the **Generic (SSL Offloading)** option, see Configuring with the Offloading Portal Wizard on page 163.

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

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

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

8 In the **Homepage URI (optional)** field, optionally enter a URI to a specific resource on the Web server to which the user is forwarded the first time the user tries to access the Application Offloading Portal. This is a string in the form of: **/exch/test.cgi?key1=value1&key2=value2**

When this field is configured, it redirects the user to the Web site's home page the first time the user accesses the portal. This happens only when the user is accessing the site with no URL path (that is, when accessing the root folder, for example: https://www.google.com/). This is not an alias for the root folder. The user can edit the URL to go back to the root folder.

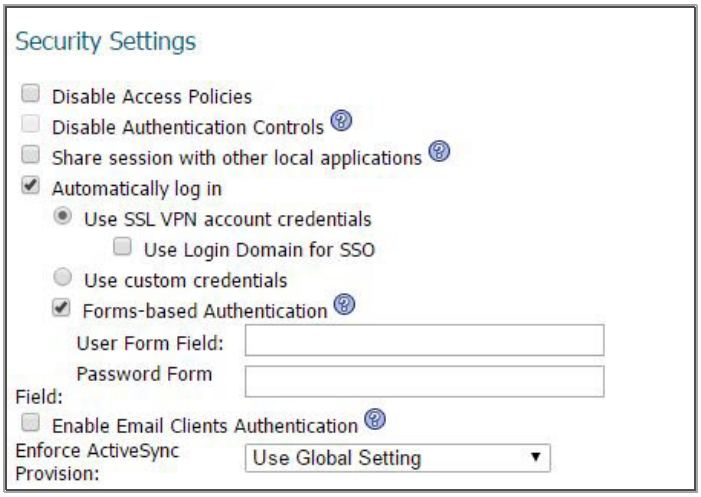
The key=value pairs allow you to specify URL query parameters in the URL. You can use these for any Web site that does not have a default redirect from the root folder to the home page URL. Outlook Web Access is one example, but note that most public sites do have a default redirect.

a Under Security Settings, select **Enable Web Application Firewall** to enable the feature.

b Select **Disable Authentication Controls, Access Policies, and CSRF Protection (if enabled)** if you need no authentication, access policies, or CSRF protection enforced. This is useful for publicly hosted Web sites.

a To configure ActiveSync authentication, clear **Disable Authentication Controls** to display the authentication fields. Select **Enable ActiveSync authentication** and then type the default domain name. The default domain name is not used when the domain name is set in the email client's setting.

9 Select **Automatically Login** to configure Single Sign-On settings.



10 For automatic login using SSO, select one of the following radio buttons:

- **Use SSL-VPN account credentials** – allow log in to the offloaded application using the credentials configured on the SMA/SRA appliance.
- **Use custom credentials** – displays **Username**, **Password**, and **Domain** fields where you can enter the custom credentials for the application or use dynamic variables. For the **Password** field, enter the custom password to be passed, or leave the field blank to pass the current user's password to the offloaded application portal. For the other fields, dynamic variables can be used, such as those shown in the following table:

Supported dynamic variables

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

11 If you selected **Automatically Login**, select **Forms-based Authentication** 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:

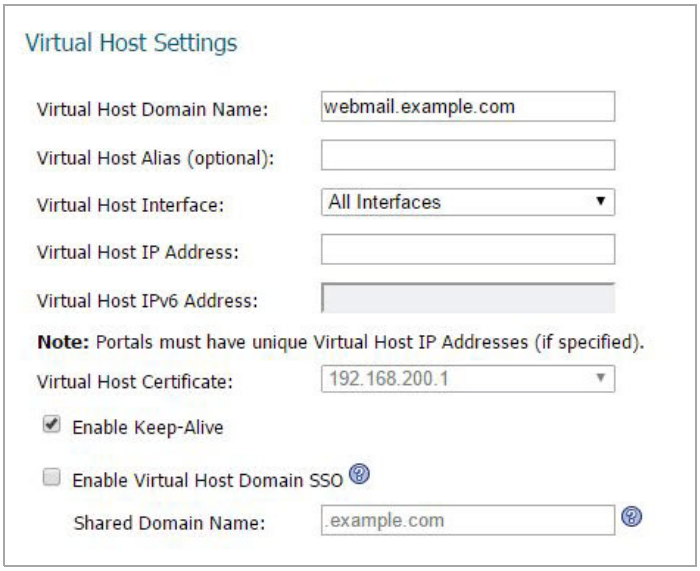
  `<input type=password name='PASSWORD' id='PASSWORD' maxlength=128>`

12 In the **Virtual Host** section, 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.

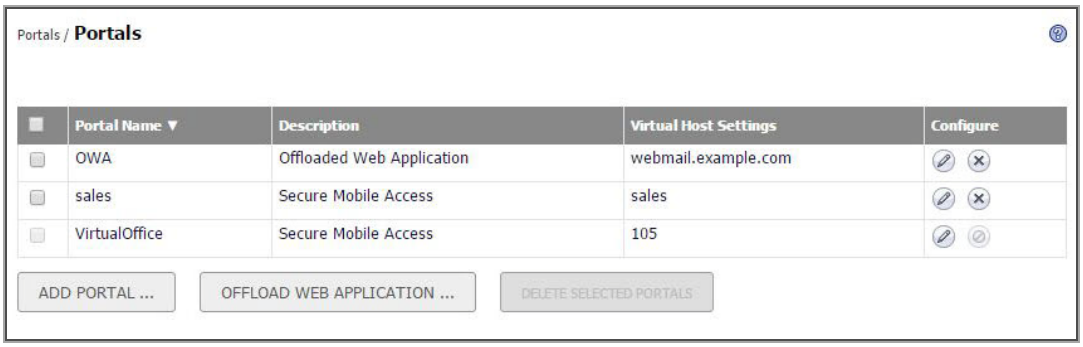
If you need to associate a certificate to this host, you should additionally set a virtual interface and import the relevant SSL certificate. You could avoid creating a virtual interface by importing a wildcard certificate for all virtual hosts on the SMA/SRA appliance.

See Configuring Virtual Meeting Settings on page 152 for more instructions on configuring the fields in this section.

13 If authentication is disabled for this portal, you have the option to **Enable HTTP access** for this Application Offloaded Portal. This feature is useful for setting up offloading in trial deployments.



14 Click **Accept**. You are returned to the **Portals > Portals** page where you see the Web application listed as an **Offloaded Web Application** under Description.



15 If you have not disabled authentication, navigate to the **Portals > Domains** page and create a domain for this portal. See Portals > Domains on page 180 for information about creating a domain.

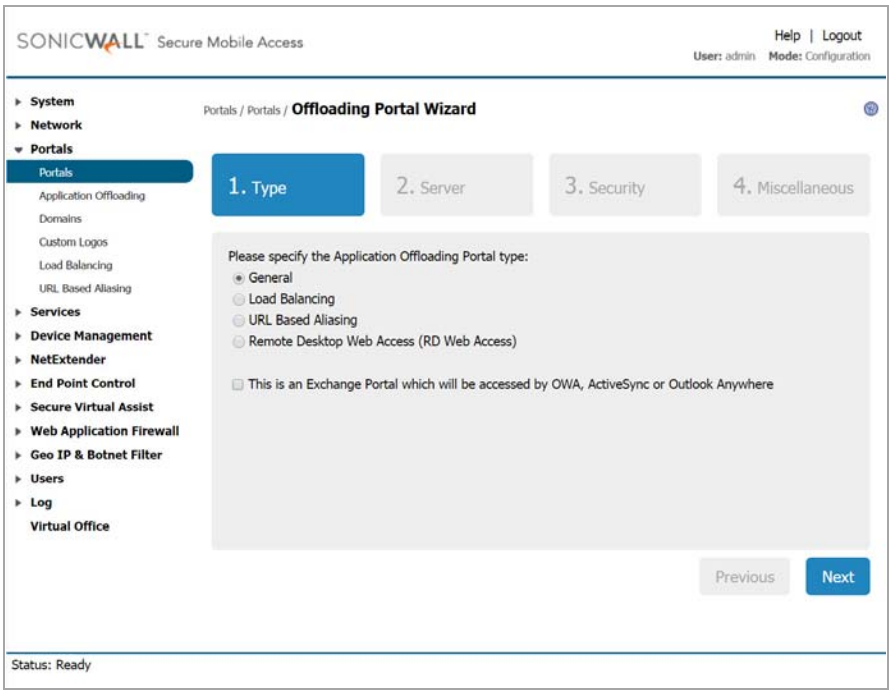
16 Update your DNS server for this virtual host domain name and alias (if any).

NOTE: In the future, without a WAF license, Anonymous Application Offloading access will not be supported. Activate a WAF subscription or use the trial version from the **System > Licenses** page.

Configuring with the Offloading Portal Wizard

To configure a portal with Offloading Portal Wizard:

1 Navigate to **Portals > Portals** and click **Offload Web Application**. The Offloading Portal Wizard opens.



2 Begin by selecting the Application Offloading Portal type. Options include:

- **General** portal - Can be selected for most scenarios.
- **Load Balancing** portal - This type of portal is used to setup a Load Balancing Offloading portal.

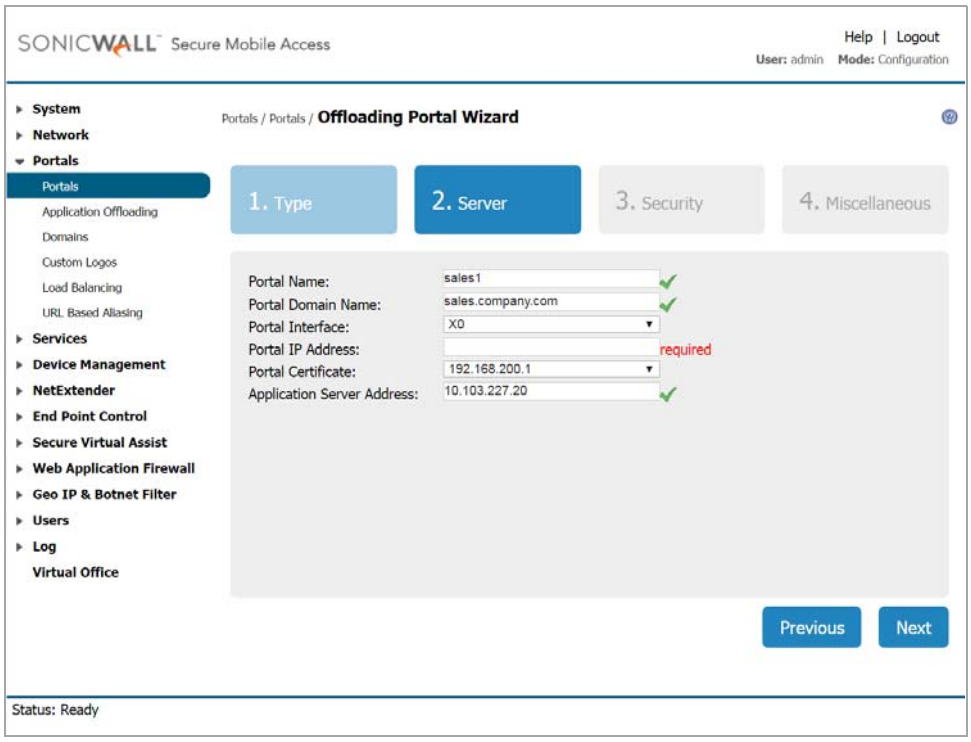
- **URL-based Aliasing** portal - Use to setup a URL-based Aliasing Offloading portal. Select **URL Based Aliasing** if you want the ability to access several Web sites using one portal and domain name. If this option is enabled, the screen options will change.
- **Remote Desktop Web Access (RD Web Access)** - The Remote Desktop (RD) Web Access page uses the SMA Agent to proxy the RDP connection to the private network to make the resource list on the RD Web site function more efficiently. Another advantage in using the RD Web Access option is that the it works for all browsers (Chrome, Firefox, and Internet Explorer).

3 Click **This is an Exchange Portal which will be accessed by OWA, ActiveSync or Outlook Anywhere** if using an Exchange portal.

4 Click **Next**.

General Server Settings

When **General** is selected on the initial page, the **Server** page appears as follows. The portal and application server settings can be set on this page.



1 In the **Portal Name** field, enter a unique name to identify different portals.

2 In the **Portal Domain Name** field, enter the domain name used to access the offloading portal.

3 In the **Portal Interface** field, enter the network interface to which the portal is bound. If one specific network interface is selected, a new IP address is assigned to the portal.

4 In the **Portal IP Address** field, enter the IP address where the portal is located.

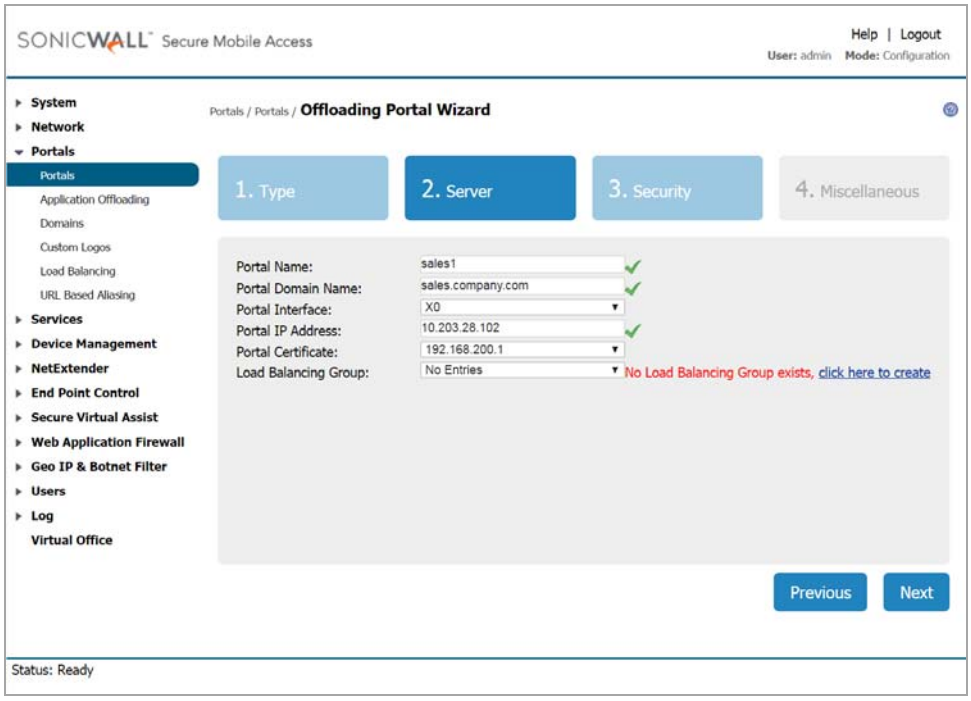
5 The **Portal Certificate** drop-down lists all certificates that have been imported.

6 The **Application Server Address** field accepts settings relevant to the application server. This can simply be the IP address of the application server. The scheme of the address is “HTTPS” by default. The port and default path can also be set in this single field.

All these settings are verified instantly from the Appliance when the mouse leaves the input field (green check). If the input fails, the reason it failed is shown. Only when all fields are satisfied, can you click **Next** to go to the next tab.

Load Balancing Server Settings

When **Load Balancing** is selected on the initial page, the **Server** page appears as follows.



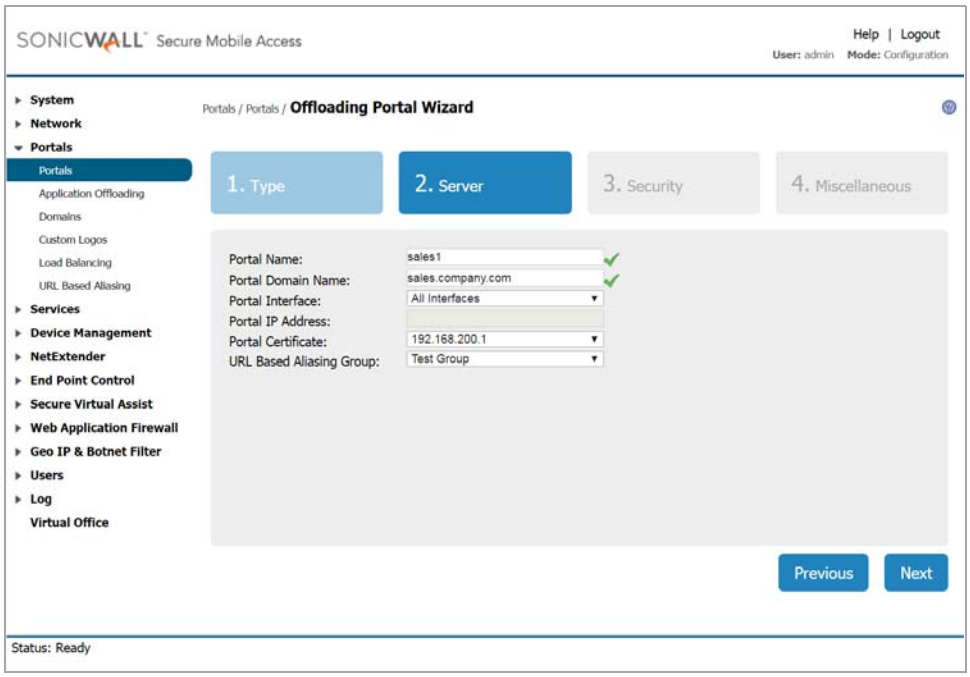
1. In the **Portal Name** field, enter a unique name to identify different portals.
2. In the **Portal Domain Name** field, enter the domain name used to access the offloading portal.
3. In the **Portal Interface** field, enter the network interface to which the portal is bound. If one specific network interface is selected, a new IP address is assigned to the portal.
4. In the **Portal IP Address** field, enter the IP address where the portal is located.
5. The **Portal Certificate** drop-down lists all certificates that have been imported.
6. The **Load Balancing Group** field replaces the **Application Server Address** field to show the existing Load Balancing Group to which you can assign to this portal. If no Load Balancing Group exists, you can create a new one by clicking “click here to create.”

All these settings are verified instantly from the Appliance when the mouse leaves the input field (green check). If the input fails, the reason it failed is shown. Only when all fields are satisfied, can you click **Next** to go to the next tab.

URL-based Aliasing Server Settings

Select **URL Based Aliasing** on the initial page when you want the ability to access several Web sites using one portal and domain name. When this option is enabled, the screen options change. You will need to select the

URL Based Aliasing Group from the drop down list. When **URL Based Aliasing** is selected on the initial page, the **Server** step appears as follows:



1 In the **Portal Name** field, enter a unique name to identify different portals.

2 In the **Portal Domain Name** field, enter the domain name used to access the offloading portal.

3 In the **Portal Interface** field, enter the network interface to which the portal is bound. If one specific network interface is selected, a new IP address is assigned to the portal.

4 The **Portal IP Address** field is not required if **All Interfaces** is selected in the **Portal Interface** field, but you need to enter the **Portal IP Address** of specific X0, X1, X2, and X3 interfaces.

5 The **Portal Certificate** drop-down lists all certificates that have been imported.

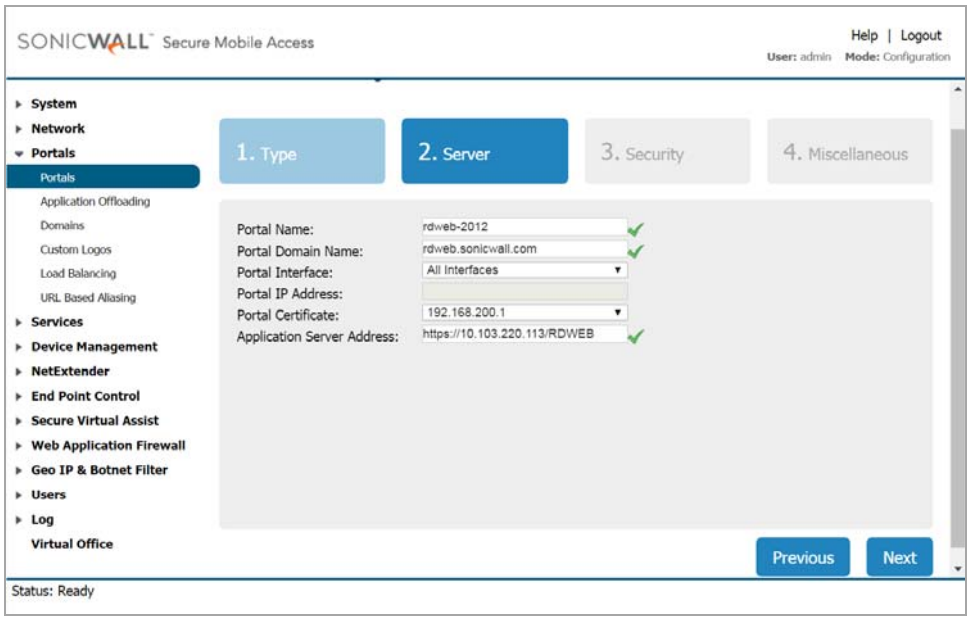
6 Any existing **URL Based Aliasing Group**(s) are listed in the drop-down and available to assign to this portal. If no **URL Based Aliasing Group** exists, you can create a new one by clicking the "**click here to create**" hyperlink.

All these settings are verified instantly from the Appliance when the mouse leaves the input field (green check). If the input fails, the reason it failed is shown. Only when all fields are satisfied, can you click **Next** to go to the next tab.

Remote Desktop Web Access Server Settings

Select **Remote Desktop Web Access (RD Web Access)** on the initial page when you want the ability to use the SMA Agent to proxy the RDP connection to the private network to make the resource list on the RD Web site function more efficiently. When this option is enabled, the screen options change. You will need to select

Remote Desktop Web Access (RD Web Access) from the drop down list. When **Remote Desktop Web Access (RD Web Access)** is selected on the initial page, the **Server** step appears as follows.



1 In the **Portal Name** field, enter a unique name to identify different portals.

2 In the **Portal Domain Name** field, enter the domain name used to access the offloading portal.

3 In the **Portal Interface** field, enter the network interface to which the portal is bound. If one specific network interface is selected, a new IP address is assigned to the portal.

4 The **Portal IP Address** field is not required if **All Interfaces** is selected in the **Portal Interface** field, but you need to enter the **Portal IP Address** of specific X0, X1, X2, and X3 interfaces.

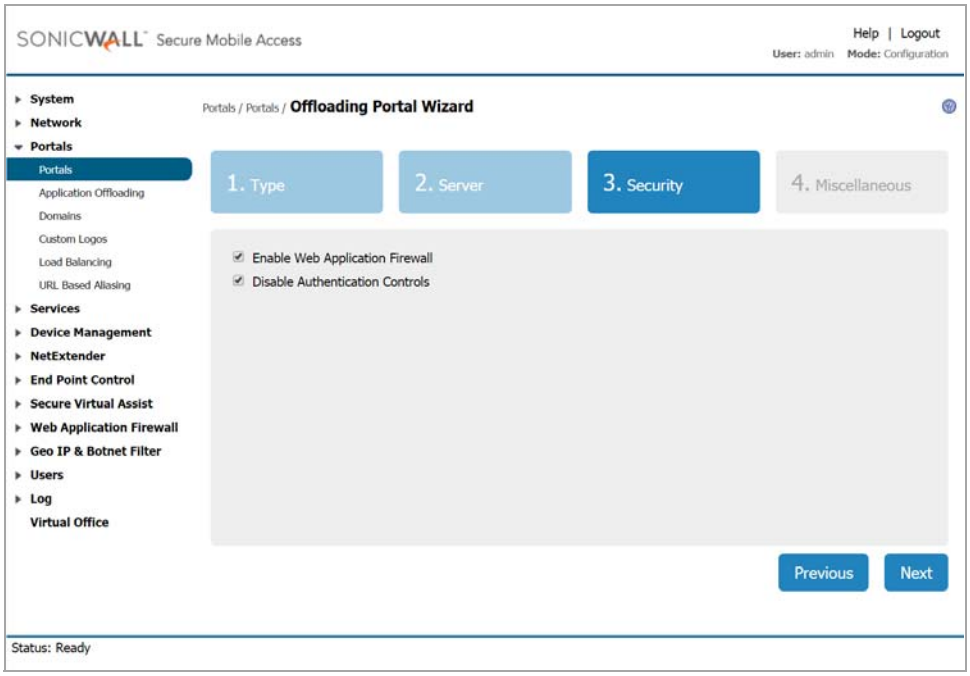
5 The **Portal Certificate** drop-down lists all certificates that have been imported.

6 The **Application Server Address** field accepts settings relevant to the application server. This can simply be the IP address of the application server. The scheme of the address is “HTTPS” by default. The port and default path can also be set in this single field.

All these settings are verified instantly from the Appliance when the mouse leaves the input field (green check). If the input fails, the reason it failed is shown. Only when all fields are satisfied, can you click **Next** to go to the next tab.

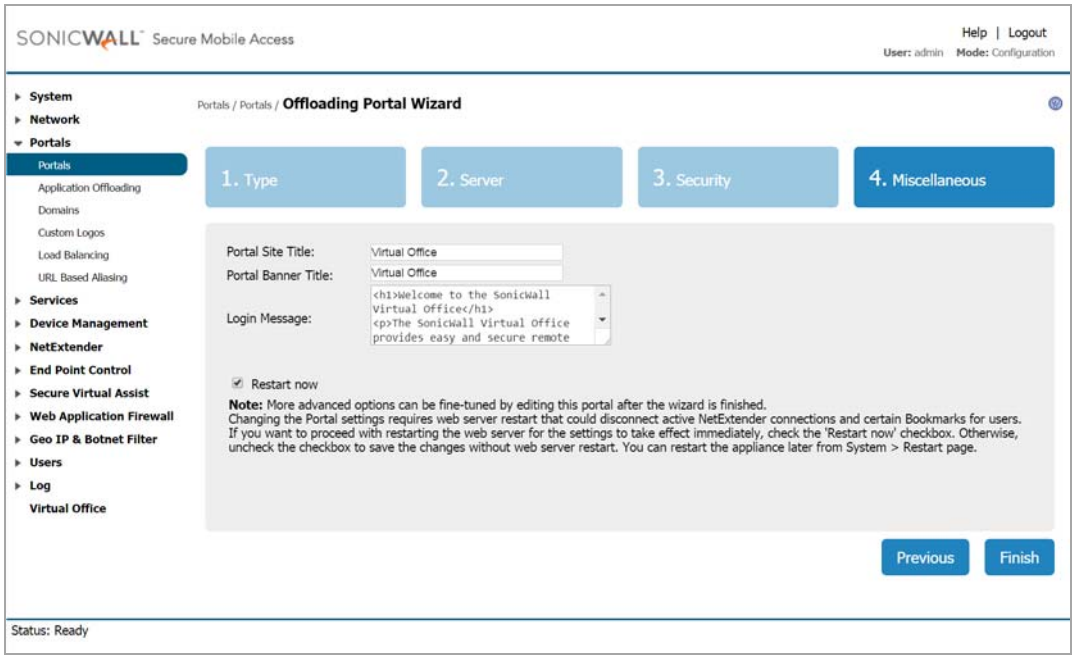
Configuring the Security Settings

The third step is for the Security settings, including **Enable Web Application Firewall** and **Disable Authentication Controls**. However, both options require a Web Application Firewall license.



Configuring the Miscellaneous Settings

The fourth and last step includes the general portal settings.



Portal Site Title, **Portal Banner Title**, and **Login Message** are set by default, but they can still be customized.

Restart Now - Gracefully restarts the appliance immediately after clicking **Finish**.

More advanced options can be fine-tuned by editing this portal after the wizard has finished. Changing the Portal settings requires a web server restart that could disconnect any active NetExtender connections and certain Bookmarks. If you want to proceed with restarting the web server for the settings to take effect

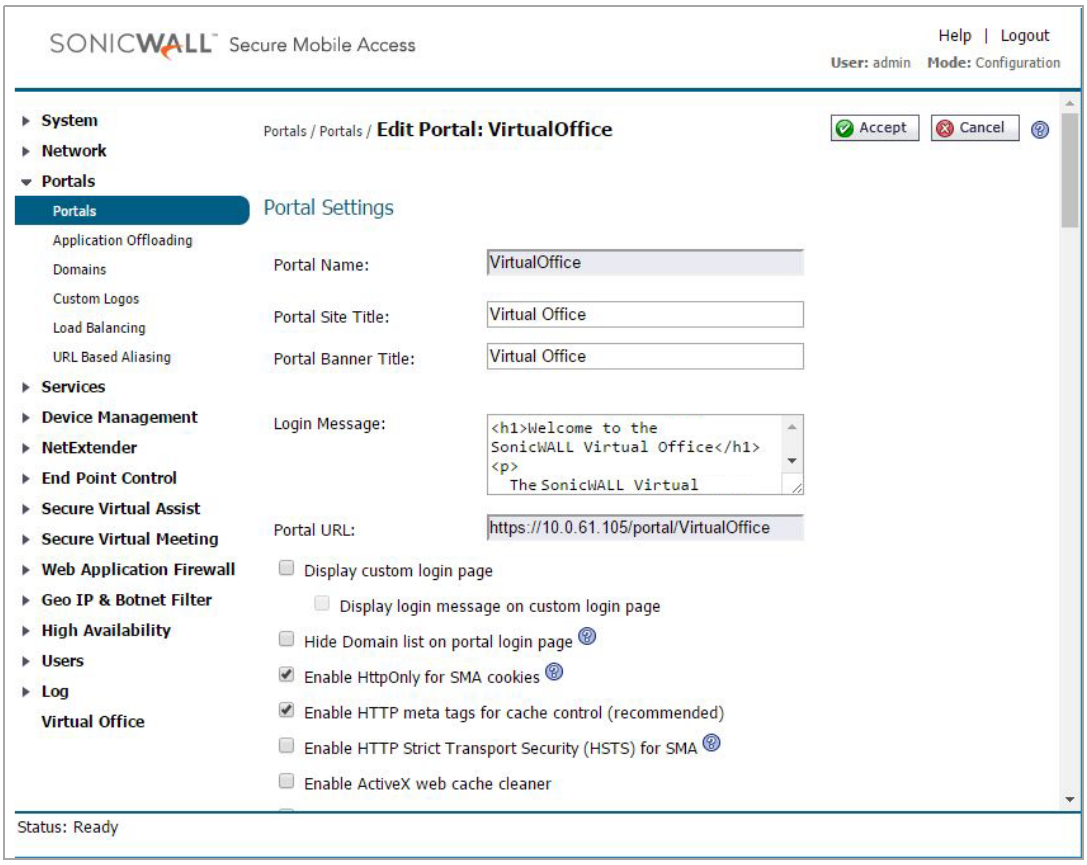
immediately, check **Restart now**. Otherwise, uncheck the check box to save the changes without web server restarting. You can restart the appliance later from the **System > Restart** page.

The wizard ends after clicking **Finish**. The page is blocked and you are redirected to the portal list page after the App Offloading portal is successfully created.

Modifying the General Settings

To edit the General settings:

1 You can edit the **Portal Name**, **Portal Site Title**, the **Portal Banner Title**, and the **Login Message** as needed.



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

> **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.

3 Select **Display login message on custom login page** to display the login message (from the **Login Message** field) when users log in to the custom login page.

4 Select **Hide Domain list on portal login page** to replace the Domain list box displayed on the login page to a text box for you to type in the correct domain name.

5 Select **Enable HttpOnly for SMA cookies** to secure SMA cookies using the HTTPOnly flag.

Some client-side technologies such as Java applets do not have access to cookies marked HTTPOnly. This can break access to the web application when using an HTTP/HTTPS Bookmark or the App Offloading Portal. Disable this option to restore compatibility for these web applications.

6 Select **Enable HTTP meta tags for cache control** 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 client browsers from caching the SMA/SRA appliance 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 a user Web browser cache.

7 Select **Enforce login uniqueness** (disabled by default) to restrict each account to a single session at a time. When login uniqueness is not enforced, ActiveSync or Outlook Anywhere client accounts can have multiple, simultaneous sessions.

8 Select the **Enforcement method**. Options include **Automatically logout existing session** and C**onfirm logout of existing session**.

9 Select **Enforce client source uniqueness** to prevent multiple connections by a user with the same client source address when connecting with a SonicWall Inc. client (NetExtender, Mobile Connect, Virtual Assist etc.). This prevents a user from consuming multiple licenses when a user reconnects after an unexpected network interruption.

For example, a user on an unreliable network is disconnected due to a network issue. If login uniqueness is NOT enabled, the user session on the appliance stays active for this type of disconnect until the timeout value is reached. The user reconnects and consumes a second license with the potential of consuming more licenses before the original connection timeout disconnects them.

10 Specify the link(s) for the **Small** / **Medium** / **Wide** / **Large** Logo to be used with Live Tile.

11 Specify the **Background Color** for Live Tile. If no value is specified, the default color is #0085C3.

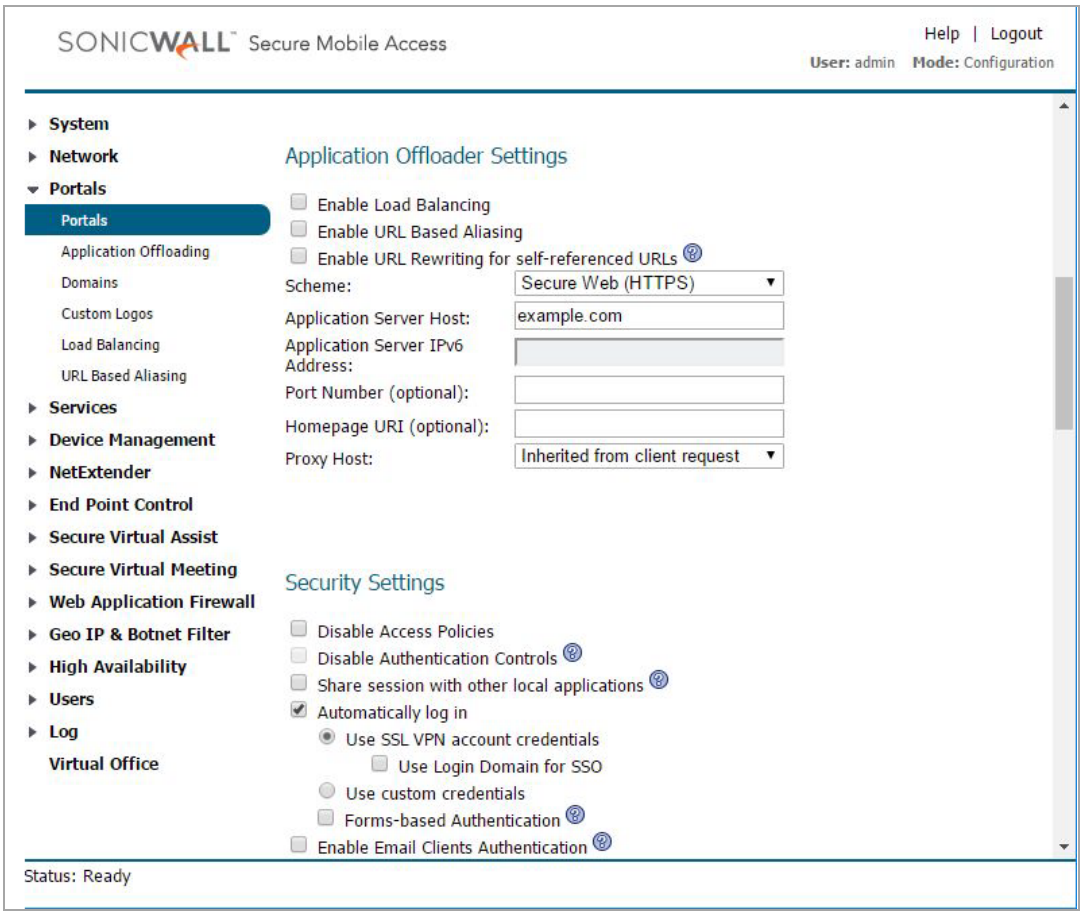
12 Specify the **Site Name** to be displayed for Live Tile. If no value is specified, the default is the Portal Name.

13 Click **Accept** to preserve your settings.

Configuring the Offloading Settings

1 Navigate to **Portals > Portals** and click the **Configure** icon for the portal you would like to edit. The **General** tab of the Portal Settings screen opens.

2 Go to the **Application Offloading Settings** section.



3 On the **Offloading** tab, select **Enable Load Balancing** for load balancing among offloaded application servers.

4 Select **Enable URL Based Aliasing**. As a result, some fields become hidden and **Enable URL Rewriting for self-referenced URLs** is automatically selected.

5 Select the group you wish to add a portal for from the **URL Based Aliasing Group** drop down list.

6 If not using a **URL Based Aliasing Group**, select one of the following from the **Scheme** drop-down list:

- **Web (HTTP)** – access the Web application using HTTP (default scheme)
- **Secure Web (HTTPS)** – access the Web application using HTTPS
- **Auto (HTTP/HTTPS)** – allows the user to determine the actual scheme used to talk to the backend server when accessing an offloading portal. Access is still under the control of the access policy.

  When using the Auto scheme, users can type http://www.example.virtual.host.com or https://www.example.virtual.host.com in browser's address bar to test this feature. Even scheme set to Auto, it's still under the control of the access policy.

CAUTION: It is the Administrator's responsibility to configure the correct scheme used to talk to the backend server. Auto (HTTP/HTTPS) Scheme can operate only if HTTP access is enabled for the Virtual Host (under the Virtual Host tab) and authentication is disabled (under the Offloading tab), which may be insecure. Therefore, you will be prompted to click OK to enable HTTP for Virtual Host.

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

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

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

10 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 the first time the user tries to access the Application Offloading Portal. This is a string in the form of: **/exch/test.cgi?key1=value1&key2=value2**

When this field is configured, it redirects the user to the Web site's home page the first time the user accesses the portal. This happens only when the user is accessing the site with no URL path (that is, when accessing the root folder, for example: `https://www.google.com/`). This is not an alias for the root folder. The user can edit the URL to go back to the root folder.

The key=value pairs allow you to specify URL query parameters in the URL. You can use these for any Web site that does not have a default redirect from the root folder to the home page URL. Outlook Web Access is one example, but note that most public sites do have a default redirect.

11 Select a **Proxy Host** from the drop-down menu to provide the ability to select which host name is sent to the backend server. Options include **Inherited from client request**, V**irtual Hostname**, and **Application Server Host (backend)**. The **Inherited from client request** option is the default value.

Security Settings

1 Under Security Settings, select **Enable Web Application Firewall** to enable the feature.

2 Select **Disable Access Policies** to prevent existing Access Policies from taking precedence.

3 Select **Disable Authentication Controls, Access Policies, and CSRF Protection (if enabled)** if you need no authentication, access policies, or CSRF protection enforced. This is useful for publicly hosted Web sites.

4 To configure ActiveSync authentication, clear the **Disable Authentication Controls** check box to display the authentication fields. Select **Enable ActiveSync authentication** and then type the default domain name. The default domain name will not be used when the domain name is set in the email client's setting.

5 Select **Automatically log in** to configure Single Sign-On settings.

6 For **Automatically log in** using SSO, select one of the following radio buttons:

- **Use SSL-VPN account credentials** – allow login to the offloaded application using the credentials configured on the SMA/SRA appliance
- **Use custom credentials** – displays **Username**, **Password**, and **Domain** fields where you can enter the custom credentials for the application or use dynamic variables. For the **Password** field, enter the custom password to be passed, or leave the field blank to pass the current user's password to the offloaded application portal. For the other fields, dynamic variables can be used, such as those shown below:

Supported dynamic variables

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

7 If you selected **Automatically Log in**, select **Forms-based Authentication** to configure Single Sign-On for forms-based authentication.

- Configure **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 **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:

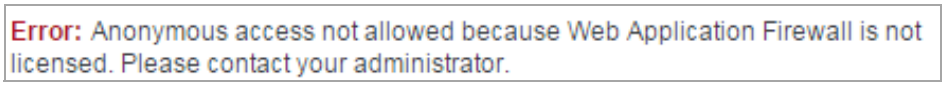
  ```
  <input type=password name='PASSWORD' id='PASSWORD' maxlength=128>
  ```

8 Select **Enable Email Clients Authentication** to allow the exchange portal to be accessed by Email clients, such as ActiveSync, Outlook, or OWA. When selected, specify a **Default Domain Name** from the drop down list. The **Default Domain Name** is set automatically when creating or editing a Domain. The Domain Name is used as the default for SMA authentication if the domain name is not specified in the Email client.

NOTE: This option is not necessary for OWA.

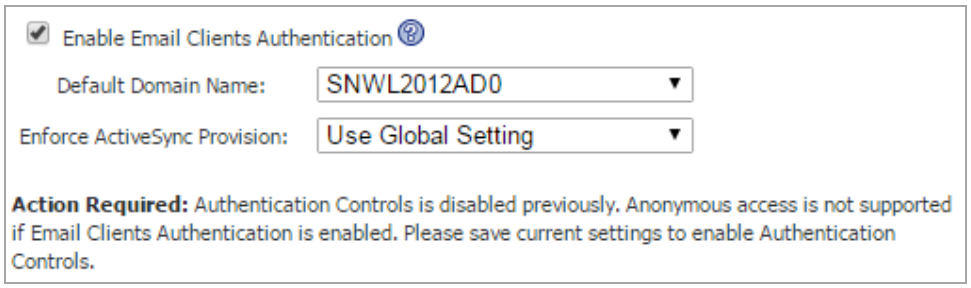
If the Authentication Controls are already disabled (and WAF is not licensed) after upgrading to 8.5, an Action Required message appears on the Portal page. The **Disable Authentication Controls** option is also disabled. Click Save to finalize the Authentication Controls setting.

If you access the portal under these conditions, an error message displays.



A log message is generated at the Notice level that reads; *Anonymous Offloaded Connection could not be processed because WAF is not licensed. Activate the WAF subscription service or Free Trial from the **System > Licenses** page*.

The same is true for the Exchange portal access when the **Authentication Controls** are disabled.

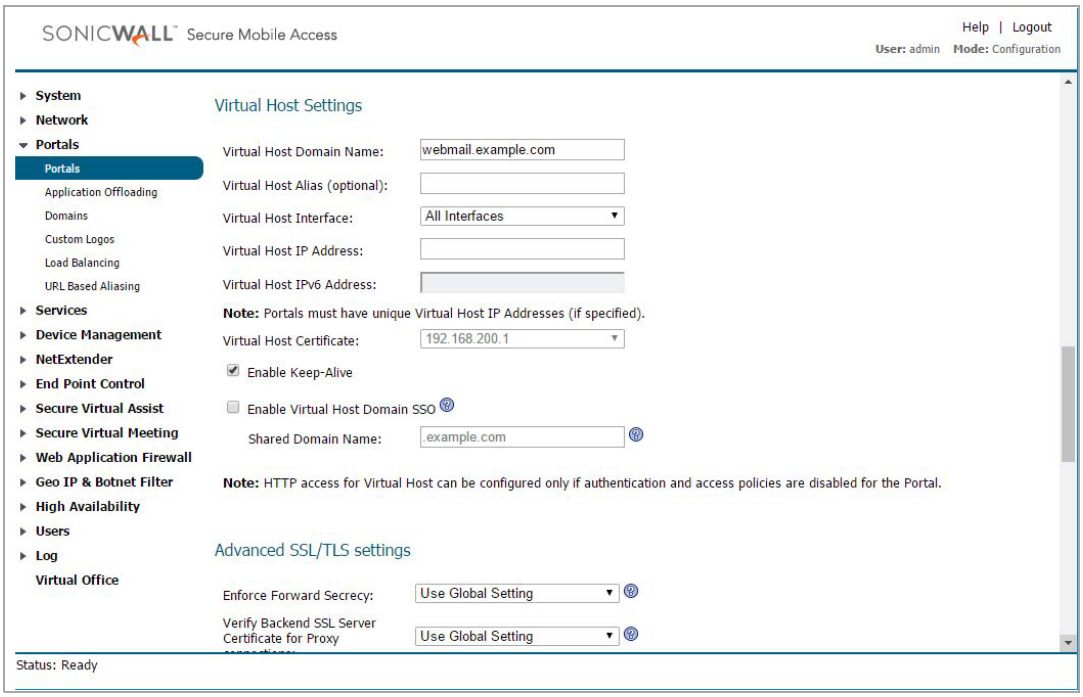


The log message reads, *Anonymous Exchange access could not be processed, please enable Authentication Controls for the portal.*

Configuring an HTTP/HTTPS Application Offloading Portal

To offload a Web application and create a portal for it:

1 Navigate to **Portals > Portals** and scroll to the **Virtual Host Settings** section. This allows you to access the Portal directly.

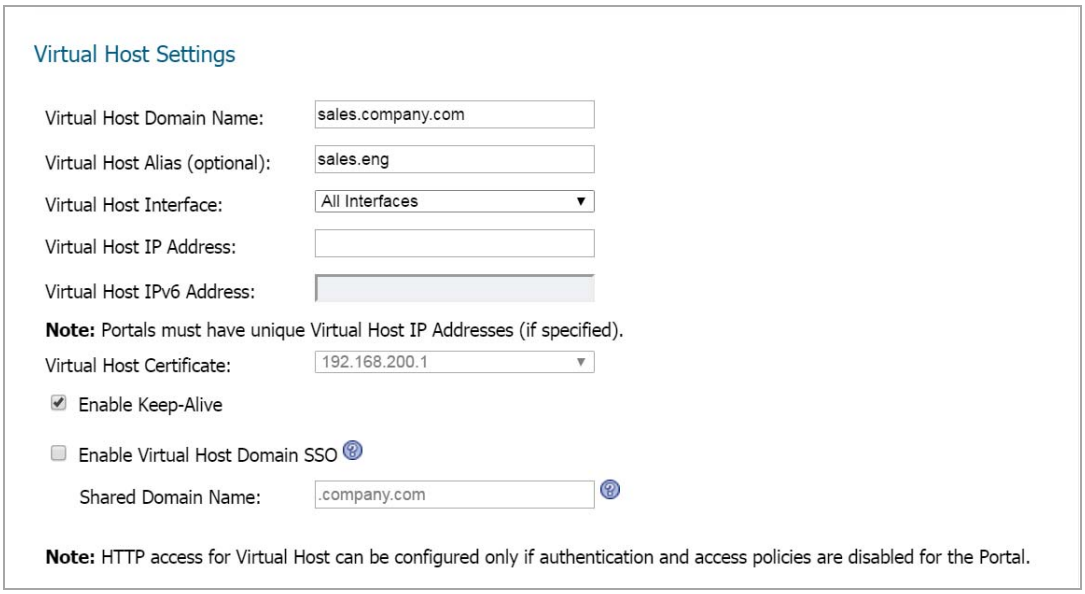


2 Enter a descriptive name in the **Virtual Host Domain Name** field.

3 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. The **Virtual Host Alias** is set to the Autodiscover address of ActiveSync if ActiveSync access has been enabled. The Autodiscover address is generated automatically from the **Virtual Host Domain Name**.

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 SMA/SRA appliance.

4 If authentication is disabled for this portal, you have the option to **Enable HTTP access** for this Application Offloaded Portal. This feature is useful for setting up offloading in trial deployments.



5 Click **Accept**. You are returned to the **Portals > Portals** page where you will see the Web application listed as an **Offloaded Web Application** under Description.

6 If you have not disabled authentication, navigate to the **Portals > Domains** page and create a domain for this portal.

7 Update your DNS server for this virtual host domain name and alias (if any).

Using Offloaded Applications

An offloaded application has its own portal page on the SMA/SRA appliance. The portal can be accessed directly by entering the URL in a Web browser. You can also create an External Web site Bookmark on the SMA Virtual Office portal that takes you to the offloaded application portal.

To use an offloaded application:

1 For direct access, point your Web browser to the URL of the offloaded application portal.

2 For access through an External Web site Bookmark, log in to the SonicWall Inc. Virtual Office and then click on the bookmark.

A new window is launched in your default browser that connects to the offloaded application portal specified in the bookmark.

3 On the portal page, enter your login credentials to access the application if authentication is required.

Configuring Application Offloading with SharePoint 2013

When the SharePoint 2013 server is accessed through an offloaded portal, basic functionalities, such as adding, editing, or deleting documents, tasks, or calender events are supported. The client integration is supported if

the offloaded portal's authentication controls are enabled or disabled. However, when the Authentication Controls are enabled, the client is only supported on Internet Explorer under the following caveats:

- The offloaded portal created for SharePoint must use a valid certificate.
- The Scheme used by the offloaded portal and the back end SharePoint must be the same. If the back end SharePoint is running on HTTP, the offloaded portal must enable HTTP access and be accessed with HTTP.
- The same Scheme between the offloaded portal and the back end SharePoint means that URL Rewriting for the offloaded portal does *not* need to be enabled.
- The **Share session with other local application** option must be enabled. This check box is located on the **Portals** > **Portals** > **Offloading** tab.
- The **Restrict Request Headers** option must be disabled. This check box is located on the **Services** > **Settings** page.
- If using Windows Vista or Windows 7 with the client, the offloaded portal should be added as a "Trusted Site" on the Internet Explorer browser. To configure your trusted sites, navigate to **Tools** > **Internet Options**. On the **Security** tab, click the **Trusted Sites** icon.
- The **Share session with other local applications** option must be enabled at login.

Microsoft Outlook Anywhere with Autodiscover Overview

The Outlook Anywhere with Autodiscover Application Offloading is a feature that provides the ability for clients using Outlook 2013, Outlook 2010, or Outlook 2007 to access the Outlook Exchange Server from the Internet. Autodiscover support provides a simple configuration of the user's account by only requiring the user's email address and password. Autodiscover also helps to update settings on the client side when Outlook Exchange server settings have changed.

Outlook Anywhere with Autodiscover is supported by the Application Offloading portal; both Access Policy and Authentication can be enforced.

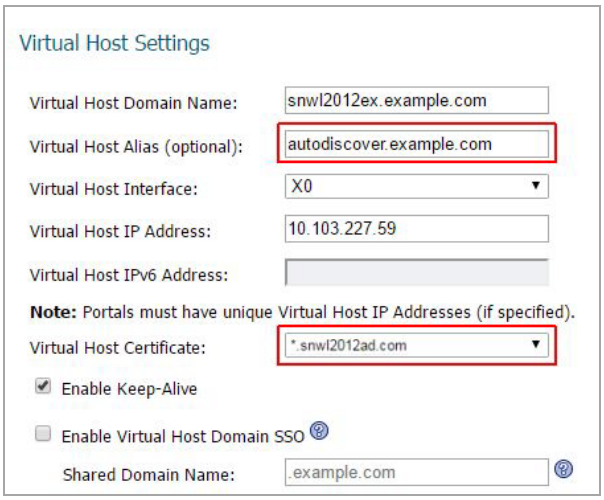
NOTE: If Authentication Control of the SMA/SRA appliance is enabled, only the Basic Authentication for Outlook Anywhere can be supported.

Configuring the Outlook Anywhere Portal

To configure the Outlook Anywhere Application Offloading portal:

1 Enable Outlook Anywhere on the Exchange Server. Verify that it is properly configured.

2 Create an Application Offloading portal based on the following settings:



Because Autodiscover uses a different URL for fetching configuration, set the Autodiscover URL as the **Virtual Host Alias** name. Verify that the Autodiscover URL is aligned with the Exchange Server settings.

3 Specify the **Virtual Host Certificate**. A wildcard certificate is preferred if Autodiscover is enabled.

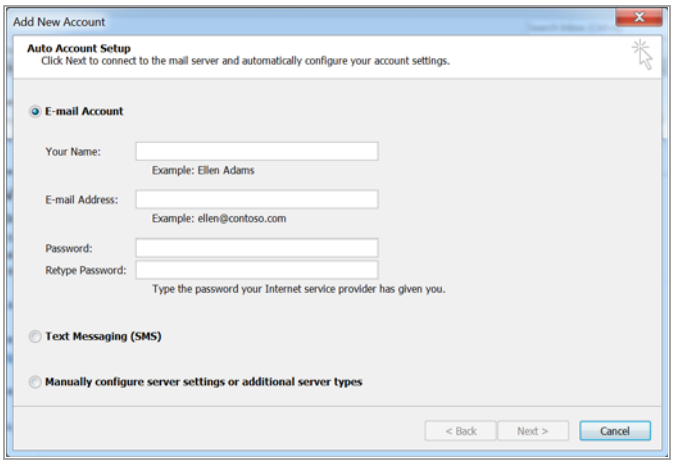
4 Navigate to the **Offloading** tab.

5 Select **Enable Email Clients Authentication**.

6 Select the **Default Domain Name** from the drop-down list. This domain name is used as the default domain for Secure Mobile Access authentication if the domain name is not specified in Outlook.

7 Open Microsoft Outlook.

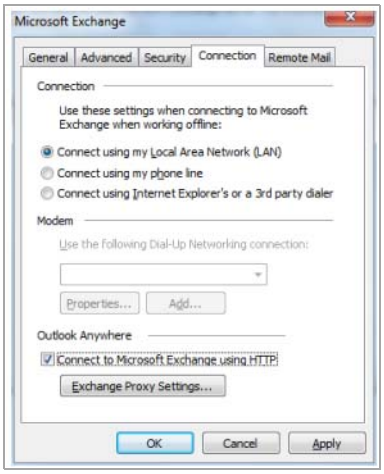
8 On the **File** > **Info** page, click **Add Account**. The Add New Account window displays.



You can select **Auto Account Setup** or **Manually configure server settings or additional server types** to configure the email account. If Autodiscover is configured, select **Auto Account Setup**. If Autodiscover is not enabled or does not function properly, select **Manually configure server settings or additional server types** to specify Outlook Anywhere settings manually. Then, click **Next**.

9 On the Microsoft Exchange Settings window, click **More Settings**.

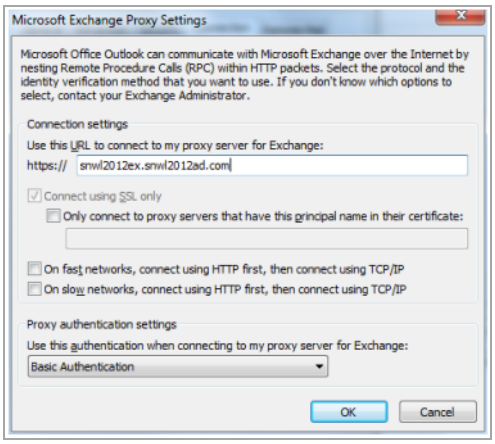
10 Under the Connection tab, select **Connect to Microsoft Exchange using HTTP** under the Outlook Anywhere section.



11 Next, click **Exchange Proxy Settings**.

12 On the Microsoft Exchange Proxy Settings Screen, specify the host name of the Outlook Anywhere portal in the **Use this URL to connect to my proxy server for Exchange** field.

13 Next, select the proxy authentication setting from the drop-down list. If Secure Mobile Access authentication is enabled, select **Basic Authentication**.



14 Click **OK** to save the configuration, and then exit out of Microsoft Outlook.

15 Open Microsoft Outlook to start a new session. Log messages are generated when the Outlook Anywhere portal is accessed.

NOTE: If Authentication Control of the Secure Mobile Access portal is enabled, only Basic Authentication can be supported. Be sure to select **Basic Authentication** on the Exchange server for Outlook Anywhere. If Authentication Control of Secure Mobile Access is disabled, other authentication methods are supported.

NOTE: To provide better protection for the Exchange Server, anonymous Outlook Anywhere access is not supported.

Portals > Domains

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

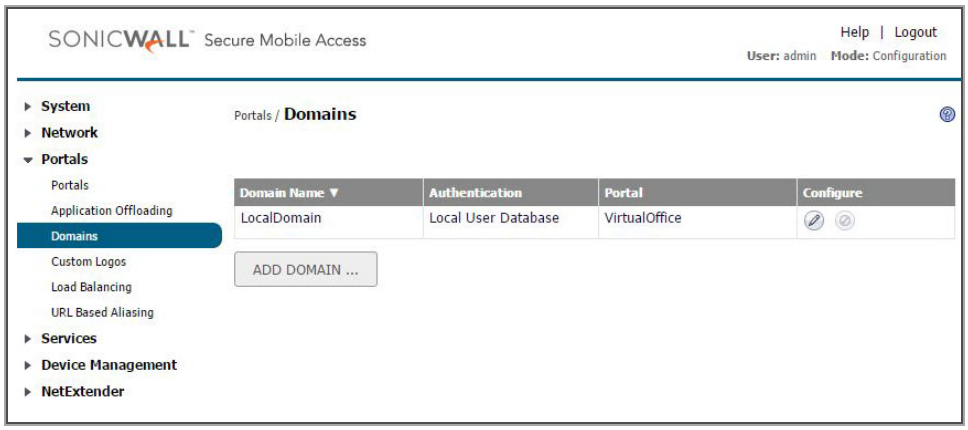
Portals > Domains Overview

The **Portals > Domains** page allows the administrator to add and configure a domain, including settings for:

- Authentication type (local user database, Active Directory, LDAP, or RADIUS)
- Domain name
- Portal name

- Group (AD, RADIUS) or multiple Organizational Unit (LDAP) support (optional)
- Client digital certificate requirements (optional)
- One-time passwords (optional)

Portals > Domains Page



Viewing the Domains Table

All of the configured domains are listed in the table in the **Portals > Domains** window. The domains are listed in the order in which they were created. You can reverse the order by clicking the up/down arrow next to the **Domain Name** column heading.

Removing a Domain

To delete a domain:

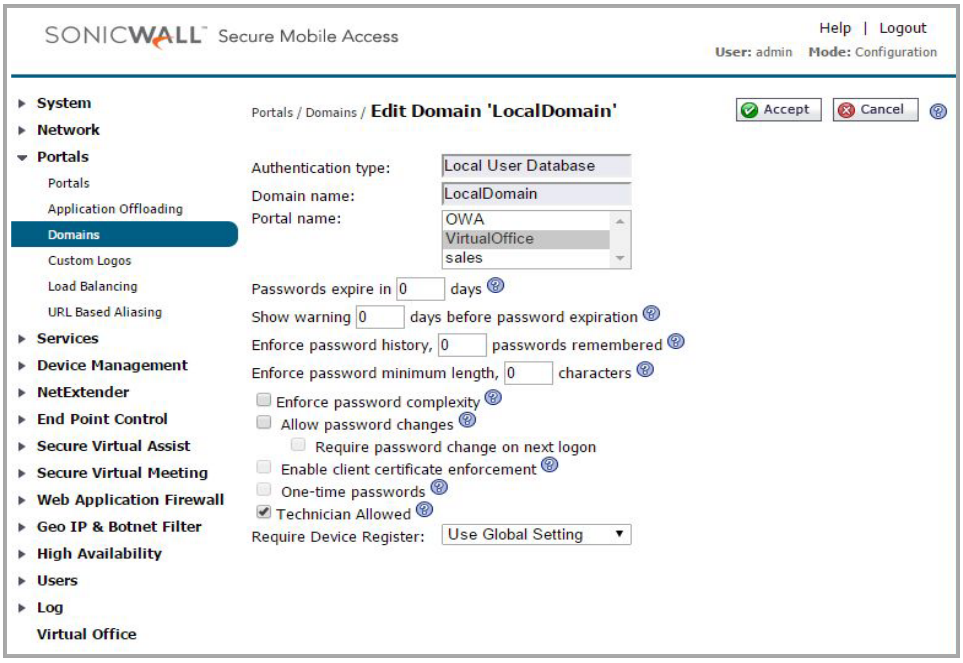
1. Navigate to **Portals > Domains**.
2. In the table, click the delete icon in the same row as the domain that you wish to delete.
3. Click **OK** in the confirmation dialog box.

   After the SMA/SRA appliance has been updated, the deleted domain is no longer be displayed in the table.

   NOTE: The default **LocalDomain** domain cannot be deleted.

Adding or Editing a Domain

You can add a new domain or edit an existing one from the **Portals > Domains** page. To add a domain, click **Add Domain** to display the Add Domain window.



To edit an existing domain, click the **Configure** icon to the right of the domain you wish to edit.

The interface provides the same fields for both adding and editing a domain, but the **Authentication Type** and **Domain Name** fields cannot be changed when editing an existing domain.

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 on page 400 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 can be created that require authentication to remote authentication servers. The SMA/SRA appliance supports RADIUS, LDAP, Active Directory, and Digital Certificate 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** window. The selected portal is applied to all users in the new domain. Domain choices is displayed in the login page of the Portal that was selected. Domains are case-sensitive when logging in.

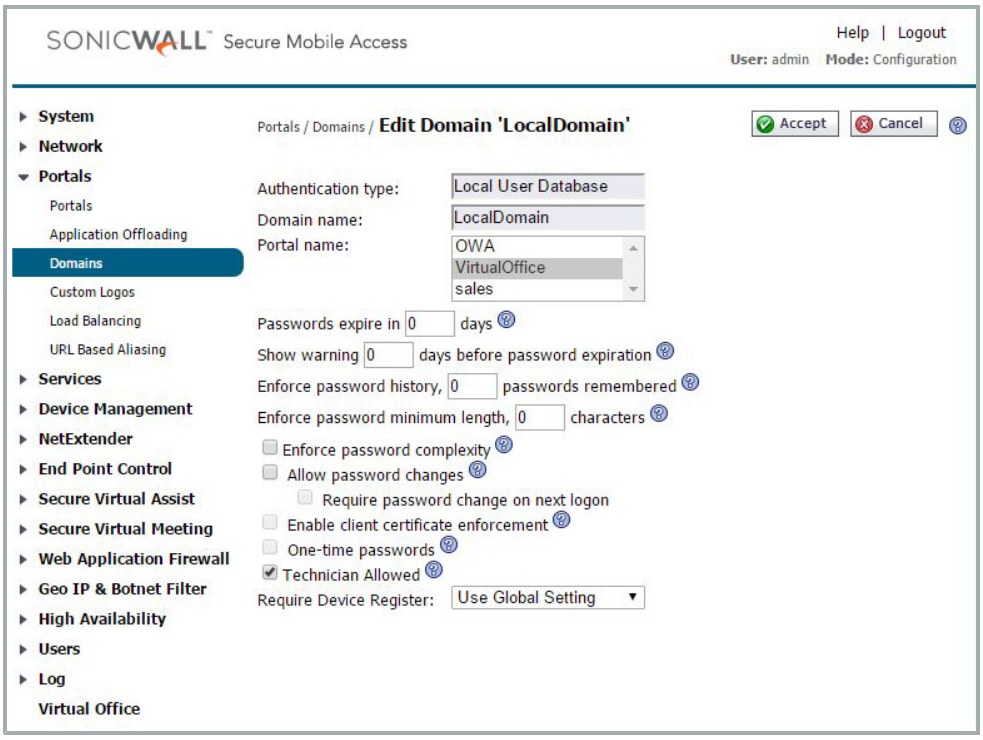
You can create multiple domains that authenticate users with user names and passwords stored on the SMA/SRA appliance to display different portals (such as a Secure Mobile Access portal page) to different users.

For convenient configuration of SMA/SRA appliance administrator accounts, you can create a domain that provides administrator access for all users who log in to that domain. Either LDAP or Active Directory authentication is used for this type of domain.

Adding or Editing a Domain with Local User Authentication

To add or edit a domain for local database authentication:

1 Navigate to the **Portals > Domains** window and click **Add Domain** or the Configure icon for the domain to edit. The **Add Domain** or **Edit Domain** window is displayed.



2 If adding the domain, select **Local User Database** from the **Authentication Type** drop-down list.

3 If adding the domain, enter a descriptive name for the authentication domain in the **Domain Name** field (maximum 24 characters). This is the domain name users select to log in to the Secure Mobile Access portal.

4 Select the name of the layout in the **Portal Name** field. Additional layouts can be defined in the **Portals > Portals** page.

5 All newly created domains in the local database user type should be set with a default password expiration value, as well as the “show expiration warning days” option set to 15. You can manually change it upon creation. Optionally, force all users in the Local User Database to change their password at set intervals or the next time they login. To force users to change their password at set intervals, type the expiration interval in the **Passwords expire in *x* days** field. To force users to change their password the next time they log in, check **Require password change on next logon**.

NOTE: A specific local domain user can be forced to change their password. Use the General tab on the **Users > Local Users > Edit** page.

If the domain is set with concrete password expiration days, you should also set the user expiration to 0. That means using the domain expiration setting. The domain setting detection is automatic after submitting the “adding user” request. Also, you can manually change it on creation.

The default password expiration value is two years (730 days).

On upgrade, the existing values for password expiration should remain as they are.

A notice was added on the **System > Status** page to recommend setting the expiration from all local database domains. The notice has a list of domains (top 5) that need that setting. If you set the default password expiration for all the domains, then the message is dismissed.

6 If you set a password expiration interval, type the number of days before expiration that users should receive notifications in the **Show warning *x* days before password expiration** field.

When configured and a password is expiring, a notification is displayed on the user's Virtual Office page or the Administrator's management console identifying the number of days before their password expires. Notifications also include a link to a screen where the password can be changed.

7 Optionally add the number of unique new passwords that is associated with a user account before an old password can be re-used for the account in the **Enforce password history, *x* passwords remembered** field. The value specified must be between 0 and 10 passwords.

8 Optionally **Enforce password minimum length** by entering a value between 1 and 14 characters. This is the minimum amount of characters accepted for a user password.

9 Optionally select **Enforce password complexity**. When this option is enforced, at least *three* of the four following parameters must be met when setting a password:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)

10 Optionally select **Allow password changes**. This allows users to change their own passwords after their account is set up.

11 Optionally select **Enable client certificate enforcement** 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 appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this check box 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 matches the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

12 Optionally select **One-time passwords** to enable the One-time password feature. A drop-down list appears, 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 uses 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 are not allowed to log in.
- **using domain name** - Users in the domain uses the One Time Password feature. One Time Password emails for all users in the domain are sent to username@domain.com.
    - If you select **using domain name**, an **E-mail domain** field appears following the drop-down list. Type in the domain name where one-time password emails are sent (for example, abc.com).

13 If **Technician Allowed** is enabled, Secure Virtual Assist can log in as a technician role in this domain.

14 Click **Accept** to update the configuration. After the domain has been added, the domain is added to the table on the **Portals > Domains** page.

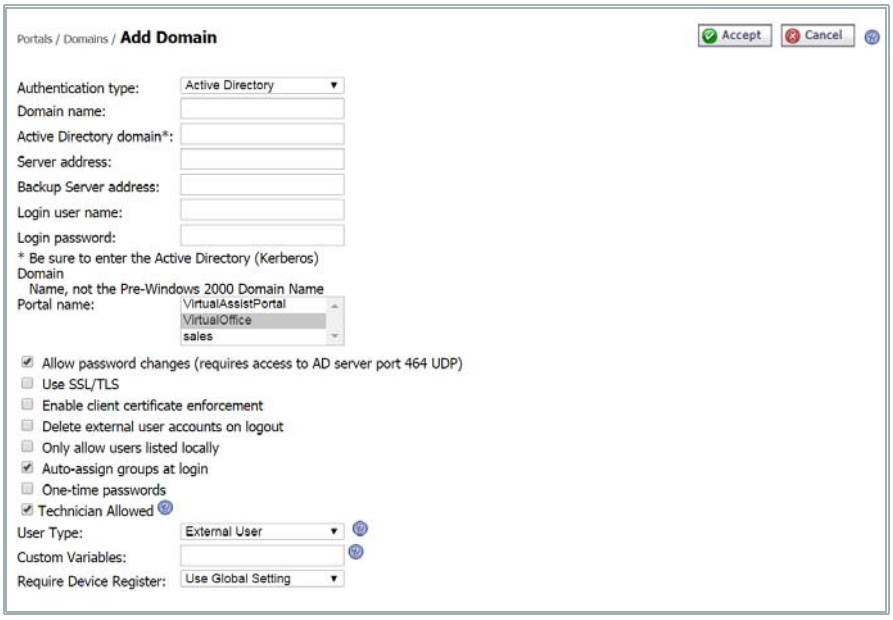
Adding or Editing a Domain with Active Directory Authentication

To configure Windows Active Directory authentication:

1 Click **Add Domain** or the Configure icon for the domain to edit. The **Add Domain** or **Edit Domain** window is displayed.

> **NOTE:** Of all types of authentication, Active Directory authentication is most sensitive to clock skew, or variances in time between the SMA/SRA 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 on page 187.

2 If adding the domain, select **Active Directory** from the **Authentication type** drop-down list. The Active Directory configuration fields are displayed.



3 If adding the domain, enter a descriptive name for the authentication domain in the **Domain name** field. This is the domain name users select in order to log in to the SMA/SRA appliance portal. It can be the same value as the **Server address** field or the **Active Directory domain** field, depending on your network configuration.

4 Enter the Active Directory domain name in the **Active Directory domain** field.

5 Enter the IP address or host and domain name of the Active Directory server in the **Server address** field.

6 Enter the IP address or host and domain name of the back up server in the **Backup Server address** field.

7 Enter the user name for login in the **Login user name** field.

8 Enter the password for login in the **Login password** field.

9 Enter the name of the layout in the **Portal name** field. Additional layouts can be defined in the **Portals > Portals** page.

10 Optionally select **Allow password changes**. Enabling this feature allows a user to change their password through the Virtual Office portal by selecting **Options** 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.

11 Optionally select **Use SSL/TLS**. This option allows for the needed SSL/TLS encryption to be used for Active Directory password exchanges. This check box should be enabled when setting up a domain using Active Directory authentication.

12 Optionally select **Enable client certificate enforcement** 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 appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this check box 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 matches the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

13 Select **Delete external user accounts on logout** to delete users who are not logged into a domain account after they log out.

14 Select **Only allow users listed locally** to allow only users with a local record in the Active Directory to login.

15 Select **Auto-assign groups at login** to assign users to a group when they log in.

Users logging into Active Directory domains are automatically assigned in real time to Secure Mobile Access groups based on their external AD group memberships. If a user's external group membership has changed, their Secure Mobile Access group membership automatically changes to match the external group membership.

16 Optionally, select **One-time passwords** to enable the One Time Password feature. A drop-down list appears, 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 uses 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 are not allowed to login.
- **using domain name** - Users in the domain uses the One Time Password feature. One Time Password emails for all users in the domain are sent to username@domain.com.

17 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 appears, 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 is used. If you select **custom**, the **Custom attribute** field appears. 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 is taken from their individual policy settings.

If you select **using domain name**, an **E-mail domain** field appears following the drop-down list. Type in the domain name where one-time password emails are sent (for example, abc.com).

18 If **Technician Allowed** is enabled, Secure Virtual Assist can log in as a technician role in this domain.

19 Select the type of user from the **User Type** drop-down list. All users logging in through this domain are treated as this user type. The choices depend on user types defined already. Some possible choices are:

- **External User** – Users logging into this domain are treated as normal users without administrative privileges.
- **External Administrator** – Users logging into this domain are treated as administrators, with local Secure Mobile Access admin credentials. These users are presented with the admin login page.

  This option allows the Secure Mobile Access administrator to configure a domain that allows Secure Mobile Access admin privileges to all users logging into that domain.

  SonicWall Inc. recommends adding filters that allow administrative access only to those users who are in the correct group. You can do so by editing the domain on the **Users > Local Groups** page.
- **Read-only Administrator** – Users logging into this domain are treated as read-only administrators and can view all information and settings, but cannot apply any changes to the configuration. These users are presented with the admin login page.

20 Click **Accept** to update the configuration. After the domain has been added, the domain is added to the table on the **Portals > Domains** page.

Active Directory Troubleshooting

If your users are unable to connect using Active Directory, verify the following configurations:

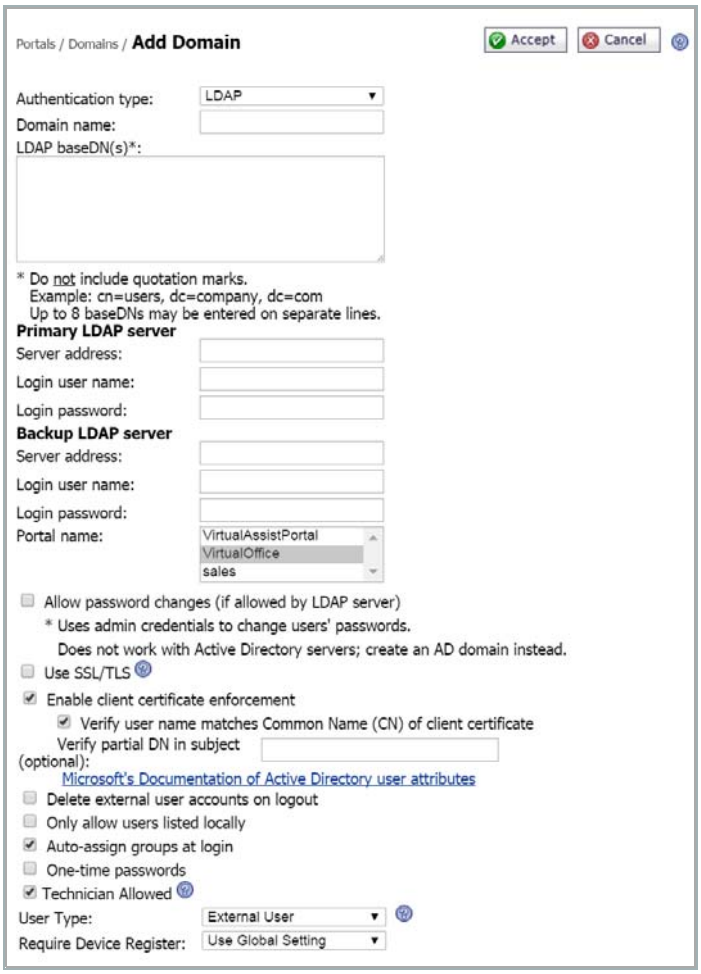
- The time settings on the Active Directory server and the SMA/SRA appliance must be synchronized. Kerberos authentication, used by Active Directory to authenticate clients, permits a maximum 15-minute time difference between the Windows server and the client (the SMA/SRA appliance). The easiest way to solve this issue is to configure Network Time Protocol on the **System > Time** page of the Secure Mobile Access 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.

Adding or Editing a Domain with LDAP Authentication

To configure a domain with LDAP authentication:

1 Click **Add Domain** or the Configure icon for the domain to edit. The **Add Domain** or **Edit Domain** window is displayed.

2 If adding the domain, select **LDAP** from the **Authentication Type** menu. The LDAP domain configuration fields are displayed.



3 If adding the domain, enter a descriptive name for the authentication domain in the **Domain name** field. This is the domain name users select in order to log in to the SMA/SRA appliance user portal. It can be the same value as the Primary LDAP **Server address** field.

4 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 are automatically included when parents are added to this field.

NOTE: Do not include quotes (“”) in the **LDAP BaseDN** field.

5 Enter the IP address or domain name of the Primary LDAP server in the **Server Address** field.

6 Enter the common name and password of a user that has been delegated control of the primary server in the **Login Username** and **Login Password** fields.

> **NOTE:** When entering **Login Username** and **Login Password**, remember that the SMA/SRA appliance binds to the LDAP tree with these credentials and users can log in with their sAMAccountName.

7 Optionally enter the IP address or domain name of a backup LDAP server in the **Server Address** field, under the Backup LDAP server section.

8 Optionally enter the common name and password of a user that has been delegated control of the backup server in the **Login user name** and **Login password** fields, under the Backup LDAP server section.

9 Enter the name of the layout in the **Portal name** field. Additional layouts can be defined in the **Portals > Portals** page.

10 Optionally select **Allow password changes (if allowed by LDAP server)**. This option, if allowed by your LDAP server, enables users to change their LDAP password during a Secure Mobile Access session.

11 Optionally select **Use SSL/TLS**. 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.

12 Optionally select **Enable client certificate enforcement** 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 appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this check box 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 matches the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

13 Select **Auto-assign groups at login** to assign users to a group when they log in.

Users logging into LDAP domains are automatically assigned in real time to Secure Mobile Access groups based on their external LDAP attributes. If a user's external group membership has changed, their Secure Mobile Access group membership automatically changes to match the external group membership.

14 Optionally select **One-time passwords** to enable the One Time Password feature. A drop-down list appears, 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 uses 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 are not allowed to login.
- **using domain name** - Users in the domain use the One Time Password feature. One Time Password emails for all users in the domain are 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 appears, 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 are used. If you select **custom**, the **Custom attribute** field appears. 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 is 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 appears instead of the **LDAP e-mail attribute** drop-down list. Type in the domain name where one-time password emails are sent (for example, abc.com).

15 Select the type of user from the **User Type** drop-down list. All users logging in through this domain is treated as this user type. The choices depend on user types defined already. Some possible choices are:

- **External User** – Users logging into this domain are treated as normal users without administrative privileges.
- **External Administrator** – Users logging into this domain are treated as administrators, with local Secure Mobile Access admin credentials. These users are presented with the admin login page.

  This option allows the Secure Mobile Access administrator to configure a domain that allows Secure Mobile Access admin privileges to all users logging into that domain.

  SonicWall Inc. recommends adding filters that allow administrative access only to those users who are in the correct group. You can do so by editing the domain on the **Users > Local Groups** page.
- **Read-only Administrator** – Users logging into this domain are treated as read-only administrators and can view all information and settings, but cannot apply any changes to the configuration. These users are presented with the admin login page.

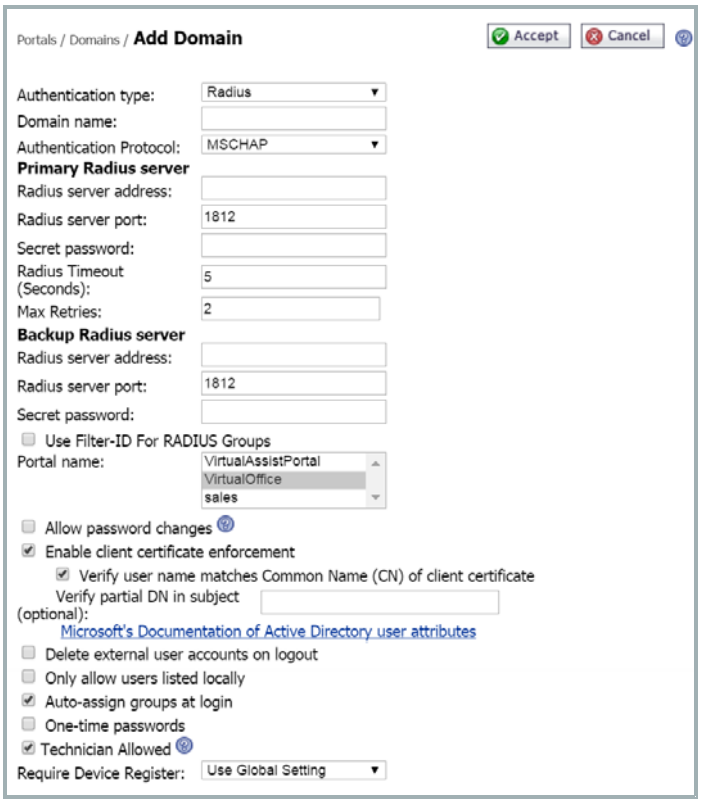
16 Click **Accept** to update the configuration. After the domain has been added, the domain is added to the table on the **Portals > Domains** page.

Adding or Editing a Domain with RADIUS Authentication

To configure a domain with RADIUS authentication:

1 On the **Portals > Domains** page, click **Add Domain** or the Configure icon for the domain to edit. The **Add Domain** or **Edit Domain** window is displayed.

2 If adding the domain, select **RADIUS** from the **Authentication type** menu. The **RADIUS configuration** fields are displayed.



3 If adding the domain, enter a descriptive name for the authentication domain in the **Domain name** field. This is the domain name users selects in order to log in to the Secure Mobile Access portal.

4 Select the proper **Authentication Protocol** for your RADIUS server. Choose from **PAP**, **CHAP**, **MSCHAP**, or **MSCHAPV2**.

5 Under **Primary Radius server**, enter the IP address or domain name of the RADIUS server in the **RADIUS server address** field.

6 Enter the RADIUS server port in the **RADIUS server port** field.

7 If required by your RADIUS configuration, enter an authentication secret in the **Secret password** field.

8 Enter a number (in seconds) for RADIUS timeout in the **RADIUS Timeout (Seconds)** field.

9 Enter the maximum number of retries in the **Max Retries** field.

10 Under **Backup Radius Server**, enter the IP address or domain name of the backup RADIUS server in the **RADIUS server address** field.

11 Enter the backup RADIUS server port in the **RADIUS server port** field.

12 If required by the backup RADIUS server, enter an authentication secret for the backup RADIUS server in the **Secret password** field.

13 Optionally, if using RADIUS for group-based access, select **Use Filter-ID for RADIUS Groups**.

14 Click the name of the layout in the **Portal name** drop-down list.

15 If you selected the Authentication Protocol for your RADIUS server as MSCHAP or MSCHAPV2, you have the option to select **Allow password changes**. Note that if you enable password changes, you must also deploy the LAN Manager authentication.

16 Optionally select **Enable client certificate enforcement** 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 appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this check box 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 matches the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

17 Select **Delete external user accounts on logout** to delete users who are not logged into a domain account after they log out.

18 Select **Auto-assign groups at login** to assign users to a group when they log in.

Users logging into RADIUS domains are automatically assigned in real time to Secure Mobile Access groups based on their external RADIUS filter-IDs. If a user's external group membership has changed, their Secure Mobile Access group membership automatically changes to match the external group membership.

19 Optionally select **One-time passwords** to enable the One-time password feature. A drop-down list appears, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

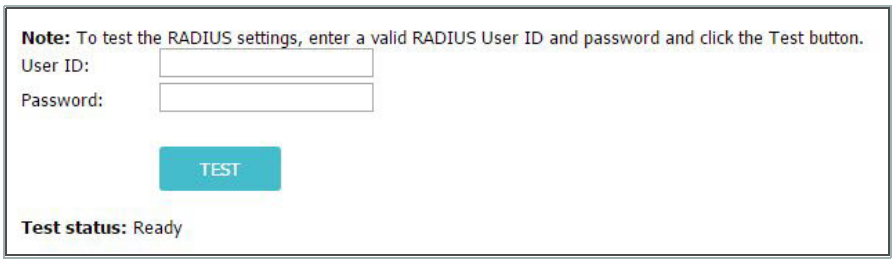
- **if configured** - Only users who have a One Time Password email address configured uses the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured is not allowed to login.
- **using domain name** - Users in the domain use the One Time Password feature. One Time Password emails for all users in the domain is sent to username@domain.com.

20 If you select **using domain name**, an **E-mail domain** field appears following the drop-down list. Type in the domain name where one-time password emails are sent (for example, abc.com).

21 If you select **Technician Allowed**, Secure Virtual Assist can be used as a technician in this domain.

22 Click **Accept** to update the configuration. After the domain has been added, the domain is added to the table on the **Portals > Domains** page.

23 Click **Configure** next to the RADIUS domain you added. The **Test** tab of the **Edit Domain** page displays.



24 Enter your RADIUS user ID in the **User ID** field and your RADIUS password in the **Password** field.

25 Click **Test**. The SMA/SRA appliance connects to your RADIUS server.

26 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.

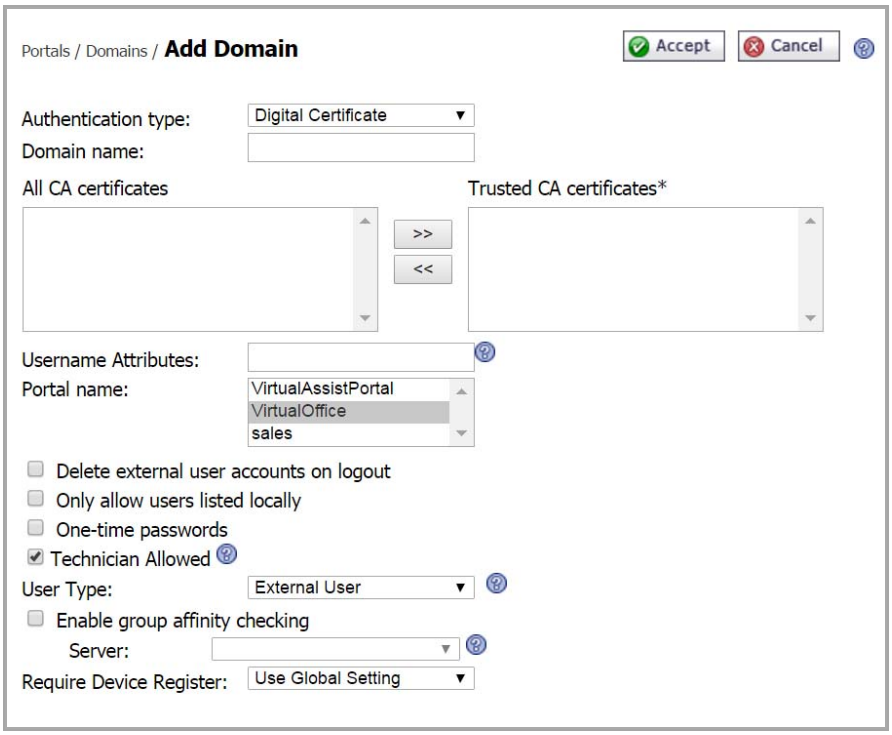
> **NOTE:** The SMA/SRA appliance attempts to authenticate against the specified RADIUS server using PAP authentication. It is generally required that the RADIUS server be configured to accept RADIUS client connections from the SMA/SRA appliance. Typically, these connections appear to come from the SMA/SRA appliance X0 interface IP address. Refer to your RADIUS server documentation for configuration instructions.

Adding or Editing a Domain with Digital Certificates

To add or edit a domain for digital certificate authentication:

1 Navigate to the **Portals > Domains** window and click **Add Domain** or **Configure** for the domain to edit. The **Add Domain** or **Edit Domain** window is displayed.

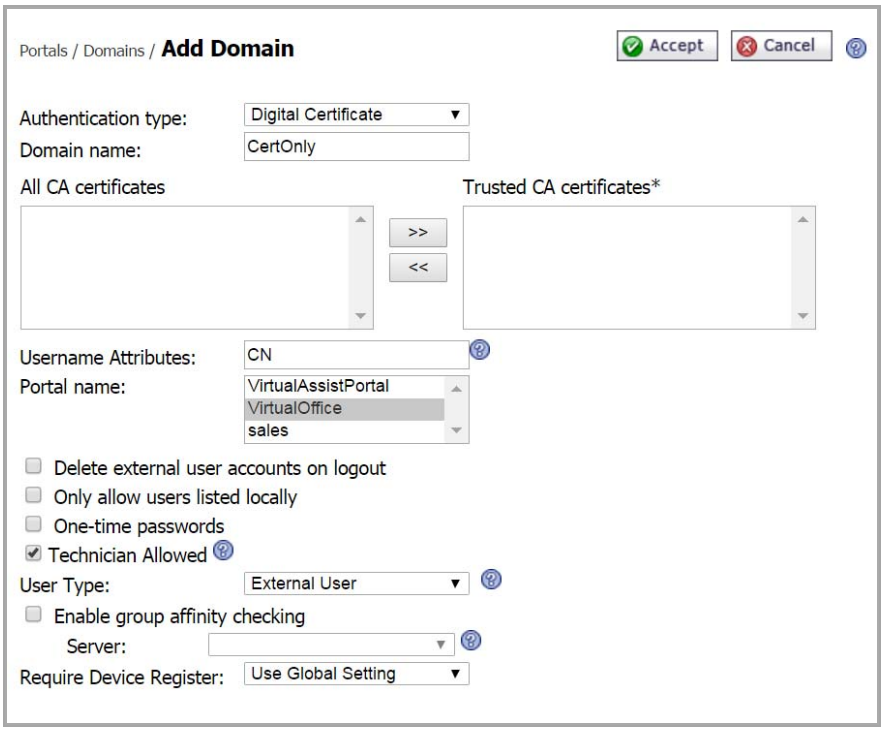
2 If adding the domain, select **Digital Certificate** from the **Authentication Type** menu. The **Digital Certificate configuration** field is displayed.



3 If adding the domain, enter a descriptive name for the authentication domain in the **Domain name** field. This is the domain name users selects in order to log in to the Secure Mobile Access portal.

4 Select one or more certificates from the **All CA certificates** list to be added to the **Trusted CA certificates** list. The All CA certificates list displays all available certificates for the SMA/SRA appliance that were imported from the system certificate setting.

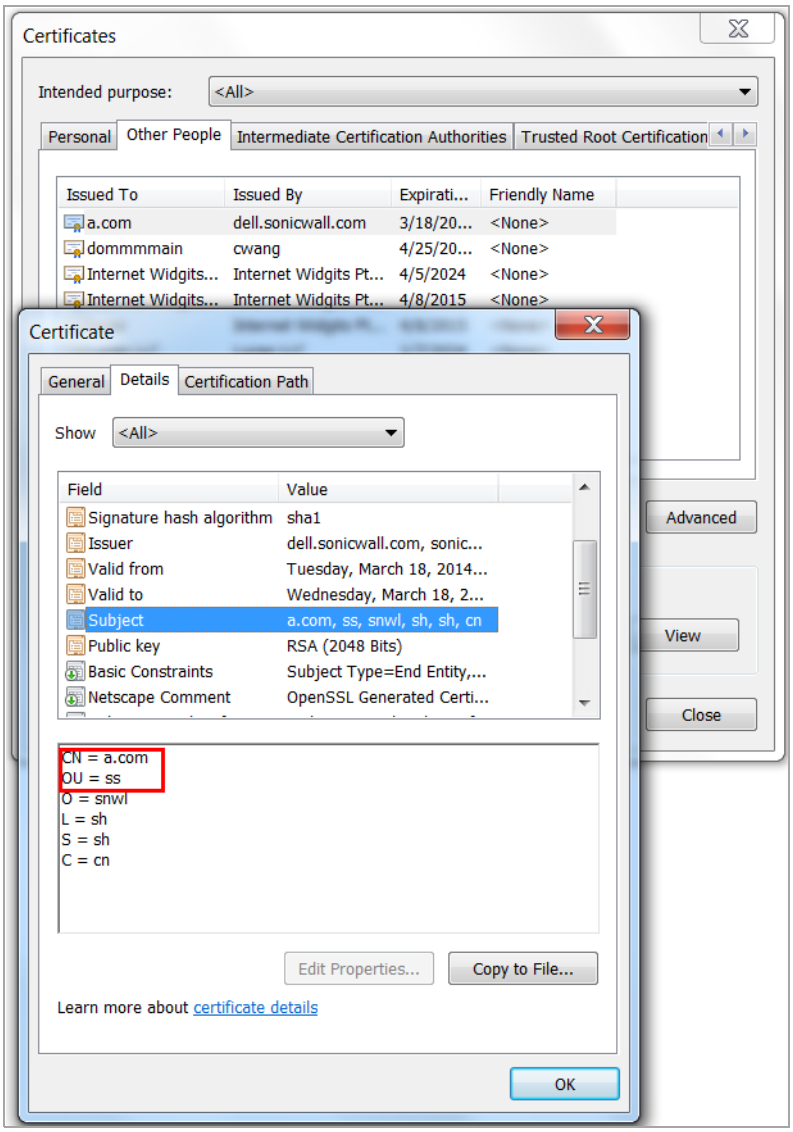
5 Enter the **Username Attribute** as **CN**. This uses the CN attribute of the client certificate as the login username.



6 Click **Accept** to save changes. Next, you need to import the client certificate to your Web browser.

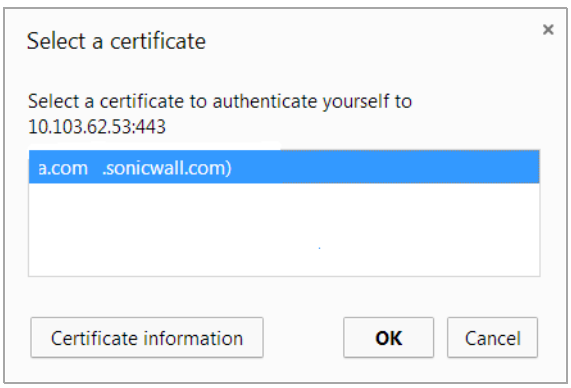
To import the client certificate:

1 Navigate to the Certificate details on your Web browser's settings.



2 Select the CA domain. A dialogue window displays. Choose a client certificate to authenticate. Click **OK**.

The authentication completes if the CA of the client certificate is on the Trusted CA certificates list. If the client certificate is not on the Trusted CA certificates list, the appliance blocks access and displays an error message.



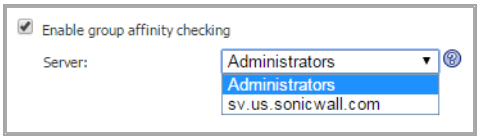
3 Next, the client certificate user must be authorized.

To authorize the client certificate:

1 Navigate to the **Portals > Domains** window and click the Configure icon for the domain to edit.

2 Select **Enable group affinity checking**.

3 Select one of the available domains from the drop-down list to designate as the **Server**.



4 Click **Accept**.

NOTE: Only Active Directory or LDAP servers and domains are supported.

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 on page 46.

SonicWall Inc.'s implementation of two-factor authentication either uses two separate RADIUS authentication servers, or 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 IdentiKey and Digipass tokens.

To configure two-factor authentication, you must first configure a RADIUS domain. For information see Adding or Editing a Domain with RADIUS Authentication on page 190.

The following sections describe how to configure the supported third-party authentication servers:

- Configuring the RSA Authentication Manager on page 196
- Configuring the VASCO IdentiKey Solution on page 201

Configuring the RSA Authentication Manager

The following sections describe how to configure the RSA Authentication Manager version 6.1 to do two-factor authentication with your SMA/SRA appliance:

- Adding an Agent Host Record for the SMA/SRA Appliance on page 197
- Adding the SMA/SRA Appliance as a RADIUS Client on page 197
- Setting the Time and Date on page 198
- Importing Tokens and Adding Users on page 199

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 is slightly different.

If you are using VASCO instead of RSA, see Configuring the VASCO IdentiKey Solution on page 201.

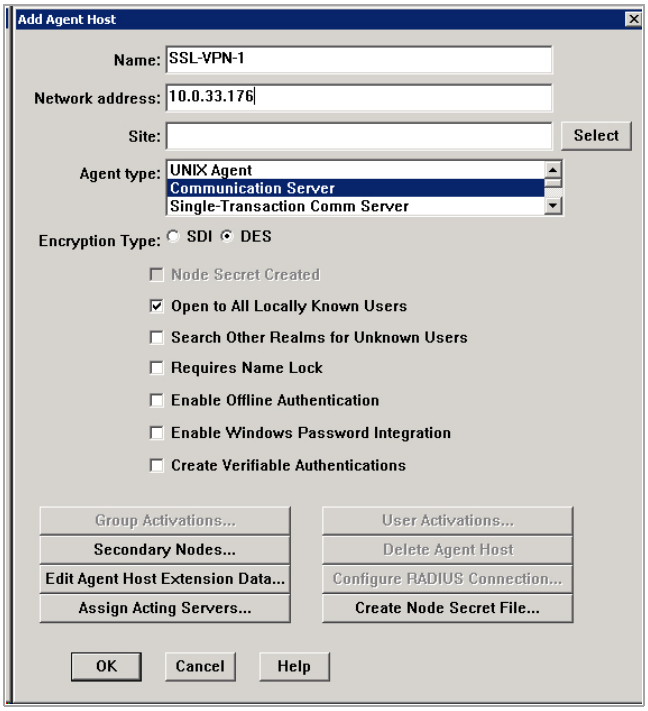
Adding an Agent Host Record for the SMA/SRA Appliance

To establish a connection between the SMA/SRA 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 SMA/SRA appliance within its database and contains information about communication and encryption.

To create the Agent Host record for the SMA/SRA appliance:

1 Launch the RSA Authentication Manager.

2 On the **Agent Host** menu, select **Add Agent Host**. The **Add Agent Host** window displays.



3 Enter a hostname for the SMA/SRA appliance in the **Name** field.

4 Enter the IP address of the SMA/SRA appliance in the **Network address** field.

5 Select **Communication Server** in the **Agent type** window.

6 By default, the **Enable Offline Authentication** and **Enable Windows Password Integration** options are enabled. SonicWall Inc. recommends disabling all of these options except for **Open to All Locally Known Users**.

7 Click **OK**.

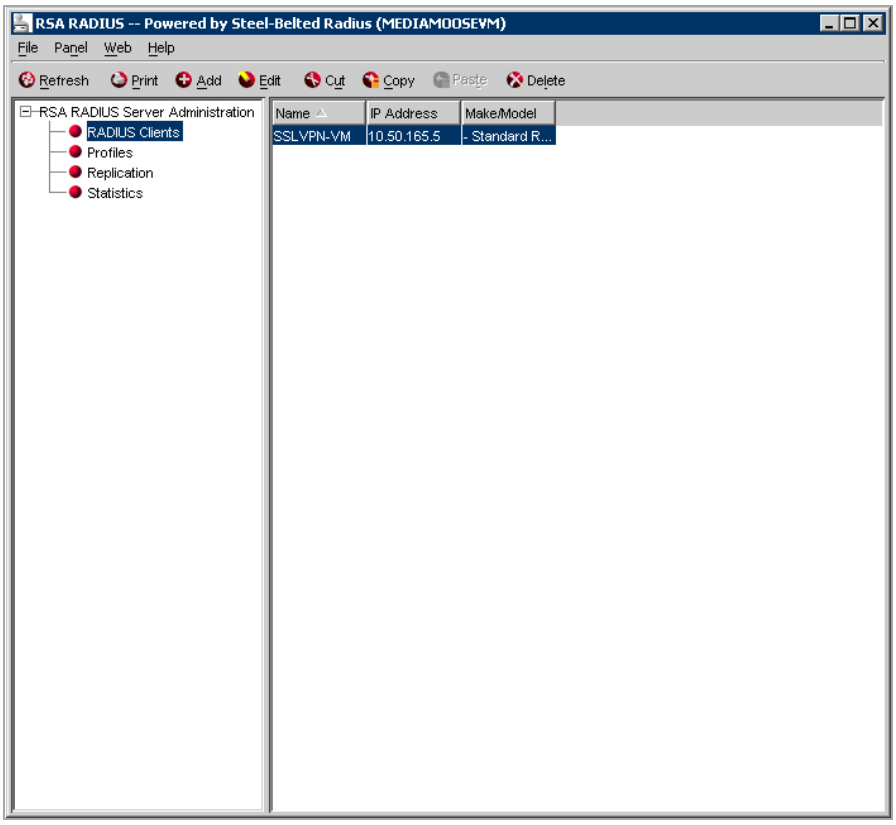
Adding the SMA/SRA Appliance as a RADIUS Client

After you have created the Agent Host record, you must add the SMA/SRA appliance to the RSA Authentication Manager as a RADIUS client.

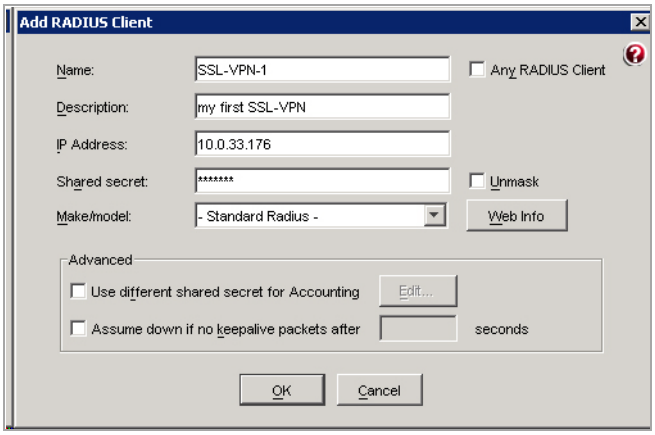
To do so, complete the following steps:

1 In RSA Authentication Manager, go to the **RADIUS** menu and select **Manage RADIUS Server**. The **RSA RADIUS Manager** displays.

2 Expand the **RSA RADIUS Server Administration** tree and select **RADIUS Clients**.



3 Click **Add**. The **Add RADIUS Client** window displays.



4 Enter a descriptive name for the SMA/SRA appliance.

5 Enter the IP address of the SMA/SRA appliance in the **IP Address** field.

6 Enter the shared secret that is configured on the SMA/SRA appliance in the **Shared secret** field.

7 Click **OK** and close the RSA RADIUS Manager.

Setting the Time and Date

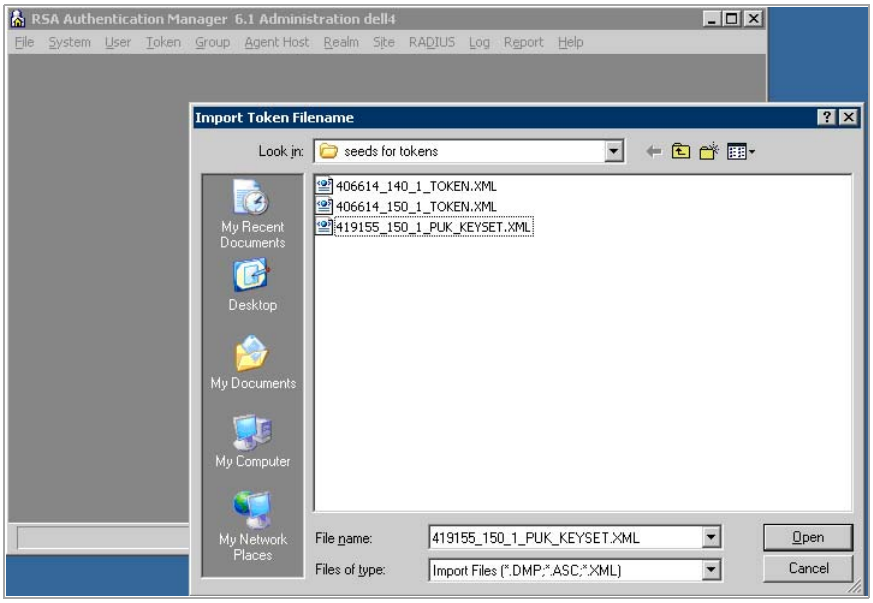
Because two-factor authentication depends on time synchronization, it is important that the internal clocks for the RSA Authentication Manager and the SMA/SRA appliance are set correctly.

Importing Tokens and Adding Users

After you have configured the RSA Authentication Manager to communicate with the SMA/SRA appliance, you must import tokens and add users to the RSA Authentication Manager.

To import tokens and add users:

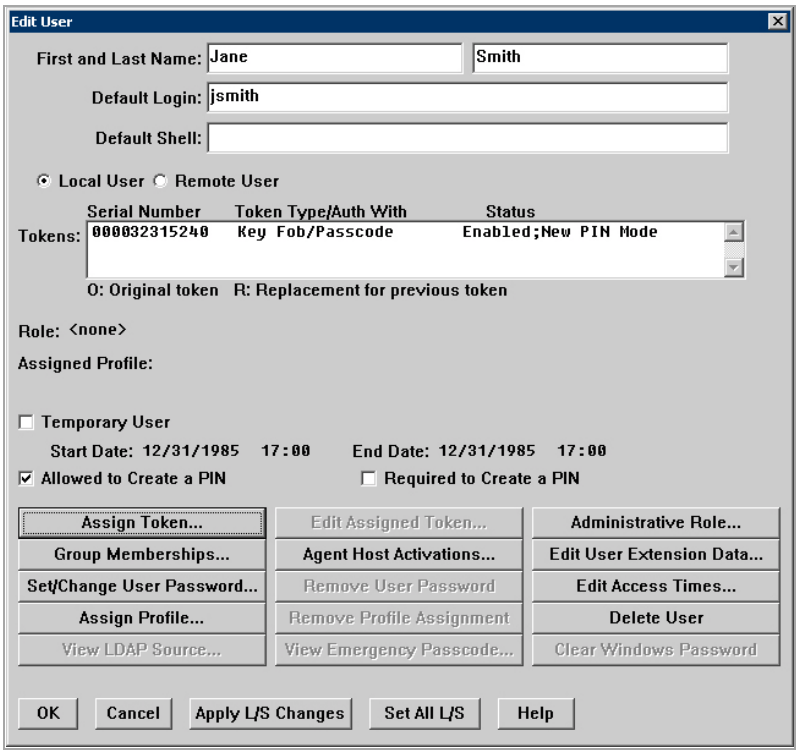
1 To import the token file, select **Token > Import Tokens**.



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.

3 The **Import Status** window displays information on the number of tokens imported to the RSA Authentication Manager.

4 To create a user on the RSA Authentication Manager, click on **User > Add user**.

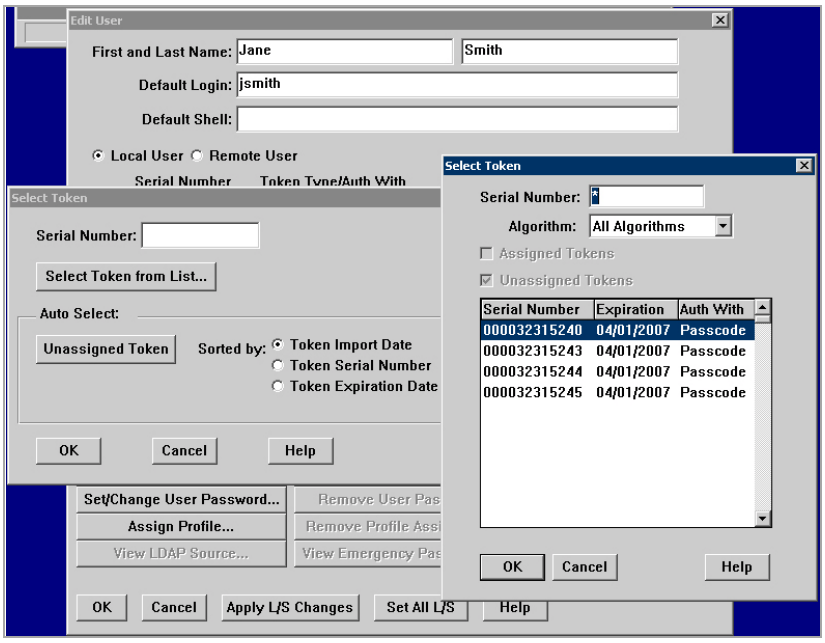


5 Enter the user's **First and Last Name**.

6 Enter the user's username in the **Default Login** field.

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.

8 To assign a token to the user, click **Assign Token**. Click **Yes** on the confirmation window that displays. The **Select Token** window displays.



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 **Unassigned Token** and the RSA Authentication Manager assigns a token to the user. Click **OK**.

10 Click **OK** in the **Edit User** window. The user is added to the RSA Authentication Manager.

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 *Secure Mobile Access User Guide* for more information.

Configuring the VASCO IdentiKey Solution

The VASCO IdentiKey solution works with Secure Mobile Access. The following sections describe how to configure two-factor authentication using VASCO's IdentiKey version 3.2:

NOTE: This configuration procedure is specific to VASCO IdentiKey version 3.2. If you are using a different version of VASCO IdentiKey, the procedure is slightly different.

If you are using RSA instead of VASCO, see Configuring the RSA Authentication Manager on page 196.

Setting the Time

The DIGIPASS token is based on time synchronization. Because the two-factor authentication depends on time synchronization, it is important that the internal clocks for the SMA/SRA appliance and the VASCO IdentiKey are set correctly.

Navigate to **System > Time** on the SMA/SRA appliance to select the correct time zone.

Setting DNS and the Default Route

The default route for the SMA/SRA appliance is an interface on the firewall that corresponds with the DMZ Zone. The IP address of this firewall DMZ interface needs to be configured as the default route for the SMA/SRA appliance.

To configure Domain Name Service and the default route:

1 On the Secure Mobile Access management interface, navigate to **Network > DNS** and set the correct DNS settings and/ or WINS Settings.

2 Navigate to **Network > Routes** and set the correct **Default Route** for the Secure Mobile Access **X0** interface.

Setting NetExtender Client Address Range and Route

To configure the NetExtender client address range and route on the SMA/SRA appliance:

1 Navigate to **NetExtender > Client Addresses** to set the **NetExtender Client Address Range**.

Client Addresses are assigned in the same subnet of the SMA/SRA X0 interface. Exclude the SMA/SRA appliance X0 interface and the firewall DMZ interface IP address.

2 Navigate to **NetExtender > Client Routes**.

Click **Add Client Route** to select the correct Client Routes for the authenticated remote users accessing the private networks by way of the SMA/SRA connection.

The client route corresponds with the subnet connected to the X0 (LAN) interface of the SonicWall Inc. NSA, TZ, or SuperMassive 9000 series.

Creating a Portal Domain with RADIUS Authentication

To create a domain using RADIUS authentication on the SMA/SRA appliance:

1 Navigate to **Portal > Domains** and click **Add Domain**.

2 Select **Radius** from the **Authentication Type** drop-down list.

3 Enter the **Domain Name** that users use in order to log in to the Secure Mobile Access portal.

Configuring a Policy on VASCO IdentiKey

To add a new policy in the VASCO Identikey Web Administration interface:

1 Log in to the Vasco Identikey Web Administration window.

2 Click the **Policies** tab and select **Create**.

NOTE: There are policies available by default, and you can also create new policies to suit your needs

3 Fill in a policy name and choose the option most suitable in your situation. If you want the policy to inherit a setting from another policy, choose the inherit option. If you want to copy an existing policy, choose the copy option, and if you want to make a new policy, choose the create option.

NOTE: Configure the policy properties to use the appropriate back-end server. This can be the same authentication service as previously used in the SMA/SRA appliance.

Use the following settings for the policy:

Policy settings

Local Auth	Default (DIGIPASS/Password)
Back-End Auth	Default (None)
Dynamic User Registration	Default (No)
Password Autolearn	Default (No)
Stored Password Proxy	Default (No)
Windows Group Check	Default (No Check)

Registering the SMA/SRA as a VASCO Client

To register the SMA/SRA appliance as a VASCO client:

1. In the Vasco Identikey Web Administration window, click the **Clients** Tab and choose **Register**.
2. Select **RADIUS Client** for **Client Type**.
3. Enter the IP address of the SMA/SRA appliance.
4. In the **Policy ID** field, select your new policy.
5. Fill in the **Shared Secret** you entered for the RADIUS server properties on the SMA/SRA appliance.
6. Click **Create**.

Configuring a VASCO IdentiKey User

To create a new user:

1. In the Vasco Identikey Web Administration window, click the **Users** tab and select **Create**.
2. Fill in the **User ID** field.
3. Select the **Domain**.
4. Select the **Organizational Unit**.
5. Click **Create**.

   The user appears in the list of users in the Vasco Identikey Web Administration management interface.

Importing DIGIPASS

To import a DIGIPASS:

1. In the Vasco Identikey Web Administration window, click on the **DIGIPASS** tab and select **Import**.
2. Browse for the ***.DPX** file.
3. Enter the **Transport Key**.
4. Click **UPLOAD**.

   A confirmation message pops up when the DIGIPASS is imported successfully.

Assigning a DIGIPASS to a User

There are two ways to assign a DIGIPASS to a user. You can search for a DIGIPASS and assign it to a user or search for a user and assign the user to a DIGIPASS.

1. Do one of the following:
   - On the **Users** tab, select the check box next to the user and then click **Assign DIGIPASS**.
   - On the **DIGIPASS** tab, select the check box next to the DIGIPASS and then click **NEXT**.

NOTE: If the **User ID** is left blank, press **Find** and a list of all the available users in the same domain appears. If no users appear, make sure the domains of the DIGIPASS and the user match.

When a user is assigned to a DIGIPASS, a confirmation message pops up.

Verifying Two-Factor Authentication

To test the two-factor authentication SMA/SRA connectivity with VASCO IdentiKey:

1. Connect your PC on the WAN (X1) interface of the SMA/SRA by pointing your browser to its IP address.
2. Log in to the Local Domain as an Administrator.
3. Navigate to **Portal > Domains** and click **Configure** to test the RADIUS connectivity to VASCO IdentiKey.
4. If the RADIUS Authentication is successful, log out of the Administrator account and log in to the WAN (X1) interface of Secure Mobile Access with the User Name you created.

Portals > Custom Logos

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, refer to Adding a Custom Portal Logo on page 156.

Portals > Load Balancing

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

Portals > Load Balancing Overview

The **Portals > Load Balancing** page allows the administrator to configure back end Web servers for a load balanced deployment. This default landing page for the load balancing feature allows the administrator to configure load balancing groups, and lists general properties of any existing load balancing groups.

NOTE: This feature also requires a Load Balanced Portal with virtual host to be configured in the **Portals > Portals** page.

Portals > Load Balancing Page

Configuration Scenarios

Load Balancing for Secure Mobile Access is a robust feature that has multiple uses, including:

Balancing a Farm of Web Servers – This is useful when the SMA/SRA appliance with a higher horse power is offering protection and balancing the load of a relatively low powered farm of Web servers. In this case, Web Application Firewall, URL rewriting and other CPU intensive operations are enabled on the Load Balancer.

Balancing a Low-Powered Cluster – A relatively low powered SMA/SRA cluster can be balanced for improved scalability. In this case, Web Application Firewall, URL rewriting, and other scalable features are enabled on the low powered SMA/SRA appliances.

Load Balanced Pair – In this scenario, the Load Balancer can have one portal configured for the front-end, and another Application Offloading portal configured to act as a Virtual Backend Server. This Virtual Backend Server and the second SMA/SRA device are configured as the Load Balancing Members and also take up the load of the Security Services. The Load Balancer in the previous two scenarios is essentially a dummy proxy without the load of any Security Services to burden it.

Load Balancing Settings

The following table lists **Portals > Load Balancing** configuration options. Additional per-group configuration options are described in Configuring a Load Balancing Group on page 205.

Load balancing configuration options

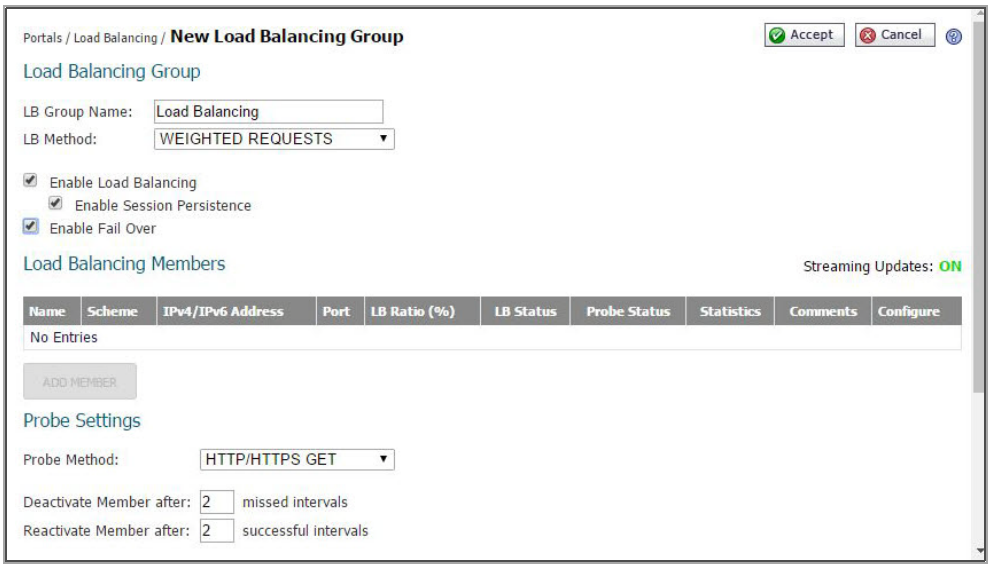
Option	Description
Enable Load Balancing	Enables the load balancing feature across all currently active groups.
Enable Fail Over	Enables/disables all probing, monitoring, and failover features.
Probe Interval	Determines the frequency (in seconds) at which the load balancing feature checks the status of backend nodes.

Configuring a Load Balancing Group

This section provides configuration details for creating a new load balancing group and consists of the following sections:

Adding a New Load Balancing Group

1 In the **Portals > Load Balancing** page, click **Add Group**. The New Load Balancing Group configuration information displays.



2 Enter a friendly **LB Group Name** for this load balancing group.

3 Select a load balancing method from the **LB Method** drop-down list. Options include:

- **Weighted Requests** – Keeps track of the number of incoming requests (including successfully completed requests) to decide which member should handle the next incoming request. The LB Ratio decides the percentage distribution.
- **Weighted Traffic** – Keeps track of the number of bytes of inbound/outbound data to decide which member should handle the next incoming request.
- **Least Requests** – Keeps track of the number of incoming requests (excluding successfully completed requests) that are currently being serviced to decide which Member should handle the next incoming request.

4 Select **Enable Load Balancing** to enable this group for load balancing.

5 The **Enable Session Persistence** option is automatically selected when the group is enabled. This option allows the administrator to enable continuous user sessions by forwarding the “requests” part of the same session to the same backend member.

6 Select **Enable Failover** to enable probing, monitoring, and failover features.

> **NOTE:** It is important to ensure that the same member receives all cookies to keep the user authenticated. However, for improved performance in certain situations, all backend members might be able to accept the session cookies of all users. In this case, the administrator can decide to turn off Session persistence. The Load Balancer then strictly adheres to the LB method and LB factors in distributing the load.

7 To add a new member to the group, see Adding New Members to a Load Balancing Group on page 207.

Configuring Probe Settings

To configure probe settings for this load balancing group in the **Probe Settings** section of the **Portals > Load Balancing** screen:

1 Select a **Probe Method** from the drop-down list. Options include:

- **HTTP/HTTPS GET** – The Load Balancer sends a HTTP(S) GET request periodically (based on the configured Probe interval) to see if the HTTP response status code is not greater than or equal to 500 to ensure there are no Web server errors. This is the most reliable method to determine if a Web server is alive. This method ignores SSL Certificate warnings while probing.
- **TCP Connect** – The Load Balancer completes a 3-way TCP handshake periodically to monitor the health of a backend node.
- **ICMP Ping** – The Load Balancer sends a simple ICMP Ping request to monitor if a backend node is alive.

2 In the **Deactivate Member after** field, enter the number of missed intervals required to fail the node. The default value is 2.

3 In the **Reactivate Member after** field, enter the number of successful intervals required to reinstate the node as functional. The default value is 2.

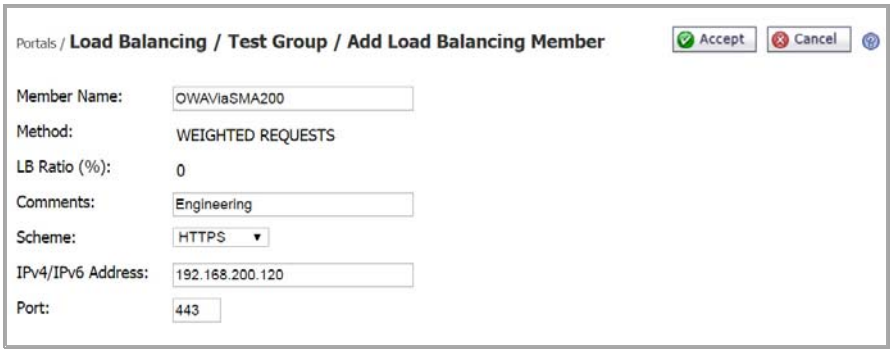
4 In the **Display error page when there is no resource available to fail over** text box, enter a custom message or Web page to display in the event that all of the configured backend nodes have failed. HTML formatting is allowed in this field.

Adding New Members to a Load Balancing Group

NOTE: You must create a Load Balancing group before you can begin adding members to the group.

To add members to a new or existing load balancing group:

1 When editing or adding a group from the **Portals > Load Balancing** page, click **Add Member**. The Load Balancing Member screen displays.

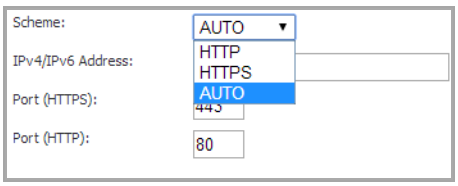


2 Enter a **Member Name** to uniquely identify this member within the Load Balancing Group.

3 Enter a friendly name or description in the **Comment** field to identify this group by mousing over the group's page.

4 Select a **Scheme** to connect to the backend server. Select one of the following options from the drop-down list: **HTTP**, **HTTPS**, or **AUTO**. The default value is HTTPS.

If AUTO is selected, specify two port numbers for HTTPS and HTTP.



NOTE: To enable HTTP access for the App Offloading Portal, select **Enable HTTP access**, located on the **Virtual Host** tab of the portal.

5 Enter the back end HTTP(S) server IP address in the **IPv4/IPv6 Address** field.

6 Enter the **Port** for the backend server. The default value for an HTTPS connection is 443. For Auto schemes, enter the port numbers for HTTPS and HTTP.

7 Click **Accept** to add this member to the group.

Portals > URL Based Aliasing

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

URL Based Aliasing overview

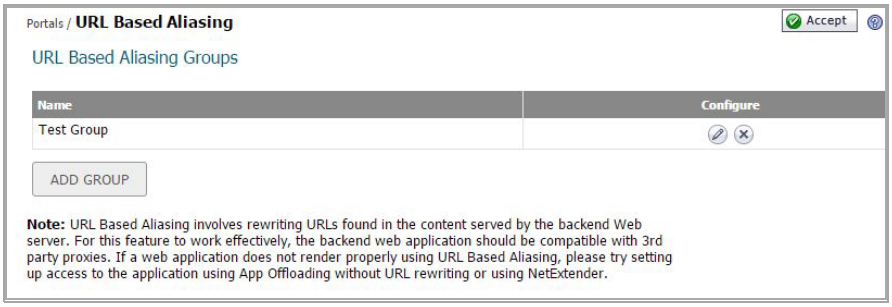
URL Based Aliasing provides the ability to access several different Web sites through one portal using one domain name. This feature is designed to be consistent with the Load Balancing setting. Because URL Based Aliasing involves rewriting URLS found in the content served by the backend Web server, the backend Web application should be compatible with third-party proxies. If a Web application does not render properly using URL Based Aliasing, you might need to set up access to the application using App Offloading without URL rewriting or using NetExtender.

Adding a URL Based Aliasing group

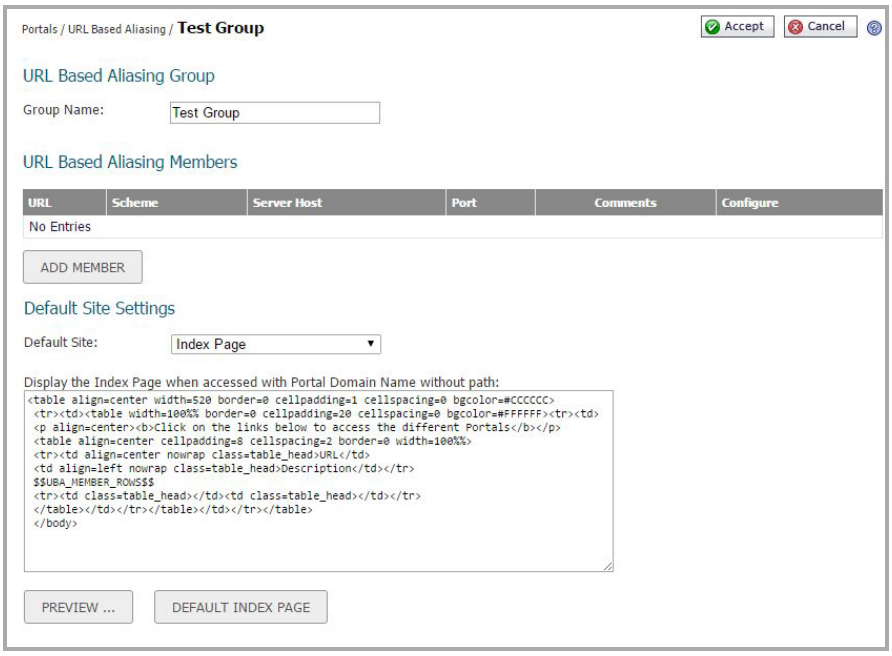
See also:

To add a URL Based Aliasing group:

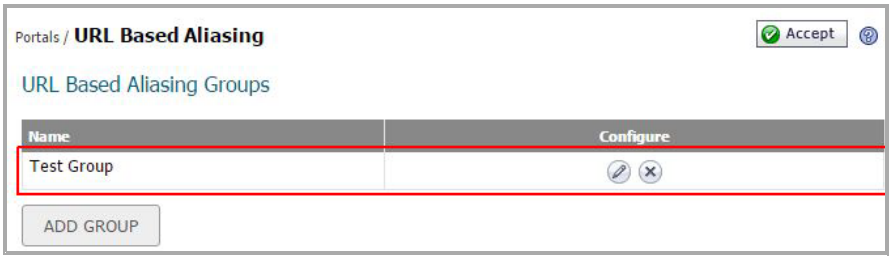
1 Navigate to the **Portals** > **URL Based Aliasing** page.



2 Under the URL Based Aliasing Groups section, click **Add Group**. The New URL Based Aliasing Group page displays.



3 Enter a **Group Name** in the field provided. Then, click **Accept**. The newly added group displays on the URL Based Aliasing Groups list.



Adding members

NOTE: You must create a URL Based Aliasing group before you can begin adding members to the group.

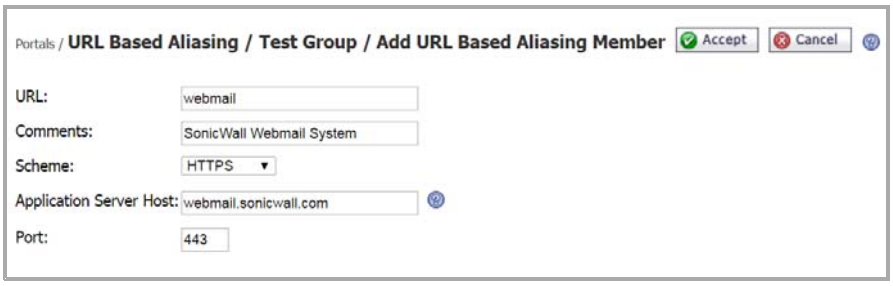
URL Based Aliasing allows you to add up to 100 members to a group.

To add members to a URL Based Aliasing group:

1 Navigate to the **Portals** > **URL Based Aliasing** page.

2 Click the **Configure** icon of the group you want to modify. The Group URL Based Aliasing Settings page displays.

3 Click **Add Member**. The Add URL Based Aliasing Member page displays.



Configure the following fields:

- **URL** — Enter the URL or name of the member.
- **Comments** — Enter any additional information. Anything entered in this field displays on the Index page.
- **Scheme** — Select from the drop-down list the scheme of the backend server. Select between HTTP, HTTPS, or AUTO.
- **Application Server Host** — Enter a Hostname, IPv4 address, or IPv6 address of the host.
- **Port** — Specify the port number. The default value is 443.

4 Click **Accept** to save changes and add a member to the group. The newly added member appears on the **URL Based Aliasing Settings** page.

Repeat steps 2 through 4 for each member you wish to add to the group.

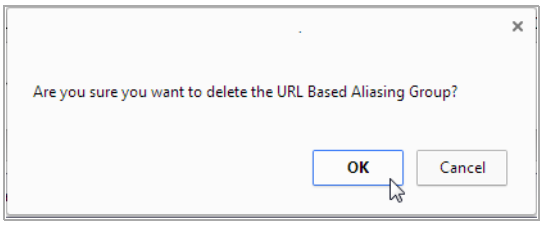
Deleting a group

To delete a specific group:

1 Navigate to the **Portal** > **URL Based Aliasing** page.

2 Click the **Delete** icon of the group you wish to delete.

3 A confirmation for deleting the group appears. Click **OK**.



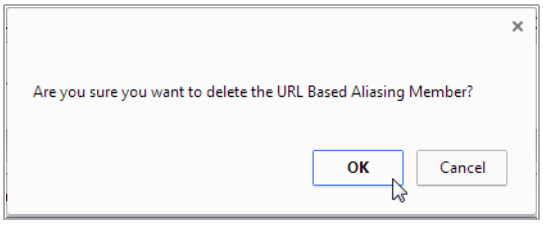
Deleting a member

To delete a specific member from a group:

1 Navigate to the URL Based Aliasing group settings page in which the member belongs.

2 Click the **Delete** icon of the member you wish to delete.

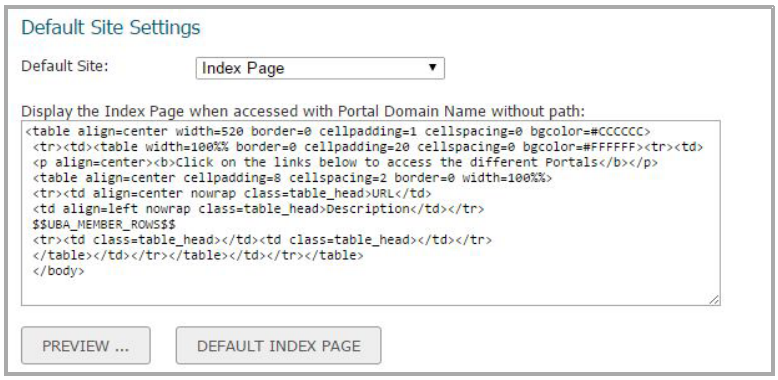
3 A confirmation for deleting the member appears. Click **OK**. Repeat these procedures for each group you want to delete.



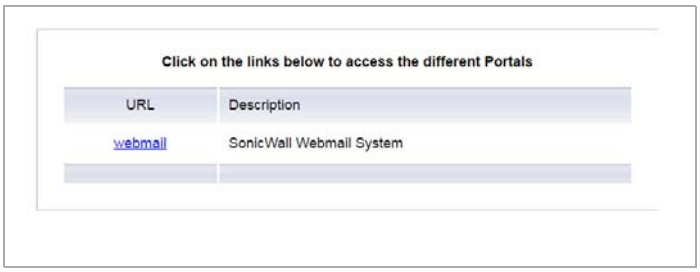
Default Site Settings

The Default Site Settings section provides the ability to set a default site when accessing the portal without any URL specified. The default value in the drop-down list is Index Page.

The Default Site Settings can be customized by editing the HTML, and then clicking **Accept**.



- Click **Preview...** to view the Index Page. To modify how this page appears, edit the HTML in the Default Site Settings section and click **Accept**.



- Click the **Default Index Page** to indicate the default page.

NOTE: Use the URL webmail.sonicwall.com. You are directed to the Index page that has hyperlink access for configured sites.

Part 3

Configuring Services & Clients

- Services Configuration
- Device Management Configuration
- NetExtender Configuration
- End Point Control
- Secure Virtual Assist Configuration
- Secure Virtual Meeting
- Web Application Firewall Configuration
- Geo IP and Botnet Filter
- High Availability Configuration

6

Services Configuration

This section provides information and configuration tasks specific to the **Services** pages on the Secure Mobile Access web-based management interface, including configuring settings, bookmarks, and policies for various application layer services, such as HTTP/HTTPS, Citrix, RDP, and VNC.

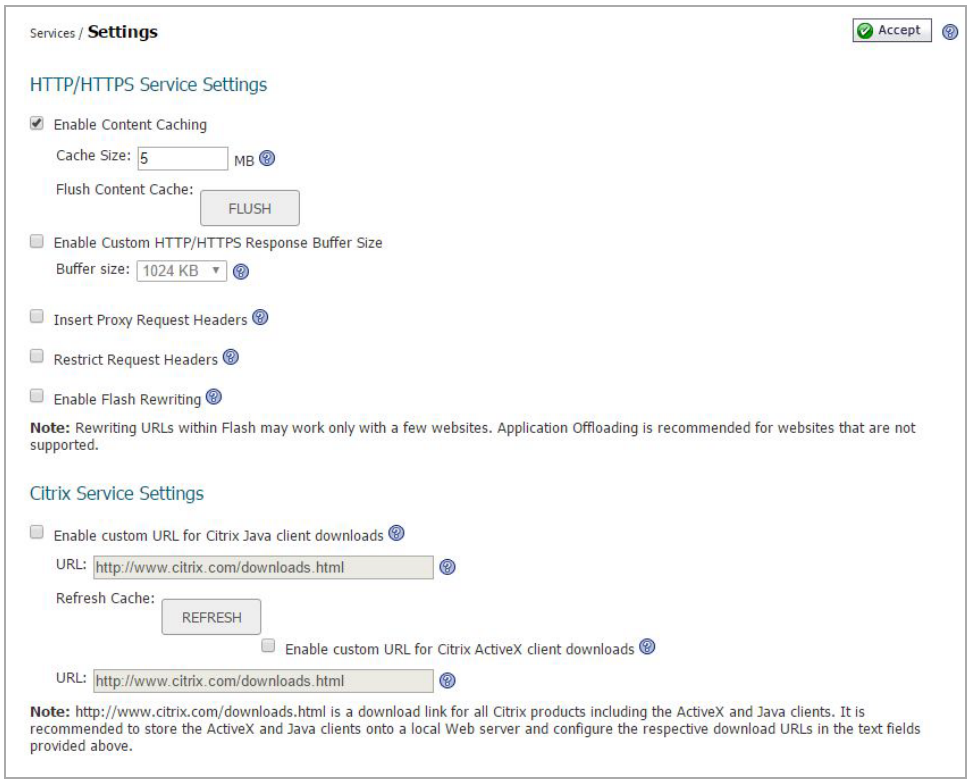
Topics:

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.

Services > Settings page



HTTP/HTTPS Service Settings

Administrators can take the following steps to configure HTTP/HTTPS Service Settings:

1. **Enable Content Caching** is selected by default. Administrators can disable the check box if they choose to do so. However, changing the Enable Content Cache setting restarts Secure Mobile Access 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 can set any size in the valid range from two to 20 MB. Select **Flush** to flush the content cache.

2. Check **Enable Custom HTTP/HTTPS Response Buffer Size**, if you wish to establish a response buffer. 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.

3. Check **Insert Proxy Request Headers** to insert these types of headers into the HTTP/HTTPS requests to the backend Web server. The following headers are 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 SMA/SRA proxy server.

4. Check **Restrict Request Headers** to strip unrecognized HTTP request headers.

5. Check **Enable Flash Rewriting** to rewrite URLs contained in Flash files. Rewriting URLs in Flash might work only with a few websites. Application Offloading is recommended for unsupported Web sites. This feature is disabled by default.

Citrix Service Settings

The administrator needs to host the Citrix clients on a local Web server and have Secure Mobile Access download these clients from there. For example, place the following Citrix Receiver clients on the Web server:

- For ActiveX: Receiver for Windows 3.0 – CitrixReceiver.exe
- For Java: Receiver for Java 10.1 – JICAComponents.zip

To configure Citrix Service Settings, complete the following steps:

1. Select **Enable custom URL for Citrix Java client downloads** 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 is used.
2. Select **Enable custom URL for Citrix ActiveX client downloads** 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 is used.

NetExtender/Mobile Connect Service Settings

1. Enable Compression to reduce file size when desired.
2. Enable verbose NetExtender debug logging. The mcd.log file would be part of Tech Support Reports (TSRs) generated from the **System > Diagnostics** page. Select the default log level from the **Log Level** drop-down menu; levels are listed from lowest to highest:
   - Debug
   - Info
   - Notice – default
   - Warning
   - Error

   All logs adhere to the default level set here unless specifically overridden.
3. To make changes to the logs in the Overrides section, deselect the Adhere to default level checkbox. All drop-down menus for all service categories become active.
4. **Enable Packet Capture** for NetExtender/Mobile Connect connections. Click **Download All** to download all of the saved Packet Captures. Click **Delete All** to delete all of the saved Packet Captures. Use this option for troubleshooting only, as it can affect the throughput adversely.

   NOTE: To capture the IPv4/IPv6 stream, disable the **Compression** option.

5. Based on the Packet Capture Type specified, a unique Pcap file is saved. Select the capture type from the **Capture Type** drop-down menu; types include:
   - **Per User** - Selecting **Per User** saves a unique Pcap file for each user while Packet Capture is on.
   - **Per NetExtender Client IP** - Selecting **Per NetExtender Client IP** saves a unique Pcap file for each Remote IP assigned by the SMA.
   - **Per User Session** - Selecting **Per User Session** saves a unique Pcap file for each User Session.
   - **Per Client IP** - Selecting **Per Client IP** saves a unique Pcap file for each Client IP that originally initiated a connection to the SMA.

Mobile Connect Default Policy Settings

Select from the following Mobile Connect default policy settings:

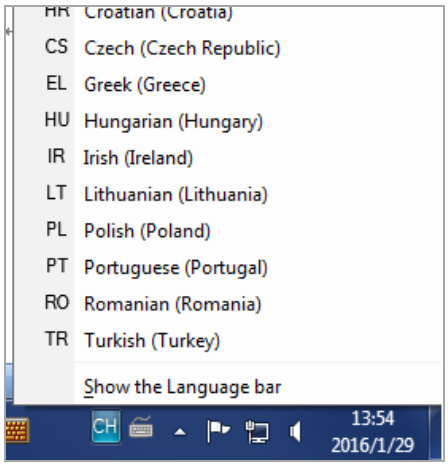
- **Allow Open in** - Allow a file to be opened in other apps, however, the Mobile Connect policies will not be enforced by other apps.
- **Allow Copy** - Allows portions of the file to be copied onto the clipboard,
- **Allow Print** - Allows a file to be printed.
- **Allow Caching** - Allows a file to be cached on the client, stored securely, and encrypted.

Global Portal Settings

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.

European keyboards

Some European characters cannot be input using US language keyboards. The keyboard type must be set and match on the Remote Server, the HTML5 server, or the Local Client computers.



The available keyboards are listed as follows:

Countries	Keyboards	Languages
Bosnia	Bosnian (Cyrillic)	Bosnian (Cyrillic, Bosnia and Herzegovina)
Bulgaria	Bulgarian	Bulgarian (Bulgaria)
Croatia	Croatian	Croatian (Croatia)
Czech Republic	Czech	Czech (Czech Republic)
Greece	Greek	Greek (Greece)
Hungary	Hungarian	Hungarian (Hungary)
Ireland	Irish	Irish (Ireland)
Lithuania	Lithuanian	Lithuanian (Lithuania)
Poland	Polish(214)	Polish (Poland)
Portugal	Portuguese	Portuguese (Portugal)

Countries	Keyboards	Languages
Romania	Romanian (Legacy)	Romanian (Romania)
Turkey	Turkish F	Turkish (Turkey)
Turkey	Turkish Q	Turkish (Turkey)
English	United States-International	English (United States)

To parse the input correctly, set the same language for the HTML5 Canvas (<canvas>) element by clicking the language identifier beside the S shield to trigger the language selection menu.

Language selection menu

Keep the keyboard language settings consistent between these three areas:

1 Local client machine

2 HTML5 settings

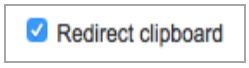
3 Remote RDP server machine

The Bookmark administrator can set the default language keyboard in the bookmark settings. When the bookmark is launched, the default language identifier is shown beside the S shield.

Copy/Paste text across the RDP session

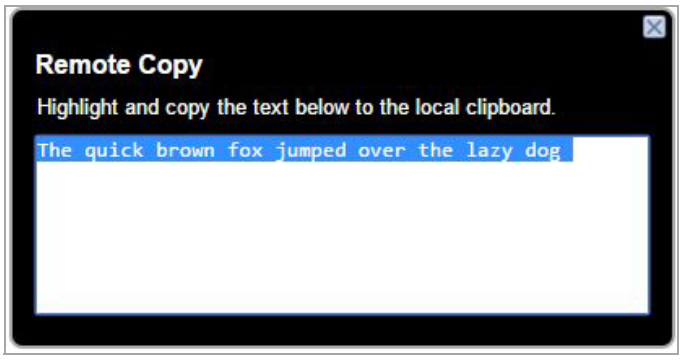
NOTE: Text cannot be copied and pasted to or from remote computers when using an HTML5 client in a Chrome, Edge, or Firefox browser.

The Bookmark administrator can also enable or disable the copy/paste functionality in the bookmark settings with the Redirect clipboard option, as well as enable or disable the copy/paste feature between local and remote sessions with **Redirect clipboard** and **Remote Copy**.



When enabled, after launching the bookmark and attempting to copy text from the remote server, an icon blinks below the S shield.

Click the blinking icon, and a dialog pops up with the copied text in the input field. You can copy the text manually from there and paste it to the local machine.



In the other direction, it works very smoothly just like copying/pasting locally. Simply copy the local string and paste it on remote machine.

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, complete the following tasks:

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%**).
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 following the **Email Body** field for additional attributes.
3. In the **One Time Password Format** drop-down list, select one of the following three options:
   - **Characters** – Only alphabetic characters are used when generating the one-time password.
   - **Characters and Numbers** – Alphabetic characters and numbers are used when generating the one-time password.
   - **Numbers** – Only numbers are used when generating the one-time password.
4. Use the **One Time Password Length** fields to adjust the range of characters allowed for one-time passwords.
5. Click **Accept** 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 One Time Password Overview on page 49.

Policy Match Log Settings

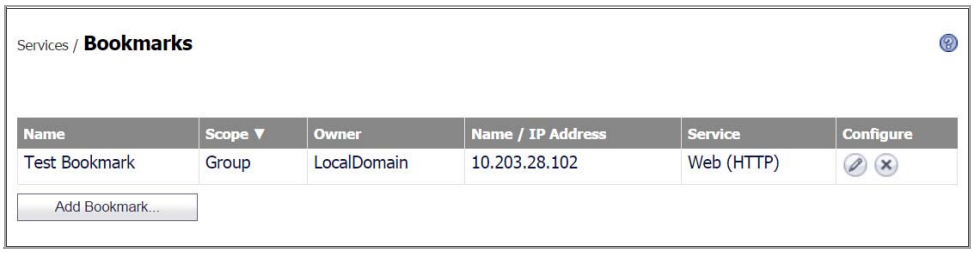
The Policy Match Log Settings allows you to access statistic information for policies. Policy Match Log Settings logs who matches set policies, where the user is from, and what destination the user is accessing. This information is then logged in the **Services** > **Policies** page.

To enable Policy Match Log:

1. Navigate to the **Services > Settings** page and scroll to Policy Match Log Settings section.
2. **Enable Policy Match** by selecting the respective check box.
3. **Enable Policy Match for Allow Action** allows you to set the server log matched information for Allow types.
4. **Enable Policy Match for Deny Action** allows you to set the server log matched information for Deny types.
5. In the **Keep log data field**, specify the amount of days you want the data to be kept in the log. The default value is 0.

Services > Bookmarks

The **Services > Bookmarks** page within the Secure Mobile Access web-based management interface provides a single interface for viewing bookmarks and access to configure bookmarks for users and groups.



NOTE: Alternative solutions (HTML5 bookmarks) have been developed to replace the notoriously insecure Java bookmarks. In the SMA 8.6 release, the Java bookmarks have been deprecated and disabled by default. If a Java bookmark is still required, contact Support for the steps necessary to enable the bookmark.

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

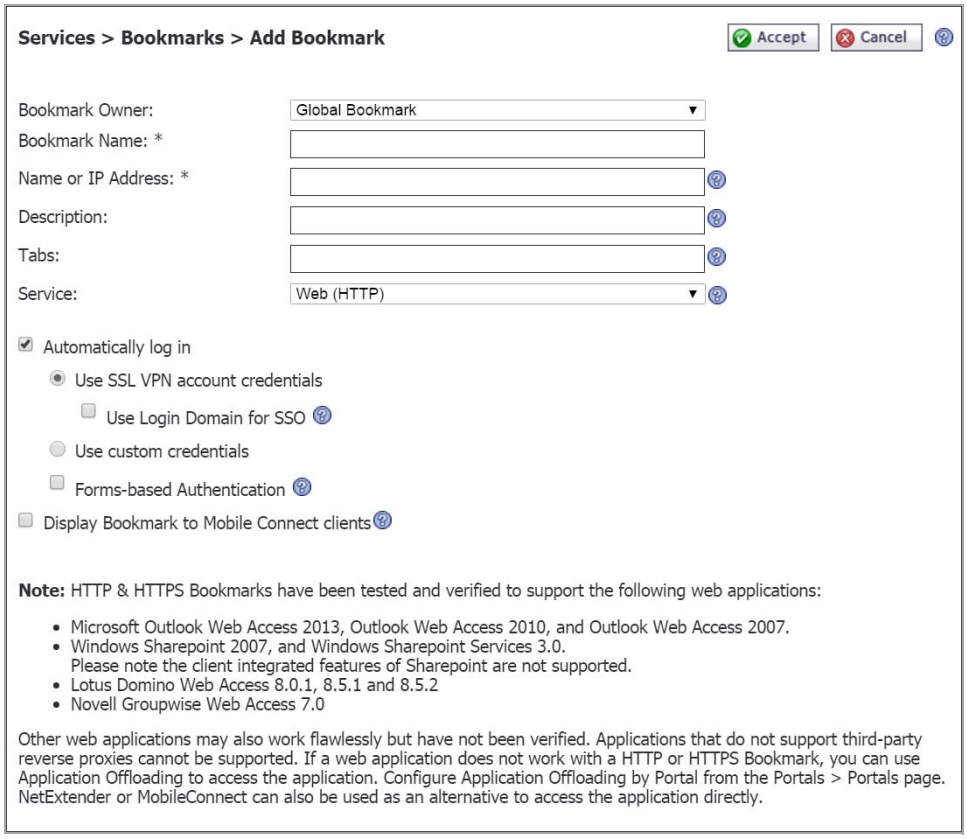
NOTE: The Secure Shell Version 1 (SSHv1) service type has also been removed. Existing SSHv1 bookmarks are still present within the system, but are hidden on the Portal page. If Java bookmarks have been enabled manually, they will be visible.

See:

- Adding or Editing a Bookmark on page 221

Adding or Editing a Bookmark

To add a bookmark, navigate to the **Services > Bookmarks** screen within the Secure Mobile Access management interface and select **Add Bookmark...**. The **Add Bookmark** window opens.



Complete the following steps to add a service bookmark:

1. Use the **Bookmark Owner** drop-down menu to select whether the bookmark is owned as a **Global Bookmark**, a **LocalDomain Group Bookmark**, or a bookmark assigned to an individual **User**.
2. Specify the **Bookmark Name** field with a friendly name for the service bookmark.
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 for File Shares (CIFS) bookmarks.

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 Name and IP address formats based on service type table.

Name and IP address formats based on service type

Service Type	Format	Example for Name or IP Address Field
RDP - HTML5	IP Address	10.20.30.4
	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 VNC - HTML5	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 following 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
SSHv2	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
HTTP HTTPS	URL	www.sonicwall.com
	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

Name and IP address formats based on service type (Continued)

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\
		10.20.30.4\status.doc
	IP\File	**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 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**.

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 - HTML5 and Native)

- 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 might 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** field.
- In the **Start in the following folder** field, optionally enter the local folder in which to execute application commands.
- Select **Login as console/admin session** to allow login as console or admin. Login as admin replaces login as console in RDC 6.1 and newer.

- Select **Enable wake-on-LAN** to enable waking up a computer over the network connection. Selecting this check box 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 **Send WOL packet to host name or IP address** that can be applied in tandem with a MAC address of another machine to wake.
- Check **Server is TS Farm** if the bookmark is used to launch a terminal service farm. A terminal service bookmark requires the client to have a compatible client installed to connect to the terminal server.

Terminal Services (RDP - HTML5)

- 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 might want to provide a path to where your application resides on your remote computer by typing the path in the **Application Path** field.

NOTE: RDP - HTML5 bookmarks are supported using the default browser on iOS and Android devices.

- In the **Colors** drop-down list, select the default color depth for the terminal service screen when users execute this bookmark.
- Select **Enable wake-on-LAN** to enable waking up a computer over the network connection. Selecting this check box 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 **Send WOL packet to host name or IP address** that can be applied in tandem with a MAC address of another machine to wake.
- Select **Login as console/admin session** to allow login as console or admin. Login as admin replaces login as console in RDC 6.1 and newer.
- Check **Server is TS Farm** if the bookmark is used to launch a terminal service farm. A terminal service bookmark requires the client to have a compatible client installed to connect to the terminal server.
- Click **Show Advanced Windows options** and select the desired check boxes for the following options: **Desktop background**, **Menu/window animation**, **Show window contents while dragging/resizing**, and **Enable Compression**.
- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in 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 on page 396.

Virtual Network Computing (VNC)

- In the **Encoding** drop-down menu, select the desired encoding transfer format. Options include Raw, RRE, CoRRE, Hextile, Zlib, and Tight.
- Use the **Compression Level** drop-down menu to select the desired compression level for data.
- 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**.
- Enable or disable the **Use CopyRect** function using the associated check box.
- Enable or disable the use of only **Restricted Colors (256 Colors)** by using the associated check box.

  NOTE: Mac screen sharing does not support restricted colors, so do not enable that option if Mac screen sharing is accessed.

- Enable **View Only** to control to prevent taking control over VNC.
- Enable **Share Desktop** to allow desktop view to be shared over VNC.
- Enable the **Display Bookmark to Mobile Connect clients** option to display your bookmark in Mobile Connect clients. Mobile Connect must be running version 2.0 or newer to view and access the Bookmark. Support varies by device and could require supported third-party applications being installed.

HTML5 bookmark features

Available features

Feature	HTML5 version
Encoding	Yes (Not configurable, determined by the VNC server, supported encoding: Raw, Copyrect, RRE, hextile, Tight, TightPNG, and Zlib)
Compression Level	No
JPEG Image Quality	No
Cursor Shape Updates	Yes (Enabled by default. Not supported on IE. For mobile browsers, “Cursor shape updates” is always disabled)
Use CopyRect	Yes (Not configurable)
Restricted Colors (256 Colors)	No
View Only	Yes
Share Desktop	Yes
Display Bookmark to Mobile Connect clients	Yes

Virtual Network Computing (VNC - HTML5)

- Enable **View Only** to control to prevent taking control over VNC.
- Enable **Share Desktop** to allow desktop view to be shared over VNC.

Citrix Portal (Citrix)

- In the **Resource Window Size** drop-down list, select the default screen size to be used for Citrix sessions when users execute this bookmark.

- Select to have a **Smart** or **Manual Access Type selection** for this bookmark. A new Citrix bookmark is **Smart** by default. The launch sequence is as follows: HTML5, Native, and ActiveX. Selecting Manual allows you to change, enable, or disable the Access Type launch methods.
- Select **Disable client detection by Citrix server** to disable the client detection done by the Citrix server when using the bookmark. The SMA/SRA appliance always completes a Citrix client detection when using Citrix. Enabling client detection on the Citrix server makes this client detection redundant.

NOTE: This feature is compatible with Citrix XenApp 5.0 or later by using an ActiveX client.

- If the Citrix Web server is configured with SSL, to enable SSL encryption for communication between the SMA/SRA appliance and the Citrix server, select **HTTPS Mode**.
- To explicitly set the Citrix ICA server address for the Citrix ICA session, select **Always use specified Citrix ICA Server** and then type the server IP address into the **ICA Server Address** field.

  Some Citrix deployments have the Citrix Web Interface on one IP address and the ICA server listening on a different address. If the Citrix Web Interface and Citrix ICA server do not share the same IP address, use this setting to explicitly set the ICA server address.
- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in 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 on page 396.
- Select **Display Bookmark to Mobile Connect clients** to display this Citrix bookmark in Mobile Connect clients. Support varies between devices and could require supported third-party applications to be installed.

NOTE: Mobile Connect must be running version 2.0 or newer to view and access the Citrix bookmark.

- Select **Force MC Secure Web Browser** to force Mobile Connect user to utilize the in-app Secure Web Browser instead of the configured third-party app. Mobile Connect must be running version 5.0 or newer for this option to be in effect. This setting overrides the user setting for HTTP and HTTPS bookmarks, and is only available for RDP, VNC, SSH, Telnet, HTTP, HTTPS, and External Website services.
  - Select **Allow Edit URL in Secure Web Browser** to allow the user to edit the URL in the Mobile Connect Secure Web Browser. Mobile Connect must be running version 5.0 or newer for this option to take effect. Enabling this option overrides the Mobile Connect client Bookmark settings for Web Bookmarks (HTTP/HTTPS). This setting is only available for HTTP/HTTPS bookmarks.
- Click **OK**.

Web (HTTP)

- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in 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 on page 396.
- Select **Forms-based Authentication** 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>.

- Select **Display Bookmark to Mobile Connect clients** to display this bookmark in Mobile Connect clients. Support varies between devices and could require supported third-party applications to be installed.

NOTE: Mobile Connect must be running version 2.0 or newer to view and access the Web (HTTP) bookmark.

- Select **Force MC Secure Web Browser** to force Mobile Connect user to utilize the in-app Secure Web Browser instead of the configured third-party app. Mobile Connect must be running version 5.0 or newer for this option to be in effect. This setting overrides the user setting for HTTP and HTTPS bookmarks.
    - Select **Allow Edit URL in Secure Web Browser** to allow the user to edit the URL in the Mobile Connect Secure Web Browser. Mobile Connect must be running version 5.0 or newer for this option to take effect. Enabling this option overrides the Mobile COnnect client Bookmark settings for Web Bookmarks (HTTP/HTTPS).

Secure Web (HTTPS)

- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in 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 on page 396.
- Select **Forms-based Authentication** 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>.
- Select **Display Bookmark to Mobile Connect clients** to display this HTTPS bookmark in Mobile Connect clients. Support varies between devices and could require supported third-party applications to be installed.

NOTE: Mobile Connect must be running version 2.0 or newer to view and access the HTTPS bookmark.

- Select **Force MC Secure Web Browser** to force Mobile Connect user to utilize the in-app Secure Web Browser instead of the configured third-party app. Mobile Connect must be running version 5.0 or newer for this option to be in effect. This setting overrides the user setting for HTTP and HTTPS bookmarks.
    - Select **Allow Edit URL in Secure Web Browser** to allow the user to edit the URL in the Mobile Connect Secure Web Browser. Mobile Connect must be running version 5.0 or newer for this option to take effect. Enabling this option overrides the Mobile COnnect client Bookmark settings for Web Bookmarks (HTTP/HTTPS).

External Web Site

- **HTTPS Mode** — The HTTPS mode is used to encrypt Web communication by using the SSL protocol.
- **Disable security warning** — If this bookmark does not refer to an Application Offloaded Web site and this check box is disabled, then a security warning dialog is displayed.

- **Automatically log in** — Enable Virtual Host Domain SSO for this bookmark. If the host in the bookmark refers to a portal which has the same shared domain with this portal, it could be logged in automatically with this portal's credential.
- Select **Display Bookmark to Mobile Connect clients** to display this External Web Site bookmark in Mobile Connect clients. Support varies between devices and could require supported third-party applications to be installed.

NOTE: Mobile Connect must be running version 2.0 or newer to view and access the External Web Site bookmark.

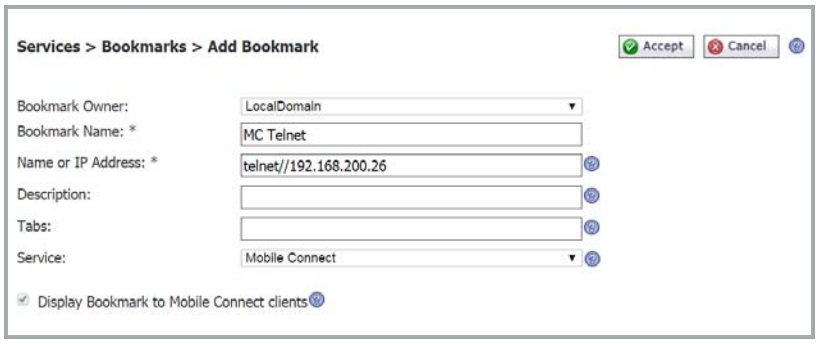
- Select **Force MC Secure Web Browser** to force Mobile Connect user to utilize the in-app Secure Web Browser instead of the configured third-party app. Mobile Connect must be running version 5.0 or newer for this option to be in effect. This setting overrides the user setting for HTTP and HTTPS bookmarks.
    - Select **Allow Edit URL in Secure Web Browser** to allow the user to edit the URL in the Mobile Connect Secure Web Browser. Mobile Connect must be running version 5.0 or newer for this option to take effect. Enabling this option overrides the Mobile COnnect client Bookmark settings for Web Bookmarks (HTTP/HTTPS).

Mobile Connect

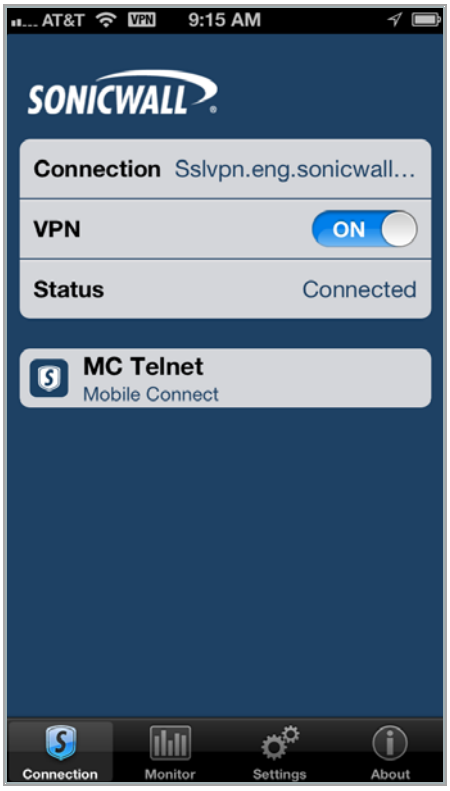
The Mobile Connect bookmark allows a custom bookmark to be defined for display in Mobile Connect after the user is connected. This bookmark is meant to support any third-party app, whether an in-house app or a public app in the App Store or Google Play. The bookmark also enables calling third-party apps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

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

- Enter the **Bookmark Name** and the **Name or IP Address**. The Name or IP Address field is the custom URL scheme.
- Enable **Display Bookmark to Mobile Connect clients** to send bookmark information to Mobile Connect clients.

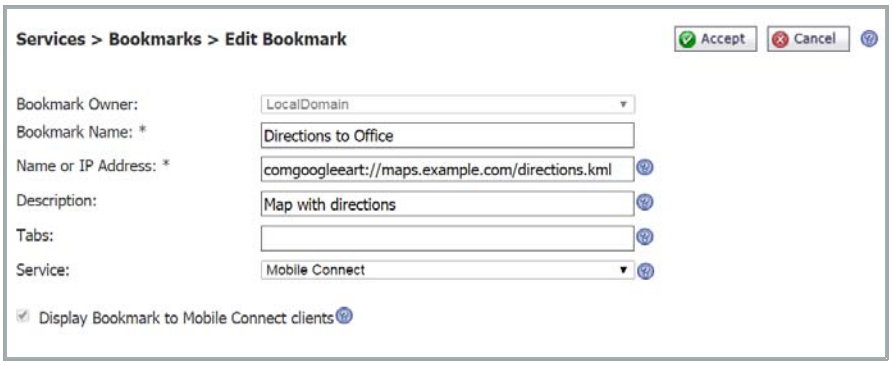


After the Mobile Connect bookmark on Secure Mobile Access is successfully configured, the bookmark displays on your mobile device:

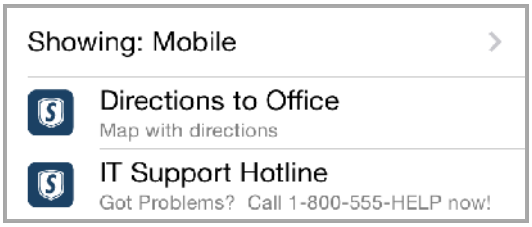


The following example of a Mobile Connect bookmark shows how you can create a bookmark using Google Earth to display a map with specific directions.

First, you must create the bookmark with the URL scheme:



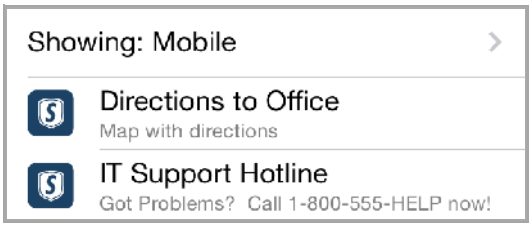
This bookmark is now available to access from your mobile device.



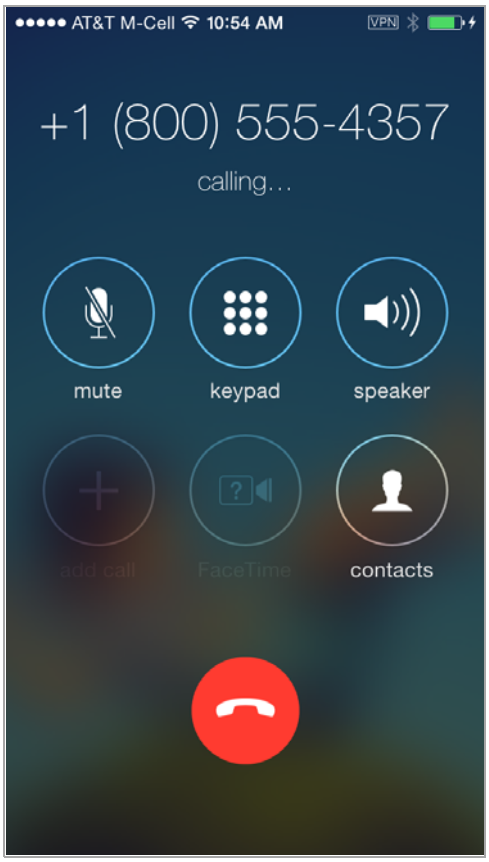
Click the newly added bookmark. For the “Directions to Office” bookmark, a Google Map displays:

The following example shows another way to use the Mobile Connect bookmark. In this example, you add a bookmark that launches the Phone app on iOS to make a call to the IT Support Hotline.

This bookmark is now available to access from your mobile device.



Click the newly added bookmark. For the “IT Support Hotline” bookmark, the iOS Phone app begins a call to the IT Support Hotline:



File Shares (CIFS)

NOTE: SMB2 and SMB3 protocols are currently not supported. Servers should be configured to allow communication from a Linux based client.

- To restrict access on the client UI, select **Set user to access the specific files/folders**. To completely restrict access, navigate to the **Services** > **Policies** page to set a policy for access constraints. For more information, see Adding a Policy on page 234.
- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in 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 on page 396.
- Enable **Display Bookmark to Mobile Connect clients** to send bookmark information to Mobile Connect clients.

  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 disables access to the DFS file shares from other domains. The SMA/SRA appliance is not a domain member and is not 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) and SSH File Transfer Protocol (SFTP)

- 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 Secure Mobile Access session for log in 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 on page 396.
- Enable **Display Bookmark to Mobile Connect clients** to send bookmark information to Mobile Connect clients.

Telnet HTML5 Settings

- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in 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 on page 396.
- Select **Display Bookmark to Mobile Connect clients** to display this External Web Site bookmark in Mobile Connect clients. Support varies between devices and could require supported third-party applications to be installed.

NOTE: Mobile Connect must be running version 2.0 or newer to view and access the External Web Site bookmark.

- Select **Force MC Secure Web Browser** to force Mobile Connect user to utilize the in-app Secure Web Browser instead of the configured third-party app. Mobile Connect must be running version 5.0 or newer for this option to be in effect. This setting overrides the user setting for HTTP and HTTPS bookmarks.
    - Select **Allow Edit URL in Secure Web Browser** to allow the user to edit the URL in the Mobile Connect Secure Web Browser. Mobile Connect must be running version 5.0 or newer for this option to take effect. Enabling this option overrides the Mobile COnnect client Bookmark settings for Web Bookmarks (HTTP/HTTPS).

Secure Shell Version 2 (SSHv2)

SSHv2 HTML5 Settings

- Select the **Default Font Size**. Supported options range from 12 to 99 points.
- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in 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 on page 396.

SSHv2 Common Settings

- Optionally select **Automatically accept host key**. This option allows the browser to keep the server's public host key in local storage automatically.

- Select **Display Bookmark to Mobile Connect clients** to display this External Web Site bookmark in Mobile Connect clients. Support varies between devices and could require supported third-party applications to be installed.

NOTE: Mobile Connect must be running version 2.0 or newer to view and access the External Web Site bookmark.

- Select **Force MC Secure Web Browser** to force Mobile Connect user to utilize the in-app Secure Web Browser instead of the configured third-party app. Mobile Connect must be running version 5.0 or newer for this option to be in effect. This setting overrides the user setting for HTTP and HTTPS bookmarks.
    - Select **Allow Edit URL in Secure Web Browser** to allow the user to edit the URL in the Mobile Connect Secure Web Browser. Mobile Connect must be running version 5.0 or newer for this option to take effect. Enabling this option overrides the Mobile COnnect client Bookmark settings for Web Bookmarks (HTTP/HTTPS).
- If using an SSHv2 server without authentication, such as a SonicWall Inc. firewall, you can select **Bypass username**.
- Click **Accept** to update the configuration. After the configuration has been updated, the new group bookmark displays in the **Edit Local Group** page.

Editing a Bookmark

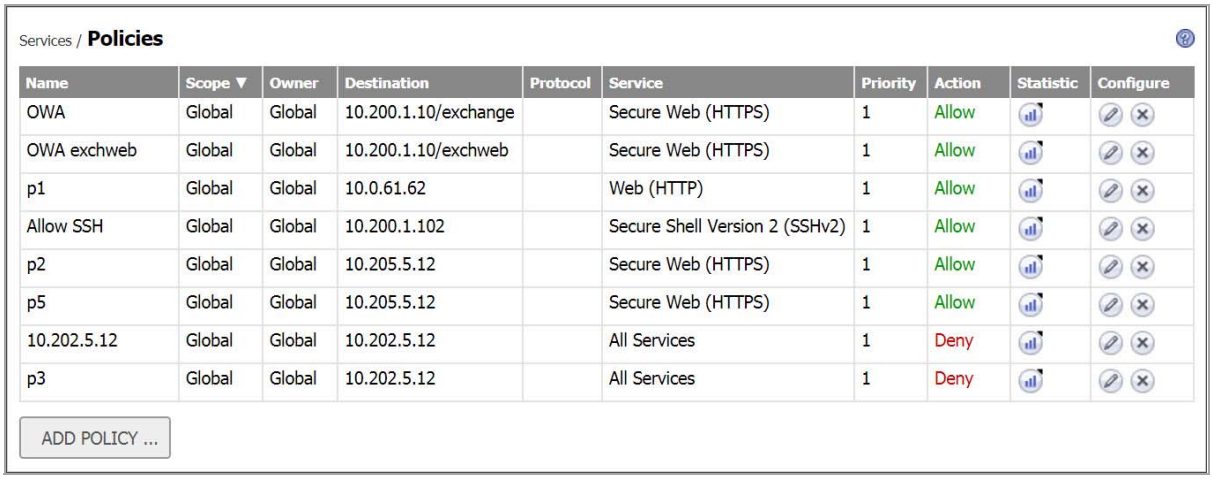
To edit a service bookmark, navigate to the **Services > Bookmarks** screen. Click on the **pencil icon** in the **Configure** column. A new **Edit Bookmark** window opens with the bookmark's current configuration. Make all desired adjustments and select **OK**. The edited bookmark still displays in 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 opens and asks if you are sure you want to delete the specified bookmark. Click **OK** to delete the bookmark. The bookmark no longer appears in the **Services > Bookmarks** screen.

Services > Policies

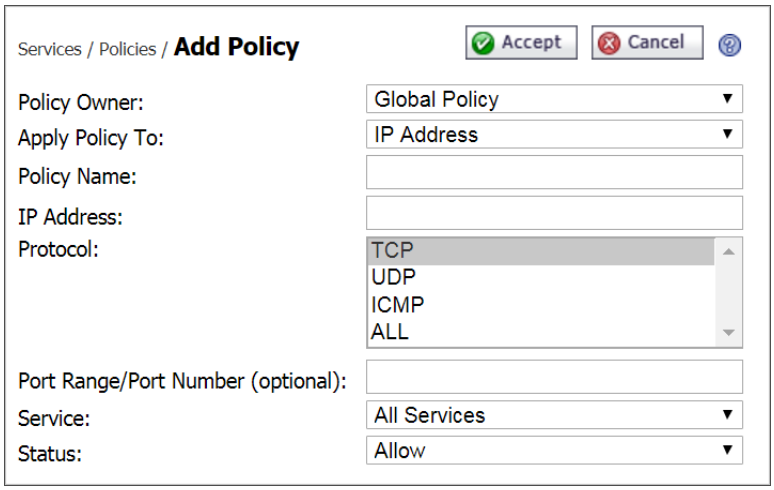
The **Services > Policies** page within the Secure Mobile Access web-based management interface provides a single interface for viewing service policies and access to configure policies for users and groups.



See:

Adding a Policy

To add a policy, navigate to the **Services > Policies** screen within the Secure Mobile Access management interface and select **Add Policy...** The **Add Policy** window opens.



Administrators can follow the following steps to add a service policy:

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**.

2 In the **Apply Policy To** drop-down menu, select whether the policy is applied to an individual host, a range of network addresses, all addresses, a network object, a server path, or a URL object. 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 Secure Mobile Access policies apply to the destination address(es) of the Secure Mobile Access connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the SMA/SRA 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 on page 397.

3 Complete the appropriate step that follows 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 on page 369.
- **IP Network** - 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 Network on page 370.
- **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 on page 370.

- **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 Adding Network Objects on page 139
- **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 on page 370.
- **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 on page 371.
- **All IPv6 Address** - If your policy applies to all IPv6 addresses, you do not need to enter any IP address information. See Adding or Editing User Bookmarks on page 374.
- **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. See Adding a Policy for an IPv6 Address on page 373.
- **IPv6 Network** - 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 Network on page 374.

4 Select the desired **Protocol**. The available value options in the Protocol field include: **TCP**, **UDP**, **ICMP**, and **ALL**. You can select multiple items among **TCP**, **UDP** and **ICMP**. However, when **ALL** is selected, all others options are deselected.

> **NOTE:** The protocol setting only appears when the Service is set to “NetExtender & Mobile Connect” or “All Services.”

5 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.

6 Select **ALLOW** or **DENY** from the **Status** drop-down list to either allow or deny SMA connections for the specified service and host machine.

> **NOTE:** One or more policies can be added to deny a specific access method that was selected during the wizard.

> **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.

7 Click **Accept** to update the configuration. After the configuration has been updated, the new policy is displayed in the **Services > Policies** window.

NOTE: SonicWall Inc. recommends that administrators set up a Global Deny ALL policy that allows access to only trusted hosts. This prevents outbound requests to malicious hosts from Secure Mobile Access.

To create a Global Deny ALL policy:

1 From the **Services > Policy** page, click **Add Policy**.

2 For **Policy Owner**, select **Global Policy** from the drop-down list.

3 For **Apply Policy To**, select **All Addresses** from the drop-down list.

4 For **Policy Name**, create a friendly name for this policy, such as “Deny ALL.”

5 Select the desired **Protocol**. The available value options in the Protocol field include: **TCP**, **UDP**, **ICMP**, and **ALL**. You can select multiple items among **TCP**, **UDP**, and **ICMP**. However, when **ALL** is selected, all others options are deselected.

NOTE: The protocol setting only appears when the Service is set to “NetExtender & Mobile Connect” or “All Services.”

6 The **IP Address Range** automatically defaults to **All IP Addresses**.

7 For **Service**, select **All Services** from the drop-down list.

8 For **Status**, select **Deny** from the drop-down list.

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 opens with the bookmark’s current configuration. Make all desired adjustments and select **Accept**. The edited bookmark still displays 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 opens and asks if you are sure you want to delete the specified policy. Click **OK** to delete the policy. The policy no longer appears in the **Services > Policies** screen.

7

Device Management Configuration

This section provides information and configuration tasks specific to the Device Management pages on the Secure Mobile Access web-based management interface.

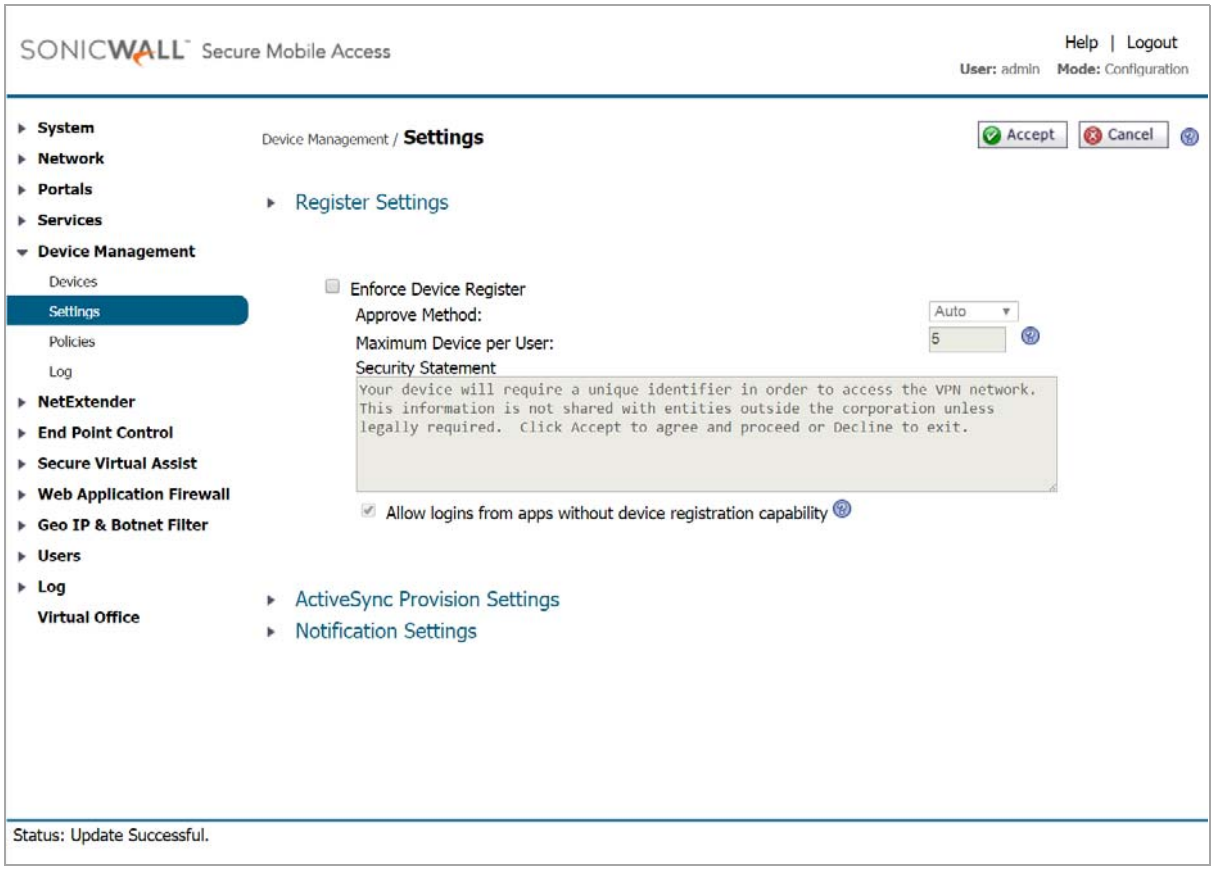
Topics:

Device Management > Devices

Secure Mobile Access obtains the client device's unique Device ID. With that information, you can view all devices, change device status, and delete unwanted devices.

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

Device Management > Settings



Register settings

Enforce Device Register

This option is used to disable or enable the Personal Device Authorization (PDA). It is disabled by default.

Approve Method

There are two methods: **Auto** and **Manual**. 1) The **Manual** mode means that each device first registered by one user is set to the “pending” or “wait for the administrator to approve” status. 2) The device will be set as approved by the system in auto mode. Auto mode can reduce the workload of the administrator.

Maximum Device per User

This option limits the maximum devices each user can register.

Security Statement

This alert message appears on the client when the user logs in. You can customize this security statement.

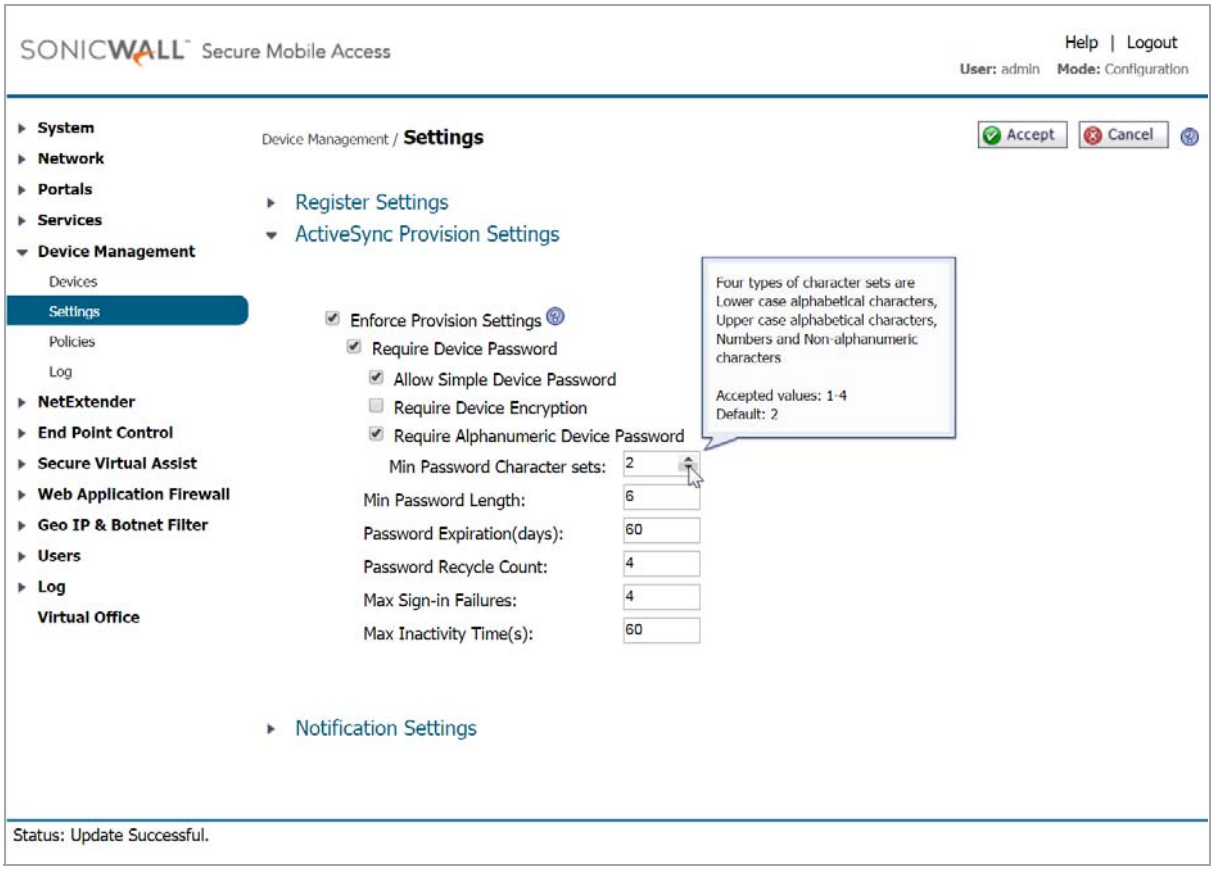
Allow logins from apps without device registration capacity

This option applies to SMA Connect Agent devices, such as Linux/Android/iOS/Windows phones. When you enable this option, devices are able to access the appliance without device registration.

Described above is a global configuration, you can customize the registration settings at domain level when you enable device register. The domain level settings have a higher priority than the global settings.

ActiveSync Provision Settings

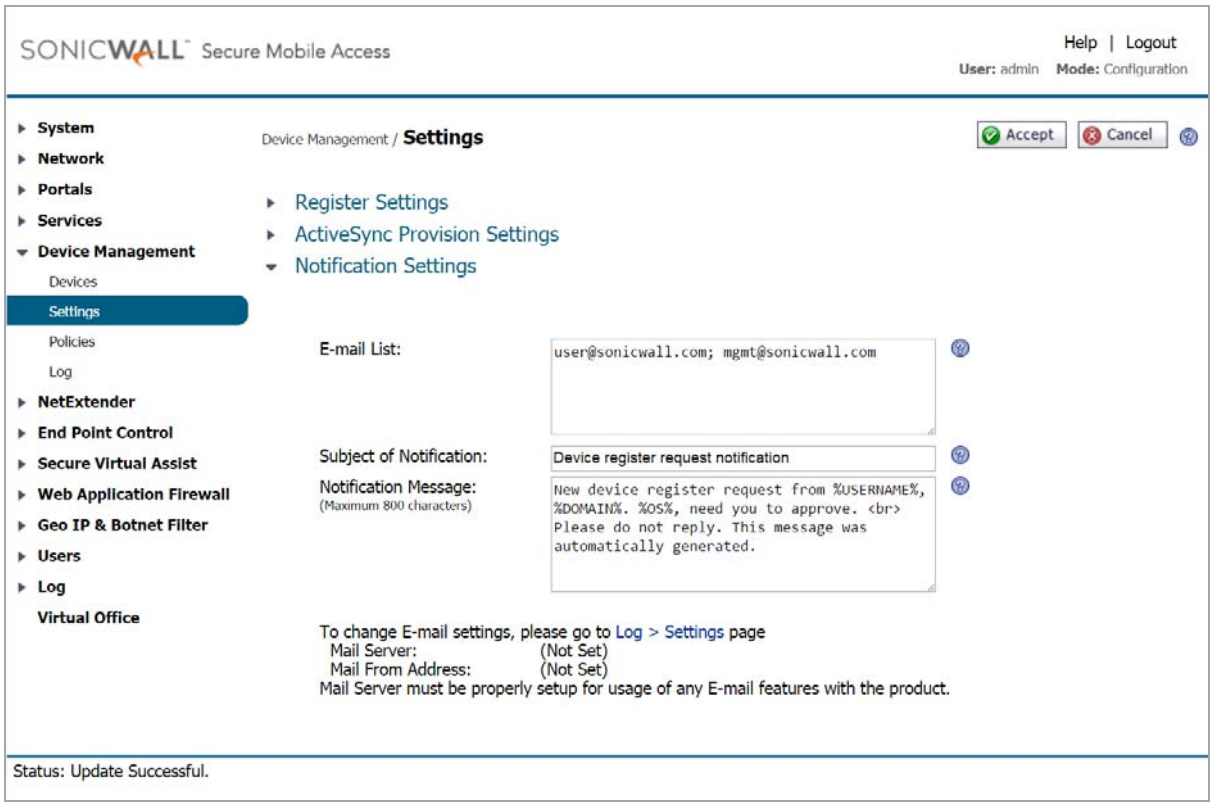
ActiveSync Provision Settings can be applied specifically to ActiveSync devices. Provision settings can override the settings on a backend Exchange server. Mobile devices are not able to sync when the Provision settings are not satisfied.



Notification Settings

You can list a set of email addresses here. When a new registration request arrives, an email notification is sent to these addresses notifying the recipients to handle the request.

The notification email's Subject and Message can be customized.



Device Management > Policies

Device policies are global and initially apply to each device register request. The device takes the policy's defined action when matching policies. When unmatched, the device gets it's status according to the option of the approved method. This can reduce the workload of administrator.

There are two types of device policies: **Device Id** and **OS**. The Device Id has a higher priority than OS by default.

There are also two Operators: **Matches Regex** and **Equals String**. Equals String is case sensitive. Equals String has priority to Matches Regex by default.

The Action option has three choices: **Reject**, **Approve**, and **Pending**. The device takes on the defined action when it matches the policies.

Device Management > Log

The Device Management Log helps you acquire additional information about your devices, including logs on new device register requests, device status changes, deleted devices, and mail notifications.

8

NetExtender Configuration

This section provides information and configuration tasks specific to the NetExtender pages on the Secure Mobile Access web-based management interface.

NetExtender is an Secure Mobile Access client for Windows, Mac, Linux, or Android smart phone 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 three ways: Using **NetExtender** on the Secure Mobile Access user portal, using the Microsoft Installer (MSI), or by using the NetExtender standalone client that is installed by clicking one of the **NetExtender Clients** in the Secure Mobile Access 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, by path name or from the shortcut bar on Linux systems, and with the icon on Android smart phones.

The SMA/SRA appliance supports client certificates in both the standalone Windows NetExtender client and the NetExtender Mobile client.

On Windows systems, NetExtender supports establishing a VPN session before logging in to Windows. NetExtender supports IPv6 client connections from Windows systems running Vista or newer, and from Linux clients. An IPv6 address pool for NetExtender is optional, while an IPv4 address pool is necessary.

For more information on NetExtender concepts, see NetExtender Overview on page 41. For information about using or installing the NetExtender, NetExtender Mobile, or NetExtender Android clients, see the latest *Secure Mobile Access User Guide*, available on the Secure Mobile Access pages of the SonicWall Inc. Support Web site at: SMA Documentation.

Topics:

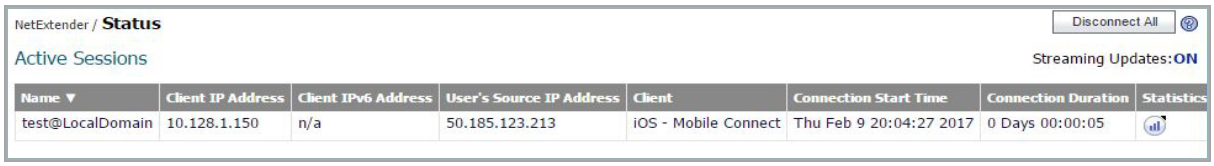
NetExtender > Status

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.

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. The following the NetExtender Status table provides a description of the status items.

NetExtender Status

Status Item	Description
Name	The user name.
NetExtender Client IP Address	The IP address assigned by NetExtender to the client machine.
User's Source IP Address	The IP address of the workstation which the user is logged into.
Location	The geographical location of the source IP for each session.
Connection Start Time	The time when the user first established connection with the SMA/SRA appliance expressed as day, date, and time (HH:MM:SS).
Connection Duration	The amount of time since the user first established connection with the SMA/SRA appliance expressed as number of days and hours, minutes, and seconds (HH:MM:SS).
Statistics	Displays a tooltip showing the outbound, inbound, and total number of packets and bytes transferred during the session, and the current, maximum, and average throughput.
Disconnect	Provides the administrator the ability to disconnect a NetExtender session.

NetExtender > Client Settings

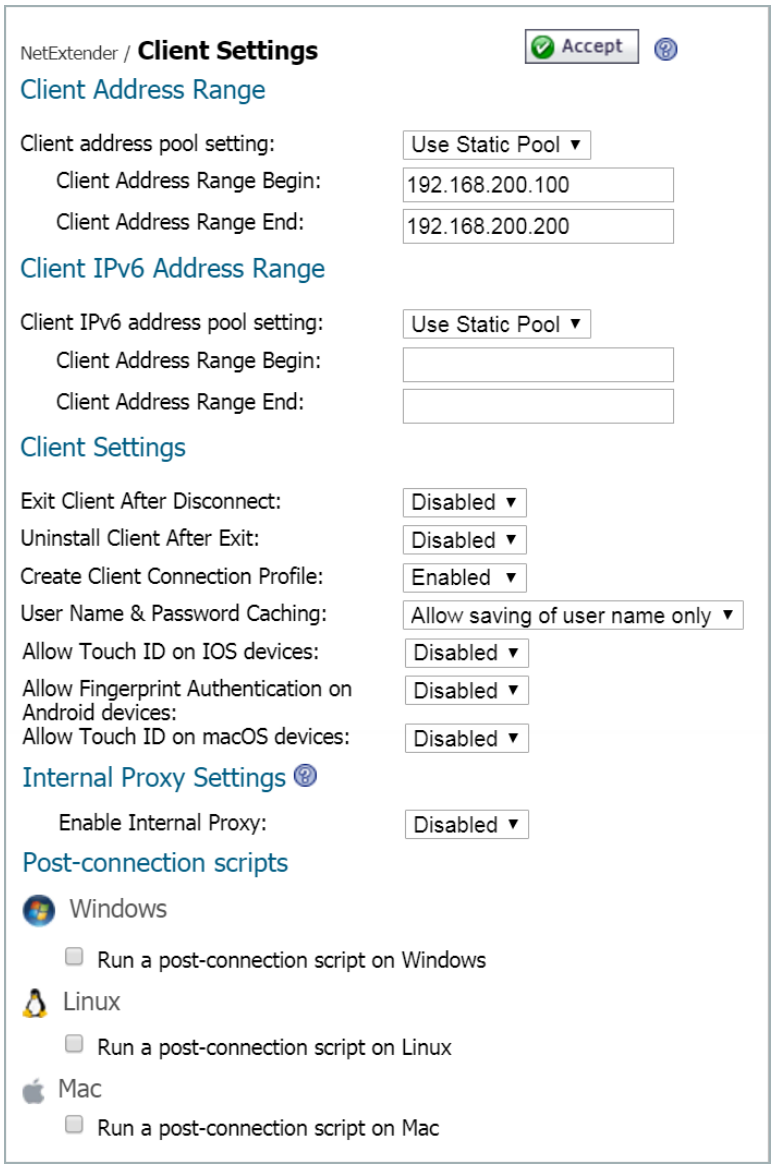
This section provides an overview of the **NetExtender > Client Settings** page and a description of the configuration tasks available on this page.

- NetExtender > Client Settings Overview on page 244
- Configuring the Global NetExtender IP Address Range on page 244
- Configuring Global NetExtender Settings on page 245

NetExtender > Client Settings Overview

The **NetExtender > Client Settings** page allows the administrator to specify the client address range.

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 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 is 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 SMA/SRA appliance is connected, and in cases where there are other hosts on the same segment as the SMA/SRA appliance, it must not overlap or collide with any assigned addresses. You can determine the correct subnet in one of the following ways:

- You can 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 using a Static IP:

1. Navigate to the **NetExtender** > **Client Settings** page.
2. Under **NetExtender Client Address Range**, select **Use Static Pool** from the drop-down list.
3. Supply a beginning client IPv4 address in the **Client Address Range Begin** field.
4. Supply an ending client IPv4 address in the **Client Address Range End** field.
5. Under **NetExtender Client IPv6 Address Range**, optionally select **Use Static Pool** from the drop-down list.
6. Supply a beginning client IPv6 address in the **Client Address Range Begin** field.
7. If using IPv6, supply an ending client IPv6 address in the **Client Address Range End** field.
8. Click **Accept**.
9. The **Status** message displays **Update Successful. Restart for current clients to obtain new addresses.**

To specify your global NetExtender address range using a DHCP:

1. Navigate to the **NetExtender** > **Client Settings** page.
2. Under **NetExtender Client Address Range**, select **Use DHCP** from the drop-down list.
3. Under **Select Interface**, use the drop-down list to select the interface to use for DHCP.
4. Supply the **DHCP Server** in the field provided.
5. Under **NetExtender Client IPv6 Address Range**, optionally select **Use DHCP** from the drop-down list.
6. Under **Select Interface**, use the drop-down list to select the interface to use for DHCPv6.
7. Supply the **DHCPv6 Server** in the field provided.
8. Click **Accept**.
9. The **Status** message displays **Update Successful. Restart for current clients to obtain new addresses.**

Configuring Global NetExtender Settings

The SMA/SRA appliance provides several settings to customize the behavior of NetExtender when users connect and disconnect.

To configure global NetExtender client settings, complete the following steps:

1. Navigate to the **NetExtender** > **Client Settings** page.

   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 SMA/SRA server. To reconnect, users have to either return to the Secure Mobile Access portal or launch NetExtender from their Programs menu. This option applies to all supported platforms except Android smart phones.
- **Uninstall Client After Exit** - The NetExtender client automatically uninstalls when the user exits the client user interface. This occurs when the user right-clicks the NetExtender tray icon and selects Exit. To reconnect, users have to return to the Secure Mobile Access portal and select NetExtender to reinstall it. This option only applies to Windows clients. It does not apply to Android, Mac, or Linux clients.
- **Create Client Connection Profile** - The NetExtender client creates a connection profile recording the SMA Server name, the Domain name and optionally the username and password.

2 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.

3 In the **Allow client to use Touch ID on IOS devices**, the control only blocks future attempts to log in with fingerprint technology on IOS devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.

4 In the **Allow client to use Fingerprint Authentication on Android devices**, the control only blocks future attempts to log in with fingerprint technology on Android devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.

5 In the **Allow client to use Touch ID on macOS devices**, the control only blocks future attempts to log in with fingerprint technology on macOS devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.

6 Click **Accept**.

Configuring Internal Proxy Settings

NetExtender supports the provisioning of connections so that all user traffic is routed through a designated internal proxy server. After enabling the Internal Proxy feature, users are able to specify which Proxy server to use. After NetExtender connects to the SMA/SRA appliance, the internal proxy settings are pushed to the client and used as proxy settings for the NetExtender virtual adapter.

To configure Internal Proxy settings:

1 Navigate to the **NetExtender** > **Client Settings** page.

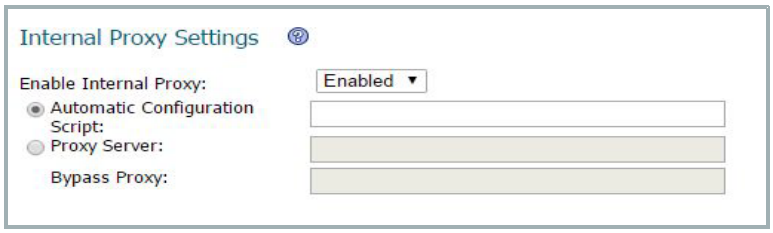
2 Under **Internal Proxy Settings**, select **Enabled** for Enable Internal Proxy.

3 Select one of the following for the Internal Proxy Server:

- **Automatic Configuration Script—**Select this option to set the script to auto configure the proxy.
- **Proxy Server**—Manually set the proxy server.
- **Bypass Proxy**—Set the host that is bypassed to the proxy server.

4 Click **Accept** to save all changes.

NetExtender > Client Settings > Internal Proxy Settings

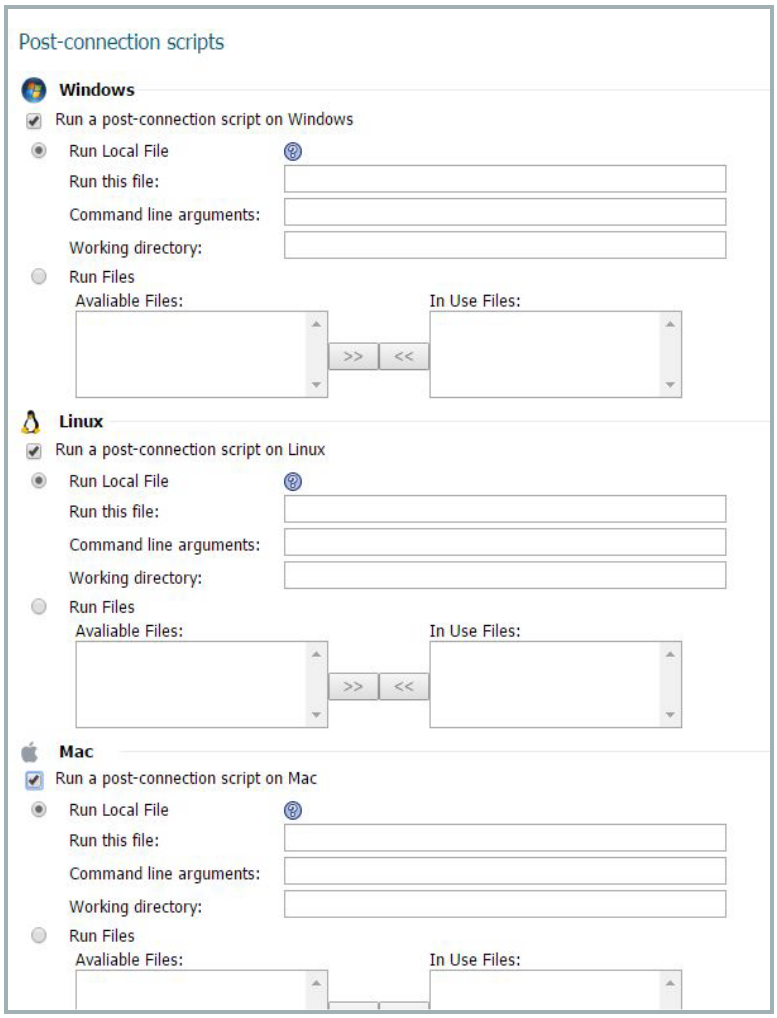


Configuring Post-Connection Scripts

To run post-connection scripts for a Windows, Linux, or Mac system:

1. Navigate to the **NetExtender** > **Client Settings** page.
2. Under **Post-Connection Scripts**, find the operating system you want to run post-connection scripts to. Then, select **Run a post-connection script** for that operating system.
3. Select **Run Local File** if you have the post-connection script(s) available on your local client machine. Select the **Run Files** for the radio button if you have post-connection script(s) uploaded to the server.
4. For local files, set the script path on the **Run this file** field.
5. For local files, set the **Command line arguments**.
6. For local files, set the directory in the **Working directory** field.
7. For remote files, you can select the **Available Files** to move into the **In Use Files** boxes, and vice versa. The script files in the In Use Files box runs after the client is connected.
8. Click **Accept** to save settings.

NetExtender > Client Settings > Post-Connection Scripts



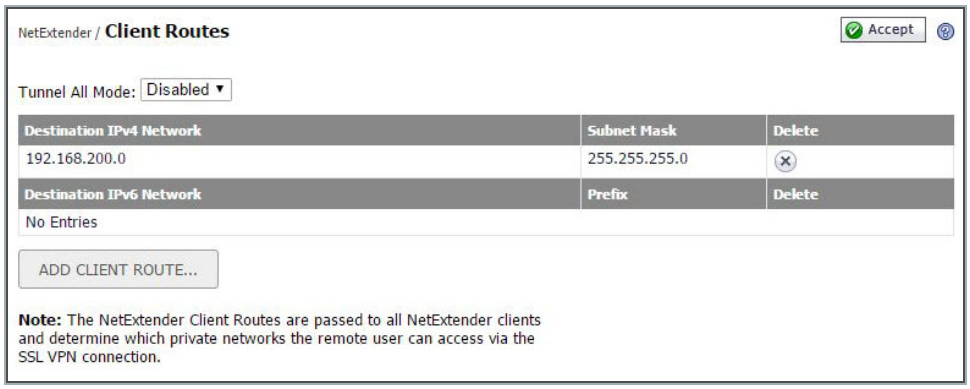
NetExtender > Client Routes

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.

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 by way of the Secure Mobile Access connection.

Group-level NetExtender routes should be assigned from both primary and additional groups if the user-level option to **Add Group NetExtender Client Routes** is enabled. User-level **Routes** must always be pushed to the NX client, and global routes must still depend on the **Add Global NetExtender Client Routes** option as they did before. IPv4 and IPv6 routes both follow these rules.

NOTE: With group access policies, all traffic is allowed by default. This is the opposite of the default behavior of SonicWall Inc. Unified Threat Management (UTM) appliances, where all inbound traffic is denied by default. If you do not create policies for your SMA/SRA appliance, then all NetExtender users might be able to access all resources on your internal network(s).

Additional allow and deny policies can be created by destination address or address range and by service type.

NOTE: The most specific policy takes precedence over less specific policies. For example, a policy that applies to only one IP address has 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) takes 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 takes precedence over a group policy that denies access to a single IP address.

To add NetExtender client routes:

1. Navigate to the **NetExtender** > **Client Routes** page.
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 Secure Mobile Access NetExtender tunnel.
3. Click **Add Client Route**. The **Add Client Route** dialog box displays.
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.

   You can enter an IPv6 route in the **Destination Network** field, in the form 2007::1:2:3:0.
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.
6. Click **Accept**.
7. Repeat this procedure for all necessary routes.

NetExtender > Advanced Settings

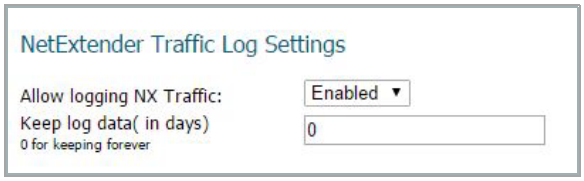
The **NetExtender > Advanced Settings** page allows you to set traffic log settings and upload post connection script files.

Topics:

- NetExtender Traffic Log on page 250
- Post Connection Script Files on page 250

NetExtender Traffic Log

Traffic logging allows you log traffic information over the NetExtender tunnel by enabling the **Allow logging Nx Traffic**. You can configure how many days to keep the log data, where expired data is automatically removed. Leave the value as 0 to keep log data forever. View the log data in the **NetExtender > Log** page.

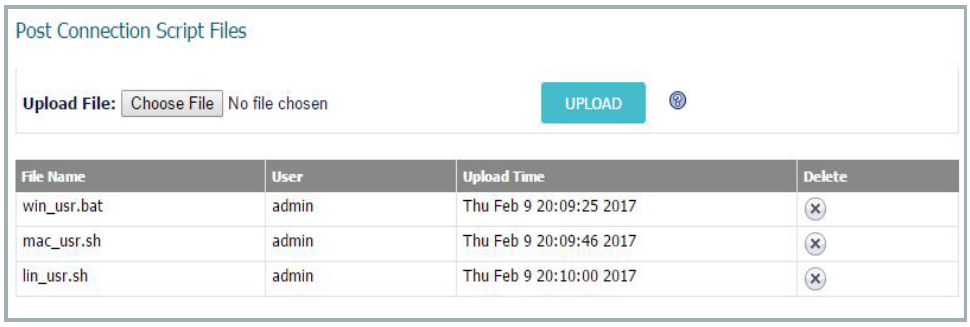


Post Connection Script Files

Administrators are now able to upload or delete post connection script files for NetExtender. Navigate to the **NetExtender > Advanced Settings** page and scroll down to the Post Connection Script Files section.

Click **Choose File** to upload a file from your local system. Then, click **Upload**. After uploaded, the file displays in a list.

To delete a script file, locate the file you want to delete, and click the '**X**' delete icon.



NetExtender > Client Downloads

The **NetExtender > Client Downloads** page allows you to download available NetExtender and Mobile Connect clients for your appliances and/or mobile devices. Simply click the link of the file extension to begin downloading to your local system.

NOTE: Clients require a download from software.sonicwall.com. If the clients are not available, the page will state (not available) where the download link should be. Make sure your appliance can access software.sonicwall.com and that it is properly registered through **System > Licenses**.

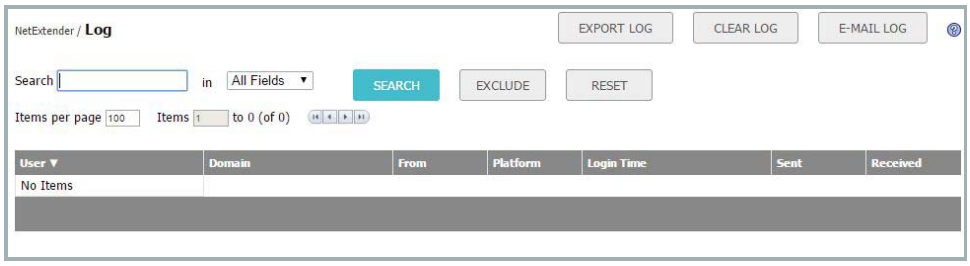
The following systems/mobile devices are supported:

- Windows
- Mac OS X
- Linux 32-bit
- Linux 64-bit
- Android
- Apple iOS

NetExtender > Log

The **NetExtender > Log** page allows you to view and search for data logs. If you enabled logging NetExtender traffic on the **NetExtender > Advanced Settings** page, you are able to view the data logs on this page.

The following options are available:



- **Search**—Enter a value you want to search for in the Logs, then click **Search**. Optionally, you can select a specific field in the drop-down list to narrow your search:
  - All Fields
  - User
  - Domain
  - From
  - Platform
  - Login Time
  - Sent
  - Received
- **Exclude**—Excludes the value you has specified in the search.
- **Reset**—Clears the search field as well as any search results.
- **Export Log**—Click this button to export the current log to your local system.
- **Clear Log**—Allows you to clear the current log entries.
- **E-Mail Log**—Allows you to email the current log to the email address you specify when prompted.

You can view the logs as a Summary Log or a Detailed Log. The Summary Log allows your to see traffic information based on the NetExtender session. The Detailed Log allows you to view traffic information based on the User.

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 on page 252
- Configuring Group-Level NetExtender Settings on page 256

Configuring User-Level NetExtender Settings

All of the global settings for NetExtender (IP address ranges, DNS settings, 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

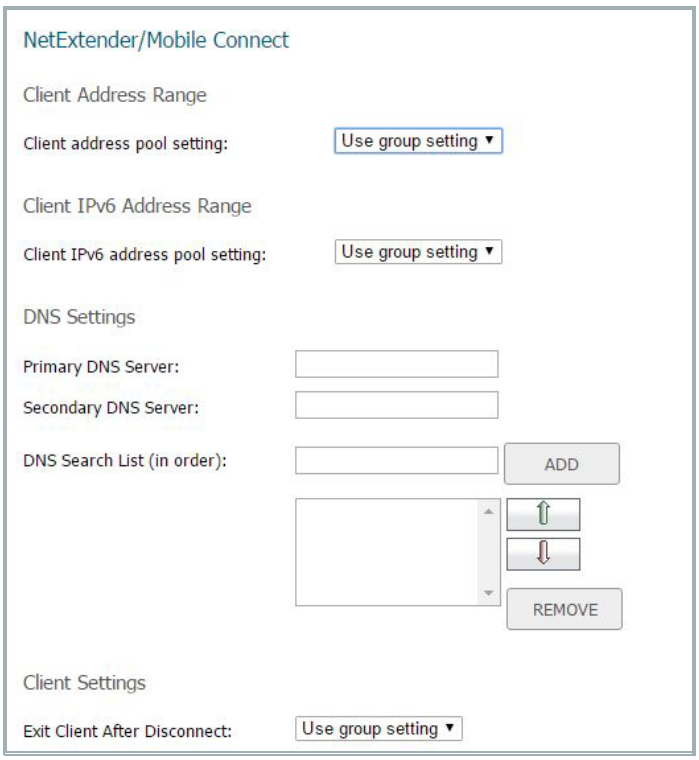
rules to govern access. This user segmentation allows for granular control of access to the network—allowing users access to necessary resources while restricting access to sensitive resources to only those who require it.

To configure custom settings for individual users:

1 Navigate to the **Users > Local Users** page.

2 Click on the configure icon for the user you want to edit. The **Edit User** window is launched.

3 Go to the **NetExtender/Mobile Connect** section.



See also:

- Configuring User Client IP Address Range on page 253
- Configuring User DNS Settings on page 254
- Configuring User NetExtender Settings on page 254
- Configuring User NetExtender Routes on page 255

Configuring User Client IP Address Range

To configure a user client IP address range:

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.

2 To give this user the same IP address every time the user connects, enter the IP address in both fields.

3 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.

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 is using the same username that is not recommended, there is no need to configure more than one IP address for the user client IP address range.

4 Click **Accept**.

Configuring User DNS Settings

To configure custom NetExtender DNS settings for a user:

1 In the **Primary DNS Server** field, type in the IP address of the main DNS server.

2 In the **Secondary DNS Server** field, optionally type the IP address of the backup DNS server.

3 In the **DNS Domain** field, type the domain for the DNS servers.

4 Click **Accept**.

Configuring User NetExtender Settings

The following NetExtender settings can be configured for the user:

- **Exit Client After Disconnect** - The NetExtender client exits when it becomes disconnected from the SMA/SRA server. To reconnect, users should either return to the Secure Mobile Access portal and click NetExtender or launch NetExtender from their Programs menu.
- **Uninstall Client After Exit** - The NetExtender client automatically uninstalls when it terminates or when the user selects Exit (as opposed to simply disconnecting). To reconnect, users should return to the Secure Mobile Access portal and click NetExtender. This option only applies to Windows clients. It does not apply to Android, Mac, or Linux clients.
- **Create Client Connection Profile** - The NetExtender client creates a connection profile recording the SMA/SRA 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.
- In the **Allow client to use Touch ID on IOS devices**, the control only blocks future attempts to log in with fingerprint technology on IOS devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.
- In the **Allow client to use Fingerprint Authentication on Android devices**, the control only blocks future attempts to log in with fingerprint technology on Android devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.

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 previous options.

Configuring User NetExtender Routes

To configure user NetExtender routes:

1 Go to the **Client Routes** section.

2 Click **Add Client Route**.

3 Type the IPv4 or IPv6 address of the trusted network to which you would like to provide access with NetExtender in the **Destination Network** field.

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.

5 Click **Accept**.

6 Repeat steps 1 through 5 for all necessary routes.

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 Secure Mobile Access NetExtender tunnel.

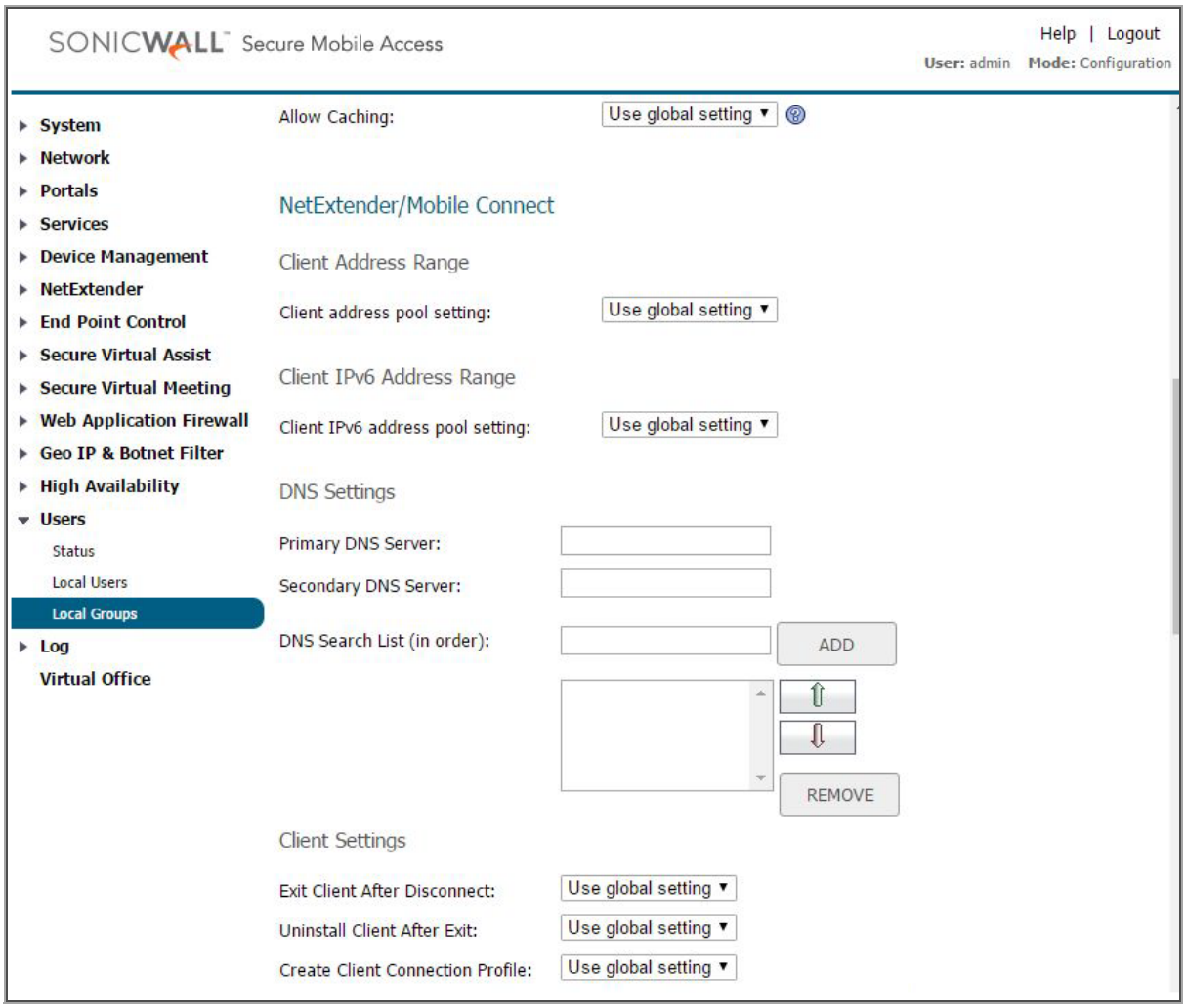
8 To also add the global NetExtender client routes (which are configured on **NetExtender** > **Client Routes** page) to the user, select **Add Global NetExtender Client Routes**.

9 To also add the group NetExtender client routes for the group the user belongs to, select **Add Group NetExtender Client Routes**. Group NetExtender routes are configured on the **NetExtender/Mobile Connect** page of the **Edit Group** window that is accessed through the **Users > Local Groups** page.

10 Click **Accept**.

NOTE: When using an external authentication server, local user names are not typically configured on the SMA/SRA 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:

1 Navigate to the **Users > Local Groups** page.

2 Click on the configure icon for the group you want to edit. The **Edit Group Settings** window is launched.

3 Click the **NetExtender/Mobile Connect** page.

See also:

- Configuring Group Client IP Address Range on page 257
- Configuring Group DNS Settings on page 257
- Configuring Group Client Settings on page 257
- Configuring Group NetExtender Routes on page 258

Configuring Group Client IP Address Range

To configure group-level NetExtender address ranges:

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.
2. 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.
3. Click **Accept**.

Configuring Group DNS Settings

To configure custom NetExtender DNS settings for a group:

1. In the **Primary DNS Server** field, type in the IP address of the main DNS server.
2. In the **Secondary DNS Server** field, optionally type the IP address of the backup DNS server.
3. In the **DNS Domain** field, type the domain for the DNS servers.
4. Click **Accept**.

Configuring Group Client Settings

The following Client settings can be configured for the group:

- **Exit Client After Disconnect** - The NetExtender client exit when it becomes disconnected from the SMA/SRA server. To reconnect, users in the group should either return to the Secure Mobile Access portal and click NetExtender or launch NetExtender from their Programs menu.
- **Uninstall Client After Exit** - The NetExtender client automatically uninstalls when it terminates or when the user selects Exit (as opposed to simply disconnecting). To reconnect, users in the group should return to the Secure Mobile Access portal and click NetExtender. This option only applies to Windows clients. It does not apply to Android, Mac, or Linux clients.
- **Create Client Connection Profile** - The NetExtender client creates a connection profile recording the SMA/SRA 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.
- In the **Allow client to use Touch ID on IOS devices**, the control only blocks future attempts to log in with fingerprint technology on IOS devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.
- In the **Allow client to use Fingerprint Authentication on Android devices**, the control only blocks future attempts to log in with fingerprint technology on Android devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.

To have the user inherent the NetExtender settings from the global NetExtender settings, select **Use Global Settings** for any of the previous options.

Configuring Group NetExtender Routes

To configure NetExtender client routes:

1. To add a NetExtender client route that is only added to this user, click the **Routes** page in the **Edit User Settings** window.
2. To add a NetExtender client route that is only added to users in this group, click **Add Client Route**.
3. Type the IPv4 or IPv6 address of the trusted network to which you would like to provide access with NetExtender in the **Destination Network** field.
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.
5. Click **Accept**. Repeat this procedure for all necessary routes.
6. 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 Secure Mobile Access NetExtender tunnel.
7. To also add the global NetExtender client routes (which are configured on **NetExtender** > **Client Routes** page) to users in this group, select **Add Global NetExtender Client Routes**.
8. Click **Accept**.

9

End Point Control

This section provides information and configuration tasks specific to the **End Point Control** pages on the Secure Mobile Access web-based management interface.

Topics:

Configuring End Point Control

In traditional VPN solutions, accessing your network from an untrusted site like an employee-owned computer or a kiosk at an airport or hotel increases the risk to your network resources. The SMA/SRA appliance provides secure access from any Web-enabled system, including devices in untrusted environments. Secure Mobile Access supports End Point Control (EPC), a default service available on SMA 400/200, SRA 4600/1600, and SMA 500v Virtual Appliance.

EPC verifies that the user's environment is secure before establishing a connection. EPC protects sensitive data and ensures that your network is not compromised when accessed from devices in untrusted environments. EPC also protects the network from threats originating from client devices participating in the SMA/SRA.

EPC is checked when users log in to the web portal from a web browser that blocks any access to the private network from untrusted sites. The EPC portal checking process uses the browser plug-ins on your system.

EPC is supported on iOS and Android mobile devices using Mobile Connect, allowing device profiles to be created for these mobile devices. This provides security protection from threats against client devices and protection to the SMA/SRA appliance from threats originating from client devices participating in the SSL VPN. For more information on Mobile Connect, refer to the *Mobile Connect User Guides*.

Secure Mobile Access provides these end point security controls by completing host integrity checking and security protection mechanisms before a tunnel session is begun. Host integrity checks help ensure that the client system is in compliance with your organization's security policy. SonicWall Inc. end point security controls are tightly integrated with access control to analyze the client system and apply access controls based on the results.

EPC supports the Windows, Linux, and Mac NetExtender client. It also supports Mobile Connect for iOS, Android, OSX, Windows Phone, and Windows Next. For Web Portal login, EPC is supported only on Windows

platforms. EPC enhancements are supported on the SonicWall Inc. SMA 400/200, SRA 4600/1600, and SMA 500v Virtual Appliance platforms.

NOTE: When the EPC feature is active other features might run slower because of the increased traffic.

To configure EPC:

1. Image the appliance with the latest Secure Mobile Access firmware, as explained in the Getting Started Guide for your appliance.
2. Configure Device Profiles that allow or deny user authentication based on various global, group, or user attributes. See End Point Control > Device Profiles on page 260.
3. Add and configure groups and users to allow or deny End Point Control profiles. See End Point Control > Status on page 266.
4. Configure users to inherit their group profiles. See Users > Local Groups > Edit EPC Settings on page 261.
5. Enable End Point Control. See End Point Control > Status on page 266.
6. Connect to NetExtender and monitor the End Point Control log. See End Point Control > Log on page 267.

End Point Control > Device Profiles

Create device profiles to configure authentication guidelines for users or groups of users based on various global, group, or user attributes. For example, you can select groups that use an Antivirus program or users with a specific Windows version.

Two kinds of profiles are available: **Allow** profiles and **Deny** profiles. **Allow** profiles identify attributes of the client's network that must be present before a user is authenticated, and **Deny** profiles identify attributes of the network that *cannot* be present. If multiple profiles are defined for a group or user, connection to the SMA/SRA appliance is granted only when a client's environment fulfills all **Allow** profiles for the group or user and does not fulfill any **Deny** profiles.

Use the **End Point Control > Device Profiles** page to manage device profiles.

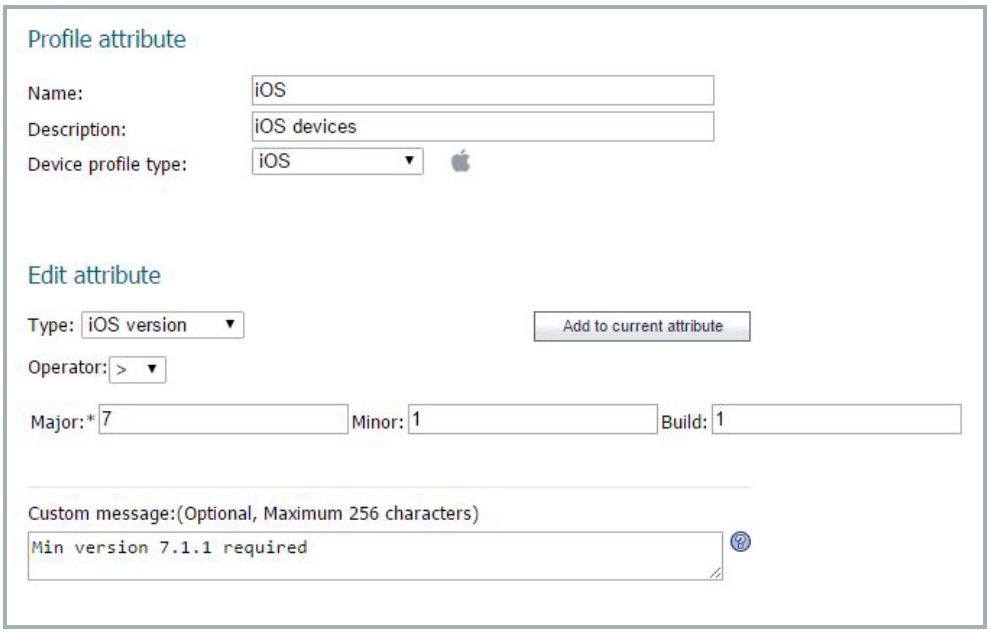
End Point Control > Device Profiles

The **End Point Control > Device Profiles** page lists all device profiles and identifies the platform where the profile can be used. This page also contains buttons that allow you to add, edit, or delete profiles. Hover the mouse over an icon or button to identify it.

To create a device profile:

1. On the **End Point Control > Device Profiles** page, click **Add Device Profile**.

The Add Device Profile page is displayed.



2 In the **Name** field, type the name that is used to identify the profile.

3 In the **Description** field, optionally type a brief description of the profile that helps identify the profile.

4 Select whether the profile is being created for **Windows**, **Mac**, **Linux**, **iOS**, or **Windows Phone** clients.

5 Use the **Type** drop-down list to select the attribute used to select users. The remaining fields on this page vary based on your selection.

6 Click **Add to current attribute**.

7 Repeat 5 and 6 for each attribute that should be included in the profile.

8 You can optionally enter a custom message that shows the user the EPC check has failed. The Administrator could enter text to indicate how to fix the issue or the reason the policy failed.

9 To complete the profile, click **Accept** at the upper right of the page.

Users > Local Groups > Edit EPC Settings

After creating device profiles, assign them to the local groups that uses them to authenticate users. Device profiles can be **Allow** profiles and **Deny** profiles. **Allow** profiles identify attributes of the client's network that must be present before a user is authenticated, and **Deny** profiles identify attributes of the network that *cannot* be present. If multiple profiles are defined for a group, connection to the SMA/SRA appliance is granted only when a client's environment fulfills all **Allow** profiles for the group and does not fulfill any **Deny** profiles. Use the **EPC** page on the **Users > Local Groups > Edit** page to assign device profiles to a group.

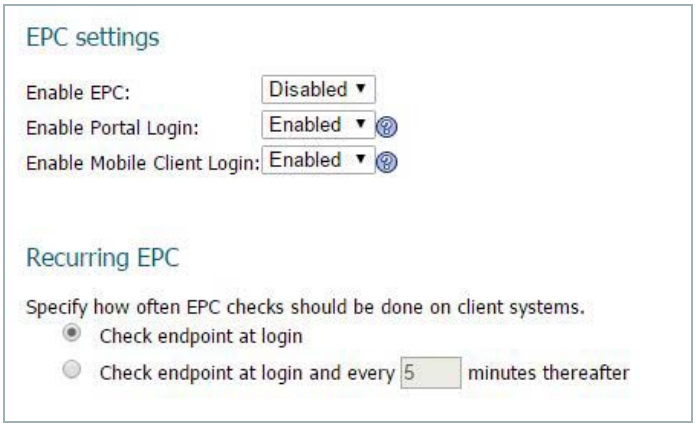
NetExtender login can be disabled on platforms where EPC is enabled.

EPC portal checking uses the NetExtender browser plug-in. EPC is checked when users log in to the web portal from a web browser that blocks any access to the private network from untrusted sites.

To configure device profiles to be used when authenticating users in a local group:

1 Navigate to the **Users > Local Groups** page and click **Edit** for the Global group or a local group to be configured for EPC.

2 When the Edit Local Group page appears, go to the EPC settings section. Use the **EPC** page to enable or disable EPC for the group, select how to handle authentication requests from unsupported clients, and to add or remove device profiles.



3 In the **Enable EPC** field, select **Enabled** to enable EPC for the group, **Disabled** to disable EPC for the group, or **Use global setting** to either enable or disable EPC based on whether EPC is enabled on the **Users > Local Users > Edit Global Policies** or **Users > Local Groups > Edit Global Policies** page.

4 In the **Enable Portal Login** field, set the default action to **Enabled** to allow or **Disabled** to block logins from these portals when EPC is enabled.

5 EPC is supported for iOS and Android mobile clients. In the **Enable Mobile Client Login** field, set the default action to **Enabled** to allow or **Disabled** to block logins from these clients when EPC is enabled.

6 Fields in the **Recurring EPC** section vary, depending on whether you are configuring EPC for the Global group or a local group. To configure EPC for the Global group, select **Check endpoint at login** to do EPC checks only when users login, or select **Check endpoint at login and every *x* minutes thereafter** to also do EPC checks at set intervals. For example, to do EPC checks whenever a user logs in and every *x* minutes thereafter while the user is logged in, select **Check endpoint at login and every *x* minutes thereafter** and type the number of minutes to wait between EPC checks.

   OR

   To configure EPC for a local group, select **Use global setting** or **Custom Setting** from the **Recurring EPC** drop-down list. If you select **Use global setting**, the local group inherits the EPC settings from the Global group. If you select **Custom Setting**, the **Check endpoint at login** and **Check endpoint at login and every *x* minutes thereafter** prompts are displayed and you can configure EPC, as explained for the Global group.

7 Either select **Inherit global device profiles** to use all defined Allow and Deny device profiles for the group.

   OR

   Add or remove profiles using the Edit EPC page:

   a To add or remove an **Allow** profile for the group, click **Add Allow Profiles**.

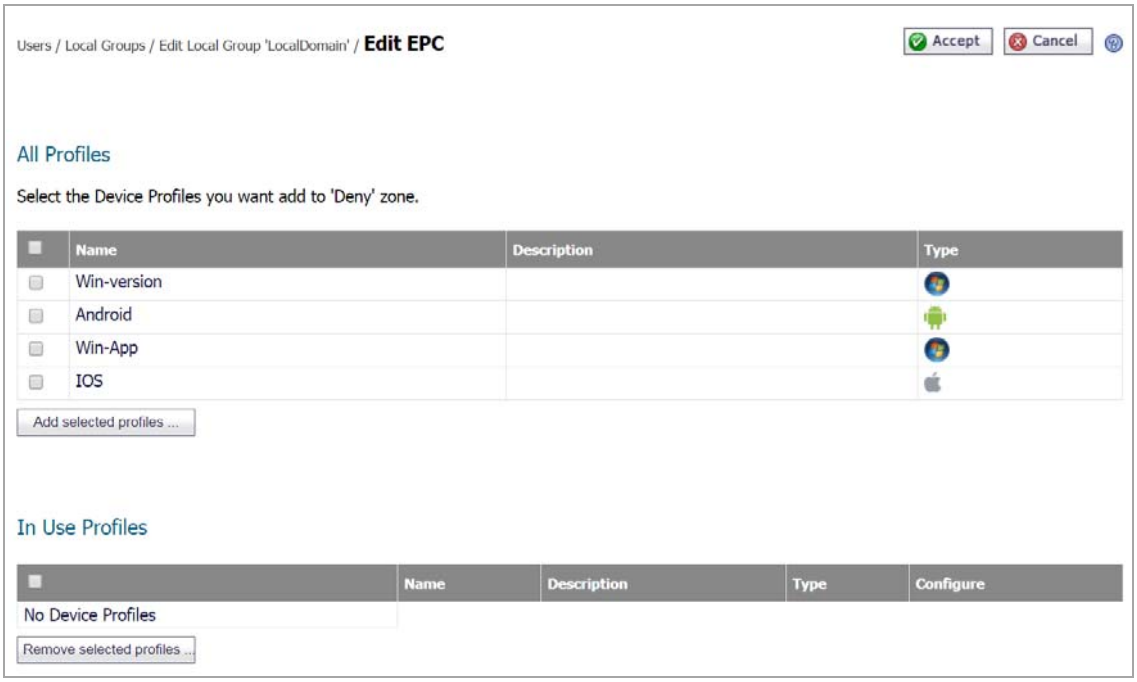
   b In the Edit EPC page, select the profiles from the **All Profiles** list that you want to add to the group and click **Add selected profiles**. Selected profiles are then moved to the **In Use Profiles** list on the page that lists all device profiles that are used for the group.

   c To disable a profile without deleting it, clear **Enabled** next to the profile. To enable a profile, select **Enabled**. This allows you to selectively enable or disable a profile that is used periodically.

   d To remove an Allow profile from the group, select the profile from the **In Use Profile**s list and click **Remove selected profiles**.

e To add or remove a Deny profile for the group, click **Add Deny Profiles** and follow the preceding steps b and d.

8 Click **Accept** to save your changes.



Users > Local Users > Edit EPC Settings

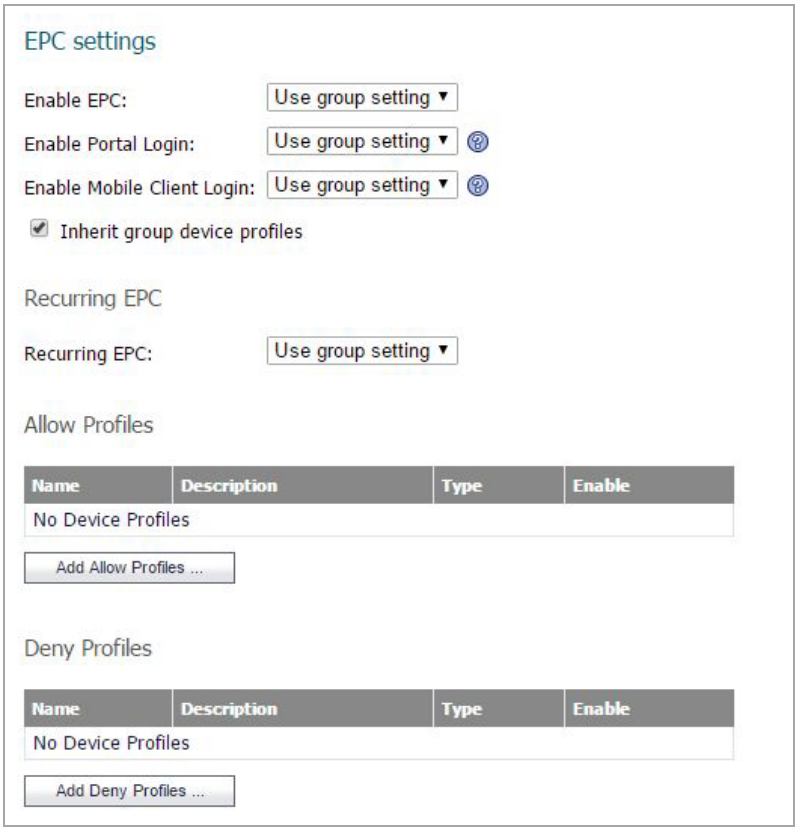
After creating device profiles, assign them to the local users. Device profiles can be **Allow** profiles and **Deny** profiles. **Allow** profiles identify attributes of the client's network that must be present before a user is authenticated, and **Deny** profiles identify attributes of the network that *cannot* be present. If multiple profiles are defined for a user, connection to the SMA/SRA appliance is granted only when a client's environment fulfills all **Allow** profiles for the user and does not fulfill any **Deny** profiles. Use the **EPC** page on the **Users > Local Users > Edit** page to assign device profiles to a user.

NetExtender login can be disabled on platforms where EPC is enabled.

To configure device profiles to be used when authenticating a local user:

1 Navigate to the **Users > Local Users** page and click **Edit** for the user to be configured for EPC.

2 When the Edit Local User page appears, click the **EPC** page. Use the **EPC** page to enable or disable EPC for the user, select how to handle authentication requests from unsupported clients, and to add or remove device profiles.



3 In the **Enable EPC** field, select **Enabled** to enable EPC for the user, **Disabled** to disable EPC for the user, or **Use group setting** to either enable or disable EPC based on whether EPC is enabled on the **End Point Control > Settings** page.

4 In the **Enable Portal Login** field, set the default action to **Enabled** to allow or **Disabled** to block logins when EPC is enabled.

5 EPC is supported for iOS and Android mobile clients. In the **Enable Mobile Client Login** field, set the default action to **Enabled** to allow logins or **Disabled** to block logins from these clients when EPC is enabled. Or set the default action to **Use group setting** to either enable or disable EPC based on whether EPC is enabled on the **End Point Control > Settings** page

6 In the **Recurring EPC** section, configure when EPC checks should be conducted. Select **Check endpoint at login** to do EPC checks only when users login, or select **Check endpoint at login and every *x* minutes thereafter** to also do EPC checks at set intervals. For example, to do EPC checks whenever a user logs in and every *x* minutes thereafter while the user is logged in, select **Check endpoint at login and every *x* minutes thereafter** and type the number of minutes to wait between EPC checks.

7 Fields in the **Recurring EPC** section vary, depending on whether you are configuring EPC for the Global group or a local user. To configure EPC for the Global group, select **Check endpoint at login** to do EPC checks only when users login, or select **Check endpoint at login and every *x* minutes thereafter** to also do EPC checks at set intervals. For example, to do EPC checks whenever a user logs in and every *x* minutes thereafter while the user is logged in, select **Check endpoint at login and every *x* minutes thereafter** and type the number of minutes to wait between EPC checks.

OR

To configure EPC for a local user, select **Use global setting** or **Custom Setting** from the **Recurring EPC** drop-down list. If you select **Use global setting**, the local user inherits the EPC settings from the Global

group. If you select **Custom Setting**, the **Check endpoint at login** and **Check endpoint at login and every** *x* **minutes thereafter** prompts are displayed and you can configure EPC, as explained for the Global group.

8 Either select **Inherit group device profiles** to use all defined Allow and Deny device profiles for the user.

OR

Add or remove profiles using the **Edit EPC** page:

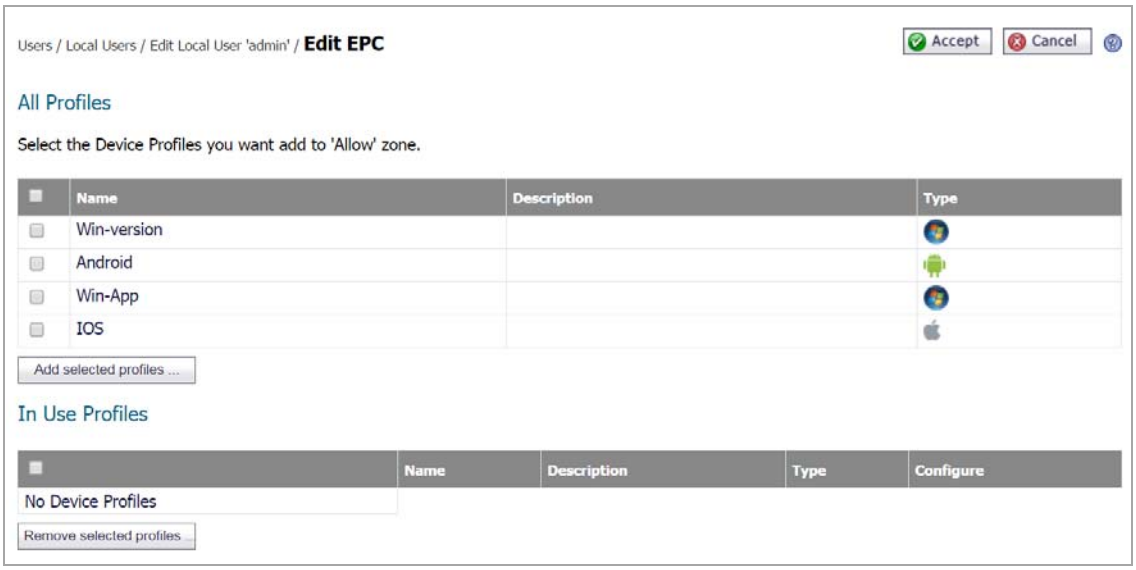
a To add or remove an **Allow** profile for the user, click **Add Allow Profiles**.

b In the Edit EPC page, select the profiles from the **All Profiles** list that you want to add for the user and click **Add selected profiles**. Selected profiles are then moved to the **In Use Profiles** list on the page that lists all device profiles that are used for the user.

c To remove an Allow profile for the user, select the profile from the **In Use Profiles** list and click **Remove selected profiles**.

d To add or remove a Deny profile for the user, click **Add Deny Profiles** and follow the preceding steps b and d.

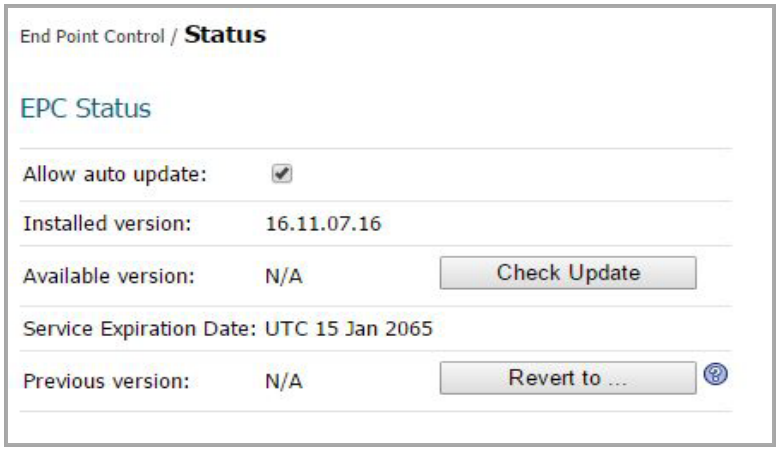
9 Click **Accept** to save your changes.



End Point Control > Status

The **End Point Control > Status** page allows you to configure auto updates, view the current EPC version being used, update the EPC version, and the service expiration date.

End Point Control > Status



1 Select **Allow auto update** to enable the OPSWAT to update automatically.

2 The Installed version displays the current version being used.

3 Click **Check Update** to instantly query if there are any available updates. If there is a new update available, the button changes to **Apply Update**.

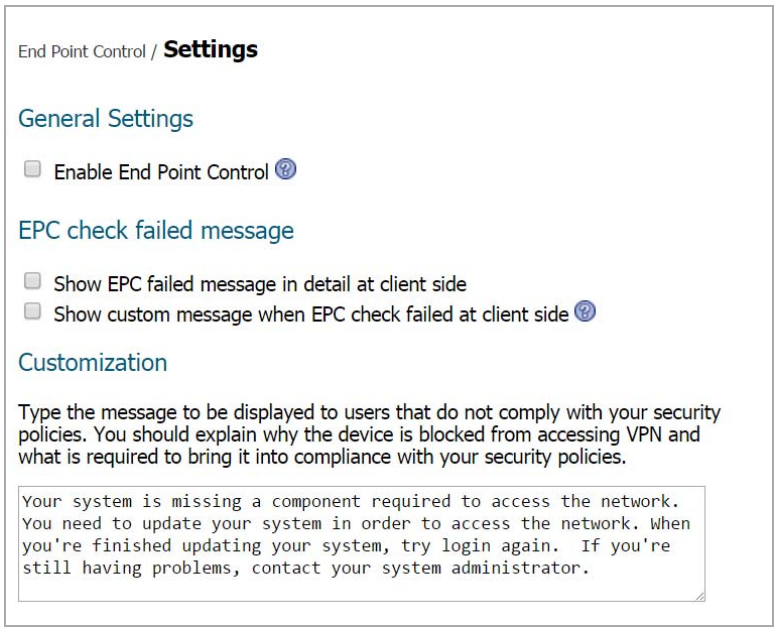
4 The Service Expiration Date displays when the current service expires.

5 Click **Previous Settings** to apply the previous version of the service.

End Point Control > Settings

EPC is globally enabled or disabled on the **End Point Control > Settings** page. When EPC is disabled, it is disabled at the global, group, and user level. The Settings page also is used to customize the message displayed when a NetExtender client login fails EPC security checking.

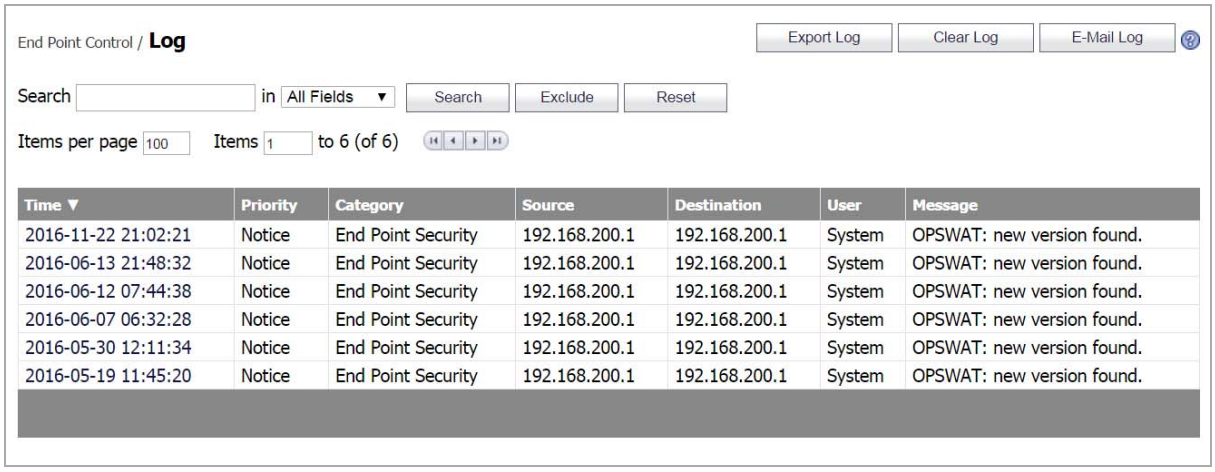
End Point Control > Settings



End Point Control > Log

The **End Point Control > Log** page lists all client logins blocked by EPC. This log can be searched, filtered, e-mailed, and exported.

End Point Control > Log



Time ▼	Priority	Category	Source	Destination	User	Message
2016-11-22 21:02:21	Notice	End Point Security	192.168.200.1	192.168.200.1	System	OPSWAT: new version found.
2016-06-13 21:48:32	Notice	End Point Security	192.168.200.1	192.168.200.1	System	OPSWAT: new version found.
2016-06-12 07:44:38	Notice	End Point Security	192.168.200.1	192.168.200.1	System	OPSWAT: new version found.
2016-06-07 06:32:28	Notice	End Point Security	192.168.200.1	192.168.200.1	System	OPSWAT: new version found.
2016-05-30 12:11:34	Notice	End Point Security	192.168.200.1	192.168.200.1	System	OPSWAT: new version found.
2016-05-19 11:45:20	Notice	End Point Security	192.168.200.1	192.168.200.1	System	OPSWAT: new version found.

Use this page to complete the following functions:

- Click **Export Log** to save a zip file containing the full text of all logged sessions.

- Click **Clear Log** to erase all log messages.
- Click **E-mail Log** to send the log to the e-mail address configured on the **Log > Settings** page.
- Use the **Search** options to filter log messages. Note that the search is case sensitive. In the drop-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 per page. 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.

10

Secure Virtual Assist Configuration

This section provides information and configuration tasks specific to the **Secure Virtual Assist** pages on the Secure Mobile Access web-based management interface.

Secure Virtual Assist is an easy to use tool that allows Secure Mobile Access 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. This feature is now supported on Windows and MacOS.

For more information on Secure Virtual Assist concepts, see Secure Virtual Assist Overview on page 52. You can also view the *Secure Mobile Access Secure Virtual Meeting and Secure Virtual Assist Feature Module* for additional information.

Topics:

Secure Virtual Assist > Status

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

The **Secure 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. For the technician, the page displays the portal, domain, and status.

Virtual Assist > Status

On the right side of the screen, **Streaming Updates** indicates that changes to the status of customers is dynamically updated. Click **ON/OFF** to enable/disable Streaming Updates, respectively.

Click **Logout** 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 Secure Virtual Assist Technician Session on page 55
- Performing Secure Virtual Assist Technician Tasks on page 58

Secure Virtual Assist > Settings

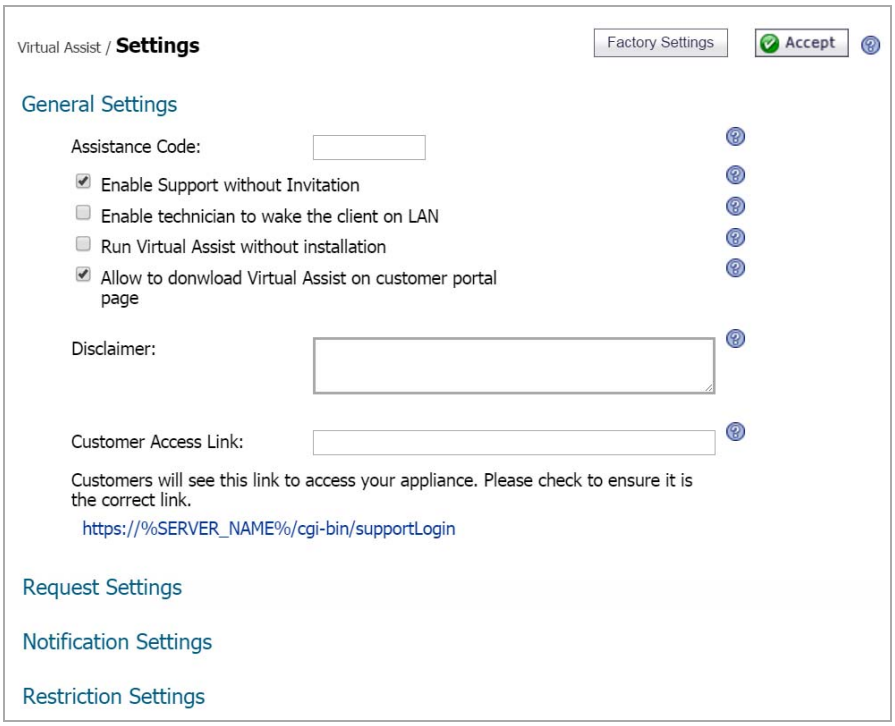
This section describes the **Secure Virtual Assist > Settings** page and the configuration tasks available on this page. The Virtual Assist options are divided into the following pages:

- General Settings on page 271
- Request Settings on page 272
- Notification Settings on page 273
- Restriction Settings on page 275

General Settings

To configure Virtual Assist general settings:

1 Navigate to the **Secure Virtual Assist > Settings** page.



2 To require customers to enter a password before being allowed to access Virtual Assist, enter the password in the **Assistance Code** window.

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.

4 (Optional) Select **Enable technician to make to wake the client on LAN** to wake a client running Virtual Assist on the LAN if both are in the same subnet. The client can be woken when powered off, in the Sleep state, or in the Hibernate state. This feature can be enabled globally, per portal, or from the client.

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

5 (Optional) Select **Run Virtual Assist without installation** to run Virtual Assist from the web without installing it on the local machine. This feature can be enabled globally or per portal.

6 (Optional) Select **Allow to download Virtual Assist on customer portal** if you would like to provide your customers the ability to download the Virtual Assist client.

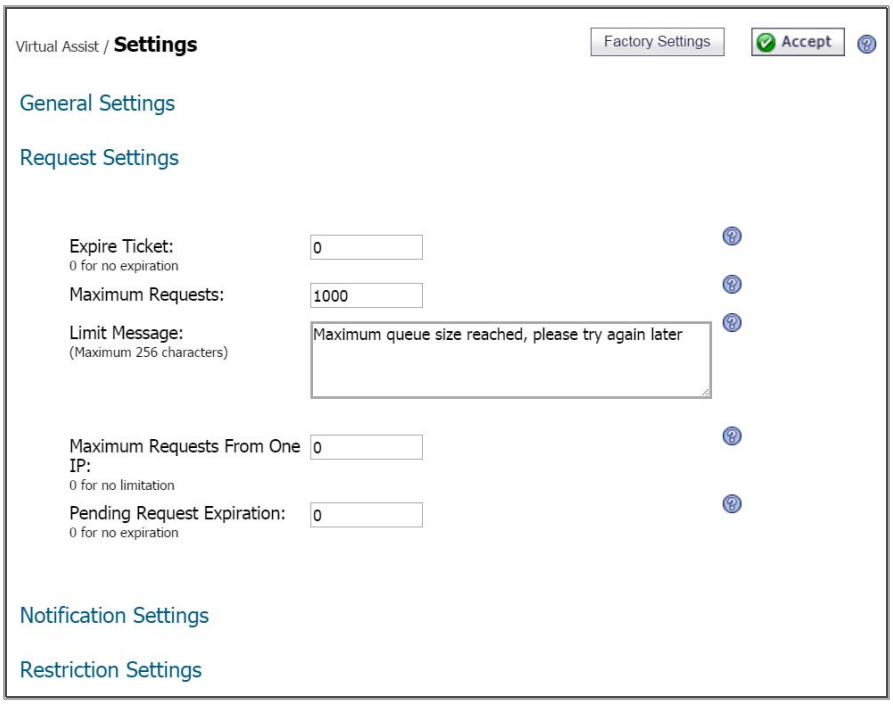
7 (Optional) To present customers with a legal disclaimer, instructions, or any other additional information, enter the text in the **Disclaimer** field. HTML code is allowed in this field. Customers are presented with the disclaimer and required to click “Accept” before beginning a Virtual Assist session.

8 To include a link to Virtual Assist on the portal login page, select **Display Virtual Assist link from Portal Login**. Customers can then click on a link to go directly to the Virtual Assist portal login page without having to log in to the Virtual Office.

Request Settings

To configure Virtual Assist request settings:

1 On the **Secure Virtual Assist > Settings** page, click the **Request Settings** tab at the bottom of the page.



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 have to reinitiate their Virtual Assist request.

3 To limit the number of customers allowed in the Virtual Assist queue, enter a value in the **Maximum Request** field.

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.

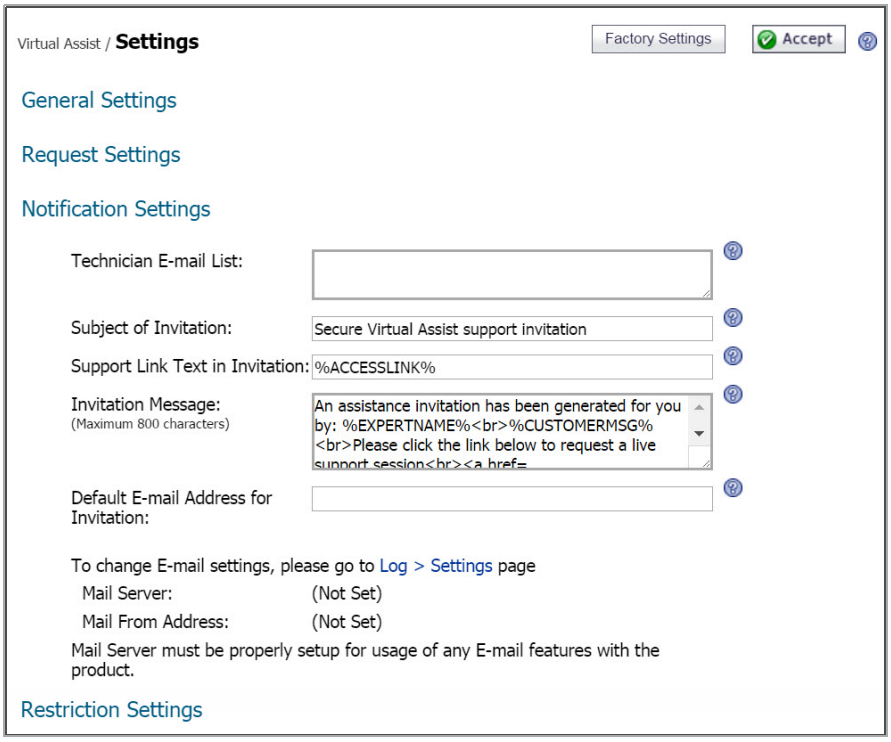
5 Entering a value in the **Maximum requests From One IP** field can be useful if individual customers are repeatedly requesting help. However, this might cause problems for customers using DHCP behind a single IP address. The default **0** does not limit request from individual IP addresses.

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:

1 On the **Secure Virtual Assist > Settings** page, click the **Notification Settings** tab at the bottom of the page.



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).

3 The next three fields allow you to customize the email invitation:

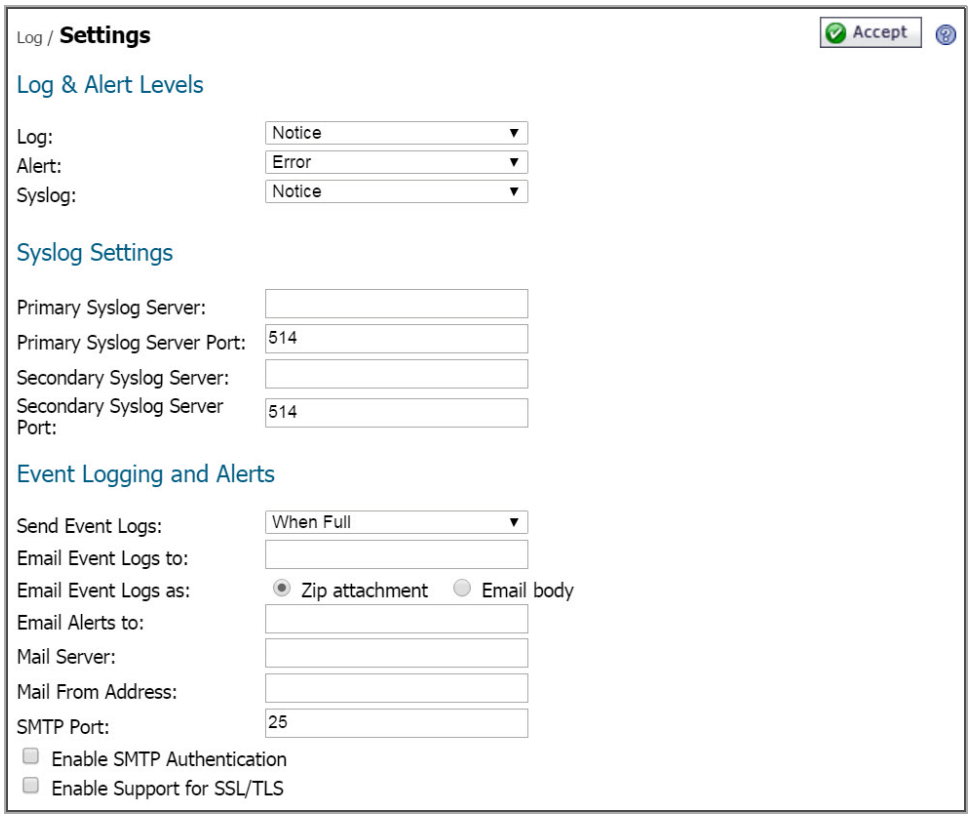
- **Subject of Invitation** - The email subject line.
- **Support Link Text in Invitation** - Text that introduces the link to the URL for accessing Virtual Assist.
- **Invitation Message** - The body of the invitation email message.
- **Default Email Address for Invitation** - The default source email.

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** page.
- %SUPPORTLINK% - The URL for accessing Virtual Assist.
- %ACCESSLINK% - The URL for accessing the Secure Mobile Access Virtual Office.

NOTE: The currently configured mail server and email return address are listed at the bottom of the **Secure 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 also allows blocked email notifications to the technician in deployments where a third-party email filter might block emails sent to the customer without providing an error to the Virtual Assist client.

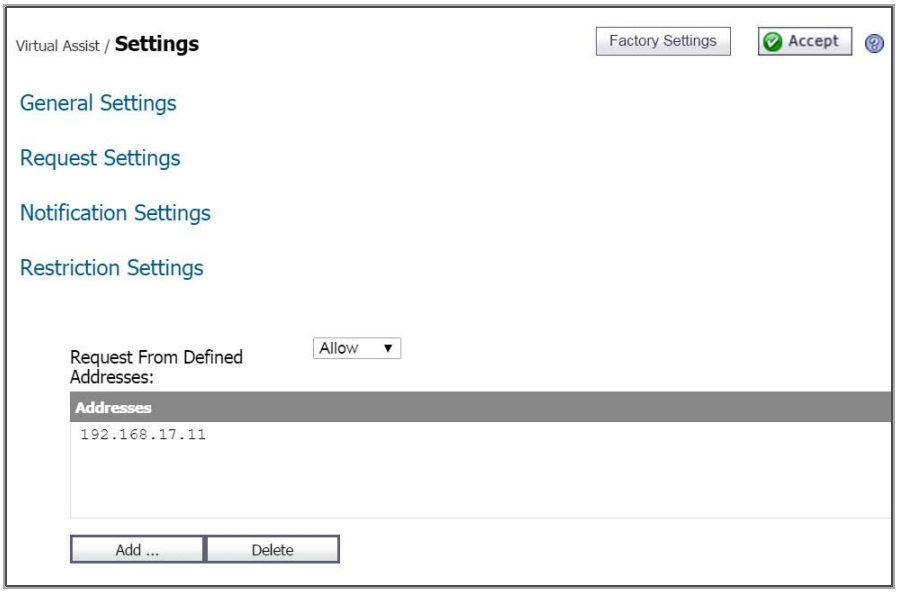
Log > Settings



Restriction Settings

To configure Virtual Assist restriction settings:

1 On the **Secure Virtual Assist > Settings** page, click the **Restriction Settings** tab at the bottom of the page.



2 To deny Virtual Assist requests from specific IP addresses or networks, select **Deny** from the **Request From Defined Addresses** drop-down menu.

3 To allow Virtual Assist requests only from specific IP addresses or networks, select **Allow** from the **Request From Defined Addresses** drop-down menu.

4 To add an IP address or network to the Deny or Allow list, click **Add ...**. The **Admin Addresses** window displays. See Adding an Address to Restriction Settings on page 275.

5 To delete a configured restriction setting, select the desired address in the **Addresses** field and click **Delete**. The address is removed from the field.

Adding an Address to Restriction Settings

To add an IP address or network to the Deny or Allow list for Virtual Assist restriction settings:

1 On the **Secure Virtual Assist > Settings** page, click the **Restriction Settings** tab at the bottom of the page.

2 Click **Add ...**. The **Admin Addresses** window displays.

3 In the **Source Address Type** drop-down menu, select which of the following you want to specify:

- IP Address
- IP Network
- IPv6 Address
- IPv6 Network

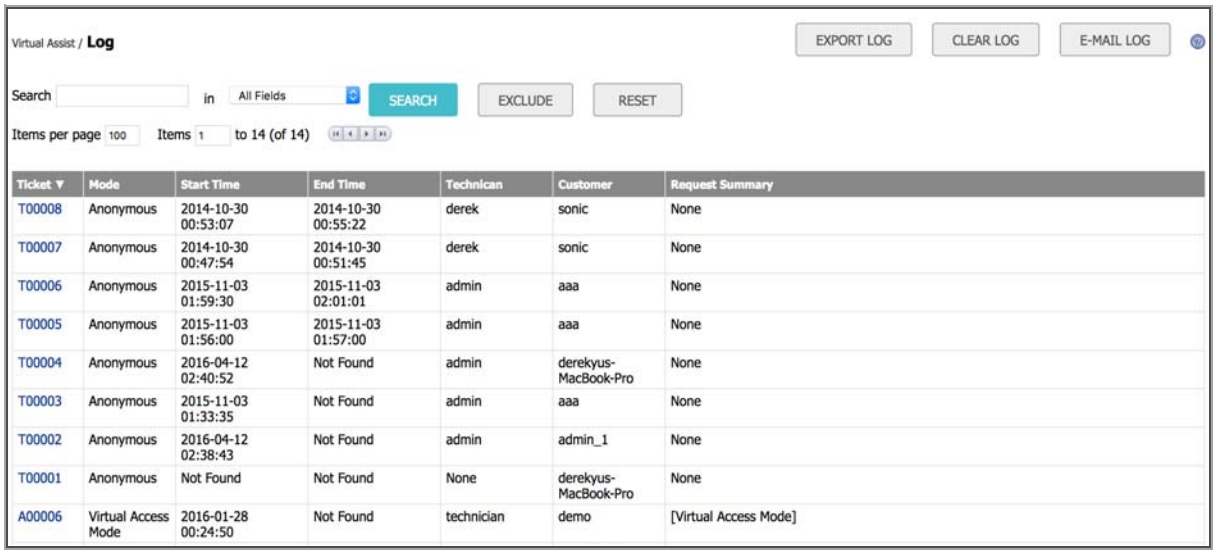
4 Enter the information to define the address or network and click **Accept**.

Secure Virtual Assist > Log

The **Secure 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.

Virtual Assist > Log



Ticket	Mode	Start Time	End Time	Technican	Customer	Request Summary
T00008	Anonymous	2014-10-30 00:53:07	2014-10-30 00:55:22	derek	sonic	None
T00007	Anonymous	2014-10-30 00:47:54	2014-10-30 00:51:45	derek	sonic	None
T00006	Anonymous	2015-11-03 01:59:30	2015-11-03 02:01:01	admin	aaa	None
T00005	Anonymous	2015-11-03 01:56:00	2015-11-03 01:57:00	admin	aaa	None
T00004	Anonymous	2016-04-12 02:40:52	Not Found	admin	derekyus-MacBook-Pro	None
T00003	Anonymous	2015-11-03 01:33:35	Not Found	admin	aaa	None
T00002	Anonymous	2016-04-12 02:38:43	Not Found	admin	admin_1	None
T00001	Anonymous	Not Found	Not Found	None	derekyus-MacBook-Pro	None
A00006	Virtual Access Mode	2016-01-28 00:24:50	Not Found	technician	demo	[Virtual Access Mode]

Click on the **Ticket Number** to view details about a session, or ticket. The **Secure Virtual Assist > Log > <ticket number>** page is displayed. Click **Save Log** to save the information on the page. To return to the **Secure 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 drop-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.

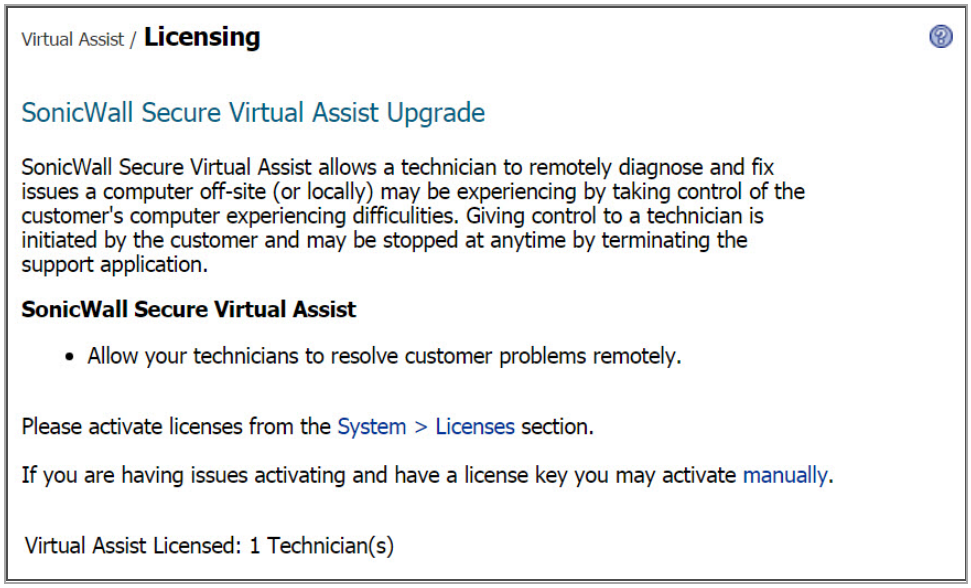
Secure Virtual Assist > Licensing

This section provides an overview of the **Secure Virtual Assist > Licensing** page and a description of the configuration tasks available on this page.

- Secure Virtual Assist > Licensing Overview on page 277
- Enabling Secure Virtual Assist on page 277

Secure Virtual Assist > Licensing Overview

Secure Virtual Assist is a licensed service.



Enabling Secure Virtual Assist

By default, Virtual Assist is enabled on portals that are created after Virtual Assist is licensed. Virtual Assist is disabled by default on all portals that were created before the Secure Virtual Assist license is purchased.

For users, administrator rights are not required for basic screen sharing support. For full installation of the client, admin rights might be necessary, but full installation is not necessary to use the service. Secure Virtual Access or unattended mode requires admin rights.

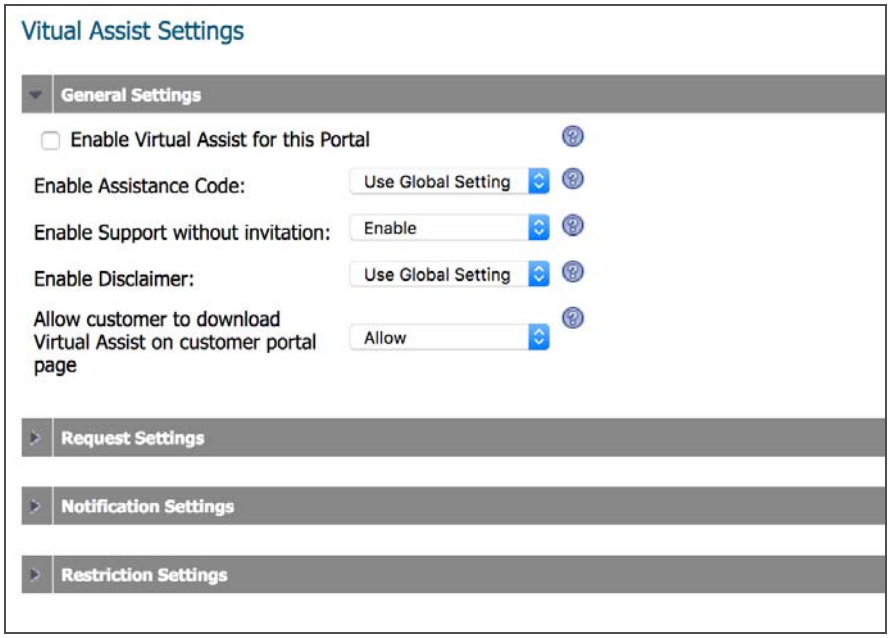
To configure Virtual Assist:

1 To purchase and activate a Secure Virtual Assist license, navigate to **System > Licensing** and click on the link to **Activate, Upgrade, or Renew services.**

For more information, see System > Licenses on page 95.

2 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 **Add Portal**. See Portals > Portals on page 142.

3 In the **Edit Portal** window that displays, click the **Virtual Assist** page.



4 Click on **Enable Virtual Assist for this Portal** and click **Accept**. Virtual Assist is now enabled and ready to use. Secure Mobile Access users now see the Virtual Assist icon on the Virtual Office page.

5 Clear **Display Technician Button** to hide the technician button on the Virtual Office window and require technicians to login directly through the client.

6 Select **Display Request Help Button** to display the help button on the Virtual Office for users to launch Virtual Assist.

7 Select **Enable Virtual Access Mode** to allow Secure Virtual Access connections to be made to this portal. This must be enabled for Virtual Assist to function on this portal.

8 Select **Display Virtual Access Setup Link** to display the Secure Virtual Access Setup link on the Virtual Office.

9 (Optional) Select **Run Virtual Assist without installation** to run Virtual Assist from the web without installing it on the local machine. This feature can be enabled globally or per portal.

10 Use the **Wake customer on LAN** feature to allow Technicians to wake a client running Virtual Assist on the LAN if both are in the same subnet. The client can be woken when powered off, in the Sleep state, or in the Hibernate state. This feature can be enabled globally or per portal.

- Select **Use Global Setting** to apply the global setting to this portal.
- Select **Enable** this feature, no matter what is selected for the global setting.
- Select **Disable** this feature, no matter what is selected for the global setting.

ⓘ **NOTE:** To use Wake Client, this feature must be configured on the client machine, as explained in the *Secure Mobile Access User Guide*.

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

12 Check **Enable Assistance Code** to require a user to enter the designated code before requesting assisting. Checking this check box displays an **Assistance Code** field, where you specify the code users must enter.

13 (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.

14 When **Enable Disclaimer** is enabled, the customer should offer a code when requesting support. If the option is disabled, the code is not necessary.

15 (Optional) Select **Allow to download Virtual Assist on customer portal page** if you would like to provide your customers the ability to download the Virtual Assist client.

16 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. Secure Mobile Access users now see the **Virtual Assist** icon on the Virtual Office page.

11

Secure Virtual Meeting

This section provides information and configuration tasks specific to the **Secure Virtual Meeting** pages on the Secure Mobile Access web-based management interface and a description of the configuration tasks available for Virtual Meeting.

Topics:

For information about using Virtual Meeting, see the *Secure Mobile Access User Guide*. You can also view the *Secure Mobile Access Secure Virtual Meeting and Secure Virtual Assist Feature Module* for additional information.

Secure Virtual Meeting > Status

The **Secure Virtual Meeting > Status** page displays a summary of current active meetings and attendees, in addition to upcoming meetings.

Virtual Meeting > Status

On the right side of the screen, **Streaming Updates** indicates that changes to the status of customers are dynamically updated. Click **ON/OFF** to enable/disable Streaming Updates, respectively.

Click **Logout** next to a meeting in the Meeting Info section to delete an upcoming meeting.

Secure Virtual Meeting > Settings

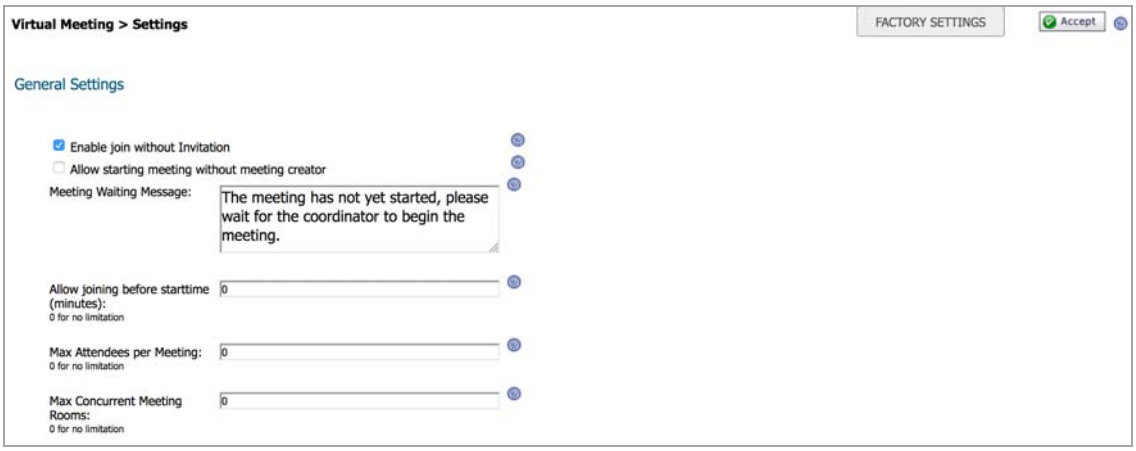
This section describes the **Secure Virtual Meeting > Settings** page and the configuration tasks available for Virtual Meeting. The Virtual Meeting settings are divided into the following pages:

General Settings

Use the General Settings page to configure general Virtual Meeting settings.

To configure Virtual Meeting general settings:

1 Navigate to the **Secure Virtual Meeting > Settings** page.



2 Select **Enable join without Invitation** to allow Participants to join the meeting without clicking the link in the e-mail invitation. Participants run the Virtual Meeting client and join the meeting directly with a meeting code set by the Coordinator.

3 Select **Allow starting meeting without meeting creator** to allow a meeting to start without the Coordinator present. If enabled and a scheduled meeting has no Coordinator in the meeting room at the scheduled start time, a participant is selected to become the Coordinator and begin the meeting. The meeting ends if this check box is not selected and the Coordinator is not present at the start time.

4 In the **Meeting Waiting Message** field, type the message to be displayed to Participants in the lobby waiting for the meeting to start. The lobby is a waiting room and meeting room, where you can initiate virtual meeting functions like chats and email invites.

5 In the **Allow joining before start time** field, select the number of minutes that Participants are allowed to join a meeting before it starts. Select 0 if Participants are allowed to join a meeting at any time, but you might want to consider that a license is in use from the time a Participant enters the lobby. See Licensing Overview on page 283 for additional licensing information.

6 In the **Max Attendees per Meeting** field, select the maximum number of attendees that could join any given meeting. Select 0 if the number of meeting attendees is unlimited.

> **NOTE:** Secure Virtual Meeting uses Secure Virtual Assist licenses and one Secure Virtual Assist technician license is required for every three active Virtual Meeting attendees.

7 In the **Max Concurrent Meeting Rooms** field, select the maximum number of meetings that can take place simultaneously on the appliance.

For example, your company has five Secure Virtual Assist technician licenses and two of them are being used for Virtual Assist technicians. Any number of Virtual Meetings can occur concurrently, but the number of concurrent users in the lobby is limited to nine (5-2=3 licenses available, 3x3=9 licenses for meeting users available).

Notification Settings

To configure Virtual Meeting notification settings:

1 On the **Secure Virtual Meeting > Settings** page, click the **Notification Settings** tab at the bottom of the page.

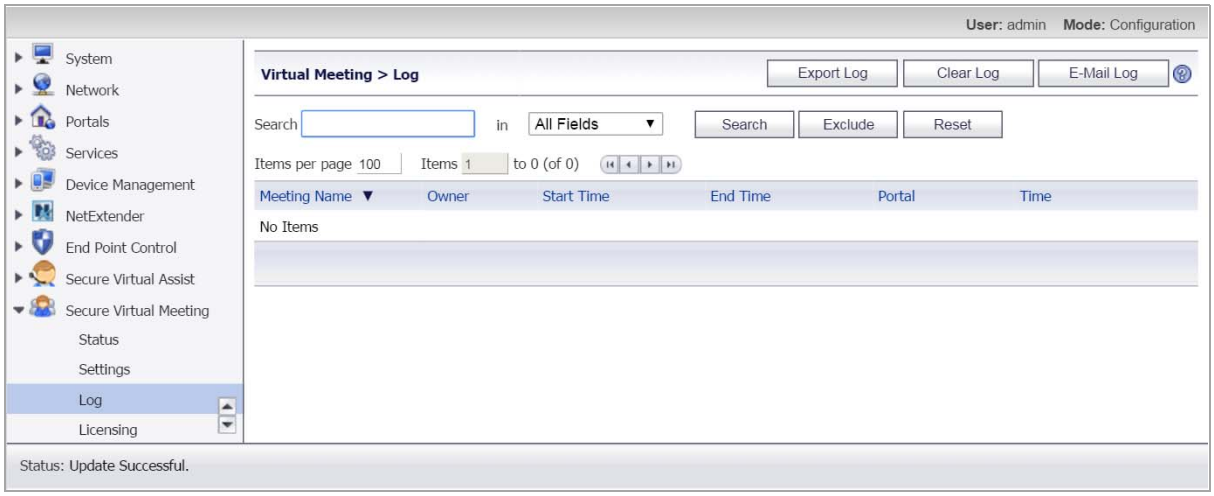
2 In the **Subject of Invitation** field type the subject used for Virtual Meeting e-mail invitations sent to Participants. The subject could include variables such as %MEETINGNAME%. Move the mouse pointer over the icon to the right of this field to display possible variables.

3 In the **Invitation Message** field type the text you want to include in the body of the Virtual Meeting e-mail invitation. The body can include variables. Move the mouse pointer over the icon to the right of this field to display possible variables.

Secure Virtual Meeting > Log

The **Secure Virtual Meeting > Log** page provides access to detailed information about recent meetings.

The log shows the meeting name, owner, meeting time, portal used time, and the time the meeting was created.



Click the meeting name to display additional information about a specific meeting. To return to the **Secure Virtual Meeting > Log** page, click the browser's Back button.

Click **Export Log** to create a zip file containing the full text of all logged meetings. The zip file contains a summary log file and a detail log file for each meeting that can be viewed in Microsoft Word.

Click **Clear Log** to erase all log messages.

Click **Email Log** to send the log to the e-mail 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 drop-down menu, select the field you want to search, and click **Search** to display only 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 displayed log messages by heading.

Secure Virtual Meeting > Licensing

This section provides an overview of the **Secure Virtual Meeting > Licensing** page and a description of the configuration tasks available on this page.

Licensing Overview

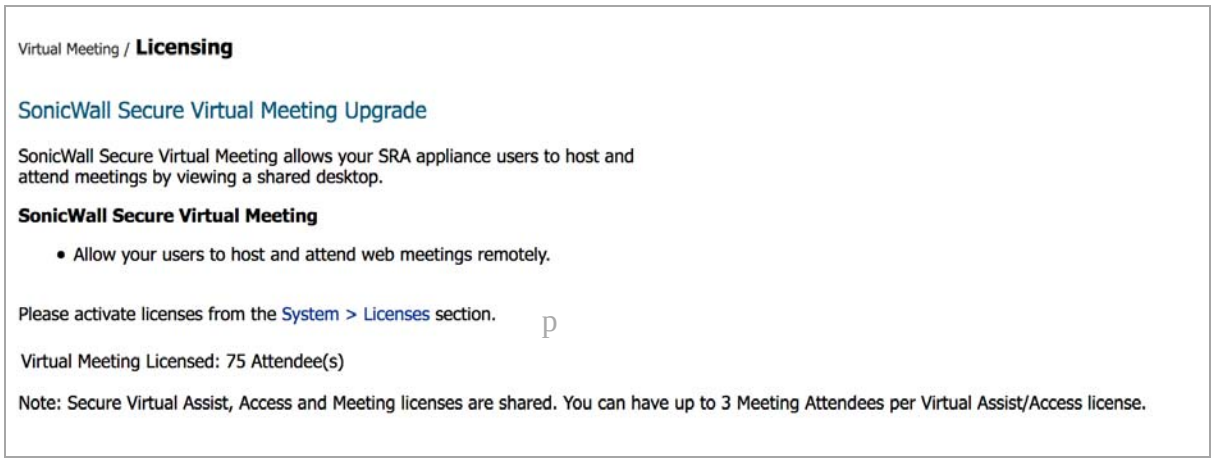
Secure Virtual Meeting is part of the Secure Virtual Assist package. Multiple Virtual Meetings and Virtual Assist sessions can occur simultaneously. However, one Virtual Assist technician license is required for every three active Virtual Meeting users. For example, your company has five Virtual Assist technician licenses and two of them are being used for Virtual Assist technicians. Any number of Virtual Meetings can occur concurrently, but the number of concurrent users in the lobby is limited to 9 (5-2=3 licenses available, 3x3=9 licenses for meeting users available).

Licenses are assigned on a first come, first served basis. Secure Virtual Meeting licenses are considered in use when an attendee is in the lobby. Secure Virtual Assist/Access licenses are considered in use when the connection is active and screen sharing is occurring.

Licensing Information

The **Secure Virtual Meeting > Licensing** page displays the Secure Virtual Assist license status that is also displayed on the **System > Licenses** page. See Licensing Overview on page 283 for an explanation of how Secure Virtual Assist licenses are used for Secure Virtual Meeting. The Licensing page also contains links to the **System > Licenses** page where you can obtain a license.

Secure Virtual Meeting Licensing



12

Web Application Firewall Configuration

This section provides information and configuration tasks specific to the **Web Application Firewall** pages on the Secure Mobile Access (web-based management interface.

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

For more information on Web Application Firewall concepts, see Web Application Firewall Overview on page 68.

Topics:

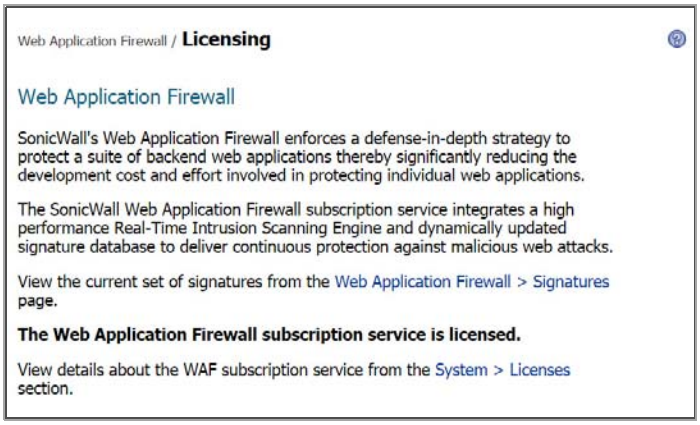
Licensing Web Application Firewall

The Secure Mobile Access Web Application Firewall must be licensed before you can begin using it. You can access the MySonicWall Web site directly from the Secure Mobile Access management interface to obtain a license.

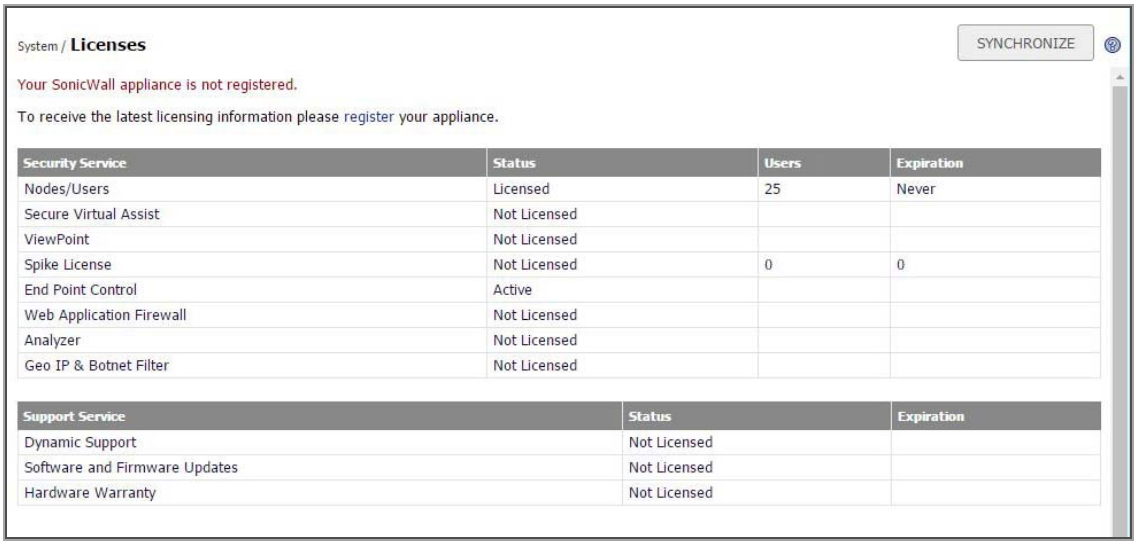
The **Web Application Firewall > Licensing** page in the Secure Mobile Access management interface provides a link to the **System > Licenses** page, where you can connect to MySonicWall and purchase the license or start a free trial. You can view all system licenses on the **System > Licenses** page of the Secure Mobile Access management interface.

To view license details and obtain a license on MySonicWall for Web Application Firewall:

1 Log in to your SMA/SRA appliance and navigate to **Web Application Firewall > Licensing**.



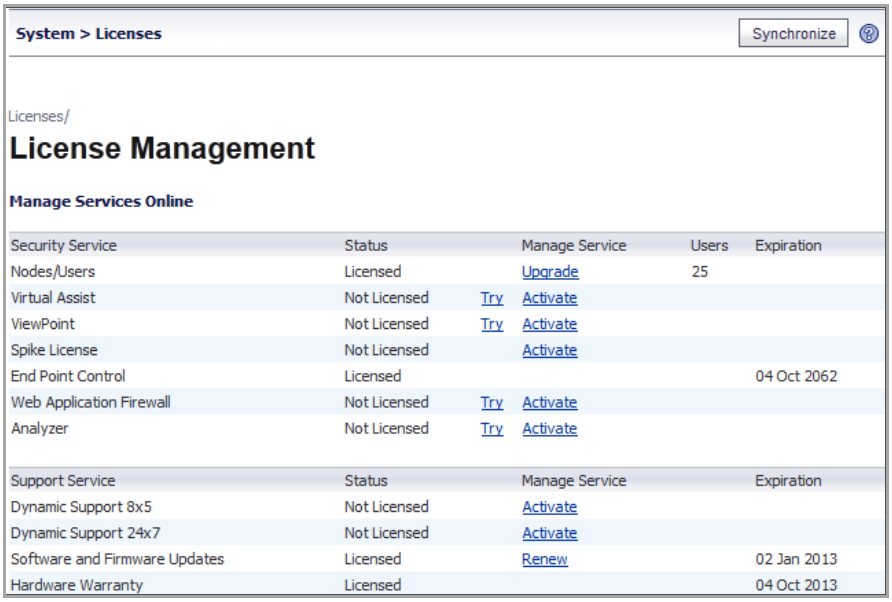
2 If Web Application Firewall is not licensed, click the **System > Licenses** link. The **System > Licenses** page is displayed.



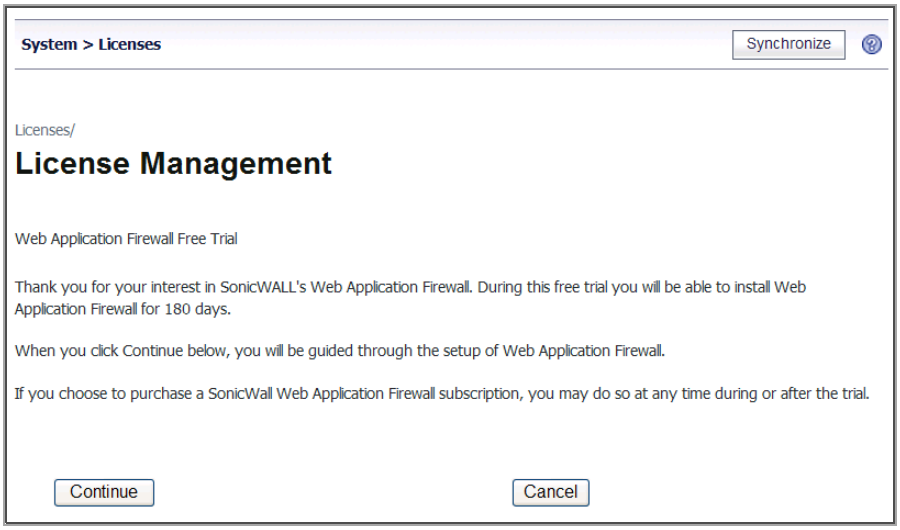
3 Under Manage Security Services Online, click the **Activate, Upgrade, or Renew services** link. The MySonicWall Login page is displayed.

4 Type your MySonicWall credentials into the fields, and then click **Submit**.

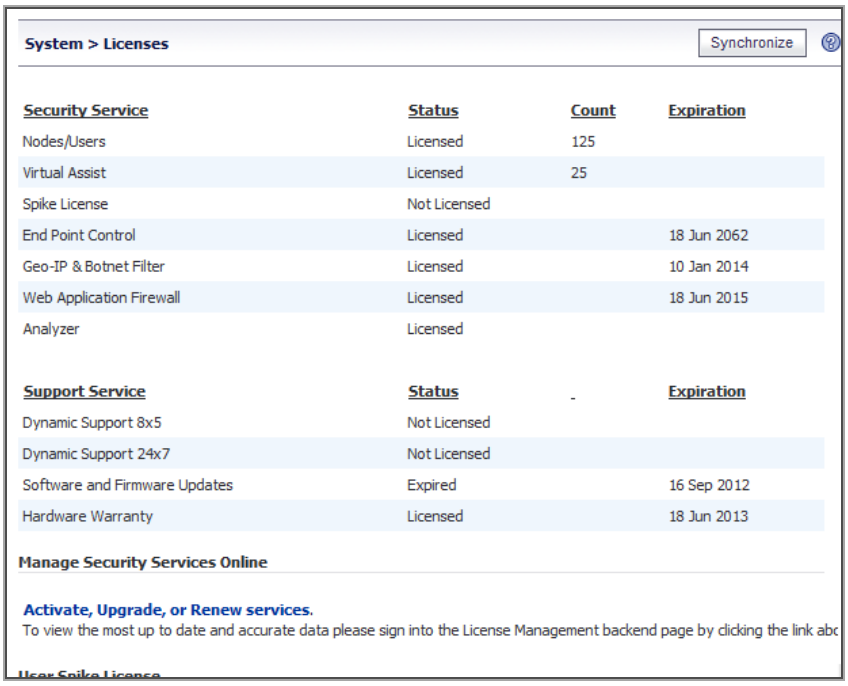
5 The **System > Licenses** page is displayed.



6 Click **Try** to start a 30 day free trial, or click **Activate** to subscribe to the service for 1 year. The screen that follows is displayed after selecting the free trial.



7 Click **Synchronize** to view the license on the **System > Licenses** page.



Web Application Firewall is now licensed on your SMA/SRA appliance. Navigate to **Web Application Firewall > Settings** to enable it, and then restart your appliance to completely activate Web Application Firewall.

Configuring Web Application Firewall

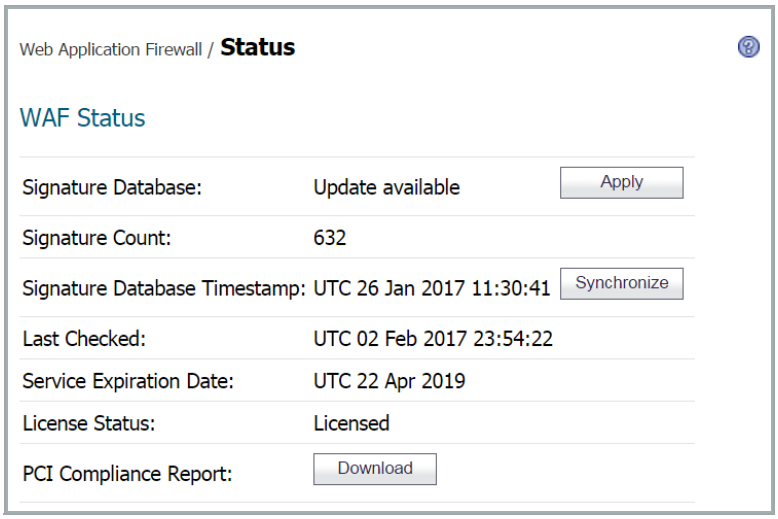
NOTE: Web Application Firewall requires the purchase of an additional license.

Topics:

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 displays the license status and expiration date. **Synchronize** allows you to

download the latest signatures from the SonicWall Inc. online database. You can use **Download** to generate and download a PCI compliance report file.

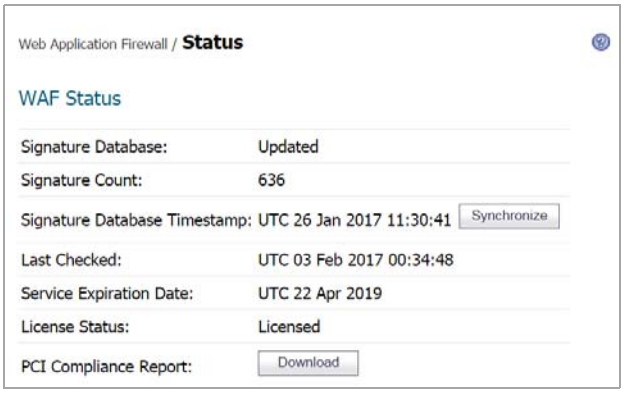


Viewing Status and Synchronizing Signatures

To view the status of the signature database and Web Application Firewall service license, and synchronize the signature database, complete the following steps in the Secure Mobile Access management interface:

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



2 If updates are available for the signature database, **Apply** is displayed. Click **Apply** to download the updates.

You can select an option to update and apply new signatures automatically on the **Web Application Firewall > Settings** page. If this automatic update option is enabled, **Apply** disappears from the **Web Application Firewall > Status** screen as soon as the new signatures are automatically applied.

3 To synchronize the signature database with the SonicWall Inc. online database server, click **Synchronize**. The timestamp is updated.

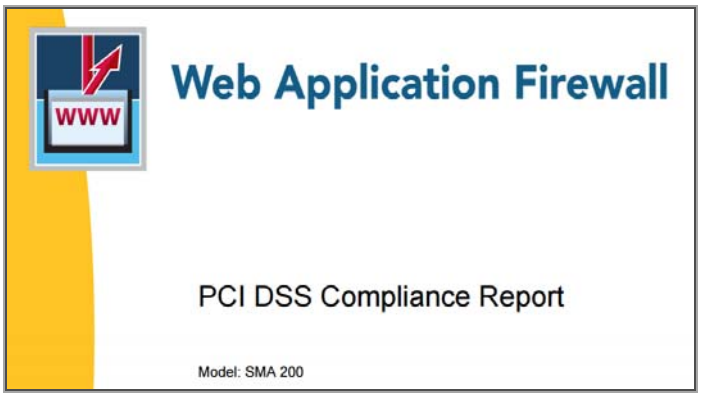
Downloading a PCI Compliance Report

To download a PCI DSS 6.5/6.6 compliance report:

1 Navigate to **Web Application Firewall > Status**.

2 Click **Download**.

3 In the File Download dialog box, click **Open** to create the PCI report as a temporary file and view it with Adobe Acrobat, or click **Save** to save the report as a PDF file.



Configuring Web Application Firewall Settings

The **Web Application Firewall > Settings** page allows you to enable and disable Web Application Firewall on your SMA/SRA 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 other Web Application Firewall settings. The following sections describe the procedures for enabling and configuring Web Application Firewall settings:

Enabling Web Application Firewall and Configuring General Settings

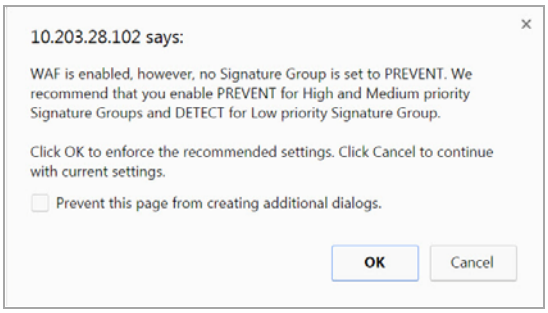
To enable and activate Web Application Firewall, you must select the check box to globally enable it and select at least one of the check boxes in the Signature Groups table. The settings in the General Settings section on this page allow you to globally manage your network protection against attacks by selecting the level of protection for high, medium, or low priority attacks. You can also clear **Global Enable Web Application Firewall** to temporarily disable Web Application Firewall without losing any of your custom configuration settings.

You can enable automatic signature updates in the **General Settings** section, 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 **Web Application Firewall > Logs** and **Logs > View** pages. For more information about CSRF/XSRF attacks, see How is Cross-Site Request Forgery Prevented? on page 74.

To configure global settings for Web Application Firewall:

1. On the **Web Application Firewall > Settings** page, expand the **General Settings** section.
2. Select **Enable Web Application Firewall**.
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.



4. Select **Apply Signature Updates Automatically** to enable new signatures to be automatically downloaded and applied when available. You do not have to click **Apply** on the **Web Application Firewall > Status** page to apply the new signatures.
5. Select the desired level of protection for **High Priority Attacks** in the Signature Groups table. Select one of the following options:

- Select **Prevent All** to block access to a resource when an attack is detected. Selecting **Prevent All** automatically selects **Detect All**, turning on logging.
- Clear **Prevent All** and select **Detect All** to log attacks while allowing access to the resource.
- To globally disable all logging and prevention for this attack priority level, clear both check boxes.

6 Select the desired level of protection for **Medium Priority Attacks** in the Signature Groups table.

7 Select the desired level of protection for **Low Priority Attacks** in the Signature Groups table.

8 When finished, click **Accept**.

Configuring Global Exclusions

There are three 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, you can lower the action level from Prevent to Detect for certain hosts, or you can set Web Application Firewall to take no action.

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.

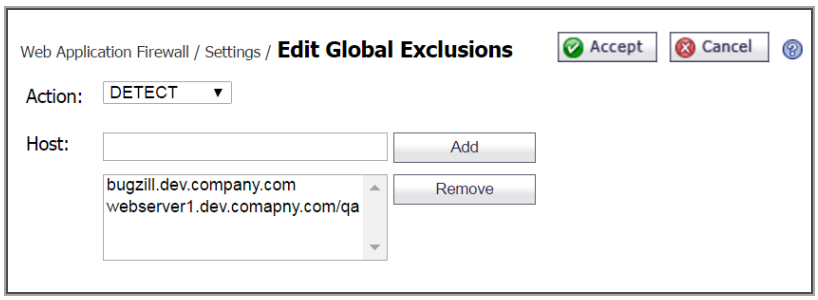
To configure global exclusions:

1 On the **Web Application Firewall > Settings** page, expand the **General Settings** section.

2 Click **Global Exclusions**.

3 In the Edit Global Exclusions page, the action you set overrides the signature group settings for the resources configured on these host pages. Select one of the following from the **Action** drop-down list:

- **Disable** – Disables Web Application Firewall inspection for the host.
- **Detect** – Lowers the action level from prevention to only detection and logging for the host.
- **No Action** – Web Application Firewall inspects host traffic, but takes no action.



4 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. Up to 32 characters are allowed. To determine the correct host entry for this exclusion, see Determining the Host Entry for Exclusions on page 303.

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.company.com/exchange**, then all files and folders under **exchange** are also excluded.

5 Click **Add** to move the host name into the list box.

6 Repeat Step 4 and Step 5 to add more hosts to this exclusion.

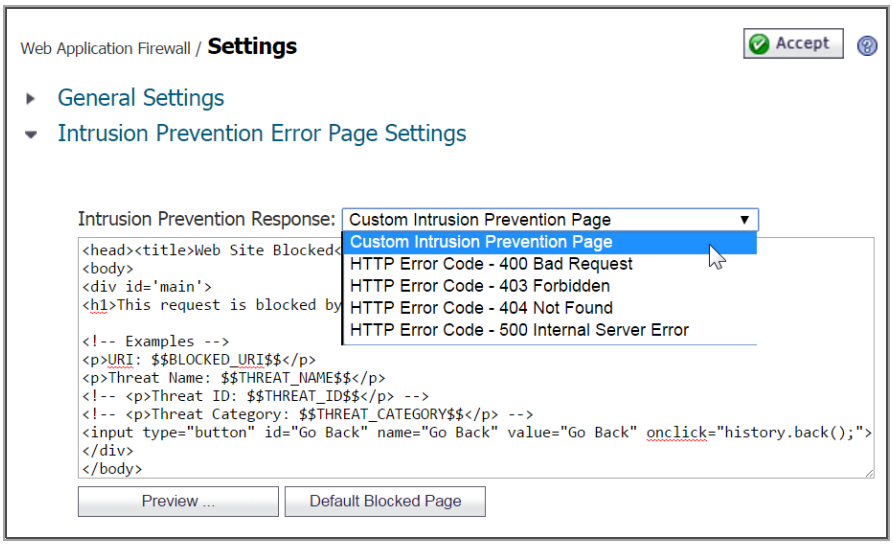
7 When finished, click **Accept**.

Configuring Intrusion Prevention Error Page Settings

To configure the error page to use when intrusions are detected:

1 Expand the **Intrusion Prevention Error Page Settings** section.

2 In the **Intrusion Prevention Response** drop-down list, select the type of error page to be displayed when blocking an intrusion attempt.



3 To create a custom page, select **Custom Intrusion Prevention Page** and modify the sample HTML in the text box.

4 To view the resulting page, click **Preview**.

5 To reset the current customized error page to the default error page, click **Default Blocked Page** and then click **OK** in the confirmation dialog box.

6 If you do not want to use a customized error page, select one of the following for the error page:

- HTTP Error Code 400 Bad Request
- HTTP Error Code 403 Forbidden
- HTTP Error Code 404 Not Found
- HTTP Error Code 500 Internal Server Error

7 When finished, click **Accept**.

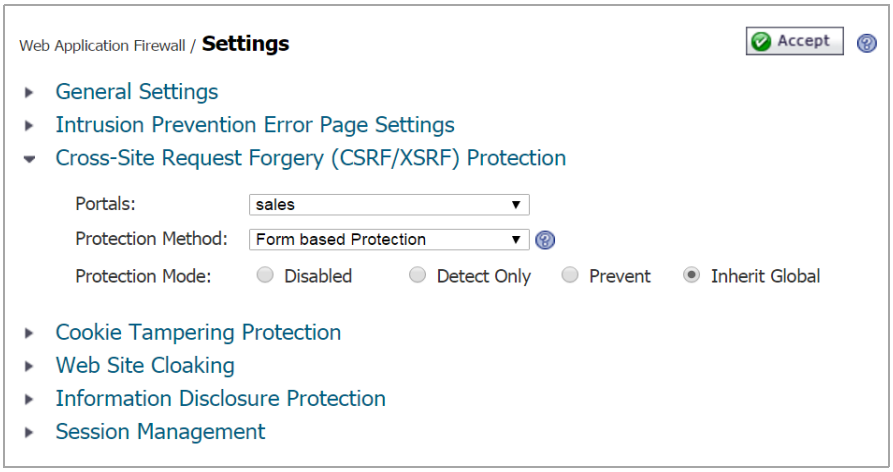
Configuring Cross-Site Request Forgery Protection Settings

Cross-Site Request Forgery (CSRF) is configured independently for each Application Offloading portal. New with this release is the Form-based Protection Method that provides a seamless solution and results in less false positives. Optionally, you can select the original Protection Method, URL Rewrite-based Protection Method.

When a CSRF attack is detected, log entries are created in both the **Web Application Firewall > Logs** and **Logs > View** pages. For more information about CSRF/XSRF attacks, see How is Cross-Site Request Forgery Prevented? on page 74.

To configure the settings for CSRF protection with the URL Rewrite-based Protection Method:

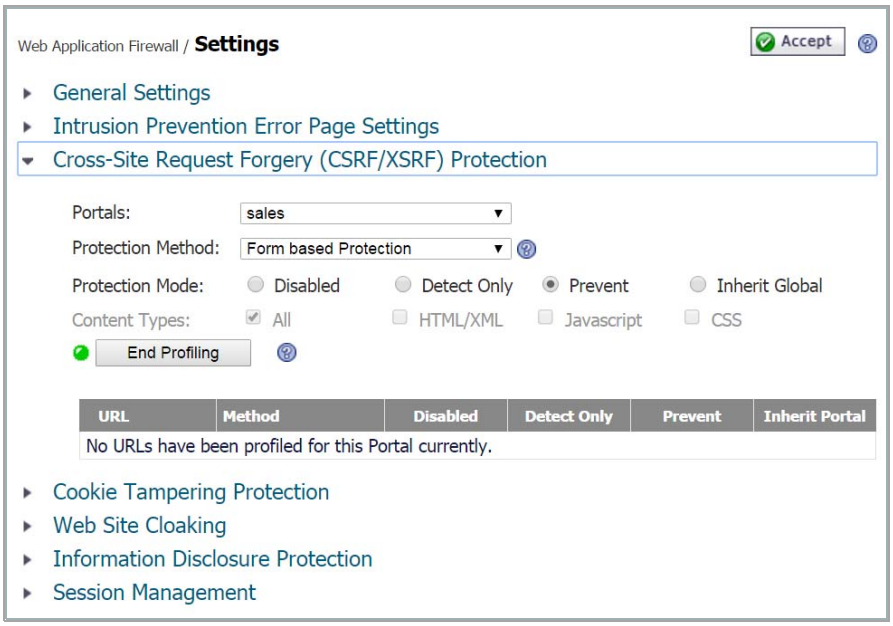
1. Expand the **Cross-Site Request Forgery (CSRF/XSRF) Protection** section.
2. In the **Portals** drop-down list, select the Portal to which these CSRF protection settings apply. To make these CSRF settings the default for all portals, select **Global**.
3. Select **URL Rewrite-based Protection** from the **Protection Method** drop-down list.
4. For **Protection Mode**, select the desired level of protection against CSRF attacks. You can select **Detect Only** to log these attacks, or **Prevent** to log and block them. Select **Disabled** to disable CSRF protection on the portal.
5. When finished, click **Accept**.



To configure the settings for CSRF protection with the Form-based Protection Method:

1. Expand the **Cross-Site Request Forgery (CSRF/XSRF) Protection** section.
2. In the **Portals** drop-down list, select the Portal to which these CSRF protection settings apply. To make these CSRF settings the default for all portals, select **Global**.
3. Select **Form-based Protection** from the **Protection Method** drop-down list.
4. For **Content Types**, select the types of content you want to be profiled by CSRF. You can select **All**, **HTML/XML**, **JavaScript**, or **CSS**.
5. Click **Begin Profiling** to start the CSRF Form-based Protection. If you wish to stop profiling, click **End Profiling**.

6 When finished, click **Accept**.



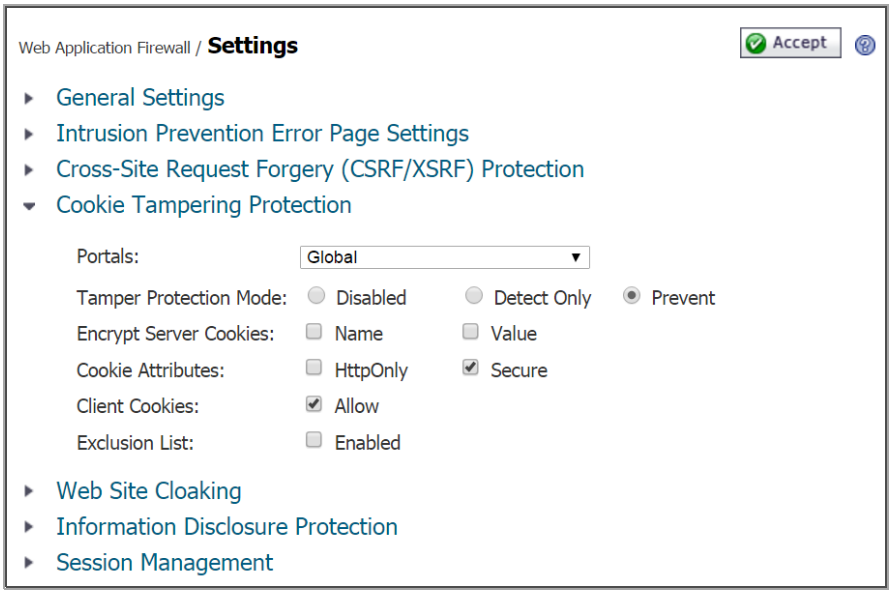
NOTE: If you are upgrading from a previous firmware version and switch the Protection Method to **Form-based Protection**, the controls might appear grayed and disabled. Simply click **Accept** to activate the controls.

Configuring Cookie Tampering Protection Settings

Cookie tampering protection is configured independently for each Application Offloading portal.

To configure the settings for cookie tampering protection:

1 Expand the **Cookie Tampering Protection** section.



2 In the **Portals** drop-down list, select the Application Offloading portal to which these cookie tampering protection settings apply. To make these cookie tampering settings the default for all portals, select **Global**.

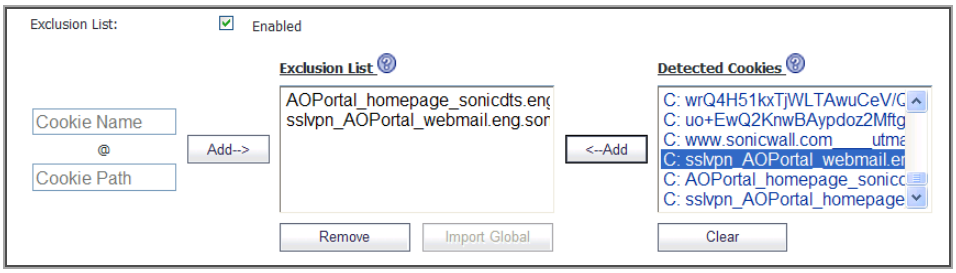
3 For **Tamper Protection Mode**, select the desired level of protection against cookie tampering. You can select **Detect Only** to log these attacks, or **Prevent** to log and block them. Select **Disabled** to disable cookie tampering protection on the portal.

4 For **Encrypt Server Cookies**, select **Name** to encrypt cookie names, and/or select **Value** to encrypt cookie values. This affects client-side script behavior because it makes cookie names or values unreadable. Only server-side cookies are encrypted by these options.

5 For **Cookie Attributes**, select **HttpOnly** to append the *HttpOnly* attribute to server-side cookies, and/or select **Secure** to append the *Secure* attribute to server-side cookies. The attribute *HttpOnly* prevents the client-side scripts from accessing the cookies that are important in mitigating attacks such as Cross Site Scripting and session hijacking. The attribute *Secure* ensures that the cookies are transported only in HTTPS connections. Both together add a strong layer of security for the server-side cookies.

6 For **Client Cookies**, select **Allow** if an application on the portal needs all of the client cookies. When disabled, client-side cookies are not allowed to be sent to the backend systems. This option does not affect server-side cookies.

7 For the **Exclusion List**, select **Enabled** to display additional fields for configuration.



8 To enter a custom cookie name and path to the **Exclusion List**, click in the **Cookie Name** field to type in the name of the cookie, and click in the **Cookie Path** field to type in the path. Then click > **Add**.

9 To add one or more already-detected cookies to the **Exclusion List**, select the desired cookies in the **Detected Cookies** list, holding the **Ctrl** key while clicking multiple cookies, and then click < **Add** to add them to the **Exclusion List**.

10 To remove cookies from the **Exclusion List**, select the cookies to be removed and then click **Remove**.

11 To clear the **Detected Cookies** list, click **Clear**.

12 When finished, click **Accept**.

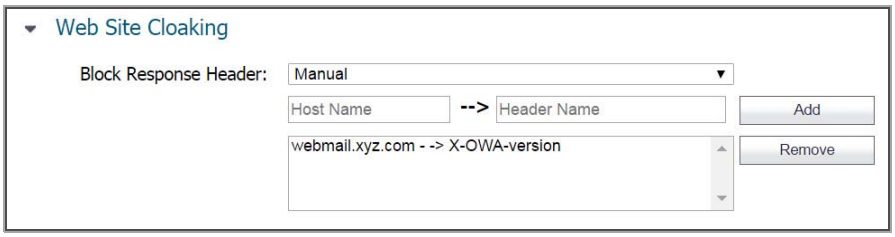
Configuring Web Site Cloaking

Under **Web Site Cloaking**, you can filter out headers in response messages that could provide information to clients about the backend Web server that could possibly be used to find a vulnerability.

To configure Web site cloaking:

1 Expand the **Web Site Cloaking** section.

2 In the **Block Response Header** fields, select **Manual** and type the server host name into the first field and type the header name into the second field, then click **Add**.



For example, if you set the host name to “webmail.xyz.com” and the header name to “X-OWA-version,” headers with the name “X-OWA-version” from host “webmail.xyz.com” is blocked. In general, listed headers are not sent to the client if an HTTP/HTTPS bookmark or off-loaded application is used to access a listed Web server.

To block a certain header from all hosts, set the host name to an asterisk (*). You can add up to 64 host/header pairs. In the HTTP protocol, response headers are not case-sensitive.

NOTE: Blocking does not occur for headers such as Content-Type that are critical to the HTTP protocol.

3 To remove a host/header pair from the list to be blocked, select the pair in the text box and then click **Remove**.

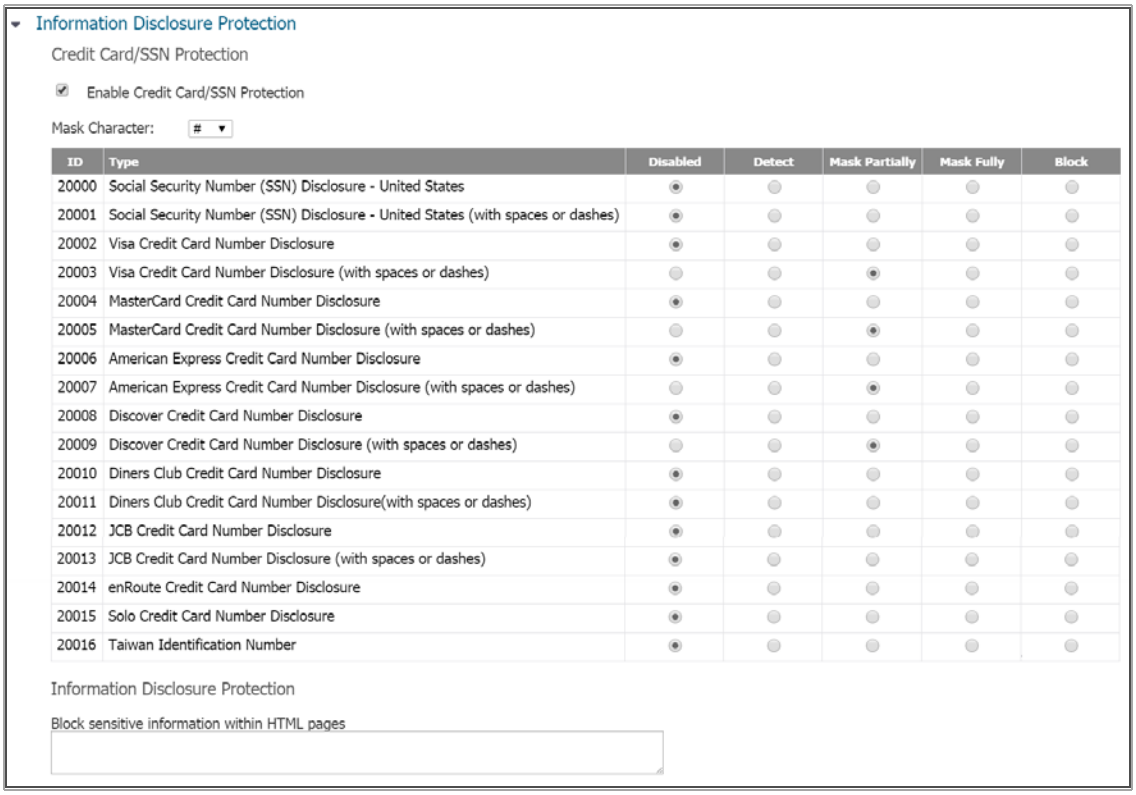
4 When finished, click **Accept**.

Configuring Information Disclosure Protection

Under **Information Disclosure Protection**, you can protect against inadvertent disclosure of credit card and Social Security numbers (SSN) in HTML Web pages. You can also enter confidential text strings that should not be revealed on any Web site protected by Web Application Firewall.

To configure information disclosure protection:

1 Expand the **Information Disclosure Protection** section. The table contains a row for each possible pattern or representation of a social security number or credit card number that Web Application Firewall can detect in the HTML response.



ID	Type	Disabled	Detect	Mask Partially	Mask Fully	Block
20000	Social Security Number (SSN) Disclosure - United States	◉	○	○	○	○
20001	Social Security Number (SSN) Disclosure - United States (with spaces or dashes)	◉	○	○	○	○
20002	Visa Credit Card Number Disclosure	◉	○	○	○	○
20003	Visa Credit Card Number Disclosure (with spaces or dashes)	○	○	◉	○	○
20004	MasterCard Credit Card Number Disclosure	◉	○	○	○	○
20005	MasterCard Credit Card Number Disclosure (with spaces or dashes)	○	○	◉	○	○
20006	American Express Credit Card Number Disclosure	◉	○	○	○	○
20007	American Express Credit Card Number Disclosure (with spaces or dashes)	○	○	◉	○	○
20008	Discover Credit Card Number Disclosure	◉	○	○	○	○
20009	Discover Credit Card Number Disclosure (with spaces or dashes)	○	○	◉	○	○
20010	Diners Club Credit Card Number Disclosure	◉	○	○	○	○
20011	Diners Club Credit Card Number Disclosure(with spaces or dashes)	◉	○	○	○	○
20012	JCB Credit Card Number Disclosure	◉	○	○	○	○
20013	JCB Credit Card Number Disclosure (with spaces or dashes)	◉	○	○	○	○
20014	enRoute Credit Card Number Disclosure	◉	○	○	○	○
20015	Solo Credit Card Number Disclosure	◉	○	○	○	○
20016	Taiwan Identification Number	◉	○	○	○	○

2 Select **Enable Credit Card/SSN Protection**.

3 In the **Mask Character** drop-down list, select the character to be substituted when masking the SSN or credit card number.

4 In the table, select the level of protection desired for each representation of a SSN or credit card number. You can select one of the following in each row:

- **Disabled** – Do not match numbers in this format. No logging or masking is done.
- **Detect** – Detect numbers in this format and create a log entry when detected.
- **Mask Partially** – Substitute the masking character for the all digits in the number, except the last few digits such that the confidentiality of the number is still preserved.
- **Mask Fully** – Substitute the masking character for all digits in the number.
- **Block** – Do not transmit or display the number at all, even in masked format.

5 Below the table, in the **Block sensitive information within HTML pages** text box, type confidential text strings that should not be revealed on any Web site protected by Web Application Firewall. This text is case insensitive, can include any number of spaces between the words, but cannot include wildcard characters. Add new phrases on separate lines. Each line is pattern matched within any HTML response.

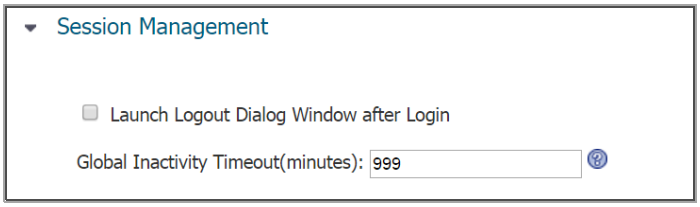
6 When finished, click **Accept**.

Configuring Session Management Settings

Under **Session Management**, you can control whether the logout dialog window is displayed when a user logs into the user portal or into an application offloaded portal. You can also set the inactivity timeout for users in this section.

To configure session management settings:

1 Expand the **Session Management** section.



2 Select **Launch Logout Dialog Window after Login** to display the session logout popup dialog box when the user portal is launched or when a user logs into an application offloaded portal.

3 In the **Global Inactivity Timeout** field, type the number of inactive minutes allowed before the user is logged out. This setting can be overridden by Group or User settings.

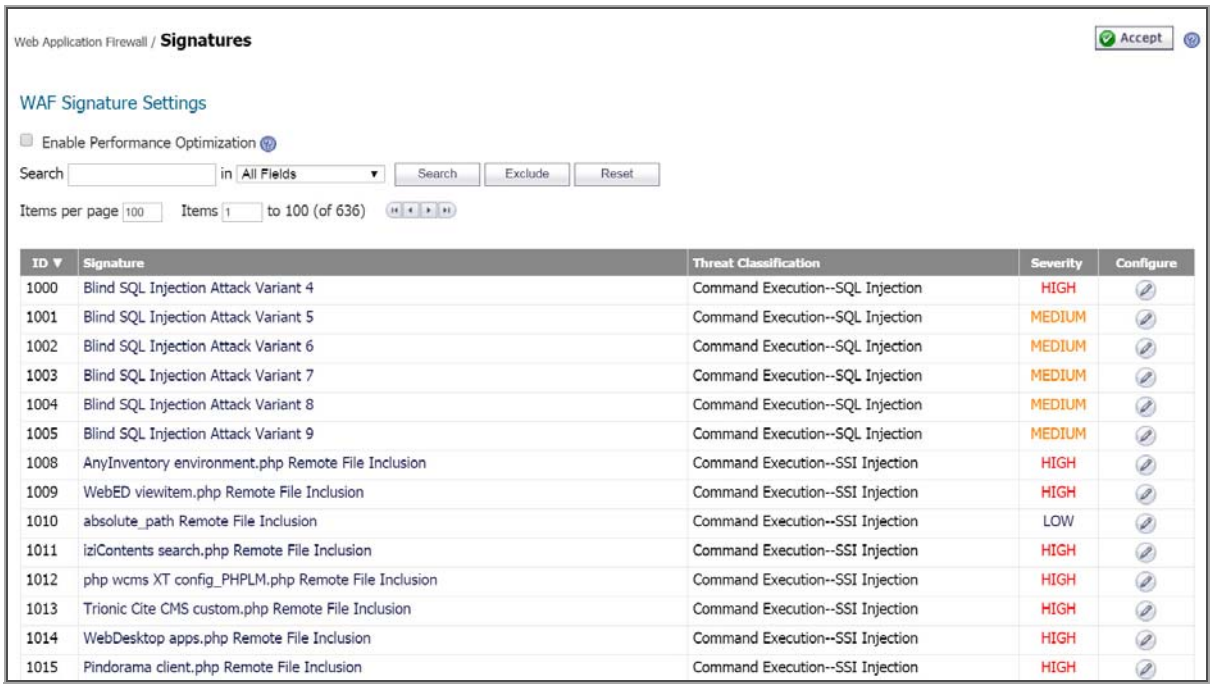
NOTE: To mitigate CSRF attacks, it is important to keep a low idle timeout value for user sessions, such as 10 minutes.

4 When finished, click **Accept**.

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. 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.



ID	Signature	Threat Classification	Severity	Configure
1000	Blind SQL Injection Attack Variant 4	Command Execution--SQL Injection	HIGH	
1001	Blind SQL Injection Attack Variant 5	Command Execution--SQL Injection	MEDIUM	
1002	Blind SQL Injection Attack Variant 6	Command Execution--SQL Injection	MEDIUM	
1003	Blind SQL Injection Attack Variant 7	Command Execution--SQL Injection	MEDIUM	
1004	Blind SQL Injection Attack Variant 8	Command Execution--SQL Injection	MEDIUM	
1005	Blind SQL Injection Attack Variant 9	Command Execution--SQL Injection	MEDIUM	
1008	AnyInventory environment.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	
1009	WebED viewitem.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	
1010	absolute_path Remote File Inclusion	Command Execution--SSI Injection	LOW	
1011	iziContents search.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	
1012	php wcms XT config_PHPLM.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	
1013	Trionic Cite CMS custom.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	
1014	WebDesktop apps.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	
1015	Pindorama client.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	

The list of signatures can be sorted by the contents of any column in ascending or descending order by clicking the column heading. In addition, signatures can be divided into pages and filtered by searching for a key word. To display only signatures containing a key word in all fields or a specific field, type the key word in the Search field, select **All Fields** or a specific field to search, and click **Search**. Or, click **Exclude** to display only signatures that do not contain the key word. Click **Reset** to display all signatures. All matches are highlighted. The default is 50 signatures per page.

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 General Settings on page 291.

Signature Groups	Prevent All	Detect All
High Priority Attacks	☑	☑
Medium Priority Attacks	☑	☑
Low Priority Attacks	☐	☑

See the following sections:

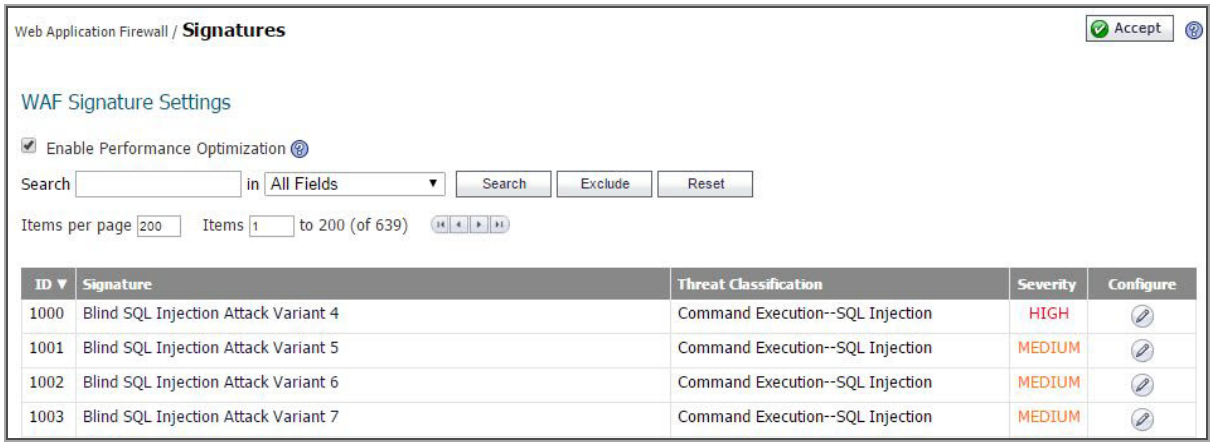
- Enabling Performance Optimization on page 300
- Configuring Signature Based Custom Handling and Exclusions on page 301
- Reverting a Signature to Global Settings on page 302
- Removing a Host from a Per-Signature Exclusion on page 303

Enabling Performance Optimization

The Performance Optimization option allows you to disable some relatively less severe signatures that significantly affect the performance of certain Web applications. These signatures are identified by the SonicWall Inc. signature team and the list is pushed out to SMA/SRA appliances. When you select **Enable Performance Optimization**, these signatures are disabled for Web Application Firewall.

The **Web Application Firewall > Signatures** page indicates the disabled signatures by displaying them in gray, as shown in Enabling Performance Optimization.

Enabling Performance Optimization



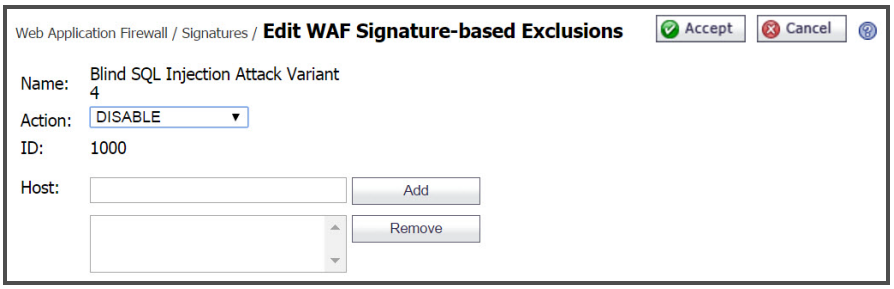
Configuring Signature Based Custom Handling and Exclusions

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 blocks 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, complete the following steps:

1 On the **Web Application Firewall > Signatures** page, click **Configure** for the signature that you wish to change. The **Edit WAF Signature-based Exclusions** screen displays.



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

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 303.

   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.yourcompany.com/exchange**, then all files and folders under **exchange** are also excluded.

4 If you specified a host, click **Add** to move the host name into the list box.

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.

6 Click **Accept**. If the Host list contains host entries, Secure Mobile Access 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.

7 Click **OK** in the confirmation dialog box.

8 Click **Accept** 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 continues 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:

1 On the **Web Application Firewall > Signatures** page, click **Configure**  for the signature that you wish to change.

2 In the Edit WAF Signature-based Exclusions screen, select **INHERIT GLOBAL** from the **Action** drop-down list.

3 The **Host** field might 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.

4 Click **Accept**. Secure Mobile Access verifies that each host entry is valid.

5 Click **OK** in the confirmation dialog box.

6 Click **Accept** 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 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, complete the following steps:

1. On the **Web Application Firewall > Signatures** page, click **Configure** for the signature that you wish to change.
2. Select the host entry in the list box under the Host field, and then click **Remove**.
3. Repeat Step 2 to remove other listed hosts, if desired.
4. Click **Accept**. Secure Mobile Access verifies that each host entry is valid.
5. Click **OK** in the confirmation dialog box.
6. Click **Accept** 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 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:

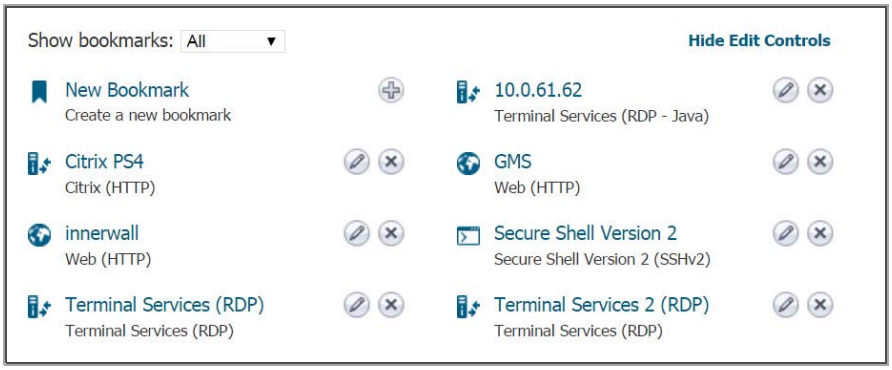
- Viewing the Host Entry in a Bookmark on page 303
- Viewing the Host Entry in an Off-loaded Application on page 304

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.

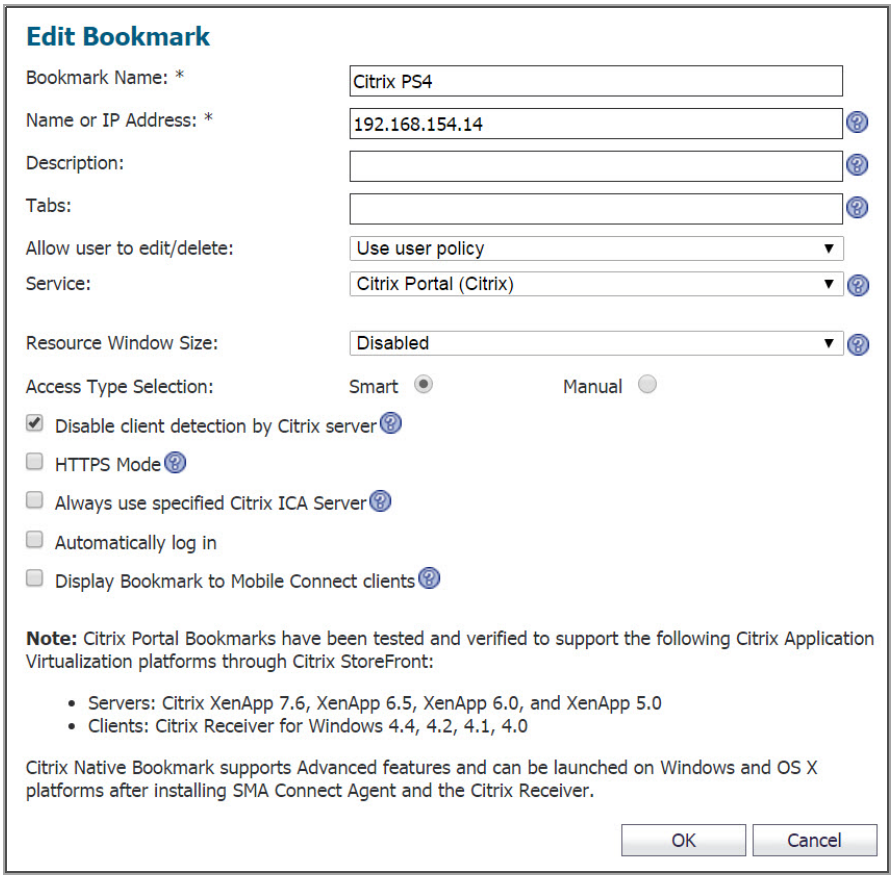
To view the host entry in a bookmark:

1. Navigate to the Virtual Office page, and click **Show Edit Controls** above the list of bookmarks.



2 Click **Edit** for the bookmark.

3 In the Edit Bookmark screen, view the host entry in the **Name or IP Address** field.



4 Click **Cancel**.

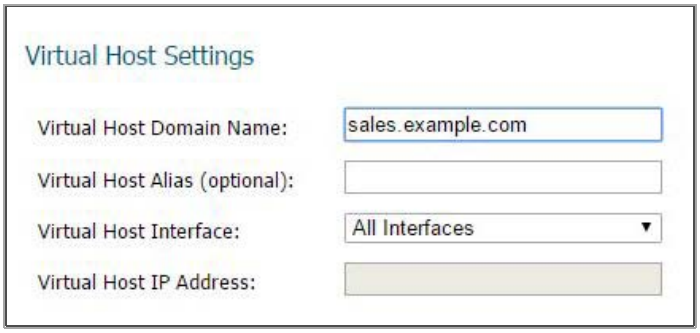
Viewing the Host Entry in an Off-loaded Application

You can determine exactly what host name to enter in your exclusion by viewing the configuration details of the off-loaded application. In an off-loaded application, you use the virtual host domain name.

To view the virtual host domain name in an off-loaded application:

1 Navigate to the **Portals > Portals** page and click **Configure** next to the off-loaded application.

2 In the Edit Portal screen, click the **Virtual Host** page.



3 View the host entry for your exclusion in the **Virtual Host Domain Name** field.

4 Click **Cancel**.

Configuring Custom Rules and Application Profiling

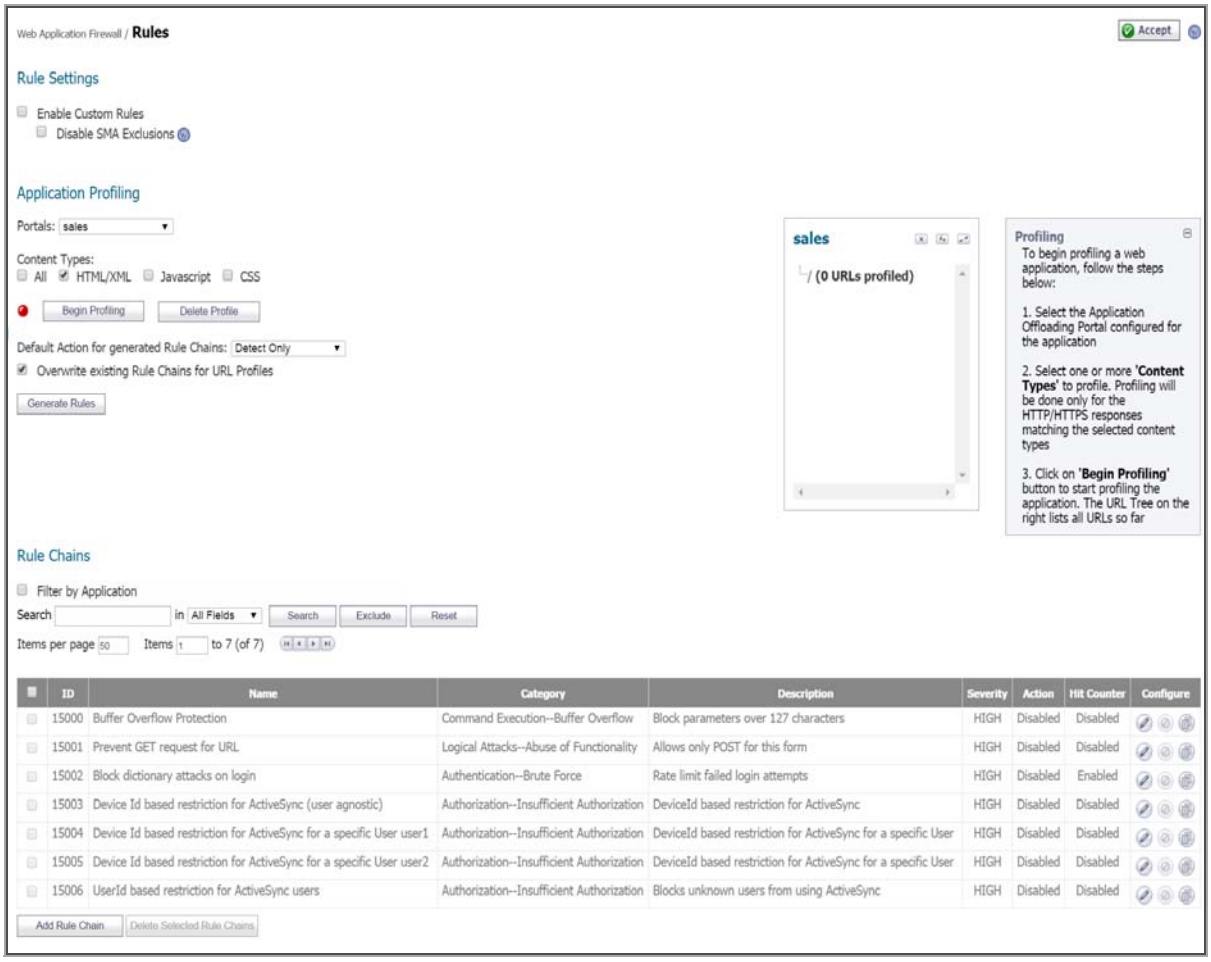
The **Web Application Firewall > Rules** page allows you to configure custom rules and application profiling.

Application profiling allows you to generate custom rules in an automated manner based on a trusted set of inputs used to develop a profile of what inputs are acceptable by an application. Other inputs are denied, providing positive security enforcement. When you place the SMA/SRA appliance in learning mode in a staging environment, it learns valid inputs for each URL accessed by the trusted users. At any point during or after the learning process, custom rules can be generated based on the “learned” profiles. For more information about application profiling, see How Does Application Profiling Work? on page 78.

NOTE: Application profiling is supported only on the SMA 400, SRA 4600, and SMA 500v Virtual Appliance.

Custom rules created on this page have all the same properties as the signatures that SonicWall Inc. pushes out to Web Application Firewall-enabled appliances. Web Application Firewall > Rules Page shows the Rules page.

Web Application Firewall > Rules Page



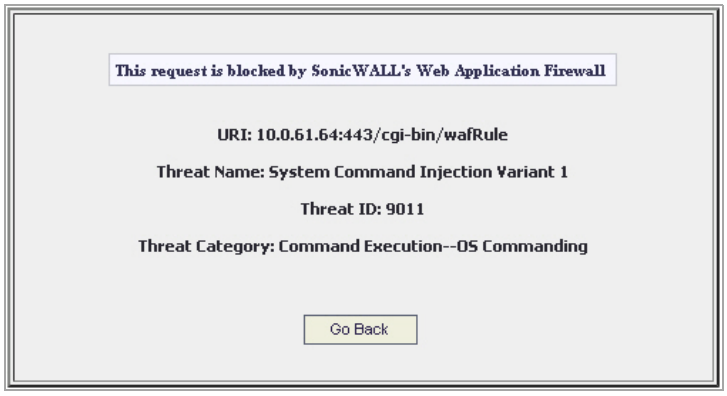
To add a rule manually, you create a **rule chain** and then add rules within it. A rule chain is a collection of rules and includes additional attributes such as the severity rating, name, description, hit counters for rate limiting, and the action to take when the rule chain matches some traffic. Rule Chains shows all rule chain fields.

Rules in the **Web Application Firewall > Rules** page can be divided into pages and filtered by searching for a key word. To display only rules containing a key word in all fields or a specific field, type the key word in the Search field, select **All Fields** or a specific field to search, and click **Search**. Or, click **Exclude** to display only rules that do not contain the key word. Click **Reset** to display all rules. All matches are highlighted. The default is 50 rules per page.

Rule Chains

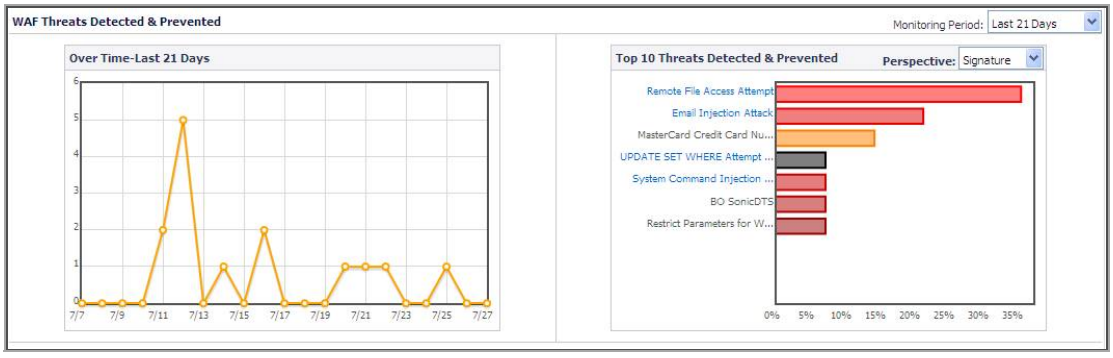
Custom rules and rule chains can be used to distinguish between legitimate and illegitimate traffic as defined by a Web application that is using a certain URI or running on a certain portal. One rule in the chain is configured to match the URI or portal host name, while another rule is created that matches an undesirable value for another element of the HTTP(S) traffic. When the rule chain (both rules) matches some traffic, the configured action is done to block or log the bad traffic from that URI or portal. When the request is blocked, the user sees a custom block page such as that in Block Page.

Block Page



The **Web Application Firewall > Monitoring** page also shows the activity in the graphs. Monitoring Page After Blocking shows several detected and prevented threats during a 12 hour period. For more information about the Monitoring page, see Using Web Application Firewall Monitoring on page 321.

Monitoring Page After Blocking



Rules are matched against both inbound and outbound HTTP(S) traffic. When all rules in a rule chain find a match, the action defined in the rule chain is done. You can also enable rate limiting in rule chains to trigger an action only after the number of matching attacks exceeds a threshold within a certain time period. You can configure the action to block the traffic and log the match, or to simply log it. You can also set the action to **Disabled** to remove the rule chain from active status and stop comparing traffic against those rules.

The Custom Rules feature can be enabled or disabled using the **Enable Custom Rules** global setting.

NOTE: Rule chains are enforced in the order that the rule chains were added. This order can be changed by deleting and re-creating rule chains.

Similarly, rules within rule chains are enforced in the order that the rules were added. This order can be changed by deleting and re-creating rules.

Configuring Application Profiling

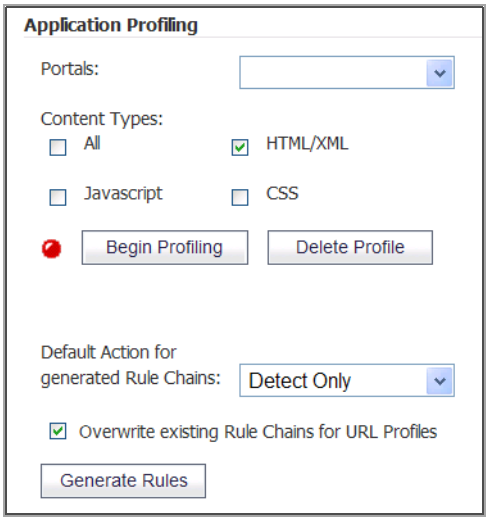
You can create URL profiles by putting the SMA/SRA appliance into learning mode while applications are in use by trusted users, and then use those URL profiles to generate rule chains that prevent malicious misuse of the applications.

NOTE: Application profiling is supported only on the SMA 400, SRA 4600, and SMA 500v Virtual Appliance.

To configure application profiling and automatically generate rules:

1 Navigate to the **Web Application Firewall > Rules** page.

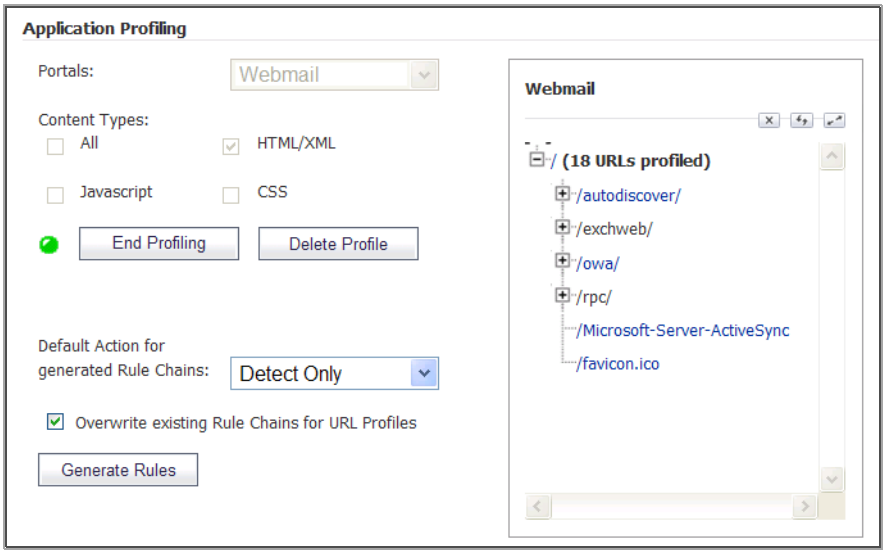
2 Under **Application Profiling**, select one or more portals with the application(s) to be profiled from the **Portals** drop-down list. Use Shift+click or CTRL+click to select multiple portals.



3 For **Content Types**, select the type of content to be profiled:

- **All** – Includes all content types such as images, HTML, and CSS.
- **HTML/XML** – Selected by default, this is the most important from a security standpoint, because it typically covers the more sensitive Web transactions.
- **Javascript** – Appropriate for an application written in Javascript.
- **CSS** – Select CSS to profile the cascading style sheet content used to control the formatting of Web pages written in HTML, XHTML, or XML variants.

4 Click **Begin Profiling** to start the "learning" process. Trusted users should be using the relevant applications on the selected portal during the active profiling period. **Begin Profiling** changes to **End Profiling**. Profiling continues until you click **End Profiling**.

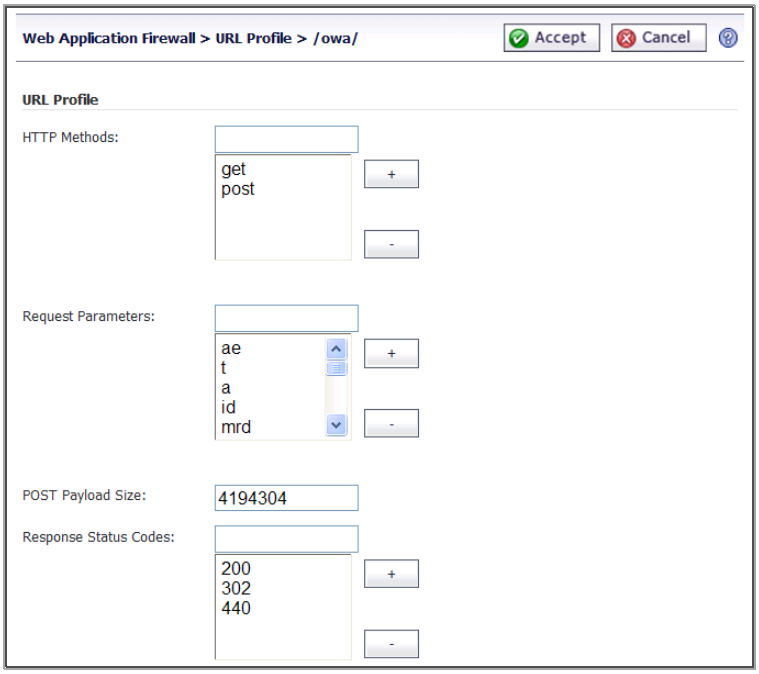


During profiling, the Secure Mobile Access records inputs and stores them as URL profiles. The URL profiles are listed as a tree structure on the **Web Application Firewall > Rules** page in the Application Profiling section.

5 After a period of time adequate to record inputs from normal application use, click **End Profiling** to stop the profiling process.

6 Optionally click any of the links in the URL profile tree display to edit the learned values. Click  to expand all URLs at that level in the tree. You can also click  to refresh all URLs in the list or click  to delete a selected URL.

The editing page for the clicked URL is displayed.



7 To add a value, type the value into the field next to the parameter and then click the plus button. To remove a value, select it in the list and then click the minus button.

8 Click **Accept** when finished editing. Repeat for other URLs as needed.

9 Before generating the rules from the URL profiles, select one of the following actions from the **Default Action for generated Rule Chains** drop-down list:

- **Disabled** – The generated rules are disabled rather than active.
- **Detect Only** – Content triggering the generated rule is detected and logged.
- **Prevent** – Content triggering the generated rule is blocked and logged.

10 Select **Overwrite existing Rule Chains for URL Profiles** to overwrite rule chains that have already been generated from a URL profile.

11 Click **Generate Rules** to generate rules from the URL profiles. If a URL profile has been modified, those changes are incorporated.

If rule chains are successfully generated, the status bar indicates how many rule chains were generated, including any that were overwritten.

12 If you do not want to accept the generated rule chains, click **Delete Selected Rule Chains** that is available following the rule chain list. All of the automatically added rule chains are pre-selected right after generation for easy deletion of the group.

13 Click **Accept** to apply the generated rule chains to the Secure Mobile Access configuration.

Configuring Rule Chains

You can add, edit, delete and clone rule chains. Example rule chains (with Rule Chain ID greater than 15000) are available in the Secure Mobile Access management interface for administrators to use as reference. These cannot be edited or deleted. You can view the rules associated with the rule chain by clicking its **Edit Rule Chain** icon under **Configure**.

For ease of configuration, you can clone example rule chains or regular rule chains. Cloning a rule chain clones all rules associated with the chain. After cloning the rule chain, you can edit it by clicking its Edit Rule Chain icon under Configure.

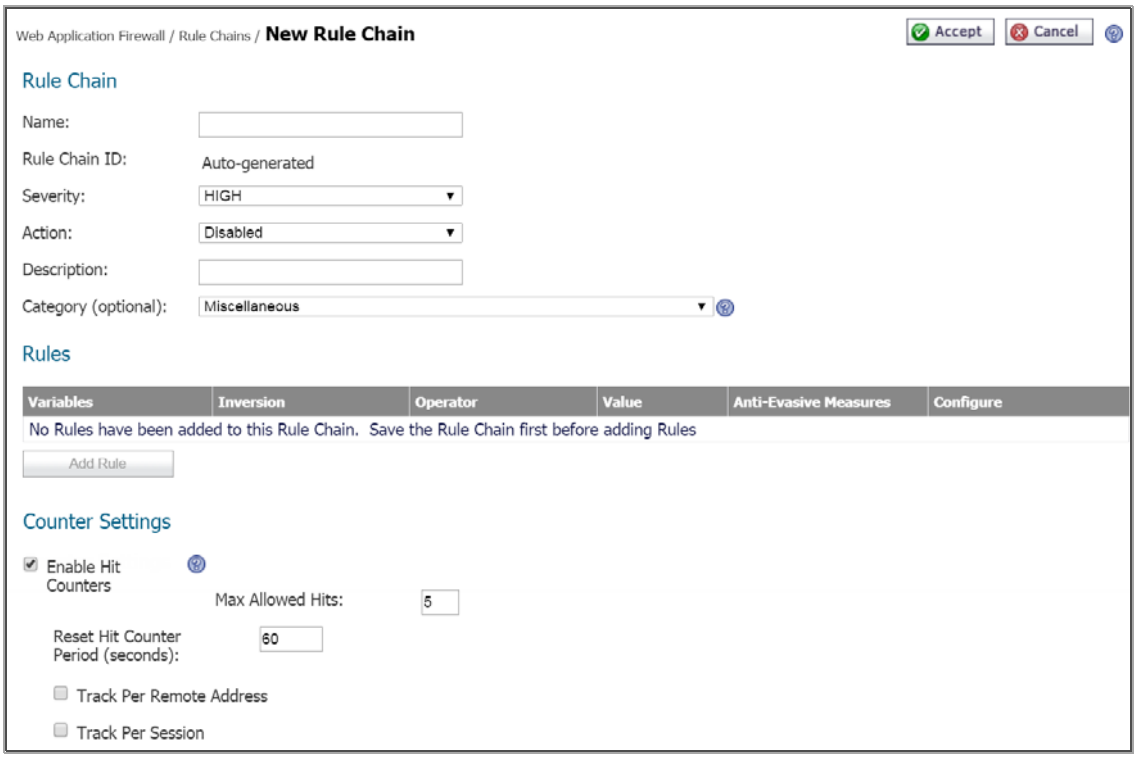
Adding or Editing a Rule Chain

To add or edit a rule chain:

1 On the **Web Application Firewall > Rules** page, click **Add Rule Chain** to add a new rule chain.

To edit an existing rule chain, click its **Edit Rule Chain** icon  under **Configure**.

The New Rule Chain screen or the screen for the existing rule chain displays. Both screens have the same configurable fields in the **Rule Chain** section.



2 On the New Rule Chain page, type a descriptive name for the rule chain in the **Name** field.

3 Select a threat level from the **Severity** drop-down list. You can select **HIGH**, **MEDIUM**, or **LOW**.

4 Select **Disabled**, **Detect Only**, or **Prevent** from the **Action** drop-down list.

- **Disabled** – The rule chain should not take effect.
- **Detect Only** – Allow the traffic, but log it.
- **Prevent** – Block traffic that matches the rule and log it.

The **Disabled** option allows you to temporarily deactivate a rule chain without deleting its configuration.

5 In the **Description** field, type a short description of what the rule chain matches or other information.

6 Select a category for this threat type from the **Category** drop-down list. This field is for informational purposes, and does not change the way the rule chain is applied.

7 Under **Counter Settings**, to enable tracking the rate at which the rule chain is being matched and to configure rate limiting, select **Enable Hit Counters**. Additional fields are displayed.

8 In the **Max Allowed Hits** field, enter the number of matches for this rule chain that must occur before the selected action is triggered.

9 In the **Reset Hit Counter Period** field, enter the number of seconds allowed to reach the Max Allowed Hits number. If Max Allowed Hits is not reached within this time period, the selected action is not triggered and the hits counter is reset to zero.

10 Select **Track Per Remote Address** to enforce rate limiting against rule chain matches coming from the same IP address. Tracking per remote address uses the remote address as seen by the SMA/SRA appliance. This covers the case where different clients sit behind a firewall with NAT enabled, causing them to effectively send packets with the same source IP.

11 Select **Track Per Session** to enable rate limiting based on an attacker's browser session. This method sets a cookie for each browser session. Tracking by user session is not as effective as tracking by remote IP if the attacker initiates a new user session for each attack.

12 Click **Accept** to save the rule chain. A **Rule Chain ID** is automatically generated.

13 Next, add one or more rules to the rule chain. See Configuring Rules in a Rule Chain on page 312 for detailed information.

Cloning a Rule Chain

To clone a rule chain:

1 On the **Web Application Firewall > Rules** page, click its Clone Rule Chain icon under **Configure**.

2 Click **OK** in the confirmation dialog box.

You can now edit the rule chain to customize it. See Adding or Editing a Rule Chain on page 309.

Deleting a Rule Chain

NOTE: Deleting a rule chain also deletes all the associated rules.

To delete a rule chain:

1 On the **Web Application Firewall > Rules** page, click the Delete Rule Chain icon under **Configure** for the rule chain you want to delete.

2 Click **OK** in the confirmation dialog box.

3 Click **Accept**.

Correcting Misconfigured Rule Chains

Misconfigured rule chains are not automatically detected at the time of configuration. When a misconfiguration occurs, the administrator must log in and fix or delete the bad rules.

NOTE: If any rules or rule chains are misconfigured, the appliance does not enforce any custom rules or rule chains.

It is difficult to detect a false positive from a misconfigured rule chain unless a user runs into it and reports it to the administrator. If the rule chain has been set to PREVENT, then the user sees the Web Application Firewall block page (as configured on the **Web Application Firewall > Settings** page). If not, there is a log message indicating that the "threat" has been detected.

Consider a scenario in which the administrator inadvertently creates a custom rule chain that blocks access to all portals of the SMA/SRA appliance. For example, the admin might have wanted to enforce a rule for an Application Offloading portal. However, he or she forgot to add another rule to narrow the criteria for the match to requests for that portal, host or URL. If the first rule was too broad, then this means a denial of service for the appliance. Specifically, the administrator creates a rule chain to deny using the GET HTTP method for a specific URL that expects a POST request.

For this, the administrator needs to create two rules:

1 The first rule is to match GET requests.

2 The second rule is to match a specific URL.

If the administrator forgets to create the second rule, then access to the SMA/SRA appliance is denied, because the Secure Mobile Access web-based management interface depends on the GET method.

To fix a misconfigured rule chain, complete the following tasks:

1 Point your browser to https://<SMA IP>/cgi-bin/welcome.

If you try to reach the welcome page by simply using the URL https://<SMA IP>/, the usual redirect to https://<SMA IP>/cgi-bin/welcome might not work. To repair misconfigured rules, you need to explicitly go to https://<SMA IP>/cgi-bin/welcome, where <SMA IP> is the host name or IP address of your SMA/SRA appliance.

2 Log in as **admin**.

3 Navigate to the **Web Application Firewall > Rules** page.

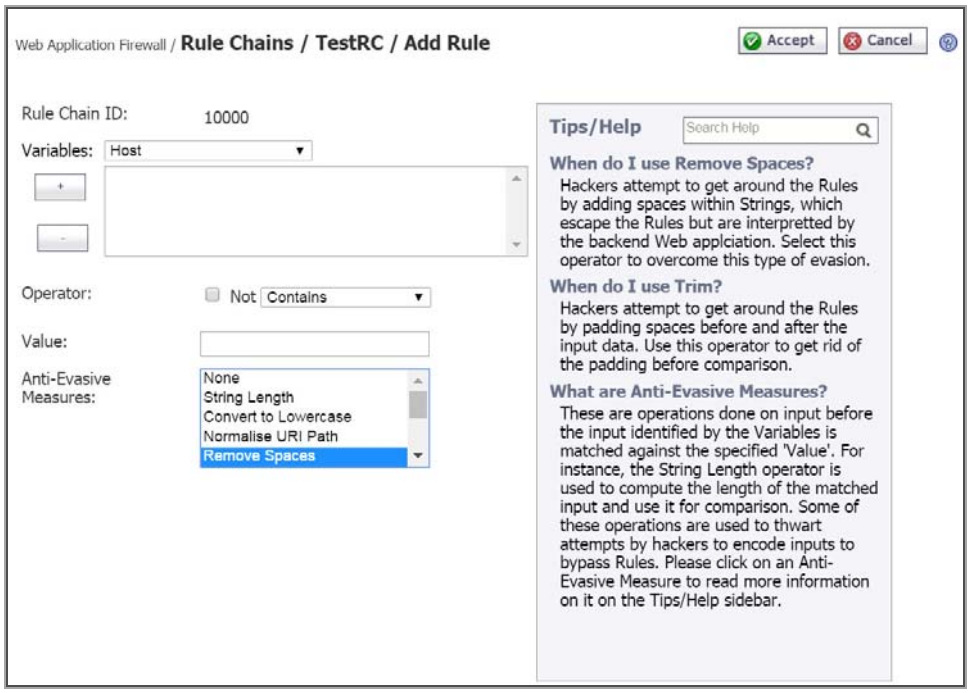
4 Edit or delete the bad rules.

5 Click **Accept**.

Configuring Rules in a Rule Chain

You can add, edit, delete and clone rules. A rule is a condition that is checked against inbound or outbound HTTP(S) traffic. Each rule chain can have one or more rules configured, and must have at least one rule before it can be used. Add Rule page shows the Add Rule page.

Add Rule page



Rules allow the administrator to employ both a positive security model and a negative security model. In a positive security model, policies are written only to allow known traffic and block everything else.

A rule has several components:

- **Variables** – These are HTTP protocol entities that are scanned by Web Application Firewall to help identify legitimate or illegitimate traffic. Multiple variables can be matched against the configured value in the **Value** field. The '+' and '-' buttons allow you to add variables from the **Variables** drop-down list or delete them from the list of selected variables. You can combine multiple variables as required to match

the specified value. If multiple variables are configured, then the rule is matched if any one of the configured variables matches the target value. See About Variables on page 313 for more information about variables.

- **Operators** – These are arithmetic and string operators. The **Not** check box is an inversion operator used to match any value except the configured condition. See About Operators on page 315 for more information about the operators.
- **Value** – This entity can be a number, literal string, or a regular expression that is compared with the scanned target. It is compared with the value of the configured variable(s) according to the specified operator.

  To compare the variable(s) to more than one value, you can enter multiple values separated by spaces into the **Value** field, and select the **Matches Keyword** operator. Delimiting by spaces only works if the **Matches Keyword** operator is selected.
- **Anti-Evasive MEASUREs** – This field allows you to apply measures beyond those supported by the **Operators** field, especially to enforce Anti-Evasive protection. See About Anti-Evasive Measures on page 316 for more information about these measures.

The following sections provide detailed information about rules:

About the Tips/Help Sidebar

You can select a variable in the **Variables** drop-down list to display more information about that variable in the **Tips/Help** sidebar. The sidebar explains when each variable would be used and where it is found in the HTTP protocol. An example use case is provided for each variable.

You can also select an entry in the **Anti-Evasive Measures** drop-down list to display more information about it in the **Tips/Help** sidebar.

The sidebar also provides context-sensitive search. When you click on a variable and then search for a particular keyword, the search results are only related to variables.

About Variables

Variables are HTTP protocol entities that are scanned by Web Application Firewall to help identify legitimate or illegitimate traffic. Multiple variables can be matched against the configured value in the **Value** field. The '+' and '-' buttons allow you to add variables from the **Variables** drop-down list or delete them from the list of selected variables.

You can combine multiple variables as required to match the specified value. If multiple variables are configured, then the rule is matched if any one of the configured variables matches the target value.

A variable can represent a single value or a collection. If a variable represents a collection, such as **Parameter Values**, then a specific variable within the collection can be configured by entering its name in the selection text box to the right of the colon (**:**). For example, the value for the **URI** or **Host** variable is unique in each HTTP(S)

request. For such variables, the selection text box is not displayed. Other variables, such as **Request Header Values** and **Response Header Names**, represent a collection.

If you need to test the collection itself against an input, then you would leave the selection text box empty. However, if you need to retrieve the value of a specific item in the collection, you would specify that item in the selection text box. For example, if you need to test if the parameter **password** exists in the HTTP(S) request, then you would configure the variable **Parameter Names** and leave the selection text box empty. You would set the **Operator** to **String equals** and the **Value** to **password**. But, if you want to check whether the value of the password parameter matches a particular string, such as "foo," then you would select the **Parameter Values** variable and specify **password** in the selection text box. In the **Value** field, you would enter **foo**.

the Variables for Use in Rules table describes the available variables.

Variables for Use in Rules

Variable Name	Collection	Description
Host	No	Refers to the host name or the IP address in the Host header of an HTTP request. This typically refers to the host part of the URL in the address bar of your browser.
URI	No	Refers to the combination of path and the query arguments in a URL.
HTTP Method	No	Refers to the method, such as GET and POST, used by the browser to request a resource on the Web server.
HTTP Status Code	No	Refers to the response status from the Web server. You can use this to configure actions for various error codes from the Web server.
Parameter Values	Yes	Refers to the collection of all request parameter values, including the values of all query arguments and form parameters that are part of the current request. To match against some aspect of the entire list of parameter values, such as the number of parameter values, leave the selection field empty. To match against the value of a particular parameter, specify the name of the parameter in the selection field to the right of the colon.
Parameter Names	Yes	Refers to the collection of all request parameter names, including the names of all query arguments and form parameters that are part of the current request. To match against some aspect of the entire list of parameter names, leave the selection field empty. To match against the name of a particular parameter, specify the parameter name in the selection field to the right of the colon.
Remote Address	No	Refers to the client's IP address. This variable allows you to allow or block access from certain IP addresses.
Request Header Values	Yes	Refers to the collection of all HTTP(S) request header values for the current request. To match against some aspect of the entire list of request header values, leave the selection field empty. To match against a particular header value, specify the name of the header in the selection field to the right of the colon. For example, to block Ajax requests, select **Request Header Values** as the Variable, specify **X-Request-With** in the selection text box, and specify **ajax** in the **Value** field.

Variables for Use in Rules (Continued)

Variable Name	Collection	Description
Request Header Names	Yes	Refers to the collection of all HTTP(S) request header names for the current request. To match against some aspect of the entire list of request header names, leave the selection field empty. To match against a particular header name, specify the name of the header in the selection field to the right of the colon. For example, to block requests that are not referred by a trusted host, select **Request Header Names** as the **Variable**, specify **Referrer** in the selection text box, enter the host names or IP addresses of the trusted hosts in the **Value** field, select the **Not** check box and select the **Matches Keyword** operator.
Response Header Values	Yes	Refers to the collection of all HTTP(S) response header values for the current request. To match against some aspect of the entire list of response header values, leave the selection field empty. To match against a particular header value, specify the name of the header in the selection field to the right of the colon.
Response Header Names	Yes	Refers to the collection of all HTTP(S) response header names for the current request. To match against some aspect of the entire list of response header names, leave the selection field empty. To match against a particular header name, specify the name of the header in the selection field to the right of the colon.
Response Content Length	No	Refers to the size of the response payload.
Response Payload	No	Refers to the Web page content that is displayed to the user.
Portal Hostname	No	Refers to the virtual host name of the Secure Mobile Access portal which accepts the request from the client. To create a rule chain that applies to a particular virtual host, one rule would match the host and another would specify other criteria for the match.
Portal Address	No	Refers to the IP address or virtual IP address of the Secure Mobile Access portal which accepts the request from the client.
Request Path	No	Refers to the relative path used to access a particular resource in a Web site.

About Operators

There are a number of arithmetic and string operators. The **Not** check box is an inversion operator that results in a match for any value except the configured condition.

These operators can be used in conjunction with **Anti-Evasive Measures**. For example, you might use the **Equals String** operator with **Convert to Lowercase** or **Normalize URI Path** in **Anti-Evasive Measures**.

the Rule Operators table describes the available operators for use with rules.

Rule Operators

Operator	Type	Description
Contains	String	One or more of the scanned variables contains the content of the **Value** field.
Equals String	String	The scanned variable(s) match the alphanumeric string in the **Value** field exactly.
=	Arithmetic	The scanned variable is equal to the content of the **Value** field.
>	Arithmetic	The scanned variable is greater than the content of the **Value** field.
>=	Arithmetic	The scanned variable is greater than or equal to the content of the **Value** field.
<	Arithmetic	The scanned variable is less than the content of the **Value** field.
<=	Arithmetic	The scanned variable is less than or equal to the content of the **Value** field.
Matches Keyword	String	One or more of the scanned variables matches one of the keywords in the **Value** field. If multiple keywords are specified, they should be separated by spaces.
Matches Regex	String	One or more of the scanned variables matches the regular expression in the **Value** field. An example of a regular expression that matches any four decimal numbers is **\d{4}**.

About Anti-Evasive Measures

Anti-evasive measures are applied to input identified by the selected variables before the input is matched against the specified value. For instance, the **String Length** measure is used to compute the length of the matched input and use it for comparison. Some of the anti-evasive measures are used to thwart attempts by hackers to encode inputs to bypass Web Application Firewall rules. You can click on an anti-evasive measure in the list to read more information on it in the **Tips/Help** sidebar.

The anti-evasive measures can be used in conjunction with regular operators. There are ten measures to choose from in the **Anti-Evasive Measures** field, including the **None** measure which leaves the input alone.

Multiple anti-evasive measures can be selected together and individually enforced. You can select multiple measures by holding the **Ctrl** key while clicking an additional measure. When the **None** measure is selected along with other measures in your rule, the input is compared as is and also compared after decoding it or converting it with another measure. the Anti-Evasive Measures for Rules table describes the anti-evasive measures available for use with rules.

Anti-Evasive Measures for Rules

Measure	Description
None	Use the **None** measure when you want to compare the scanned input to the configured variable(s) and value(s) without changing the input.
String Length	Use the **String Length** measure when the selected variable is a string and you want to compute the length of the string before applying the selected operator.

Anti-Evasive Measures for Rules (Continued)

Measure	Description
Convert to Lowercase	Use the **Convert to Lowercase** measure when you want to make case-insensitive comparisons by converting the input to all lowercase before the comparison. When you use this measure, make sure that strings entered in the **Value** field are all in lowercase. This is an anti-evasive measure to prevent hackers from changing case to bypass the rule.
Normalize URI Path	Use the **Normalize URI Path** measure to remove invalid references, such as back-references (except at the beginning of the URI), consecutive slashes, and self-references in the URI. For example, the URI www.eshop.com/././//login.aspx is converted to www.eshop.com/login.aspx. This is an anti-evasive measure to prevent hackers from adding invalid references in the URI to bypass the rule.
Remove Spaces	Use the **Remove Spaces** measure to remove spaces within strings in the input before the comparison. Extra spaces can cause a rule to not match the input, but are interpreted by the backend Web application. This is an anti-evasive measure to prevent hackers from adding spaces within strings to bypass the rule.
Base64 Decode	Use the **Base64 Decode** measure to decode base64 encoded data before the comparison is made according to the rule. Some applications encode binary data in a manner convenient for inclusion in URLs and in form fields. Base64 encoding is done to this type of data to keep the data compact. The backend application decodes the data. This is an anti-evasive measure to prevent hackers from using base64 encoding of their input to bypass the rule.
Hexadecimal Decode	Use the **Hexadecimal Decode** measure to decode hexadecimal encoded data before the comparison is made according to the rule. This is an anti-evasive measure to prevent hackers from using hexadecimal encoding of their input to bypass the rule.
URL Decode URL Decode (Unicode)	Use the **URL Decode** measure to decode URL encoded strings in the input. Use the **URL Decode (Unicode)** measure to handle **%uXXXX** encoding. URL encoding is used to safely transmit data over the Internet when URLs contain characters outside the ASCII character set. **NOTE**: Do not use these measures against an input that has been decoded already. This is an anti-evasive measure to prevent hackers from using URL encoding to bypass rules, knowing that the backend Web server can interpret their malicious input after decoding it. For example, the URI www.eshop.com/hack+URL%3B is converted to www.eshop.com/hack URL by this operator before the comparison is made.
Trim	Use the **Trim** measure to remove spaces before and after the input data before the comparison. Extra spaces can cause a rule to not match the input, but are interpreted by the backend Web application. This is an anti-evasive measure to prevent hackers from adding spaces before and after the input data to bypass the rule.

Example Use Cases for Rules

This section provides examples of positive and negative security models, as well as several examples showing the use of anti-evasive measures to provide a deeper understanding of these anti-evasive techniques.

Example – Positive Security Model: Blocking Bad Logins

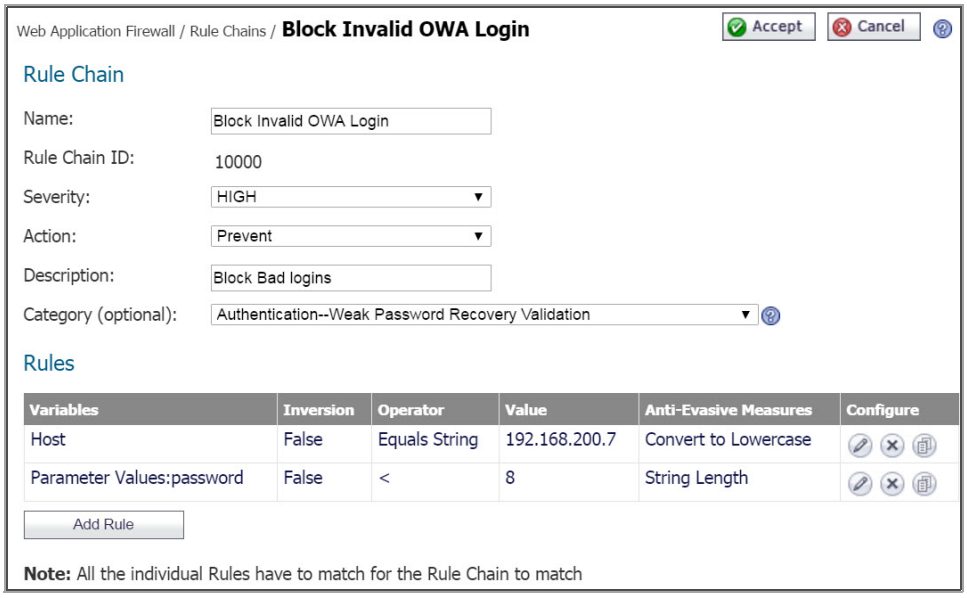
To prevent log in to an Application Offloaded Web site if the length of the password is less than 8 characters, you would create a rule chain containing the following two rules:

1 Select **Host** as the **Variable** and click **+** to add it, set the **Operator** to **Equals String**, and set **Value** to the Virtual Host name of the portal. This checks that the Host header of the login request matches the site you are trying to protect. In this case, the rule chain is only being applied to one site.

2 Select **Parameter Value** as the **Variable** and type **password** into the selection field, then click + to add the variable and selected item to the rule, set the **Operator** to **<** (less than), and set **Value** to **8**. Select **String Length** in the **Anti-Evasive Measures** list to compute the length of the password form parameter.

The action for the rule chain would be set to **Prevent**. Example Rule Chain – Blocking Bad Logins shows the rule chain for this example.

Example Rule Chain – Blocking Bad Logins



Example – Positive Security Model: Blocking a Form Submission with Unwanted Parameters

This rule chain blocks a form submission if the form has a request parameter other than **formId** or if the value of **formId** contains more than four digits. To accomplish this, you would need two rule chains:

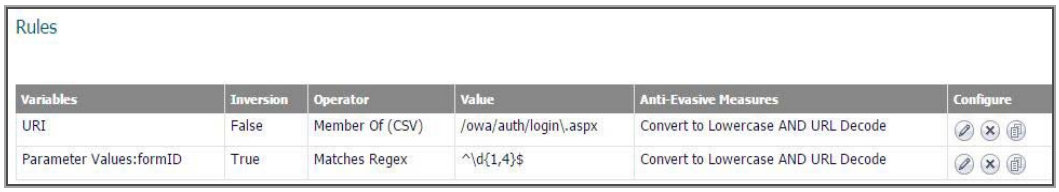
1 The first rule chain contains two rules:

- The first rule identifies the URL where the form is submitted.
- The second rule checks if **Parameter Names** does not match the name of the valid parameter, **formId**. It uses the **Equals String** operator with the **Not** inversion check box selected.

2 The second rule chain contains two rules:

- The first rule identifies the URL where the form is submitted.
- The second rule checks if the value contained by the **Parameter Value: formId** variable matches the regular expression **^\d{1,4}$** which matches anything that consists of one to four digits. The

Not inversion check box is selected to change the rule to match anything that does not consist of one to four digits.


Rules

Variables	Inversion	Operator	Value	Anti-Evasive Measures	Configure
URI	False	Member Of (CSV)	/owa/auth/login\.aspx	Convert to Lowercase AND URL Decode	
Parameter Values:formID	True	Matches Regex	^\d{1,4}$	Convert to Lowercase AND URL Decode	

Example – Negative Security Model: Blocking Malicious Input to a Form

To block malicious input to a form, you would create a rule chain containing the following two rules:

1 The first rule identifies the URL for the form.

2 The second rule identifies the form parameter, **shell_cmd** and the bad input, **traceroute**.

Variables	Inversion	Operator	Value	Anti-Evasive Measures	Configure
URI	False	Matches Regex	/exec.cgi	Convert to Lowercase AND URL Decode	
Parameter Values:shell_cmd	False	Equals String	traceroute	Convert to Lowercase AND URL Decode	

Example – Using URL Decode and None

If a hacker perceives that a Request URI is being scanned for CR and LF characters (carriage return and line feed), the hacker might attempt to sneak those characters into the request by completing URL encoding on the characters before adding them to the request. The URI then contains **%0D** and **%0A** characters that could be used to launch an HTTP response splitting attack. The **URL Decode** and/or **URL Decode (Unicode)** measures can be used to thwart this type of attack by decoding the scanned input before comparing it against the configured value(s) to check for a match.

Specifically, if a request is made to the URI http://www.host.com/foo%20bar/ and the **URL Decode** measure is selected, the scanned URI becomes http://www.host.com/foo bar/ after decoding that can now be safely matched. To thwart a hacker who sends a non-encoded request in addition to the encoded one, the administrator can select the **None** and the **URL Decode** options in the rule.

Example – Using Convert to Lowercase and URL Decode with Parameter Values

An administrator wants to check whether the content of the variable **Parameter Values** matches the value **foo bar** in order to block such a request. Because the backend application accepts case-insensitive inputs (foo bar and FOO BAR), the hacker can pass **foo BAR** in the request and evade the rule. To prevent this evasion, the administrator specifies **Convert to Lowercase** as an anti-evasive measure and configures the value as **foo bar** in all lower case. This causes all request parameter values to be converted to lower case and compared against the value for a case-insensitive check.

Similarly, the hacker could pass **foo%20BAR**, which is the URL encoded version typically used by browsers. To prevent this evasion, the administrator specifies **URL Decode** as the anti-evasive measure to apply to the request entity. The input **foo%20BAR** is URL decoded to **foo BAR**. If the input is already **foo BAR**, then URL decoding is not applied.

Example – Using String Length and URL Decode with Parameter Values:ID

Comparing against a decoded input allows the administrator to use the **String Length** measure to check the length of the input against the matching variable. For example, if a Web application ID parameter should not be more than four characters, the administrator could select **Parameter Values** in the **Variable** field, enter **ID** in the selection field, click **+** to add the variable and selected item to the rule, enter **4** in the **Value** field, select **>** in the **Operator** list, and select both **URL Decode** and **String Length** in the **Anti-Evasive Measures** list.

Deleting a Rule

To delete a rule from a rule chain:

1. On the **Web Application Firewall > Rules** page, click the Edit Rule Chain icon under **Configure** for the rule chain from which you want to delete a rule. The page for that rule chain opens.
2. Click the Delete icon under **Configure** for the rule you want to delete.
3. Click **OK** in the confirmation dialog box.
4. Click **Accept**.

Cloning a Rule

To clone a rule:

1. On the **Web Application Firewall > Rules** page, click the Edit Rule Chain icon under **Configure** for the rule chain which contains the rule you want to clone. The page for that rule chain opens.
2. Click the Clone icon under **Configure** for the rule you want to clone.
3. Click **OK** in the confirmation dialog box.

You can now edit the rule to customize it. See Adding or Editing a Rule on page 320.

Adding or Editing a Rule

To add or edit a rule in a rule chain:

1. Click the Edit Rule Chain icon under **Configure** for the rule chain on which you want to add or edit a rule. The page for that rule chain opens.
2. Click **Add Rule** to add a new rule, or click the Edit icon under **Configure** for the rule you want to edit.
3. In the Add Rule page or the page for the edited rule, select a variable from the **Variables** drop-down list. See About Variables on page 313 for information about the available variables.
4. If the chosen variable is a collection of variables, a selection field is displayed to the right of the **Variables** field, after the colon. If you wish to make a comparison against a particular member of the collection, type the name of that item into the selection field.

   To test the collection itself against an input, leave the selection field blank. For example, to test whether a certain parameter exists in the request, you could select the **Parameter Names** variable and then type the specific parameter name into the **Value** field (but not into the variable selection field).
5. Click **Plus** [+] to add the variable to the rule. Repeat Step 2 through Step 5 to add more variables.

   To delete a variable, select it in the large text box and click **Minus** [-].
6. Select a string or arithmetic operator from the **Operators** drop-down list. To complete the inverse operation, select **Not**.
7. In the **Value** field, type in the value to be compared with the selected variable(s) in the scanned HTTP(S) input. If you selected the **Matches Keyword** operator, you can compare the input against multiple values by typing in each value separated by a space. Each value is compared individually.
8. Select one or more measures from the **Anti-Evasive Measures** list. Hold **Ctrl** on your keyboard while clicking to select multiple measures.

9 Click **Accept** when finished.

Using Web Application Firewall Monitoring

The **Web Application Firewall > Monitoring** page provides two pages: **Local** and **Global**. The pages for both display statistics and graphs for detected/prevented threats over time and top 10 threats. The Local page also displays Web server status statistics and graphs of the number of requests and the amount of traffic during the selected monitoring period.

The monitoring functions of each page are explained in the following sections:

- Monitoring on the Local page on page 321
- Monitoring on the Global page on page 326

Monitoring on the Local page

The Local page displays statistics and graphs for the local appliance. Graphs are displayed for Web Server Status and WAF Threats Detected & Prevented. For the latter, you can use the Perspective options to change the view between Signature, Severity, and Server, and you can display the statistics in list format rather than as graphs.

Using the Control Buttons

The control buttons are displayed at the top of the page. They control the statistics that are displayed on this page. On the Local page, you can use the control buttons to turn streaming updates on or off, refresh the data on the page, clear the graphs, and download a report. If streaming is turned on, Web Application Firewall statistics information is fetched periodically, and displayed in the graphs and threat list. If streaming is turned off, no new information can be displayed.

To use the control buttons, complete the following steps:

1 Select the **Local** page. The active page name is displayed in red or pink, while the inactive page name is blue. The control buttons act on the page that is currently displayed.

2 To turn streaming on or off, click the **ON** or **OFF** indicator next to **Streaming Updates**.

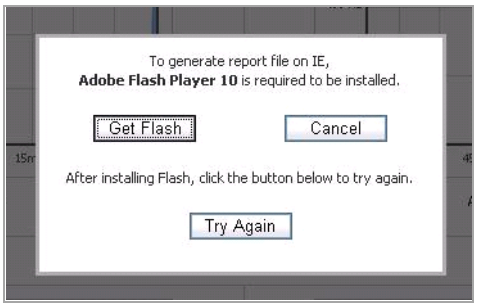
3 To refresh the display, click **Refresh**.

4 To clear all Web Application Firewall statistics from the graphs and list, click **Clear Graphs**.

5 To generate a PDF report containing Web Application Firewall statistics, click **Download Report**.

NOTE: Internet Explorer requires Adobe Flash Player version 10 or higher to generate the report.

6 If prompted to install Adobe Flash Player, click **Get Flash** and then after the installation click **Try Again** to generate the PDF report from Internet Explorer.



Monitoring Web Server Status

On the **Local** page, below the control buttons, this page displays graphs for Web server status. One graph shows the number of Web requests detected over time, and another graph shows the amount of traffic in kilobytes (KB).

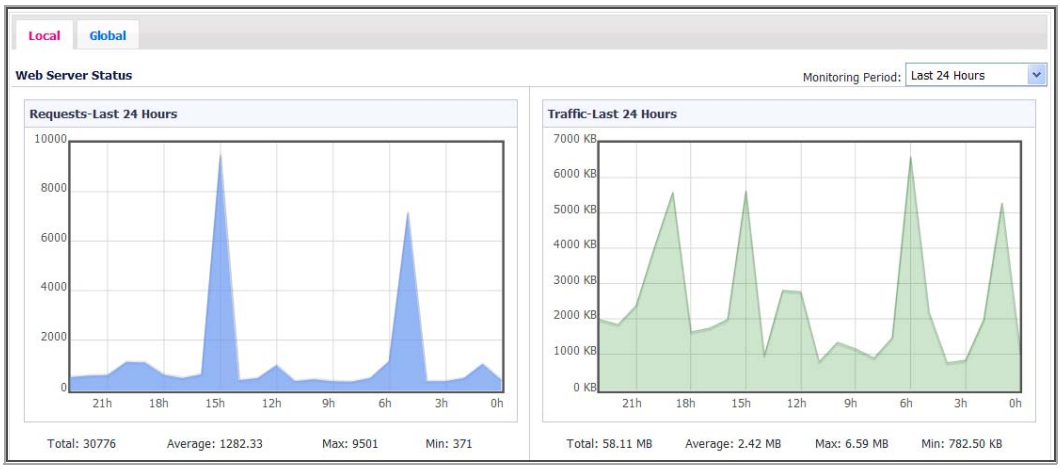
The Web servers tracked are those servers within the local network of the SMA/SRA appliance that provide HTTP/HTTPS bookmarks, offloaded applications, and other Web services. The Traffic graph indicates the amount of HTTP/HTTPS payload data that is sent to client browsers.

You can view Web server activity on the **Local** page over different time periods by selecting one of the following options from the **Monitoring Period** drop-down list:

- Last 60 Seconds
- Last 60 Minutes
- Last 24 Hours
- Last 30 Days

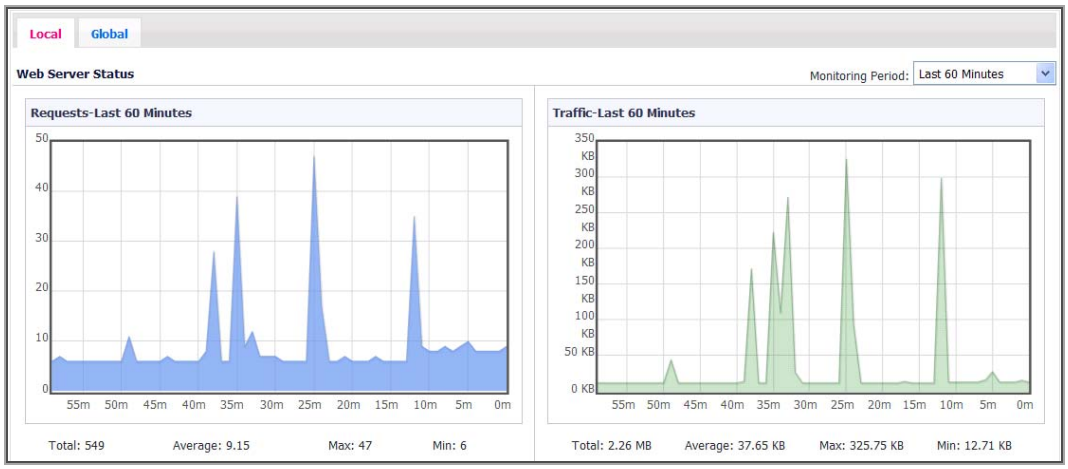
Web Server Status For Last 24 Hours shows a 24 hour period of Web server activity.

Web Server Status For Last 24 Hours



Web Server Status For Last 60 Minutes shows a 60 minute period of Web server activity.

Web Server Status For Last 60 Minutes



Monitoring Detected and Prevented Threats

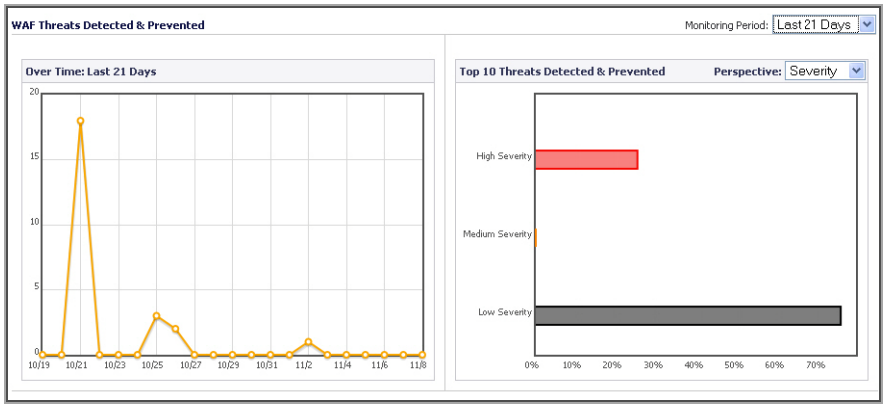
On the **Local** page below the Web server status graphs, the **Web Application Firewall > Monitoring** page displays graphs indicating the number of detected and prevented threats. Two graphs are presented, one showing the number of threats over time, and the other showing the top ten threats that were detected and prevented during that time frame.

You can change the time frame displayed in both graphs or change the view to display all threats in list format by selecting one of the following options from the **Monitoring Period** drop-down list:

- Last 12 Hours
- Last 14 Days
- Last 21 Days
- Last 6 Months
- All in Lists

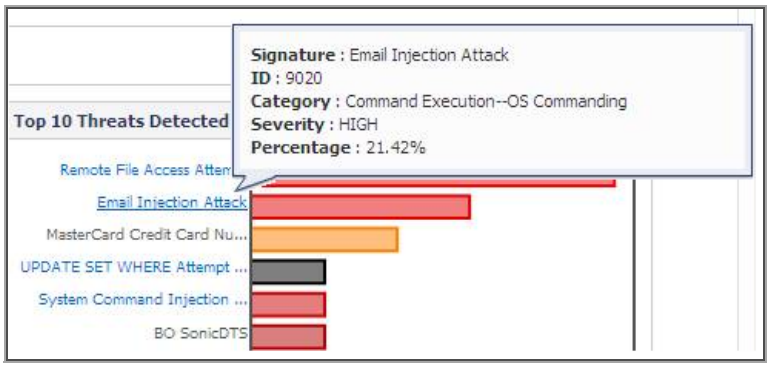
Threats Over Last 21 Days shows the number and severities of threats detected and prevented over the last 21 days.

Threats Over Last 21 Days



When displaying the top 10 threats graph with **Perspective** set to **Signature**, hovering your mouse pointer over the signature ID causes a tooltip to appear with details about the threat.

Threat Details Tooltip



Viewing Threats in List Format

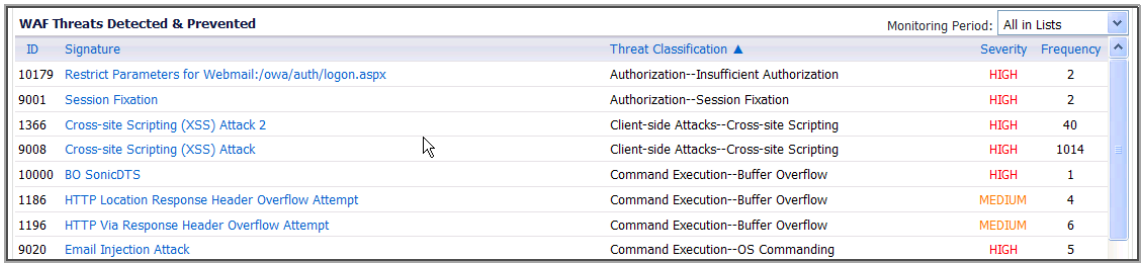
To see the threats in list format rather than as a graph, select **All in Lists** from the **Monitoring Period** drop-down list. Threats in List Format shows the list format.

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

The initial, default sorting order lists the high severity threats with highest frequency values first. You can change the order of listed threats by clicking on the column headings to sort them by ID, signature name, classification, severity, or frequency. Click again to toggle between ascending and descending order. The active sorting column is marked by an arrowhead pointing upwards for ascending order, and downwards for descending order.

Threats in List Format

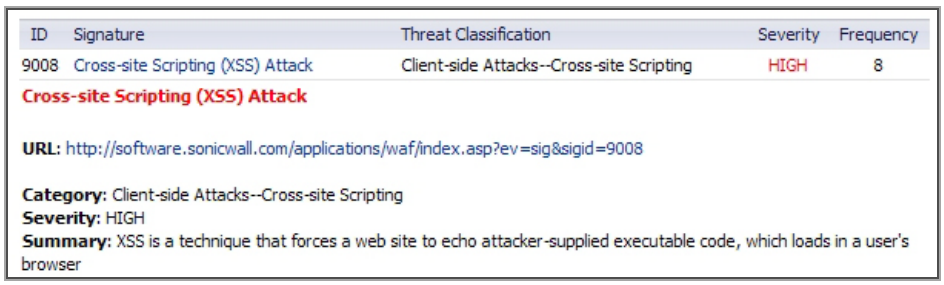


ID	Signature	Threat Classification ▲	Severity	Frequency
10179	Restrict Parameters for Webmail:/owa/auth/logon.aspx	Authorization--Insufficient Authorization	HIGH	2
9001	Session Fixation	Authorization--Session Fixation	HIGH	2
1366	Cross-site Scripting (XSS) Attack 2	Client-side Attacks--Cross-site Scripting	HIGH	40
9008	Cross-site Scripting (XSS) Attack	Client-side Attacks--Cross-site Scripting	HIGH	1014
10000	BO SonicDTS	Command Execution--Buffer Overflow	HIGH	1
1186	HTTP Location Response Header Overflow Attempt	Command Execution--Buffer Overflow	MEDIUM	4
1196	HTTP Via Response Header Overflow Attempt	Command Execution--Buffer Overflow	MEDIUM	6
9020	Email Injection Attack	Command Execution--OS Commanding	HIGH	5

To view and hide threat details:

1. On the **Web Application Firewall > Monitoring page**, select **All in Lists** from the **Monitoring Period** drop-down list. The list of detected or prevented threats is displayed in the **WAF Threats Detected & Prevented** table.
2. To display details about a threat, click on the threat. The details include the following:
   - **URL** – The URL to the SonicWall Inc. 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

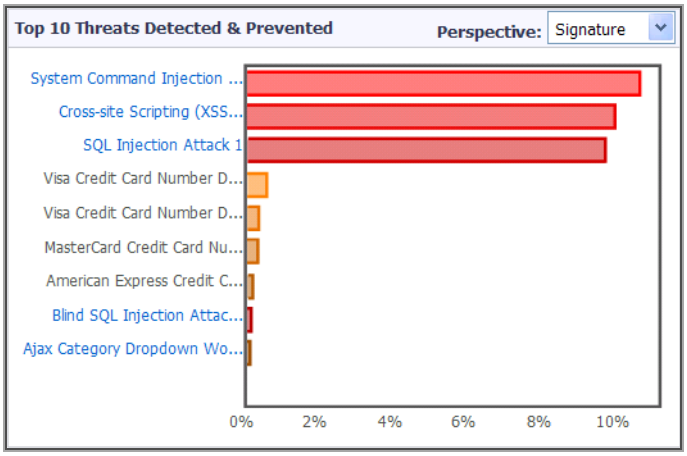


3 To collapse the threat details, click the threat link again.

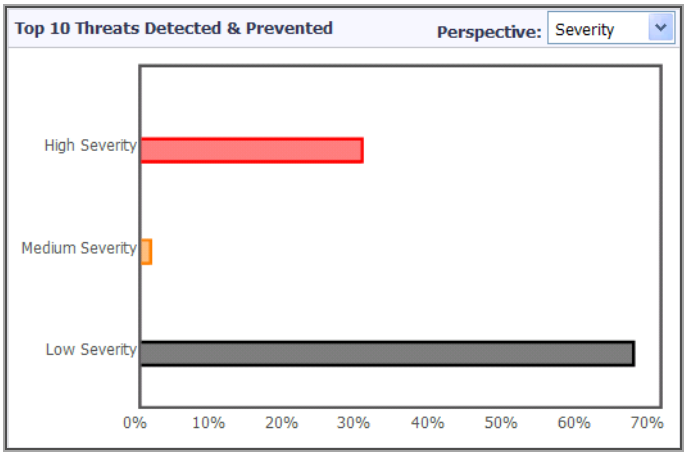
Changing Perspective

For the Top 10 Threats graph, you can select the following display options from the **Perspective** drop-down list:

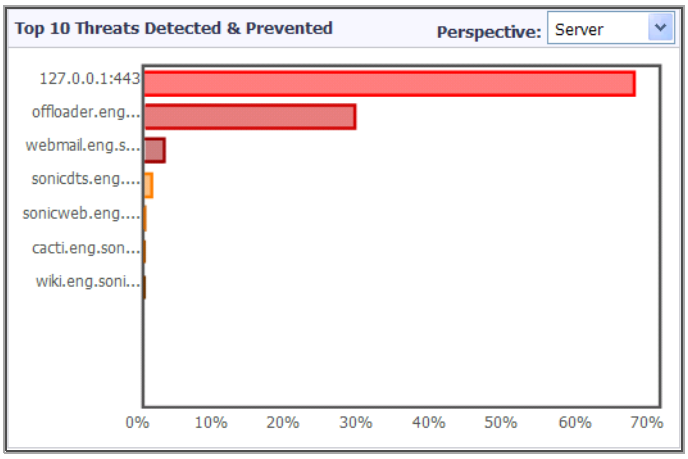
- Signature – The name of each threat shown is listed at the left side of the graph.



- Severity – High, medium, and low severity threats are displayed using color coding.



- Server – The server names are listed at the left side of the graph.

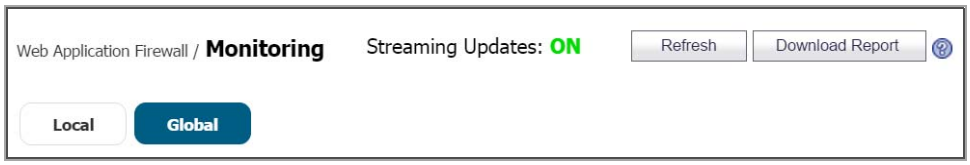


Monitoring on the Global page

The **Global** page displays statistics and graphs for threats reported by all SMA/SRA appliances with Web Application Firewall enabled. Graphs are displayed for WAF Threats Detected & Prevented.

Using the Control Buttons

The control buttons are displayed at the top of the page. They control the statistics that are displayed on this page. On the **Global** page, you can use the control buttons to turn streaming updates on or off, refresh the data on the page, and download a report. If streaming is turned on, Web Application Firewall statistics information is fetched periodically, and displayed in the graphs and threat list. If streaming is turned off, no new information can be displayed.



To use the control buttons, complete the following steps:

1 Select the **Global** page. The active page name is displayed in red or pink, while the inactive page name is blue. The control buttons act on the page that is currently displayed.

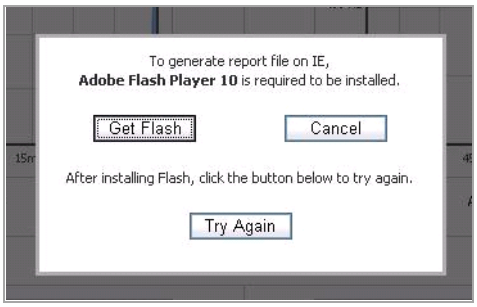
2 To turn streaming on or off, click the **ON** or **OFF** indicator next to **Streaming Updates**.

3 To refresh the display, click **Refresh**.

4 To generate a PDF report containing Web Application Firewall statistics, click **Download Report**.

> **NOTE:** Internet Explorer requires Adobe Flash Player version 10 or higher to generate the report.

5 If prompted to install Adobe Flash Player, click **Get Flash** and then after the installation click **Try Again** to generate the PDF report from Internet Explorer.



Monitoring Detected and Prevented Threats

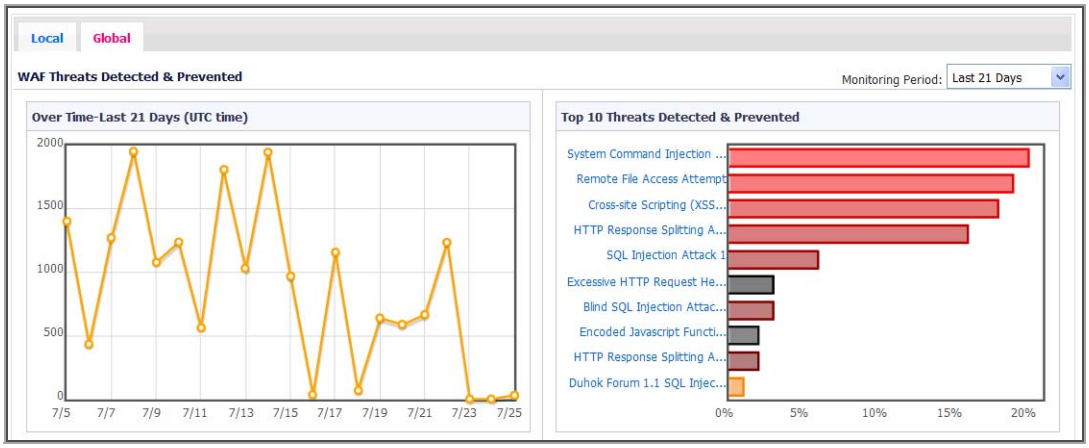
At the top of the **Global** page, the **Web Application Firewall > Monitoring** page displays graphs indicating the number of detected and prevented threats. Two graphs are presented, one showing the number of threats over time, and the other showing the top ten threats that were detected and prevented during that time frame.

You can change the time frame displayed in both graphs by selecting one of the following options from the **Monitoring Period** drop-down list:

- Last 12 Hours
- Last 14 Days
- Last 21 Days
- Last 6 Months

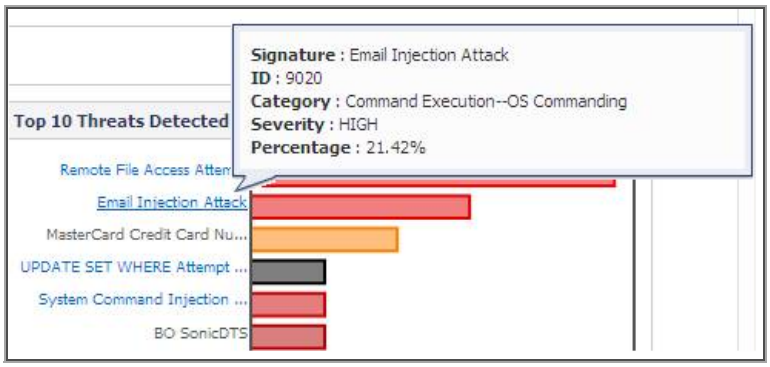
Threats Over Last 21 Days shows the number and severities of threats detected and prevented over the last 21 days.

Threats Over Last 21 Days



Hovering your mouse pointer over the signature ID causes a tooltip to appear with details about the threat.

Threat Details Tooltip

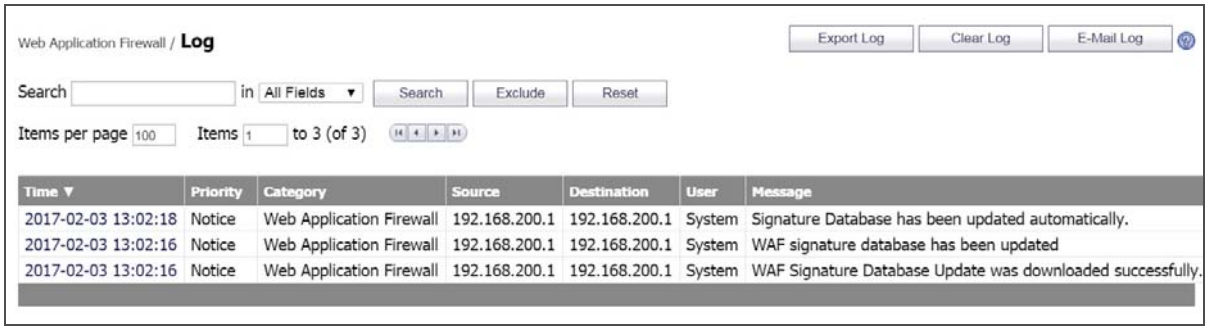


The local signature database on the appliance is accessed to get detailed threat information, but if the database is not up-to-date, some detailed information for the Top 10 Threats might not be available. In this case, the threat color in the graph is light grey, and the severity is displayed as unknown in the tooltip for this threat. The following error message is also displayed below the graphs:

"Warning: Web Application Firewall Signature Database for this device is not current. Synchronize the Database from the **Web Application Firewall > Status** page"

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 on page 328
- Controlling the Log Pagination on page 329
- Viewing Log Entry Details on page 329
- Exporting and Emailing Log Files on page 330
- Clearing the Log on page 330

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:

1. On the **Web Application Firewall > Log** page, type the value to search for into the **Search** field.
2. Select the column in which to search from the drop-down list to the right of the Search field.
3. Do one of the following:
   - To start searching for log entries containing the search value, click **Search**.
   - 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, complete the following steps:

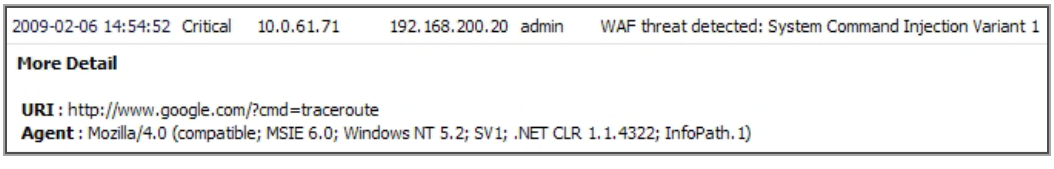
1. On the **Web Application Firewall > Log** page, enter the number of log entries that you want on each page into the **Items per Page** field. The Log page display changes to show the new number of entries.
2. To view the log entries beginning at a certain number, type the starting number into the **Item** field and press **Enter** on your keyboard.
3. To view the first page of log entries, click the left-most button in the arrow control pad.
4. To view the previous page of log entries, click the left arrow in the arrow control pad.
5. To view the next page of log entries, click the right arrow in the arrow control pad.
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:

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.



2. To collapse the details for a log entry, click again on the entry.

Exporting and Emailing Log Files

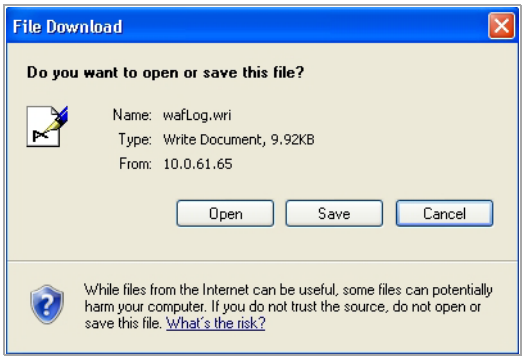
You can export the current contents of the Web Application Firewall log to a file, or email the log contents by using the buttons in the top right corner of the **Web Application Firewall > Log** page.

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 Secure Mobile Access management interface. If no address is configured, the Status line at the bottom of the browser displays an error message when you click **E-Mail Log** on the **Web Application Firewall > Log** page.

To export or email the log:

1 To export the log contents, click **Export** in the top right corner of the **Web Application Firewall > Log** page. The File Download dialog box is displayed.



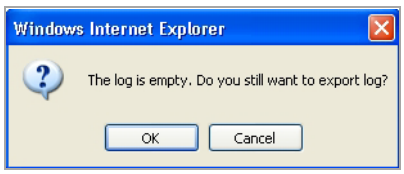
2 In the File Download dialog box, do one of the following:

- 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**.

3 To email the log contents, click **E-Mail Log** 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 causes a confirmation dialog box to display.



To clear the Web Application Firewall log:

1 On the top right corner of the **Web Application Firewall > Log** page, click **Clear**.

2 Click **OK** in the confirmation dialog box.

Verifying and Troubleshooting Web Application Firewall

One way to verify the correct configuration of Web Application Firewall is by viewing the **Web Application Firewall > Monitoring** page. This page displays statistics and graphs for detected/prevented threats over time and top 10 threats. The **Local** page also displays Web server status statistics and graphs of the number of requests and the amount of traffic during the selected monitoring period. 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 - Restarting the appliance could 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 might 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 is used by SonicWall Inc. 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 **Apply** 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 **Apply** on the **Web Application Firewall > Status** page.

- WAF engine is being started with the factory default signature database.

  The Web Application Firewall engine is using the factory default signature database for traffic inspection. This could 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 because of database errors and as a precautionary measure the factory default database has been used.

13

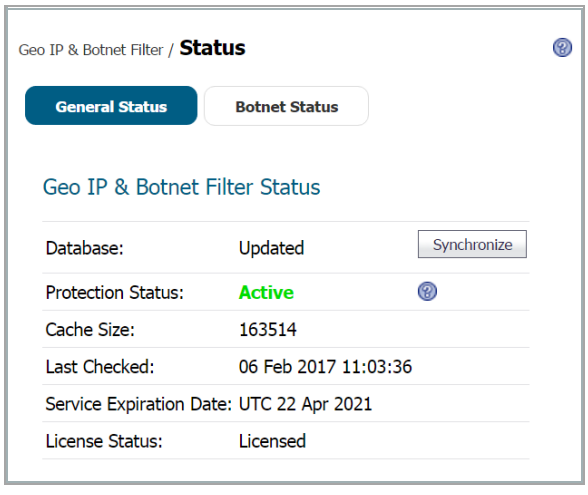
Geo IP and Botnet Filter

This section provides information and configuration tasks specific to the Geo IP and Botnet Filter page on the Secure Mobile Access management interface. The Geo IP feature enables administrators to monitor and enforce policies effectively based on the geographical locations of remote users. The Botnet Filter feature enforces a strong and anti-evasive defense against any rogue activity from Botnets using a dynamically updated database maintained by SonicWall Inc.. Botnets pose huge security risks such as Denial of Service (DoS) attacks and Data Leakage. They are hard to identify and control because of the transient nature of their origins. These features are disabled by default.

Topics:

Status

The **Geo IP & Botnet Filter > Status** page contains two pages of information: General Status and Botnet Status.



See:

General Status

The **General Status** page shows general information about the Geo IP & Botnet filter and offers an option to synchronize the database. When the Geo IP & Botnet Filter is enabled, the General Status page provides the following information:

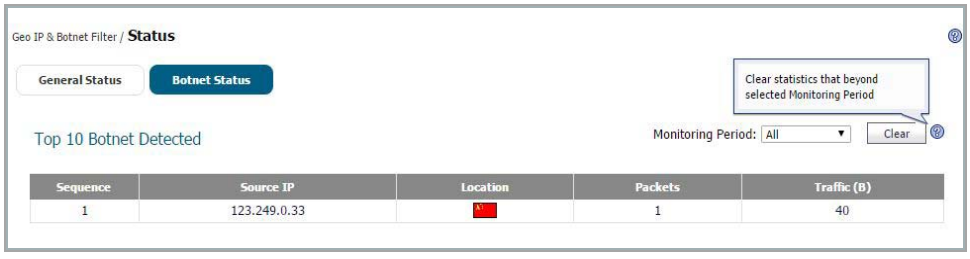
- **Database** shows the update status and provides **Synchronize** to manually synchronize updates. When **Synchronize** is clicked, the server immediately checks for new updates on the backend server.
- **Server Status** shows whether the backend server is connected. Offline status might indicate that the network settings need to be changed.
- **Cache Count** shows the total number of Geo IP and Botnet caches. All caches are managed automatically by the server.
- **Last checked** displays the most recent timestamp of the cache.
- **Service Expiration Date** shows the license expiration date of the Geo IP & Botnet Filter service.
- **License Status** identifies whether the Geo IP & Botnet Filter service is licensed. The Geo IP & Botnet Filter is a subscription service that includes a free trial.

When the Geo IP & Botnet Filter is licensed but disabled, the Status page displays a warning that contains a link to the Settings page where the feature can be enabled:

Botnet Status

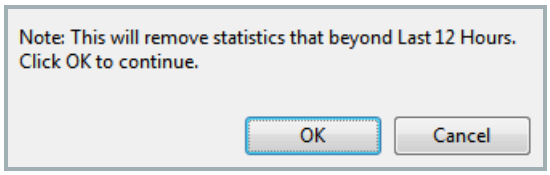
The **Botnet Status** page shows traffic statistics for Botnet IP addresses for the current reporting period. Statistics are shown for the top 10 IP addresses detected by the Botnet Filter during the selected period.

NOTE: If the location of an IP address changes, each location is shown as a different IP address and statistics are divided.



Use the **Monitoring Period** drop-down list to select the reporting period: Last 12 Hours, Last 14 Days, Last 21 Days, Last 6 Months, or All recorded traffic data.

Click **Clear** to clear statistics that are beyond the selected Monitoring Period. Before clearing, a popup window displays to confirm the clear action:



TIP: Clear should be used in conjunction with the Monitoring Period. For example, if **Last 12 Hours** is selected for the Monitoring Period, when clicking **Clear**, all histories that are beyond the "Last 12 Hours" are cleared, while the latest "Last 12 Hours" histories are kept.

Settings

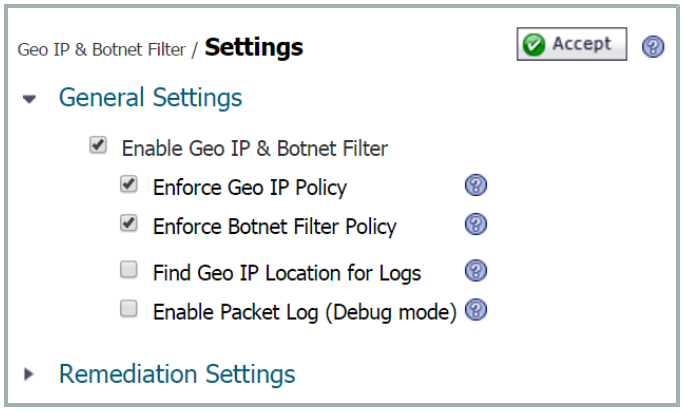
The **Geo IP & Botnet Filter > Settings** page is used to enable/disable the Geo IP and Botnet Filter and configure Remediation Settings. The **Geo IP & Botnet Filter > Settings** page contains these pages:

- General Settings on page 335
- Remediation Settings on page 336

General Settings

Use the General Settings section of the **Geo IP & Botnet Filter > Settings** page to globally enable or disable the Geo IP & Botnet Filter that is disabled by default.

NOTE: An IP address can be manually identified as a Botnet IP address by using the **Botnet Test** diagnostic tool accessed from the **System > Diagnostics** page.



To enable the Geo IP & Botnet Filter:

1. Select **Enable Geo IP & Botnet Filter** to globally enable this feature. When enabled, a Location column is added to the **NetExtender > Status**, **Virtual Assist > Status**, **Virtual Meeting > Status**, and **User > Status** pages that identifies the location of users' source IP addresses. Mousing over an icon in the Location column displays the City (if applicable), Region, and Country of the source IP.
2. Click **Accept**.

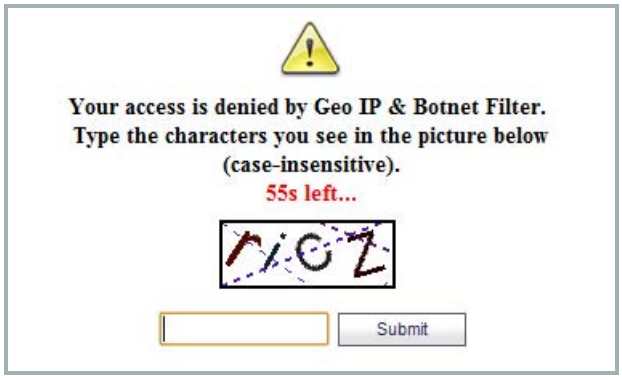
When this feature is enabled, the General Settings section displays four sub-features that can be individually enabled or disabled:

- **Enforce Geo IP Policy** — Select this option to enforce Geo IP policies.
- **Enforce Botnet Filter Policy** — Select this option to enable blocking of IP addresses in the SonicWall Botnet Database (for which no defined Policy is required) and enforce Botnet Filter policies. If this is disabled, Botnet IP addresses are not blocked, however, they are still detected and included in the Botnet Filter Statistics.
- **Find Geo IP Location for Logs** — When this option is enabled, a column indication the location of the source IP is added to the following screens: **End Point Control > Log**, **Web Application Firewall > Log**, **Geo IP & Botnet Filter > Log**, and **Log > Views**.
- **Enable Packet Log (Debug mode)** — Select this option to generate logs for allowed or denied packets. This option is for debug purposes only. Enabling the Packet Log makes logs increase rapidly if the log level is set to Debug.

Remediation Settings

Access to resources protected by an SMA/SRA appliance from aggressive IP addresses is denied when Geo IP & Botnet Filter is enabled. Remediation provides valid users an opportunity to prove that they are real users rather than “bots” and be allowed access.

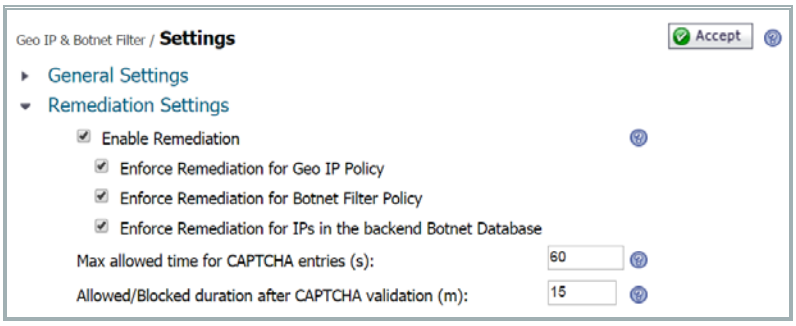
For web access, user are redirected to the CAPTCHA page, as shown in the following figure. A countdown timer tells the time that remains for the user to complete remediation. The user must finish remediation within the allotted time, otherwise the user IP address is added to the block list and all access from that IP address is blocked for a period of time.



If remediation is successful within the verification time, the user is directed to the requested page. A CAPTCHA session is then created to record the remediation status. During the valid duration, all access from the IP address is allowed. After the valid duration, the CAPTCHA session expires. If the user is still logged in, access is not interrupted, but after the user login session expires the CAPTCHA session is deleted and remediation is required again.

To enable Remediation and configure the settings:

1 Click **Remediation Settings**.



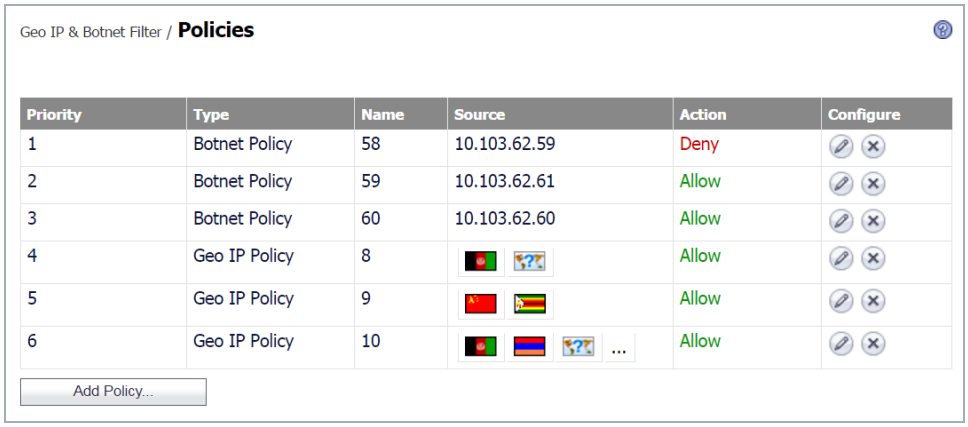
2 Click **Enable Remediation**. Denied users cannot access resources protected by the appliance without CAPTCHA-based remediation. Remediation can be enforced separately for the IP addresses defined by your Geo IP Policy, Botnet Filter Policy, and/or in the backend Botnet Database. Select additional options as needed.

3 In the **Max allowed time for CAPTCHA entries (s)** field, enter the number of seconds that the user has to complete Remediation. The minimum/maximum range is 30-300 seconds, the default is 60 seconds.

4 In the **Allowed/Blocked duration after CAPTCHA validation (m)** field, enter the number of minutes that the user is allowed/blocked after completing the CAPTCHA validation. The minimum value is five minutes and the maximum is 30, the default is 15 minutes.

Access Policies

The **Geo IP & Botnet Filter > Policies** page is used to view, add, edit, and delete Geo IP and Botnet Filter access policies. Up to a total of 64 Geo IP and Botnet Filter access policies can be created.



Each policy is automatically assigned a different priority with 1 being the highest priority. A policy's priority determines the order of enforcement, which is identified by the order policies are listed on the Settings page.

- Botnet Filter policies have a higher priority than Geo IP policies. Geo IP policies are prioritized according to the time they were created with those created first having the higher priority.
- Botnet Filter policies defined for a single IP address have a higher priority than Botnet Filter policies defined for a subnet, and each type is then prioritized based on the time they were created with those created first having the higher priority.

- Custom created policies are enforced first, which means if an IP address is listed in the SonicWALL Botnet Filter database, but the administrator defines an allow policy for this IP, then access from this IP is allowed.

A policy can be modified by clicking the edit button, but a policy name cannot be modified.

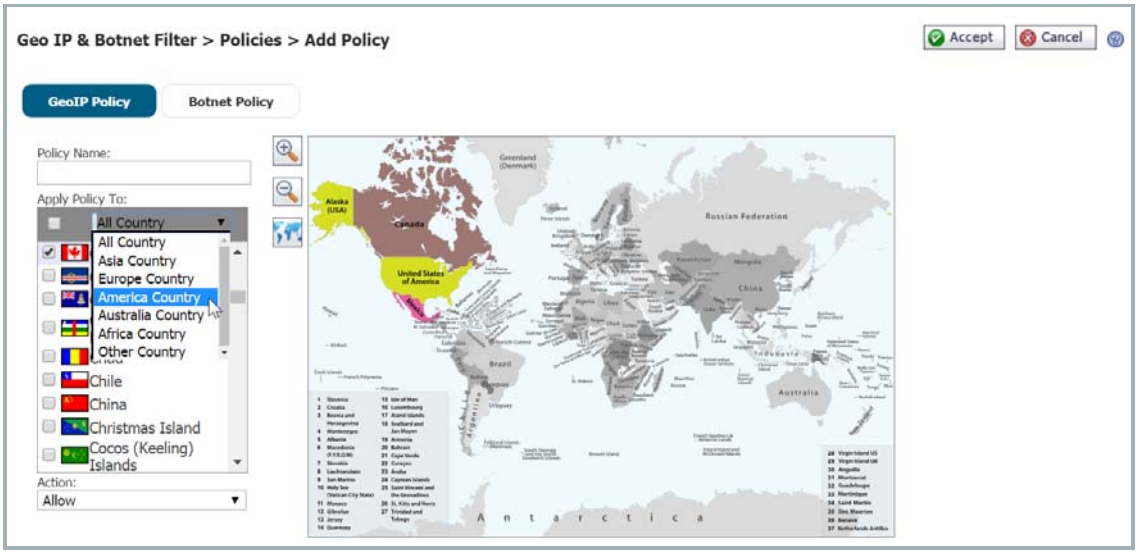
A policy can be deleted by clicking the delete button.

To create a new access policy, click the **Add policy...** button. Two types of policies can be added:

- **Geo IP Policy** tab

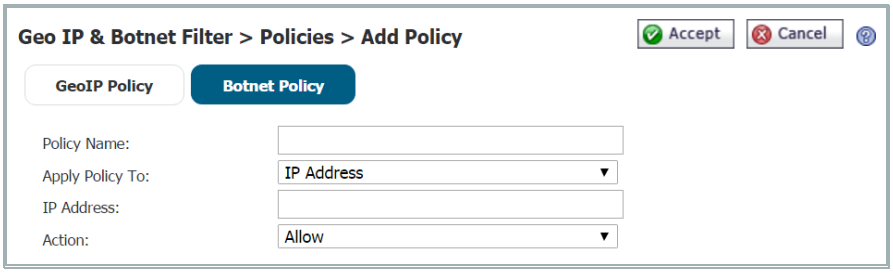
  A Geo IP policy allows or denies traffic from specified countries. Enter a **Policy Name**, then select the **Countries** you want to allow or deny. You can sort countries by continent, just click the drop-down and select the desired continent, to display all the countries within that continent in the **Apply Policy To** list. You can also select countries directly from the map.

  The map displays selected/deselected countries by color. The deselected countries display gray, while the selected countries display in color. Mouse over a country in the **Apply Policy To** list and the corresponding country blinks on the map. Use the Zoom tool to zoom in or out on the map. If you do not wish to use the map, hide it by clicking the **Map** icon to the left of the map.



- **Botnet Policy**

  A Botnet Policy allows or denies access from a specified IPv4 IP address or IP address range. Up to 64 policies can be created. Enter a **Policy Name**, then select an **IP address or IP range** you want to allow or deny (based on your selection in the Action drop-down.



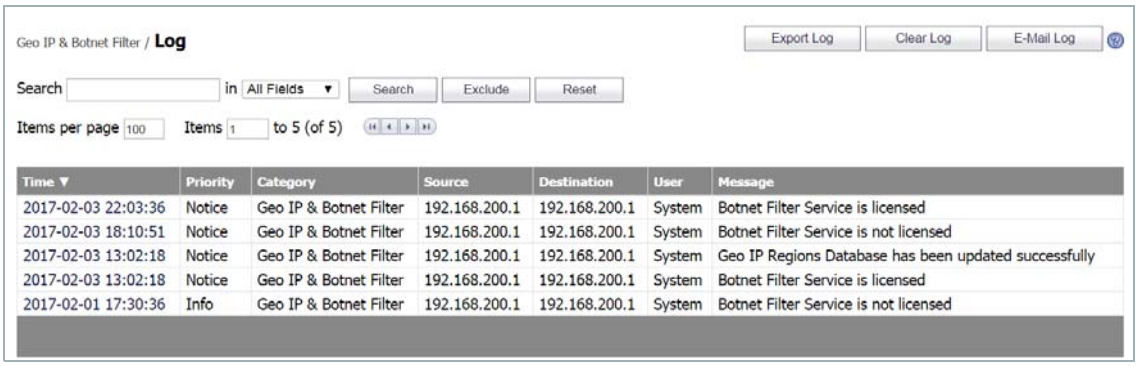
Log

The **Geo IP & Botnet Filter > Log** page lists information detected by the Geo IP & Botnet Filter:

- Location information that identifies the geographical location of the source IP for each event log message generated by Geo IP. Location information is also displayed on applicable Secure Mobile Access log and status pages. If Geo IP logging is disabled, this column contains a Not Logged icon. If a location or country flag is not available, this column contains an Unknown icon.

  Mousing over an icon in the Location field displays the City (if available), Region, and Country of the source IP.

- Traffic detected by the Botnet Filter. Traffic from each IP is logged only one time per second, no matter if it is denied or allowed.



Several functions can be completed on this page, including a flexible search mechanism and the ability to export the log to a file or email it.

- Click on a log entry displays more information about the event, if available.
- Click on any of the headings to sort the log messages alphabetically by heading.

Searching the Log

Search for a value contained in a specific column of the log table or search for log entries that do **not** contain the specified value.

To view and search the log:

1. On the **Geo IP & Botnet Filter > Log** page, type the value to search for into the **Search** field. The search value is case sensitive.
2. Select the column in which to search from the drop-down list to the right of the Search field.
3. Do one of the following:
   - To start searching for log entries containing the search value, click **Search**.
   - To start searching for log entries that do not contain the search value, click **Exclude**.
   - To clear the Search field 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:

1. On the **Geo IP & Botnet Filter > Log** page, enter the number of log entries that you want on each page into the **Items per Page** field. The Log page changes to show the new number of entries.
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.
3. To view the first page of log entries, click the left-most button  in the arrow control pad.
4. To view the previous page of log entries, click the left arrow  in the arrow control pad.
5. To view the next page of log entries, click the right arrow  in the arrow control pad.
6. To view the last page of log entries, click the right-most button  in the arrow control pad.

Exporting and Emailing Log Files

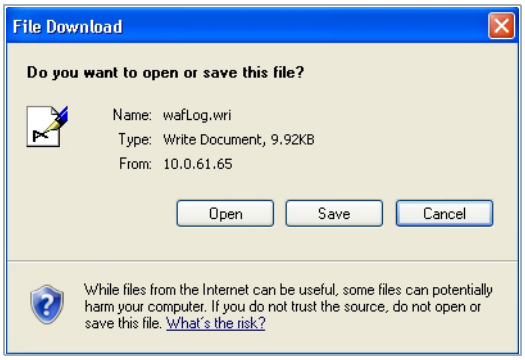
You can export the current contents of the log to a file, or email the log contents by using the buttons in the top right corner of the **Geo IP & Botnet Filter > Log** page.

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 Secure Mobile Access management interface. If no address is configured, the Status line at the bottom of the browser displays an error message when you click **E-Mail Log**.

To export or email the log:

1 To export the log contents, click **Export** in the top right corner of the **Geo IP & Botnet Filter > Log** page. The File Download dialog box is displayed.



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**.

3 To email the log contents, click **E-Mail Log** in the top right corner of the **Geo IP & Botnet Filter > 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 log on the **Geo IP & Botnet Filter > Log** page. The entries on the page are removed, and any attempt to export or email the log file while it is still empty causes a confirmation dialog box to display.

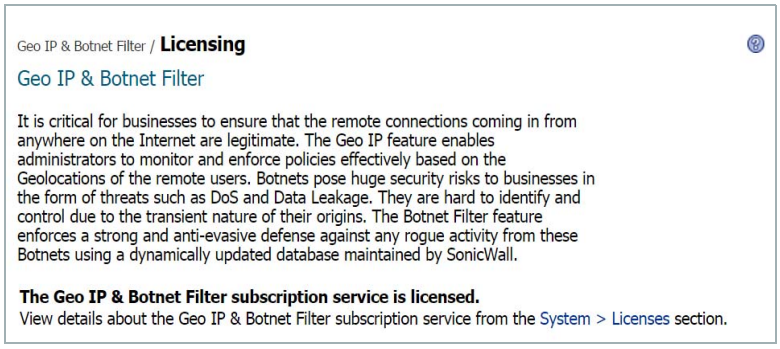
To clear the log, complete the following steps:

1 On the top right corner of the **Geo IP & Botnet Filter > Log** page, click **Clear**.

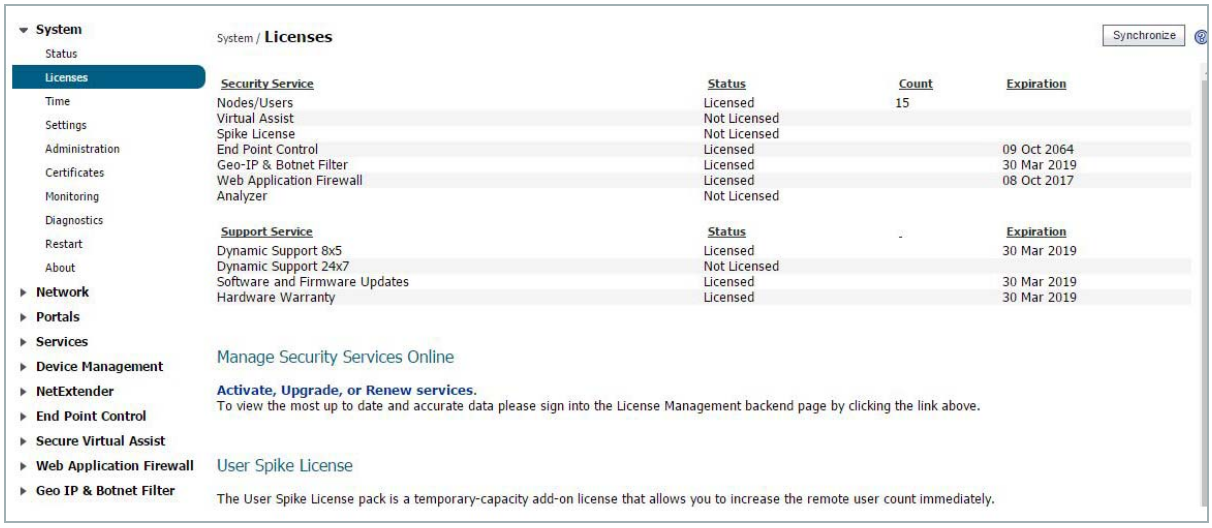
2 Click **OK** in the confirmation dialog box.

Licensing

Geo IP & Botnet Filter is a subscription service that includes a free trial that expires one year after the release date. The licensing status of the Geo IP & Botnet Filter subscription service is shown on the **Geo IP & Botnet Filter > Licensing** page.



The Licensing page also includes a brief description of the feature and a link to the **System > Licenses** page where you can activate, upgrade, and renew licenses.



14

High Availability Configuration

This section provides information and configuration tasks specific to the **High Availability** page on the Secure Mobile Access web-based management interface.

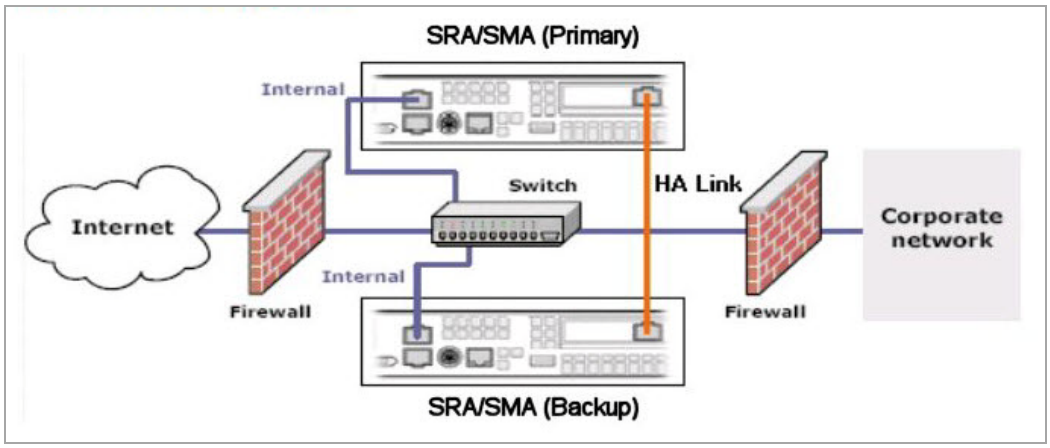
High Availability allows two identical SMA/SRA appliances or SMA 500v Virtual Appliances to provide a reliable, continuous connection to the public Internet. The two SMA/SRA appliances are deployed at the same time and connected together, and are called a High Availability Pair (HA Pair).

Topics:

High Availability Overview

High Availability requires one SMA/SRA appliance configured as the primary device, and an identical SMA/SRA configured as the backup device.

High availability configuration



During normal operation, the primary device is in an active state, and services all connections. The backup device is in an idle state. When the primary device loses connectivity, the backup transitions to the active state and begins to service outside connections. The necessary data is synchronized between primary and backup devices, including settings data and session data.

The failover applies to loss of functionality or network-layer connectivity on the primary appliance. The failover to the backup unit occurs when critical services are affected, physical (or logical) link failure is detected, or when the primary unit loses power.

Stateful High Availability Support

When Stateful High Availability is licensed and enabled, the HA pair provides stateful user authentication failover, as authentication credentials are continuously synchronized in real time between the members of the HA pair. This allows connections initiated by the active device to failover to the backup without requiring the user to authenticate again.

The HA pair does not provide stateful application session failover for sessions such as NetExtender or Virtual Assist. Disruption to users depends on the TCP/IP disconnect tolerance of the applications that they are using at the time the failover occurs.

Supported Platforms

High Availability is supported on the SMA 400, SRA 4600, and the SMA 500v Virtual Appliance.

Configuring High Availability

High Availability (HA) requires one SMA 400, SRA 4600, or SMA 500v Virtual Appliance configured as a primary device and an identical SMA/SRA configured as a backup device. The HA connection between two SMA/SRA appliances is in an Active/Passive state. The session information is synchronized between the HA pair to help avoid re-authentication of users in the event of a failover to the backup device.

See the following sections for configuration information:

- Physical Connectivity on page 344
- Preparing for High Availability on page 344
- Configuring High Availability Settings on a hardware appliance on page 346
- Enabling Interface Monitoring on page 349
- Configuring Network Monitoring Addresses on page 350
- Configuring Management Settings for Idle Unit on page 350
- Synchronizing Firmware on page 351
- Synchronizing Settings on page 351
- Synchronizing Licenses on page 351

Physical Connectivity

You can select the interface to use for HA control traffic. The HA link should connect the identical ports of the SMA/SRA HA Pair, for example X3 of the primary appliance to X3 of the backup appliance.

During normal operation, the primary device is in an active state and services all connections, while the backup device is in an idle state. When the primary device loses connectivity, the backup transitions to the active state and begins to service outside connections.

Preparing for High Availability

Before configuring the options on the **High Availability > Settings** page, prepare your devices for High Availability with the following steps:

1 Configure both SMA/SRA appliances as separate devices with independent IP addresses on your subnet.

NOTE: SMA/SRA appliances in an HA pair cannot be deployed behind a proxy.

2 Upload the latest Secure Mobile Access firmware to both devices. High Availability does not work unless both devices have the same firmware version installed.

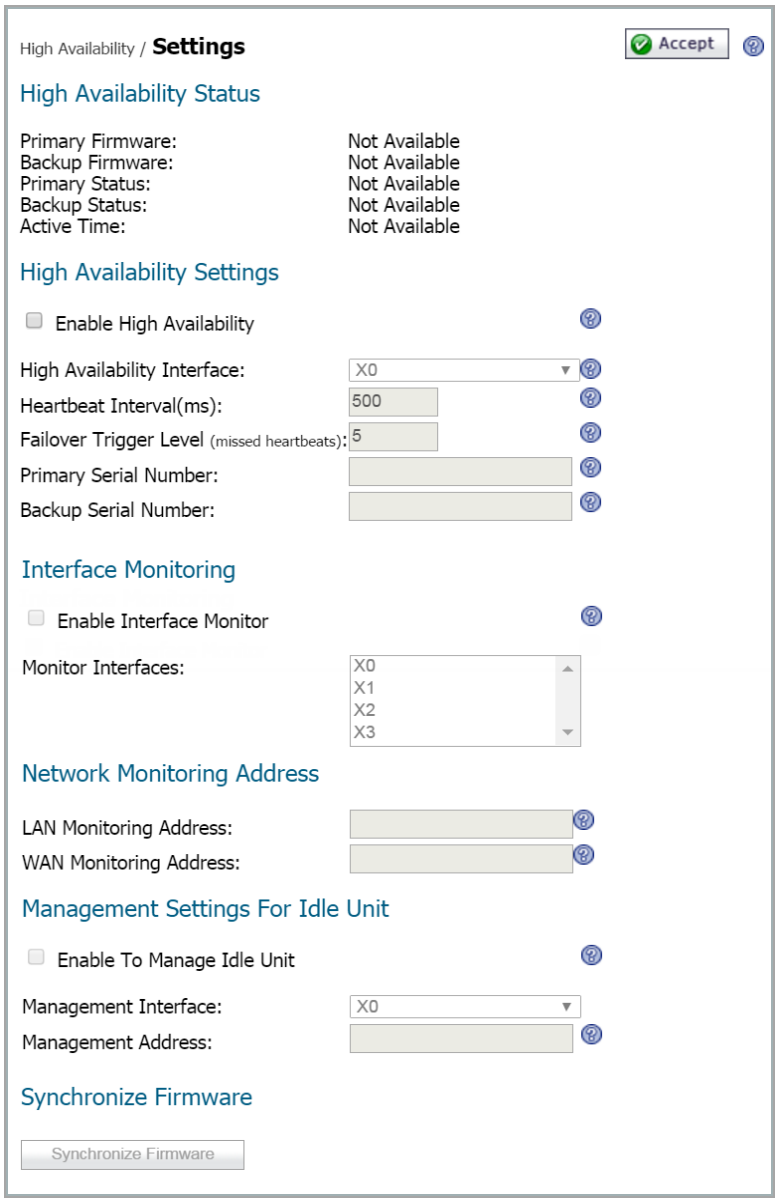
3 Connect the X3 interfaces of the two appliances together with a CAT 5E or better cable to ensure a gigabit connection.

NOTE: SonicWall Inc. recommends that you backup and download the settings for both SMA/SRA appliances at this stage.

4 In a browser, log in to the primary unit and navigate to the **Network > Interfaces** page. Confirm that the X3 port is active by checking the **Status** that should show **1000 Mbps Full Duplex**.

Configuring High Availability Settings on a hardware appliance

The **High Availability > Settings** page provides settings for configuring High Availability.



NOTE: The contents of this page vary slightly for a Virtual Appliance, as explained in Configuring High Availability Settings on a Virtual Appliance on page 348.

To enable High Availability and configure the options in the High Availability Settings section:

1. In a browser, log in to the primary unit and navigate to the **High Availability > Settings** page.
2. Select **Enable High Availability**.

   The HA interface can only be set when the unit is in the HA unconnected mode, and both units must be set to the same interface.

3 Select the **High Availability Interface** from the drop-down list. The HA interface can only be set when the unit is in the HA unconnected mode, and the interface must be set to the same interface on both units.

4 Enter a number of milliseconds for the **Heartbeat Interval**. The heartbeat is used to test the connectivity between the primary and backup devices. The heartbeat interval controls how often the two units communicate. The minimum is 500 milliseconds (a half second), and the maximum is 300,000 milliseconds (five minutes).

5 Enter a value for the **Failover Trigger Level**. This is the number of heartbeats that must be missed before failover occurs. The minimum is four, and the maximum is 99.

6 In the **Primary Serial Number** field, type in the serial number of the primary device. The maximum length is 12 characters.

7 In the **Backup Serial Number** field, type in the serial number of the backup device. The maximum length is 12 characters.

8 Click **Accept**.

9 In the browser, open a new page and point it to the IP address of the backup unit. Log in to the backup.

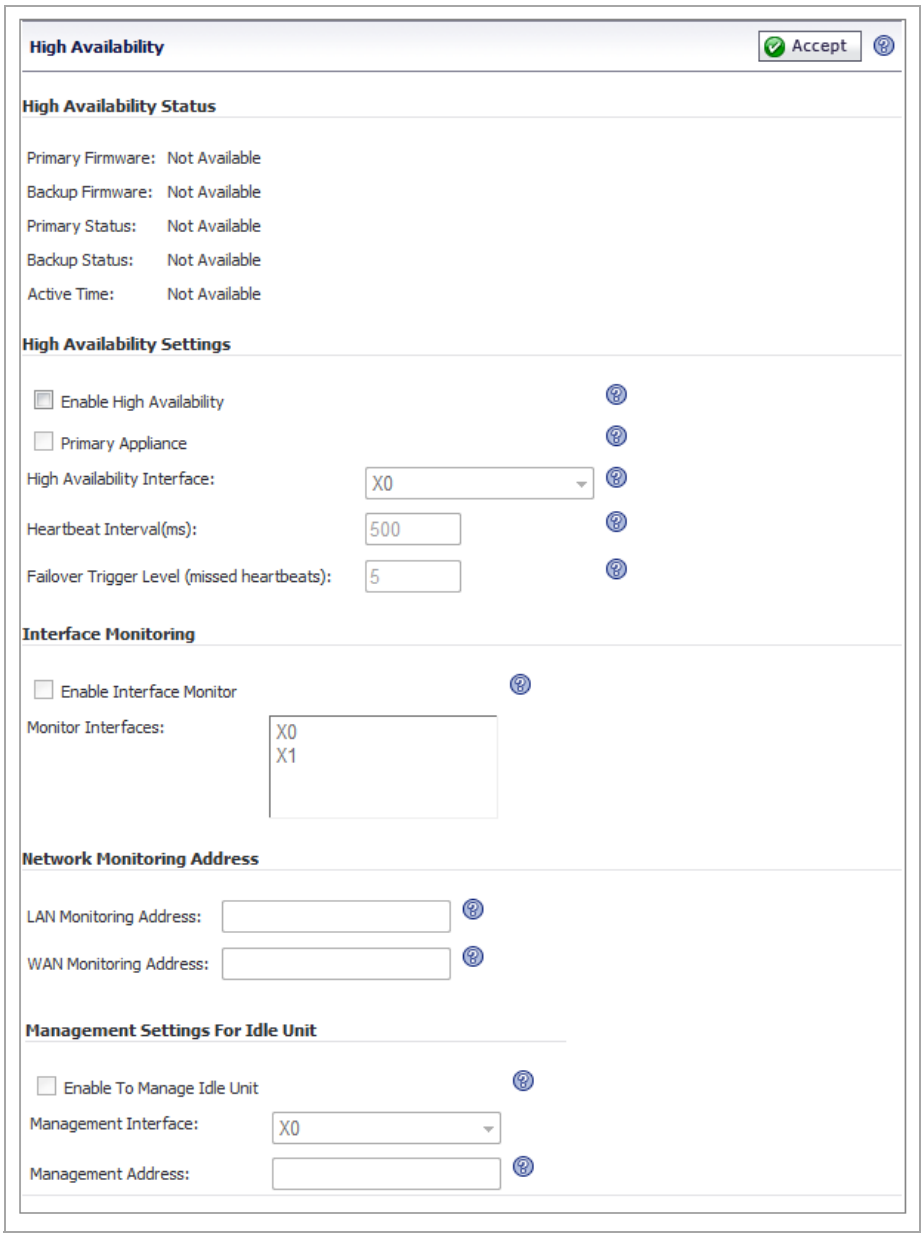
10 Repeat 1 through 8 on the backup unit.

When you click **Accept**, the backup device becomes IDLE and you are no longer able to access it with its IP address. The primary device is now Active with the same settings it had before the HA configuration.

The appliances in the HA Pair immediately begin to synchronize data from the primary to the backup unit. When failover occurs and the primary is down, the backup unit becomes Active with the same settings as the primary.

Configuring High Availability Settings on a Virtual Appliance

The **High Availability > Settings** page provides settings for configuring High Availability.



To enable High Availability for a Virtual Appliance and configure the options in the High Availability Settings section:

1. In a browser, log in to the primary unit and navigate to the **High Availability > Settings** page.
2. Select **Enable High Availability**.

   The HA interface can only be set when the unit is in the HA unconnected mode, and both units must be set to the same interface.
3. Select **Primary Appliance** if this Virtual Appliance is the primary appliance in the HA pair.

4 Select the **High Availability Interface** from the drop-down list. The HA interface can only be set when the unit is in the HA unconnected mode, and the interface must be set to the same interface on both units.

5 Enter a number of milliseconds for the **Heartbeat Interval**. The heartbeat is used to test the connectivity between the primary and backup devices. The heartbeat interval controls how often the two units communicate. The minimum is 500 milliseconds (a half second), and the maximum is 300,000 milliseconds (five minutes).

6 Enter a value for the **Failover Trigger Level**. This is the number of heartbeats that must be missed before failover occurs. The minimum is four, and the maximum is 99.

7 Click **Accept**.

8 In the browser, open a new page and point it to the IP address of the backup unit. Log in to the backup.

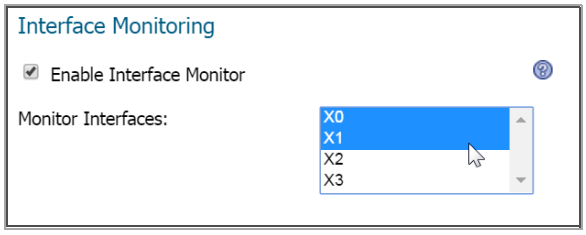
9 Configure High Availability on the backup unit.

When you click **Accept**, the backup device becomes IDLE and you are no longer able to access it with its IP address. The primary device is now Active with the same settings it had before the HA configuration.

The appliances in the HA Pair immediately begin to synchronize data from the primary to the backup unit. When failover occurs and the primary is down, the backup unit becomes Active with the same settings as the primary.

Enabling Interface Monitoring

In the Interface Monitoring section of the page, you can enable monitoring of the working interfaces to which VPN users connect.



The monitored interfaces available for selection are X0, X1, and X2. When Interface Monitoring is enabled and configured, if any of the monitored interfaces loses connectivity on the active unit and is still reachable on the idle unit, failover occurs.

To enable interface monitoring:

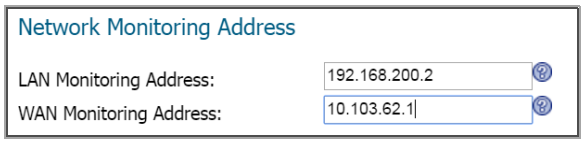
1 On the **High Availability > Settings** page under Interface Monitoring, select **Enable Interface Monitor**.

2 In the **Monitor Interfaces** list, select the interfaces that you want to monitor.

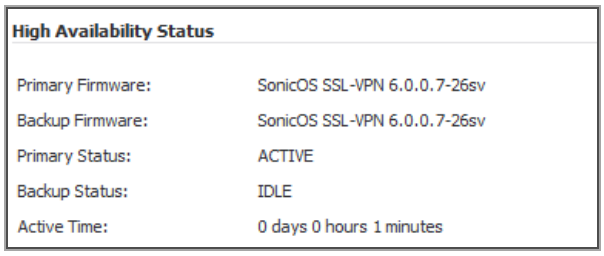
3 Click **Accept**.

Configuring Network Monitoring Addresses

In the Network Monitoring Address section, you can configure monitoring of the LAN and WAN IP addresses. When Network Monitoring is configured, if the LAN or WAN connection is lost on the active unit, but is reachable on the idle unit, failover occurs.



When configured, the LAN and WAN connection status is detected and displayed in the High Availability Status section at the top of the page.

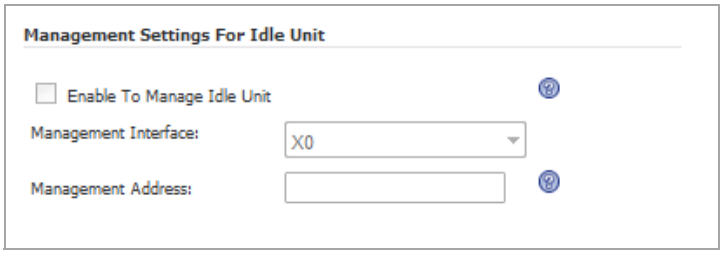


To configure network monitoring:

1. On the **High Availability > Settings** page under Network Monitoring Address, type the LAN IP address into the LAN Monitoring Address field.
2. Type the WAN IP address into the WAN Monitoring Address field.
3. Click **Accept**.

Configuring Management Settings for Idle Unit

In the Network Monitoring Address section, you can configure management settings for the idle unit.



High Availability configuration is limited for SMA 500v Virtual Appliances. Use the **High Availability > Settings** page to enable High Availability on the SMA 500v Virtual Appliance, designate it as the primary or secondary unit, and select the interface. Note the following limitations when configuring management settings for an SMA 500v Virtual Appliance:

- High Availability is not supported on an SMA 500v Virtual Appliance in Single Network Interface mode.
- The Synchronize Firmware function is not supported for an SMA 500v Virtual Appliance.

To configure management settings for the idle unit:

1. On the **High Availability > Settings** page under Management Settings for Idle Unit, check **Enable To Manage Idle Unit**.

2 Select the **management interface** using the drop-down list.

3 Type the idle unit's management IP address in the **Management Address** field.

NOTE: If a management IP address is not entered, the **High Availability Status > Backup Status** field displays as "not available," regardless of the actual status of the unit. Enter the management IP address of the idle unit if you wish to view the status of it.

4 Click **Accept**.

Synchronizing Firmware

You can synchronize firmware from the active unit to the idle unit in the HA pair by clicking **Synchronize Firmware**.

This allows you to synchronize firmware between the units after upgrading the active unit to a different version.

NOTE: Synchronizing firmware on an SMA 500v Virtual Appliance is currently not supported.

Synchronizing Settings

Synchronize settings by clicking **Accept**. Synchronizing settings does not synchronize firmware, but synchronizes settings from the active to the idle unit.

The appliances in the HA Pair immediately begin to synchronize data from the primary to the backup unit. When failover occurs and the primary is down, the backup unit becomes Active with the same settings as the primary.

Synchronizing Licenses

To synchronize licenses between two SMA/SRA appliances in an HA pair, log in to MySonicWall.com and bind the two SMA/SRA appliances together. Both appliances share the primary unit's license information.

NOTE: There is no function in the Secure Mobile Access management interface to synchronize licenses between the two units in the HA pair, all license synchronization is controlled through MySonicWall.

Technical FAQ

1 After HA is enabled, can the idle device be used separately?

No. After HA is configured, only one device can be in use at any one time. During failover the Idle device becomes Active. Two devices in HA mode cannot be used as separate SMA/SRA appliances.

2 What happens if we remove the HA interface cable from the devices?

If you remove the HA interface cable, then the IDLE device can be re-configured to work as a standalone. However, this causes an IP conflict, as both the primary and backup devices have the same IP configuration.

3 Can the HA interface settings be amended, after HA is enabled?

When HA is configured, the 'Edit' button for the HA interface is dimmed and disabled. So the HA interface setting cannot be changed after the devices are in HA mode.

4 Can the X0, X1 and X2 interface settings be amended after HA mode is set up?

Yes, the X0, X1 and X2 interface settings can be amended on the primary device and these new settings are copied to the backup device.

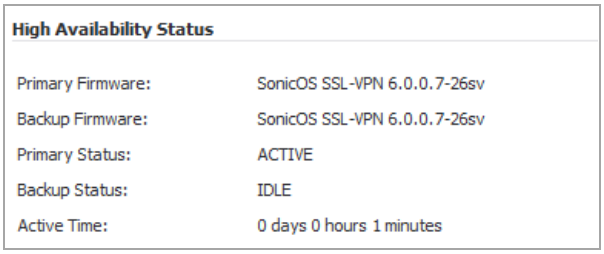
5 Can the synchronization status between the devices be viewed in the Secure Mobile Access management interface?

Yes. These can be viewed on the Active SMA/SRA in the **Log > View** page. The log message: "Finish synchronizing all data," appears.

6 Is there any provision to make sure that the backup device is working correctly?

Yes. There are many messages on the **Log > View** page regarding Active and Idle device transitions.

You can check the High Availability page for the device status; one should be ACTIVE and the other is IDLE, as indicated in the image that follows:



If the LAN and WAN monitoring IP addresses are configured in the Network Monitoring Address section, the status of those interfaces is displayed.

You can also check the **Network > Interfaces** page for the X3 interface status, this should be "HA Link-Connected."

7 Are firmware and settings synchronized to the Idle unit?

Yes, both firmware and settings are synchronized between Active and Idle nodes. The Synchronize Firmware button allows you to synchronize firmware from the Active to the Idle unit. When settings are changed, clicking **Accept** synchronizes settings.

8 Does the HA configuration for SMA/SRA appliances differ from the HA configuration of SonicWall Inc. firewall devices?

Yes. HA configuration on a firewall is very different. Along with other items, firewall HA is also available in Active/Active state and can be assigned a virtual IP address. HA with SMA/SRA appliances is currently available only in Active/Passive mode.

9 How are settings applied to the Idle device?

Settings from the Active device are copied over to the Idle device as soon as HA configuration is complete. You can check the success of this in the active device logs.

10 What happens to the backup device settings?

The backup device settings are deleted and replaced with the primary device settings. If you wish to keep any settings from the backup device, it is recommended that you download a backup of the settings before switching to HA.

11 How do I view the status of the Backup unit?

Enter the management IP address of the idle unit into the **High Availability > Settings > Management Settings For Idle Unit > Management Address** text-field, then click **Accept**. Navigate to the **High Availability Status** and view the status in the **Backup Status** field. If the management IP address of the idle unit is not entered, the Backup Status displays as "Not Available."

12 Can I deploy an HA pair behind a proxy?

No, SMA/SRA appliances in an HA pair cannot be deployed behind a proxy. They communicate with the backend servers directly to download signatures and so on.

Part 4

Configuring Users & Logs

- Users Configuration
- Log Configuration

15

Users Configuration

This section provides information and configuration tasks specific to the **Users** pages on the Secure Mobile Access 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 SMA/SRA appliance.

Topics:

Users > Status

The **Users > Status** page provides information about users and administrators who are currently logged into the SMA/SRA appliance. This section provides general information about how the SMA/SRA appliance manages users through a set of hierarchical policies.

This section contains the following sub-sections:

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 the SMA/SRA appliance. Each entry displays the name of the user, the group in which the user belongs, the portal the user is logged into, the IP address of the user, a time stamp indicating when the user logged in, the duration of the session, and the cumulative idle time during the session. An administrator could 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:

Active User Information

Column	Description
Name	A text string that indicates the ID of the user.
Group	The group to which the user belongs.
Portal	The name of the portal that the user is logged into.
IP Address	The IP address of the workstation which the user is logged into.
Location	The geographical location of the source IP for each user.
Login Time	The time when the user first established connection with the SMA/SRA 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 SMA/SRA 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 SMA/SRA appliance.
Logout	Displays an icon that enables the administrator to log the user out of the appliance.

Access Policies Concepts

The Secure Mobile Access web-based management interface provides granular control of access to the SMA/SRA appliance. Access policies provide different levels of access to the various network resources that are accessible using the SMA/SRA 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 Secure Mobile Access services. Certain policies take precedence.

The Secure Mobile Access 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. Host names 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 that 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 Secure Mobile Access 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

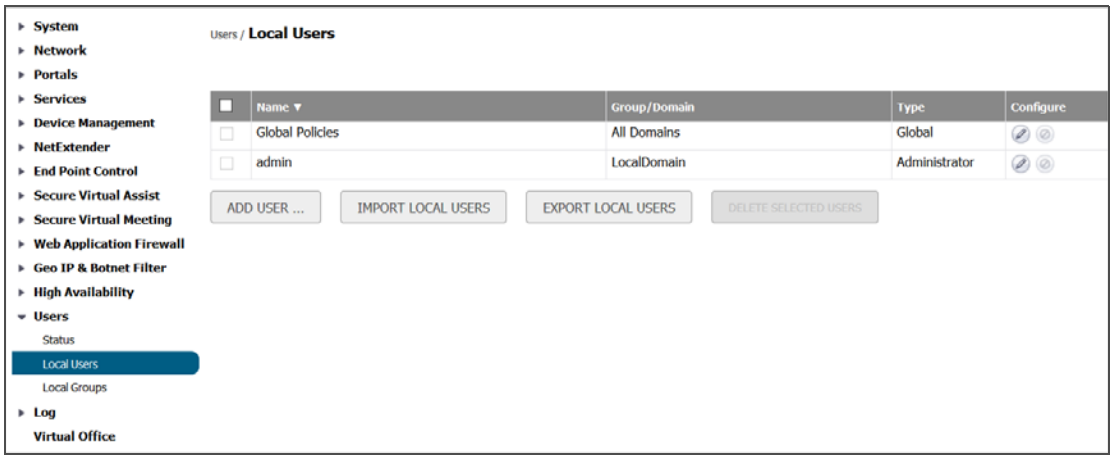
This section provides an overview of the **Users > Local Users** page and a description of the configuration tasks available on this page.

- Users > Local Users Overview on page 357
- Removing a User on page 358
- Adding a Local User on page 358
- Importing Local Users on page 359
- Exporting Local Users on page 360
- Editing User Settings on page 360

For global configuration settings, see Global Configuration on page 429.

Users > Local Users Overview

The **Users > Local Users** page allows you to Import, Export, Add, Configure, and Delete users.



Local Users

The Local Users page allows the administrator to add and configure users by specifying a User Name, selecting a Domain and Group, creating and confirming password, and selecting user type (user, administrator, or read-only administrator).

NOTE: Users configured to use RADIUS, LDAP, or Active Directory authentication do not require passwords because the external authentication server validates 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 is not 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 needs to create the user manually in the Local User database.

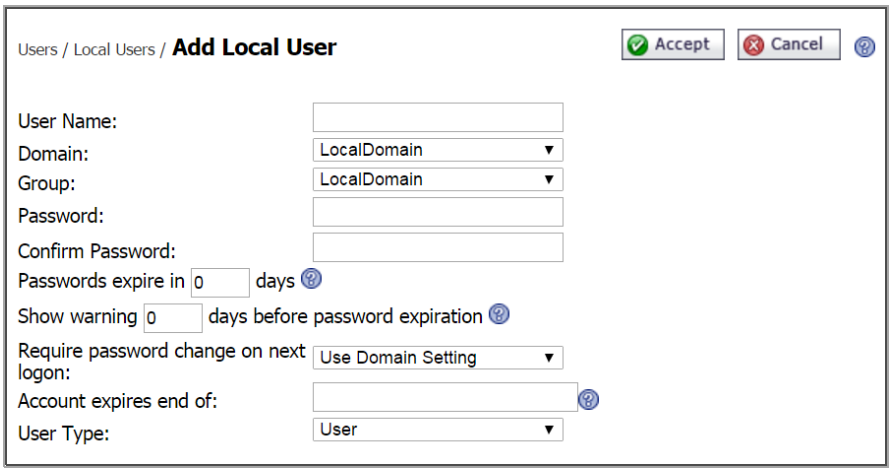
Removing a User

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. After deleted, the user is removed from the **Local Users** window.

Adding a Local User

To create a new local user:

1 Navigate to the **Users** > **Local Users** page and click **Add User**. The **Add Local User** window is displayed.



2 In the **Add Local User** window, enter the username for the user in the **User Name** field. This is the name the user enters in order to log in to the Secure Mobile Access user portal.

3 Select the name of the domain to which the user belongs in the **Domain** drop-down list.

4 Select the name of the group to which the user belongs in the **Group** drop-down list.

5 Type the user password in the **Password** field.

6 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.

7 Optionally, force a user in the Local User Database to change their password at set intervals or the next time they login. To force a user to change their password at set intervals, type the expiration interval in the **Passwords expire in *x* days** field.

8 If you set a password expiration interval, type the number of days before expiration that users should receive notifications in the **Show warning *x* days before password expiration** field.

When configured and a password is expiring, a notification is displayed on the user's Virtual Office page or the Administrator's management console identifying the number of days before their password expires. Notifications also include a link to a screen where the password can be changed.

9 Optionally, use **Require password change on next logon** to force a user to change their password the next time they log in by selecting **Use Domain Setting** or **Enabled**. Selecting **Use Domain Setting** uses the setting configured on the **Portals > Domains** page.

10 With the **Account expires end of** setting, you can set an expiration date with a pull-down calendar. No setting indicates the account never expires.

11 From the **User Type** drop-down list, select a user type option. The available user types are **User**, **Administrator**, or **Read-only Administrator**.

> **TIP:** If the selected group is in a domain that uses external authentication, such as Active Directory, RADIUS, or LDAP, then the **Add User** window closes and the new user is added to the **Local Users** list.

12 Click **Accept** to update the configuration. After the user has been added, the new user is displayed on the **Local Users** window.

> **NOTE:** Entering RADIUS, LDAP, 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 SMA/SRA appliance, then global policies and bookmarks applies 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 Secure Mobile Access configuration files. Bookmarks must be stored on the SMA/SRA appliance because LDAP and RADIUS 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, the SMA/SRA appliance automatically creates a corresponding local user entity when an external domain user creates a personal bookmark so that it might store the bookmark information.

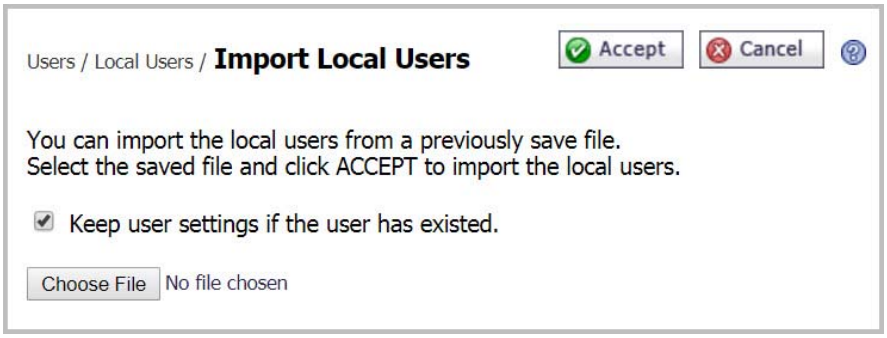
Importing Local Users

Import Local Users allows you to import new users from external files using the JSON format, which can be used later to provide useful information on those users and their attributes.

To import new local users,

1 Navigate to **Users > Local Users**.

2 Select **IMPORT LOCAL USERS**. The **Import Local Users** page appears.



3 Using **Browse**, navigate to location of the JSON-formatted local users file, select it, and click **Import**.

4 Enable **Keep user settings if the user has existed** to keep existing users. Otherwise, existing users are overridden.

Exporting Local Users

Export Local Users allows you to export a JSON file of all added users, which can be used later to provide useful information on those users and their attributes.

To export a file of all local users,

1 Navigate to Users > Local Users.

2 Click **EXPORT LOCAL USERS**. All local users (except the default “admin” user) are downloaded to your local directory.

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 Local User** page has several pages as described in the following table:

Edit Local User pages

Tab	Description
General	Enables you to create a password and an inactivity timeout, and specify Single Sign-On settings for automatic log in to bookmarks for this user.
Groups	Enables you to add a group membership, configure a primary group, and control whether groups are automatically assigned at login.
Portal	Enables you to enable, disable, or use group settings on this portal for NetExtender, File Shares, Virtual Assist, and Bookmark settings.
NetExtender/Mobile Connect	Enables you to specify a NetExtender client address range, including for IPv6, as well as Mobile Connect Default Policy Settings, and to configure client settings.
Routes	Enables you to specify Tunnel All mode and NetExtender client routes.
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.

Edit Local User pages (Continued)

Tab	Description
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.
EPC	Enables you to configure End Point Control profiles used by local groups.

If the user authenticates to an external authentication server, then the **User Type** and **Password** fields are not shown. The password field is not configurable because the authentication server validates the password. The user type is not configurable because the SMA/SRA appliance only allows users that authenticate to the internal user database to have administrative privileges. Also, the user type **External** is 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 page of the **Edit User Settings** window:

- Modifying General User Settings on page 361
- Modifying Group Settings on page 363
- Modifying Portal Settings on page 363
- Modifying User NetExtender Settings on page 364
- Modifying NetExtender Client Routes on page 367
- Adding User Policies on page 367
- Adding or Editing User Bookmarks on page 374
- Configuring Login Policies on page 397

Modifying General User Settings

The **General page** provides configuration options for a user's password, inactivity timeout value, and bookmark single sign-on (SSO) control. the Application Support table provides detailed information about application-specific support of SSO, global/group/user policies and bookmark policies.

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
Terminal Services (RDP - HTML5)	Yes	Yes	Yes
Virtual Network Computing (VNC - HTML5)	Yes	Yes	Yes
File Transfer Protocol (FTP)	Yes	Yes	Yes
Telnet	No	Yes	Yes
Telnet (HTML5)	Yes	Yes	Yes
Secure Shell (SSH)	No	Yes	Yes
Web (HTTP)	Yes	Yes	Yes
Secure Web (HTTPS)	Yes	Yes	Yes
File Shares (CIFS)	Yes	Yes	Yes
Citrix Portal (Citrix)	No	Yes	Yes

NOTE: SSO cannot be used in tandem with two-factor authentication methods.

To modify general user settings:

1 In the left column, navigate to the **Users** > **Local Users**.

2 Click the configure icon next to the user you want to configure. The **General** page of the **Edit User Settings** window displays. The **General page** displays the following non-configurable fields: **User Name**, **Primary Group**, **In Domain**, and **User Type**. If information supplied in these fields needs to be modified, then remove the user as described in Removing a User on page 358 and add the user again.

3 To set or change the user password, type the password in the **Password** field. Re-type it in the **Confirm Password** field.

4 Optionally, force a user in the Local User Database to change their password at set intervals or the next time they login. To force a user to change their password at set intervals, type the expiration interval in the **Passwords expire in *x* days** field. To force a user to change their password the next time they log in, check **Change password at next logon**.

NOTE: A specific local domain user can be forced to change their password. Use the **General** page on the **Users > Local Users > Edit** page.

5 If you set a password expiration interval, type the number of days before expiration that users should receive notifications in the **Show warning *x* days before password expiration** field.

When configured and a password is expiring, a notification is displayed on the user's Virtual Office page or the Administrator's management console identifying the number of days before their password expires. Notifications also include a link to a screen where the password can be changed.

6 To set the inactivity timeout for the user, meaning that they are 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.

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 takes precedence over the group timeout and the group timeout takes 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.

7 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.

8 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**.

Bookmark modification controls provide custom access to predetermined sources, and can prevent users from needing support.

9 Under **Single Sign-On Settings**, select one of the following options from the **Automatically log into bookmarks** drop-down menu:

- **Use Group Setting**: 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 might be expecting the username to be prefixed by the domain name. In this instance, SSO fails and the user has 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.

10 Click **Accept** to save the configuration changes

Modifying Group Settings

On the **Groups** page, you can add a group membership for users, configure a primary group, and control whether groups are automatically assigned at user login.

Users logging into Active Directory, LDAP, and RADIUS domains are automatically assigned in real time to Secure Mobile Access groups based on their external AD group memberships, LDAP attributes, or RADIUS filter-IDs.

NOTE: If a user's external group membership has changed, their Secure Mobile Access group membership automatically changes to match the external group membership.

To configure settings on the Groups page:

1 To set a group as the primary group, click the "Set Primary Group" star corresponding to the group you wish to set as the primary.

2 To add a group of which users are a member, click **Add Group**. The group must be already configured from **Users > Local Groups**.

3 Select the desired group from the drop-down list.

4 Select **Make primary group** to make this the primary group membership for users.

5 Click **Add Group** to add the selected group to the **Group Memberships** list.

6 Under **Group Settings**, select one of the following from the **Auto-assign groups at login** drop-down list:

- **Use group setting** – Use the setting configured for the group.
- **Enabled** – Enable automatic assignment of users to groups upon login.
- **Disabled** – Disable automatic assignment of users to groups upon login.

7 Click **Accept**.

Modifying Portal Settings

The **Portal page** provides configuration options for portal settings for this user.

To configure portal settings for this user:

1 On the **Portal** page 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 are 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 previous settings for each of the following portal features:

- **NetExtender** – Because Mobile Connect acts as a NetExtender client when connecting to the appliance, this setting applies to both NetExtender and Mobile Connect.
- Launch NetExtender after login
- File Shares
- Virtual Assist Technician
- Virtual Assist Request Help
- Virtual Access Setup Link
- Allow User to Add Bookmarks
- **Allow User to Edit/Delete Bookmarks** – Applies to user-owned bookmarks only.

2 Click **Accept**.

Modifying User NetExtender Settings

This feature is for external users, who inherits the settings from their assigned group upon login. NetExtender client settings can be specified for the user, or use the group settings. For information about configuring group settings, see Editing Group Settings on page 401.

To enable NetExtender/Mobile Connect ranges and configure Static client settings for a user:

1 Navigate to **Users > Local Users**.

2 Click the configure icon next to the user you want to configure.

3 In the **Edit Local User** page, select the **NetExtender/Mobile Connect** page.

a Under **Client Address Range**, select **Use Static Pool** from the drop-down list.

b Supply a beginning client IPv4 address in the **Client Address Range Begin** field.

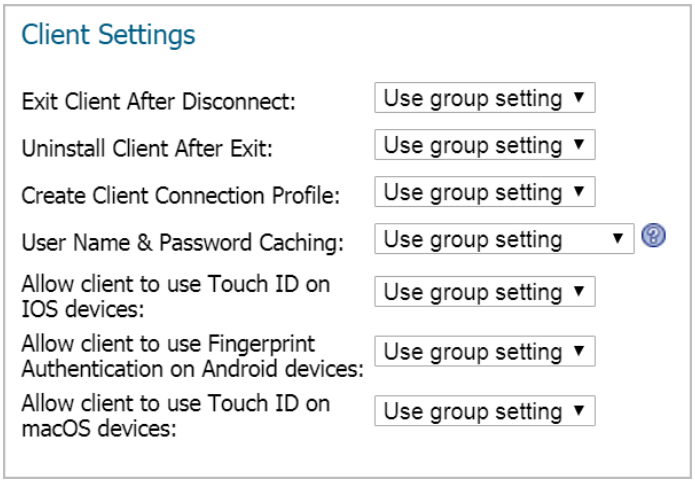
c Supply an ending client IPv4 address in the **Client Address Range End** field.

d Under **Client IPv6 Address Range**, optionally select **Use Static Pool** from the drop-down list.

e Supply a beginning client IPv6 address in the **Client Address Range Begin** field.

f If using IPv6, supply an ending client IPv6 address in the **Client Address Range End** field.

4 Under **Client Settings**:



Select one of the following from the **Exit Client After Disconnect** drop-down list:

- **Use group setting** - Take the action specified by the group setting. See Editing Group Settings on page 401.
- **Enabled** - Enable this action for the user. Overrides the group setting.
- **Disabled** - Disable this action for all members of the group. Overrides the global setting.

5 In the **Uninstall Client After Exit** drop-down list, select one of the following:

- **Use group setting** - Take the action specified by the group setting. See Editing Group Settings on page 401.
- **Enabled** - Enable this action for the user. Overrides the group setting.
- **Disabled** - Disable this action for all members of the group. Overrides the global setting.

6 In the **Create Client Connection Profile** drop-down list, select one of the following:

- **Use group setting** - Take the action specified by the group setting. See Editing Group Settings on page 401.
- **Enabled** - Enable this action for the user. Overrides the group setting.
- **Disabled** - Disable this action for all members of the group. Overrides the global setting.

7 In the **User Name & Password Caching** drop-down list, select one of the following:

- **Use group setting** - Take the action specified by the group setting. See Editing Group Settings on page 401.
- **Allow saving of user name only** - Allow caching of the user name. The user only needs to enter a password when starting NetExtender. Overrides the group setting.
- **Allow saving of user name & password** - Allow caching of the user name and password. The user is automatically logged in when starting NetExtender. Overrides the group setting.
- **Prohibit saving of user name & password** - Do not allow caching of the user name and password. The user is required to enter both user name and password when starting NetExtender. Overrides the group setting.

8 In the **Allow client to use Touch ID on IOS devices**, the control only blocks future attempts to log in with fingerprint technology on IOS devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.

9 In the **Allow client to use Fingerprint Authentication on Android devices**, the control only blocks future attempts to log in with fingerprint technology on Android devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.

10 In the **Allow client to use Touch ID on macOS devices**, the control only blocks future attempts to log in with fingerprint technology on macOS devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.

11 In the **Internal Proxy Settings** section, select from the drop-down list to enable or disable the Internal Proxy feature. See NetExtender > Client Settings on page 243 for more information.

12 Click **Accept**.

To enable NetExtender ranges and configure DHCP client settings for a user:

1 Navigate to **Users > Local Users**.

2 Click the configure icon next to the user you want to configure.

3 In the **Edit Local User** page, select the **NetExtender/Mobile Connect** page.

   a Under **Client Address Range**, select **Use DHCP** from the drop-down list.

   b Under **Select Interface**, use the drop-down list to select the interface to use for DHCP.

   c Supply the **DHCP Server** in the field provided.

   d Under **Client IPv6 Address Range**, optionally select **Use DHCPv6** from the drop-down list.

   e Under **Select Interface**, use the drop-down list to select the interface to use for DHCPv6.

   f Optionally supply the **DHCPv6 Server** in the field provided.

4 Under **Client Settings**, select one of the following from the **Exit Client After Disconnect** drop-down list:

- **Use group setting** - Take the action specified by the group setting. See Editing Group Settings on page 401.
- **Enabled** - Enable this action for the user. Overrides the group setting.
- **Disabled** - Disable this action for all members of the group. Overrides the global setting.

5 In the **Uninstall Client After Exit** drop-down list, select one of the following:

- **Use group setting** - Take the action specified by the group setting. See Editing Group Settings on page 401.
- **Enabled** - Enable this action for the user. Overrides the group setting.
- **Disabled** - Disable this action for all members of the group. Overrides the global setting.

6 In the **Create Client Connection Profile** drop-down list, select one of the following:

- **Use group setting** - Take the action specified by the group setting. See Editing Group Settings on page 401.
- **Enabled** - Enable this action for the user. Overrides the group setting.
- **Disabled** - Disable this action for all members of the group. Overrides the global setting.

7 In the **User Name & Password Caching** drop-down list, select one of the following:

- **Use group setting** - Take the action specified by the group setting. See Editing Group Settings on page 401.

- **Allow saving of user name only** - Allow caching of the user name. The user only needs to enter a password when starting NetExtender. Overrides the group setting.
- **Allow saving of user name & password** - Allow caching of the user name and password. The user is automatically logged in when starting NetExtender. Overrides the group setting.
- **Prohibit saving of user name & password** - Do not allow caching of the user name and password. The user is required to enter both user name and password when starting NetExtender. Overrides the group setting.

8 In the **Allow client to use Touch ID on IOS devices**, the control only blocks future attempts to log in with fingerprint technology on IOS devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.

9 In the **Allow client to use Fingerprint Authentication on Android devices**, the control only blocks future attempts to log in with fingerprint technology on Android devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.

10 In the **Allow client to use Touch ID on macOS devices**, the control only blocks future attempts to log in with fingerprint technology on macOS devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.

11 In the **Internal Proxy Settings** section, select from the drop-down list to enable or disable the Internal Proxy feature. See NetExtender > Client Settings on page 243 for more information.

12 Click **Accept**.

Modifying NetExtender Client Routes

The **Routes** page provides configuration options for NetExtender client routes. For procedures on modifying NetExtender client route settings, see NetExtender > Client Routes on page 249.

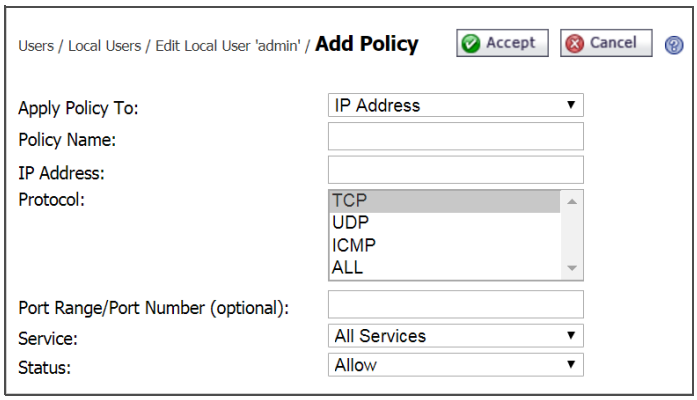
Adding User Policies

The **Policies** page provides policy configuration options.

NOTE: User policies are the highest priority-type of policy, and are enforced before group policies or global policies.

To add a user access policy:

1 On the **Policies** page, click **Add Policy**. The **Add Policy** window is displayed.



2 In the **Apply Policy To** drop-down list, select whether the policy is applied to an individual host, a range of addresses, all addresses, a network object, a server path, or a URL object. You can also select an individual IPv6 host, a range of IPv6 addresses, or all IPv6 addresses. The **Add Policy** window changes depending on what type of object you select in the **Apply Policy To** drop-down list.

NOTE: These Secure Mobile Access policies apply to the destination address(es) of the SMA/SRA connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the SMA/SRA gateway with a policy created on the **Policies** page. However, it is possible to control source logins by IP address with a login policy created on the user's **Login Policies** page. For more information, refer to Configuring Login Policies on page 397.

- **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 on page 369.
- **IP Network** - 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 Network on page 370.
- **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 on page 370.
- **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 Adding Network Objects on page 139
- **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 on page 370.
- **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 on page 371.
- **All IPv6 Address** - If your policy applies to all IPv6 addresses, you do not need to enter any IP address information. See Adding or Editing User Bookmarks on page 374.

- **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. See Adding a Policy for an IPv6 Address on page 373.
- **IPv6 Network** - 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 Network on page 374.

3 Select the desired **Protocol**. The available value options in the Protocol field include: **TCP**, **UDP**, **ICMP**, and **ALL**. You can select multiple items among **TCP**, **UDP**, and **ICMP**. However, when **ALL** is selected, all others options are deselected.

NOTE: The protocol setting only appears when the Service is set to "NetExtender & Mobile Connect" or "All Services."

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.

5 Select **Allow** or **Deny** from the **Status** drop-down list to either permit or deny SMA/SRA 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.

6 Click **Accept** to update the configuration. After the configuration has been updated, the new policy is displayed in the **Edit Local User** page.

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

1 Navigate to **Users > Local Users**.

2 Click the configure icon next to the user you want to configure.

3 Select the **Policies** page.

4 Click **Add Policy...**

5 In the **Apply Policy to** field, click the IP Address option.

6 Define a name for the policy in the **Policy Name** field.

7 Type an IP address in the **IP Address** field.

8 Select the desired **Protocol**. The available value options in the Protocol field include: **TCP**, **UDP**, **ICMP**, and **ALL**. You can select multiple items among **TCP**, **UDP**, and **ICMP**. However, when **ALL** is selected, all others options are deselected.

NOTE: The protocol setting only appears when the Service is set to "NetExtender & Mobile Connect" or "All Services."

9 In the **Port Range/Port Number** field, optionally enter a port range or an individual port.

10 In the **Service** drop-down list, click on a service object.

11 In the **Status** drop-down list, click on an access action, either **Allow** or **Deny**.

12 Click **Accept**.

Adding a Policy for an IP Network

1 In the **Apply Policy to** field, click the **IP Network** option.

2 Define a name for the policy in the **Policy Name** field.

3 Type a starting IP address in the **IP Network Address** field.

4 Type a subnet mask value in the **Subnet Mask** field in the form 255.255.255.0.

5 Select the desired **Protocol**. The available value options in the Protocol field include: **TCP**, **UDP**, **ICMP**, and **ALL**. You can select multiple items among **TCP**, **UDP**, and **ICMP**. However, when **ALL** is selected, all others options are deselected.

> **NOTE:** The protocol setting only appears when the Service is set to "NetExtender & Mobile Connect" or "All Services."

6 In the **Port Range/Port Number** field, optionally enter a port range or an individual port.

7 In the **Service** drop-down list, click on a service option.

8 In the **Status** drop-down list, click on an access action, either **Allow** or **Deny**.

9 Click **Accept**.

Adding a Policy for All Addresses

1 In the **Apply Policy to** field, select the **All Addresses** option.

2 Define a name for the policy in the **Policy Name** field.

3 Select the desired **Protocol**. The available value options in the Protocol field include: **TCP**, **UDP**, **ICMP**, and **ALL**. You can select multiple items among **TCP**, **UDP**, and **ICMP**. However, when **ALL** is selected, all others options are deselected.

> **NOTE:** The protocol setting only appears when the Service is set to "NetExtender & Mobile Connect" or "All Services."

4 The **IP Address Range** field is read-only, specifying All IP Addresses.

5 In the **Service** drop-down list, click on a service option.

6 In the **Status** drop-down list, click on an access action, either **Allow** or **Deny**.

7 Click **Accept**.

Setting File Shares Access Policies

To set file share access policies:

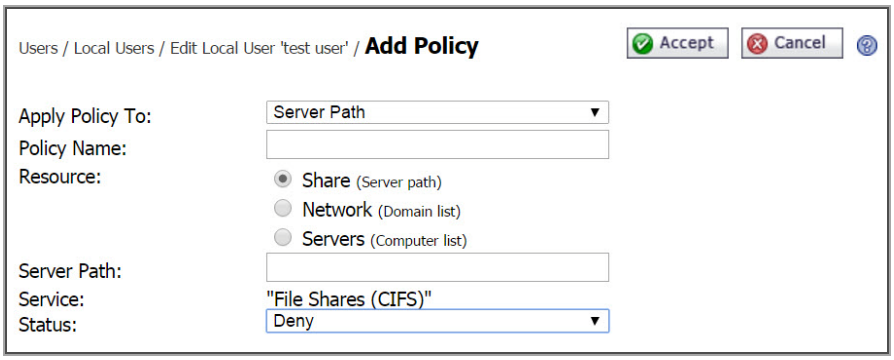
1 Navigate to **Users > Local Users**.

2 Click the configure icon next to the user you want to configure.

3 Select the **Policies** page.

4 Click **Add Policy**.

5 Select **Server Path** from the **Apply Policy To** drop-down list.



6 Type a name for the policy in the **Policy Name** field.

7 Select **Share** in the **Resource** field.

8 Type the server path in the **Server Path** field.

9 From the **Status** drop-down list, select **Allow** 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 371.

10 Click **Accept**.

Adding a Policy for a File Share

To add a file share access policy:

1 Navigate to **Users > Local Users**.

2 Click the configure icon next to the user you want to configure.

3 Select the **Policies** page.

4 Click **Add Policy...**

5 Select **Server Path** from the **Apply Policy To** drop-down list.

6 Type a name for the policy in the **Policy Name** field.

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.

8 Select **Allow** or **Deny** from the **Status** drop-down list.

9 Click **Accept**.

Adding a Policy for a URL Object

To create object-based HTTP or HTTPS user policies:

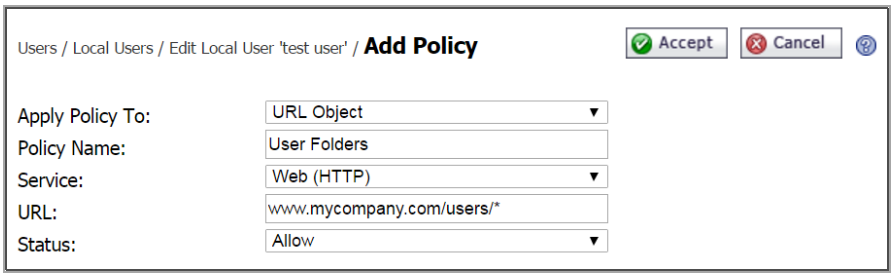
1 Navigate to **Users > Local Users**.

2 Click the configure icon next to the user you want to configure.

3 Select the **Policies** page.

4 Click **Add Policy**.

5 In the **Apply Policy To** drop-down menu, select the **URL Object** option.



6 Define a name for the policy in the **Policy Name** field.

7 In the **Service** drop-down list, choose either **Web (HTTP)** or **Secure Web (HTTPS)**.

8 In the **URL** field, add the URL string to be enforced in this policy.

> **NOTE:** In addition to standard URL elements, the administrator can enter the port, path and wildcard elements to the URL field. For more information on using these additional elements, see Policy URL Object Field Elements on page 372.
>
> 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.

9 In the **Status** drop-down list, click on an access action, either **Allow** or **Deny**.

10 Click **Accept**.

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 can enter the port, path and wildcard elements to this field. The following chart provides an overview of standard URL field elements:

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 such as [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 might contain wildcard characters. The scope of the wildcard characters is limited only to the specific part contained between file path separators.

Standard URL field elements (Continued)

Element	Usage
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. For example **[!acd]**, **[!8a0]** **[<range>]** – Matches any character falling within the specified ASCII range. Can be an alphanumeric character. For example, **[a-d]**, **[3-5]**, **[H-X]**

NOTE: Entries in the URL field cannot contain (“http://,” “https://”) elements. Entries can also not contain fragment delimiters such as “#.”

Adding a Policy for All IPv6 Addresses

To add a policy for all IPv6 addresses:

1. In the **Apply Policy To** field, select the **All IPv6 Address** option.
2. Define a name for the policy in the **Policy Name** field.
3. The **IPv6 Address Range** field is read-only, specifying all IPv6 addresses.
4. In the **Service** drop-down list, click on a service option.
5. In the **Status** drop-down list, click on an access action, either **Allow** or **Deny**.
6. Click **Accept**.

Adding a Policy for an IPv6 Address

To add a policy for an IPv6 address:

1. Navigate to **Users > Local Users**.
2. Click the configure icon next to the user you want to configure.
3. Select the **Policies** page.
4. Click **Add Policy...**
5. In the **Apply Policy To** field, click the **IPv6 Address** option.
6. Define a name for the policy in the **Policy Name** field.
7. Type an IPv6 address in the **IPv6 Address** field in the form 2001::1:2:3:4.
8. In the **Port Range/Port Number** field, optionally enter a port range or an individual port.
9. In the **Service** drop-down list, click on a service object.
10. In the **Status** drop-down list, click on an access action, either **Allow** or **Deny**.
11. Click **Accept**.

Adding a Policy for an IPv6 Network

To add a policy for an IPv6 Network:

1. In the **Apply Policy To** field, click the **IPv6 Network** option.
2. Define a name for the policy in the **Policy Name** field.
3. Type a starting IPv6 address in the **IPv6 Network Address** field.
4. Type a prefix value in the **IPv6 Prefix** field, such as 64 or 112.
5. In the **Port Range/Port Number** field, optionally enter a port range or an individual port.
6. In the **Service** drop-down list, click on a service option.
7. In the **Status** drop-down list, click on an access action, either **Allow** or **Deny**.
8. Click **Accept**.

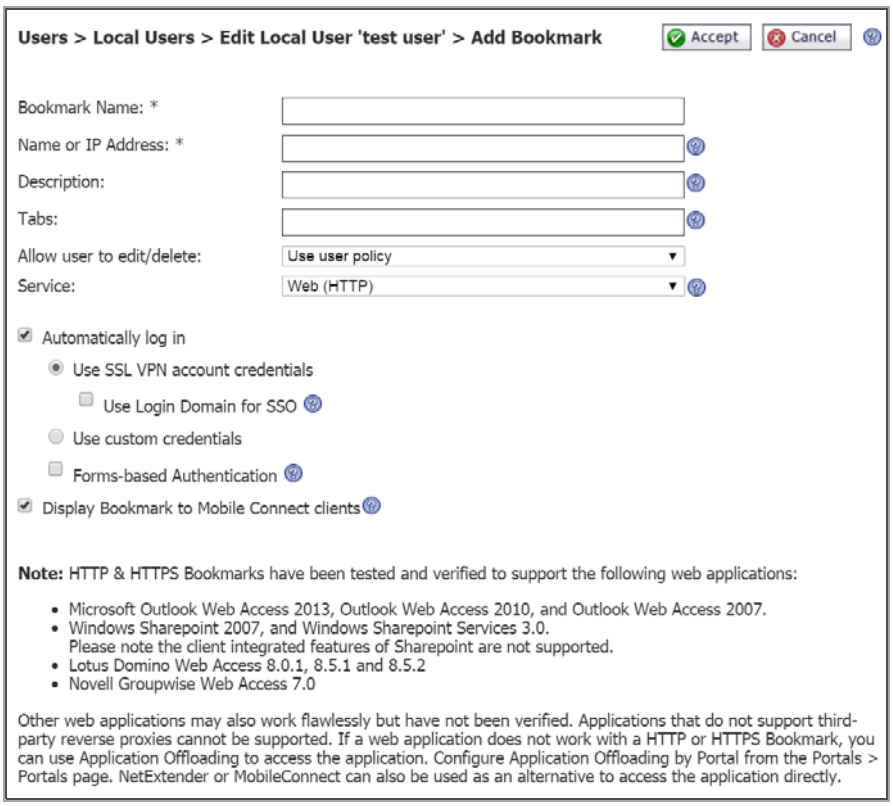
Adding or Editing User Bookmarks

The **Bookmarks** page provides configuration options to add and edit user bookmarks. In addition to the main procedure that follows, see the following:

- Creating a Citrix Bookmark for a Local User on page 393
- Creating Bookmarks with Custom SSO Credentials on page 396

To define user bookmarks:

1. In the **Edit User Settings** window, click the **Bookmarks** page.
2. Click **Add Bookmark**. The **Add Bookmark** window displays.



When user bookmarks are defined, the user sees the defined bookmarks from the Secure Mobile Access Virtual Office home page.

1 Type a descriptive name for the bookmark in the **Bookmark Name** field.

2 Enter the fully qualified domain name (FQDN) or the IPv4 or 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.

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 the Bookmark Name or IP Address Formats by Service Type table.

Bookmark Name or IP Address Formats by Service Type

Service Type	Format	Example for Name or IP Address Field
RDP - HTML5	IP Address	10.20.30.4
RDP - Native	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
VNC - HTML5	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.
Citrix (Citrix Web Interface) Citrix - HTML5 Citrix - Native Citrix - ActiveX	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 client port.	

Bookmark Name or IP Address Formats by Service Type (Continued)

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 (CIFS)	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.
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
Telnet - HTML5	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
SSHv2	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

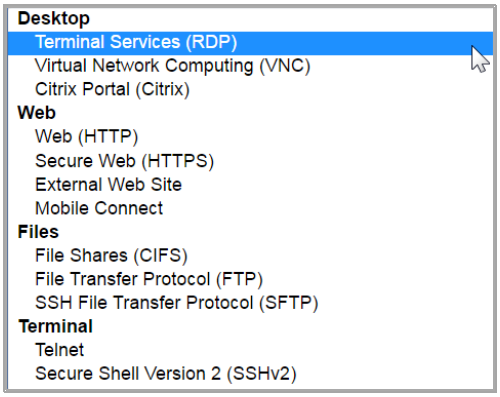
TIP: When creating a **Virtual Network Computing (VNC)** bookmark to a Linux server, you must specify the port number and server number in addition to the Linux server IP the **Name or IP Address** field in the form of **ipaddress:port:server**. For example, if the Linux server IP address is 192.168.2.2, 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**.

3 Optionally, you can enter a friendly description to be displayed in the bookmark table by filling in the **Description** field.

4 Optionally, you can enter a comma-separated list of tabs where this bookmark appears in the **Tabs** field. For example: Favorites, Tab1, Tab 2. Note that standard tabs, such as Desktop, Web, Terminal, or Mobile, do not need to be specified.

5 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.

6 Select one of the service types from the **Service** drop-down list.



For the specific service you select from the **Service** drop-down list, additional fields might appear. Use the following information for the chosen service to complete the building of the bookmark:

Terminal Services (RDP) or Terminal Services (RDP - HTML5)

NOTE: HTML5 RDP bookmarks are only supported with Per User licensing on Terminal Server connections. These bookmarks do not work if the Terminal Server's licensing mode is Per Device.

- In the **Screen Size** drop-down list, select the default terminal services screen size to be used when users execute this bookmark. *(Option available for all Terminal Services.)*

  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 might 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. *(Option available for all Terminal Services.)*

- Select an **Access Type Selection**. **Smart** or **Manual**.

  - **Smart**: Allows the firmware to decide which mode to launch on the client.

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

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

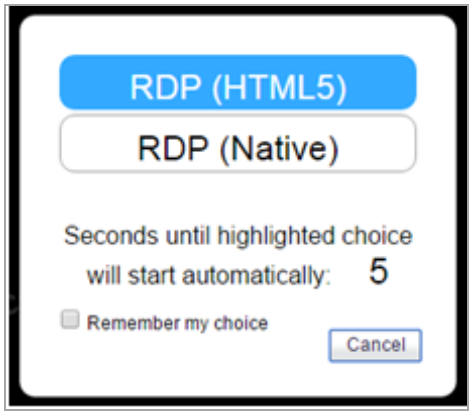
    

    The launch sequence is as follows: **HTML5** and **Native**. Selecting Manual allows you to change, enable, or disable the launch methods. If you select **Native** to launch the RDP bookmark, then the SMA Connect Agent launches the RDP Client on the local machine to do the RDP connection.

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

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

After the **Choose during Launch** option is enabled, while launching the unified bookmark, if there are multiple modes available for the client, a menu is provided from which you can choose within a five second count-down. When only one mode is available, the bookmark is also run immediately.

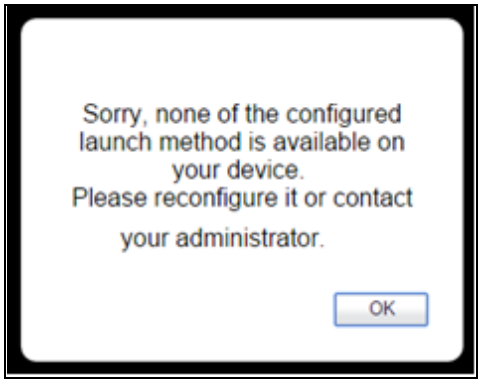


If the **Remember my choice** option is selected during the launch time, the selected mode is remembered through a cookie.

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

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

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



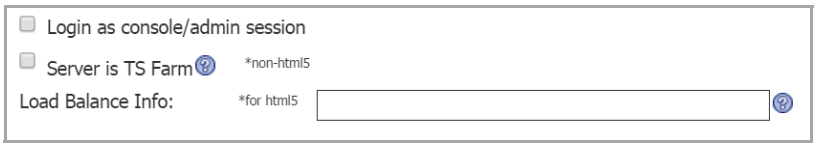
- Select **Enable wake-on-LAN** to enable waking up a computer over the network connection. Selecting this check box causes the following new fields to be displayed: *(Options available for all Terminal Services.)*
    - **MAC/Ethernet Address** – Enter one or more MAC addresses, separated by spaces, 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 **Send WOL packet to host name or IP address** that can be applied in tandem with a MAC address of another machine to wake.
- Optionally enter the local path for this application in the **Application and Path** field and specify the folder in the **Start in the following folder** field. The remote application feature displays a single application to the user. The value might also be the alias of the remote application.
- Enter the **Command-line Arguments** for the RemoteApp. *(Option available for ActiveX only.)*
- In the **Start in the following folder** field, optionally enter the local folder in which to execute application commands. *(Option available for ActiveX only.)*
- Select **Login as console/admin session** to allow login as console or admin. Login as admin replaces login as console in RDC 6.1 and newer. *(Option available for all Terminal Services.)*
- Select the **Server is TS Farm** if users are connecting to a TS Farm or Load Balanced server.

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

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

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

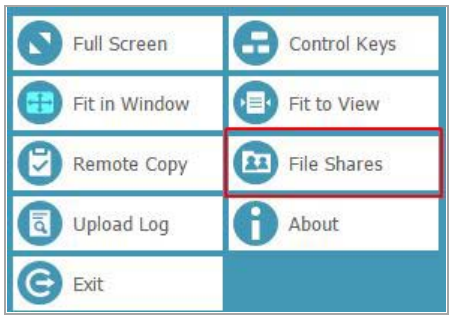
  The `<CollectionName>` is the collection name in the user's farm. This line is the "Load Balance Information." The broker server needs this information to do the load balancing (redirection).
- Enter the Terminal Services Broker information in the **Load Balance Info** box, such as `tsv://MS Terminal Services Plugin.1.`SSLVPN. Maximum length is 1024 characters. For the bookmark with complex options (like RDP), options are mixed from all the modes and distinguished with tips like *non-html5, or *for html5.



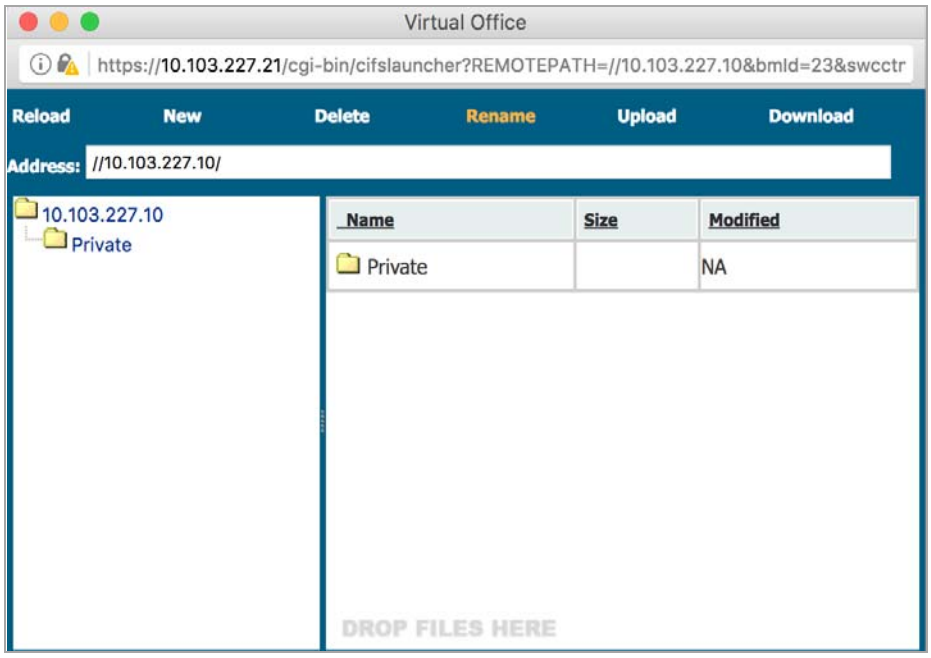
  By default, the bookmark only connects to the provided name and IP address. If you enable this feature, the SMA/SRA appliance obtains the redirected address and connects the user to the correct server. Note that Interactive Login might need to be disabled for this feature to work properly.
- For *RDP - HTML5*, select the **Default Language** from the drop-down menu.
- For Windows clients or on Mac clients running Mac OS X 10.5 or higher with RDC installed, expand **Show advanced Windows options** and select the check boxes to redirect the following features on the local network for use in this bookmark. For *RDP - HTML5 or Native*, the following Advanced Windows options are available:
    - **Desktop background**
    - **Menu/window animation**

- **Show window contents while dragging/resizing**
- **Redirect clipboard**
- **File Share**

  When you choose File Share, a new button for the feature appears on the HTML5 RDP menu when you click the **Shield** icon.



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



- **Redirect drives**
- **Redirect SmartCards**
- **Bitmap caching**
- **Auto-reconnection**
- **Visual styles**
- **Remote copy**
- **Redirect printers** - See Printer redirection **on page 468** for more information on setting up Printer Redirection
- **Redirect ports**
- **Display connection bar**

- Select the **Remote Audio** option from the drop-down list. Audio redirection enables the user to play an audio clip on the server, either remotely or locally. Valid selections are **Play on this computer**, **Play on remote computer**, or **Do not play**. Note that this feature is currently supported by Chrome, Firefox, and Safari.

NOTE: Hover your mouse pointer over the Help icon  next to certain options to display tooltips that indicate requirements.

- If the client application is RDP6, you can select any of the following options: (*Option available for all Terminal Services)*
  - **Font smoothing**
  - **Span monitors**
  - **Desktop composition**
  - **Dual monitors**
  - **Remote application**
- Select the **Connection Speed** from the drop-down list (low-speed broadband or high speed broadband) for optimized performance. (*Option available for all Terminal Services.*)
- Select the action from the drop-down list that happens in the event that the **Server Authentication fails**. Server authentication verifies that you are connecting to the intended remote computer. The strength of the verification required to connect is determined by your system security policy. (*Option available for all Terminal Services.*)
- Click **Import RDP Options**. When the RDP file finishes downloading, open it with a text editor (such as Notepad) and select the entire file content. Copy the content and paste the text into the text field in **Import RDP Options**. Click **OK**. The feature selects the support options to import into the bookmark.

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

Bookmark field	RDP option
Name or IP Address	full address:s:<value>
Screen Size	desktopheight:i:<value> desktopwidth:i:<value>
Colors	session bpp:i:<value>
Load Balance Info	loadbalanceinfo:s:<value>
Desktop Background	disable wallpaper:i:<value>
Auto-Reconnection	autoreconnection enabled:i:<value>
Menu/Window Animation	disable menu anims:i:<value>
Visual Styles	disable themes:i:<value>
Show Window contents while dragging/resizing	disable full window drag:i:<value>
Redirect clipboard & Remote Copy	redirectclipboard:i:<value>
Redirect printers	redirectprinters:i:<value>
Redirect drives	redirectdrives:i:<value>
Redirect ports	redirectcomports:i:<value>
Redirect SmartCards	redirectsmartcards:i:<value>
Display connection bar	displayconnectionbar:i:<value>
Bitmap caching	bitmapcachepersistenable:i:<value>
Remote audio	audiomode:i:<value>

Bookmark field (Continued)	RDP option (Continued)
Font smoothing	allow font smoothing:i:<value>
Span monitors	span monitors:i:<value>
Dual monitors	use multimon:i:<value>
Desktop composition	allow desktop composition:i:<value>
Remote Application	remoteapplicationmode:i:<value>
Choose your connection speed to optimize performance	connection type:i:<value>

- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in to the RDP server. Enable the **Use Login Domain for SSO** option to pass the user's domain to the RDP server. Windows 2008 and newer servers might require this option to be enabled. *(Option available for all Terminal Services.)*

  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 on page 396.

- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices. *(Option available for all Terminal Services.)*

  NOTE: RDP over HTML5 is supported using the default/standard browser in iOS or Android.

Limitations to Terminal Services Farm Bookmarks from Virtual Office

Verify access and configuration is setup properly outside the remote access appliance first by connecting with NetExtender then running your RDP client to connect as if you would were you inside your network. If NetExtender is unable to connect properly there is likely another device or setting on the network that needs to be configured properly.

Refer to your server's guide or contact Microsoft for additional help regarding Terminal Server settings if the provided instructions do not work for you to change the settings.

- Interactive Login might need to be disabled. The windows login notice prevents the proxy from obtaining the correct redirection server.
- Run gpedit.msc and go to **Computer Configuration > Windows Settings > Local Policies > Security Options** and look for Interactive logon: Message title for users attempting to log on and Interactive logon: Message text for users attempting to logon and ensure both are blank.
- Multiple RDP Sessions might need to be disabled. Multiple RDP sessions might cause more than one redirection preventing the bookmark proxy from being able to connect to the correct server. Restricting the user to on session in the Group policy prevents from occurring.
- Run gpedit.msc on the remote server and go to **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections** and set the Restrict Remote Desktop Services user to a single Remote Desktop Services session to **Enabled**.
- Note that we create a new session request when connecting to the RDP server and are unable to clear the old session through the bookmark. There might be some issues with your server setup depending on your available licenses and how disconnected sessions are handled.
- Ensure SSO is correct if that option is enabled. Improper SSO credentials prevents the bookmark from accessing the server properly. If you are running into issues, try disabling SSO and ensuring the proper credentials are entered for connection.

- HTML5 RDP Client is recommended for usage for users connecting from systems unable to take advantage of a native RDP client. Most modern browsers support the Web Sockets feature required for connection and should be available on the systems that do not have a native RDP client.

Virtual Network Computing (VNC)

- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in to the RDP server. Enable the **Use Login Domain for SSO** option to pass the user's domain to the RDP server.
- In the **Encoding** drop-down list, select one of:
  - **Raw** – Pixel data is sent in left-to-right scanline order, and only rectangles with changes are sent after the original full screen has been transmitted.
  - **RRE** – Rise-and-Run-length-Encoding uses a sequence of identical pixels that are compressed to a single value and repeat count. This is an efficient encoding for large blocks of constant color.
  - **CoRRE** – A variation of RRE, using a maximum of 255x255 pixel rectangles, allowing for single-byte values to be used. More efficient than RRE except where very large regions are the same color.
  - **Hextile** – Rectangles are split up in to 16x16 tiles of raw or RRE data and sent in a predetermined order. Best used in high-speed network environments such as within the LAN.
  - **Zlib** – Simple encoding using the zlib library to compress raw pixel data, costing a lot of CPU time. Supported for compatibility with VNC servers that might not understand Tight encoding which is more efficient than Zlib in nearly all real-life situations.
  - **Tight** – The default and the best encoding to use with VNC over the Internet or other low-bandwidth network environments. Uses zlib library to compress pre-processed pixel data to maximize compression ratios and minimize CPU usage.
- In the **Compression Level** drop-down list, select the level of compression as **Default** or from **1** to **9** where **1** is the lowest compression and **9** is highly compressed.
- The **JPEG Image Quality** option is not editable and is set at **6**.
- In the **Cursor Shape Updates** drop-down list, select **Enable**, **Ignore**, or **Disable**. The default is **Ignore**.
- Select **Use CopyRect** to gain efficiency when moving items on the screen.
- Select **Restricted Colors (256 Colors)** for more efficiency with slightly less depth of color.
- Select **Reverse Mouse Buttons 2 and 3** to switch the right-click and left-click buttons.
- Select **View Only** to disable keyboard and mouse events in the desktop window.
- Select **Share Desktop** to allow multiple users to view and use the same VNC desktop.
- Select **Display Bookmark to Mobile Connect clients** to enable bookmark viewing on Mobile Connect clients. Mobile Connect must be running version 2.0 or newer to view and access this bookmark.

  NOTE: Support varies by device and might require supported third-party applications to be installed.

Citrix Portal (Citrix)

- In the **Resource Window Size** drop-down list, select the default Citrix portal screen size to be used when users execute this bookmark.

1 Select an **Access Type Selection**. **Smart** or **Manual**.

- **Smart**: Allows the firmware to decide which mode to launch on the client.

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

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

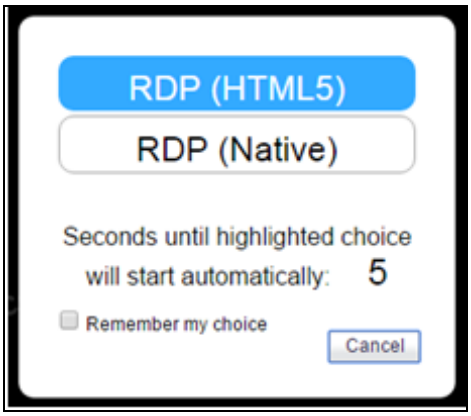
The launch sequence is as follows: **HTML5**, **Native**, and **ActiveX**. Selecting Manual allows you to change, enable, or disable the launch methods. If you select **Native** to launch the Citrix bookmark, then the SMA Connect Agent launches the Citrix Receiver on the local machine to do the Citrix connection.

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

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

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

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

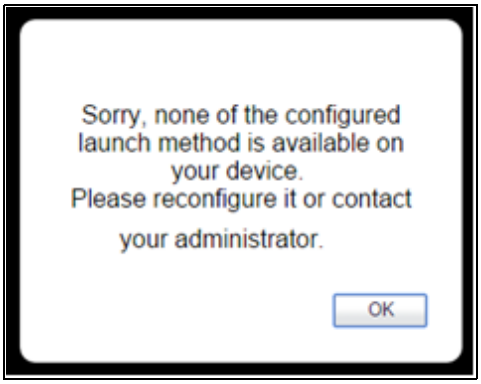


If the **Remember my choice** option is selected during the launch time, the selected mode is remembered through a cookie.

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

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

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



- Optionally select **HTTPS Mode** to use HTTPS to securely access the Citrix Portal.
- Optionally, select **Always use specified Citrix ICA Server** and specify the IP address in the **ICA Server Address** field that appears. This setting allows you to specify the Citrix ICA Server address for the Citrix ICA session. By default, the bookmark uses the information provided in the ICA configuration on the Citrix server.
- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.

Web (HTTP)

- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in 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 on page 396.
- Select **Forms-based Authentication** 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>.
- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.

Secure Web (HTTPS)

- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in 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 on page 396.
- Select **Forms-based Authentication** 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>.
- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.

External Web Site

- Select **HTTPS Mode** to use SSL to encrypt communications with this Web site.
- Select **Disable Security Warning** if you do not want to see any security warnings when accessing this Web site. Security warnings are normally displayed when this bookmark refers to anything other than an Application Offloaded Web site.
- Select **Automatically log in** to enable the virtual host domain SSO for this bookmark. If the host in the bookmark refers to a portal with the same shared domain as this portal, selecting this check box allows you to automatically be logged in with this portal's credential.
- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.

Mobile Connect

- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.

> **NOTE:** Mobile Connect must be running version 2.0 or newer to view and access this Bookmark. Support varies by device and might require supported third-party applications to be installed.

File Shares (CIFS)

NOTE: SMB2 and SMB3 protocols are currently not supported. Servers should be configured to allow communication from a Linux based client.

- To restrict access on the client UI, select **Set user to access the specific files/folders**. To completely restrict access, navigate to the **Services** > **Policies** page to set a policy for access constraints. For more information, see Adding User Policies on page 367.
- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in to the RDP server. Enable the **Use Login Domain for SSO** option to pass the user's domain 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 on page 396.
- Enable **Display Bookmark to Mobile Connect clients** to send bookmark information to Mobile Connect clients.

  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 disables access to the DFS file shares from other domains. The SMA/SRA appliance is not a domain member and is not 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 Secure Mobile Access session for log in 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 on page 396.
- Enable **Display Bookmark to Mobile Connect clients** to send bookmark information to Mobile Connect clients.

  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 disables access to the DFS file shares from other domains. The SMA/SRA appliance is not a domain member and is not able to connect to the DFS shares.

  DFS file shares on a stand-alone root are not affected by this Microsoft restriction.

SSH File Transfer Protocol (SFTP)

- 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 Secure Mobile Access session for log in 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 on page 396.
- Enable **Display Bookmark to Mobile Connect clients** to send bookmark information to Mobile Connect clients.

Telnet

- Single sign-on is supported for Telnet bookmarks. The bookmark must be configured enabling the **Automatically log in** option in the bookmark settings. If the correct username and password are set, the session is logged in automatically.
- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in 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 on page 396.
- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.

Secure Shell Version 2 (SSHv2)

- Single sign-on is supported for SSH bookmarks. The bookmark must be configured enabling the **Automatically log in** option in the bookmark settings. If the correct username and password are set, the session is logged in automatically.
- For the SSHv2 HTML5 bookmark, SSO is supported for both user name and password authentication. If SSO has failed, a menu pops-up to allow you to decide whether to manually fill in the credentials or cancel the log in.

- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in 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 on page 396.
- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.

2 Click **Accept** to update the configuration. After the configuration has been updated, the new user bookmark is displayed in the **Edit Local User** window.

Per device license support

When a Remote Desktop Session Host (RD Session Host) server is configured to use the Per-Device licensing mode, and a client computer or device connects to an RD Session Host server for the first time, the client computer or device is issued a temporary license by default. When a client computer or device connects to an RD Session Host server for the second time, if the Remote Desktop license server is activated and enough Remote Desktop Services (RDS) Per-Device Client Access Licenses (CALs) are available, the license server issues the client computer or device a permanent RDS Per-Device CAL. If the license server is not activated or does not have any RDS Per-Device CALs available, the device continues to use the temporary license. The temporary license is valid for 90 days.

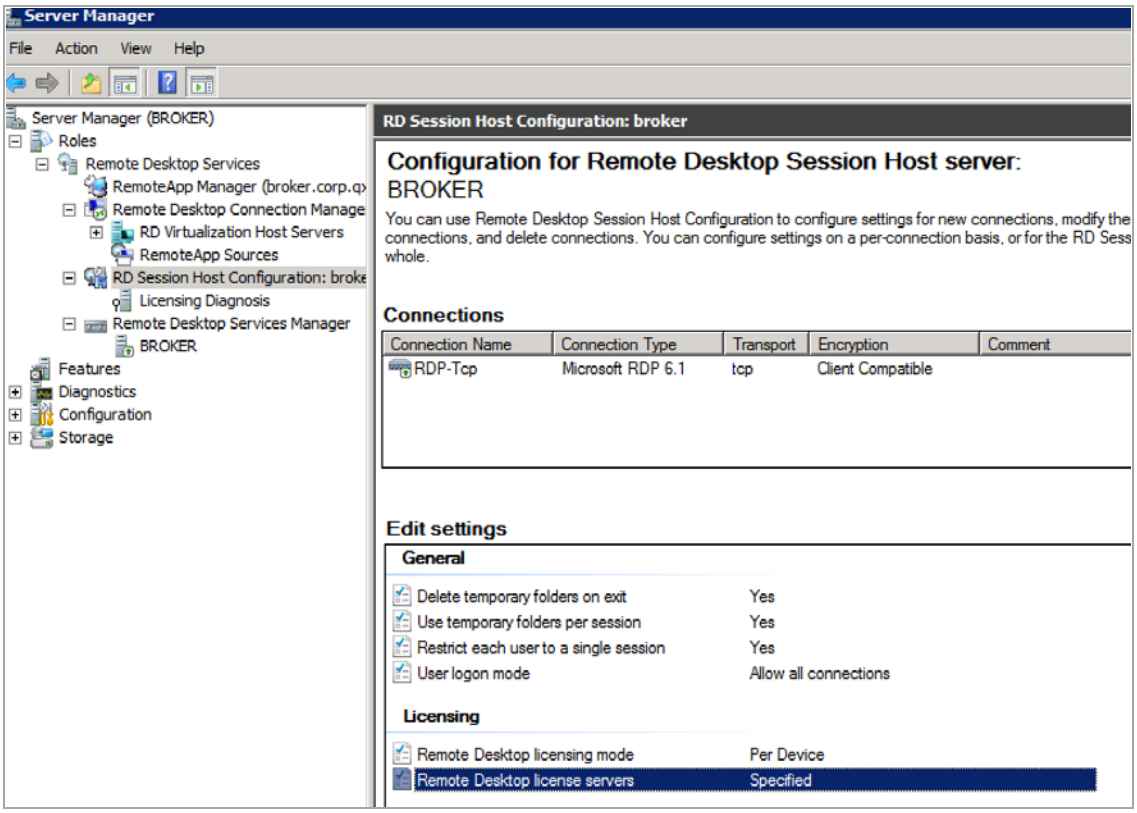
A permanent RDS Per-Device CAL issued by a license server is configured to automatically expire after a random period between 52 and 89 days, at which time the RDS Per-Device CAL returns to the pool of available RDS Per-Device CALs on the license server.

Configuring a per-device license server

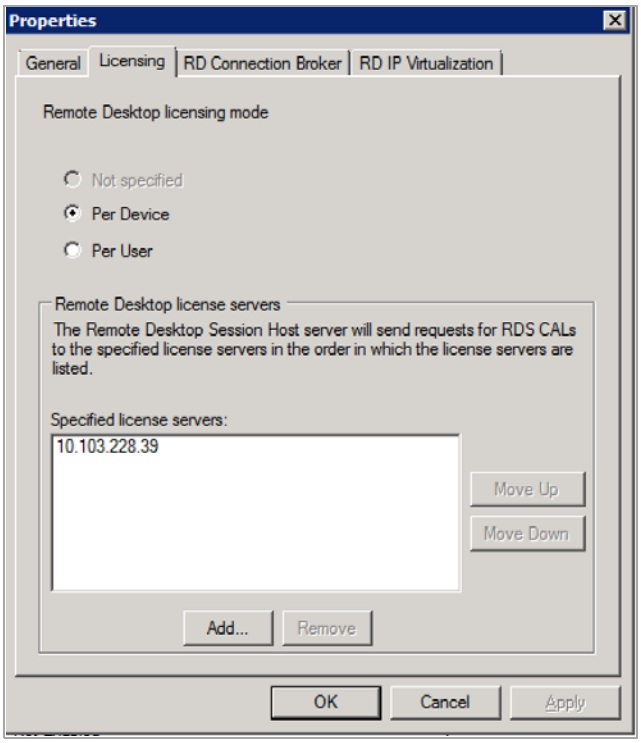
This section describes how to configure Per-Device licensing on Windows Server 2008 R2. Configuration details may vary for other server versions.

To add a license server:

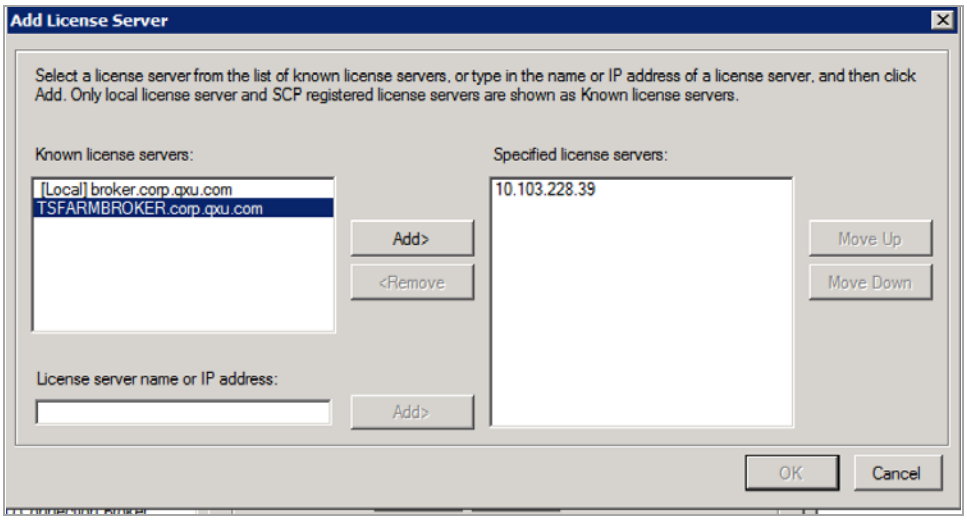
1 In the Server Manager screen under **Edit Settings**, double-click **Remote Desktop license servers**.



2 In the Properties dialog that appears, on the Licensing page, click **Add**.

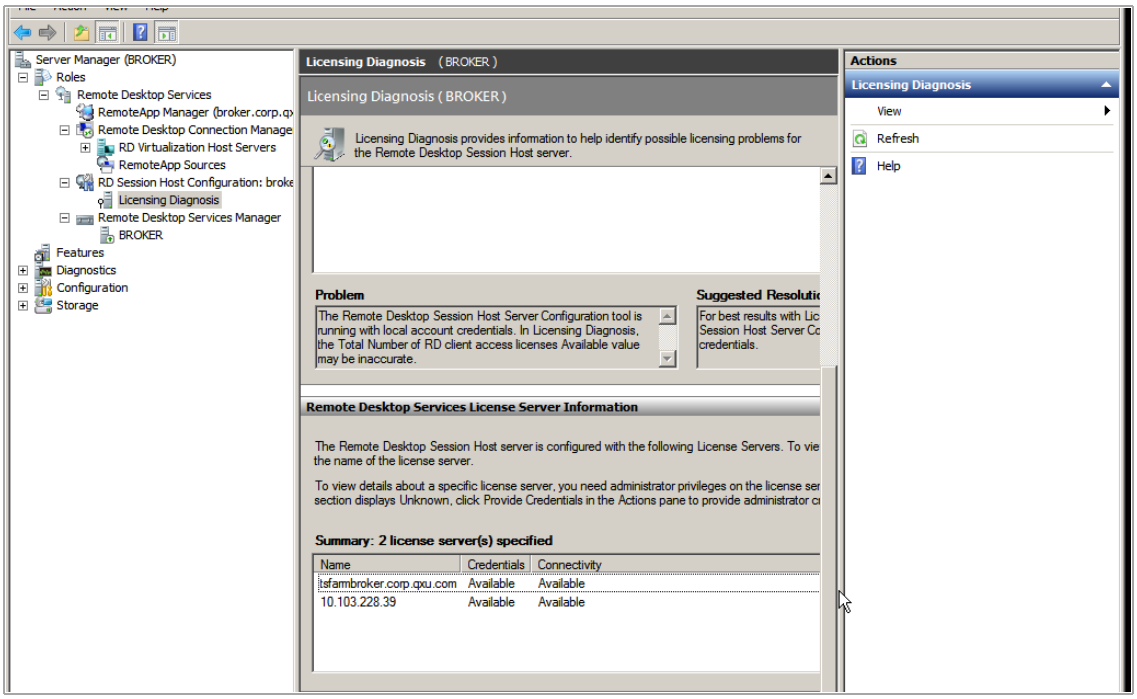


3 The **Add License Server** dialog appears. Select the License server name or IP address field and click **Add**.



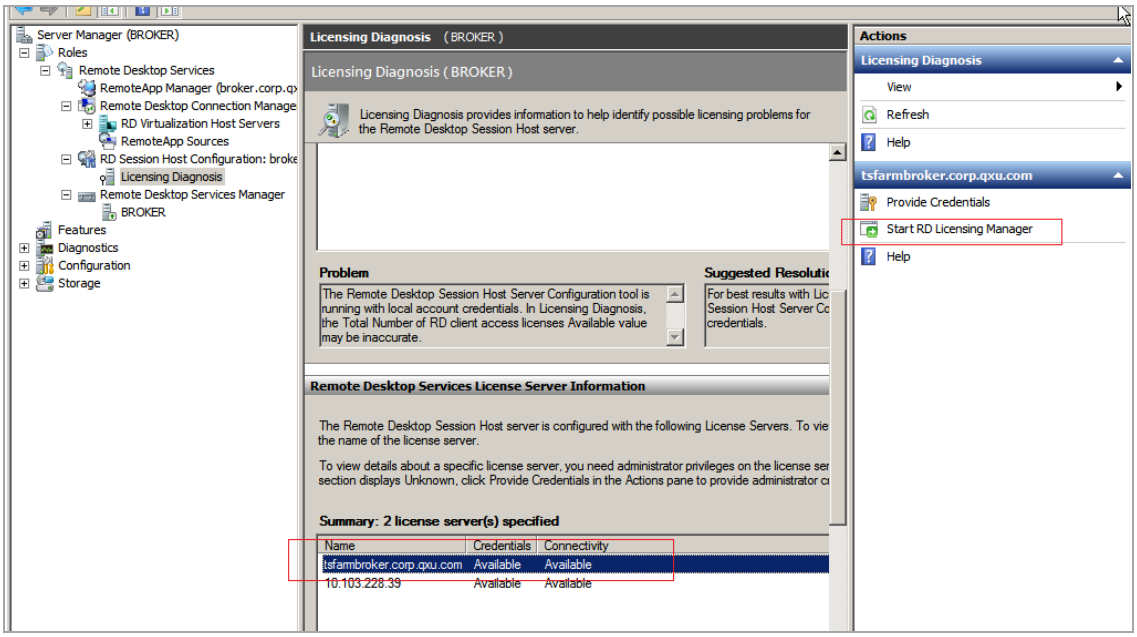
To configure a license server:

1 On the Server Manager screen, click **Licensing Diagnosis** in the left navigation pane.

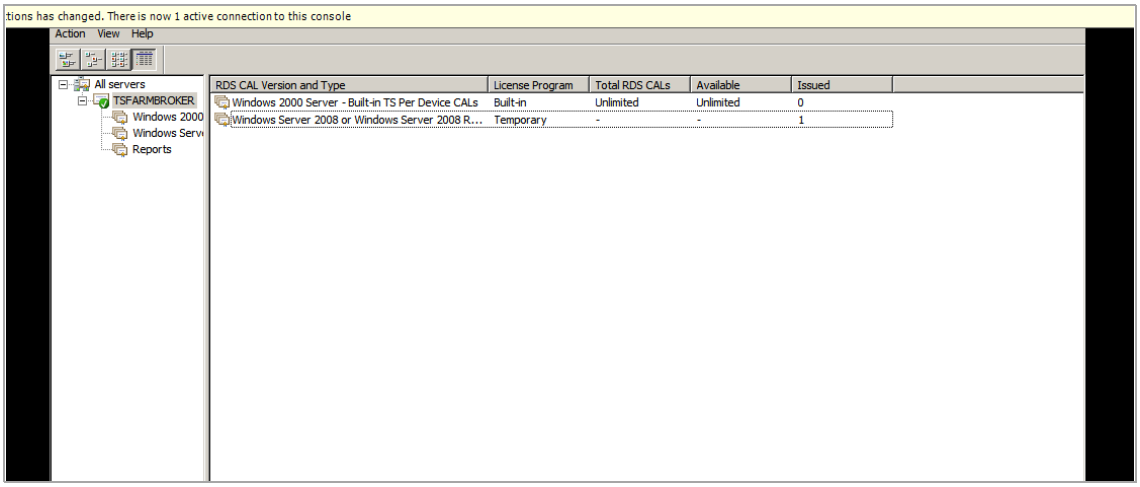


2 In the middle pane under **license server(s) specified**, select the desired server name or IP address. The right pane displays additional actions.

3 In the right pane, click **Start RD Licensing Manager**.



4 The next screen lists the available licenses, shown as **Temporary**.

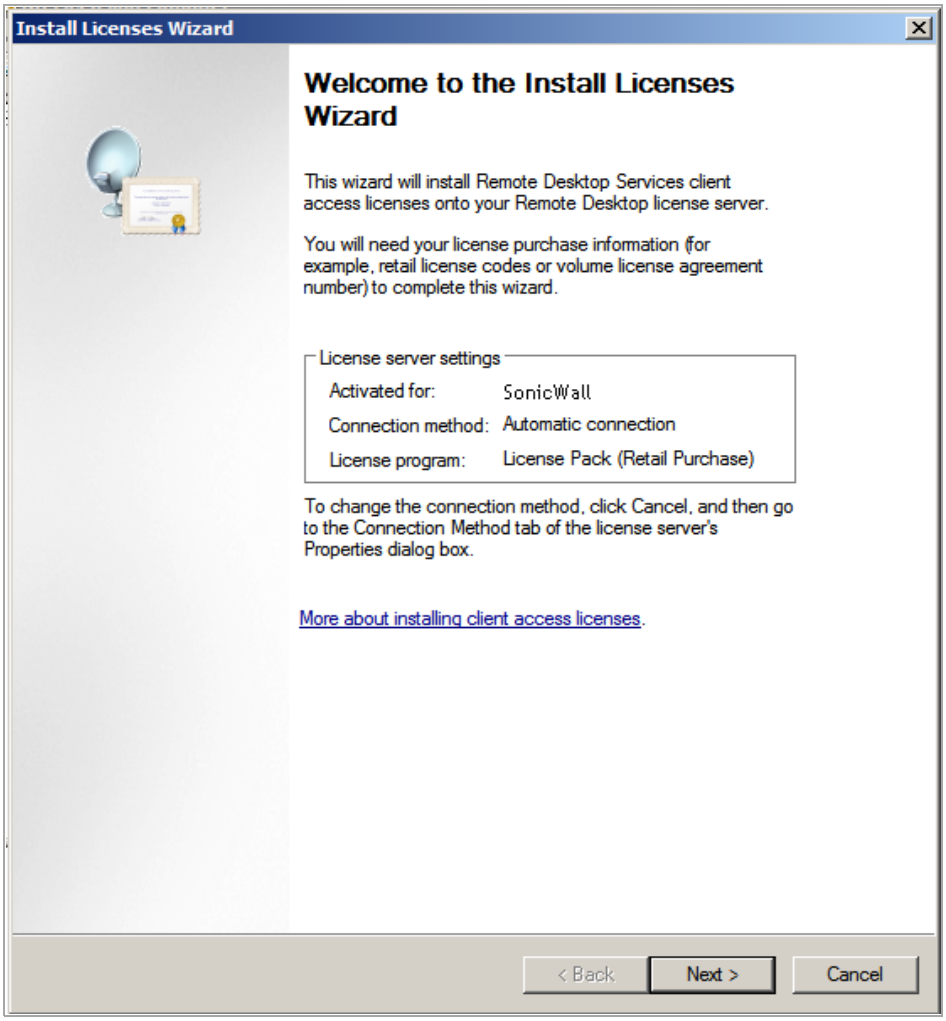


Manage your Per-Device license from this screen.

Every remote connection from different web browsers consumes a device license. You can revoke the licenses within the previous screen, but only a few times within a certain period.

To install a Remote Desktop Services client access license:

1 Right-click the server in the left pane under All servers and select install license, and then follow the wizard step by step. Make sure your Internet connection is available.



Creating a Citrix Bookmark for a Local User

Citrix bookmarks are supported on Windows, MacOS, and Linux. 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 automatically decides which Citrix client version to use.

NOTE: Citrix Java Bookmarks are no longer officially supported by SonicWall Inc. because Citrix has ended support for the Java Receiver. SonicWall Inc. recommends using HTML5, Native, or ActiveX access methods for Citrix Bookmarks.

To configure a Citrix bookmark for a user:

1 Navigate to **Users > Local Users** and click the configure icon next to the user.

2 In the **Edit Local User** page, select the **Bookmarks** page.

3 Click **Add Bookmark...**

4 Enter a name for the bookmark in the **Bookmark Name** field.

5 Enter the name or IP address of the bookmark in the **Name or IP Address** field.

> **NOTE:** HTTPS, HTTP, Citrix, SSHv2, Telnet, and VNC all take a port option :portnum. HTTP, HTTPS, and Fileshares can also have the path specified to a directory or file.

6 Optionally enter a friendly **Description** to be displayed in the bookmark table.

7 Optionally enter a comma-separated list of **Tabs** where this bookmark should appear. Standard tabs (Desktop, Web, Files, Terminal, and Mobile) do not need to be specified. For example; Favorites, Tab 1, Tab 2.

8 From the **Service** drop-down list, select **Citrix Portal (Citrix)**. The display changes.

9 Select a **Resource Window Size** selection from the drop-down list.

10 Select an **Access Type Selection**. **Smart** or **Manual**.

- **Smart**: Allows the firmware to decide which mode to launch on the client.

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

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

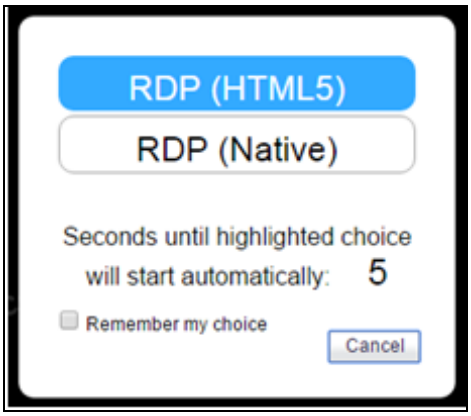
The launch sequence is as follows: **HTML5**, **Native**, and **ActiveX**. Selecting Manual allows you to change, enable, or disable the launch methods. If you select **Native** to launch the Citrix bookmark, then the SMA Connect Agent launches the Citrix Receiver on the local machine to do the Citrix connection.

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

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

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

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

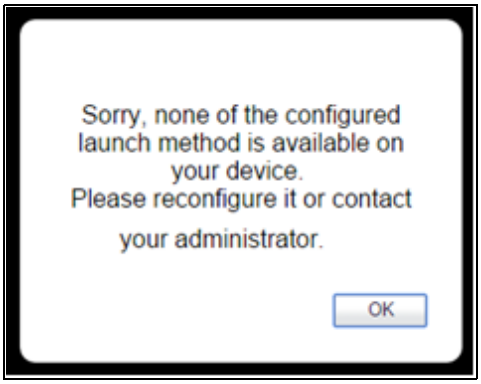


If the **Remember my choice** option is selected during the launch time, the selected mode is remembered through a cookie.

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

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

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



11 Select the box next to **HTTPS Mode** to securely access the Citrix portal.

12 Optionally, select **Always use specified Citrix ICA Server** and specify the IP address in the **ICA Server Address** field that appears. This setting allows you to specify the Citrix ICA Server address for the Citrix ICA session. By default, the bookmark uses the information provided in the ICA configuration on the Citrix server.

- **Windows** - The SMA Connect Agent tries to open the ICA file to launch the Citrix Receiver. If the Citrix Receiver is not installed, the system pops up a message.
- **Macintosh** - The SMA Connect Agent searches for the “Citrix Receiver” App; to be sure you have installed the App. The SMA Connect Agent launches the “Citrix Receiver” to make the Citrix

connection. If you have not yet installed the App, the SMA Connect Agent pops up an alert message for you to start the installation.

13 Click **Accept**.

Creating Bookmarks with Custom SSO Credentials

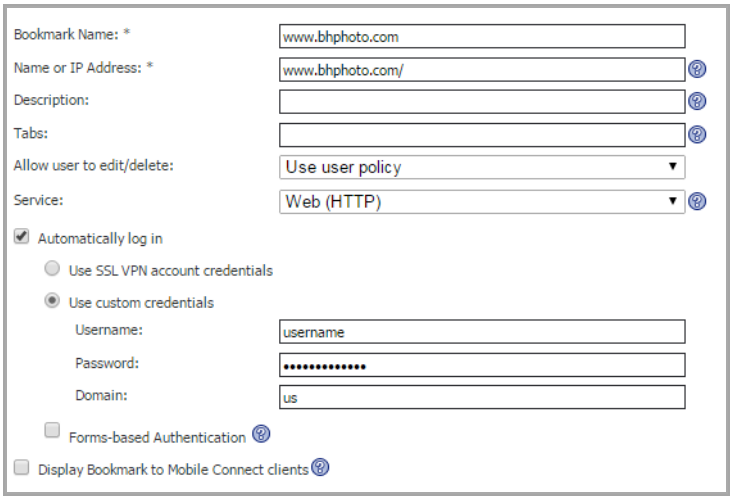
The administrator can configure custom Single Sign On (SSO) credentials for each user, group, or globally in HTTP(S), RDP (ActiveX, VNC), File Shares (CIFS), and FTP bookmarks. This feature is used to access resources such as HTTP, RDP and FTP servers that need a domain prefix for SSO authentication. Users can log in to the SMA/SRA appliance as *username*, and click a customized bookmark to access a server with *domain**username*. Either straight textual parameters or dynamic variables might be used for the **Username** and **Domain**. For the **Password** field, enter the custom password to be passed, or leave the field blank to pass the current user's password to the bookmark.

To configure custom SSO credentials, and to configure Single Sign-On for Forms-based Authentication (FBA):

1 Create or edit a Citrix, HTTP(S), RDP, File Shares (CIFS), or FTP bookmark as described in Adding or Editing User Bookmarks on page 374.

2 For a Citrix bookmark, enable the **Automatically log in** option. Only **Forms-based Authentication** can be used for a Citrix SSO bookmark.

In the **Bookmarks** page, select the **Use Custom Credentials** option.



3 In the **Username** and **Domain** fields, enter the custom text to be passed to the bookmark, or use dynamic variables, as follows:

Dynamic variables

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

4 In the **Password** field, enter the custom password to be passed, or leave the field blank to pass the current user's password to the bookmark.

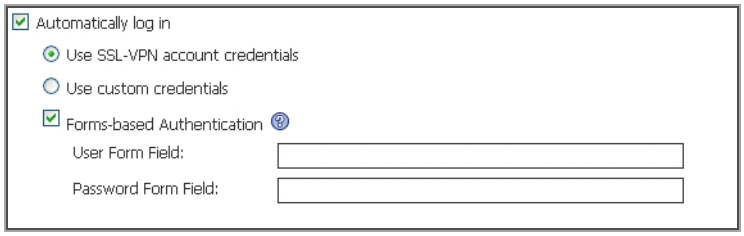
5 Select **Forms-based Authentication** to configure Single Sign-On for Forms-based authentication.

- **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:

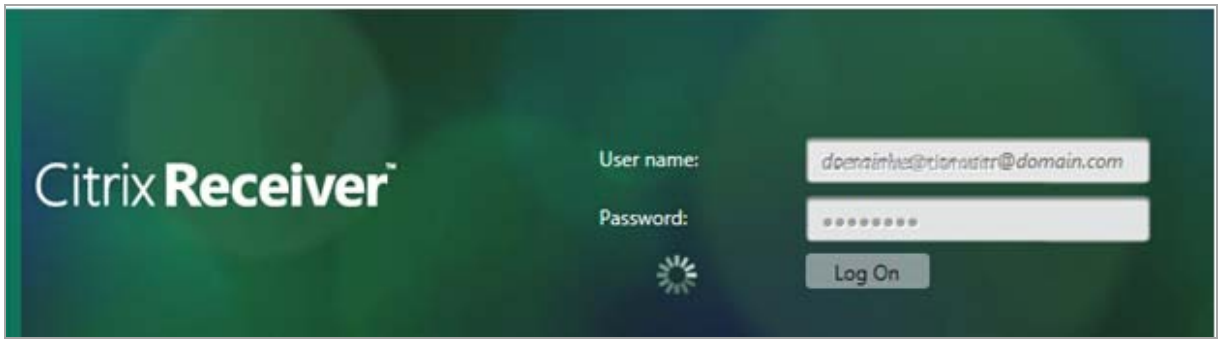
  ```
  <input type=password name='PASSWORD' id='PASSWORD' maxlength=128>
  ```



6 Check **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.

7 Click **Accept**.

After launching the Citrix bookmark, you can automatically log in to the Citrix StoreFront portal as shown in the following image and it is ready to use the **XenApp** or **XenDesktop**.



Configuring Login Policies

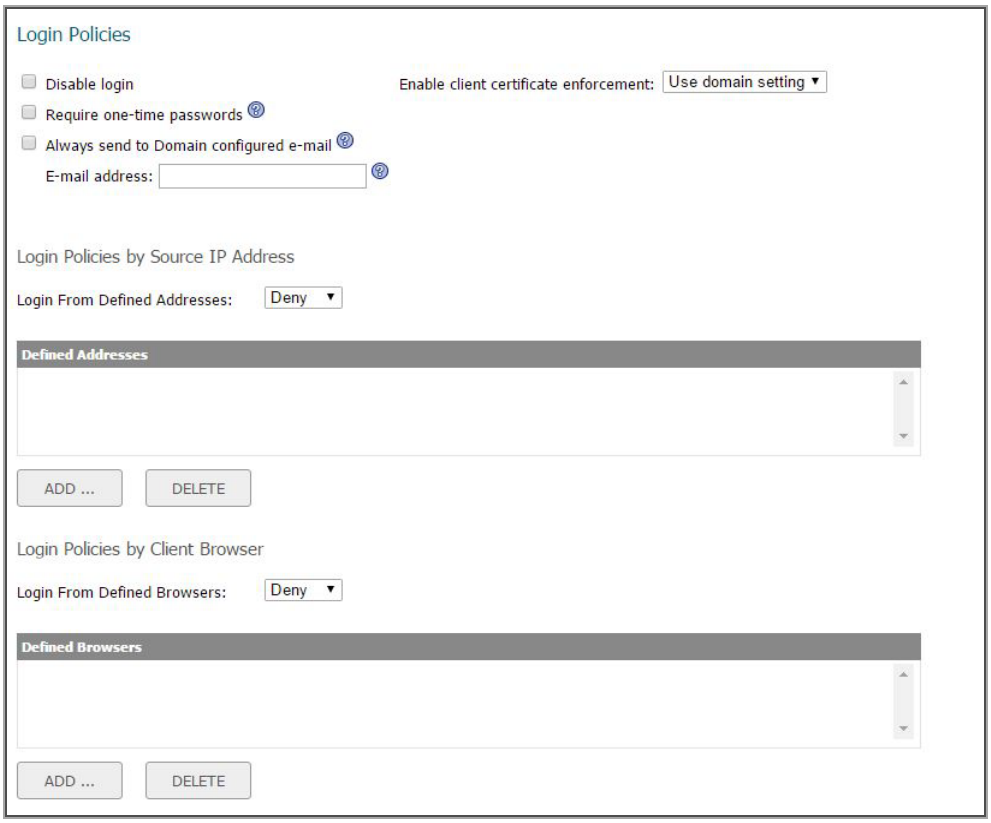
The **Login Policies page** provides configuration options for policies that allow or deny users with specific IP addresses from having login privileges to the SMA/SRA appliance.

To allow or deny specific users from logging into the appliance:

1 Navigate to the **Users > Local Users** page.

2 Click the configure icon for the user you want to configure. The **Edit Local User** page is displayed.

3 Click the **Login Policies** page. The **Edit Local User** - **Login Policies** page is displayed.



4 To block the specified user or users from logging into the appliance, select **Disable login**.

5 Optionally select **Enable client certificate enforcement** 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 appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this check box 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 matches the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

6 To require the use of one-time passwords for the specified user to log in to the appliance, select **Require one-time passwords**.

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 One Time Password Overview on page 49.

> **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 SMA/SRA appliance and that domain.

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** window is displayed.

9 In the **Define Address** window, 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** window.
- **IPv6 Address** - This enables you to select a specific IPv6 address.
- **IPv6 Network** - 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** window.

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** - Type an IPv6 address, such as **2007::1:2:3:4**.
- **IPv6 Network** - 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**.

11 Click **Add**. The address or address range is displayed in the **Defined Addresses** list in the **Edit User Settings** window. 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 is now applied to addresses in this range.

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** window is displayed.

13 In the **Define Browser** window, 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 Firefox and Internet Explorer is: javascript:document:writeln(navigator.userAgent)

14 Click **Accept**. The new login policy is saved.

Configuring End Point Control for Users

To configure the End Point Control profiles used by a local user:

1 Navigate to the **Users** > **Local Users** page.

2 Click the configure icon next to the user to be configured for EPC. The **Edit Local User** window is displayed.

3 Click the **EPC** page. The **EPC** window is displayed.

4 Configure EPC user settings and add or remove device profiles.

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 Global Configuration on page 429.

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.

Users > Local Groups Page

Group memberships are split into two groups, 'primary' and 'additional'.

Primary groups - Used to assign simple policies, such as timeouts and the ability to add/edit bookmarks. Advanced policies, such as URL or network object policies, might come from primary or additional groups.

Additional Groups - Multiple additional groups could be assigned, but in the case of conflicting policies, the primary group takes precedence over any additional groups.

Keep in mind that users can only belong to groups within a single domain.

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 no longer appears 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 are able to delete the group on the **Edit Group Settings** 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 are added, unless otherwise specified.

To create a new group:

1. Click **Add Group**. The **Add Local Group** window is displayed.
2. In the **Add Local Group** window, enter a descriptive name for the group in the **Group Name** field.
3. Select the appropriate domain from the **Domain** drop-down list. The domain is mapped to the group.
4. Click **Accept** to update the configuration. After the group has been added, the new group is added to the **Local Groups** window.

All of the configured groups are displayed in the **Users > Local Groups** page, listed in alphabetical order.

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 pages: **General**, **Portal**, **NetExtender/Mobile Connect**, **Routes**, **Policies**, and **Bookmarks**.

See the following sections for information about configuring settings:

- Editing General Group Settings on page 402
- Modifying Group Portal Settings on page 402
- Enabling Group NetExtender/Mobile Connect Settings on page 403
- Enabling Routes for Groups on page 406
- Adding Group Policies on page 407
- Editing a Policy for a File Share on page 409
- Configuring Group Bookmarks on page 410

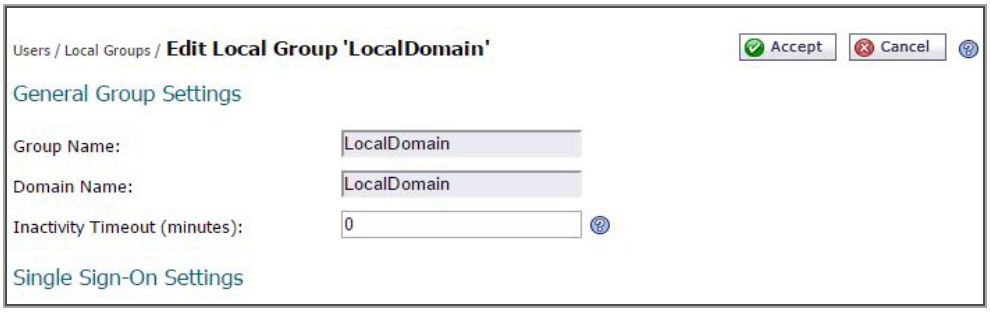
Editing General Group Settings

The **General** page provides configuration options for a group's inactivity timeout value and single sign-on settings.

To modify the general user settings:

1 In the left column, navigate to the **Users** > **Local Groups**.

2 Click the configure icon next to the group you want to configure. The **General** page of the **Edit Group Settings** window displays. The **General Group Settings** section displays the following non-configurable fields: **Group Name** and **Domain Name**.



3 To set the inactivity timeout for the group, meaning that users are signed out of the Virtual Office after no activity on their computer for the specified time period, enter the number of minutes of inactivity to allow in the **Inactivity Timeout** field. Set to 0 to use the global timeout.

> **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 takes precedence over the group timeout and the group timeout takes 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.

4 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 in the SMA/SRA appliance 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.

5 Click **Accept** to save the configuration changes.

Modifying Group Portal Settings

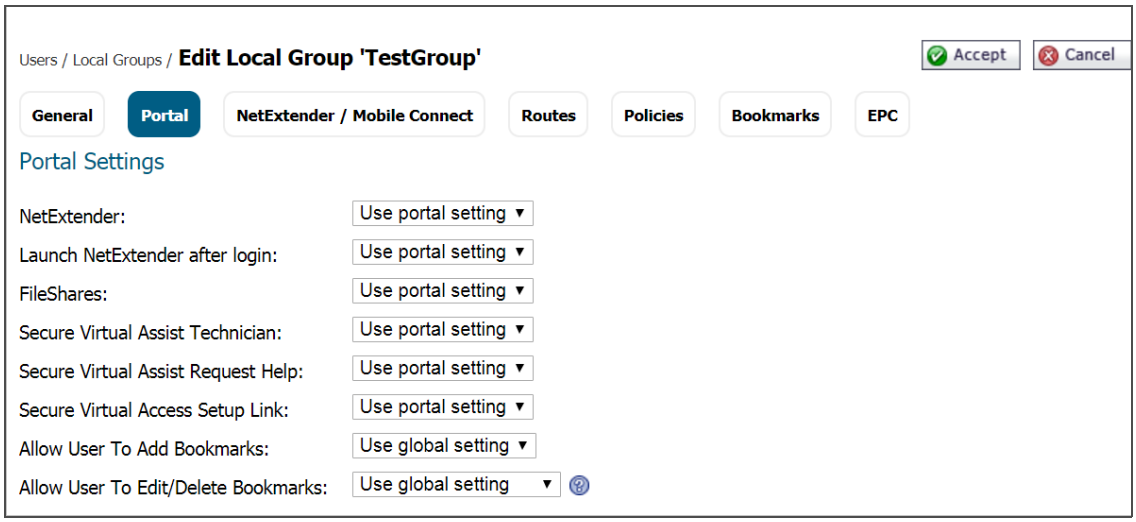
The **Portal Settings** section provides configuration options for portal settings for this group.

To configure portal settings for this group:

1 In the left column, navigate to the **Users** > **Local Groups**.

2 Click the configure icon next to the group you want to configure.

3 In the **Edit Local Group** page, click **Portal**.



4 In the **Portal Settings** section, for **NetExtender**, **Launch NetExtender after login**, **FileShares**, **Virtual Assist Technician**, **Virtual Assist Request Help**, **Virtual Access Setup Link**, select one of the following portal settings for this group:

- **Use portal setting** – The settings defined in the main portal settings are 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** page of the Edit Portal screen.
- **Enabled** – Enable this portal feature for this group.
- **Disabled** – Disable this portal feature for this group.

Because Mobile Connect acts as a NetExtender client when connecting to the appliance, the setting for NetExtender also controls access by Mobile Connect users.

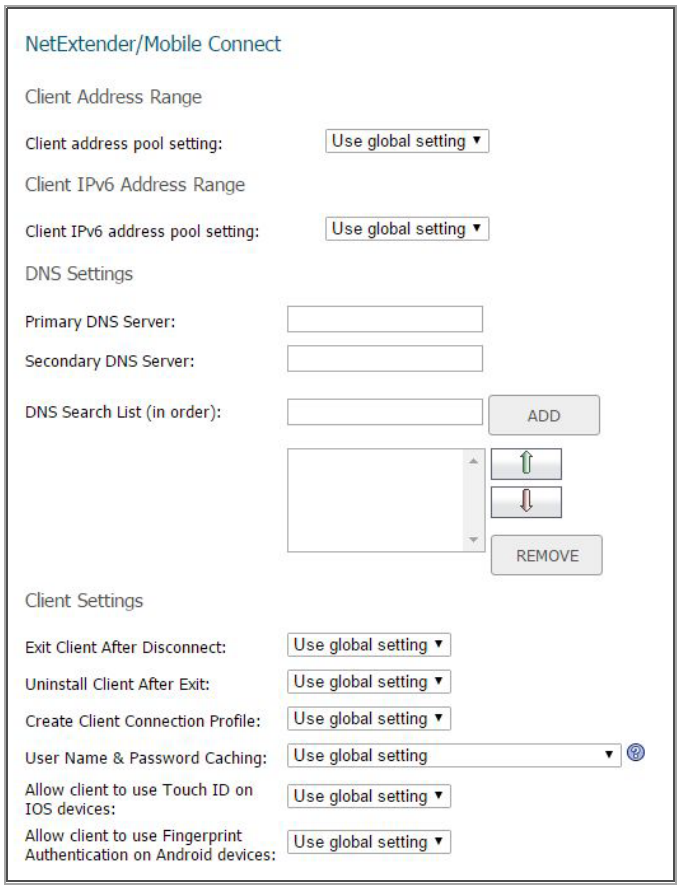
5 To allow users in this group to add new bookmarks, select **Allow** from the **Allow user to add bookmarks** drop-down menu. To prevent users from adding new bookmarks, select **Deny**. To use the setting defined globally, select **Use global setting**. See Edit Global Settings on page 429 for information about global settings.

6 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 setting defined globally, select **Use global setting**.

7 Click **Accept**.

Enabling Group NetExtender/Mobile Connect Settings

This feature is for external users, who inherits the settings from their assigned group upon login. NetExtender/Mobile Connect client settings can be specified for the group, or use the global settings. For information about configuring global settings, see Edit Global Settings on page 429.



To enable NetExtender ranges and configure DNS and client settings for a group:

1. Navigate to **Users > Local Groups**.
2. Click the configure icon next to the group you want to configure.
3. In the **Edit Local Group** page, select the **NetExtender/Mobile Connect** page.
4. Choose the **Client address pool setting**. Options include using the global settings, the DHCP settings, or a Static Pool.
5. Choose the **IPv6 address pool setting**. Options include using the global settings, the DHCPv6 settings, or a Static Pool.
6. Under **DNS Settings**, type the address of the primary DNS server in the **Primary DNS Server** field.
7. Optionally type the IP address of the secondary server in the **Secondary DNS Server** field.
8. In the **DNS Search List** field, type the DNS domain suffix and click **Add**. Next, use the up and down arrows to prioritize multiple DNS domains in the order they should be used.

   For SMA/SRA appliances supporting connections from Apple iPhones, iPads, or other iOS devices using SonicWall Inc. Mobile Connect, use this DNS Search List. This DNS domain is set on the VPN interface of the iPhone/iPad after the device makes a connection to the appliance. When the mobile device user accesses a URL, iOS determines if the domain matches the VPN interface's domain, and if so, uses the

VPN interface's DNS server to resolve the hostname lookup. Otherwise, the Wi-Fi or 3G/4G DNS server is used that is not able to resolve hosts within the company intranet.

9 Under **Client Settings**, select one of the following from the **Exit Client After Disconnect** drop-down list:

- **Use global setting** - Take the action specified by the global setting. See Edit Global Settings on page 429.
- **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.

10 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 on page 429.
- **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.

11 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 on page 429.
- **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.

12 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 on page 429.
- **Allow saving of user name only** - Allow caching of the user name for members of the group. Group members only need to enter their passwords 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 are 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 are required to enter both user name and password when starting NetExtender. Overrides the global setting.

13 In the **Allow client to use Touch ID on IOS devices**, the control only blocks future attempts to log in with fingerprint technology on IOS devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.

14 In the **Allow client to use Fingerprint Authentication on Android devices**, the control only blocks future attempts to log in with fingerprint technology on Android devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.

15 In the **Allow client to use Touch ID on macOS devices**, the control only blocks future attempts to log in with fingerprint technology on macOS devices when the option is disabled as there is no method for the server to change the client settings until the client attempts a connection. So in some cases, a client might not be conforming to previous policies for the initial connection. Configuration is allowed globally, by group, or per user.

16 Click **Accept**.

Enabling Routes for Groups

The **Routes** page allows the administrator to add and configure client routes. IPv6 client routes are supported on SMA/SRA appliances.

To enable multiple routes for a group:

1 Navigate to **Users > Local Groups.**

2 Click the configure icon next to the group you want to configure.

3 In the **Edit Local Group** page, go to the **Client Routes** section.

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 on page 429.
- **Enabled** - Force all traffic for this user, including traffic destined to the remote users' local network, over the Secure Mobile Access 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.

5 To add globally defined NetExtender client routes for members of this group, select **Add Global NetExtender Client Routes**.

6 To configure NetExtender client routes specifically for members of this group, click **Add Client Route**.

7 On the **Add Client Route** screen, 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.

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.

9 On the **Add Client Route** screen, click **Accept**.

10 On the **Edit Local Group** page, click **Accept**.

Enabling Group NetExtender Client Routes

To enable global NetExtender client routes for groups that are already created:

1 Navigate to **Users > Local Groups**.

2 Click the configure icon next to the group you want to configure.

3 In the **Client Routes** section, select **Add Global Client Routes**.

4 Click **Accept**.

Enabling Tunnel All Mode for Local Groups

This feature is for external users, who inherit the settings from their assigned group upon login. Tunnel all mode ensures that all network communications are tunneled securely through the Secure Mobile Access tunnel.

To enable tunnel all mode:

1 Navigate to **Users > Local Groups**.

2 Click the configure icon next to the group you want to configure.

3 In the **Edit Local Group** section, select **Enable** from the **Tunnel All Mode** drop-down list.

4 Click **Accept**.

NOTE: You can optionally tunnel-all Secure Mobile Access 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 window.

Adding Group Policies

With group access policies, all traffic is allowed by default. Additional allow and deny policies could be created by destination address or address range and by service type.

The most specific policy takes precedence over less specific policies. For example, a policy that applies to only one IP address has 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) takes 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 takes precedence over a group policy that denies access to a single IP address.

NOTE: Within the group policy scheme, the primary group policy is always enforced over any additional group policies.

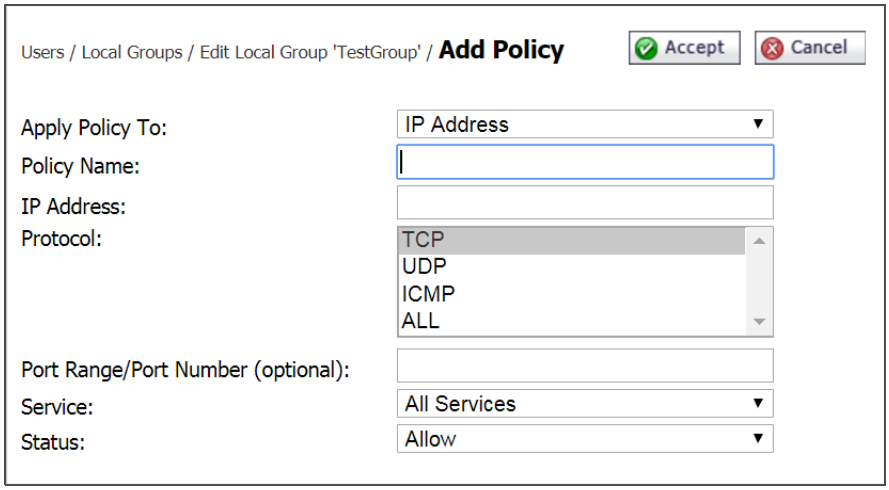
To define group access policies:

1 Navigate to **Users > Local Groups**.

2 Click the configure icon next to the group you want to configure.

3 In the **Edit Local Group** page, select the **Policies** page.

4 On the **Policies** page, click **Add Policy**. The **Add Policy** screen is displayed.



5 Define a name for the policy in the **Policy Name** field.

6 In the **Apply Policy To** drop-down list, select whether the policy is applied to an individual host, a range of addresses, all addresses, a network object, a server path, or a URL object. You can also select an individual IPv6 host, a range of IPv6 addresses, or all IPv6 addresses. The **Add Policy** window changes depending on what type of object you select in the **Apply Policy To** drop-down list.

> **NOTE:** The Secure Mobile Access policies apply to the destination address(es) of the SMA/SRA connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the SMA/SRA gateway through the policy engine. It is possible to control source logins by IP address from the user's **Login Policies** page. For more information, refer to Configuring Login Policies on page 397.

- **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 Network** - 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 Adding Network Objects on page 139.
- **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 on page 409.
- **URL Object** - If your policy applies to a predefined URL object, type the URL into the **URL** field.
- **All IPv6 Address** - If your policy applies to all IPv6 addresses, you do not need to enter any IP address information.
- **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 Network** - 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.

7 Select the desired **Protocol**. The available value options in the Protocol field include: **TCP**, **UDP**, **ICMP**, and **ALL**. You can select multiple items among **TCP**, **UDP**, and **ICMP**. However, when **ALL** is selected, all others options are deselected.

> **NOTE:** The protocol setting only appears when the Service is set to "NetExtender & Mobile Connect" or "All Services."

8 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.

9 Select **Allow** or **Deny** from the **Status** drop-down list to either permit or deny SMA/SRA connections for the specified service and host machine.

10 Click **Accept** to update the configuration. After the configuration has been updated, the new group policy is displayed in the **Edit Local Group** 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:

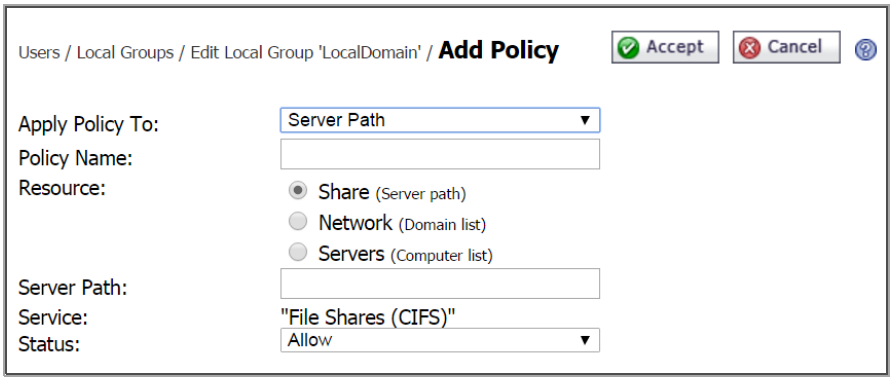
1 Navigate to **Users > Local Groups**.

2 Click the configure icon next to the group you want to configure.

3 Select the **Policies** page.

4 Click **Add Policy...**

5 Select **Server Path** from the **Apply Policy To** drop-down list.



6 Type a name for the policy in the **Policy Name** field.

7 For **Resource**, select **Share (Server path)** for the resource type.

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.

9 Select **Allow** or **Deny** from the **Status** drop-down list.

10 Click **Accept**.

Configuring Group Bookmarks

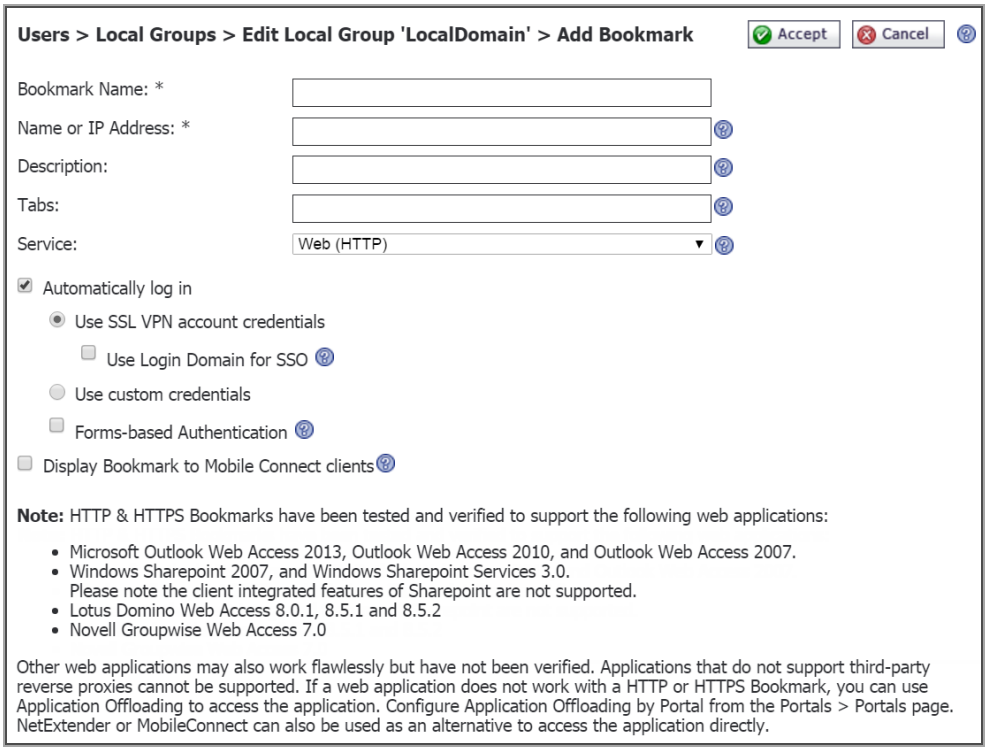
SMA/SRA appliance bookmarks provide a convenient way for Secure Mobile Access users to access computers on the local area network that they connect to frequently. Group bookmarks apply to all members of a specific group.

To define group bookmarks:

1 Navigate to the **Users** > **Local Groups** window.

2 Click the configure icon for the group for which you want to create a bookmark. The **Edit Local Group** page is displayed.

3 On the **Bookmarks** page, click **Add Bookmark**. The **Add Bookmark** screen is displayed.



> **NOTE:** When group bookmarks are defined, all group members see the defined bookmarks from the Secure Mobile Access user portal. Individual group members are not able to delete or modify group bookmarks.

4 Enter a string that is the name of the bookmark in the **Bookmark Name** field.

5 Enter the fully qualified domain name (FQDN) or the IPv4 or 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**. IPv6 is not supported for File Shares or VNC bookmarks.

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.

6 Enter a friendly description in the **Description** field to be displayed in the Bookmarks table.

7 Select one of the service types from the **Service** drop-down list. For the specific service you select from the **Service** drop-down list, additional fields might appear. Use the following information for the chosen service to complete the building of the bookmark:

Terminal Services (RDP); Terminal Services (RDP-HTML5) or Terminal Services (RDP-Native)

- In the **Screen Size** drop-down menu, 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 might want to provide a path to where your application resides on your remote computer by typing the path in the **Application and Path** field.

- In the **Colors** drop-down list, select the default color depth for the terminal service screen when users execute this bookmark.

8 Select an **Access Type Selection**. **Smart** or **Manual**.

- **Smart**: Allows the firmware to decide which mode to launch on the client.

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

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

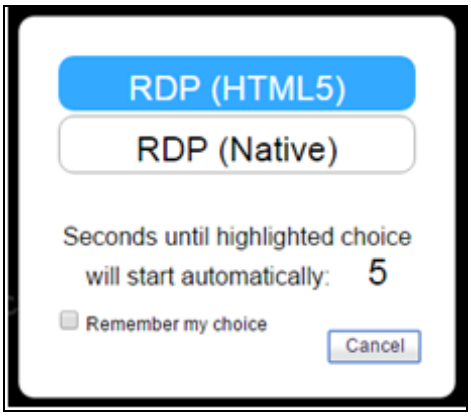
  The launch sequence is as follows: **HTML5** and **Native**. Selecting Manual allows you to change, enable, or disable the launch methods. If you select **Native** to launch the RDP bookmark, then the SMA Connect Agent launches the RDP Receiver on the local machine to do the RDP connection.

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

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

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

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

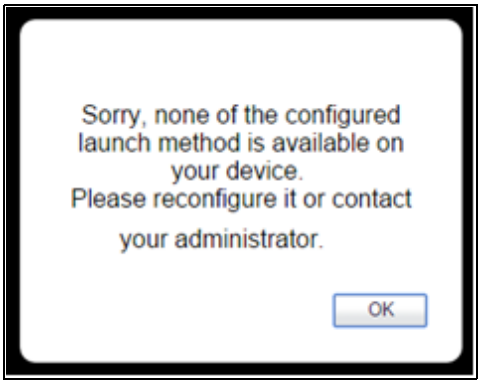


If the **Remember my choice** option is selected during the launch time, the selected mode is remembered through a cookie.

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

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

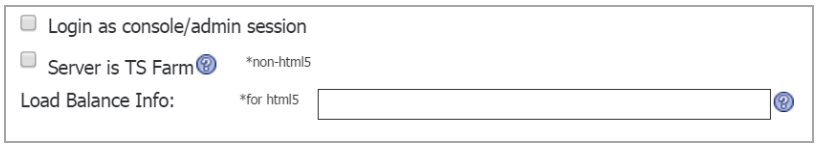
When no modes are able to run on the client with the configuration, the following notice appears.



- Optionally enter the local path for this application in the **Application and Path** field.
- Select **Enable wake-on-LAN** to enable waking up a computer over the network connection. Selecting this check box 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 **Send WOL packet to host name or IP address** that can be applied in tandem with a MAC address of another machine to wake.

- In the **Start in the following folder** field, optionally enter the local folder in which to execute application commands.
- Optionally enter the local path for this application in the **Application and Path** field and specify the folder in the **Start in the following folder** field. The remote application feature displays a single application to the user. The value can also be the alias of the remote application.
- Enter the **Command-line Arguments** for the RemoteApp. *(Option available for ActiveX or Java only.)*
- In the **Start in the following folder** field, optionally enter the local folder in which to execute application commands. *(Option available for ActiveX or Java only.)*
- Select **Login as console/admin session** to allow login as console or admin. Login as admin replaces login as console in RDC 6.1 and newer. *(Option available for all Terminal Services.)*
- Select **Server is TS Farm** if users are connecting to a TS Farm or Load Balanced server. Enter the Terminal Services Broker information in the **Load Balance Info** box, such tsv://MS Terminal Services Plugin. 1. CollectionName. Maximum length is 1024 characters. For the bookmark with complex options (like RDP), options are mixed from all the modes and distinguished with tips like *non-html5, or *for html5.



By default, the bookmark only connects to the provided name and IP address. If you enable this feature, the SMA/SRA appliance obtains the redirected address and connects the user to the correct server. Note that Interactive Login might need to be disabled for this feature to work properly.

NOTE: If this setting is enabled, set the correct SSO credentials to log in to the bookmark automatically. If this setting is not enabled, leave **Automatically log in** deselected.

- For *RDP - HTML5*, select the **Default Language** from the drop-down menu.
- For Windows clients or on Mac clients running Mac OS X 10.5 or higher with RDC installed, expand **Show advanced Windows options** and select the check boxes for to redirect the following features on the local network for use in this bookmark:
  - **Redirect Printers** - See Printer redirection **on page 468** for more information on setting up Printer Redirection
  - **Redirect Ports**
  - **Redirect Clipboard**
  - **Redirect Drives**
  - **Redirect SmartCards**
  - **Redirect Plug and Play Devices**

  Select the check boxes for any of the following additional features for use in this bookmark session:
  - **Display connection bar**
  - **Desktop background**

- **Menu/window animation**
- **Show window contents while dragging/resizing**
- **Auto-reconnection**
- **Bitmap caching**
- **Visual styles**
- Select the **Remote Audio** option from the drop-down list. Audio redirection enables the user to play an audio clip on the server, either remotely or locally. Valid selections are **Play on this computer**, **Play on remote computer**, or **Do not play**. Note that this feature is currently supported by Chrome, Firefox, and Safari.

NOTE: Hover your mouse pointer over the Help icon  next to certain options to display tooltips that indicate requirements.

- For *RDP - HTML5*, the following Advanced Windows options are available:
  - **Desktop background**
  - **Menu/window animation**
  - **Show window contents while dragging/resizing**
  - **Enable Compression**
  - **Visual Styles**
  - Select the **Remote Audio** option from the drop-down list. Audio redirection enables the user to play an audio clip on the server, either remotely or locally. Valid selections are **Play on this computer**, **Play on remote computer**, or **Do not play**. Note that this feature is currently supported by Chrome, Firefox, and Safari.
- If the client application is RDP6, you can select any of the following options: (*Option available for all Terminal Services)*
  - **Font smoothing**
- Select the **Connection Speed** from the drop-down list for optimized performance. (*Option available for all Terminal Services.*)
- Select the action from the drop-down list that happens in the event that the **Server Authentication fails**. Server authentication verifies that you are connecting to the intended remote computer. The strength of the verification required to connect is determined by your system security policy. (*Option available for all Terminal Services.*)
- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in to the RDP server. Enable the **Use Login Domain for SSO** option to pass the user's domain to the RDP server. Windows 2008 and newer servers could require this option to be enabled. *(Option available for all Terminal Services.)*

  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 on page 396.
- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices. *(Option available for all Terminal Services.)*

NOTE: RDP over HTML5 is supported using the default/standard browser in iOS or Android.

Virtual Network Computing (VNC)

- In the **Encoding** drop-down list, select one of the following:

- **Raw** – Pixel data is sent in left-to-right scanline order, and only rectangles with changes are sent after the original full screen has been transmitted.
- **RRE** – Rise-and-Run-length-Encoding uses a sequence of identical pixels that are compressed to a single value and repeat count. This is an efficient encoding for large blocks of constant color.
- **CoRRE** – A variation of RRE, using a maximum of 255x255 pixel rectangles, allowing for single-byte values to be used. More efficient than RRE except where very large regions are the same color.
- **Hextile** – Rectangles are split up in to 16x16 tiles of raw or RRE data and sent in a predetermined order. Best used in high-speed network environments such as within the LAN.
- **Zlib** – Simple encoding using the zlib library to compress raw pixel data, costing a lot of CPU time. Supported for compatibility with VNC servers that might not understand Tight encoding which is more efficient than Zlib in nearly all real-life situations.
- **Tight** – The default and the best encoding to use with VNC over the Internet or other low-bandwidth network environments. Uses zlib library to compress pre-processed pixel data to maximize compression ratios and minimize CPU usage.

- In the **Compression Level** drop-down list, select the level of compression as **Default** or from **1** to **9** where **1** is the lowest compression and **9** is highly compressed.
- The **JPEG Image Quality** option is not editable and is set at **6**.
- In the **Cursor Shape Updates** drop-down list, select **Enable**, **Ignore**, or **Disable**. The default is **Ignore**.
- Select **Use CopyRect** to gain efficiency when moving items on the screen.
- Select **Restricted Colors (256 Colors)** for more efficiency with slightly less depth of color.
- Select **Reverse Mouse Buttons 2 and 3**, to switch the right-click and left-click buttons.
- Select **View Only** if the user is not making any changes on the remote system.
- Select **Share Desktop** to allow multiple users to view and use the same VNC desktop.
- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.

Citrix Portal (Citrix)

- In the **Resource Window Size** drop-down list, select the default Citrix portal screen size to be used when users execute this bookmark.

9 Select an **Access Type Selection**. **Smart** or **Manual**.

- **Smart**: Allows the firmware to decide which mode to launch on the client.

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

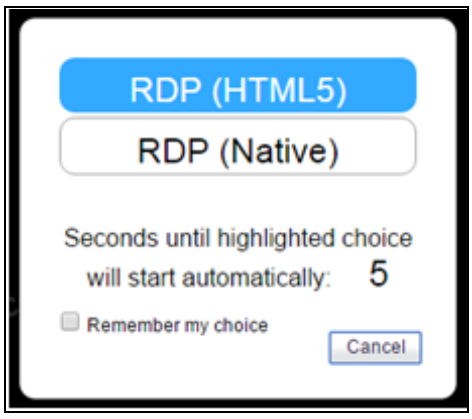
- **Manual**: Provides options to configure the modes, their priorities, and the choose method. At least one mode should be enabled in the selection box.

The launch sequence is as follows: **HTML5**, **Native**, and **ActiveX**. Selecting Manual allows you to change, enable, or disable the launch methods. If you select **Native** to launch the Citrix bookmark, then the SMA Connect Agent launches the Citrix Receiver on the local machine to do the Citrix connection. **Native** can provide advanced features when launched on Windows and OS X platforms after installing the SMA Connect Agent and Citrix Receiver.

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

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

After the **Choose during Launch** option is enabled, while launching the unified bookmark, if there are multiple modes available for the client, a menu is provided from which you can choose within a five second count-down. When only one mode is available, the bookmark is also run immediately.

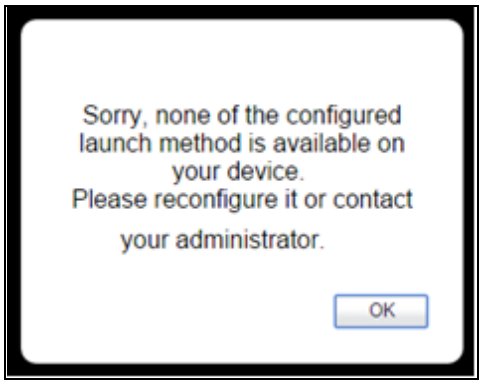


If the **Remember my choice** option is selected during the launch time, the selected mode is remembered through a cookie.

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

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

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



- Optionally select **HTTPS Mode** to use HTTPS to securely access the Citrix Portal.
- Optionally, select **Always use specified Citrix ICA Server** and specify the IP address in the **ICA Server Address** field that appears. This setting allows you to specify the Citrix ICA Server address for the Citrix ICA session. By default, the bookmark uses the information provided in the ICA configuration on the Citrix server.
- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.

Web (HTTP)

- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in to the RDP server. Enable the **Use Login Domain for SSO** option to pass the user's domain 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 on page 396.
- Select **Forms-based Authentication** 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>.
- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.

Secure Web (HTTPS)

- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in to the RDP server. Enable the **Use Login Domain for SSO** option to pass the user's domain 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 on page 396.
- Select **Forms-based Authentication** 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>.

- Select the **Display Bookmark to Mobile Connect** clients to display the bookmark on mobile devices.

External Web Site

- Select **HTTPS Mode** to use SSL to encrypt communications with this Web site.
- Select **Disable Security Warning** if you do not want to see any security warnings when accessing this Web site. Security warnings are normally displayed when this bookmark refers to anything other than an Application Offloaded Web site.
- Select **Automatically log in** to enable the virtual host domain SSO for this bookmark. If the host in the bookmark refers to a portal with the same shared domain as this portal, selecting this check box allows you to automatically be logged in with this portal's credential.
- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.

Mobile Connect

- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.

  NOTE: Mobile Connect must be running version 2.0 or newer to view and access this Bookmark. Support varies by device and might require supported third-party applications to be installed.

File Shares (CIFS)

NOTE: SMB2 and SMB3 protocols are currently not supported. Servers should be configured to allow communication from a Linux based client.

- To restrict access on the client UI, select **Set user to access the specific files/folders**. To completely restrict access, navigate to the **Services** > **Policies** page to set a policy for access constraints. For more information, see Adding User Policies on page 367.
- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in to the RDP server. Enable the **Use Login Domain for SSO** option to pass the user's domain 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 on page 396.
- Enable **Display Bookmark to Mobile Connect clients** to send bookmark information to Mobile Connect clients.

  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 disables access to the DFS file shares from other domains. The SMA/SRA appliance is not a domain member and is not 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) and SSH File Transfer Protocol (SFTP)

- 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 Secure Mobile Access session for log in 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 on page 396.

Telnet HTML5 Settings

- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in 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 on page 396.
- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.

Secure Shell Version 2 (SSHv2) HTML5 Settings

- Select the **Default Font Size**. Supported options range from 12 to 99 points.
- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current Secure Mobile Access session for log in 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 on page 396.

SSHv2 Common Settings

- Optionally select **Automatically accept host key**. This option allows the browser to keep the server's public host key in local storage automatically.
- Select **Display Bookmark to Mobile Connect clients** to display the bookmark on mobile devices.
- Click **Accept** to update the configuration. After the configuration has been updated, the new group bookmark displays in the **Edit Local Group** page.

Configuring Group End Point Control

To configure the End Point Control profiles used by local groups:

1. Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** page.
2. Click the configure icon next to the group to be configured for EPC. The **Edit Local Group** window is displayed.
3. Click the **EPC** page. The **EPC** window is displayed.
4. Configure EPC group settings and add or remove device profiles, as explained in Users > Local Groups on page 400.

Group Configuration for LDAP Authentication Domains

NOTE: The Microsoft Active Directory database uses an LDAP organization schema. The Active Directory database might be queried using Kerberos authentication (the standard authentication type; this is labeled "Active Directory" domain authentication in the Secure Mobile Access management interface), or using LDAP database queries. An LDAP domain configured in the Secure Mobile Access management interface can authenticate to an Active Directory server.

Lightweight Directory Access Protocol (LDAP) is a standard for querying and updating a directory. Because LDAP supports a multilevel hierarchy (for example, groups or organizational units), the SMA/SRA appliance can query this information and provide specific group policies or bookmarks based on LDAP attributes. By configuring LDAP attributes, the SMA/SRA 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 SMA/SRA appliance.

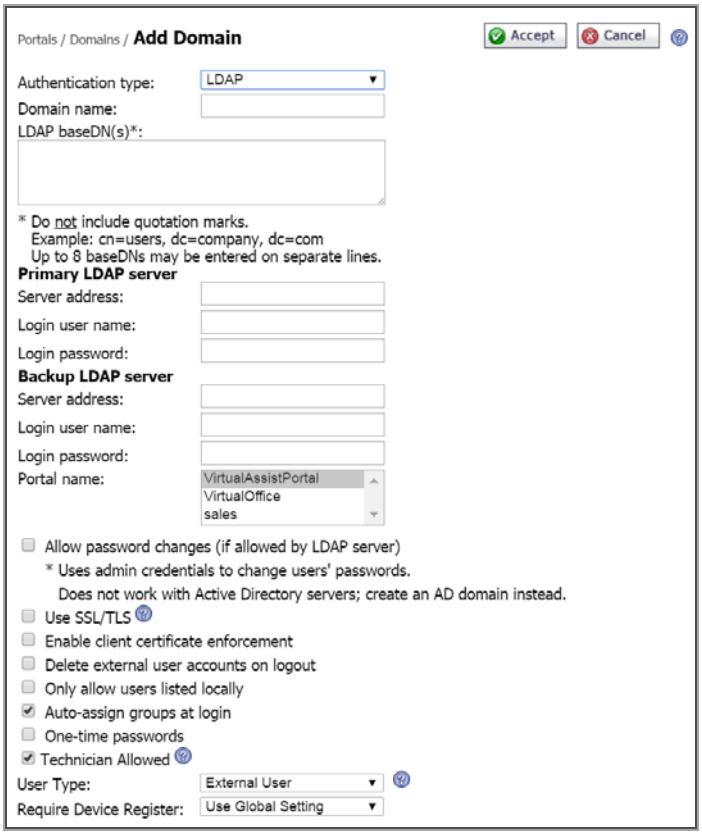
After an LDAP authentication domain is created, a default LDAP group is created with the same name as the LDAP domain name. Although additional groups can be added or deleted from this domain, the default LDAP group cannot be deleted. If the user for which you created LDAP attributes enters the Virtual Office home page, the bookmark you created for the group the user is in displays in the Bookmarks Table.

For an LDAP group, you can 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 has a bookmark assigned when entering the Virtual Office environment, complete the following steps:

1 Navigate to the **Portals > Domains** page and click **Add Domain** to display the **Add New Domain** window.

2 Select **LDAP** from the **Authentication Type** menu. The LDAP domain configuration fields are displayed.



3 Enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users select in order to log in to the Secure Mobile Access user portal. It can be the same value as the **Server address** field.

4 Enter the IP address or domain name of the server in the **Server address** field.

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 is automatically included when parents are added to this field.

NOTE: Do not include quotes (“”) in the **LDAP BaseDN** field.

6 Enter a **Server address** that has been delegated control of the container that server is in.

7 Enter the user name 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 SMA/SRA appliance binds to the LDAP tree with these credentials and users can log in with their SMA AccountName.

8 Enter a **Backup Server address**.

9 Enter the backup user name along with the corresponding backup password in the **Login user name** and **Login password** fields

10 Select the name of the portal in the **Portal name** field. Additional layouts can be defined in the **Portals > Portals** page.

11 Select **Allow password changes (if allowed by LDAP server)** if you want to be able to change user's passwords. The admin account must be used when changing user passwords.

12 Optionally select **Use SSL/TLS**. This option allows for the needed SSL/TLS encryption to be used for Active Directory password exchanges. This check box should be enabled when setting up a domain using Active Directory authentication.

13 Optionally select **Enable client certificate enforcement** 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 appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this check box 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 matches the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

14 Select **Delete external user accounts on logout** to delete users who are not logged into a domain account after they log out.

15 Select **Only allow users listed locally** to allow only users with a local record in the Active Directory to login.

16 Select **Auto-assign groups at login** to assign users to a group when they log in.

Users logging into Active Directory domains are automatically assigned in real time to Secure Mobile Access groups based on their external AD group memberships. If a user's external group membership has changed, their Secure Mobile Access group membership automatically changes to match the external group membership.

17 Optionally, select **One-time passwords** to enable the One Time Password feature. A drop-down list appears, 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 uses 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 are not allowed to login.
- **using domain name** - Users in the domain uses the One Time Password feature. One Time Password emails for all users in the domain are sent to username@domain.com.

18 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 appears, 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 is used. If you select **custom**, the **Custom attribute** field appears. 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 is taken from their individual policy settings.

If you select **using domain name**, an **E-mail domain** field appears following the drop-down list. Type in the domain name where one-time password emails are sent (for example, abc.com).

19 If **Technician Allowed** is enabled, Secure Virtual Assist can log in as a technician role in this domain.

20 Select the type of user from the **User Type** drop-down list. All users logging in through this domain are treated as this user type. The choices depend on user types defined already. Some possible choices are:

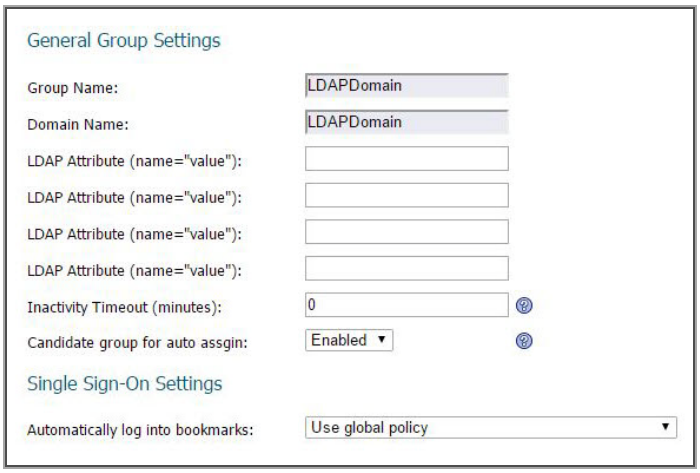
- **External User** – Users logging into this domain are treated as normal users without administrative privileges.
- **External Administrator** – Users logging into this domain are treated as administrators, with local Secure Mobile Access admin credentials. These users are presented with the admin login page.

  This option allows the Secure Mobile Access administrator to configure a domain that allows Secure Mobile Access admin privileges to all users logging into that domain.

  SonicWall Inc. recommends adding filters that allow administrative access only to those users who are in the correct group. You can do so by editing the domain on the **Users > Local Groups** page.
- **Read-only Administrator** – Users logging into this domain are treated as read-only administrators and can view all information and settings, but cannot apply any changes to the configuration. These users are presented with the admin login page.

21 Click **Accept** to update the configuration. After the domain has been added, the domain is added to the table on the **Portals > Domains** page.

22 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** page.



23 On the **General** page, you can 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 Inc. 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"
```

24 Type an inactivity timeout value (in minutes) in the **Inactivity Timeout** field. Enter **0** (zero) to use the global inactivity timeout setting.

25 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 log in to bookmarks.
- **User-controlled (enabled by default for new users)** – Enable SSO to log in to bookmarks for new users, and allow users to change this setting.
- **User-controlled (disabled by default for new users)** – Disable SSO to log in to bookmarks for new users, and allow users to change this setting.
- **Enabled** – Enable SSO to log in to bookmarks
- **Disabled** – Disable SSO to log in to bookmarks

26 Click **Accept** when done.

LDAP Attribute Information

When configuring LDAP attributes, the following information could 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 SMAAccountName (login name). For example, if your Active Directory login name is **gkam** and your full name is **guitar kam,** when logging into the SMA/SRA appliance 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 login with the SMAAccountName.
- 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 is 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 is 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 SMA/SRA appliance, then the user is not able to log in to 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 in to the portal.

Example of LDAP Users and Attributes

If a user is manually added to a LDAP group, then the user setting takes 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 is a member of SMA/SRA appliance Group1.

But if the administrator manually adds the user Jane to SMA/SRA appliance Group2, then the LDAP attributes is ignored and Jane is a member of Group2.

Sample LDAP Attributes

You can 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 ldap search 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 are saved.

For instructions on querying an LDAP server from a Window server, refer to:

http://technet.microsoft.com/en-us/library/cc783845(v=ws.10).aspx

http://technet.microsoft.com/en-us/library/cc755809(v=ws.10).aspx

http://technet.microsoft.com/en-us/library/cc731033(v=ws.10).aspx

Group Configuration for Active Directory and RADIUS Domains

For authentication to RADIUS 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 SMA/SRA appliance validates with the appropriate Active Directory or RADIUS server that the user is authorized to login. If the user is authorized, the SMA/SRA appliance checks to see if a user exists in the SMA/SRA appliance database for users and groups. If the user is defined, then the policies and bookmarks defined for the user applies.

For example, if you create a RADIUS domain in the SMA/SRA 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 log in to the portal, policies, bookmarks and other user settings applies to the users. If the AAA user does not exist in the SMA/SRA appliance, then only the global settings, policies and bookmarks applies to the user.

This section contains the following subsections:

- Bookmark Support for External (Non-Local) Users on page 425
- Adding a RADIUS Group on page 426
- Adding an Active Directory Group on page 426

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 are propagated to applicable users, while individual users can create only personal bookmarks.

Because bookmarks are stored within the SMA/SRA appliance’s local configuration files, it is necessary for group and user bookmarks to be correlated to defined group and user entities. When working with local (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 or 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 Secure Mobile Access configuration files. The need to store bookmarks on the SMA/SRA appliance itself is because LDAP and RADIUS 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, the SMA/SRA appliance 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 SMA/SRA appliance, the moment jdoe adds a personal bookmark, a local user called jdoe is created on the SMA/SRA appliance as type External, and can then be managed like any other local user by the administrator. The external local user remains 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** page allows the administrator to enable user access to the SMA/SRA appliance based on existing RADIUS group memberships. By adding one or more RADIUS groups to a Secure Mobile Access group, only users associated with specified RADIUS group(s) are allowed to login.

To add a RADIUS group:

1. In the **Users > Local Groups** page, click **Configure** for the RADIUS group you want to configure.
2. In the **RADIUS Groups** page and click **Add Group...**. The Add RADIUS Group page displays.
3. Enter the **RADIUS Group** name in the corresponding field. The group name must match the RADIUS Filter-Id exactly.
4. Click **Accept**. The group displays in the RADIUS Groups section.

Adding an Active Directory Group

The **AD Groups** page allows the administrator to enable user access to the SMA/SRA appliance based on existing AD group memberships. By adding one or more AD groups to a Secure Mobile Access 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.

To add an AD group:

1. In the **Users > Local Groups** page, click **Configure** for the AD group you want to configure.
2. In the **AD Groups** page and click **Add Group...**. The Add Active Directory Group page displays.
3. Enter the **Active Directory Group** name in the corresponding field.
4. Optionally, select **Associate with AD group** if you wish to associate the Secure Mobile Access group with your AD group. This step can also be completed at a later time in the **Edit Group** page under the **AD Groups page**.
5. Click **Accept**. The group displays in the Active Directory Groups section. The process of adding a group can take several moments. Do not click **Add** more than one time during this process.

Creating a Citrix Bookmark for a Local Group

To configure a Citrix bookmark for a user:

1. Navigate to **Users > Local Groups**.
2. Click the configure icon next to the group you want to configure.
3. In the **Edit Group Settings** window, select the **Bookmarks** tab.

4 Click **Add Bookmark...**

5 Enter a name for the bookmark in the **Bookmark Name** field.

6 Enter the name or IP address of the bookmark in the **Name or IP Address** field.

7 From the **Service** drop-down list, select **Citrix Portal (Citrix)**.

8 Select the **Resource Window Size** from the drop-down list.

9 Select an **Access Type Selection**. **Smart** or **Manual**.

- **Smart**: Allows the firmware to decide which mode to launch on the client.

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

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

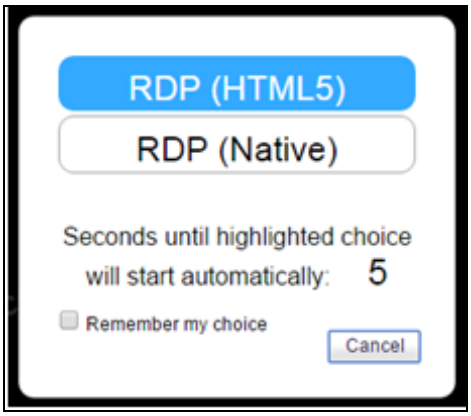
The launch sequence is as follows: **HTML5**, **Native**, and **ActiveX**. Selecting Manual allows you to change, enable, or disable the launch methods. If you select **Native** to launch the Citrix bookmark, then the SMA Connect Agent launches the Citrix Receiver on the local machine to do the Citrix connection.

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

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

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

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

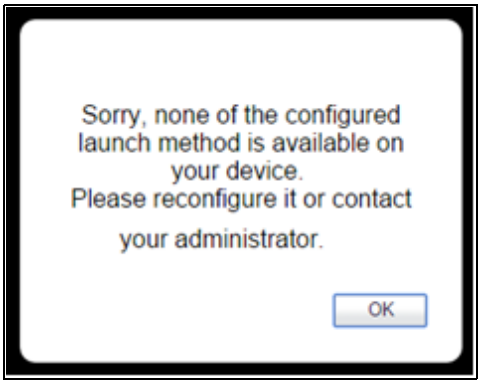


If the **Remember my choice** option is selected during the launch time, the selected mode is remembered through a cookie.

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

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

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



10 Optionally select **HTTPS Mode** to enable HTTPS mode.

11 Optionally, select **Always use specified Citrix ICA Server** and specify the IP address in the **ICA Server Address** field that appears. This setting allows you to specify the Citrix ICA Server address for the Citrix ICA session. By default, the bookmark uses the information provided in the ICA configuration on the Citrix server.

12 Click **Accept**.

Global Configuration

SMA/SRA 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 on page 429
- Edit Global Policies on page 431
- Edit Global Bookmarks on page 433

Edit Global Settings

To edit global settings:

1 Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** window.

2 Click the configure icon next to **Global Policies**. The **Edit Global Policies** window is displayed.

3 On the **General** tab, to set the inactivity timeout for all users or groups, meaning that users are 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 takes precedence over the group timeout and the group timeout takes 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.

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**.

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.

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.

7 Click **Accept** to save the configuration changes.

8 Navigate to the **NetExtender / Mobile Connect** tab.

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.

10 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.

11 In the **Exit Client After Disconnect** drop-down list, select **Enabled** or **Disabled**.

12 In the **Uninstall Client After Exit** drop-down list, select **Enabled** or **Disabled**.

13 In the **Create Client Connection Profile** drop-down list, select **Enabled** or **Disabled**.

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 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 are 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 are required to enter both user name and password when starting NetExtender.

15 Navigate to the **Routes** tab.

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 Secure Mobile Access NetExtender tunnel. **Tunnel All Mode** is disabled by default.

17 To add a client route, click **Add Client Route...**

18 In the **Add Client Route** window, 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.

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.

20 Click **Accept** to save the configuration changes.

21 Navigate to the **Policies** tab.

22 To add a policy, click **Add Policy...**

23 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**.

24 Enter a name for the policy in the **Policy Name** field.

25 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 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.

26 Select the desired **Protocol**. The available value options in the Protocol field include: **TCP**, **UDP**, **ICMP**, and **ALL**. You can select multiple items among **TCP**, **UDP**, and **ICMP**. However, when **ALL** is selected, all others options are deselected.

> **NOTE:** The protocol setting only appears when the Service is set to "NetExtender & Mobile Connect" or "All Services."

27 Click **Accept** to save the configuration changes.

28 Click the **Bookmarks** tab.

29 To add a bookmark, click **Add Bookmark...**

30 Enter a bookmark name in the **Bookmark Name** field.

31 Enter the bookmark name or IP address in the **Name or IP Address** field.

32 Select one of the following services from the **Service** drop-down list: **Terminal Services (RDP)**, **Virtual Network Computing (VNC)**, **Citrix Portal (Citrix)**, **Web (HTTP)**, **Secure Web (HTTPS)**, **File Shares (CIFS)**, **File Transfer Protocol (FTP)**, **SSH File Transfer Protocol (SFTP)**, **Telnet**, or **Secure Shell Version 2 (SSHv2)**.

> **NOTE:** IPv6 is not supported on File Shares bookmarks.

33 In the fields that appear based on your **Service** settings, fill in the appropriate information. For example, if you select **Terminal Services (RDP)**, you need to select the desired screen size from the **Screen Size** drop-down list.

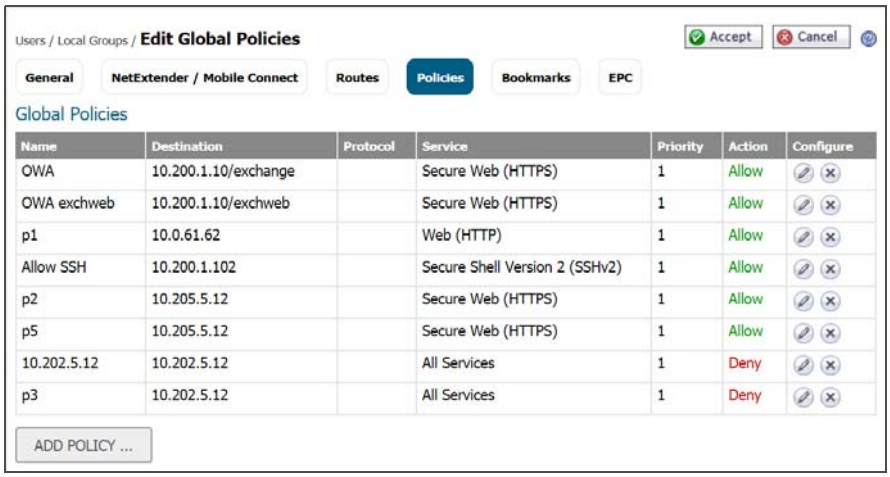
34 Click **Accept** to save the configuration changes.

Edit Global Policies

To define global access policies:

1 Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** window.

2 Click the configure icon next to **Global Policies**. The **Edit Global Settings** window is displayed.



3 On the **Policies** tab, click **Add Policy**. The **Add Policy** window is displayed.

NOTE: User and group access policies takes precedence over global policies.

4 In the **Apply Policy To** drop-down list, select one of the following: **IP Address**, **IP Network**, **All Addresses**, **Network Object**, **Server Path**, **URL Object**, **All IPv6 Address**, **IPv6 Address**, or **IPv6 Network**.

5 Type a name for the policy in the **Policy Name** field.

NOTE: SMA/SRA appliance policies apply to the destination address(es) of the SMA/SRA connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the SMA/SRA 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 Network** 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 Network** 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.

6 Select the desired **Protocol**. The available value options in the Protocol field include: **TCP**, **UDP**, **ICMP**, and **ALL**. You can select multiple items among **TCP**, **UDP**, and **ICMP**. However, when **ALL** is selected, all others options are deselected.

NOTE: The protocol setting only appears when the Service is set to “NetExtender & Mobile Connect” or “All Services.”

7 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.

8 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.

9 Select **ALLOW** or **DENY** from the **Status** drop-down list to either permit or deny SMA/SRA connections for the specified service and host machine.

10 Click **Accept** to update the configuration. After the configuration has been updated, the new policy is displayed in the **Edit Global Settings** window. The global policies are 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:

1 Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** window.

2 Click the configure icon next to **Global Policies**. The **Edit Global Settings** window is displayed.

3 Select the **Policies** tab.

4 Click **Add Policy**.

5 Select **Server Path** from the **Apply Policy To** drop-down list.

6 Type a name for the policy in the **Policy Name** field.

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)

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.

9 Select **PERMIT** or **DENY** from the **Status** drop-down list.

10 Click **Accept**.

Edit Global Bookmarks

To edit global bookmarks:

1 Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** page.

2 Click the configure icon next to **Global Policies**. The **Edit Global Policies** window is displayed.

3 Click **Add Bookmark**. An **Add Bookmark** window is displayed.

NOTE: When global bookmarks are defined, all users see the defined bookmarks from the Secure Mobile Access user portal. Individual users are not able to delete or modify global bookmarks.

4 To edit a bookmark, enter a descriptive name in the **Bookmark Name** field.

5 Enter the domain name or the IP address of a host machine on the LAN in the **Name or IP Address** field.

6 Select the service type in the **Service** drop-down list.

7 Click **Accept** to update the configuration. After the configuration has been updated, the new global bookmark is displayed in the bookmarks list in the **Edit Global Settings** window.

Edit EPC Settings

To configure global End Point Control profiles for local groups or users:

1 Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** page.

2 Click the configure icon next to **Global Policies**. The **Edit Global Policies** window is displayed.

3 Click the EPC tab. The **EPC** window is displayed.

4 Configure EPC global settings and add or remove device profiles, as explained in Users > Local Groups on page 400 and Users > Local Groups on page 400.

16

Log Configuration

This section provides information and configuration tasks specific to the **Log** pages on the Secure Mobile Access web-based management interface.

Topics:

Log > View

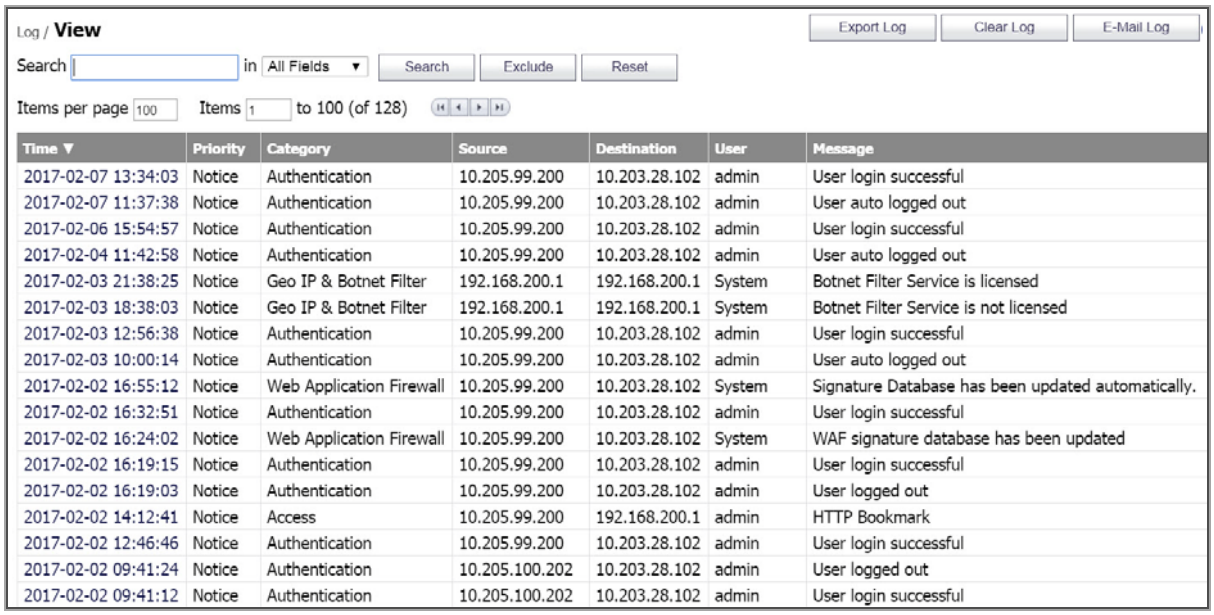
The SMA/SRA appliance supports web-based logging, syslog logging and email alert messages. In addition, The SMA/SRA appliance can be configured to email the event log file to the Secure Mobile Access administrator before the log file is cleared.

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 Secure Mobile Access event log. The event log can also be automatically sent to an email address for convenience and archiving.

Log > View



Time ▼	Priority	Category	Source	Destination	User	Message
2017-02-07 13:34:03	Notice	Authentication	10.205.99.200	10.203.28.102	admin	User login successful
2017-02-07 11:37:38	Notice	Authentication	10.205.99.200	10.203.28.102	admin	User auto logged out
2017-02-06 15:54:57	Notice	Authentication	10.205.99.200	10.203.28.102	admin	User login successful
2017-02-04 11:42:58	Notice	Authentication	10.205.99.200	10.203.28.102	admin	User auto logged out
2017-02-03 21:38:25	Notice	Geo IP & Botnet Filter	192.168.200.1	192.168.200.1	System	Botnet Filter Service is licensed
2017-02-03 18:38:03	Notice	Geo IP & Botnet Filter	192.168.200.1	192.168.200.1	System	Botnet Filter Service is not licensed
2017-02-03 12:56:38	Notice	Authentication	10.205.99.200	10.203.28.102	admin	User login successful
2017-02-03 10:00:14	Notice	Authentication	10.205.99.200	10.203.28.102	admin	User auto logged out
2017-02-02 16:55:12	Notice	Web Application Firewall	10.205.99.200	10.203.28.102	System	Signature Database has been updated automatically.
2017-02-02 16:32:51	Notice	Authentication	10.205.99.200	10.203.28.102	admin	User login successful
2017-02-02 16:24:02	Notice	Web Application Firewall	10.205.99.200	10.203.28.102	System	WAF signature database has been updated
2017-02-02 16:19:15	Notice	Authentication	10.205.99.200	10.203.28.102	admin	User login successful
2017-02-02 16:19:03	Notice	Authentication	10.205.99.200	10.203.28.102	admin	User logged out
2017-02-02 14:12:41	Notice	Access	10.205.99.200	192.168.200.1	admin	HTTP Bookmark
2017-02-02 12:46:46	Notice	Authentication	10.205.99.200	10.203.28.102	admin	User login successful
2017-02-02 09:41:24	Notice	Authentication	10.205.100.202	10.203.28.102	admin	User logged out
2017-02-02 09:41:12	Notice	Authentication	10.205.100.202	10.203.28.102	admin	User login successful

The **Log > View** page displays log messages in a sortable, searchable table. The SMA/SRA appliance can store up to 1GB of log data in the log file system with a limit of 50MB for each log file. Each log entry contains the date and time of the event and a brief message describing the event. After the log file reaches the log size limit, the log entry is cleared and optionally emailed to the Secure Mobile Access 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:

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 SMA/SRA 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 cannot 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 Secure Mobile Access 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.
Location	The geographical location of the source IP for each event log message.
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:

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.

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 SMA event log. The SMA/SRA 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 SMA/SRA appliance can store up to 1GB of log data in the log file system. Logs are displayed in a sortable, searchable table. The appliance can alert you of events, such as a successful login or an exported configuration. Alerts can be immediately emailed upon generation or the admin can choose the format of the logs included in the email- in-line text appearing within the email body or as a zipped attachment (default). Each log entry contains the date and time of the event and a brief message describing the event. After the log file reaches the 50 MB log size limit, the log entry is cleared and optionally emailed to the Secure Mobile Access administrator.

Each log entry displays the following information:

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 SMA/SRA 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 cannot 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 Secure Mobile Access 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 Secure Mobile Access event log. This feature is useful archiving email and in testing email configuration and email filters for multiple SMA/SRA appliances.

To use the E-mail Log feature:

1 Navigate to **Log > View**.

2 Click **E-mail Log**.

3 The message **Log has been successfully sent** appears.

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 439.

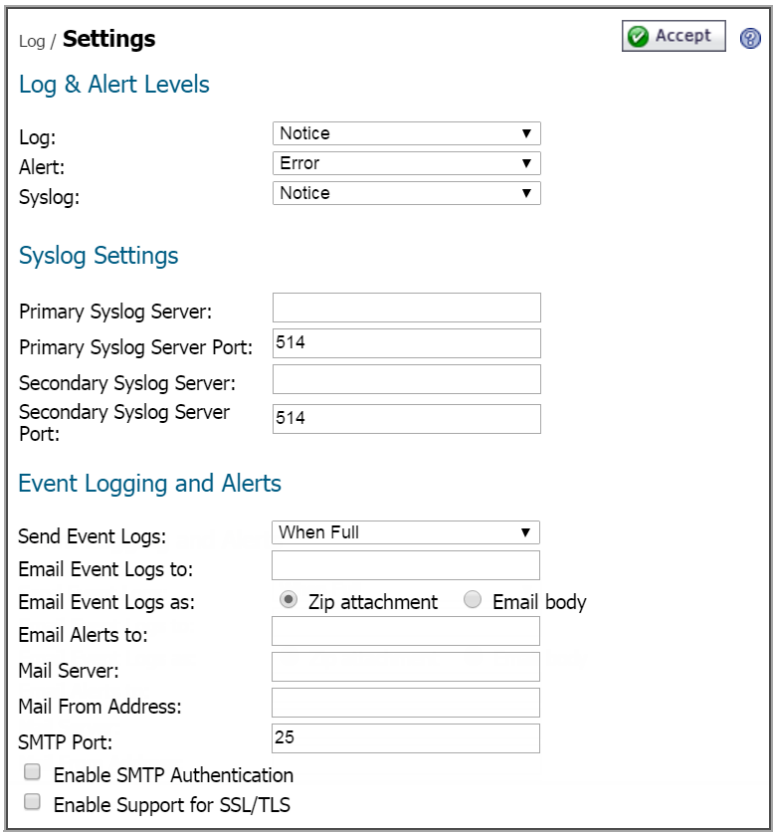
Log > Settings

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.

Log > Settings Page



Log & Alert Levels

The Log & Alert Levels 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.

Syslog Settings

The Syslog Settings section allows the administrator to specify the primary and secondary Syslog servers.

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.

Configuring Log Settings

To configure log and alert settings, complete the following steps:

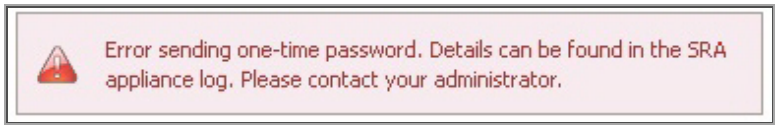
1. To begin configuring event log, syslog and alert settings, navigate to the **Log > Settings** page.
2. In the **Log & Alert Levels** section, define the severity level of log messages that are identified as log (event log), alert, or syslog messages. Log levels are organized from most to least critical. If a level is selected for a specific logging service, then that log level and more critical events are logged. For example, if the Error level is selected for the Log service, then all Emergency, Alert, Critical, and Error events are stored in the internal log file.
3. 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.
4. If you have a backup or second syslog server, enter the server's IP address or domain name in the **Secondary Syslog Server** field.
5. Designate when log files are cleared and emailed to an administrator in the **Send Event Logs** field. If the option **When Full** is selected, the event log is emailed when it reaches the maximum file size of 50MB. The log file is then cleared. 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 is still sent if the log file is full before the end of the period. In the **Log > View** page, you can click **Clear Log** to delete the current event log. The event log is not emailed in this case.
6. To receive event log files through 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 is emailed to the specified email address before the event log is cleared. If this field is left blank, log files are not emailed.
7. To receive alert messages through email, enter your full email address (username@domain.com) or an email pager address in the **Email Alerts to** field. An email is sent to the email address specified if an alert event occurs. If this field is left blank, alert messages are not emailed.

   ⓘ **NOTE:** Define the type of events that will generate alert messages on the **Log > Categories** page.

8. 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 are not emailed.
9. Specify a **Mail From Address** in the corresponding field. This address appears in the from field of all log and alerts emails.
10. To use SMTP authentication when sending log files, select **Enable SMTP Authentication**. The display changes to expose related fields. Enter the user name, password, and the SMTP port to use. The default port is 25.
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 on page 49.

To configure the mail server:

1 Log in to the Secure Mobile Access management interface using administrator credentials.

2 Navigate to **Log > Settings**.

3 Type the email address where you want logs sent to in the **Email Events Logs to** field.

4 Type the email address where you want alerts sent to in the **Email Alerts to** field.

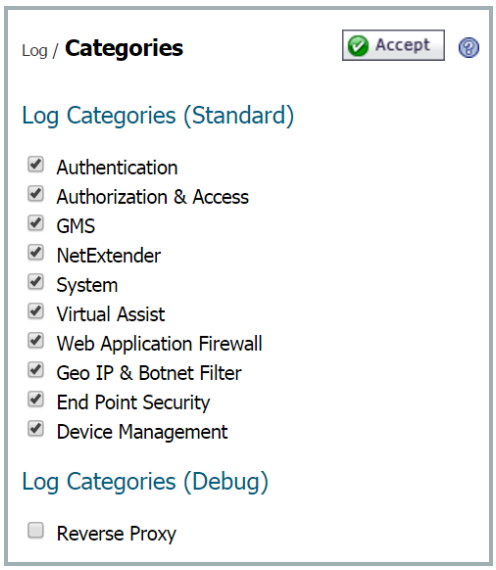
5 Type the IP address for the mail server you are using in the **Mail Server** field.

6 Type the email address for outgoing mail from your SMA/SRA appliance in the **Mail From Address** field.

7 Click **Accept** in the upper right 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 check boxes for each of the following log categories:

- Authentication
- Authorization & Access
- GMS
- NetExtender
- System
- Virtual Assist
- Web Application Firewall
- High Availability (SMA 400/200, SRA 4600)

- Geo IP & Botnet Filter
- End Point Security
- Device Management
- Reverse Proxy

After 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 on page 441
- Adding a ViewPoint Server on page 441

Log > ViewPoint Overview

The **Log > ViewPoint** page allows the administrator to add the SMA/SRA appliance to a ViewPoint server for installations that have SonicWall Inc. ViewPoint available, or are managed by the SonicWall Inc. Global Management System (GMS) appliance management software. This feature requires a ViewPoint license key.

ViewPoint is an integrated appliance management solution that:

- Creates dynamic, web-based reports of SMA/SRA appliance and remote access activity
- Generates both real-time and historical reports to provide a complete view of activity through your SMA/SRA Appliance
- Enables remote access monitoring
- Enhances network security
- Helps you to anticipate future bandwidth needs

TIP: For more information about monitoring your SonicWall Inc. appliances with ViewPoint, visit http://www.sonicwall.com/us/support/3887.html

Adding a ViewPoint Server

This feature requires a ViewPoint license key.

To add the SMA/SRA appliance to a ViewPoint server and enable ViewPoint reporting on your SMA/SRA appliance:

1. Navigate to the **Log > ViewPoint** page in the Secure Mobile Access web-based 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.

2. In the ViewPoint Settings section, click **Add**. The Add ViewPoint Server screen displays.
3. In the Add ViewPoint Server screen, enter the **Hostname or IP Address** of your ViewPoint server.
4. Enter the **Port** which your ViewPoint server communicates with managed devices.

5 Click **Accept** at the top of the page to add this server.

6 To start ViewPoint report logging for the server you just added, select **Enable ViewPoint**.

Log > Analyzer

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

- Log > Analyzer Overview on page 442
- Adding an Analyzer Server on page 442

Log > Analyzer Overview

The **Log > Analyzer** page allows the administrator to add the SMA/SRA appliance to an Analyzer server for installations that have SonicWall Inc. Analyzer available, or are managed by the SonicWall Inc. Global Management System (GMS) version 7.0 or higher appliance management software. This feature requires an Analyzer license key.

SonicWall Inc. Analyzer is a software application that creates dynamic, web-based network reports. The Analyzer Reporting Module generates both real-time and historical reports to offer a complete view of all activity through SonicWall Inc. network security appliances. With Analyzer Reporting, you can monitor network access, enhance security, and anticipate future bandwidth needs. The Analyzer Reporting Module:

- Displays bandwidth use by IP address and service
- Identifies inappropriate Web use
- Provides detailed reports of attacks
- Collects and aggregates system and network errors
- Shows VPN events and problems
- Presents visitor traffic to your Web site
- Provides detailed daily logs to analyze specific events.

TIP: For more information about monitoring your SonicWall Inc. appliances with Analyzer, visit http://www.sonicwall.com/us/support/6631.html

Adding an Analyzer Server

This feature requires an Analyzer license key.

To add the SMA/SRA appliance to an Analyzer server and enable Analyzer reporting on your SMA/SRA appliance:

1 Navigate to the **Log > Analyzer** page in the Secure Mobile Access web-based management interface.

NOTE: If you are using Analyzer for the first time on this appliance or if you do not have a valid license, the page provides a link to the **System > Licenses** page to activate your license.

2 In the Analyzer Settings section, click the **Add**. The Add Analyzer Server screen displays.

3 In the Add Analyzer Server screen, enter the **Hostname or IP Address** of your Analyzer server.

4 Enter the **Port** which your Analyzer server communicates with managed devices. The default is 514.

5 Click **Accept** at the top of the page to add this server.

6 To start Analyzer report logging for the server you just added, select **Enable Analyzer**.

Part 5

Using Virtual Office

- Virtual Office Configuration

17

Virtual Office Configuration

This section provides information and configuration tasks specific to the **Virtual Office** page on the Secure Mobile Access web-based management interface.

Topics:

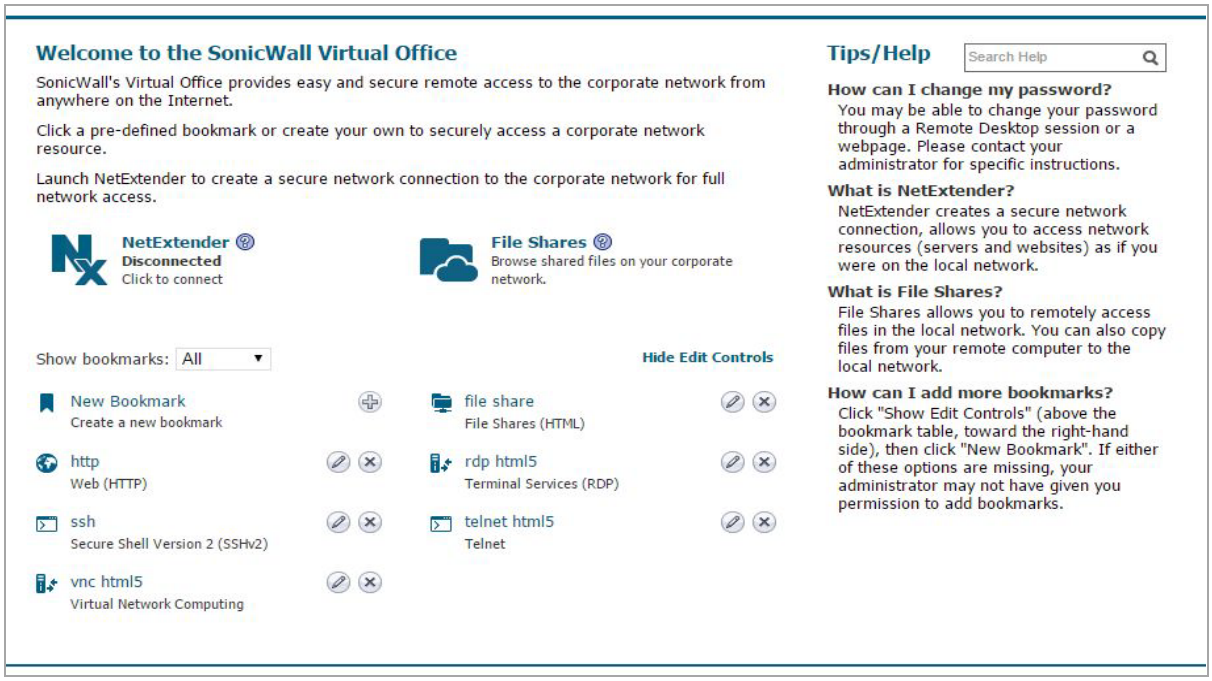
Virtual Office

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 Secure Mobile Access 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 to create and access bookmarks, file shares, NetExtender sessions, Secure Virtual Assist, and Secure Virtual Meeting.



Using the Virtual Office

To use the Virtual Office:

1 From the Secure Mobile Access web-based management interface, click **Virtual Office** in the navigation bar.

2 A new browser window opens to the Virtual Office home page.

> **NOTE:** When you launch the Virtual Office from the Secure Mobile Access web-based management interface, you are automatically logged in with your administrator credentials.

The **Logout** button does not appear in the Virtual Office when you are logged on as an administrator. To log out, you must close the browser window.

3 From the Virtual Office home page, you can:

- Launch and install Secure Mobile Access Connect Agents
- 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 Secure 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 *Secure Mobile Access User Guide*.

SMA Connect Agent

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

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

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

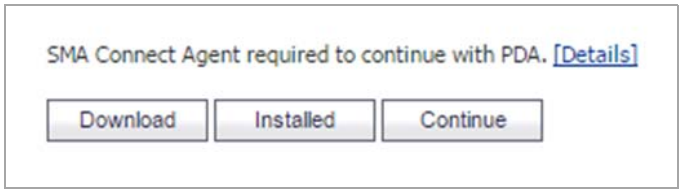
Topics:

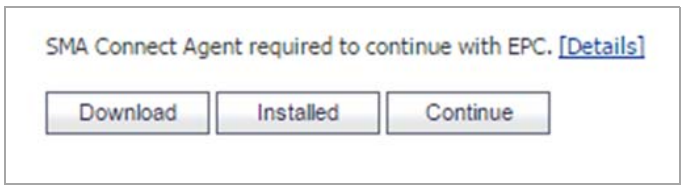
Supported Operating Systems

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

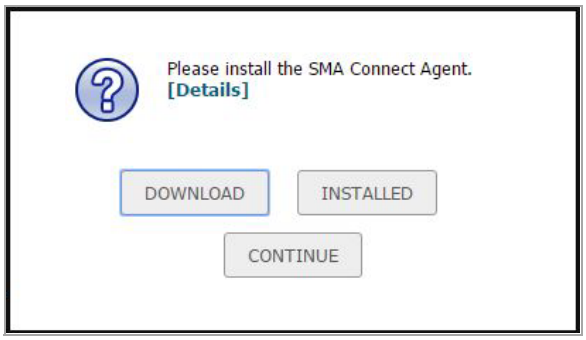
Downloading and Installation

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





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



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

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

Setting up the SMA Connect Agent

Proxy Configuration

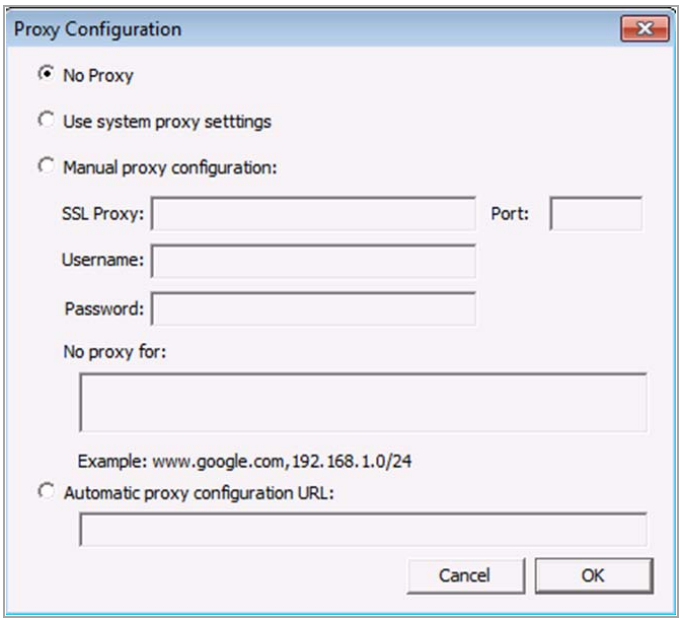
SMA supports proxy deployment, where all client browsers are configured to redirect to a proxy server, but an appliance sits between the client browsers and the proxy server. All SMA features are supported in this scenario, including supporting domain exclusions when the domain is part of a virtual hosting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

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

There are four options to setup the proxy configuration:

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

- **Automatic proxy configuration URL** -

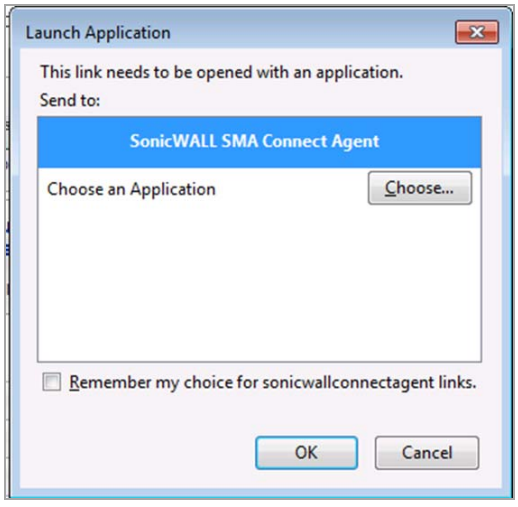


Logs

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

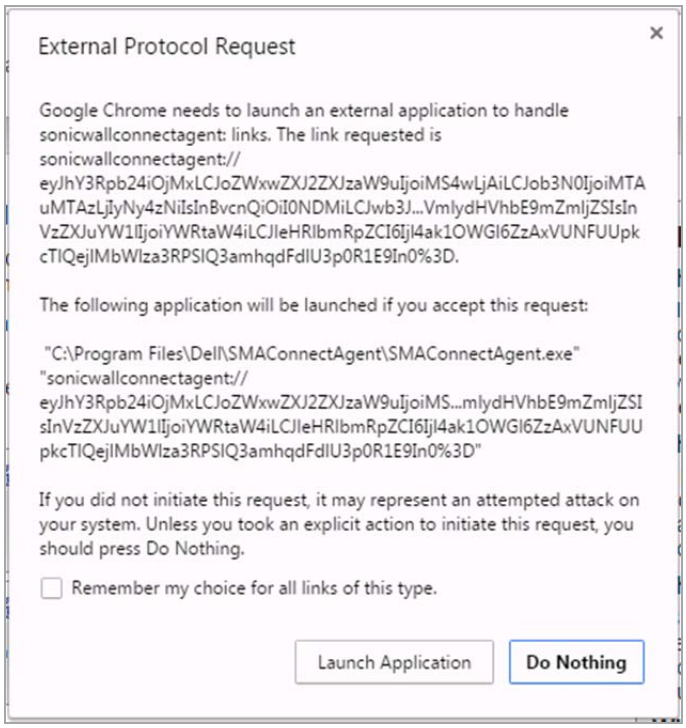
Browser Warning

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

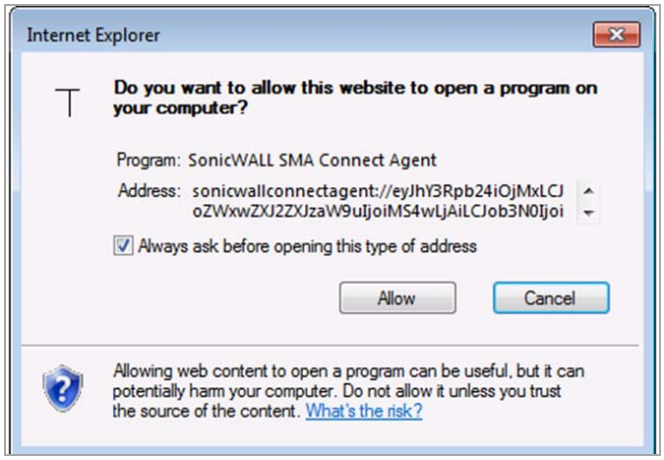


With a Firefox warning window, press **OK** to launch the SMA Connect Agent.

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



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



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

End Point Control (EPC)

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

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

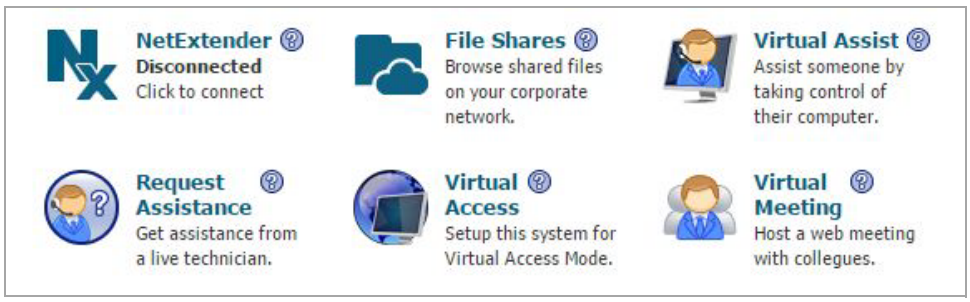
If the EPC feature (Appliance side) enables the “Show EPC failed message in detail at client side,” the SMA Connect Agent records the detailed fail message in the log. Then, you can view the tray Log.

PDA (Personal Device Authorization)

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

SonicWall Application

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



Net-Extender cannot run on Macintosh. Therefore, the SMA Connect Agent does not support the Net-Extender connection on Macintosh.

Part 6

Appendices

- Using Online Help
- Configuring the SMA/SRA Appliance with a Third-Party Gateway
- Use Cases
- NetExtender Troubleshooting
- Frequently Asked Questions
- Using the Command Line Interface
- Using SMS Email Formats
- Support Information

A

Using Online Help

This appendix describes how to use the **Online Help** on the Secure Mobile Access web-based management interface. This appendix also contains information about context-sensitive help.

Online Help Button

Online Help is located in upper right corner of the Secure Mobile Access management interface.

Online Help launches the online help in a separate Web browser. **Online Help** links to the main page of the online help document.

Using Context Sensitive Help

Context-sensitive help is available on most pages of the Secure Mobile Access 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 Secure Mobile Access 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 check boxes throughout the Secure Mobile Access 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.

B

Configuring the SMA/SRA Appliance with a Third-Party Gateway

This appendix shows methods for configuring various third-party firewalls for deployment with a Secure Mobile Access (SMA) or Secure Remote Access (SRA) appliance.

Topics:

Cisco PIX Configuration for SMA/SRA Appliance Deployment

Topics:

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 Inc. 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 an SMA/SRA appliance. You need a valid Cisco SmartNET maintenance contract for your Cisco PIX and a CCO log in to obtain newer versions of the PIX OS.

NOTE: The WAN/DMZ/LAN IP addresses used in the deployment method examples that follow are not valid and need to be modified to reflect your networking environment.

Management Considerations for the Cisco Pix

Both deployment methods described in the sections that follow use the PIX's WAN interface IP address as the means of external connectivity to the internal SMA/SRA appliance. The PIX has the ability to be managed through 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 SMA/SRA appliance, you do not have to deactivate the HTTP/S management interface on the PIX.

Method One – SMA/SRA Appliance on LAN Interface

1. From a management system, log in to the SMA/SRA appliance's Secure Mobile Access management interface. By default the management interface is X0 and the default IP address is 192.168.200.1.
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 **OK** to save and activate the change.
3. Navigate to the **Network > Routes** page and change the Default Gateway to **192.168.100.1** When done, click **Accept** in the upper-right corner to save and activate the change.
4. Navigate to the **NetExtender > Client Addresses** page. You 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 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 **Accept** in the upper-right corner to save and activate the change.
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.
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 **Accept** in the upper-right corner to save and activate the change.
7. Navigate to the **System > Restart** page and click **Restart…**
8. Install the SMA/SRA appliance's X0 interface on the LAN network of the PIX. Do not hook any of the appliance's other interfaces up.
9. Connect to the PIX's management CLI by way of the console port, telnet, or SSH and enter configure mode.
10. Issue the command **'clear http'** to shut off the PIX's HTTP/S management interface.
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)
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)
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)
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)
15. Issue the command **'access-group sslvpn in interface outside'**
16. Exit config mode and issue the command **'wr mem'** to save and activate the changes.

17 From an external system, attempt to connect to the SMA/SRA appliance using both HTTP and HTTPS. If you cannot access the SMA/SRA appliance, check all previous steps 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 – SMA/SRA 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 are using the default numbering scheme of the SMA/SRA appliance.

1. From a management system, log in to the SMA/SRA appliance's Secure Mobile Access management interface. By default the management interface is X0 and the default IP address is 192.168.200.1.
2. Navigate to the **Network > Routes** page and make sure the Default Gateway is set to 192.168.200.2 When done, click **Accept** in the upper-right corner to save and activate the change.
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 **Accept** in the upper-right corner to save and activate the change.
4. Navigate to the **NetExtender > Client Routes** page. Add a client route for **192.168.100.0** and **192.168.200.0**.
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 **Accept** in the upper-right corner to save and activate the change.
6. Navigate to the **System > Restart** page and click **Restart…**
7. Install the SMA/SRA appliance's X0 interface on the unused DMZ network of the PIX. Do not hook any of the appliance's other interfaces up.
8. Connect to the PIX's management CLI by way of console port, telnet, or SSH and enter configure mode.

9 Issue the command **'clear http'** to shut off the PIX's HTTP/S management interface.

10 Issue the command '**interface ethernet2 auto'** (or whatever interface you are using)

11 Issue the command '**nameif ethernet2 dmz security4'** (or whatever interface you are using)

12 Issue the command '**ip address dmz 192.168.200.2 255.255.255.0'**

13 Issue the command **'nat (dmz) 1 192.168.200.0 255.255.255.0 0 0'**

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)

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)

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'**

17 Issue the command '**access-list dmz-to-inside permit ip host 192.168.200.1 any'**

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)

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)

20 Issue the command **'static (inside,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0 0 0'**

21 Issue the command **'access-group sslvpn in interface outside'**

22 Issue the command **'access-group dmz-to-inside in interface dmz'**

23 Exit config mode and issue the command **'wr mem'** to save and activate the changes.

24 From an external system, attempt to connect to the SMA/SRA appliance using both HTTP and HTTPS. If you cannot access the SMA/SRA appliance, check all previous steps 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

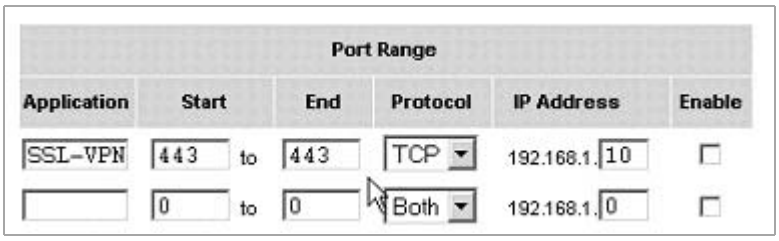
The SMA/SRA appliance should be configured on the LAN switch of the Linksys wireless router. This guide assumes that your Linksys is assigned a single WAN IP, through DHCP by the cable ISP and is using the default LAN IP address scheme of 192.168.1.0/24.

NOTE: Version 2.07.1 firmware or newer is recommended for this setup.

To configure your Linksys for operation with the SMA/SRA appliance, you must forward the SSL (443) port to the IP address of the SMA/SRA appliance.

1 Log in to the Linksys device.

2 Navigate to the **Applications & Gaming** tab.



3 Enter the following information:

Information to be added to Applications & Gaming tab

Application	SMA/SRA	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 SMA/SRA application uses TCP.
IP Address	192.168.1.10	The IP address assigned to the SMA/SRA appliance.
Enable	Checked	Select the check box to enable the SSL port forwarding.

4 With the configuration complete, click **Save Settings** on the bottom of the page.

The Linksys is now ready for operations with the SMA/SRA appliance.

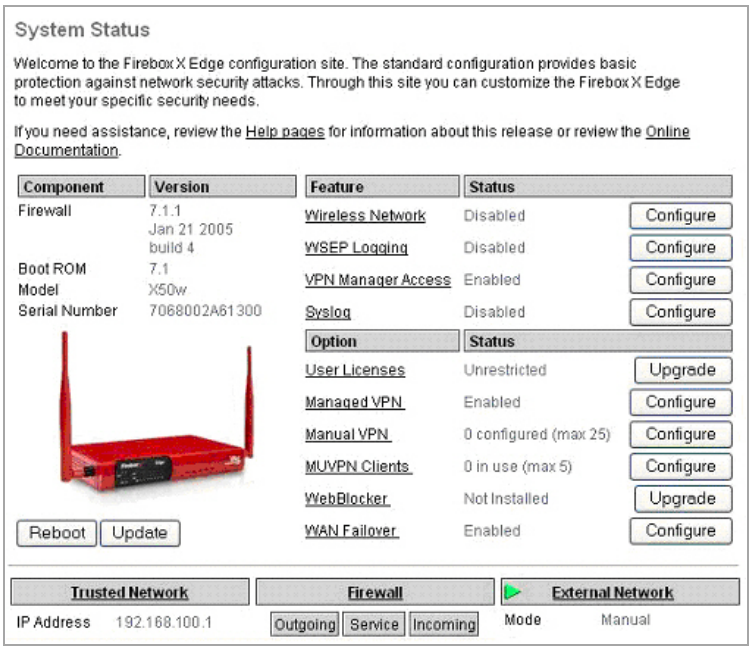
WatchGuard Firebox X Edge

This guide assumes that your WatchGuard Firebox X Gateway is configured with an IP of 192.168.100.1 and your SMA/SRA appliance is configured with an IP of 192.168.100.2.

NOTE: The steps that follow 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 should first review the notes within this guide.

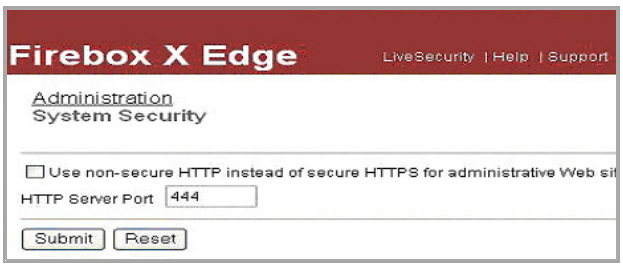
1 Open browser and enter the IP address of the WatchGuard Firebox X Edge appliance (such as 192.168.100.1). When successful, you'll be brought to the "System Status" page (See the following).



2 If the WatchGuard's management interface is already configured to accept HTTPS on port 443 you need to change the port in order to be able to manage both the SMA/SRA and WatchGuard appliances.

3 Navigate to **Administration > System Security**.

WatchGuard Administration > System Security Dialog Box

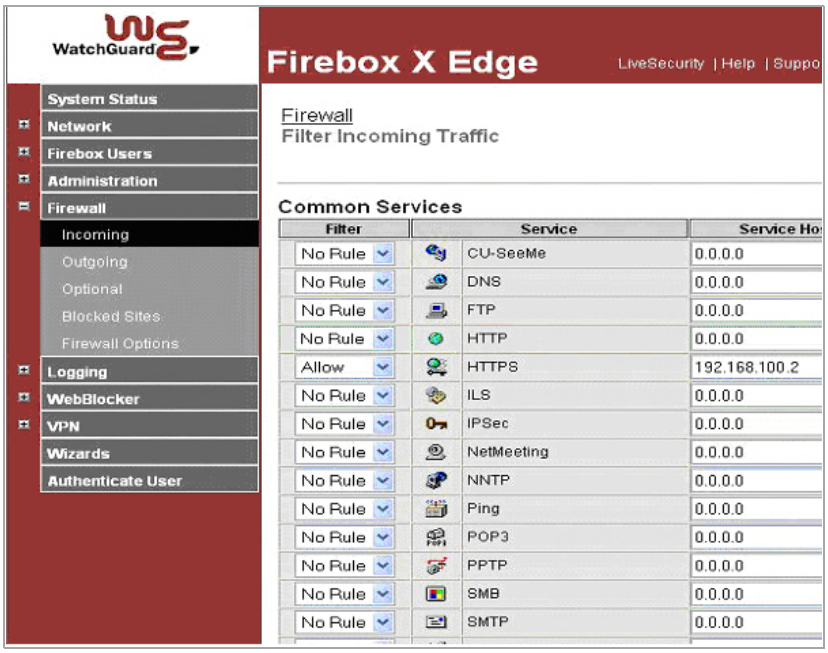


4 Clear **Use non-secure HTTP instead of secure HTTPS for administrative Web site**.

5 Change the **HTTP Server Port** to 444 and click **Submit**.

The WatchGuard is now managed from the WAN on port 444. It should be accessed as follows: https://<watchguard wan ip>:444

6 In the left navigation menu, Navigate to **Firewall > Incoming**.



7 For the **HTTPS Service**, set **Filter** to Allow and enter the WAN IP of the SMA/SRA appliance (192.168.100.2) in the **Service Host** field.

8 Click **Submit** at the bottom of the page.

Your Watchguard Firebox X Edge is now ready for operations with the SMA/SRA appliance.

NetGear FVS318

This guide assumes that your NetGear FVS318 Gateway is configured with an IP of 192.168.100.1 and your SMA/SRA appliance is configured with an IP of 192.168.100.2.

1 Click **Remote Management** from the left index of your Netgear management interface.

In order for the SMA/SRA appliance to function with your Netgear gateway device, you must verify that the NetGear's management port does not conflict with the management port used by the SMA/SRA appliance.

2 Clear the **Allow Remote Management** box.

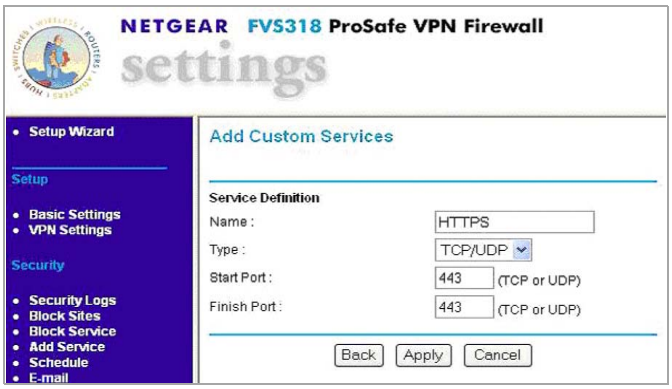
3 Click **Accept** to save changes.

NOTE: If Remote Management of the NetGear is desired, you must leave the box checked and change the default port (8080 is recommended)

4 Navigate to **Add Service** in the left navigation.

5 Click **Add Custom Service**.

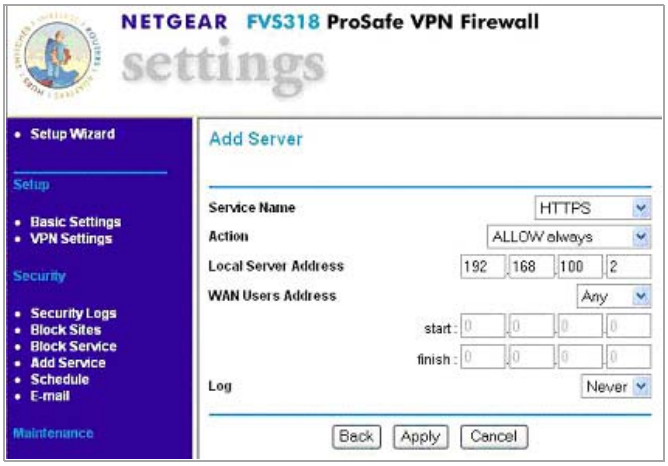
6 To create a service definition, enter the following information:



Name	HTTPS
Type	TCP/UDP
Start Port	443
Finish Port	443

7 Navigate to **Ports** in the left navigation.

Click **Add**.



8 Select HTTPS from the **Service Name** drop-down list.

9 Select ALLOW always in the **Action** drop-down list.

10 Enter the WAN IP address of the SMA/SRA appliance (ex.192.168.100.2) in the **Local Server Address** field.

11 Click Accept to save changes.

Your Netgear gateway device is now ready for operations with the SMA/SRA appliance.

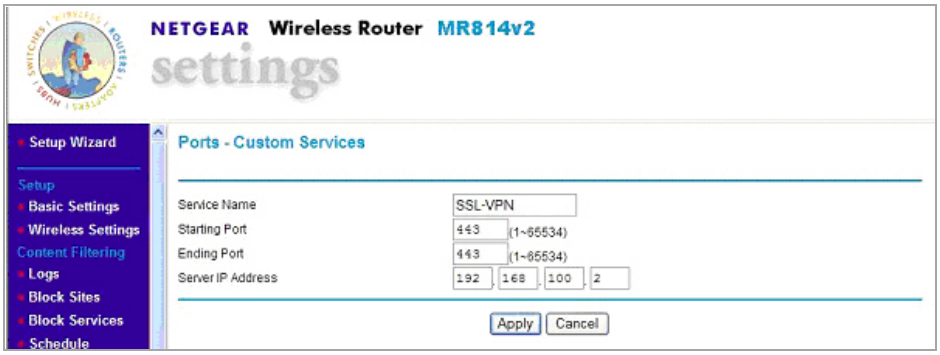
Netgear Wireless Router MR814 SSL configuration

This guide assumes that your NetGear Wireless Router is configured with an IP of 192.168.100.1 and your SMA/SRA appliance is configured with an IP of 192.168.100.2.

1 Navigate to **Advanced > Port Management** in the left index of your Netgear management interface.

2 Click **Add Custom Service** in the middle of the page.

3 Enter a service name in the **Service Name** field (ex. SMA)



4 Enter **443** in the **Starting Port** field.

5 Enter **443** in the **Ending Port** field.

6 Enter the WAN IP address of the SMA/SRA appliance (ex.192.168.100.2) in the **Local Server Address** field.

7 Click **Accept**.

Your Netgear wireless router is now ready for operations with the SMA/SRA appliance.

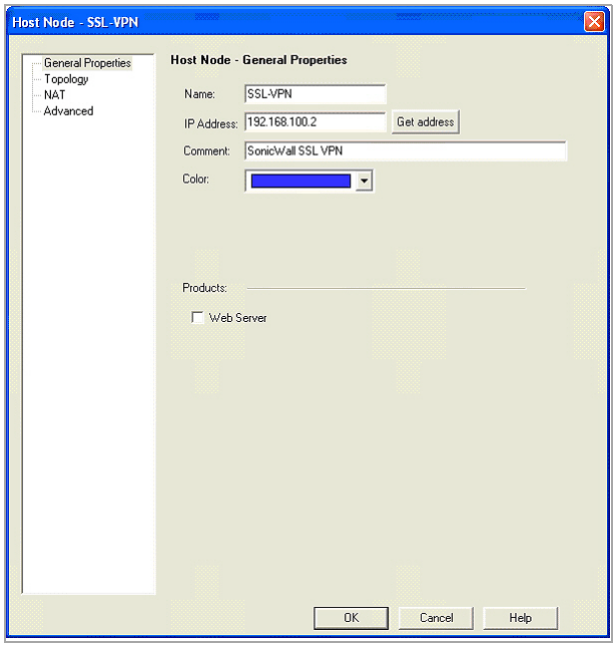
Check Point AIR 55

Topics:

Setting up an SMA/SRA Appliance 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.”

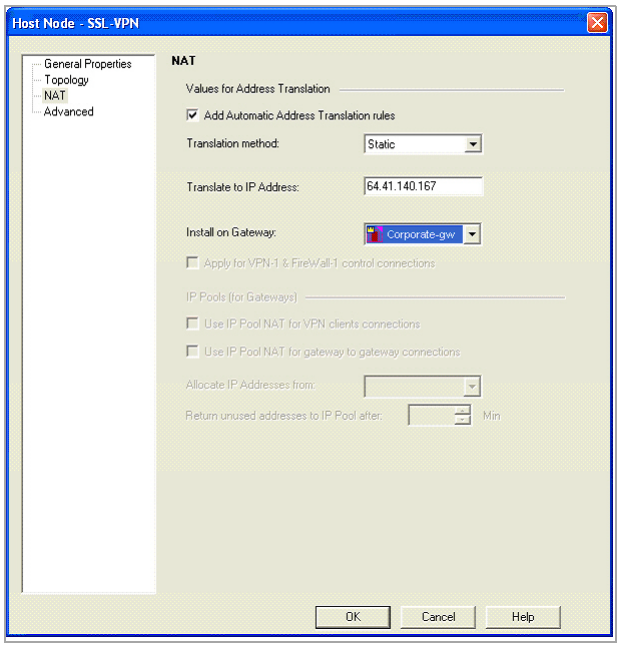
Check Point Host Node Object Dialog Box



NOTE: The object is defined as existing on the internal network. Should you decide to locate the SMA/SRA appliance on a secure segment (sometimes known as a demilitarized zone) then subsequent firewall rules 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.

Check Point NAT Properties Dialog Box



Here you should 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** automatically creates the necessary NAT rule shown in the following section.

Check Point NAT Rule Window

5	SSL-VPN	Any	Any	SSL-VPN (Valid ...	Original	Original	Corporate-g...
6	Any	SSL-VPN (Valid ...	Any	Original	SSL-VPN	Original	Corporate-g...

Static Route

Most installations of Check Point AIR55 require a static route. This route sends all traffic from the public IP address for the SMA/SRA appliance 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 automatically adds an ARP entry for a secondary external IP address (the public IP address of the SMA/SRA appliance). 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 SMA/SRA appliance.

Check Point Policy Rule Window

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON
1	Any	SSL-VPN	Any Traffic	TCP https	accept	None	Policy Targets
2	Any	Any	Any Traffic	Any	drop	None	Policy Targets

Again, should the SMA/SRA appliance be located on a secure segment of the Check Point firewall, a second rule allowing the relevant traffic to flow from the SMA/SRA appliance to the internal network is necessary.

C

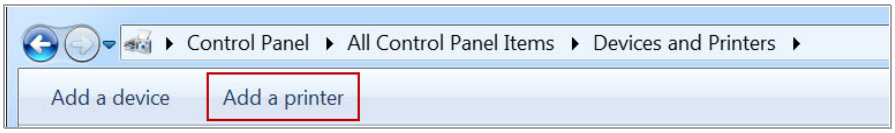
Printer redirection

This appendix provides information on installing a specific printer driver redirection, the “MS Publisher Imagesetter.” HTML5 RDP support a specific Printer Redirection if the Remote Desktop Session Host server has the driver installed. HTML5 RDP can redirect the printer to the client side. The user can select the Redirection Printer to print files to a PDF. After the PDF is created, a file pop-up viewer appears. You can “Print Preview” the PDF file or print the file directly.

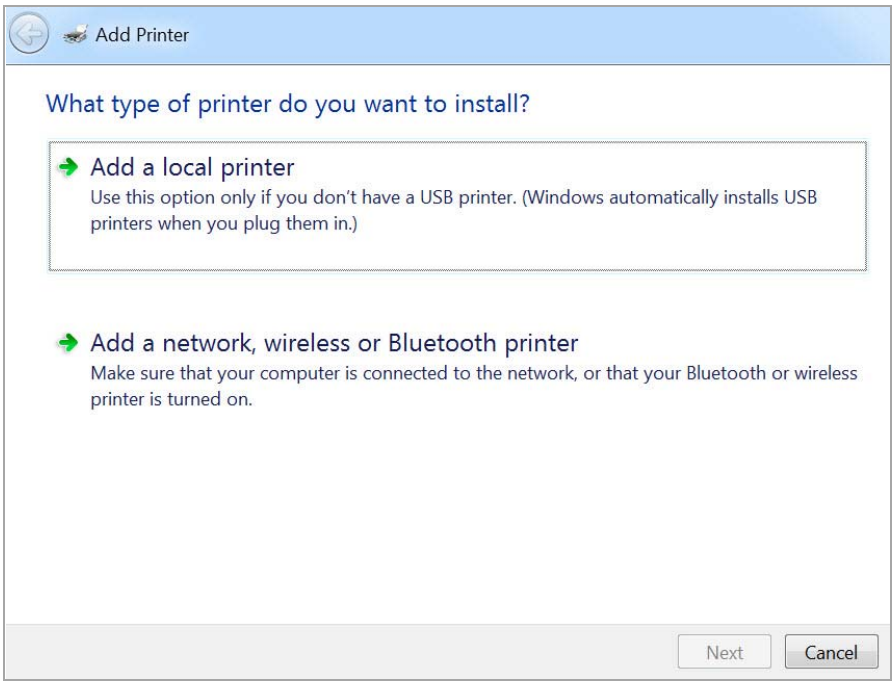
To install the MS Publisher Imagesetter on Windows 7:

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

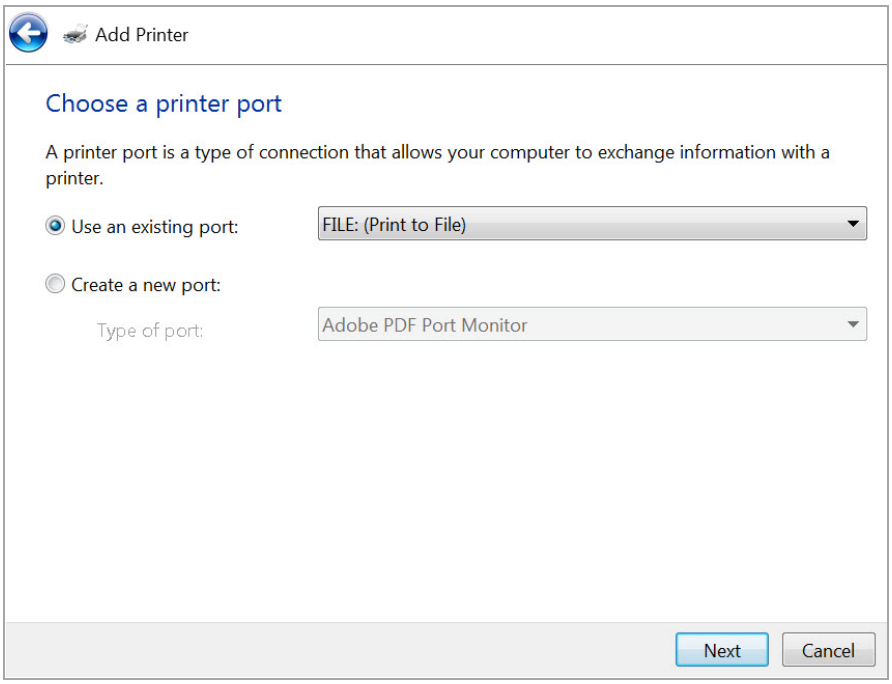
2 Click **Add a printer**.



3 Select **Add a local printer**.

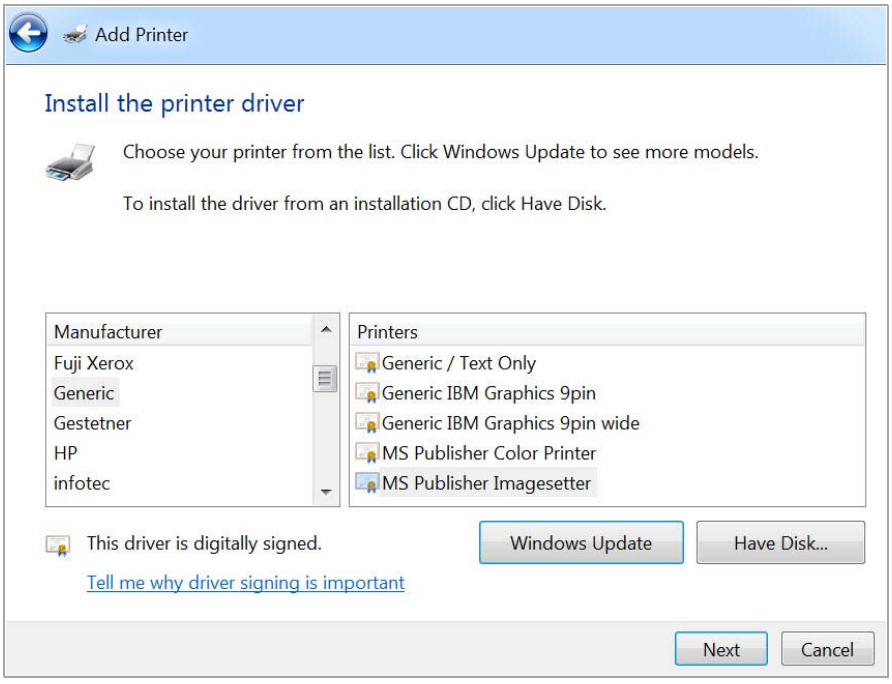


4 Select **Use an existing port** and then **FILE: (Print to File)** in the drop-down box.



5 Click **Next**.

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



7 Click **Next**.

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

9 Click **Next**.

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

11 Click **Next**.

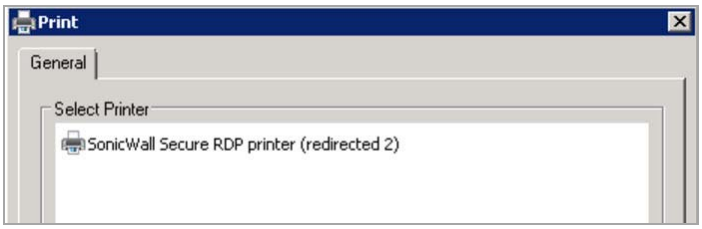
12 Select the option that best suits your sharing criteria.

13 Click **Next**.

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

Enable the Redirection Printers

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



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

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

Time-zone redirection

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

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

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

2 Use the following path:

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

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

4 Click **OK**.

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

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

D

Use Cases

This appendix provides the following use cases:

Importing CA Certificates on Windows

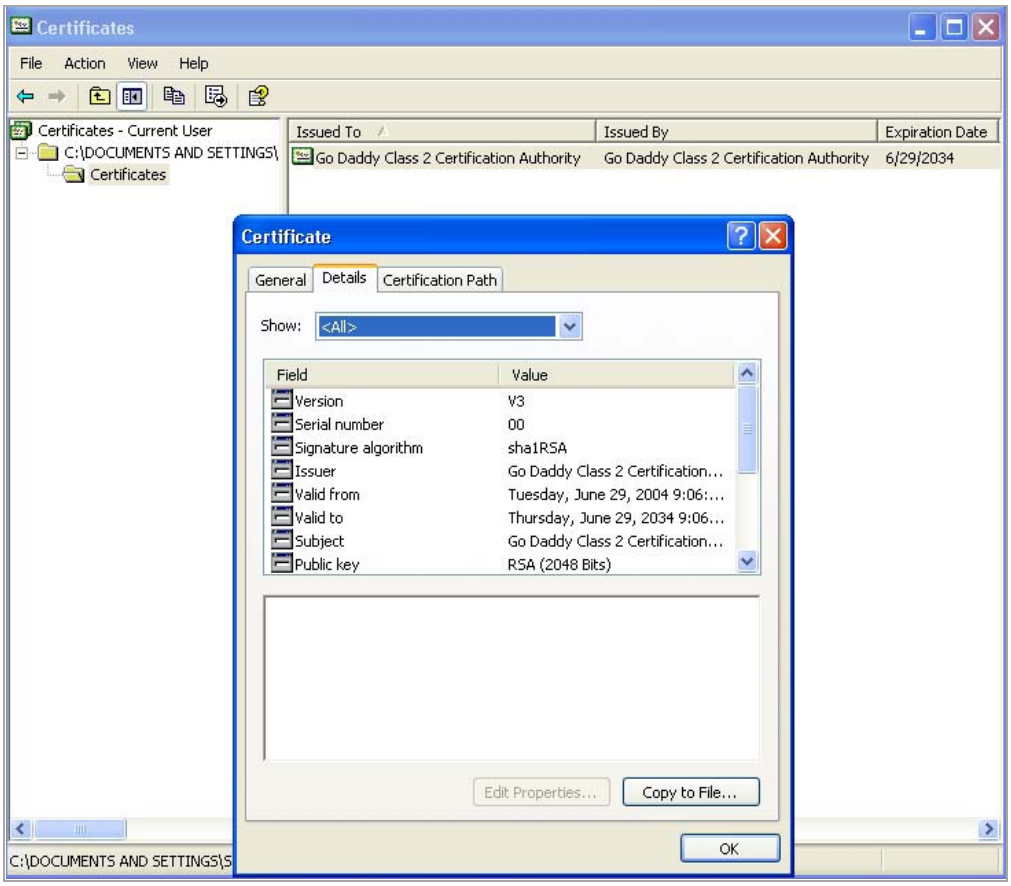
Two certificates are imported in this use case, a goDaddy certificate and a server certificate. See the following sections:

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 Secure Mobile Access (SMA) and Secure Remote Access (SRA) appliance.

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.

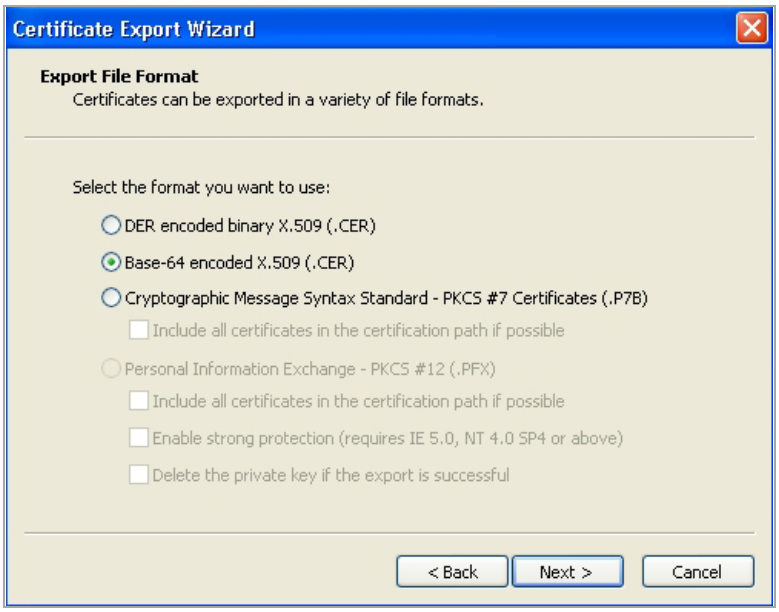
2 Double-click the certificate file and select the **Details** tab.



3 Click **Copy to File**. The Certificate Export Wizard launches.

4 In the Certificate Export Wizard, click **Next**.

5 Select **Base-64 encoded X.509 (.CER)** and then click **Next**.



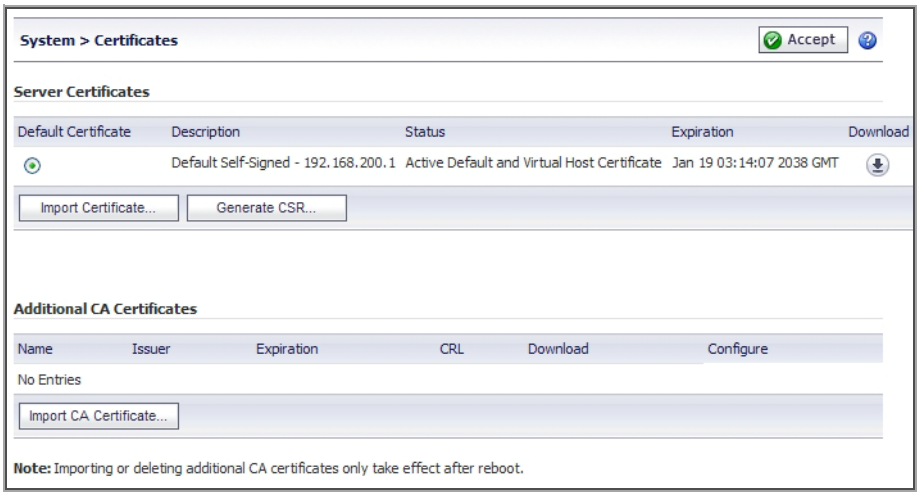
6 In the File to Export screen, type the file name in as **goDaddy.cer** and then click **Next**.

7 In the Completing the Certificate Export Wizard screen, verify the path and format and then click **Finish**.

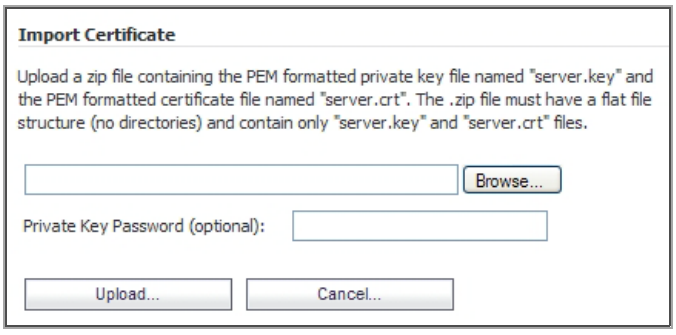
8 Click **OK** in the confirmation dialog box.

The certificate is exported in base-64 encoded format. You can view it in a text editor.

9 In the Secure Mobile Access management interface, navigate to **System > Certificates**.

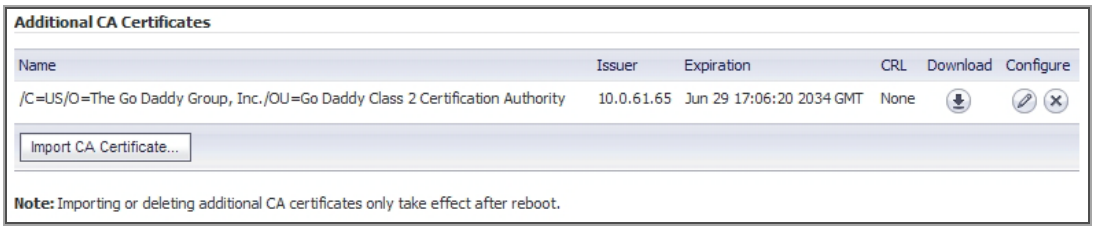


10 In the **Additional CA Certificates** section, click **Import CA Certificate**. The Import Certificate window appears.



11 In the Import Certificate window, click **Browse** and navigate to the **goDaddy.cer** file on your Windows system and double-click it.

12 Click **Upload**. The certificate is listed in the **Additional CA Certificates** table.



13 Navigate to **System > Restart** and restart the SMA/SRA appliance for the CA certificate to take effect.

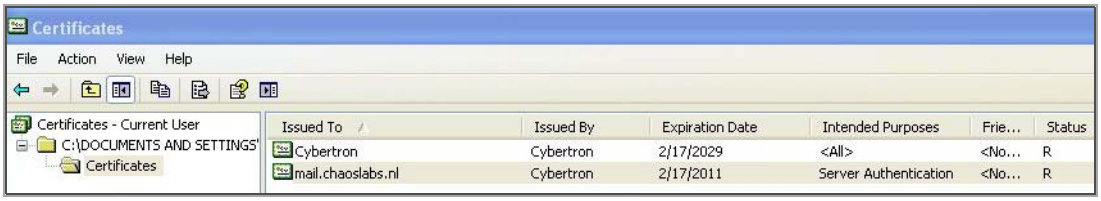
Importing a Server Certificate on Windows

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.

1 Double-click on the **mail.chaoslabs.nl.pb7** file and navigate to the certificate.



2 Double-click the certificate file and select the **Details** tab.

3 Click **Copy to File**.

4 In the Certificate Export Wizard, select **Base-64 encoded X.509 (.CER)**.

5 Click **Next** and save the file as **server.crt** on your Windows system.

The certificate is exported in base-64 encoded format.

6 Add the server.crt file to a .zip file.

7 Separately save the private key in base-64 format as **server.key**.

8 Add the **server.key** file to the .zip file that contains **server.crt**.

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 SMA/SRA appliance, 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.

While Active Directory allows users to be members in multiple groups, the SMA/SRA appliance only allows each user to belong to a single group. It is this group that determines the access policies assigned to the user.

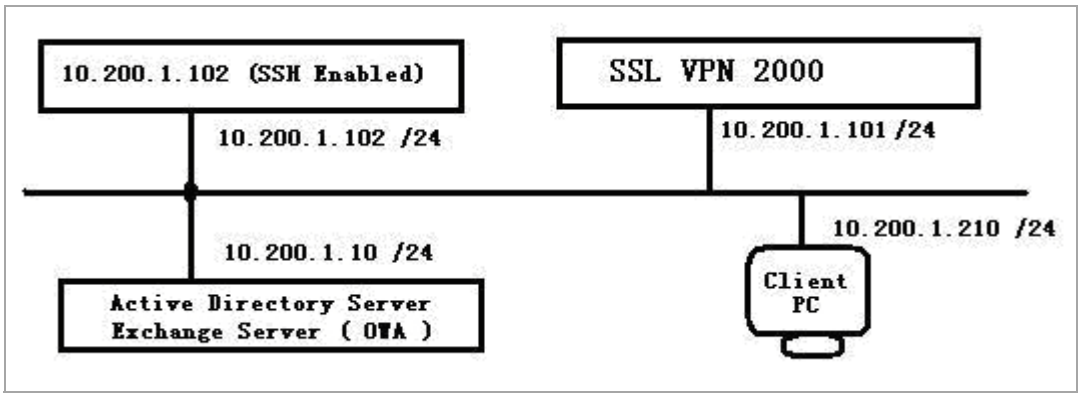
When importing a user from AD, the user is placed into the local Secure Mobile Access group with which they have the most AD groups in common. For example: Bob belongs to the Users, Administrators, and Engineering AD groups. If one Secure Mobile Access group is associated with Users, and another is associated with both Administrators and Engineering, Bob is assigned to the Secure Mobile Access 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 Secure Mobile Access 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 previously
- Deny access to these resources to all other groups

This example configuration is provided courtesy of Vincent Cai, June 2008.

Network Topology



Perform the tasks in order of the following sections:

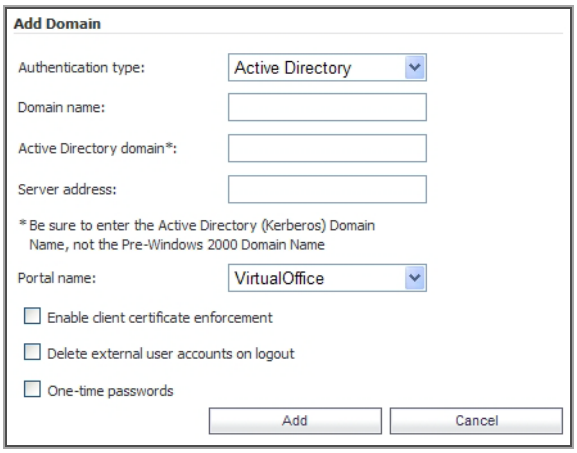
- Creating the Active Directory Domain on page 475
- Adding a Global Deny All Policy on page 476
- Creating Local Groups on page 477
- Adding the SSHv2 PERMIT Policy on page 479
- Adding the OWA PERMIT Policies on page 480
- Verifying the Access Policy Configuration on page 481

Creating the Active Directory Domain

This section describes how to create the Secure Mobile Access Local Domain, SNWL_AD. SNWL_AD is associated with the Active Directory domain of the OWA server.

1 Log in to the Secure Mobile Access management interface and navigate to the **Portals > Domains** page.

2 Click **Add Domain**. The Add Domain window appears.



3 In the **Authentication type** drop-down list, select **Active Directory**.

4 In the **Domain name** field, type **SNWL_AD**.

5 In the **Active Directory domain** field, type the AD domain name, **in.loraxmfg.com**.

6 In the **Server address** field, type the IP address of the OWA server, **10.200.1.10**.

7 Click **Add**.

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.

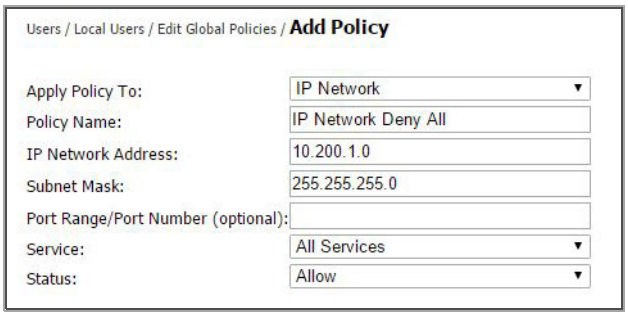
The Secure Mobile Access default policy is **Allow All**. In order to have more granular control, we add a **Deny All** policy here. Later, we can add **Permit** policies for each group, one at a time.

1 Navigate to the **Users > Local Users** page.

2 Click **Configure**  in the **Global Policies** row. The **Edit Global Policies** window appears.

3 In the **Edit Global Policies** window, click the **Policies** tab.

4 Click **Add Policy**. The Add Policy window appears.



5 Select **IP Network** from the **Apply Policy To** drop-down list.

6 In the **Policy Name** field, type the descriptive name **IP Network Deny All**.

7 In the **IP Network Address** field, type the network address, **10.200.1.0**.

8 In the **Subnet Mask** field, type the mask in decimal format, **255.255.255.0**.

9 In the **Service** drop-down list, select **All Services**.

10 In the **Status** drop-down list, select **Allow**.

11 Click **Add**.

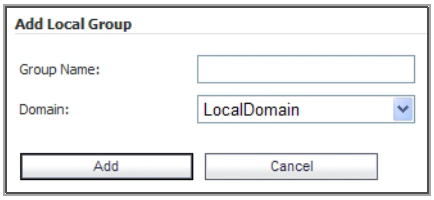
12 In the **Edit Global Policies** window, verify the **Deny All** policy settings and then click **OK**.

Creating Local Groups

This procedure creates Local Groups that belong to the SNWL_AD domain on the SMA/SRA appliance. We create one local group for each Active Directory group.

Adding the Local Groups

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.



2 In the **Add Local Group** window, type **Acme_Group** into the **Group Name** field.

3 Select **SNWL_AD** from the **Domain** drop-down list.

4 Click **Add**.

5 On the **Users > Local Groups** page, click **Add Group** to add the second local group.

6 In the Add Local Group window, type **Mega_Group** into the **Group Name** field.

7 Select **SNWL_AD** from the **Domain** drop-down list.

8 Click **Add**.

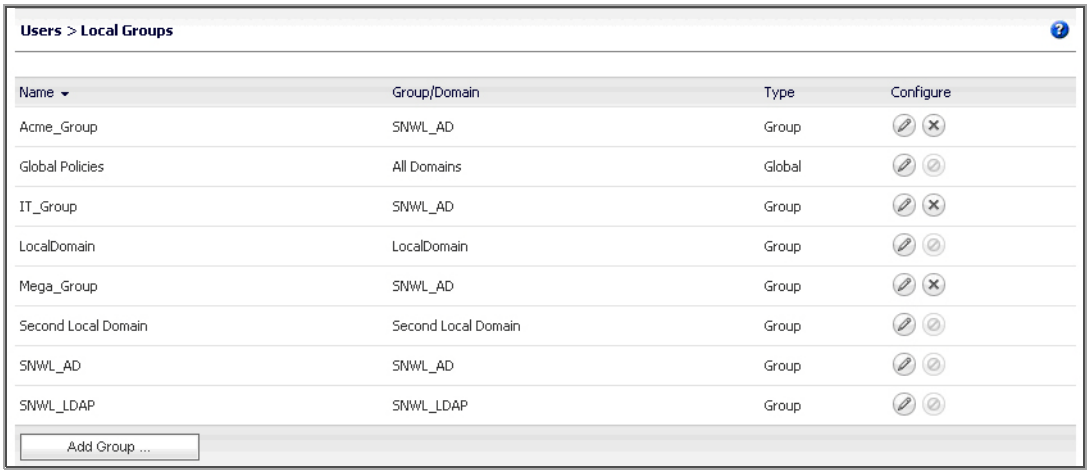
9 On the **Users > Local Groups** page, click **Add Group** to add the second local group.

10 In the Add Local Group window, type **IT_Group** into the **Group Name** field.

11 Select **SNWL_AD** from the **Domain** drop-down list.

12 Click **Add**.

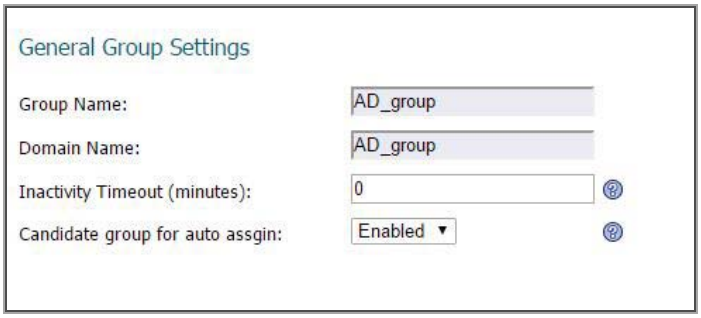
13 View the added groups on the **Users > Local Groups** page.



Configuring the Local Groups

In this procedure, we will edit each new local group and associate it with the corresponding Active Directory Group.

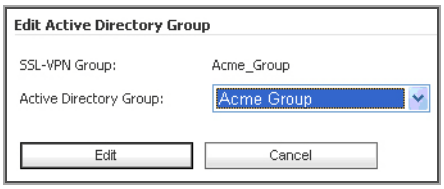
1 Click **Configure** in the **Acme_Group** row. The **Edit Group Settings** window appears.



2 In the **Edit Group Settings** window, click the **AD Groups** tab.

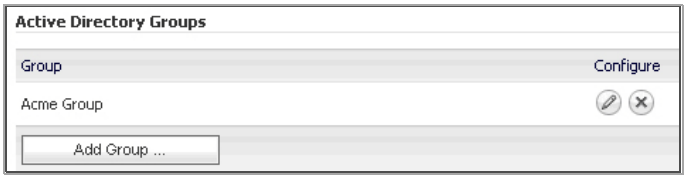
3 On the **AD Groups** tab, click **Add Group**.

4 In the **Edit Active Directory Group** window, select **Acme Group** from the **Active Directory Group** drop-down list.



5 Click **Edit**.

Acme Group is listed in the **Active Directory Groups** table on the **AD Groups** tab.



6 In the **Edit Group Settings** window, click **OK**.

7 On the **Users > Local Groups** page, click **Configure** in the **Mega_Group** row. The **Edit Group Settings** window appears.

8 In the **Edit Group Settings** window, click the **AD Groups** tab and then click **Add Group**.

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.

10 In the **Edit Group Settings** window, click **OK**.

11 On the **Users > Local Groups** page, click **Configure** in the **IT_Group** row. The **Edit Group Settings** window appears.

12 In the **Edit Group Settings** window, click the **AD Groups** tab and then click **Add Group**.

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.

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 Secure Mobile Access Local Group, **Acme_Group**, and results in SSH access for members of the Active Directory group, Acme Group.

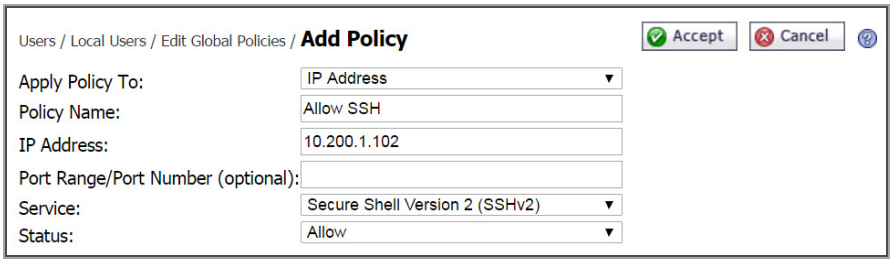
Repeat this procedure for **IT_Group** to provide SSH access to the server for members of the Active Directory group, IT Group.

1 On the **Users > Local Groups** page, click **Configure** in the **Acme_Group** row. The **Edit Group Settings** window appears.

2 In the **Edit Group Settings** window, click the **Policies** tab.

3 On the **Policies** tab, click **Add Policy**.

4 In the **Add Policy** window, select **IP Address** in the **Apply Policy To** drop-down list.



5 In the **Policy Name** field, enter the descriptive name, **Allow SSH**.

6 In the **IP Address** field, enter the IP address of the target server, **10.202.1.102**.

7 In the **Services** drop-down list, select **Secure Shell Version 2 (SSHv2)**.

8 In the **Status** drop-down list, select **ALLOW**, and then click **Accept**.

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 Secure Mobile Access 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.

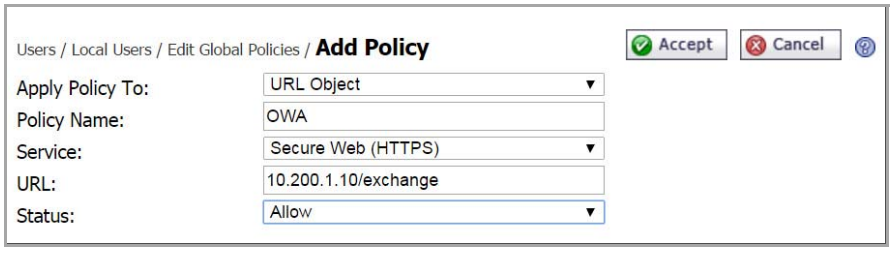
NOTE: In this configuration, members of IT_Group and Mega_Group are denied access to the https://owa-server/public folder, because these groups have access only to the /exchange and /exchweb subfolders.

The OWA policies are applied to Exchange server URL Objects rather than server IP addresses since OWA is a Web service.

1 In the **Users > Local Groups** page, click **Configure** in the **Mega_Group** row. We will create **two** PERMIT policies for Mega_Group to allow access to the OWA Exchange server.

2 In the **Edit Group Settings** window, click the **Policies** tab, and then click **Add Policy**.

3 In the **Add Policy** window, select **URL Object** in the **Apply Policy To** drop-down list.



4 In the **Policy Name** field, enter the descriptive name, **OWA**.

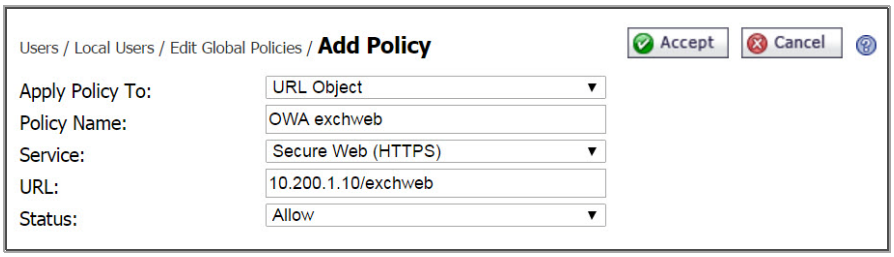
5 In the **Service** drop-down list, select **Secure Web (HTTPS)**.

6 In the **URL** field, enter the URL of the target application, **10.200.1.10/exchange**.

7 In the **Status** drop-down list, select **ALLOW**, and then click **Accept**.

8 In the **Edit Group Settings** window on the **Policies** tab, click **Add Policy**.

9 In the **Add Policy** window, select **URL Object** in the **Apply Policy To** drop-down list.



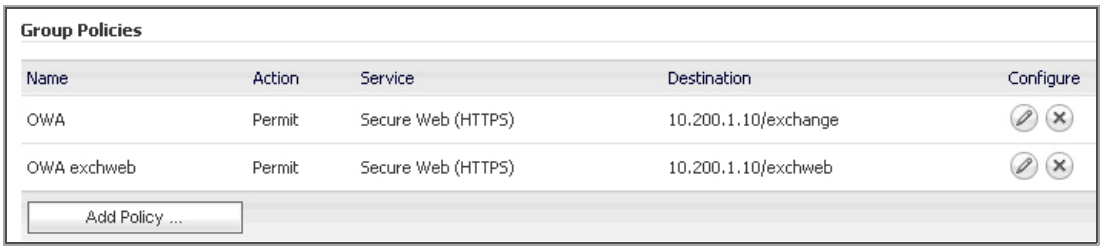
10 In the **Policy Name** field, enter the descriptive name, **OWA exchweb**.

11 In the **Service** drop-down list, select **Secure Web (HTTPS)**.

12 In the **URL** field, enter the URL of the target application, **10.200.1.10/exchweb**.

13 In the **Status** drop-down list, select **ALLOW**, and then click **Accept**.

14 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

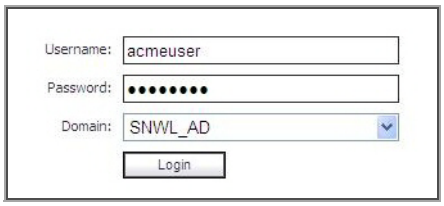
At this point:

- 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 previously

The configuration can be verified by logging in as different AD group members to the SNWL_AD domain on the SMA/SRA appliance, and attempting to access the resources.

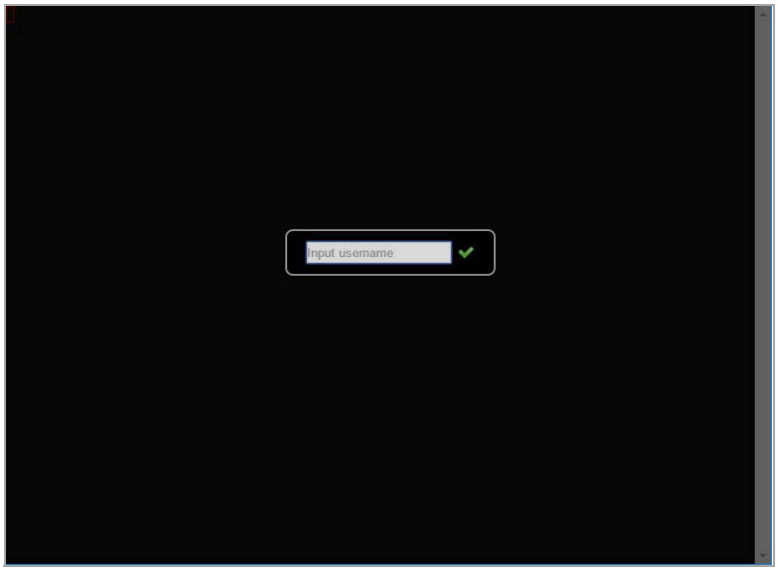
Test Result: Try Acmeuser Access

Acmeuser logs into the **SNWL_AD** domain.



The **Users > Status** page shows that **acmeuser** is a member of the local group, **Acme_Group**.

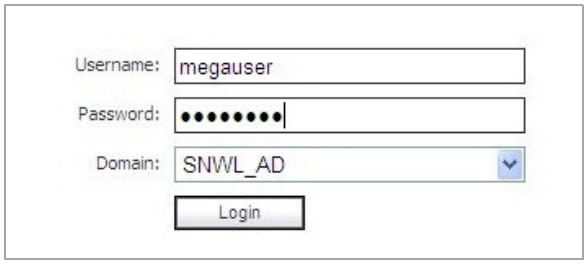
Acmeuser can access SSH, as expected.



Acmeuser tries to access to other resources like OWA 10.200.1.10, but is denied, as expected.

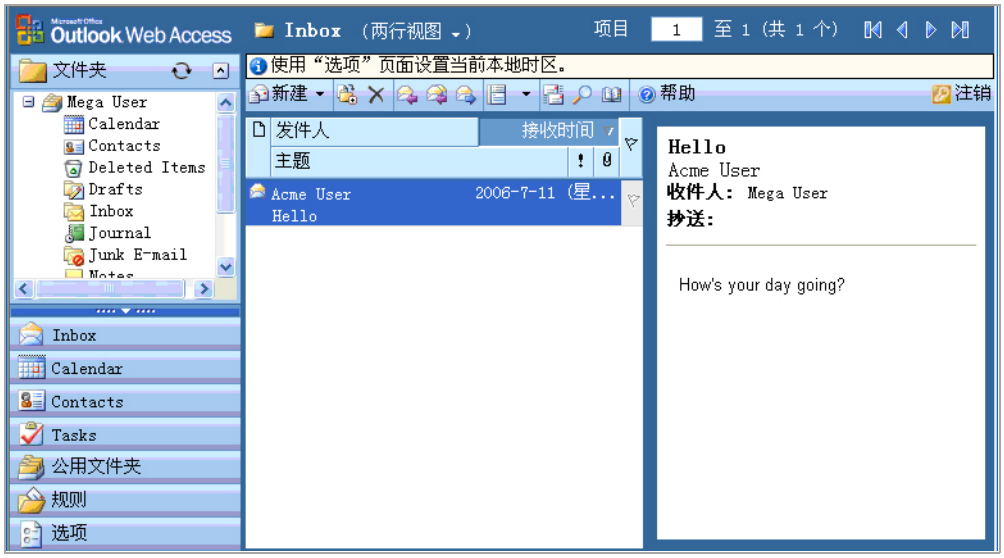
Test Result: Try Megauser Access

Megauser logs into the **SNWL_AD** domain.

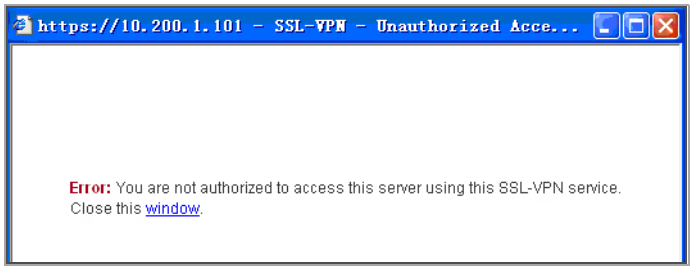


The **Users > Status** page shows that **megauser** is a member of the local group, **Mega_Group**.

Megauser can access OWA resources, as expected.



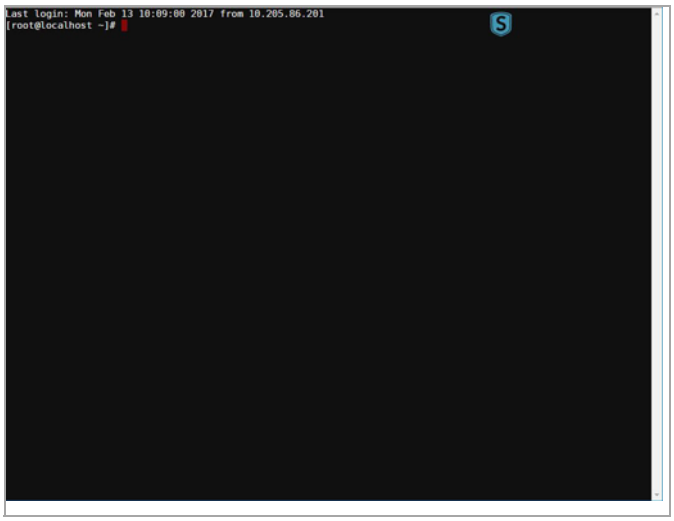
Megauser tries to access SSH, but is denied, as expected.



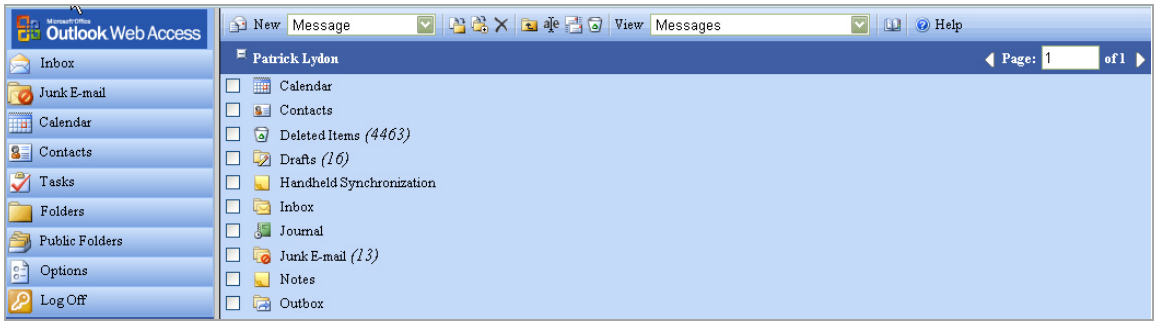
Test Result: Try Ituser Access

Ituser logs into the **SNWL_AD** domain. The **Users > Status** page shows that **ituser** is a member of the local group, **IT_Group**.

ltuser can access SSH to 10.200.1.102, as expected.



ltuser can access OWA resources, as expected.



E

NetExtender Troubleshooting

See the following tables with troubleshooting information for the Secure Mobile Access (SMA) or Secure Remote Access (SRA) NetExtender utility.

NetExtender Cannot Be Installed

Problem	Solution
NetExtender cannot be installed.	1 Check your OS Version, NetExtender only supports Windows Vista or higher, Mac OS X 10.5 or higher with Apple Java 1.6.0_10 or higher, 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 Secure Mobile Access NetExtender Adapter from Device Manager. • The log file located at **C:\Program files\SonicWall\SMA\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.

NetExtender Connection Entry Cannot Be Created

Problem	Solution
NetExtender connection entry cannot be created.	1 Navigate to Device Manager and check if the Secure Mobile Access 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 Secure Mobile Access NetExtender Adapter from Device Manager. • The log file located at **C:\Program files\SonicWall\SMA\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.

NetExtender Cannot Connect

Problem	Solution
NetExtender cannot connect.	1 Navigate to Device Manager and check if the Secure Mobile Access 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 Secure Mobile Access 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 Secure Mobile Access NetExtender Adapter from Device Manager. • The log file located at **C:\Program files\SonicWall\SMA\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.

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 Secure Mobile Access NetExtender Adapter from Device Manager. • The log file located at **C:\Program files\SonicWall\SMA\NetExtender.dbg**. • Windows memory dump file located at **C:\Windows\MEMORY.DMP**. If you cannot find this file, then you should open System Properties, click **Startup and Recovery Settings** 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 should also 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.

F

Frequently Asked Questions

This appendix contains frequently asked questions (FAQs) about the Secure Mobile Access (SMA) or Secure Remote Access (SRA) appliance.

Hardware FAQ

1 What are the hardware specs for the SMA 400 and SMA 200?

Answer:

Interfaces

SMA 200: (2) gigabit Ethernet, (2) USB, (1) console

SMA 400: (4) gigabit Ethernet, (2) USB, (1) console

Processors

SMA 200: 1.74 GHz Intel Atom™ C2358 Dual Core Processor

SMA 400: 2.40 GHz Intel Atom™ C2358 Quad Core Processor

Memory (RAM)

SMA 200: 2 GB

SMA 400: 4 GB

Flash Memory

SMA 200: 2 GB (CFAST)

SMA 400: 2 GB (CFAST)

Power Supply

SMA 200: Fixed Internal, 60W adaptor

SMA 400: Fixed Internal, 60W adaptor

Max Power Consumption

SMA 200: 26.9 W

SMA 400: 31.9 W

Total Heat Dissipation

SMA 200: 92 BTU

SMA 400: 109 BTU

Dimensions

SMA 200: 17.00 x 10.13 x 1.75 in (43.18 x 25.73 x 4.45 cm)

SMA 400: 17.00 x 10.13 x 1.75 in (43.18 x 25.73 x 4.45 cm)

Weight

SMA 200: 11 lbs (5 kg)

SMA 400: 11 lbs (5 kg)

Major Regulatory Compliance

SMA 200/400:

FCC Class A, ICES Class A, CE, C-Tick, VCCI Class A, KCC, ANATEL, BSMI, NOM, UL, cUL, TUV/GS, CB

Environment:

Temperature:

SMA 200/400: 32-105ª F, 0-40ª C

Relative Humidity:

SMA 200/400: 5-95 percent RH non-condensing

MTBF

SMA 200: 7.060 years

SMA 400: 6.870 years

2 What are the hardware specs for the SRA 4600 and SRA 1600?

Answer:

Interfaces

SRA 1600: (2) gigabit Ethernet, (2) USB, (1) console

SRA 4600: (4) gigabit Ethernet, (2) USB, (1) console

Processors

SRA 1600: 1.66 GHz Intel Atom Processor, x86

SRA 4600: 1.66 GHz Intel Atom Dual Core Processor, x86

Memory (RAM)

SRA 1600: 1 GB

SRA 4600: 2 GB

Flash Memory

SRA 1600: 1 GB

SRA 4600: 1 GB

Power Supply

SRA 1600: Internal, 100-240Vac, 50-60Mhz

SRA 4600: Internal, 100-240Vac, 50-60Mhz

Max Power Consumption

SRA 1600: 47 W

SRA 4600: 50 W

Total Heat Dissipation

SRA 1600: 158 BTU

SRA 4600: 171 BTU

Dimensions

SRA 1600: 17.00 x 10.13 x 1.75 in (43.18 x 25.73 x 4.45 cm)

SRA 4600: 17.00 x 10.13 x 1.75 in (43.18 x 25.73 x 4.45 cm)

Weight

SRA 1600: 9.5 lbs (4.3 kg)

SRA 4600: 9.5 lbs (4.3 kg)

Major Regulatory Compliance

SRA 1600/4600:

FCC Class A, EMI/EMC, FCC, CE, VCCI Class A, UL, cUL, TUV/GS, CB

Environment:

Temperature:

SRA 1600/4600: 32-105ª F, 0-40ª C

Relative Humidity:

SRA 1600/4600: 5-95 percent RH non-condensing

MTBF

SRA 1600: 18.3 years

SRA 4600: 17.8 years

3 What are the SMA 500v Virtual Appliance virtualized environment requirements?

Hypervisor: VMWare ESXi (version 5.0 and newer)

Appliance size (on disk): 2 GB

Allocated memory: 2 GB

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

4 Do the SMA/SRA appliances have hardware-based SSL acceleration onboard?

Answer: The SRA 4600 and SRA 1600 do not have a hardware-based SSL accelerator processor, however, the SMA 400/200 processor includes AES NI instructions to accelerate AES encryption.

5 What operating system do the SMA/SRA appliances run?

Answer: The appliance runs SonicWall Inc.'s own hardened Linux distribution.

6 Can I put multiple SMA/SRA 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.

7 What are the maximum number of connections allowed on the different SMA/SRA appliances?

Reference the SMA/SRA Max Count Table:

SMA/SRA Max Count Table

Type	Max Supported on SMA 200	Max Supported on SMA 400	Max Supported on SRA 1600	Max Supported on SRA 4600	Max Supported on SMA 500v Virtual Appliance
Portal entries	32	64	32	64	64
Domain entries	32	64	32	64	64
Group entries	512	512	512	512	512
User entries	1,000	2,000	1,000	2,000	2,000
NetExtender global client routes	100	100	100	100	100
NetExtender group client routes	100	100	100	100	100

SMA/SRA Max Count Table (Continued)

Type	Max Supported on SMA 200	Max Supported on SMA 400	Max Supported on SRA 1600	Max Supported on SRA 4600	Max Supported on SMA 500v Virtual Appliance
NetExtender user client routes	100	100	100	100	100
Maximum concurrent users	200	1024	200	1024	1024
Maximum concurrent Nx connections	50	500	100	500	500
Route entries	32	32	32	32	32
Host entries	32	32	32	32	32
Bookmark entries	500	500	500	500	500
User Policy entries	64	64	64	64	64
Group Policy entries	64	64	64	64	64
Global Policy entries	64	64	64	64	64
Policy address entries	32	32	32	32	32
Network Objects	128	128	128	128	128
'Address' Network Objects	32	32	32	32	32
'Network' Network Objects	64	64	64	64	64
'Service' Network Objects	64	64	64	64	64
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

Digital Certificates and Certificate Authorities FAQ

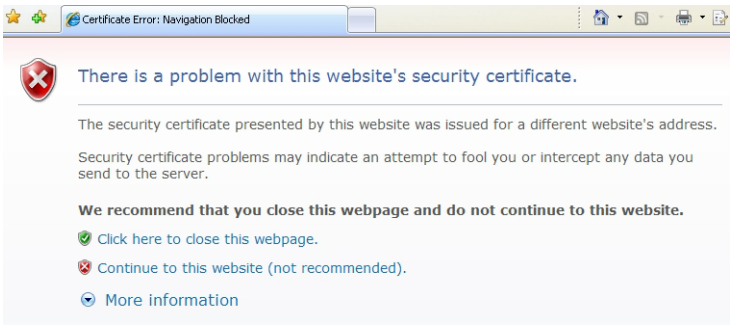
1 What do I do if when I log in to the SMA/SRA appliance my browser gives me an error, or if my Java components give me an error?

Answer: These errors can be caused by any combination of the following three factors:

- The certificate in the SMA/SRA appliance is not trusted by the browser
- The certificate in the SMA/SRA appliance could 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 previous 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 appears every time a Web browser connects to the SMA/SRA 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 should purchase and install a trusted SSL certificate onto the SMA/SRA appliance.

2 I get the following message when I log in to my SMA/SRA appliance – what do I do?

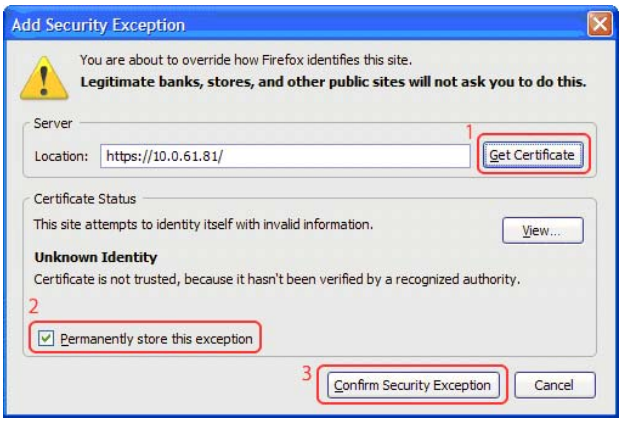


Answer: It's the same problem as noted in the previous topic, but this is the new "improved" security warning screen in Microsoft Internet Explorer. Whereas before IE5.x and IE6.x presented a pop-up that listed the reasons why the certificate is not trusted, IE simply returns a generic error page which recommends that the user close the page. The user is not presented with a direct 'Yes' option to proceed, and instead has to click on the embedded **Continue to this Website (not recommended)** link. For these reasons, it is strongly recommended that all SMA/SRA appliances, going forward, have a trusted digital certificate installed.

3 I get the following message when I log in to my SMA/SRA appliance using Firefox– what do I do?

Answer: Much like the errors shown previously for Internet Explorer, Firefox has a unique error message when any certificate problem is detected. The conditions for this error are the same as for the previous Internet Explorer errors.

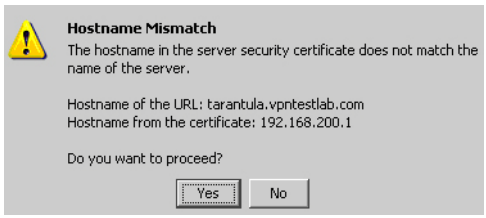
To get past this screen, click the **Or you can add an exception** link at the bottom, then click **Add Exception** that appears. In the Add Security Exception window that opens, click **Get Certificate**, ensure that **Permanently store this exception** is checked, and finally, click **Confirm Security Exception**. See the following:



To avoid this inconvenience, it is strongly recommended that all SMA/SRA 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 SMA/SRA appliance during the SSL handshake process. This error can be safely ignored.



5 Do I have to purchase a SSL certificate?

Answer: Although the level of encryption is not compromised, users accepting an untrusted certificate introduces the risk of Man-in-the-Middle attacks. SonicWall Inc. recommends installing only trusted certificates or installing the default self-signed certificate in all the clients.

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 SMA/SRA appliance?

Answer: Any CA certificate should work if the certificate is in X509v3 format, including Verisign, Thawte, Baltimore, RSA, and so on.

9 Does the SMA/SRA appliance support chained certificates?

Answer: Yes, it does. On the **System > Certificates** page, complete 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** 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 SMA/SRA 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 connect to the SMA/SRA 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 should install the Microsoft CA's root certificate into all Web browsers that 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 fails.

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. After this is done, you can successfully activate the certificate on the SMA/SRA appliance.

14 Can I have more than one certificate active if I have multiple virtual hosts?

Answer: 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 SMA/SRA 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 Does the SMA/SRA 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%
- Support for Microsoft CA Subject Names where CN=<Full user name>, for example CN=John Doe. Client certificate authentication attempts for users in Active Directory domains should 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 through file import or periodic import through 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 SMA/SRA appliance.

18 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 SMA/SRA appliance must be rebooted before it is used for client authentication. Failures to validate the client certificate also causes 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. See the following supported platforms:

Mac Requirements:

- Mac OS X 10.6.8+
- Apple Java 1.6.0_10+ (can be installed/upgraded by going to **Apple Menu > Software Update**; should be pre-installed on OS X 10.6.8+)

Linux Requirements:

- i386-compatible distribution of Linux
- Sun Java 1.6.0_10+
- Fedora 14+
- Suse: Tested successfully on 10.3
- Ubuntu 11.04+

Separate NetExtender installation packages are also downloadable from MySonicWall.com for each release.

2 Which versions of Windows does NetExtender support?

Answer: NetExtender supports:

- Vista SP2
- Windows 10
- Windows 7

3 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.

4 Can NetExtender run as a Windows service?

Answer: NetExtender can be installed and configured to run as a Windows service that allows systems to log in to domains across the NetExtender client.

5 What range do I use for NetExtender IP client address range?

Answer: This range is the pool that incoming NetExtender clients are assigned – NetExtender clients actually appear as though they are on the internal network – much like the Virtual Adapter capability found in SonicWall Inc.'s Global VPN Client. You should 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 SMA/SRA 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. You can also assign NetExtender IPs dynamically using the DHCP option.

6 What do I enter for NetExtender client routes?

Answer: These are the networks that are sent to remote NetExtender clients and should contain all networks that you wish to give your NetExtender clients access to. For example, if your SMA/SRA appliance was in one-port mode, attached to a SonicWall Inc. NSA 3500 appliance on a DMZ using 192.168.200.0/24 as the subnet for that DMZ, and the SonicWall Inc. 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.

7 What does the 'Tunnel All Mode' option do?

Answer: Activating this feature causes the SMA/SRA appliance to push down two default routes that tell the active NetExtender client to send all traffic through the SMA/SRA appliance. This feature is useful in environments where the SMA/SRA appliance is deployed in tandem with a SonicWall Inc. security

appliance running all UTM services, as it allows you to scan all incoming and outgoing NetExtender user traffic for viruses, spyware, intrusion attempts, and content filtering.

8 Is there any way to see what routes the SMA/SRA appliance 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.

9 After 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 removes 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.

10 How do I get new versions of NetExtender?

Answer: New versions of NetExtender are included in each SonicWall Inc. Secure Mobile Access firmware release and have version control information contained within. If the SMA/SRA appliance has been upgraded with new software, and a connection is made from a system using a previous, older version of NetExtender, it is automatically 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.

11 How is NetExtender different from a traditional IPSec VPN client, such as SonicWall Inc.'s Global VPN Client (GVC)?

Answer: NetExtender is designed as an extremely lightweight client that is installed through a Web browser connection, and utilizes the security transforms of the browser to create a secure, encrypted tunnel between the client and the SMA/SRA appliance.

12 Is NetExtender encrypted?

Answer: Yes, it uses whatever cipher the NetExtender client and SMA/SRA appliance negotiate during the SSL connection.

13 Is there a way to secure clear text traffic between the SMA/SRA appliance and the server?

Answer: Yes, you can configure the Microsoft Terminal Server to use encrypted RDP-based sessions, and use HTTPS reverse proxy.

14 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.

15 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.

16 Does performance change when using NetExtender instead of proxy?

Answer: Yes. NetExtender connections put minimal load on the SMA/SRA appliances, whereas many proxy-based connections might put substantial strain on the SMA/SRA appliance. Note that HTTP proxy connections use compression to reduce the load and increase performance. Content received by Secure Mobile Access from the local Web server is compressed using gzip before sending it over the Internet to the remote client. Compressing content sent from the SMA/SRA saves bandwidth and results in higher throughput. Furthermore, only compressed content is cached, saving nearly 40-50 percent of the

required memory. Note that gzip compression is not available on the local (clear text side) of the SMA/SRA appliance, or for HTTPS requests from the remote client.

17 The SMA/SRA appliance 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, RDP5, Telnet, and SSHv2. Application Offloading can also be used for Web applications. In this way, the SMA/SRA appliance functions similar to an SSL off loader and proxies Web applications pages without the need for URL rewriting.

18 Why is it required that an ActiveX component be installed?

Answer: NetExtender is installed through an ActiveX-based plug-in from Internet Explorer. Users using Firefox browsers can install NetExtender through an XPI installer. NetExtender can also be installed through an MSI installer. Download the NetExtender MSI installer from MySonicWall.com.

19 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.

20 Does NetExtender work with the 64-bit version of Microsoft Windows?

Answer: Yes, NetExtender supports 64-bit Windows 7 and Vista.

21 Does NetExtender work 32-bit and 64-bit version of Microsoft Windows 7?

Answer: Yes, NetExtender supports 32-bit and 64-bit Windows 7.

22 Does NetExtender support client-side certificates?

Answer: Yes, Windows NetExtender client supports client certificate authentication from the stand-alone client. Users can also authenticate to the Secure Mobile Access portal and then launch NetExtender.

23 My firewall is dropping NetExtender connections from my SonicWall SMA/SRA 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 SMA/SRA appliance.

General FAQ

1 Is the SMA/SRA 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, Citrix, SSHv2, SSHv2, and Telnet use browser-delivered HTML5 clients. NetExtender on Windows uses a browser-delivered client.

2 What browser and version do I need to successfully connect to the SMA/SRA appliance?

Answer: Currently supported browsers and versions are listed in the Browser Requirements section of this document.

3 What needs to be activated on the browser for me to successfully connect to the SMA/SRA appliance?

Answer:

- TLS
- Enable cookies
- Enable pop-ups for the site
- Enable Java

- Enable Javascript
- Enable ActiveX

4 What version of Java do I need?

Answer: You should install SUN's JRE 1.6.0_10 or higher (available at http://www.java.com) to use some of the features on the SMA/SRA appliance. On Google Chrome, you need Java 1.6.0 update 10 or higher.

5 What operating systems are supported?

Answer:

- Microsoft Vista
- Microsoft Windows 7
- Apple OSX 10.6.8 and newer
- Linux kernel 2.6.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 SMA/SRA 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, for example \\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 disables access to the DFS file shares from other domains. The SMA/SRA appliance is not a domain member and is not 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 SMA/SRA appliance have an SPI firewall?

Answer: No. It must be combined with a SonicWall Inc. security appliance or other third-party firewall/VPN device.

8 Can I access the SMA/SRA appliance using HTTP?

Answer: No, it requires HTTPS. HTTP connections are immediately redirected to HTTPS. You might wish to open both 80 and 443, as many people forget to type https: and instead type http://. If you block 80, it is not redirected.

9 What is the most common deployment of the SMA/SRA 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 Inc. security appliance, such as a SonicWall Inc. TZ or NSA appliance.

10 Why is it recommended to install the SMA/SRA appliance in one-port mode with a SonicWall Inc. security appliance?

Answer: This method of deployment offers additional layers of security control plus the ability to use SonicWall Inc.'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 might not have an available third interface, or a device where integrating the SMA/SRA appliance might be difficult or impossible.

12 Can I cascade multiple SMA/SRA appliances to support more concurrent connections?

Answer: No, this is not supported.

13 Why can't I log in to the Secure Mobile Access management interface of the SMA/SRA appliance?

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 in to the SMA/SRA 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 SMA/SRA appliance?

Answer: No, it is only a client-access appliance. If you require this, you need a SonicWall Inc. TZ, NSA. or SuperMassive series security appliance.

15 Can the SonicWall Inc. Global VPN Client (or any other third-party VPN client) connect to the SMA/SRA appliance?

Answer: No, only NetExtender and proxy sessions are supported.

16 Can I connect to the SMA/SRA appliance over a modem connection?

Answer: Yes, although performance is slow, even over a 56K connection it is usable.

17 What SSL ciphers are supported by the SMA/SRA appliance?

Answer: Starting with 7.5 firmware or newer, SonicWall Inc. only uses HIGH security ciphers with TLSv1, TLSv1.1, and TLSv1.2. In 8.0 firmware or newer, SSL Perfect Forward Secrecy (PFS) is supported.

18 Is AES supported in the SMA/SRA appliance?

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 might see better performance as NetExtender uses multiplexed PPP connections and runs compression over the connections to improve performance.

20 Is Two-factor authentication (RSA SecurID, etc) supported?

Answer: Yes, this is supported.

21 Does the SMA/SRA 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 supported beginning in the 5.0 release. MIBs can be downloaded from MySonicWall.

25 Does the SMA/SRA appliance have a Command Line Interface (CLI)?

Answer: Yes, the SMA/SRA appliances have a simple CLI when connected to the console port. The SMA 500v Virtual Appliance is also configurable with the CLI. The Secure Mobile Access CLI allows configuration of only the X0 interface on the SMA/SRA appliances or SMA 500v Virtual Appliance.

26 Can I Telnet or SSH into the SMA/SRA appliance?

Answer: No, neither Telnet or SSH are supported in the current release of the SMA/SRA appliance software as a means of management (this is not to be confused with the Telnet and SSH proxies that the appliance does support).

27 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.

28 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 **Logout**. If you close the Web browser using any other means, the Web cache cleaner cannot run.

29 What does the 'encrypt settings file' check box do?

Answer: This setting encrypts 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 SMA/SRA 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.

30 What does the 'store settings' button do?

Answer: By default, the settings are automatically stored on a SMA/SRA 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 are lost. This feature is most useful when you are unsure of making a change that could 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 returns to the previous state before the change was made.

31 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 Inc. strongly recommends creating system backup right before loading new software, or making significant changes to the programming of the appliance.

32 What is 'SafeMode'?

Answer: SafeMode is a feature of the SMA/SRA 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 boots into a special interface mode that allows the administrator to choose which version to boot, or load a new version of the software image.

33 How do I access the SafeMode menu?

Answer: In emergency situations, you can access the SafeMode menu by holding in **Reset** on the SMA/SRA appliance (the small pinhole button located on the front of the SMA/SRA appliances) for 12-14 seconds until the 'Test' LED begins quickly flashing yellow. After the SMA/SRA appliance 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 SMA/SRA 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 are able to boot the appliance using a previously saved backup snapshot, or you can upload a new version of software with **Upload New Software image**.

34 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.

35 What authentication methods are supported?

Answer: Local database, RADIUS, Active Directory, and LDAP.

36 I configured my SMA/SRA 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 fails. Ensure that the SMA/SRA appliance and the Active Directory server are both using NTP to keep their internal clocks synchronized.

37 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 should change the directory listing style to 'UNIX' instead of 'MS-DOS'.

38 Where can I get a VNC client?

Answer: SonicWall Inc. has done extensive testing with RealVNC. It can be downloaded at:

http://www.realvnc.com/download.html

39 Are the SRA 4600/1600 appliances fully supported by GMS or Analyzer?

Answer: Yes.

40 Does the SMA/SRA 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 might need to install the correct printer driver software on the Terminal Server you are accessing.

41 Can I integrate the SMA/SRA appliance with wireless?

Answer: Yes, refer to the *SonicWall Inc. Secure Wireless Networks Integrated Solutions Guide*, available through Elsevier, http://www.elsevierdirect.com/.

42 Can I manage the appliance on any interface IP address of the SMA/SRA appliance?

Answer: Yes, you can manage on any of the interface IP addresses.

43 Can I allow only certain Active Directory users access to log in to the SMA/SRA 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.

44 Does the HTTP(S) proxy support the full version of Outlook Web Access (OWA Premium)?

Answer: Yes.

45 Why are my RDP sessions dropping frequently?

Answer: Try adjusting the session and connection timeouts on both the SMA/SRA appliance and any appliance that sits between the endpoint client and the destination server. If the SMA/SRA appliance is behind a firewall, adjust the TCP timeout upwards and enable fragmentation.

46 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 could be supported in a future software release.

47 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.

48 What port is the SMA/SRA appliance using for the Radius traffic?

Answer: It uses port 1812.

49 Do the SMA/SRA appliances support the ability for the same user account to login simultaneously?

Answer: Yes. 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.

50 Does the SMA/SRA appliance support NT LAN Manager (NTLM) Authentication?

Answer: No.

51 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 SMA/SRA that currently supports only basic and digest authentication schemes. Contact the administrator for further assistance.' - why?

Answer: In SRA 3.5 and earlier releases, the HTTP proxy does not support Windows Authentication (formerly called NTLM). Only basic authentication is supported.

52 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 SMA/SRA appliance.

53 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.

54 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/.

55 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.

56 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:

- XenApp 7.6 (HTML5 and ActiveX only)
- XenApp 6.5
- XenApp 6.0
- XenApp 5.0

Clients:

- Receiver for Windows 4.2, 4.1, or 4.0
- Receiver for Java 10.1.006
- XenApp Web Plugiin version 14.2, 14.1, 14.0

For browsers requiring Java to run Citrix, you must have Sun Java 1.6.0_10 or higher.

57 What applications are supported using Application Offloading?

Answer: Application Offloading should support any application using HTTP/HTTPS. SMA/SRA has limited support for applications using Web services and no support for non-HTTP protocols wrapped within HTTP.

One key aspect to consider when using Application Offloading is that the application should not contain hard-coded self-referencing URLs. If these are present, the Application Offloading proxy rewrites the

URLs. Because Web site development does not usually conform to HTML standards, the proxy can only do a best-effort translation when rewriting these URLs. Specifying hard-coded, self-referencing URLs is not recommended when developing a Web site because content developers must modify the Web pages whenever the hosting server is moved to a different IP or hostname.

For example, if the backend application has a hard-coded IP and scheme within URLs as follows, then Application Off-loading needs to rewrite this URL.

<a href="http://1.1.1.1/doAction.cgi?test=foo">

This can be done by enabling the **Enable URL Rewriting for self-referenced URLs** setting for the Application Off-loading Portal, but all the URLs might not be rewritten, depending on how the Web application has been developed. (This limitation is usually the same for other WAF/SMA vendors employing reverse proxy mode.)

58 Is SSHv2 supported?

Answer: Yes, this is supported.

59 Should I create a Global Deny ALL policy?

Answer: Yes, SonicWall Inc. recommends that administrators set up a Global Deny ALL policy that allows access to only trusted hosts. This prevents outbound requests to malicious hosts from Secure Mobile Access. For more information on how to set up a Global Deny ALL policy, see Adding a Policy on page 234.

G

Using the Command Line Interface

The Command Line Interface (CLI) is a text-only mechanism for interacting with a computer operating system or software by typing commands to complete specific tasks. It is a critical part of the deployment of the SMA 500v Virtual Appliance, where basic networking needs to be configured from the console. The CLI is also supported on the SRA 4600 and 1600 appliances.

While the SMA/SRA physical appliance products have a default IP address and network configuration that requires a client's network settings to be reconfigured to connect, the network settings in an existing VMware virtual environment might conflict with the SMA/SRA appliance defaults. The CLI utility remedies this by allowing basic configuration of the network settings when deploying the Virtual Appliance.

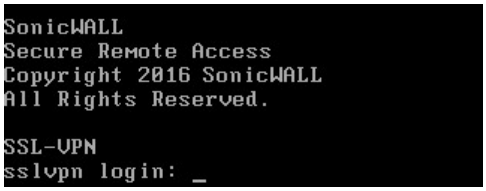
NOTE: The SonicWall Inc. Secure Mobile Access CLI allows configuration of only the X0 interface on the SRA 4600/1600 or SMA 500v Virtual Appliance.

NOTE: To use the CLI on a serial connection or in an SSH management session, you need to use a terminal emulation application (such as Tera Term) or an SSH Client application (such as PuTTY). You can find suitable, free terminal emulators on the Internet.

For the SMA/SRA physical appliances, console access is achieved by connecting a computer to the serial port. Use the following settings:

- Baud: 115200
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- No flow control

For the Virtual Appliance, the following login prompt is displayed after the firmware has fully booted:



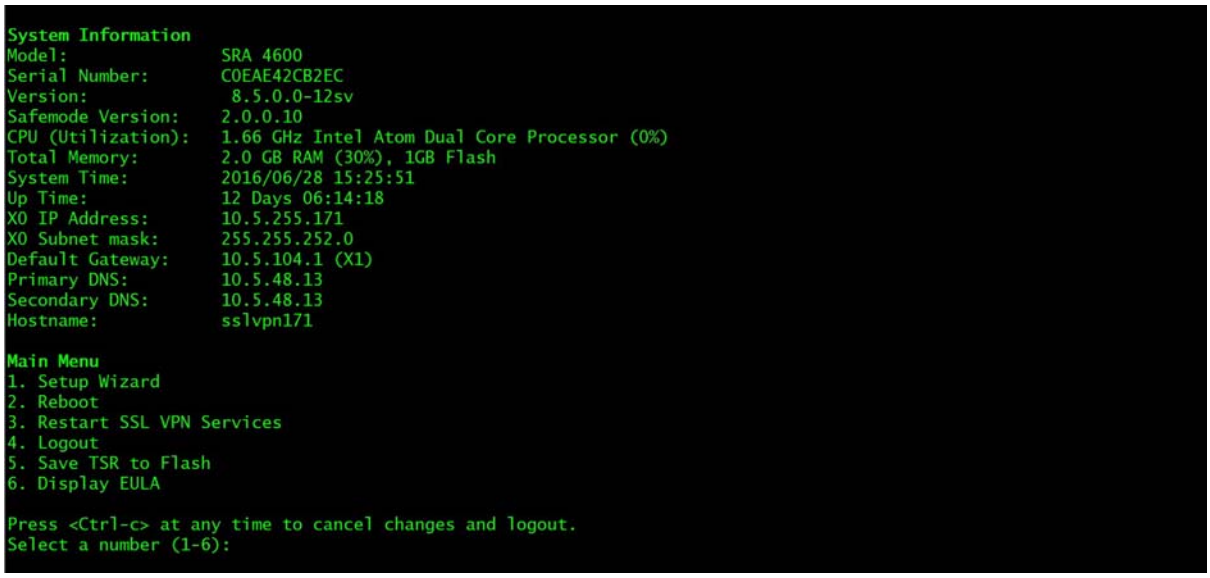
In the following examples, user input is highlighted in bold to indicate text entered by the user.

To access the CLI, login as **admin**. The password is the same as the password for the admin account that is configured on the appliance. The default is **password**.

```
sslvpn login: admin
Password: password
```

If the incorrect password is entered, the login prompt is displayed again. If the correct password is entered, the CLI is launched.

For hardware and Virtual Appliances, basic system information and network settings are displayed along with the main menu, as in the following example:



You can press **Ctrl-C** at any time to log out and exit the CLI, returning to the login prompt.

The main menu has four selections:

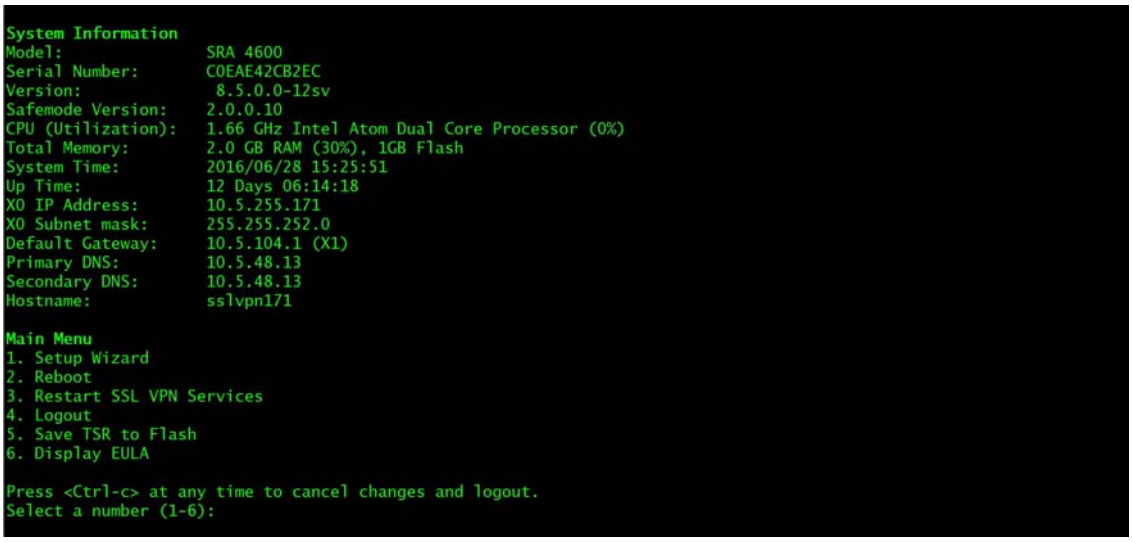
1 **Setup Wizard** – This option launches a simple wizard to change the basic network settings, starting with the X0 IP Address, X0 subnet mask, default gateway, primary and secondary DNS, and the hostname. The following CLI output illustrates an example where each field is changed:

```
X0 IP Address (default 192.168.200.1): 192.168.200.201
X0 Subnet Mask (default 255.255.255.0): 255.255.0.0
Default Gateway (default 192.168.200.2): 192.168.200.1
Primary DNS: 10.50.128.52
Secondary DNS (optional, enter "none" to disable): 4.2.2.2
Hostname (default sslvpn): sslvpn

New Network Settings:
X0 IP Address:       192.168.200.201
X0 Subnet mask:      255.255.0.0
Default Gateway:     192.168.200.1
Primary DNS:         10.50.128.52
Secondary DNS:       4.2.2.2
Hostname:            sslvpn

Would you like to save these changes (y/n)?
```

If a field is not filled out, the prior value is retained, allowing you to change only a single field. After each field has been prompted, the new network settings are shown and a confirmation message is given for the user to review and verify the changes before applying them. The following shows the result when you save the changes:

```
Would you like to save these changes (y/n)? y
Saving changes...please wait....
Changes saved!
Press <Enter> to continue...
```

After saving the changes, press **Enter** to return to the original display of the System Information and Network Settings and verify that the changes have taken effect:



If no changes are saved, the following message is displayed and pressing Enter returns to the initial display of the System Information and Network Settings:

```
No changes have been made.
Press <Enter> to continue...
```

NOTE: When applying settings that change the IP address, there might be a delay of up to five seconds as the interface settings are updated.

2 **Reboot** – Selecting this option displays a confirmation prompt and then reboots:

```
Reboot
Are you sure you want to reboot (y/n)?
```

3 **Restart SSL-VPN Services** – This option displays a confirmation prompt and then restarts the Web server and the related Secure Mobile Access daemon services. This command is equivalent to issuing the **EasyAccessCtrl restart** command.

```
Restart SSL-VPN Services
Are you sure you want to restart the SSL-VPN services (y/n)? y

Restarting SSL-VPN services...please wait.
Stopping SMM: [  OK  ]
Stopping Firebase :[  OK  ]
Stopping FTP Session:[  OK  ]
Stopping HTTPD: [  OK  ]
Cleaning Apache State: [  OK  ]
Stopping Graphd :[  OK  ]

Cleaning Temporary files........
Starting SMM: [  OK  ]
Starting firebase: [  OK  ]
Starting httpd: [  OK  ]
Starting ftpsession: [  OK  ]
Starting graphd: [  OK  ]

Restart completed...returning to main menu...
```

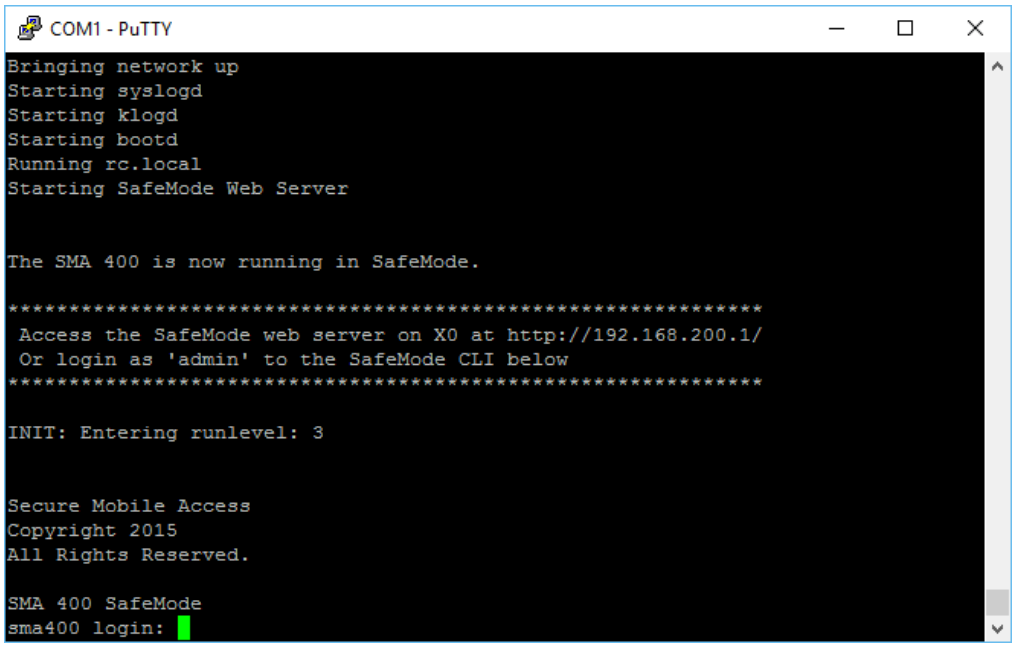
4 **Logout** – The logout option ends the CLI session and returns to the login prompt.

SafeMode

SafeMode is a limited Web management interface that provides a way to upload firmware from your computer and reboot the appliance.

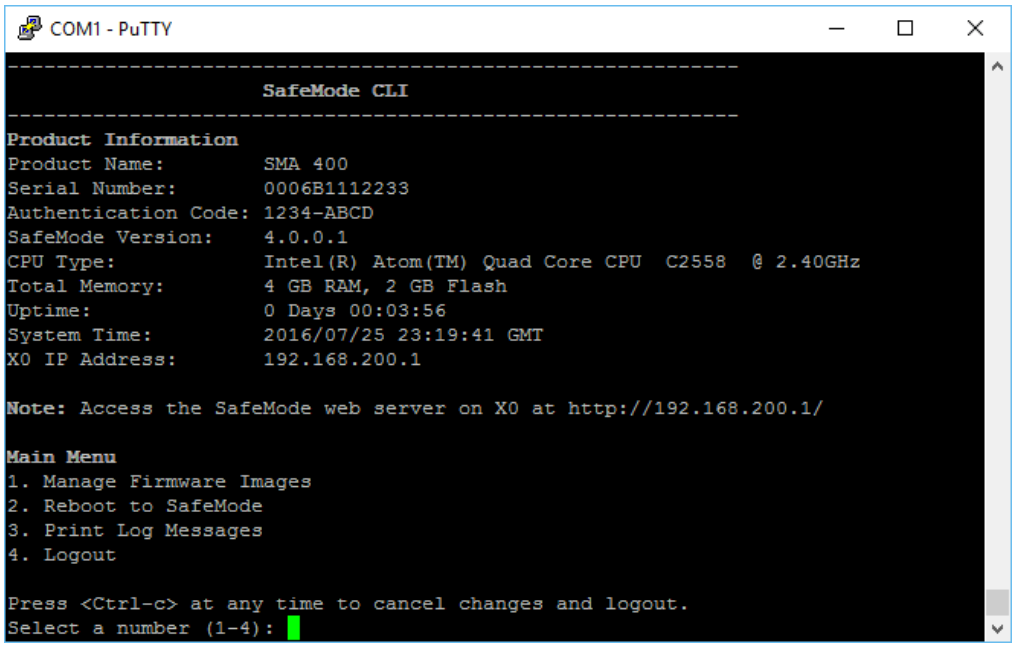
The SafeMode feature allows you to recover quickly from uncertain configuration states with a simplified management interface that includes the same settings available on the **System > Settings** page.

You can get to the SafeMode CLI, by pressing the SafeMode switch to reboot to SafeMode, and then logging in as **admin**. The password is the same as the password for the admin account that is configured on the appliance. The default is **password**.

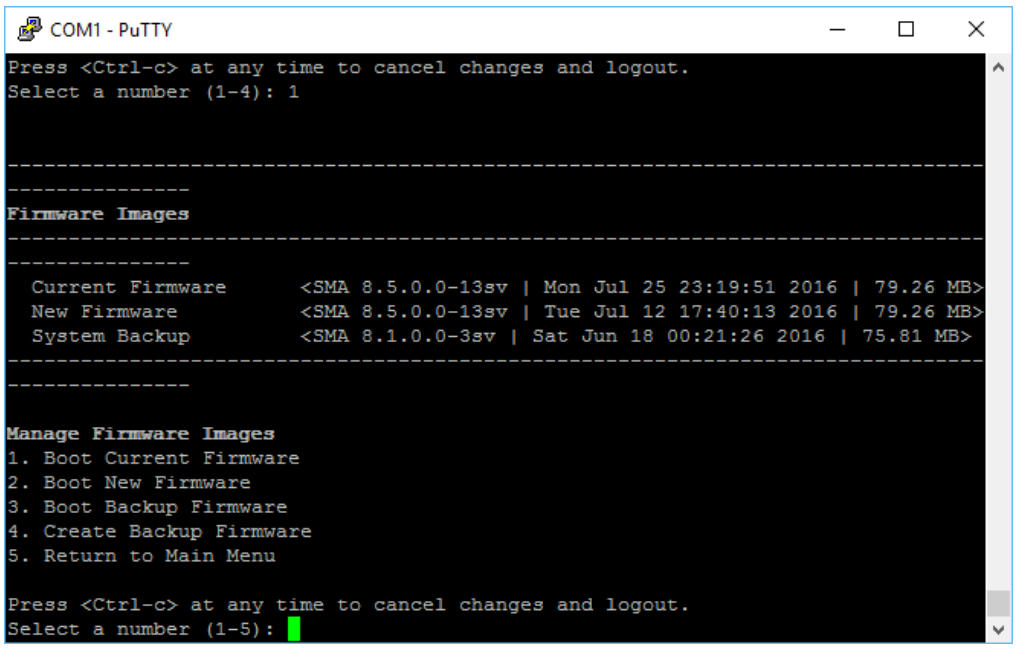



```
sma400 login: admin
Password: password
```

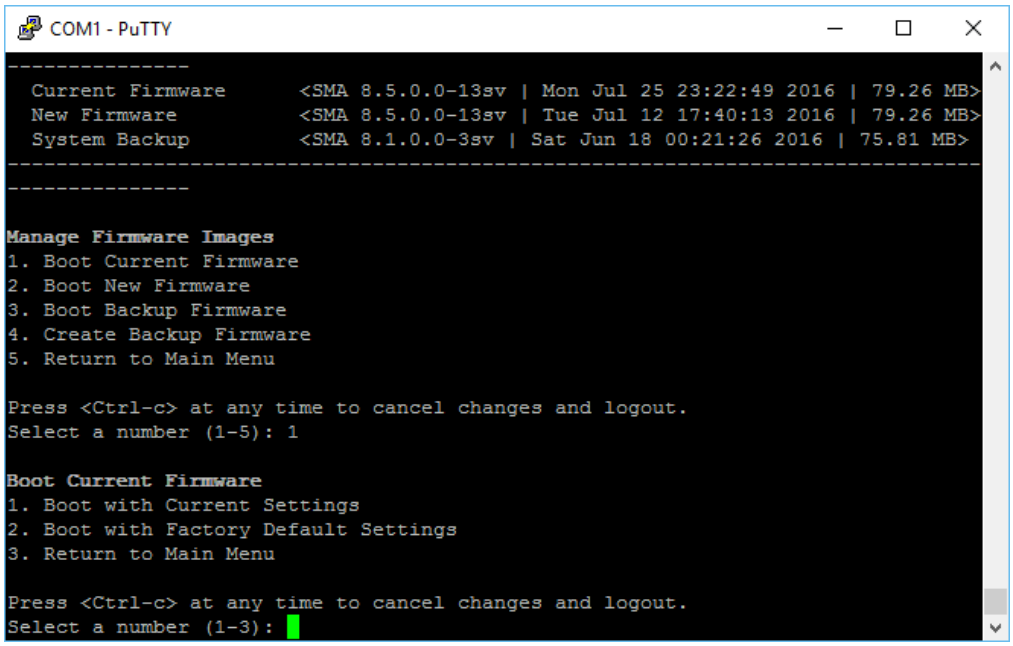
When an incorrect password is entered, the login prompt is displayed again. When the correct password is entered, the SafeMode CLI is launched.



The numbered options explain themselves. Select the number of the option you would like to perform. For the first option, to Manage Firmware Images, press 1. The following screen appears with five additional options.



The five additional options explain themselves. Select the number of the option you would like to perform. For the first option, to Boot Current Firmware, press 1. The following screen appears with three additional options.



The three additional options explain themselves. Select the number of the option you would like to perform.

For more instructions on how to restart your firewall in SafeMode, refer to the *Getting Started Guide* for your particular appliance.

H

Using 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 following list, 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 can vary. You might need additional service or information from your provider before using SMS. Contact the SMS provider directly to verify these formats and for further information on SMS services, options, and capabilities.

SMS formats based on carrier

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
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

SMS formats based on carrier (Continued)

Carrier	SMS Format
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
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

SMS formats based on carrier (Continued)

Carrier	SMS Format
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
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

SMS formats based on carrier (Continued)

Carrier	SMS Format
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
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

SMS formats based on carrier (Continued)

Carrier	SMS Format
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
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

Support Information

This appendix contains the following sections:

GNU General Public License (GPL) Source Code

SonicWall Inc. provides a machine-readable copy of the GPL open source on a CD. To obtain a complete machine-readable copy, send your written request, along with a certified check or money order in the amount of US $25.00 payable to “SonicWall, Inc.” to:

General Public License Source Code Request
SonicWall, Inc. Attn: Jennifer Anderson

5455 Great America Parkway
Santa Clara, CA 95054

Limited Hardware Warranty

All SonicWall Inc. appliances come with a 1-year Limited Hardware Warranty which provides delivery of critical replacement parts for defective parts under warranty. Visit the Warranty Information page for details on your product’s warranty:
https://support.sonicwall.com/essentials/support-offerings

SonicWall Inc., 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 Inc.), and continuing for a period of twelve (12) months, that the product is 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 Inc. 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 Inc.'s discretion, the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWall Inc.'s obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWall Inc.'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 Inc..

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE

EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

DISCLAIMER OF LIABILITY. SonicWall'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SonicWall OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SonicWall OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWall or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

End User License Agreement

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

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

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

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

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

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

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

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

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

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

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

2 **Software License**.

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

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

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

d **MSP License.**

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

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

e **Evaluation/Beta License.** If Software is obtained from Provider for evaluation purposes or in beta form, Customer shall be granted a License to use such Software and the associated Documentation solely for Customer's own non-production, internal evaluation purposes (an ***"Evaluation License"***). Each Evaluation License shall be granted for an evaluation period of up to thirty (30) days beginning (i) five (5) days after the Appliance is shipped or (ii) from the date that access is granted to the beta Software or the SaaS Software, plus any extensions granted by

Provider in writing (the “Evaluation Period”). There is no fee for an Evaluation License during the Evaluation Period, however, Customer is responsible for any applicable shipping charges or taxes which may be incurred, and any fees which may be associated with usage beyond the scope permitted herein. Beta Software licensed hereunder may include pre-release features and capabilities which may not be available in SonicWall’s generally available commercial versions of the Software. SonicWall retains the right during the term to modify, revise, or remove SonicWall beta software from Customer's premises. Customer acknowledges that SonicWall owns all modifications, derivative works, changes, expansions or improvements to beta software, as well as all reports, testing data or results, feedback, benchmarking or other analysis completed in whole or in part in conjunction with usage of beta software. NOTWITHSTANDING ANYTHING OTHERWISE SET FORTH IN THIS AGREEMENT, CUSTOMER UNDERSTANDS AND AGREES THAT EVALUATION AND BETA SOFTWARE IS PROVIDED “AS IS”, WHERE IS, WITH ALL FAULTS AND THAT SONICWALL DOES NOT PROVIDE A WARRANTY OR MAINTENANCE SERVICES FOR EVALUATION OR BETA LICENSES, AND SONICWALL BEARS NO LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES RESULTING FROM USE (OR ATTEMPTED USE) OF THE EVALUATION OR BETA SOFTWARE THROUGH AND AFTER THE EVALUATION PERIOD AND HAS NO DUTY TO PROVIDE SUPPORT TO CUSTOMER FOR SUCH SOFTWARE. BETA SOFTWARE MAY CONTAIN DEFECTS AND A PRIMARY PURPOSE OF LICENSING THE BETA SOFTWARE IS TO OBTAIN FEEDBACK ON THE SOFTWARE’S PERFORMANCE AND THE IDENTIFICATION OF DEFECTS. CUSTOMER IS ADVISED TO SAFEGUARD IMPORTANT DATA, TO USE CAUTION AND NOT TO RELY IN ANY WAY ON THE CORRECT FUNCTIONING OR PERFORMANCE OF THE BETA SOFTWARE AND/OR ACCOMPANYING MATERIALS.

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

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

access devices not provided by Provider, including but not limited to “pirate keys”, to install or access the Software.

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

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

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

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

8 **Termination.**

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

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

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

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

10 **Maintenance Services.**

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

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

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

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

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

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

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

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

b **Maintenance Period.** The first period for which Customer is entitled to receive Maintenance Services begins on the date of the registration of the Product at Provider's registration portal (the "**Registration**") and ends twelve (12) months thereafter (the ***"Initial Maintenance Period"***). Following the Initial Maintenance Period, Maintenance Services for the Product(s) may then be renewed for additional terms of twelve (12) or more months (each, a ***"Renewal Maintenance***

Period") For purposes of this Agreement, the Initial Maintenance Period and each Renewal Maintenance Period shall be considered a ***"Maintenance* Period."** For the avoidance of doubt, this Agreement shall apply to each Renewal Maintenance Period. Cancellation of Maintenance Services will not terminate Customer's rights to continue to otherwise use the Products. Maintenance fees shall be due in advance of each Renewal Maintenance Period and shall be subject to the payment requirements set forth in this Agreement. The procedure for reinstating Maintenance Services for the Products after it has lapsed is posted at https://support.sonicwall.com/essentials/support-guide. Maintenance Services are optional and only provided if purchased separately.

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

11 **Warranties and Remedies.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12 **Infringement Indemnity.** Provider shall indemnify Customer from and against any claim, suit, action, or proceeding brought against Customer by a third party to the extent it is based on an allegation that the Software directly infringes any patent, copyright, trademark, or other proprietary right enforceable in the country in which Provider has authorized Customer to use the Software, including, but not limited to the country to which the Software is delivered to Customer, or misappropriates a trade secret in such country (a ***"Claim"***). Indemnification for a Claim shall consist of the following: Provider shall (a) defend or settle the Claim at its own expense, (b) pay any judgments finally awarded against Customer under a Claim or any amounts assessed against Customer in any settlements of a Claim, and (c) reimburse Customer for the reasonable administrative costs or expenses, including without limitation reasonable attorneys' fees, it necessarily incurs in responding to the Claim. Provider's obligations under this *Infringement Indemnity* Section are conditioned upon Customer (i) giving prompt written notice of the Claim to Provider, (ii) permitting Provider to retain sole control of the investigation, defense or settlement of the Claim, and (iii) providing Provider with cooperation and assistance as Provider may reasonably request in connection with the Claim. Provider shall have no obligation hereunder to defend Customer against any Claim (a) resulting from use of the Software other than as authorized by this Agreement, (b) resulting from a modification of the Software other than by Provider, (c) based on Customer's use of any release of the Software after Provider recommends discontinuation because of possible or actual infringement and has provided a non-infringing version at no charge, or (d) to the

extent the Claim arises from or is based on the use of the Software with other products, services, or data not supplied by Provider if the infringement would not have occurred but for such use. If, as a result of a Claim or an injunction, Customer must stop using any Software (***"Infringing Software"***), Provider shall at its expense and option either (1) obtain for Customer the right to continue using the Infringing Software, (2) replace the Infringing Software with a functionally equivalent non-infringing product, (3) modify the Infringing Software so that it is non-infringing, or (4) terminate the License for the Infringing Software and (A) for non-SaaS Software, accept the return of the Infringing Software and refund the license fee paid for the Infringing Software, pro-rated over a sixty (60) month period from the date of initial delivery of such Software, or (B) for SaaS Software, discontinue Customer's right to access and use the Infringing Software and refund the unused pro-rated portion of any license fees pre-paid by Customer for such Software. This Section states Provider's entire liability and its sole and exclusive indemnification obligations with respect to a Claim and Infringing Software.

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

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

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

14 Confidential Information.

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

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

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

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

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

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

Except as permitted herein or to the extent required by Privacy Laws or legal process, Provider shall implement reasonable technical and organizational measures to prevent unauthorized disclosure of or

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

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

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

17 **SaaS Provisions**.

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

Customer represents and warrants that it has obtained all rights, permissions and consents necessary to use and transfer all Customer and/or third party data within and outside of the country in which Customer or the applicable Customer Affiliate is located (including providing adequate disclosures and obtaining legally sufficient consents from Customer's employees, customers, agents, and contractors). If Customer transmits data to a third-party website or other

provider that is linked to or made accessible by the SaaS Software, Customer will be deemed to have given its consent to Provider enabling such transmission and Provider shall have no liability to Customer in connection with any claims by a third party in connection with such transmission.

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

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

18 **General.**

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

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

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

parties have relied on the limitations and exclusions set forth in this Agreement in determining whether to enter into it.

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

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

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

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

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

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

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

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

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

m **Entire Agreement.** This Agreement is intended by the parties as a final expression of their agreement with respect to the subject matter thereof and may not be contradicted by evidence of any prior or contemporaneous agreement unless such agreement is signed by both parties. In the absence of such an agreement, this Agreement shall constitute the complete and exclusive statement of the terms and conditions and no extrinsic evidence whatsoever may be introduced in any proceeding that may involve the Agreement. Each party acknowledges that in entering into the Agreement it has not relied on, and shall have no right or remedy in respect of, any statement, representation, assurance or warranty (whether made negligently or innocently) other than as expressly set out in the Agreement. In those jurisdictions where an original (non-faxed,

non-electronic, or non-scanned) copy of an agreement or an original (non-electronic) signature on agreements such as this Agreement is required by law or regulation, the parties hereby agree that, notwithstanding any such law or regulation, a faxed, electronic, or scanned copy of and a certified electronic signature on this Agreement shall be sufficient to create an enforceable and valid agreement. This Agreement, may only be modified or amended t by a writing executed by a duly authorized representative of each party. No other act, document, usage or custom shall be deemed to amend or modify this Agreement.

J

SonicWall Support

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

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

The Support Portal enables you to:

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

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

Glossary

A

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.

C

Common Internet File System (CIFS)

A protocol that defines a standard for remote file access, allowing users with different platforms and computers to share files without installing special software.

F

File Shares

SonicWall Inc.'s network file browsing feature on the SMA/SRA appliance. This uses the Web browser to browse shared files on the network.

L

Lightweight Directory Access Protocol (LDAP)

An Internet protocol that email and other programs use to retrieve data from a server.

O

One-time Password

A randomly-generated, single-use password. One-time Password can be used to refer to a particular instance of a password, or to the feature as a whole.

S

Simple Mail Transfer Protocol (SMTP)

A protocol for sending email messages between servers.

Secure Socket Layer Virtual Private Network (SMA/SRA)

A remote access tool that utilizes a Web browser to provide clientless access to private applications.

V

Virtual Office

The user interface of the SMA/SRA appliance.

W

Windows Internet Naming Service (WINS)

A system that determines the IP address associated with a network computer.