# SRA 7.5
# Administrator Guide

### Notes, Cautions, and Warnings

**NOTE**: A NOTE indicates important information that helps you make better use of your system.

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

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

**© 2014 Dell Inc.**

Trademarks: Dell™, the DELL logo, SonicWALL™, SonicWALL ViewPoint™, Reassembly-Free Deep Packet Inspection™, Dynamic Security for the Global Network™, SonicWALL Clean VPN™, SonicWALL Clean Wireless™, SonicWALL Global Response Intelligent Defense (GRID) Network™, SonicWALL Mobile Connect™, and all other SonicWALL product and service names and slogans are trademarks of Dell Inc.

2014 – 07 P/N 232-002273-00 Rev. B

# Table of Contents


**Chapter 1. About This Guide** . . . . . 11
Guide Conventions . . . . . 11
**Chapter 2. SRA Overview** . . . . . 13
Overview of Dell SonicWALL SRA . . . . . 13
SSL for Virtual Private Networking (VPN) . . . . . 13
SRA Virtual Appliance. . . . . 13
SRA Software Components . . . . . 14
SRA Hardware Components . . . . . 15
Concepts for Dell SonicWALL SRA. . . . . 20
Encryption Overview . . . . . 20
SSL Handshake Procedure . . . . . 20
IPv6 Support Overview . . . . . 21
Browser Requirements for the SRA Administrator . . . . . 24
Browser Requirements for the SRA End User . . . . . 24
Portals Overview . . . . . 25
Domains Overview . . . . . 25
Application Offloading and HTTP(S) Bookmarks Overview . . . . . 26
Cross Domain Single Sign-On. . . . . 30
ActiveSync Authentication . . . . . 30
Network Resources Overview . . . . . 35
SNMP Overview . . . . . 41
DNS Overview . . . . . 42
Network Routes Overview . . . . . 42
NetExtender Overview . . . . . 42
Two-Factor Authentication Overview . . . . . 46
One Time Password Overview . . . . . 49
End Point Control Overview. . . . . 51
Secure Virtual Assist Overview . . . . . 52
Secure Virtual Meeting Overview . . . . . 64
Web Application Firewall Overview. . . . . 69

Navigating the SRA Management Interface . . . . . 80
Management Interface Introduction . . . . . 81
Navigating the Management Interface . . . . . 82
Navigation Bar . . . . . 86
Deployment Guidelines . . . . . 86
Support for Numbers of User Connections . . . . . 87
Resource Type Support . . . . . 87
Integration with Dell SonicWALL Products . . . . . 87
Typical Deployment . . . . . 88
Two-armed Deployment . . . . . 88
**Chapter 3. System Configuration** . . . . . 91
System > Status . . . . . 91
System > Status Overview . . . . . 92
Registering Your SRA Appliance from System Status . . . . . 94
Configuring Network Interfaces . . . . . 96
System > Licenses . . . . . 96
System > Licenses Overview . . . . . 96
Registering the SRA Appliance from System > Licenses . . . . . 98
Activating or Upgrading Licenses . . . . . 100
System > Time . . . . . 104
System > Time Overview . . . . . 105
Setting the Time . . . . . 105
Enabling Network Time Protocol . . . . . 106
System > Settings . . . . . 106
System > Settings Overview . . . . . 106
Managing Configuration Files . . . . . 108
Managing Firmware . . . . . 110
System > Administration . . . . . 111
System > Administration Overview . . . . . 111
Configuring Login Security . . . . . 113
Configuring HTTP DOS Settings . . . . . 114
Configuring Web Management Settings . . . . . 114
Configuring SNMP Settings . . . . . 114
Enabling GMS Management . . . . . 114
System > Certificates . . . . . 115
System > Certificates Overview . . . . . 115
Certificate Management . . . . . 116
Generating a Certificate Signing Request . . . . . 117
Viewing and Editing Certificate Information . . . . . 118
Importing a Certificate . . . . . 118
Adding Additional CA Certificates . . . . . 119

System > Monitoring . . . . . 119
System > Monitoring Overview . . . . . 119
Setting The Monitoring Period . . . . . 121
Refreshing the Monitors . . . . . 121
System > Diagnostics . . . . . 121
System > Diagnostics Overview . . . . . 122
Downloading & Generating the Tech Support Report . . . . . 122
Performing Diagnostic Tests . . . . . 124
System > Restart . . . . . 126
System > Restart Overview . . . . . 126
Restarting the SRA Appliance . . . . . 126
**Chapter 4. Network Configuration** . . . . . 127
Network > Interfaces . . . . . 127
Network > Interfaces Overview . . . . . 128
Configuring Network Interfaces . . . . . 128
Network > DNS . . . . . 130
Network > DNS Overview . . . . . 130
Configuring Hostname Settings . . . . . 131
Configuring DNS Settings . . . . . 131
Configuring WINS Settings . . . . . 132
Network > Routes . . . . . 132
Network > Routes Overview . . . . . 133
Configuring a Default Route for the SRA Appliance . . . . . 133
Configuring Static Routes for the Appliance . . . . . 134
Network > Host Resolution . . . . . 135
Network > Host Resolution Overview . . . . . 135
Configuring Host Resolution . . . . . 135
Network > Network Objects . . . . . 136
Network > Network Objects Overview . . . . . 136
Adding Network Objects . . . . . 137
Editing Network Objects . . . . . 138
**Chapter 5. Portals Configuration** . . . . . 141
Portals > Portals . . . . . 141
Portals > Portals Overview . . . . . 142
Adding Portals . . . . . 143
Configuring General Portal Settings . . . . . 144
Configuring Login Schedules . . . . . 147
Configuring the Home Page . . . . . 147
Configuring Per-Portal Virtual Assist Settings . . . . . 151
Configuring Virtual Host Settings . . . . . 153
Adding a Custom Portal Logo . . . . . 154

Portals > Application Offloading . . . . . 155
Application Offloading Overview . . . . . 155
Configuring an HTTP/HTTPS Application Offloading Portal . . . . . 156
Configuring Generic SSL Offloading . . . . . 160
Portals > Domains . . . . . 162
Portals > Domains Overview . . . . . 162
Viewing the Domains Table . . . . . 163
Removing a Domain . . . . . 163
Adding or Editing a Domain . . . . . 164
Adding or Editing a Domain with Local User Authentication . . . . . 165
Adding or Editing a Domain with Active Directory Authentication . . . . . 167
Adding or Editing a Domain with LDAP Authentication . . . . . 171
Adding or Editing a Domain with NT Domain Authentication . . . . . 174
Adding or Editing a Domain with RADIUS Authentication . . . . . 175
Configuring Two-Factor Authentication . . . . . 178
Portals > Custom Logo . . . . . 187
Portals > Load Balancing . . . . . 187
Portals > Load Balancing Overview . . . . . 187
Configuring a Load Balancing Group . . . . . 189
**Chapter 6. Services Configuration** . . . . . 193
Services > Settings . . . . . 193
Services > Bookmarks . . . . . 197
Services > Policies . . . . . 209
Adding a Policy . . . . . 209
Editing a Policy . . . . . 210
Deleting a Policy . . . . . 211
**Chapter 7. NetExtender Configuration** . . . . . 213
NetExtender > Status . . . . . 214
NetExtender > Status Overview . . . . . 214
Viewing NetExtender Status . . . . . 214
NetExtender > Client Settings . . . . . 215
NetExtender > Client Settings Overview . . . . . 215
Configuring the Global NetExtender IP Address Range . . . . . 215
Configuring Global NetExtender Settings . . . . . 217
Configuring Internal Proxy Settings . . . . . 218
Configuring Post-Connection Scripts . . . . . 218
NetExtender > Client Routes . . . . . 219
NetExtender > Client Routes Overview . . . . . 220
Adding NetExtender Client Routes . . . . . 220
NetExtender > Advanced Settings . . . . . 221
NetExtender Traffic Log . . . . . 221

Post Connection Scripts . . . . . 221
NetExtender > Client Downloads . . . . . 222
NetExtender > Log . . . . . 222
NetExtender User and Group Settings . . . . . 223
Configuring User-Level NetExtender Settings . . . . . 223
Configuring Group-Level NetExtender Settings . . . . . 227
**Chapter 8. End Point Control** . . . . . 231
End Point Control > Device Profiles . . . . . 232
Users > Local Groups > Edit EPC Settings . . . . . 234
Users > Local Users > Edit EPC Settings . . . . . 237
End Point Control > Settings . . . . . 240
End Point Control > Log . . . . . 240
**Chapter 9. Secure Virtual Assist Configuration** . . . . . 243
Secure Virtual Assist > Status . . . . . 243
Secure Virtual Assist > Status . . . . . 244
Secure Virtual Assist > Settings . . . . . 244
General Settings . . . . . 245
Request Settings . . . . . 247
Notification Settings . . . . . 248
Customer Portal Settings . . . . . 249
Restriction Settings . . . . . 250
Secure Virtual Assist > Log . . . . . 251
Secure Virtual Assist > Licensing . . . . . 252
Secure Virtual Assist > Licensing Overview . . . . . 252
**Chapter 10. Secure Virtual Meeting** . . . . . 255
Secure Virtual Meeting > Status . . . . . 255
Secure Virtual Meeting > Settings . . . . . 256
General Settings . . . . . 256
Notification Settings . . . . . 257
Secure Virtual Meeting > Log . . . . . 258
Secure Virtual Meeting > Licensing . . . . . 258
Licensing Overview . . . . . 259
Licensing Information . . . . . 259
**Chapter 11. High Availability Configuration** . . . . . 261
High Availability Overview . . . . . 261
Supported Platforms . . . . . 261
Configuring High Availability . . . . . 262
Physical Connectivity . . . . . 262
Preparing for High Availability . . . . . 262
Configuring High Availability Settings on a 4200 and 4600 . . . . . 263
Configuring High Availability Settings on a Virtual Machine . . . . . 265

Enabling Interface Monitoring . . . . . 266
Configuring Network Monitoring Addresses . . . . . 267
Configuring Management Settings for Idle Unit . . . . . 267
Synchronizing Firmware . . . . . 268
Synchronizing Settings . . . . . 268
Synchronizing Licenses . . . . . 268
Technical FAQ . . . . . 269
**Chapter 12. Web Application Firewall Configuration** . . . . . 271
Licensing Web Application Firewall . . . . . 271
Configuring Web Application Firewall . . . . . 275
Viewing and Updating Web Application Firewall Status . . . . . 275
Configuring Web Application Firewall Settings . . . . . 277
Configuring Web Application Firewall Signature Actions . . . . . 287
Determining the Host Entry for Exclusions . . . . . 291
Configuring Custom Rules and Application Profiling . . . . . 293
Using Web Application Firewall Monitoring . . . . . 311
Using Web Application Firewall Logs . . . . . 319
Verifying and Troubleshooting Web Application Firewall . . . . . 321
**Chapter 13. Geo IP and Botnet Filter** . . . . . 325
Status . . . . . 325
General Status . . . . . 326
Botnet Status . . . . . 326
Settings . . . . . 327
General Settings . . . . . 327
Remediation Settings . . . . . 328
Access Policies . . . . . 329
Log . . . . . 331
Licensing . . . . . 334
**Chapter 14. Users Configuration** . . . . . 335
Users > Status . . . . . 335
Access Policies Concepts . . . . . 336
Access Policy Hierarchy . . . . . 336
Users > Local Users . . . . . 337
Users > Local Users Overview . . . . . 337
Removing a User . . . . . 338
Adding a Local User . . . . . 338
Editing User Settings . . . . . 340
Users > Local Groups . . . . . 366
Users > Local Groups Overview . . . . . 366
Deleting a Group . . . . . 367
Adding a New Group . . . . . 367

Editing Group Settings . . . . . 368
Group Configuration for LDAP Authentication Domains . . . . . 382
Group Configuration for Active Directory, NT and RADIUS Domains . . . . . 386
Creating a Citrix Bookmark for a Local Group . . . . . 388
Global Configuration . . . . . 389
Edit Global Settings . . . . . 390
Edit Global Policies . . . . . 392
Edit Global Bookmarks . . . . . 394
Edit EPC Settings . . . . . 394
**Chapter 15. Log Configuration** . . . . . 397
Log > View . . . . . 397
Log > View Overview . . . . . 398
Viewing Logs . . . . . 399
Emailing Logs . . . . . 400
Log > Settings . . . . . 400
Log > Settings Overview . . . . . 401
Configuring Log Settings . . . . . 402
Configuring the Mail Server . . . . . 403
Log > Categories . . . . . 404
Log > ViewPoint . . . . . 404
Log > ViewPoint Overview . . . . . 405
Adding a ViewPoint Server . . . . . 405
Log > Analyzer . . . . . 405
Log > Analyzer Overview . . . . . 406
Adding an Analyzer Server . . . . . 406
**Chapter 16. Virtual Office Configuration** . . . . . 407
Virtual Office . . . . . 407
Virtual Office Overview . . . . . 407
Using the Virtual Office . . . . . 408
Online Help . . . . . 409
Online Help Button . . . . . 409
Using Context Sensitive Help . . . . . 409
Configuring the SRA Appliance with a Third-Party Gateway . . . . . 411
Cisco PIX Configuration for SRA Appliance Deployment . . . . . 411
Before you Begin . . . . . 411
Method One – SRA Appliance on LAN Interface . . . . . 412
Method Two – SRA Appliance on DMZ Interface . . . . . 415
Linksys WRT54GS . . . . . 417
WatchGuard Firebox X Edge . . . . . 418
NetGear FVS318 . . . . . 420
Netgear Wireless Router MR814 SSL configuration . . . . . 422

Check Point AIR 55 . . . . . 423
Setting up an SRA Appliance with Check Point AIR 55 . . . . . 423
Static Route . . . . . 424
ARP . . . . . 424
Use Cases . . . . . 427
Importing CA Certificates on Windows . . . . . 427
Importing a goDaddy Certificate on Windows . . . . . 427
Importing a Server Certificate on Windows . . . . . 430
Creating Unique Access Policies for AD Groups . . . . . 431
Creating the Active Directory Domain . . . . . 432
Adding a Global Deny All Policy . . . . . 433
Creating Local Groups . . . . . 434
Adding the SSHv2 PERMIT Policy . . . . . 437
Adding the OWA PERMIT Policies . . . . . 437
Verifying the Access Policy Configuration . . . . . 439
NetExtender Troubleshooting . . . . . 445
FAQs . . . . . 449
Hardware FAQ . . . . . 452
Digital Certificates and Certificate Authorities FAQ . . . . . 456
NetExtender FAQ . . . . . 462
General FAQ . . . . . 465
Command Line Interface . . . . . 473
SMS Email Formats . . . . . 477
Support Information . . . . . 483
Contact Information . . . . . 483
Limited Hardware Warranty . . . . . 483
GNU General Public License (GPL) Source Code . . . . . 484
End User Licensing Agreement . . . . . 484
Glossary . . . . . 491

# Chapter 1
# About This Guide

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

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

## Guide Conventions

The following conventions are 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. |

# Chapter 2

# SRA Overview

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


- Overview of Dell SonicWALL SRA on page 13
- Concepts for Dell SonicWALL SRA on page 20
- Navigating the SRA Management Interface on page 80
- Deployment Guidelines on page 86


## Overview of Dell SonicWALL SRA

The Dell SonicWALL SRA appliance provides organizations with a simple, secure and clientless method of access to applications and network resources specifically for remote and mobile employees. Organizations can use SRA 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:


- SSL for Virtual Private Networking (VPN) on page 13
- SRA Virtual Appliance on page 13
- SRA Software Components on page 14
- SRA Hardware Components on page 15


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

### SRA Virtual Appliance

The SRA Virtual Appliance is a virtual machine that runs the SRA series software on a VMware platform. All software components, features, and functionality described in this guide are supported by the SRA Virtual Appliance, except High Availability and SSL Offloading.

Deploying the SRA as a virtual appliance allows leveraging of shared computing resources to optimize utilization, easy migration and reduced capital costs. The SRA 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 SRA Virtual Appliance provides the same hardened operating system that comes with the SRA hardware appliances.

The elements of basic VMware structure must be implemented prior to deploying the SRA Virtual Appliance. For detailed information about deploying the SRA Virtual Appliance, see the *Dell SonicWALL SRA Virtual Appliance Getting Started Guide*, available at: http://www.sonicwall.com/us/support/3893.html

# SRA Software Components

SRA appliances provide clientless identity-based secure remote access to the protected internal network. Using the Virtual Office environment, 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 SRA protocols are described as clientless, the typical SRA portal combines Web, Java, and ActiveX components that are downloaded from the SRA portal transparently, allowing users to connect to a remote network without needing to manually install and configure a VPN client application. In addition, SRA 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 SRA Web-based management interface provides an end-to-end SSL VPN solution. This interface can configure SRA users, access policies, authentication methods, user bookmarks for network resources, and system settings.

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

The SRA network extension client, NetExtender, is available through the SRA Web portal via an ActiveX control on Windows or using Java on MacOS or Linux systems. It is also available through stand-alone applications for Windows, Linux, and MacOS platforms. The NetExtender standalone applications are automatically installed on a client system the first time the user clicks the NetExtender link in the Virtual Office portal. SRA 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, SSHv1 and VNC applets support MS JVM in Internet Explorer, and run on other browsers with SUN JRE 1.6.0_10 or higher.

# 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 16
- SRA 1600 Front and Back Panels Overview on page 17
- SRA 4200 Front and Back Panels Overview on page 18
- SRA 1200 Front Panel Overview on page 19

# SRA 4600 Front and Back Panels Overview

*Figure 1 SRA 4600 Front and Back Panels*

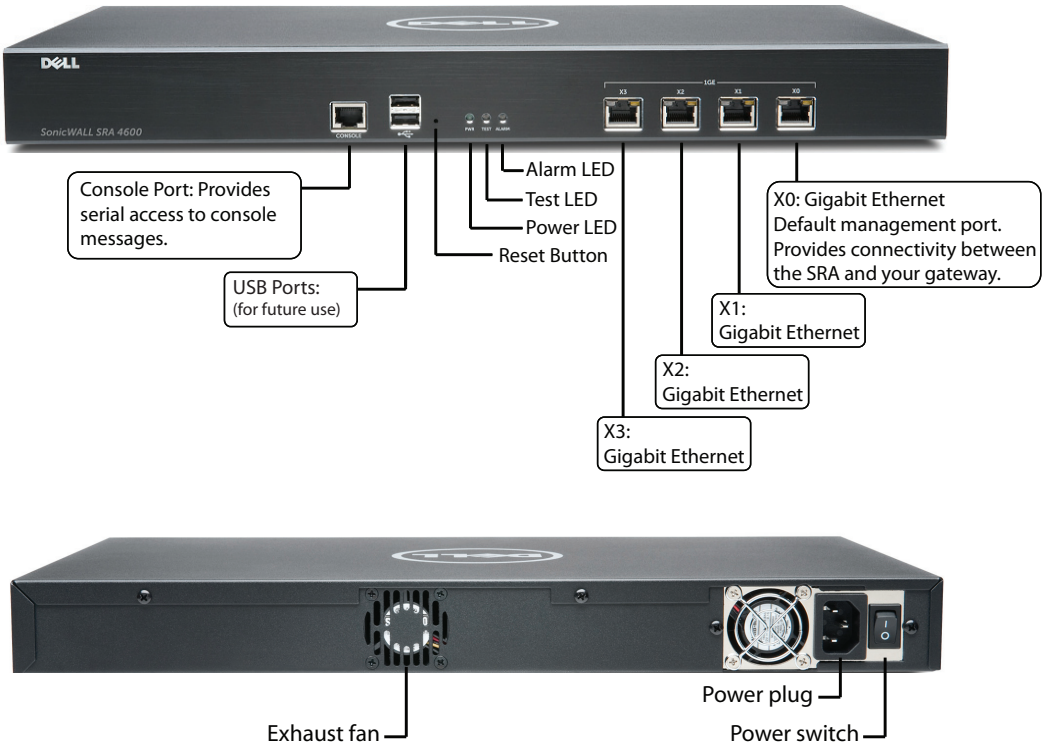



*Table 1 SRA 4600 Front Panel Features*

| 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. |

*Table 2 SRA 4600 Back Panel Features*

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

*Figure 2 SRA 1600 Front and Back Panels*

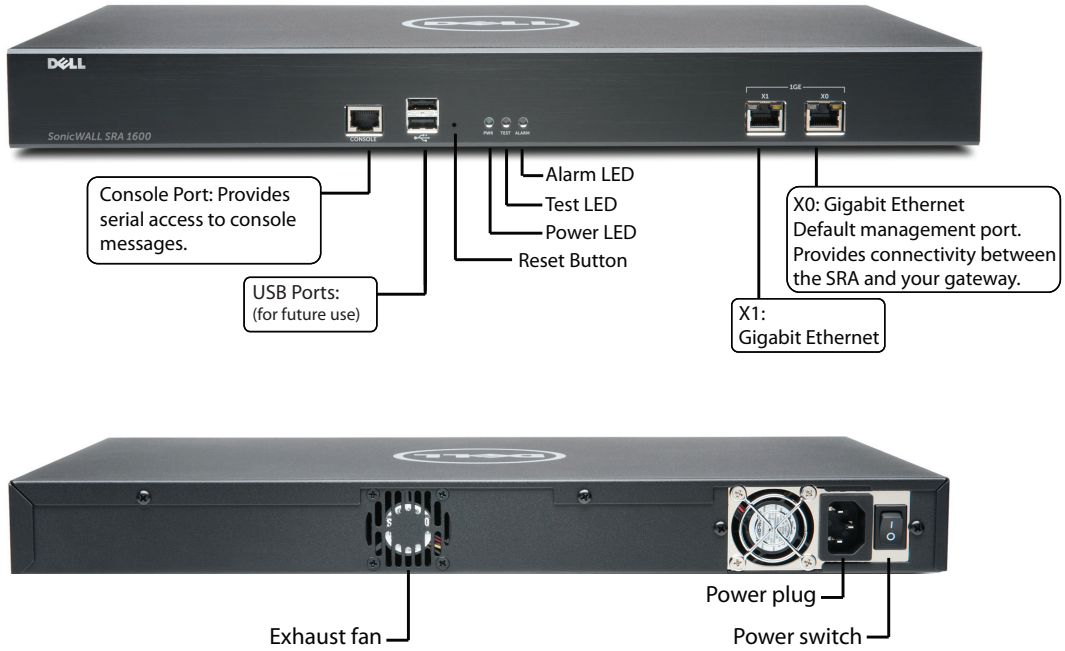



*Table 3 SRA 1600 Front Panel Features*

| 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. |

*Table 4 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. |

# SRA 4200 Front and Back Panels Overview

*Figure 3 SRA 4200 Front and Back Panels*

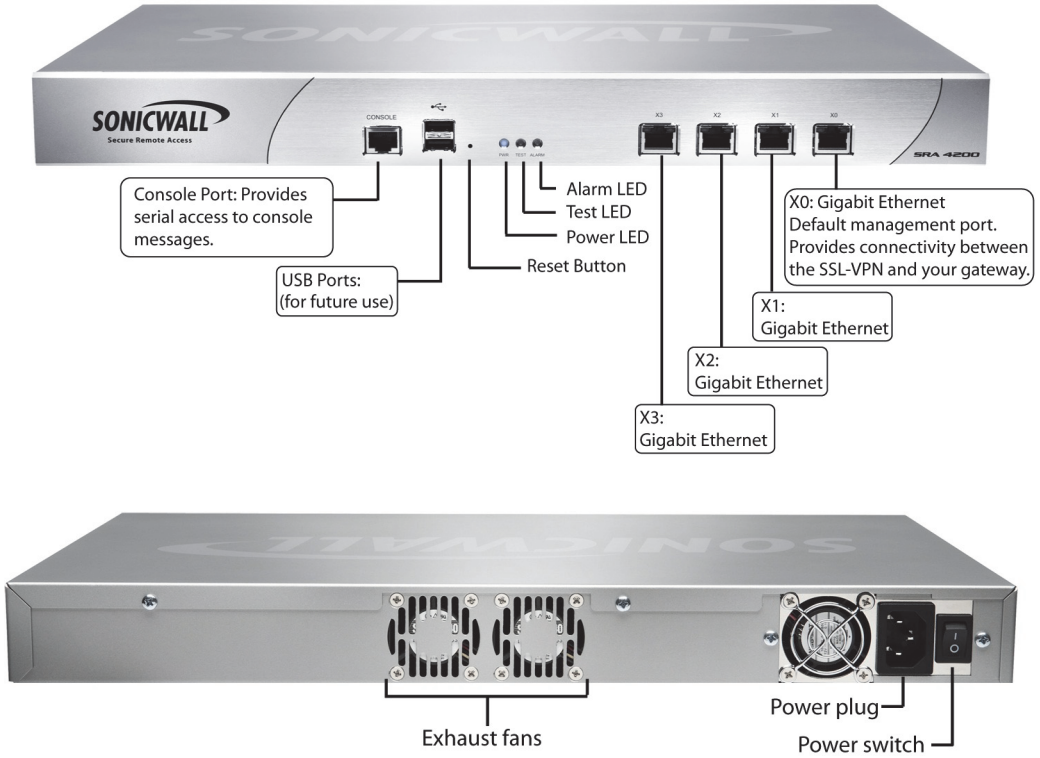



*Table 5 SRA 4200 Front Panel Features*

| 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 4200 is powered on. |
| Test LED | Indicates the SRA 4200 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 4200 and your gateway. |

*Table 6 SRA 4200 Back Panel Features*

| Back Panel Feature | Description |
|---|---|
| Exhaust fans | Provides optimal cooling for the SRA 4200 appliance. |
| Power plug | Provides power connection using supplied power cord. |
| Power switch | Powers the SRA 4200 on and off. |

# SRA 1200 Front Panel Overview

*Figure 4 SRA 1200 Front Panel*

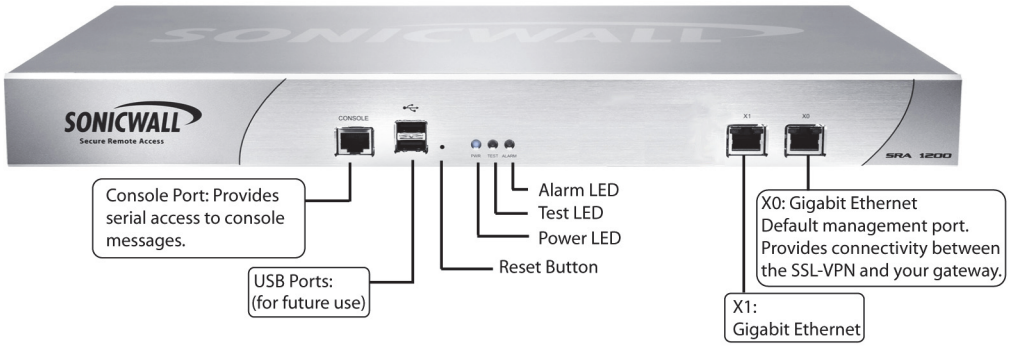



*Table 7 SRA 1200 Front Panel Features*

| 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 1200 is powered on. |
| Test LED | Indicates the SRA 1200 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 1200 and your gateway. |

# Concepts for Dell SonicWALL SRA

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


- Encryption Overview on page 20
- SSL Handshake Procedure on page 20
- IPv6 Support Overview on page 21
- Browser Requirements for the SRA Administrator on page 24
- Browser Requirements for the SRA End User on page 24
- Portals Overview on page 25
- Domains Overview on page 25
- Application Offloading and HTTP(S) Bookmarks Overview on page 26
- Cross Domain Single Sign-On on page 30
- ActiveSync Authentication on page 30
- Network Resources Overview on page 35
- SNMP Overview on page 41
- DNS Overview on page 42
- Network Routes Overview on page 42
- NetExtender Overview on page 42
- Two-Factor Authentication Overview on page 46
- One Time Password Overview on page 49
- End Point Control Overview on page 51
- Secure Virtual Assist Overview on page 52
- Web Application Firewall Overview on page 69


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

## SSL Handshake Procedure

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

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

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

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

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

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

**Step 6** The browser and the 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 SRA gateway will encrypt and decrypt data using the same encryption key. This is called symmetric encryption.

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

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

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

**Step 10** Once authenticated, the user can access the SRA 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, which is used with a DHCPv6 server, and stateless address configuration, where hosts on a link automatically configure themselves with IPv6 addresses for the link, called *link-local* addresses.

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

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

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

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

SonicOS SSL VPN supports IPv6 in the following areas:

**Services**

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

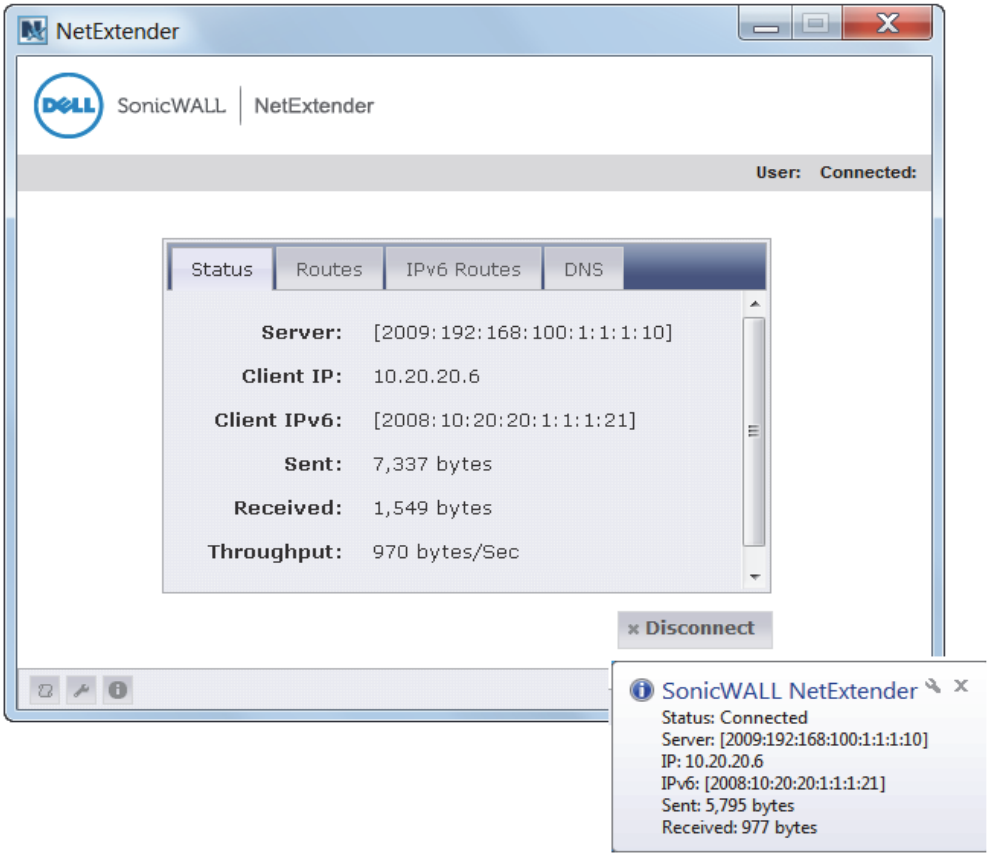
**Note** IPv6 is not supported for File Shares (CIFS).

**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 SRA appliance if the client machine supports IPv6 and an IPv6 address pool is configured on the SRA. 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.

# Browser Requirements for the SRA Administrator

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

| Minimum Browser / Version Requirements | Windows Vista | Windows 7 | Windows 8 / 8.1 | Linux | MacOS X |
|---|---|---|---|---|---|
| **Internet Explorer** | --- | IE 9 | IE 10 / 11 | --- | --- |
| **Mozilla Firefox** | Firefox 26 | Firefox 26 | Firefox 26 | Firefox 26 | Firefox 26 |
| **Google Chrome** | Chrome 32 | Chrome 32 | Chrome 32 | Chrome 32 | Chrome 32 |

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

## Windows XP and Internet Explorer 8 Update

Microsoft has ended support for Windows XP and IE8. Dell SonicWALL SRA clients will still continue to work, but may become more vulnerable to security risks and viruses. Dell SonicWALL will no longer provide fixes for issues exclusively affecting Windows XP and IE8. Dell SonicWALL strongly encourages Windows users to migrate to versions supported by Microsoft. For more information, refer to the Microsoft Windows website: http://windows.microsoft.com/en-us/windows/end-support-help

# Browser Requirements for the SRA End User

The following is a list of Web browser and operating system support for various SRA 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 SSL VPN End User Interface:

| Minimum Browser / Version Requirements | Windows Vista | Windows 7 | Windows 8 / 8.1 | Linux | MacOS X |
|---|---|---|---|---|---|
| **Apple Safari** | --- | --- | --- | --- | Safari 5 |
| **Internet Explorer** | --- | IE 9 | IE 10 / 11 | --- | --- |
| **Mozilla Firefox** | Firefox 26 | Firefox 26 | Firefox 26 | Firefox 26 | Firefox 26 |
| **Google Chrome** | Chrome 32 | Chrome 32 | Chrome 32 | Chrome 32 | Chrome 32 |

## Windows XP and Internet Explorer 8 Update

Microsoft has ended support for Windows XP and IE8. Dell SonicWALL SRA clients will still continue to work, but may become more vulnerable to security risks and viruses. Dell SonicWALL will no longer provide fixes for issues exclusively affecting Windows XP and IE8. Dell SonicWALL strongly encourages Windows users to migrate to versions supported by Microsoft. For more information, refer to the Microsoft Windows website: http://windows.microsoft.com/en-us/windows/end-support-help

# Portals Overview

The SRA appliance provides a mechanism called Virtual Office, which is a Web-based *portal* interface that provides clients with easy access to internal resources in your organization. Components such as NetExtender, 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 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

SRA appliances let you configure multiple portals, each with its own title, banner, login message, logo and set of available resources. Each portal also enables you to set individual Virtual Hosts/Domain Names 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 141.

# Domains Overview

A domain in the SRA environment is a mechanism that enables authentication of users attempting to access the network being serviced by the SRA appliance. Domain types include the SRA internal LocalDomain, and the external platforms Microsoft Active Directory, NT Authentication, LDAP, and RADIUS. Often, only one domain will suffice to provide authentication to your organization, although a larger organization may require distributed domains to handle multiple nodes or collections of users attempting to access applications through the portal. For information about configuring domains, refer to Portals > Domains on page 162.

# Application Offloading and HTTP(S) Bookmarks Overview

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.

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 may need Two-factor or Client Certificate authentication to access Outlook Web Access (OWA), but are not allowed to access OWA public folders. If authentication is enabled, multiple layers of 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 SRA 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.

For configuration information, see Portals > Application Offloading on page 155 and Adding or Editing User Bookmarks on page 352.

## 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 SRA:

- 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 SRA 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 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, which 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

On SRA 6.0 and higher, Application Offloading and HTTP(S) bookmarks are supported on the following SRA appliances:

- SRA 4600
- SRA 4200
- SRA 1600
- SRA 1200
- SRA 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

Beginning in SRA 6.0, **Sharepoint 2010** is 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:

| Sharepoint Features | Browsers |
|---|---|
| Add Announcement<br>Delete Announcement<br>Download Document<br>Add Document<br>Delete Document<br>Add New Item<br>Delete Item | Internet Explorer 8 and 9<br>Firefox 16.0+<br>Chrome 22.0+ |

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

- Microsoft Outlook Web Access 2010
  Microsoft Outlook Web Access 2007
  Microsoft Outlook Web Access 2003

**Note** In SRA 6.0 and higher, 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 SRA appliance. Before SRA 6.0, users had to disable authentication for ActiveSync offloading portals, because ActiveSync requests are different from requests sent from the browser.

Outlook Web Access is supported on the SRA 4600/4200/1600/1200 and SRA Virtual Appliance platforms.

- Windows Sharepoint 2007
  Windows Sharepoint Services 3.0
  Windows Sharepoint Services 2.0

The integrated client features of Sharepoint are not supported.

- Lotus Domino Web Access 8.0.1, 8.5.1, and 8.5.2

Domino Web Access is supported on the SRA 4600/4200/1600/1200 and SRA 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
- Windows Mobile 6.5 based phones
- Windows Mobile 6.0 based phones

**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.
- **NTLM (Microsoft NT LAN Manager)** – Provides automatic authentication between Active Directory aware applications.
- **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 8.0 or newer
- Windows 8.1, Windows 8, Windows 7, Windows XP, or Windows Server 2003 or later

## Supported Applications

When using application offloading or HTTP(S) bookmarks to access applications for Web-based clients, full feature sets are accessible to users. Application offloading and HTTP(S) bookmarks provide enhanced application support for the following software applications:

- Sharepoint Server 2007
- Sharepoint Server 2010
- Microsoft Outlook Web Access Premium
- Lotus Domino Web Access 8.0.1, 8.5.1, and 8.5.2

**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
  - For features that rely on Windows Sharepoint Services-compatible client programs, application offloading and HTTP(S) bookmarks do not support client integration capabilities on Internet Explorer.
  - Only forms-based authentication and basic authentication schemes are supported.
  - Single Sign-On is supported only for basic authentication.
  - Sharepoint 2010 is supported with application offloading, but not with HTTP(S) bookmarks.
- Microsoft OWA
  - S/MIME support and bi-directional layout support for Arabic and Hebrew in Microsoft OWA Premium are only available using Internet Explorer 8 and later. Gzip compression supported by Microsoft OWA Premium is not supported through the reverse proxy.
- Outlook Anywhere
  - SRA 4200 only with Application Offloading.
  - Outlook Anywhere uses Microsoft's MS-RPCH proprietary protocol, which may conflict with normal HTTP(S) protocol.
  - Use the Generic SSL Offloading instead of HTTP or HTTPS.

Application Offloading should support any application using HTTP/HTTPS. SRA 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. Since 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.s

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 may not be rewritten, depending on how the Web application has been developed. (This limitation is usually the same for other WAF/SRA 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 into application offloading portals after logging into the main portal.

To use Cross Domain Single Sign-on (SSO), perform the following steps:

**Step 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 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.

**Step 2** Log into the portal and create a bookmark, as explained in Adding or Editing User Bookmarks on page 352.

**Step 3** Set the service to **External Web Site**, as explained in External Web Site on page 360.

**Step 4** Enable **Automatically log in** for the bookmark, which enables Cross Domain SSO for this bookmark.

**Step 5** Specify a Host, which is a portal with the same shared domain name.

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

The shared domain names don't 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

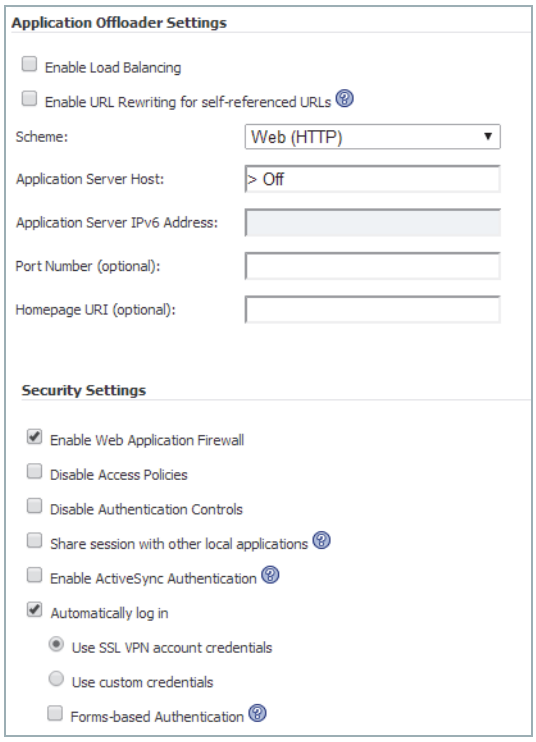
Application Offloading now supports authentication for ActiveSync. Application Offloading technology delivers Web applications using Virtual Hosting and Reverse Proxy. Users still need to authenticate with the SRA appliance before accessing the backend Web application. However, the proxy avoids URL rewriting 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 SRA appliance. Before SRA 6.0, users had to disable authentication for ActiveSync offloading portals, because ActiveSync requests are different from requests sent from the browser.

**Note** On iPhones/iPads running versions earlier than iOS 6.1.2, initial account synchronization may fail if a calendar contains a recurring invite.

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




To configure ActiveSync authentication, clear the **Disable Authentication Controls** check box to display the authentication fields. Select the **Enable ActiveSync authentication** check box 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.

## ActiveSync Log Entries

The **Log > View** page is updated when a Web application is offloaded. Most mobile systems (iPhone, Android, Windows Mobile, etc.) 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. The ActiveSync label is not used in log entries for anonymous users who use ActiveSync.

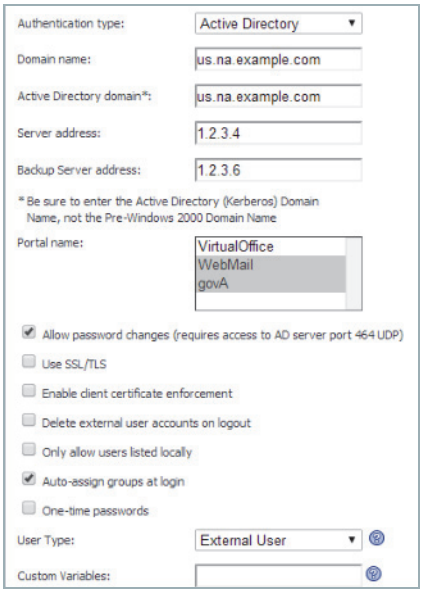
**Note** A user's credential in the Exchange server must be the same as the one in the SRA. Many authentication types are available for each domain in the SRA. If using the Local User Database, make sure the user name and password is the same as the one for the Exchange server. Fortunately, other authentication types like Active Directory can share credentials for both the Exchange server and SRA appliance. However, authentication using authentication

types that share credentials may take longer and the first ActiveSync request may time out. Once authentication succeeds, a session is created and other requests won't need to be authenticated again.

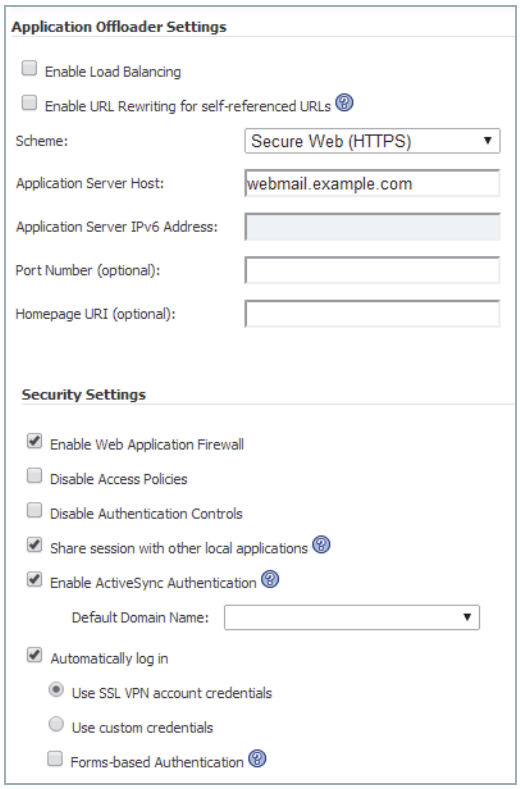
## Configuring a Portal to Check Email From an Android Device

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 will be blocked.

**Step 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 webmail.



**Step 2** In the SRA appliance, create an offloading portal with the name **webmail**.

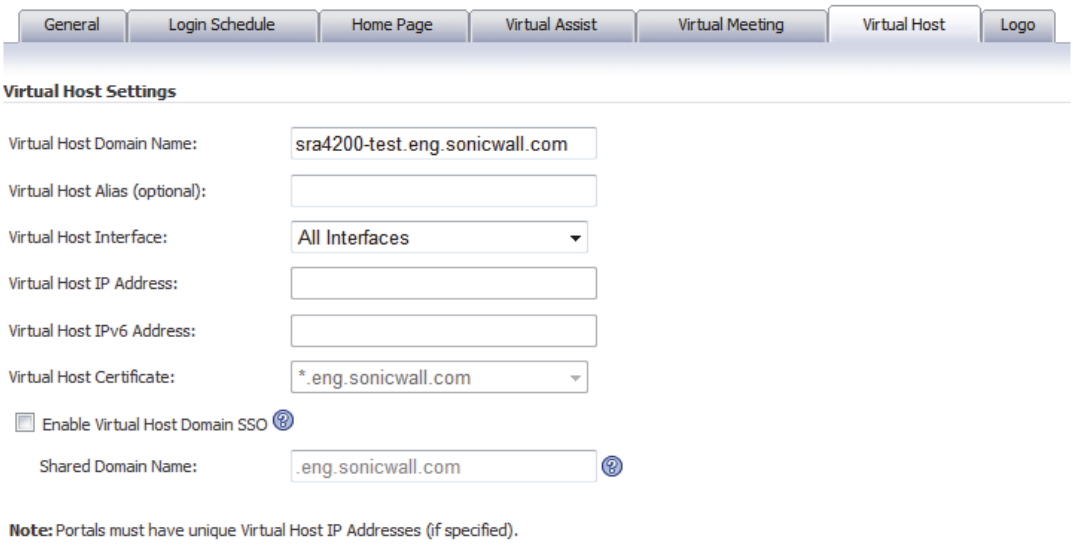



**Step 3** Set the **Scheme** to **Secure Web (HTTPS).**

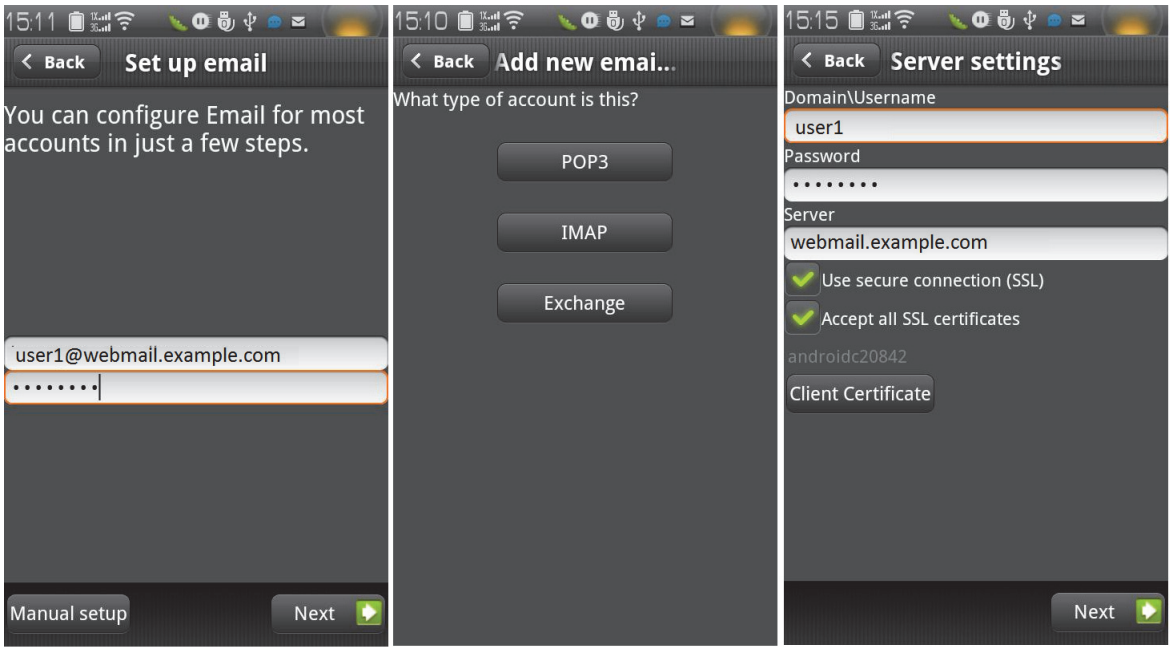
**Step 4** Set the **Application Server Host** to your Exchange server, for example *webmail.example.com*.

**Step 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.

**Step 6** Select the **Enable ActiveSync Authentication** check box. Leave the default domain name blank or input **webmail.example.com.**



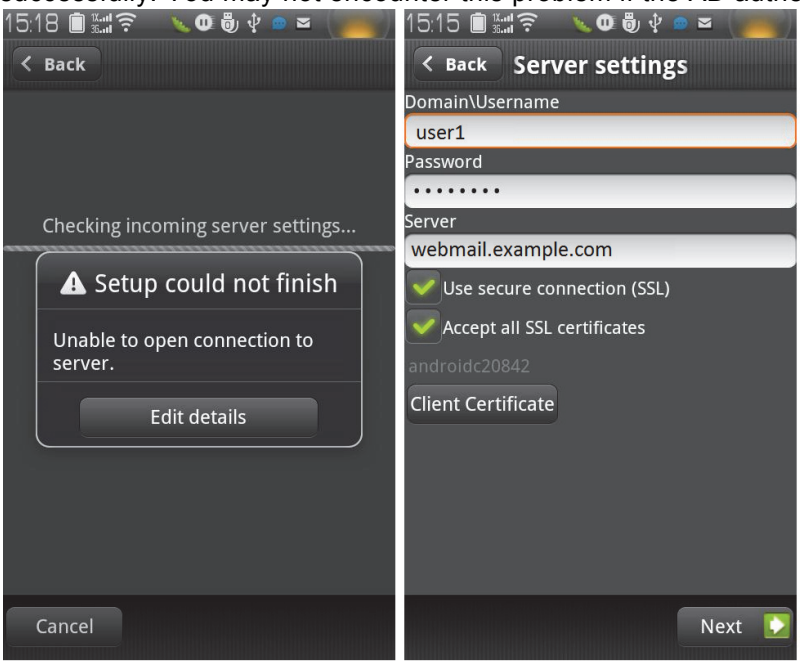

**Step 7** Turn on the Android phone, open the Email application, and type your email address and password. Click **Next**.



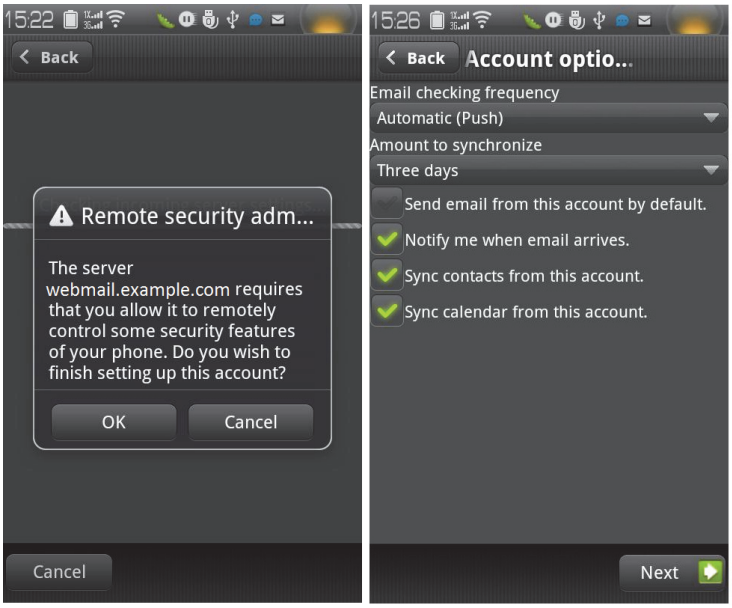

**Step 8** Choose **Exchange.**

**Step 9** 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.**

**Step 10** 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 SRA log to see if the user logged in successfully. You may not encounter this problem if the AD authentication is fast.




**Step 11** When the authentication finishes, a security warning appears. Click **OK** to continue, modify your account settings, and click **Next**.




**Step 12** Try to send and receive emails, and ensure that ActiveSync entries are included in the SRA log.

# Network Resources Overview

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


- HTTP (Web) and Secure HTTPS (Web) on page 36
- Telnet (Java) on page 36
- SSHv1 and SSHv2 (Java) on page 37
- FTP (Web) on page 37
- File Shares (CIFS) on page 37
- Remote Desktop Protocols and Virtual Network Computing on page 37
- Application Protocols Using RDP on page 38
- Microsoft Outlook Web Access on page 39
- Windows Sharepoint Services on page 40
- Lotus Domino Web Access on page 41
- Citrix Portal on page 41


## HTTP (Web) and Secure HTTPS (Web)

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

The SRA 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 SRA 4600/4200 appliances support keys of up to 2048 bits.

HTTP(S) caching is supported on the 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 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 SRA appliance and is cleared for access by the access policies. However, SRA 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 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% of the required memory. Note that gzip compression is not available on the local (clear text side) of the SRA appliance, or for HTTPS requests from the remote client.

## Telnet (Java)

A Java-based 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 SRA appliance will make a connection to the server. Communication between the user over SSL and the server is

proxied using native Telnet. The Telnet applet supports MS JVM (Microsoft Java Virtual Machine) in Internet Explorer, and requires Sun Java Runtime Environment (JRE) 1.1 or higher for other browsers.

## SSHv1 and SSHv2 (Java)

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

## FTP (Web)

Proxy access to an FTP server on the internal network, the Internet, or any other network segment that can be reached by the SRA appliance. The remote user communicates with the SRA appliance by HTTPS and requests a URL that is retrieved over HTTP by the 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 may be required.

## File Shares (CIFS)

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

## Remote Desktop Protocols and Virtual Network Computing

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

- **RDP Java** – RDP Java is a Microsoft Remote Desktop Protocol that has the advantage of broad platform compatibility because it is provided in a Java client. The RDP Java client runs on Windows, Linux, and Mac computers, and supports full-screen mode. On Windows clients, SRA appliances support many advanced options. On Mac OS X 10.5 or above, RDP Java supports the Mac native RDC client.
- **RDP ActiveX** - RDP ActiveX is also a Microsoft Remote Desktop Protocol. The RDP ActiveX client only runs on Windows, and is not supported on Mac or Linux computers. Four advanced options are supported by SRA appliances for RDP ActiveX.

- **VNC (Java)** - VNC was originally developed by AT&T, but is today widely available as open source software. Any one of the many variants of VNC servers available can be installed on most any workstation or server for remote access. The VNC client to connect to those servers is delivered to remote users through the Web browser as a Java client.

### RDP 6 Support

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

The SRA appliance supports connections with RDP 6.1 clients. RDC 6.1 is included with the following operating systems:

- Windows 7
- Windows Server 2008
- Windows Vista Service Pack 1 (SP1)
- Windows XP Service Pack 3 (SP3)

RDC 6.1 incorporates the following functionality in Windows Server 2008:

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

For more information, see Adding or Editing User Bookmarks on page 352.

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

### RDP 7 Support

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

- Windows 8
- Windows 8.1
- Windows 7
- Windows Vista SP2
- Windows Vista SP1
- Windows XP SP3

## Application Protocols Using RDP

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

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

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

### Application Support for SSO, User Policies, Bookmarks

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.

***Table 8 Application Support***

| Application | Supports SSO | Global/Group/ User Policies | Bookmark Policies |
|---|---|---|---|
| Terminal Services (RDP - ActiveX) | Yes | Yes | Yes |
| Terminal Services (RDP - Java) | Yes | Yes | Yes |
| Virtual Network Computing (VNC) | No | Yes | Yes |
| File Transfer Protocol (FTP) | Yes | Yes | Yes |
| Telnet | No | 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 |

## Microsoft Outlook Web Access

Beginning with version 5.5, SRA includes reverse proxy application support for all versions of OWA 2010, 2007, and 2003.

Microsoft OWA Premium mode is a Web client for Microsoft Outlook 2003/2007/2010 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. SRA HTTP(S) reverse proxy supports Microsoft OWA Premium.

Microsoft OWA Premium includes the following features:

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

  **Note** S/MIME support for Microsoft OWA Premium is only available on Internet Explorer 8 or higher.

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

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

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

See Creating Unique Access Policies for AD Groups on page 431 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 SRA reverse proxy application support for Windows Sharepoint 2007, Windows Sharepoint Services 3.0, and Windows Sharepoint Services 2.0 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

For features that rely on Windows Sharepoint Services-compatible client programs, SRA 5.5 Reverse Proxy does not support the client integration capabilities of Sharepoint.

Single sign-on is supported only for basic authentication.

Only forms-based authentication and basic authentication schemes are supported

## Lotus Domino Web Access

The SRA appliance reverse proxy application supports for Domino Web Access 8.0.1, 8.5.1, and 8.5.2 includes the following 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 applet requires SUN JRE 1.6.0_10 or higher.

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 plugin.

SRA appliances support client computers running the Citrix “Receiver for Windows 3.0” ActiveX client, the Citrix “Receiver for Java 10.1” Java client, Citrix XenApp plugin version 12.0.3 or earlier (including earlier versions of ICA Client) and Citrix Java client version 10.0 or earlier. The minimum working version of the Citrix ICA Client for Vista is 10.0.

SonicOS SRA 5.5 and higher supports Citrix XenApp Server 6.5, XenApp Server 6.0, XenApp Server 5.0, and XenApp Server 4.5.

# SNMP Overview

SRA appliances running SRA 5.0 or higher support Simple Network Management Protocol (SNMP), which will report 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 SRA appliance to enable it to resolve host names with IP addresses. The SRA 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 SRA appliance to reach remote IP networks through the designated default gateway. The gateway will typically be the upstream firewall to which the 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. This section contains the following subsections:


- What is NetExtender? on page 42
- Benefits on page 42
- NetExtender Concepts on page 43


For information on using NetExtender, refer to the NetExtender > Status on page 214 or refer to the *Dell SonicWALL SRA User's Guide*.

## What is NetExtender?

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

In SRA 5.5 and higher, NetExtender capabilities include the Dell SonicWALL Mobile Connect app for Apple iPhone, iPad, and iPod Touch. Mobile Connect enables secure, mobile connections to private networks protected by Dell SonicWALL security appliances. For information about installing and using Dell SonicWALL Mobile Connect, see the *Dell SonicWALL 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 with the XPCOM plugin when using Firefox. On Linux or MacOS systems, supported browsers use Java controls to automatically install NetExtender from the Virtual Office portal.

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

After installation, NetExtender automatically launches and connects a virtual adapter for SSL-secure NetExtender point-to-point access to permitted hosts and subnets on the internal network.

## NetExtender Concepts

The following sections describe advanced NetExtender concepts:


- Stand-Alone Client on page 43
- Multiple Ranges and Routes on page 44
- NetExtender with External Authentication Methods on page 45
- Point to Point Server IP Address on page 45
- Connection Scripts on page 45
- Tunnel All Mode on page 45
- Proxy Configuration on page 45


### Stand-Alone Client

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

Once the NetExtender stand-alone client has been installed, Windows users can launch NetExtender from their PC's **Start > Programs** menu and configure NetExtender to launch when Windows boots.

NetExtender can establish a VPN session before the user logs into the Windows domain. Users with Windows XP or earlier versions can click the **Logon using dial-up connection** on the Windows login screen and select NetExtender from the list of dialup connections. 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.

Mac users can launch NetExtender from their system Applications folder, or drag the icon to the dock for quick access. On Linux systems, the installer creates a desktop shortcut in /usr/share/NetExtender. This can be dragged to the shortcut bar in environments like Gnome and KDE.

NetExtender is compatible with the following Dell SonicWALL appliances:

- SRA 4600/1600
- SRA 4200/1200
- SRA Virtual Appliance
- NSA and TZ series (with SRA license)

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

NetExtender is officially supported on the following client platforms:

- Fedora 14+
- Ubuntu 11.04+
- OpenSUSE 10.3+
- Mac OS X 10.6.8+
- Android 1.6+ (rooting required)
- Windows Mobile 7.5, 7.8, and 8.0
- Windows 8.1, Windows 8, Windows XP, Windows 7, Windows Server 2003, Windows Server 2008 R2.

NetExtender may work properly on other Linux distributions, but they are not officially supported by Dell SonicWALL.

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

Multiple Ranges and Routes

Multiple range and route support for NetExtender on 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 as in the SRA 1.0 version of NetExtender. The following sections describe the new multiple range and route enhancements:


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


### 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 SRA appliance assigns IP addresses. When assigning an IP address to a NetExtender client, the 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, etc.). This segmentation is controlled by the **Add Global NetExtender Client routes** and **Add Group NetExtender Client routes** check boxes.

### NetExtender with External Authentication Methods

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

### Point to Point Server IP Address

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

### Connection Scripts

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 SRA NetExtender tunnel—including traffic destined for the remote user's local network. This is accomplished by adding the following routes to the remote client's route table:

| IP Address | Subnet mask |
|---|---|
| 0.0.0.0 | 0.0.0.0 |
| 0.0.0.0 | 128.0.0.0 |
| 128.0.0.0 | 128.0.0.0 |

NetExtender also adds routes for the local networks of all connected Network Connections. These routes are configured with higher metrics than any existing routes to force traffic destined for the local network over the SRA 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 SRA tunnel.

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

### Proxy Configuration

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)), which can push the proxy settings script to the client automatically.

- **Use automatic configuration script** - If you know the location of the proxy settings script, you can select this option and provide the URL of the script.
- **Use proxy server** - You can use this option to specify the IP address and port of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses and bypass the proxy server. If required, you can enter a user name and password for the proxy server. If the proxy server requires a username and password, but you do not specify them, a NetExtender pop-up window will prompt you to enter them when you first connect.

When NetExtender connects using proxy settings, it establishes an HTTPS connection to the proxy server instead of connecting to the SRA server directly. The proxy server then forwards traffic to the 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).

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

Beginning in SRA 5.5, two RADIUS servers can be used for two-factor authentication, allowing users to be authenticated through the Web portal or with an SRA client such as NetExtender or Secure Virtual Assist.

**Note** Single sign-on (SSO) in SRA appliances do not support two-factor authentication.

See the following sections:


- Benefits of Two-Factor Authentication on page 46
- How Does Two-Factor Authentication Work? on page 46
- 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 via 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 via 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 SRA platforms.

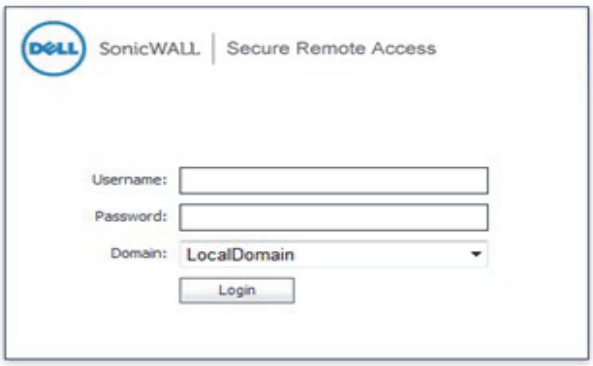
VASCO Data Security delivers reliable authentication through the use of One Time Password technology. VASCO IdentiKey combined with Dell SonicWALL SRA and firewall VPN appliances creates an open-market approach delivered through VASCO IdentiKey technology.

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 SRA 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 SRA server for authentication.

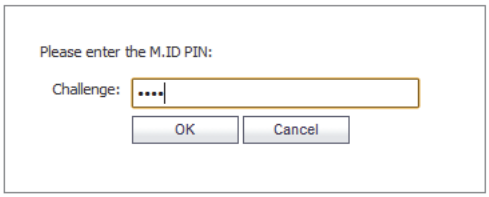
## Two-Factor Authentication Login Processes

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.

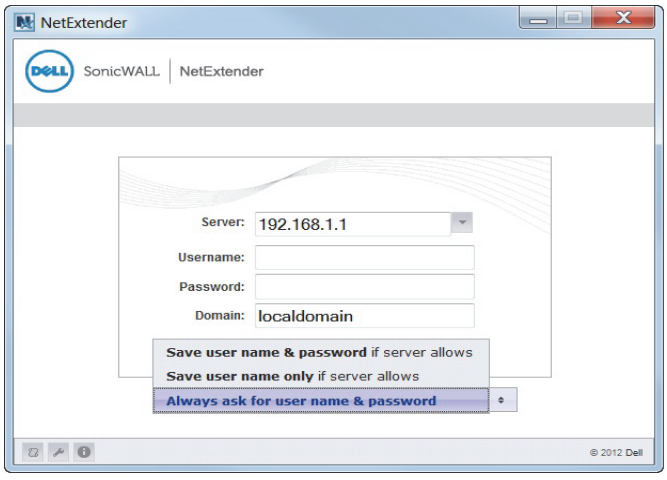



When prompting the user to input the challenge code, the message “Please enter the M.ID PIN:” is the reply message from the RADIUS server in this example; different RADIUS servers may have different reply message formats.

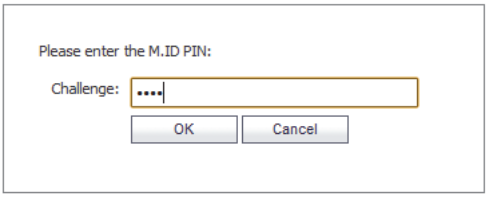



Some RADIUS servers may require the user to respond to several challenges to complete the authentication. In this example, the M.ID server asks the user to supply two challenges. The following passcode can be received through email or cellphone (if SMS is configured).

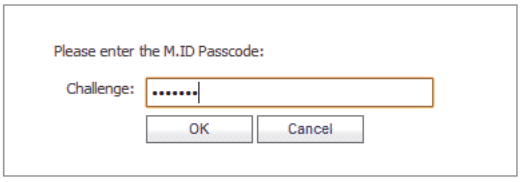
When using two-factor authentication with the NetExtender Windows client, the login process through the client is very similar to logging in through the Web page. Initially, the **Username** and **Password** fields are used to enter the first-stage credentials.



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? on page 49
- Benefits of One Time Passwords on page 49
- How Does the SRA One Time Password Feature Work? on page 50
- Configuring One Time Passwords for SMS-Capable Phones on page 50
- Verifying Administrator One Time Password Configuration on page 51


## What is One Time Password?

The SRA 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 SRA 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 Dell SonicWALL SRA users.

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

## Benefits of One Time Passwords

The SRA 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 SRA administrator before completing the SRA 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 SRA One Time Password Feature Work?

The SRA 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 SRA 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, which take precedence over those auto-configured by a domain policy and over AD/LDAP settings.

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

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

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

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

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

## Configuring One Time Passwords for SMS-Capable Phones

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

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

- Verizon: 4085551212@vtext.com
- Sprint: 4085551212@messaging.sprintpcs.com
- AT&T PCS: 4085551212@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 SMS Email Formats on page 477 for a more detailed list of SMS email formats.

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

To configure the SRA appliance to send one-time passwords to an SMS email address, follow the procedure described in Editing User Settings on page 340, and enter the user's SMS address in the **E-mail address** field.

## Verifying Administrator One Time Password Configuration

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

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

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

- Are you able to login without being prompted to check your email for One-time Password? The user account has not been enabled to use the One-time Password feature.
- Is the email address correct? If the email address for the user account has been entered incorrectly, login to the management interface to correct the email address.
- Is there no email with a one-time password? Wait a few minutes and refresh your email inbox. Check your spam filter. If there is no email after several minutes, try to login again to generate a new one-time password.
- Have you accurately typed the one-time password in the correct field? Re-type or copy and paste the one-time password within the time allotted by the user's timeout policy as set in the **Log > Settings** page.

# 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? on page 51
- Benefits of End Point Control on page 52
- How Does End Point Control Work? on page 52
- Configuring End Point Control on page 52


## 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. The SRA appliance includes End Point Control (EPC), a default service available on all SRA series appliances. EPC provides secure access from any Web-enabled system, including devices in untrusted environments. The SRA appliance supports.

## Benefits of End Point Control

The SRA appliance supports End Point Control (EPC), which 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 SRA.

## How Does End Point Control Work?

The SRA appliance provides end point security controls by performing 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.

Currently, EPC supports the Windows, Linux, and Mac NetExtender client. EPC enhancements are supported on the Dell SonicWALL SRA 4600/4200/1600/1200 and Virtual Appliance platforms.

End Point Control 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 SSL VPN from threats originating from client devices participating in the SSL VPN. For more information on Mobile Connect, refer to the *Mobile Connect User Guides*.

## Configuring End Point Control

Perform the following tasks to configure EPC:

**Step 1** Image the appliance with 7.5 firmware, as explained in the *Dell SonicWALL SRA Getting Started Guide*.

**Step 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 232.

**Step 3** Add and configure groups and users to allow or deny End Point Control profiles. See Edit EPC Settings on page 394.

**Step 4** Configure users to inherit their group profiles. See Edit EPC Settings on page 394.

**Step 5** Enable End Point Control. See End Point Control > Settings on page 240.

**Step 6** Connect to NetExtender and monitor the End Point Control log. See End Point Control > Log on page 240.

# Secure Virtual Assist Overview

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


- What is Secure Virtual Assist? **on page 53**
- Benefits of Secure Virtual Assist on page 53
- How Does Secure Virtual Assist Work? on page 53
- Launching a Secure Virtual Assist Technician Session on page 55

- Performing Secure Virtual Assist Technician Tasks on page 58
- Enabling a System for Secure Virtual Access on page 63

## What is Secure Virtual Assist?

Secure Virtual Assist is an easy to use tool that allows SRA 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

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 SRA appliance and tokenless two-factor authentication can be utilized.
- **Secure connections** - 256-bit AES SSL encryption of the data by the 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 SRA appliance.

## How Does Secure Virtual Assist Work?

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

- Basic Operation on page 53
- Remote File Transfer on page 54
- Chat Feature on page 54
- Email Invitation on page 55
- Secure Virtual Access on page 55

### Basic Operation

Secure Virtual Assist is a lightweight, thin client that installs automatically using Java from the SRA 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 may 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 via 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 SRA 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 SRA 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 performs.
9. If at anytime the customer wants to end the session, they can take control and click on the **End Virtual Assist** button in the bottom right corner of the screen.
10. When the session ends, the customer resumes sole control of the computer.

### Remote File Transfer

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

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

### Email Invitation

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

Secure Virtual Access, as part of the larger Secure Virtual Assist feature, allows technicians to gain access to systems outside the LAN of the 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 will appear only on that technician's Secure Virtual Assist support queue, within the SRA management interface. While Secure Virtual Access must be enabled per-portal, this functionality provides greater remote access flexibility for support technicians.

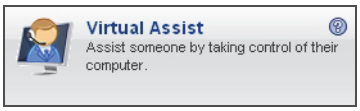
Installing and using Secure Virtual Access requires administrative privileges.

## Launching a Secure Virtual Assist Technician Session

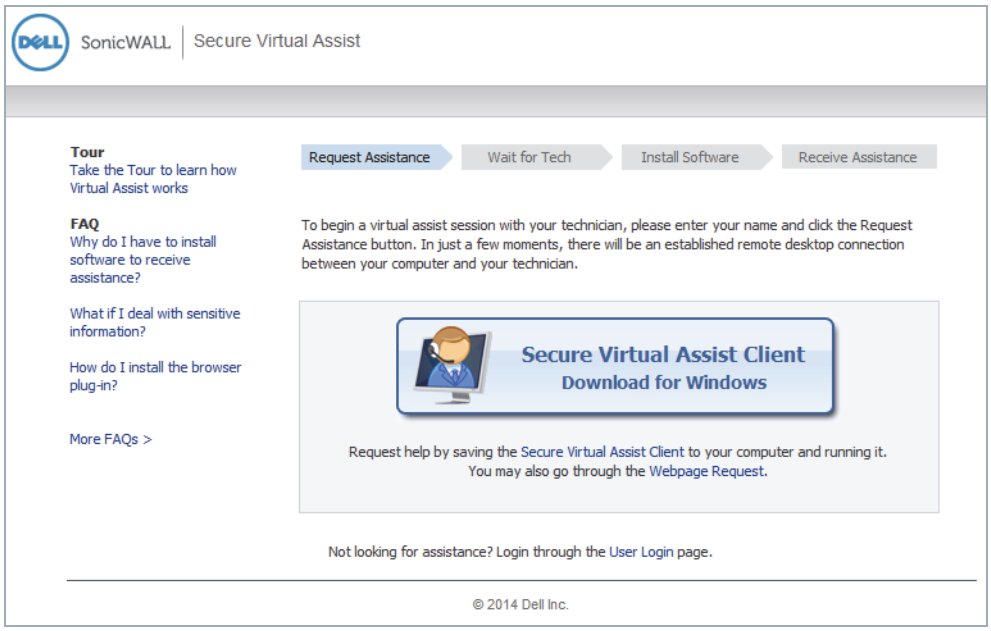
To launch a Secure Virtual Assist session as a technician, perform the following steps.

**Step 1** Log in to the SRA Virtual Office. If you are already logged in to the SRA customer interface, click on the **Virtual Office** button.

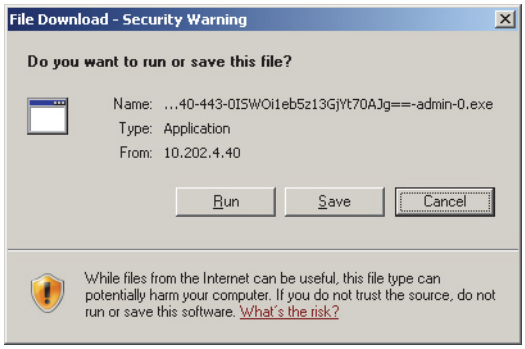
**Step 2** Click on the **Virtual Assist** button.




**Step 3** If the Virtual Assist plug-in is installed, the Virtual Assist window is displayed automatically. See Step 9 on page 58.

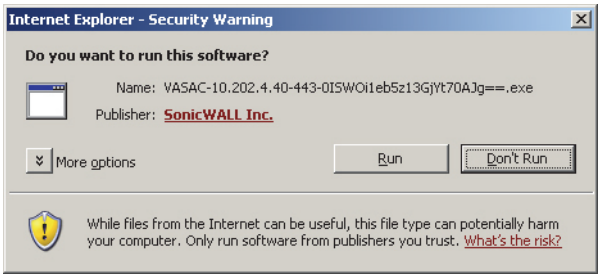


**Step 4** If the Virtual Assist plug-in is not installed, the File Download window displays, and Secure Virtual Assist attempts to automatically install. Click **Run** to launch the program directly, or click **Save** to save the installer file to your computer, and then manually launch it.

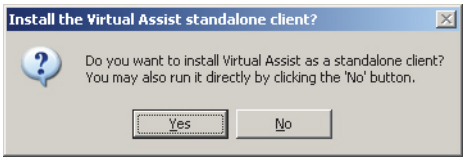



When downloading through IPv6, the File Download window displays IPv6 information.

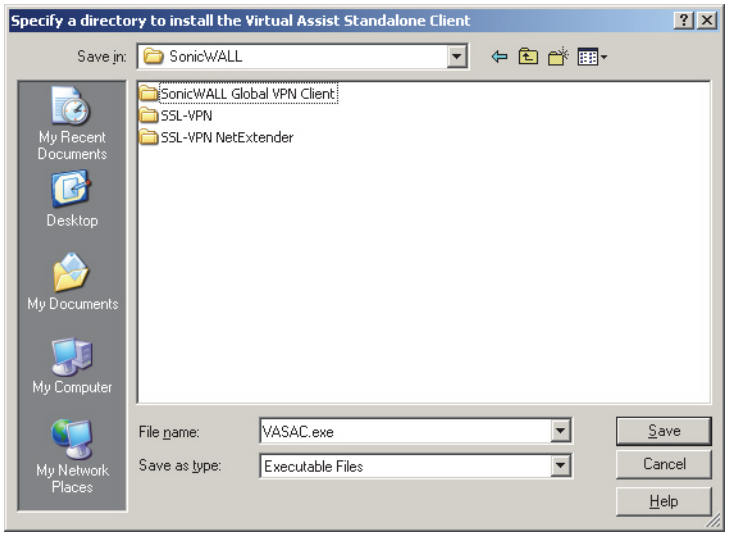
**Step 5** When you launch the installer, you may see an additional warning message. Click **Run**.



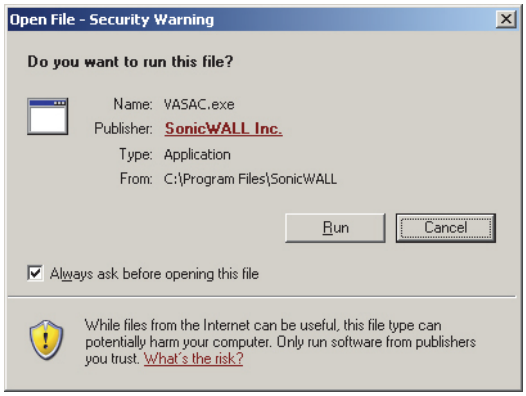
**Step 6** A pop-up window asks if you would like to install Secure Virtual Assist as a standalone client. Click **Yes** to save the application. A shortcut will be added to your desktop and a link to the application will be added to the program list on your Start Menu. Click **No** to launch Secure Virtual Assist without saving the application for future use.



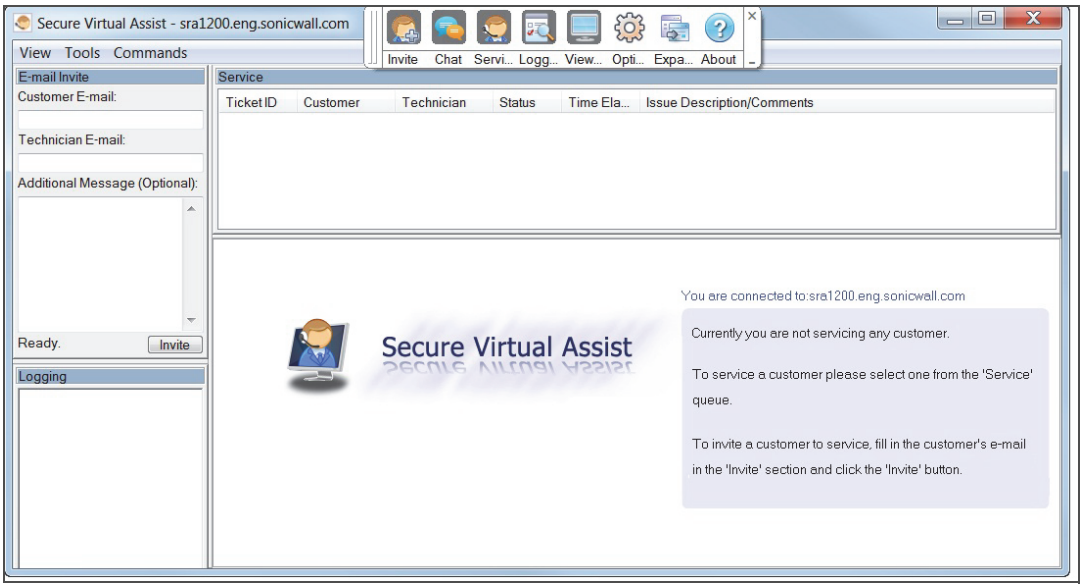

**Step 7** If you clicked **Yes** to save the application, you will be prompted to select a location to save the file. Select an appropriate location, such as C:\Program Files\SonicWALL.




**Step 8** When Secure Virtual Assist launches for the first time, you may see a security warning pop-up window. De-select the **Always ask before opening this file** check box to avoid this window in the future. Click **Run**.



**Step 9** The Secure Virtual Assist standalone application launches.




**Step 10** The technician is now ready to assist customers.

## Performing Secure Virtual Assist Technician Tasks

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

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

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

- Inviting Customers by Email on page 59
- Assisting Customers on page 59
- Using the Secure Virtual Assist Taskbar on page 60
- 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:

**Step 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.

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

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

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

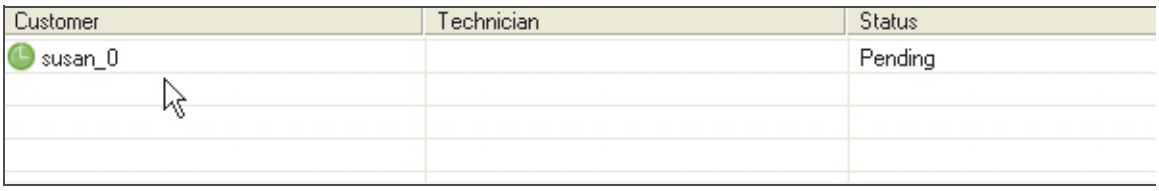
**Step 5** Click **Invite**. The customer will receive an email with an HTML link to launch Secure Virtual Assist.

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

### Assisting Customers

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

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




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

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

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

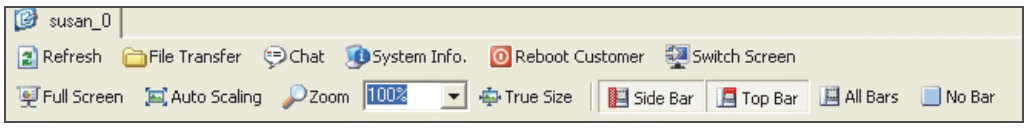
The customer has the following options during a Secure Virtual Assist session, each enabled after clicking the corresponding button.

- **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.

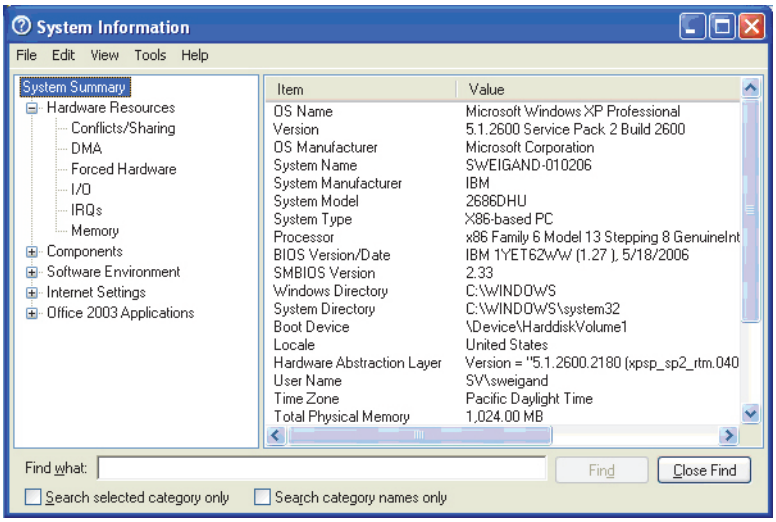
### Using the Secure Virtual Assist Taskbar

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

In Windows, the taskbar contains the following buttons:

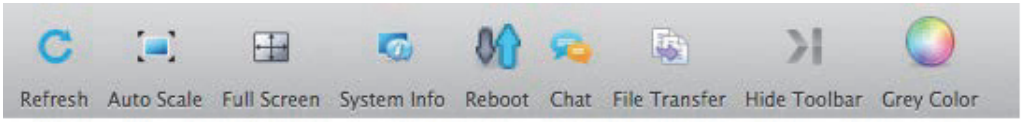



- **Refresh** - Refreshes the display of the customer's computer.
- **File Transfer** - Launches a window to transfer files to and from the customer's computer. see Using the Secure Virtual Assist File Transfer on page 62 for more information.
- **Chat** - Launches the chat window to communicate with 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 will be warned about and given the opportunity to deny the reboot.
- **Switch Screen** - Switches to a second monitor if the customer's computer has more than one monitor configured.

In MacOS, the taskbar contains the following buttons:




- **Refresh** - Refreshes the display of the customer's computer.
- **Auto Scale** - Adjusts the screen to fit the window size.
- **Full Screen** - Adjusts the screen to fill the entire window.
- **System Info** -Displays detailed information about the customer's computer similar to that shown for a Windows computer.
- **Reboot** - Reboot the customer's computer. Unless you have Requested full control, the customer will be 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

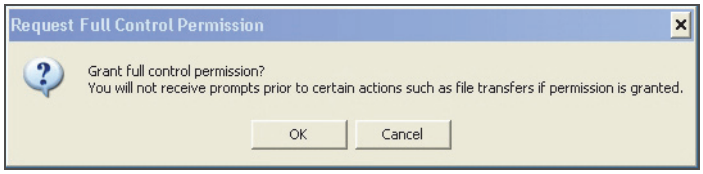
- **Full Screen** - Hides all of the Secure Virtual Assist toolbars and displays the customer's desktop on the technician's entire screen with the Secure Virtual Assist taskbar in the top left corner.

  If the Secure Virtual Assist taskbar doesn't display, move your mouse to the top middle of the screen. Right-click on the taskbar and click **Restore** to exit full-screen mode.
- **Auto Scaling** - Zooms the display to fill the entire 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%.
- **Side Bar** - Toggles the display of the side bar with the email invitation and chat windows.
- **Top Bar** - Toggles the display of the top bar with the customer queue and toolbar.
- **All Bars** - Displays both the side bar and top bar.
- **No Bar** - Hides both the side bar and top bar.

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

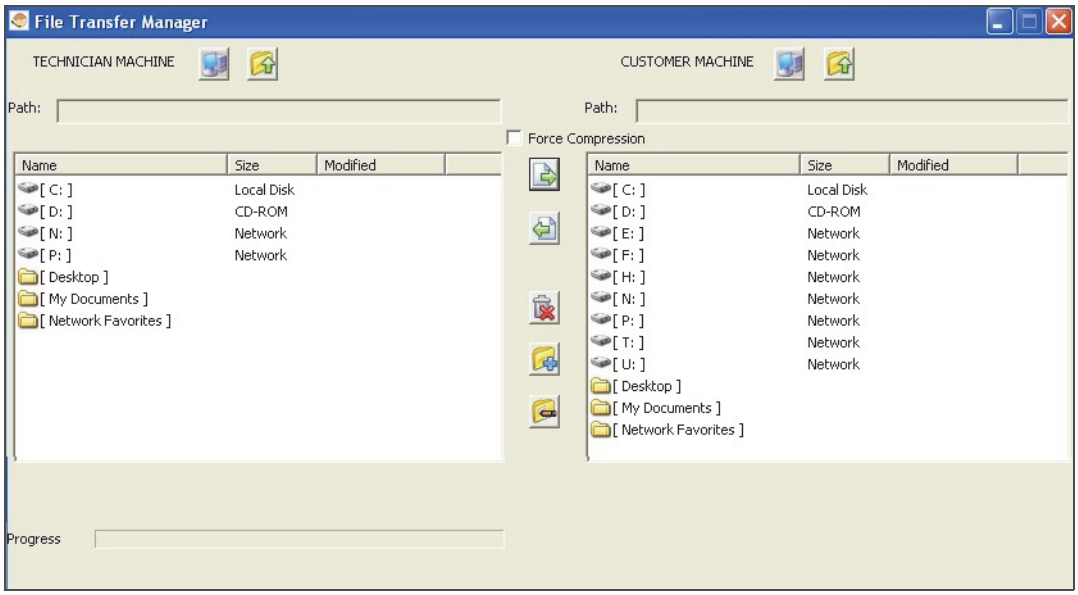
### Request Full Control

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 will appear 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 the **Exit** button to cancel a transfer in progress.

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

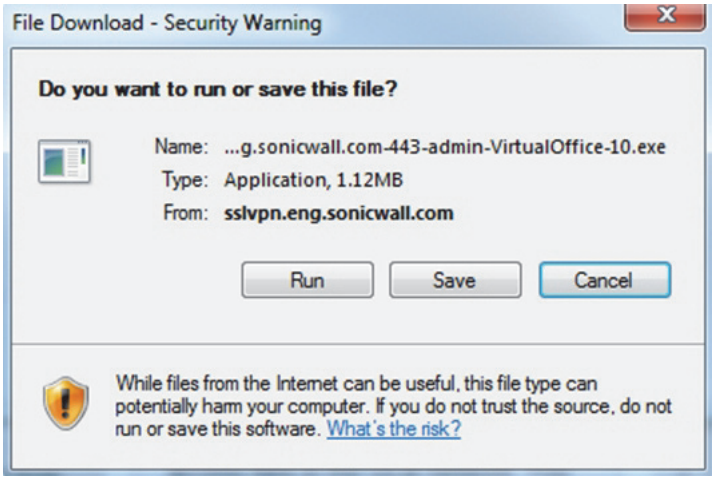
## Enabling a System for Secure Virtual Access

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

To configure Secure Virtual Access on a system:

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

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

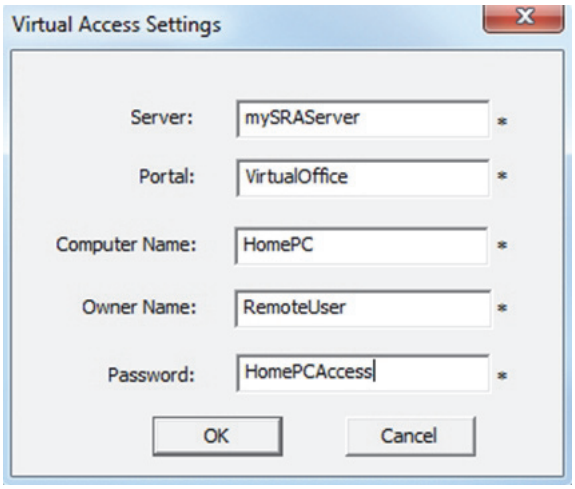



**Note** Running the file directly from this dialog box may not work on some systems. Save the file to the system and then run the application.

**Step 3** Fill in the necessary information in the provided fields to 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 login to.
- **Computer Name:** This is an identifier for the system to help differentiate between other systems that may be waiting for support in the queue.

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




**Step 4** After installation, the VASAC client should be left running in the desktop tray.

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

### Ending Secure Virtual Access Mode

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

An administrator can forcibly remove a system from the queue. If this occurs, the 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 Dell SonicWALL SRA User's Guide.

# Secure Virtual Meeting Overview

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


- What is Secure Virtual Assist? **on page 53**
- Benefits of Secure Virtual Assist on page 53
- How Does Secure Virtual Assist Work? on page 53
- Launching a Secure Virtual Assist Technician Session on page 55
- Performing Secure Virtual Assist Technician Tasks on page 58
- Enabling a System for Secure Virtual Access on page 63

## What is Secure Virtual Meeting?

Secure Virtual Meeting is a Web-based management interface for the SRA 4200 and 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

Secure Virtual Meeting provides the following benefits:

- **Secure connections** - 256-bit AES SSL encryption of the data by the SonicWALL 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 may perform several functions, such as polling meeting attendees, text chatting, and switching who shares their desktop or controls the meeting.

## User Roles

Secure Virtual Meeting has several user roles:

- **Coordinator** (Owner of the meeting) - The Coordinator must be a SonicWALL SRA user on the appliance. The Coordinator schedules, sets up, and controls the meeting. In addition, the Coordinator has the sole power to promote a Participant to the Assistant.
- **Assistant** (Coordinator-designated Assistant) - The Coordinator selects an Assistant from the list of available Participants and assigns the Assistant privileges. When the Coordinator exits the meeting, the Assistant automatically becomes the Coordinator. A meeting may have multiple Assistants, each with the same or a different set of privileges. An Assistant need not be a user of the SSL-VPN 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 may 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 may 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?

The following sections describe how Secure Virtual Meeting works, describes configuration tasks specific to the **Secure Virtual Meeting** pages on the SonicWALL SRA Web-based management interface, and how to use Secure Virtual Meeting:


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


### Configuring Secure Virtual Meeting

Secure Virtual Meeting configuration and management tasks are performed via the AMC console and consists of the following:

- Status
- Settings
- Log
- Licensing

These tasks are explained in detail in Secure Virtual Meeting chapter of the SRA Administrator's Guide and the Secure Virtual Meeting Feature Module.

### Performing Coordinator Tasks

The Virtual Meeting Coordinator performs the following tasks:

| Coordinator Tasks | Description |
|---|---|
| Logging In | Log in from a Virtual Meeting client using SRA 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 may do and appoint an Assistant to help facilitate the meeting. |

| Coordinator Tasks | Description |
|---|---|
| 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 may 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. |
| 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 performed from the lobby by clicking buttons:

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

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

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

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

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

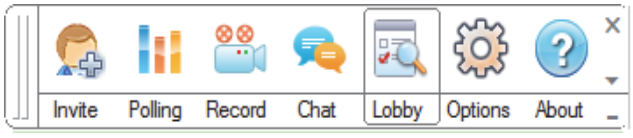
Clicking the **Start Sharing** button shares the Host desktop with all Participants in the meeting. Sharing is only available during a meeting.

Clicking the **Stop Sharing** button 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 the **Request Control** button requests that the Host give you control of the keyboard and mouse. Only Participants who aren't 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.



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

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

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

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

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

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

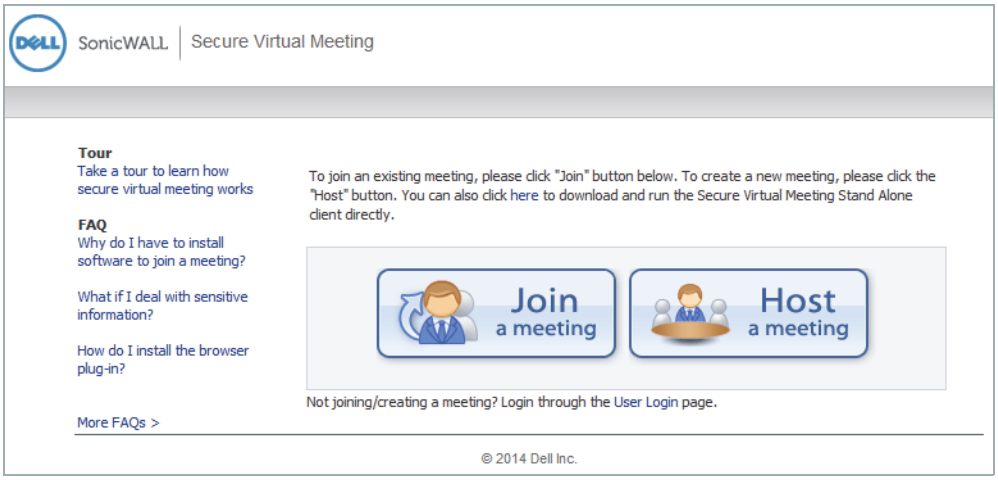
The **About** button opens the About dialog, which identifies the Secure Virtual Meeting client and version. The **About** button is available for all meeting members, including View-only Participants.

### Performing Participant Taks

Participants can be designated as View-only Participants or regular Participants. View-only Participants enter and exit meetings like other Participants, but cannot perform 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? on page 69
- Benefits of Web Application Firewall on page 72
- How Does Web Application Firewall Work? on page 72


## What is Web Application Firewall?

Web Application Firewall is subscription-based software that runs on the Dell SonicWALL SRA appliance and protects Web applications running on servers behind the SRA. Web Application Firewall also provides real-time protection for resources such as HTTP(S) bookmarks, Citrix bookmarks, offloaded Web applications, and the SRA management interface and user portal that run on the Dell SonicWALL 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. Dell SonicWALL SRA Web Application Firewall protects against these top ten, defined in 2007 as follows:

***Table 9 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. |

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

### Slowloris Protection

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

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

For more information about how Web Application Firewall protects against the OWASP top ten and Slowloris types of attacks, see How Does Web Application Firewall Work? on page 72.

### Offloaded Web Application Protection

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

### Application Profiling

Starting in SRA 5.5, 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, which adopt a negative security model. When the administrator places the device in learning mode in a staging environment, the 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

Starting in SRA 5.5, it is possible to 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 283 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. Once 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 285 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 284 for additional information.

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

Starting in SRA 5.5, 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 timeline 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. Dell SonicWALL SRA uses SSL encryption to encrypt data between the Web Application Firewall and the client. Dell SonicWALL SRA also satisfies OWASP cryptographic storage requirements by encrypting keys and passwords wherever necessary.

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

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

Deploying Web Application Firewall at the 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, which improves the proxy performance and functionality.

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

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

## How Does Web Application Firewall Work?

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

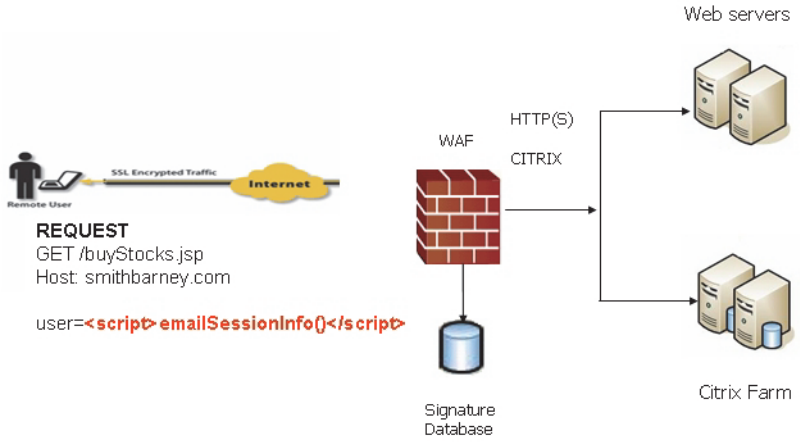
The following sections describe how Web Application Firewall and SRA appliances prevent attacks such as Slowloris or those listed in the OWASP top ten, how Web Application Firewall protects against information disclosure, and how other features work:


- How are Signatures Used to Prevent Attacks? on page 73
- How is Cross-Site Request Forgery Prevented? on page 74
- How is Information Disclosure Prevented? on page 75
- How are Broken Authentication Attacks Prevented? on page 76
- How are Insecure Storage and Communications Prevented? on page 76
- How is Access to Restricted URLs Prevented? on page 76

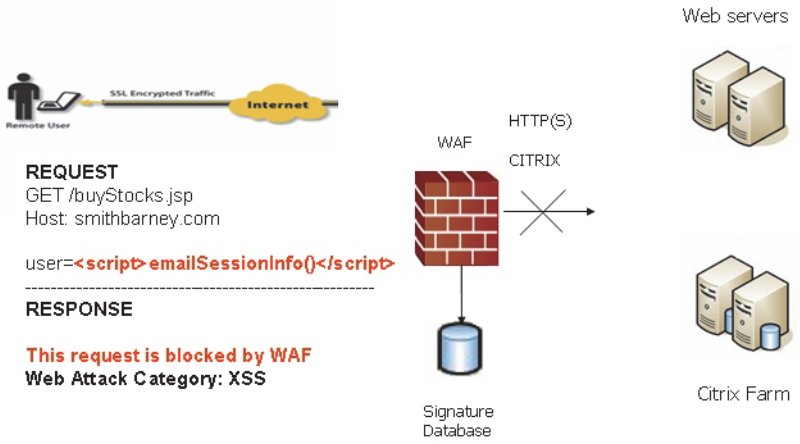
- How are Slowloris Attacks Prevented? on page 76
- What Type of PCI Compliance Reports Are Available? on page 76
- How Does Cookie Tampering Protection Work? on page 77
- How Does Application Profiling Work? on page 79
- How Does Rate Limiting for Custom Rules Work? on page 80


## How are Signatures Used to Prevent Attacks?

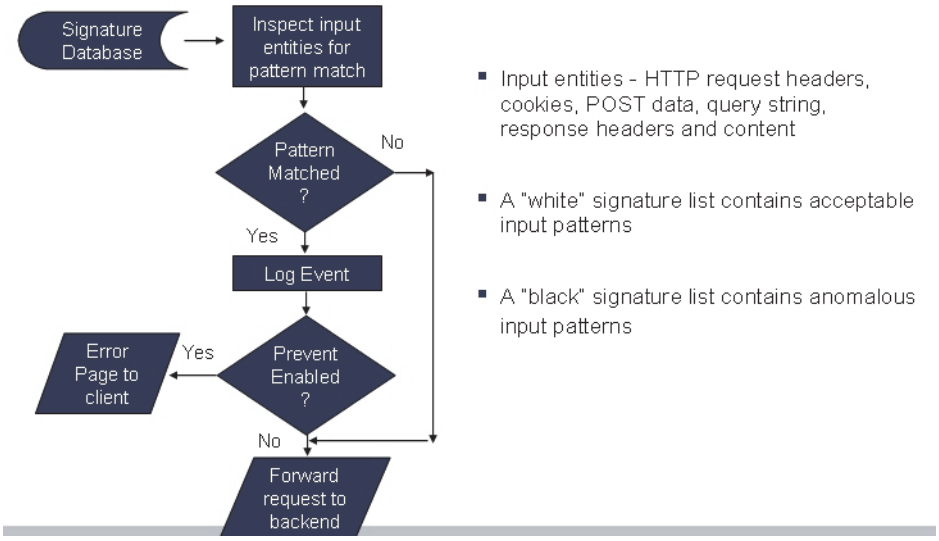
For Cross Site Scripting, Injection Flaws, Malicious File Execution, and Insecure Direct Object Reference vulnerabilities, the Web Application Firewall feature uses a black list of signatures that are known to make Web applications vulnerable. New updates to these signatures are periodically downloaded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




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



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




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

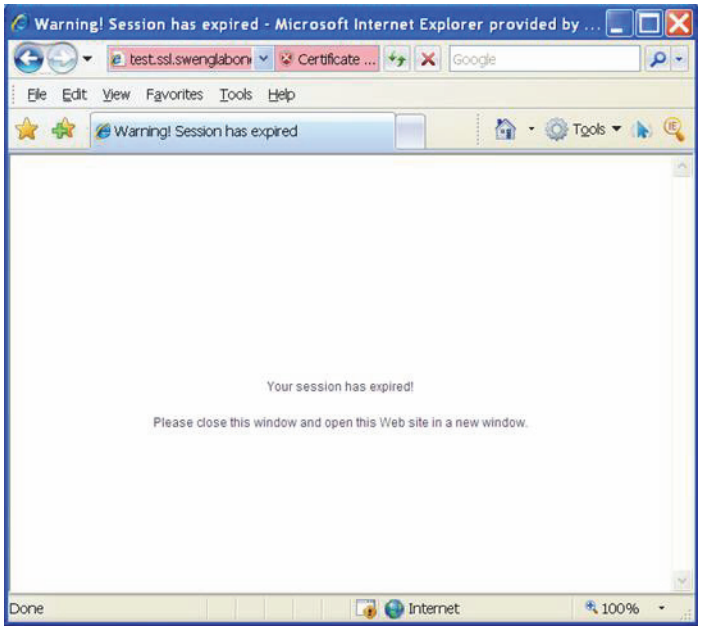
This page is customizable under Web Application Firewall > Settings in the SRA management interface. Some administrators may want to customize the HTML contents of this page. Others may not want to present a user friendly page for security reasons. Instead, they may prefer the option to present an HTTP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

## How is Cross-Site Request Forgery Prevented?

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

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

CSRF protection is provided for anonymous mode as well. If CSRF protection is enabled, then an idle timeout set to the global idle timeout is enforced for anonymous access. If the session times out, an error message is displayed, forcing the user to revisit the site in a new window. 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.

Beginning in SRA 5.5, 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. Dell SonicWALL SRA already has strong authentication capabilities with the ability to support One Time Password, Two-factor Authentication, Single Sign-On, and client certificate authentication.

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

## How are Insecure Storage and Communications Prevented?

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

## How is Access to Restricted URLs Prevented?

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

## How are Slowloris Attacks Prevented?

Slowloris attacks can be prevented if there is an upstream device, such as a Dell SonicWALL 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

An example is shown below:

Model: SRA 4200

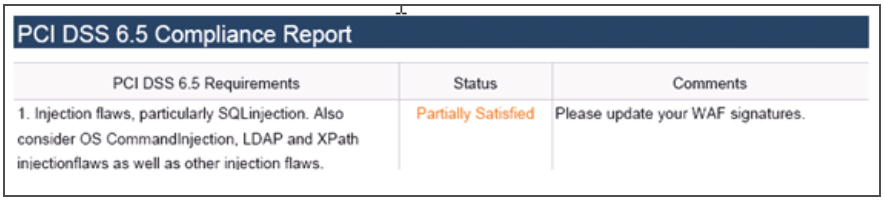
Serial Number: 0017C552EE24

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 below:



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 4 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?

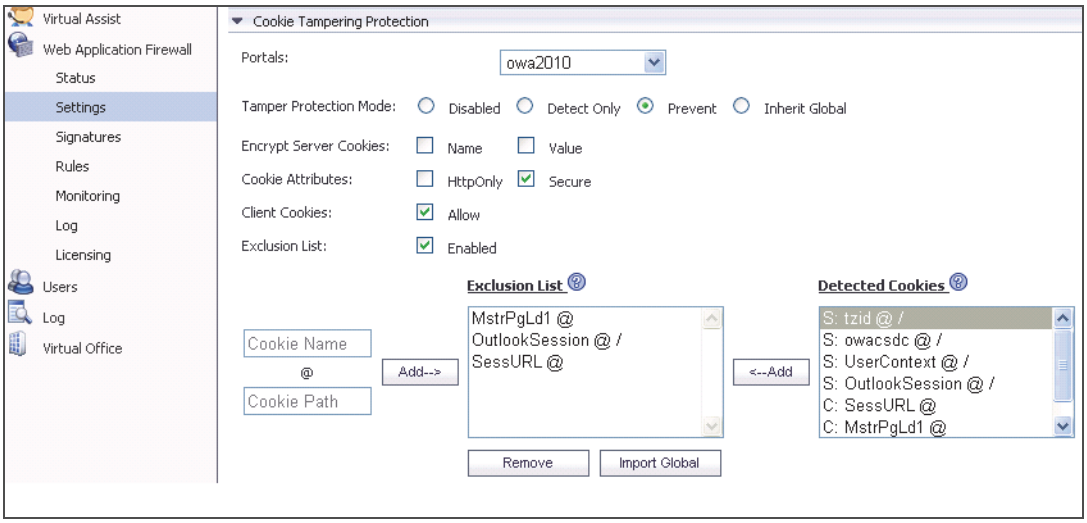
SRA appliances protect important server-side cookies from tampering.

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 will have its own setting. 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, which 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.

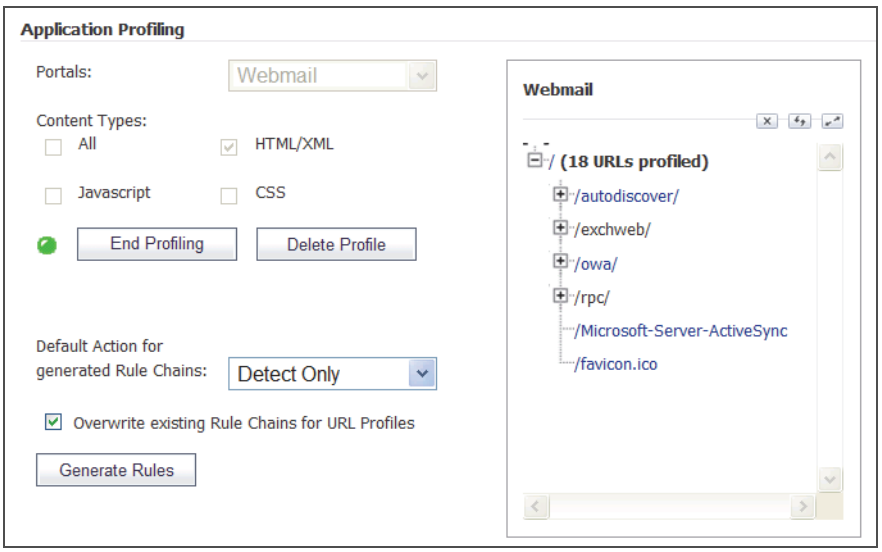
**Import Global** – Application Offloading portals can import the Global exclusion list.

## How Does Application Profiling Work?

The administrator can configure application profiling on the Web Application Firewall > Rules page. Application profiling is performed 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**, which 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 SRA appliance is placed in learning mode by clicking on the **Begin Profiling** button (the button then changes to **End Profiling**). The profiling should be done while trusted users are using applications in an appropriate way. The SRA 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 SRA 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 may 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 the **End Profiling** button 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 will be disabled rather than active.
- **Detect Only** – Content triggering the generated rule will be detected and logged.
- **Prevent** – Content triggering the generated rule will be blocked and logged.

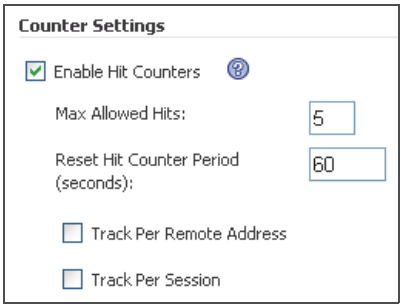
If a rule chain has already been generated from a URL profile in the past, then the rule chain will be overwritten only if the **Overwrite existing Rule Chains for URL Profiles** check box is selected. When you click the **Generate Rules** button, the rules are generated from the URL profiles. If a URL 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 management interface for administrators to use as reference.

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




Once 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. The **Track Per Remote Address** check box enables rate limiting based on the attacker's remote IP address.

The **Track Per Session** check box 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 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 will be counted together.

# Navigating the SRA Management Interface

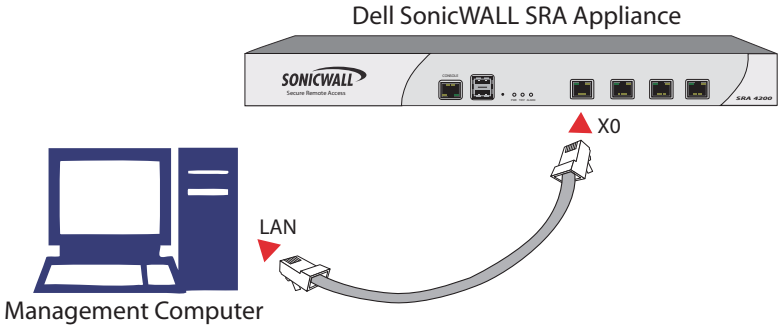
The following sections describe how to navigate the SRA management interface:


- Management Interface Introduction on page 81
- Navigating the Management Interface on page 82
- Navigation Bar on page 86

# Management Interface Introduction

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

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




**Step 2** Set the computer you use to manage your 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 *Dell SonicWALL SRA Getting Started Guide* for your model.

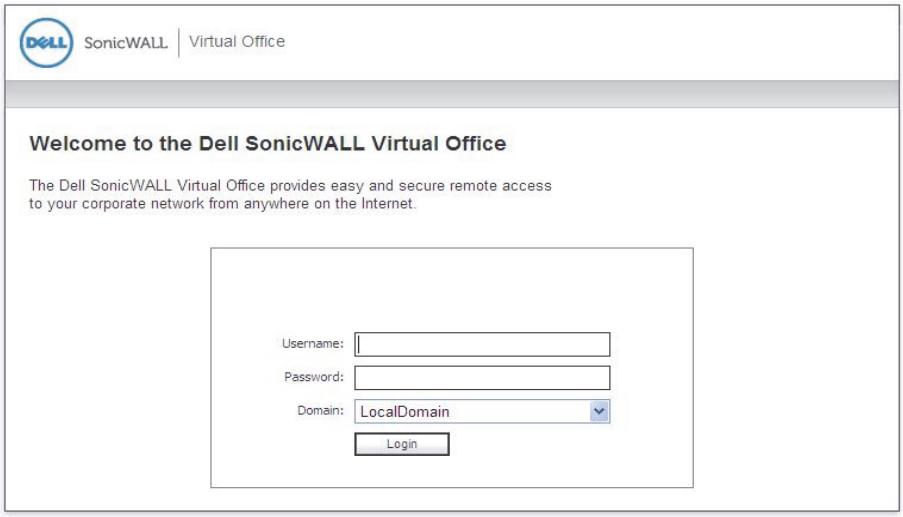
**Note** For configuring the SRA appliance using the Web-based management interface, a Web browser supporting Java and HTTP uploads, such as Internet Explorer 8 or higher, Firefox 16.0 or higher, or Chrome 22.0 or higher is recommended. Users will need to use IE 8 or higher, supporting JavaScript, Java, cookies, SSL and ActiveX in order to take advantage of the full suite of SRA applications.

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

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

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

**Note** The number and duration of login attempts can be controlled by the use of the SRA auto-lockout feature. For information on configuring the auto-lockout feature, refer to Configuring Login Security on page 113.




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

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

The **System**, **Network**, **Portals**, **NetExtender**, **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.

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

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

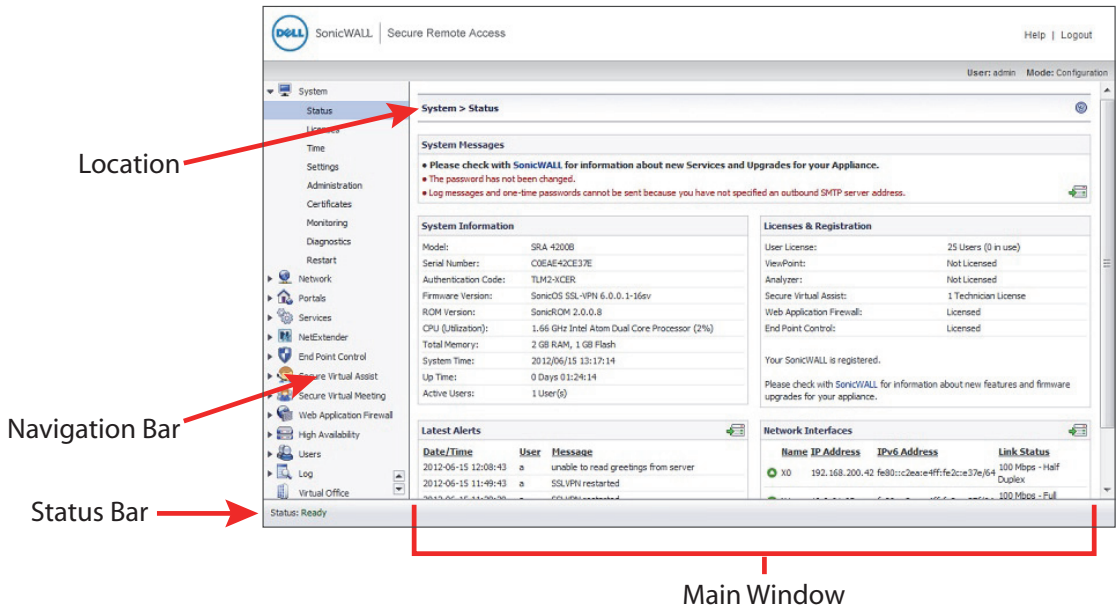
# Navigating the Management Interface

The SRA Web-based management interface allows the administrator to configure the SRA appliance. The management interface contains top level, read-only windows and configuration windows:

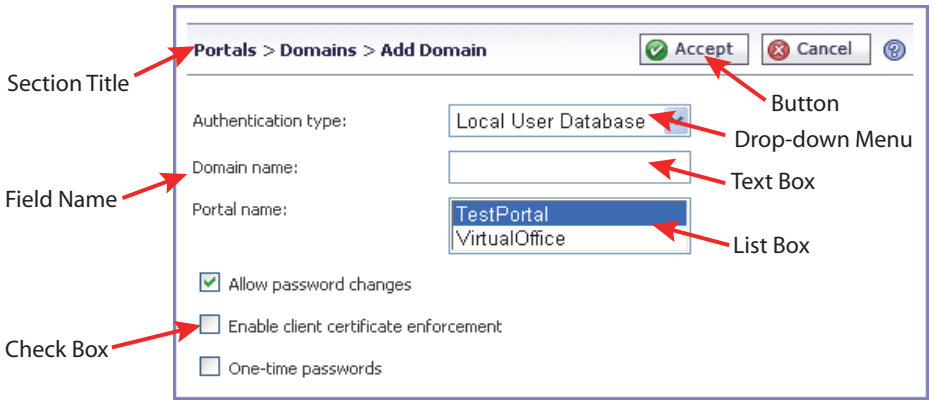
- Windows - Displays information in a read-only format.
- Configuration windows - Enables administrator interaction to add and change values that characterize objects. For example, IP addresses, names, and authentication types.

Figure 5 is a sample window in the Web-based management interface. Note the various elements of a standard SRA interface window.

***Figure 5 System > Status Page***




The following is a sample configuration window:




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

- Status Bar on page 84
- Accepting Changes on page 84
- Navigating Tables on page 84
- Restarting on page 85
- Common Icons in the Management Interface on page 85
- Tooltips in the Management Interface on page 85
- Getting Help on page 86
- Logging Out on page 86

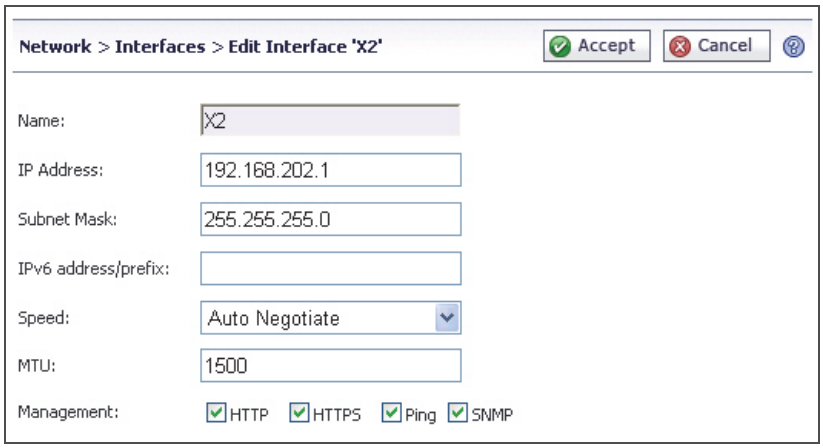
## Status Bar

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

## Accepting Changes

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

If the settings are contained in a secondary window within the management interface, the **Accept** button 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:

***Figure 6 Log > View***

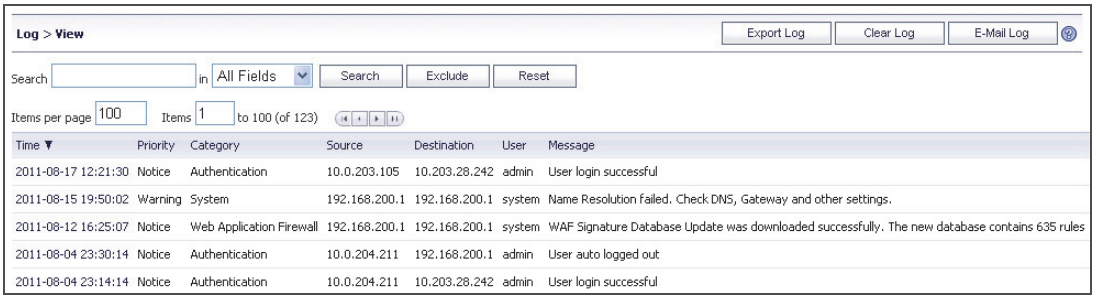


*Table 10 Navigation Buttons in the Log View Page*

| 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 SRA appliance.

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

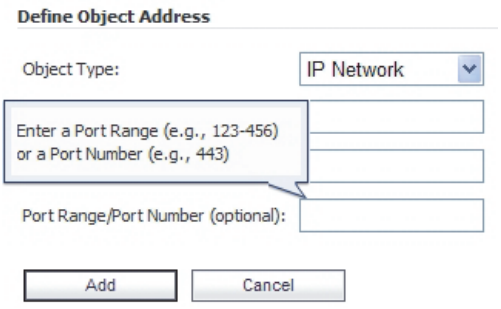
## Common Icons in the Management Interface

The following icons are used throughout the SRA management interface:

- Clicking on the configure icon displays a window for editing the settings.
- Clicking on the delete icon deletes a table entry.
- Moving the pointer over the comment icon displays text from a **Comment** field entry.

## Tooltips in the Management Interface

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



### Getting Help

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

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 SRA appliance online help requires an active Internet connection.

### Logging Out

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

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

## Navigation Bar

The SRA navigation bar is located on the left side of the SRA 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 SRA appliance. This section contains the following subsections:


- Support for Numbers of User Connections on page 87
- Resource Type Support on page 87
- Integration with Dell SonicWALL Products on page 87
- Typical Deployment on page 88
- Two-armed Deployment on page 88

# Support for Numbers of User Connections

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

| Appliance Model | Maximum Concurrent Tunnels Supported | Recommended Number of Concurrent Tunnels |
|---|---|---|
| SRA 1200/1600 | 50 | 20 |
| SRA 4200/4600 | 500 | 50 |
| SRA Virtual Appliance | 500 | 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 SRA appliance.

| Access Mechanism | Access Types |
|---|---|
| Standard Web browser | • Files and file systems, including support for FTP and Windows Network File Sharing<br>• Web-based applications<br>• Microsoft Outlook Web Access and other Web-enabled applications<br>• HTTP and HTTPS intranets |
| NetExtender | • Any TCP/IP based application including:<br>– Email access through native clients residing on the user's laptop (Microsoft Outlook, Lotus Notes, etc.)<br>– Commercial and home-grown applications<br>• 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<br>• Terminal services, RDP, VNC, Telnet, SSH, and Citrix |

# Integration with Dell SonicWALL Products

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

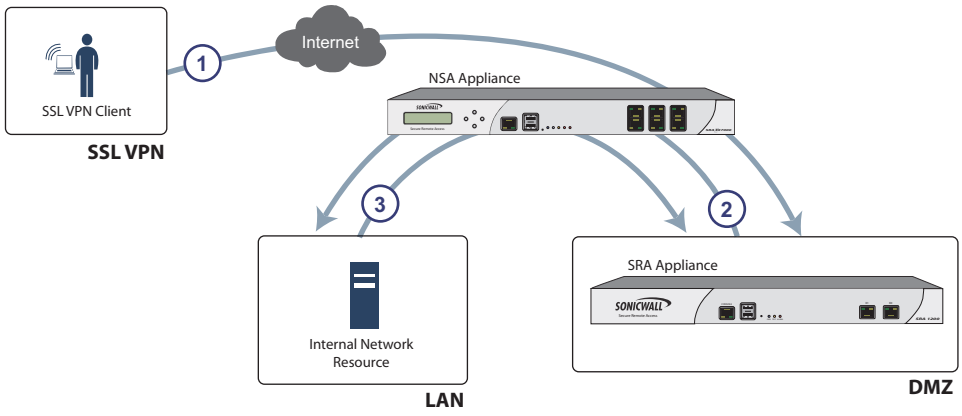
# Typical Deployment

The 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 Dell SonicWALL network security appliance, such as a NSA 4500.

This method of deployment offers additional layers of security control plus the ability to use Dell SonicWALL's Unified Threat Management (UTM) services, including Gateway Anti-Virus, Anti-Spyware, Content Filtering and Intrusion Prevention, to scan all incoming and outgoing NetExtender traffic. Dell SonicWALL 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 belowFigure 7, in one-armed mode the primary interface (X0) on the SRA appliance connects to an available segment on the gateway device. The encrypted user session is passed through the gateway to the SRA appliance (step 1). The SRA appliance decrypts the session and determines the requested resource. The SRA 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 SRA appliance through the gateway (step 3) where it is encrypted and returned to the client.

***Figure 7 Sequence of Events in Initial Connection***




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

For information about configuring the SRA appliance to work with third-party gateways, refer to Configuring the SRA Appliance with a Third-Party Gateway on page 411.

# Two-armed Deployment

The 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 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 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 SRA appliance, client requests destined for internal resources on the corporate network can be delivered to an internal router.

# Chapter 3

# System Configuration

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

This chapter contains the following sections:


- System > Status on page 91
- System > Licenses on page 96
- System > Time on page 104
- System > Settings on page 106
- System > Administration on page 111
- System > Certificates on page 115
- System > Monitoring on page 119
- System > Diagnostics on page 121
- System > Restart on page 126


# System > Status

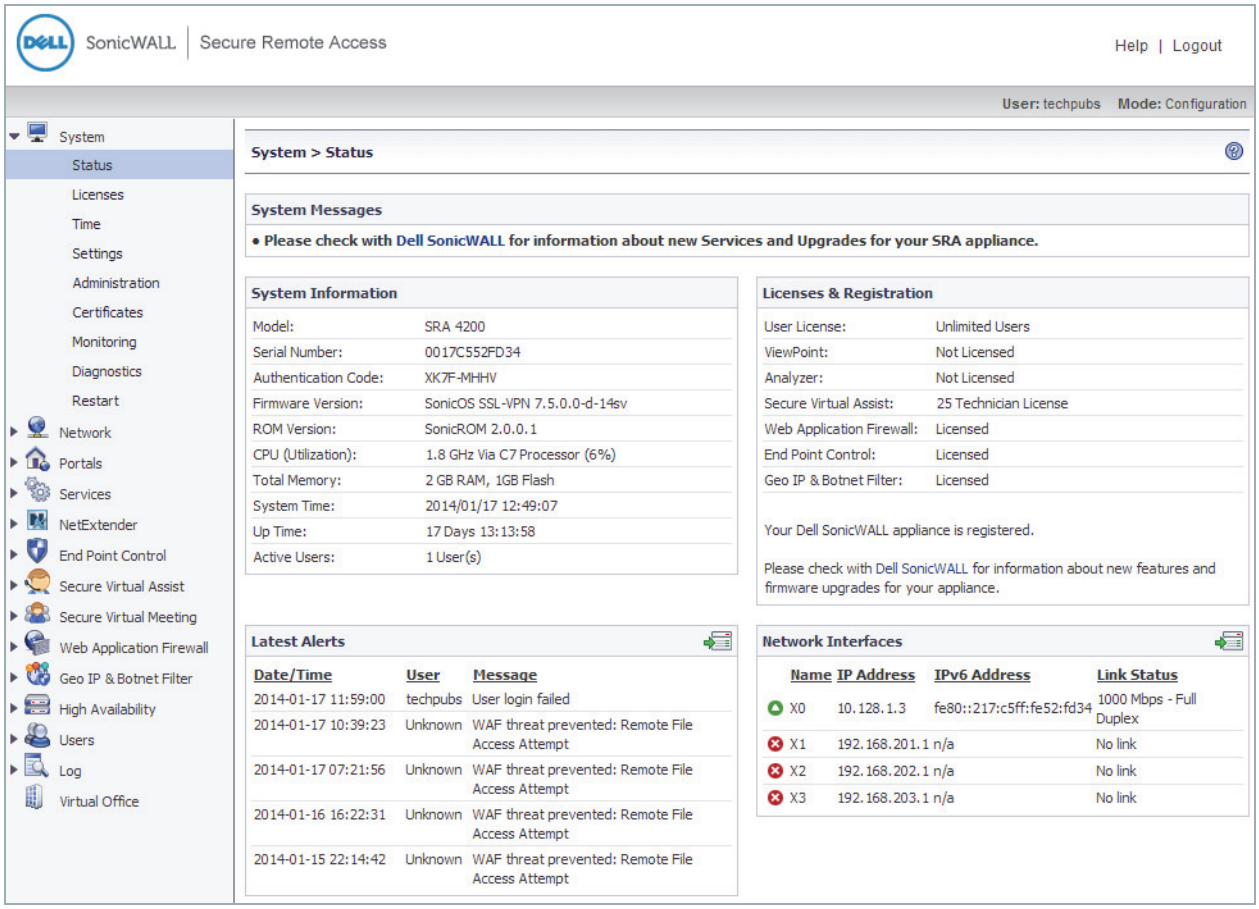
This section provides an overview of the **System > Status** page and a description of the configuration tasks available on this page.


- System > Status Overview on page 92
- Registering Your SRA Appliance from System Status on page 94
- Configuring Network Interfaces on page 96

# System > Status Overview

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

***Figure 8 System > Status Page***




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

- System Messages on page 92
- System Information on page 93
- Latest Alerts on page 93
- Licenses & Registration on page 93
- Network Interfaces on page 94

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

***Table 11 System Information***

| Field | Description |
|---|---|
| Model | The type of SRA appliance. |
| Serial Number | The serial number or the MAC address of the SRA appliance. |
| Authentication Code | The alphanumeric code used to authenticate the SRA appliance on the registration database at <https://www.mysonicwall.com>. |
| Firmware Version | The firmware version loaded on the SRA appliance. |
| ROM Version | Indicates the ROM version. The ROM code controls low-level functionality of the appliance. |
| CPU (Utilization) | The type of the 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 SRA appliance has been active since its most recent restart. |
| Active Users | The number of users who are currently logged into the management interface of the 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 SRA appliance. The status of your Analyzer, ViewPoint, Secure Virtual Assist, Spike License, 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 SRA Appliance from System Status on page 94.

To register your appliance on MySonicWALL from the **System > Licenses** page and allow the appliance to automatically synchronize registration and license status with the Dell SonicWALL server, see Registering the SRA Appliance from System > Licenses on page 98.

## Network Interfaces

The Network Interfaces section provides the administrator with a list of 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 96.

# Registering Your SRA Appliance from System Status

Register with MySonicWALL to get the most out of your 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 Dell SonicWALL SRA are correct before you register your appliance. These settings are generally configured during the initial 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 105, Configuring DNS Settings on page 131 and Configuring a Default Route for the SRA Appliance on page 133.

**Note** You need a MySonicWALL account to register the Dell SonicWALL SRA.

### Creating a MySonicWALL Account from System > Licenses

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

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

Do one of the following:

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

**Step 3** Follow the instructions to activate your MySonicWALL account.

## Registering with MySonicWALL

There are two ways to register your SRA appliance:

- Log into your MySonicWALL account directly from a browser or click the **Dell SonicWALL** link on the **System > Status** page to access MySonicWALL, enter the appliance serial number and other information there, and then enter the resulting registration code into the field on the **System > Status** page. This manual registration procedure is described in this section.

- Use the link on the **System > Licenses** page to access MySonicWALL, then enter the serial number and other information into MySonicWALL. When finished, your view of the **System > Licenses** page shows that the appliance has been automatically synchronized with the licenses activated on MySonicWALL. This procedure is described in Registering the SRA Appliance from System > Licenses on page 98.

To register your SRA appliance:

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

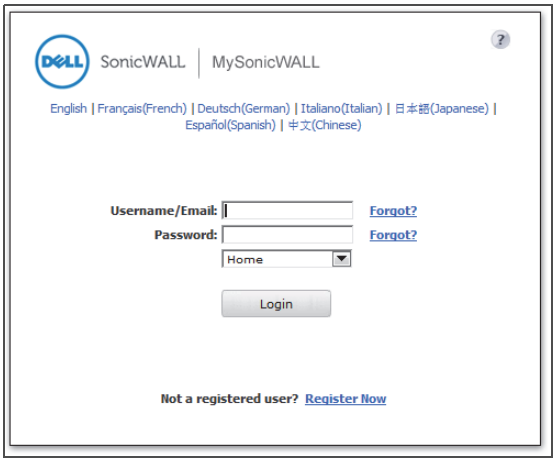
**Step 2** If the **System > Status** page is not automatically displayed in the management interface, click **System** in the left-navigation menu, and then click **Status**.

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

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

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

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




**Step 5** Enter your MySonicWALL account user name and password.

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

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

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

**Step 8** Enter a descriptive name for your SRA appliance in the **Friendly Name** field.

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

**Step 10** Click the **Register** button.

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

**Step 12** On the **System > Status** page of the SRA appliance 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 SRA appliance may be configured by clicking on the blue arrow in the corner of the Network Interfaces section of the **System > Status** page. The link redirects you to the **Network > Interfaces** page, which can also be accessed from the navigation bar. From the **Network > Interfaces** page, a 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 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 127.

# 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 on page 96
- Registering the SRA Appliance from System > Licenses on page 98
- Activating or Upgrading Licenses on page 100

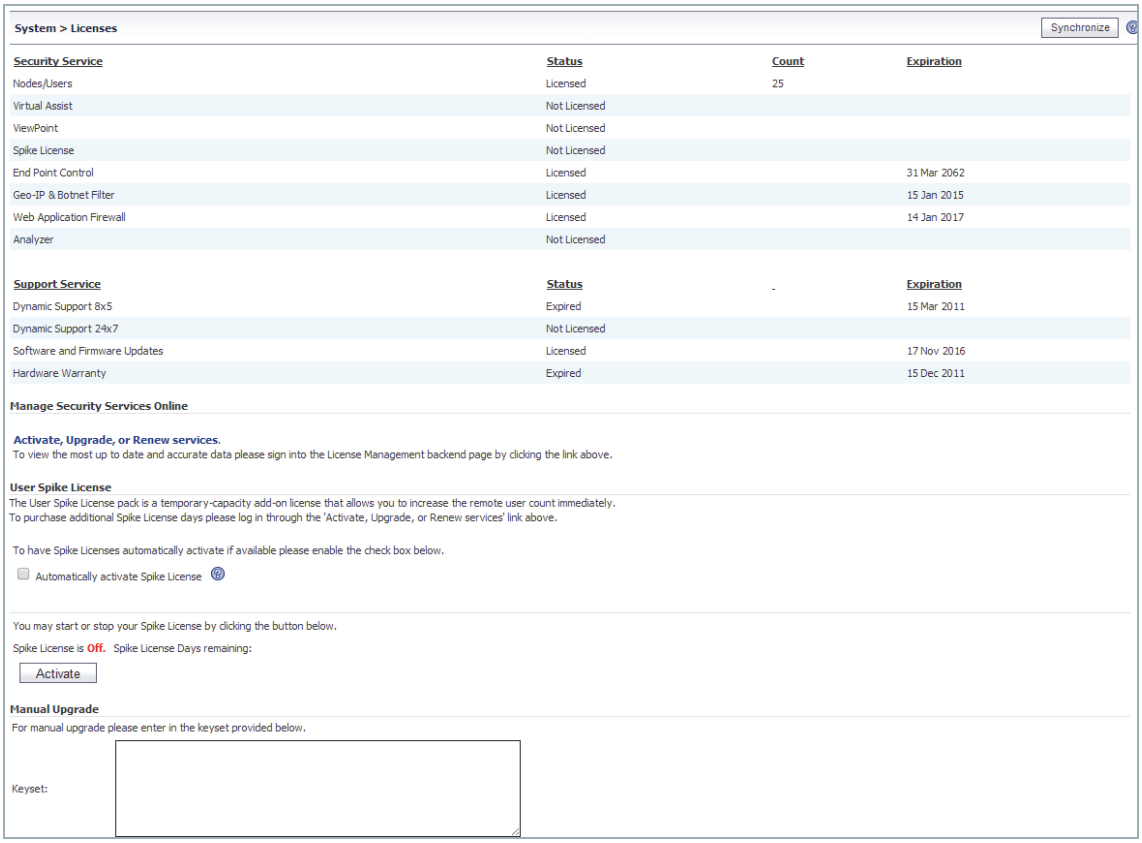

## System > Licenses Overview

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

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

The **System > Licenses** page provides a link to activate, upgrade, or renew Dell SonicWALL Security Services licenses. From this page in the SRA management interface, you can manage all the Dell SonicWALL Security Services licenses for your SRA appliance.

***Figure 9 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 SRA appliance.

The **Security Service** column lists all the available Dell SonicWALL 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, and Web Application Firewall are licensed separately as upgrades.

The number of nodes/users allowed by the license is displayed in the **Count** column. A node is a computer or other device connected to your SRA appliance with an IP address. This number refers to the maximum number of simultaneous connections to the 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 Dell SonicWALL licensing server every time the SRA appliance automatically synchronizes with it (hourly), or you can click the **Synchronize** button to synchronize immediately.

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

### Manage Security Services Online

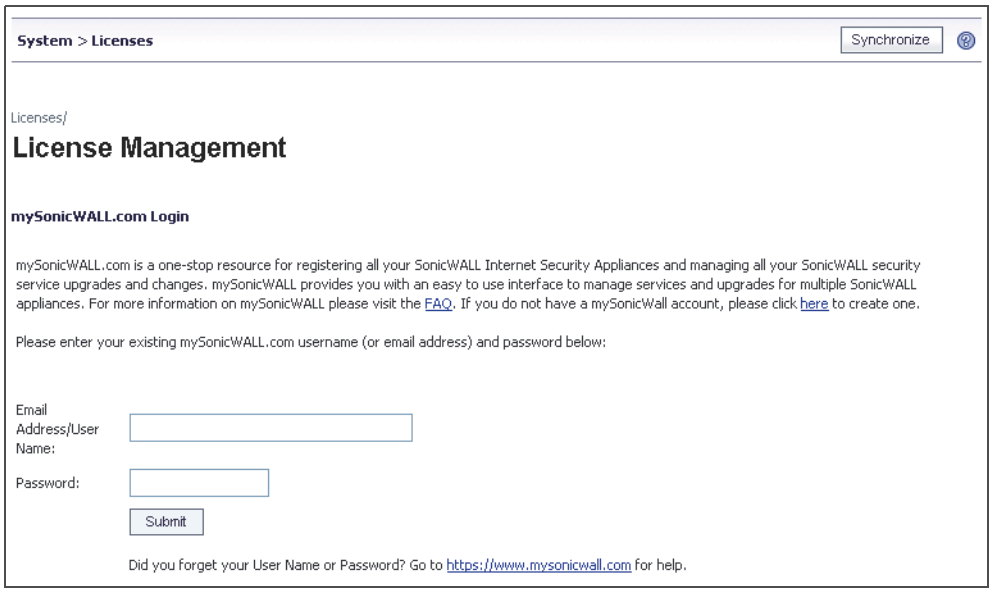
You can login to MySonicWALL directly from the **System > Licenses** page by clicking the link **Activate, Upgrade, or Renew services**. You can click this link to register your appliance, to purchase additional licenses for upgrading or renewing services, or to activate free trials.

## Registering the SRA Appliance from System > Licenses

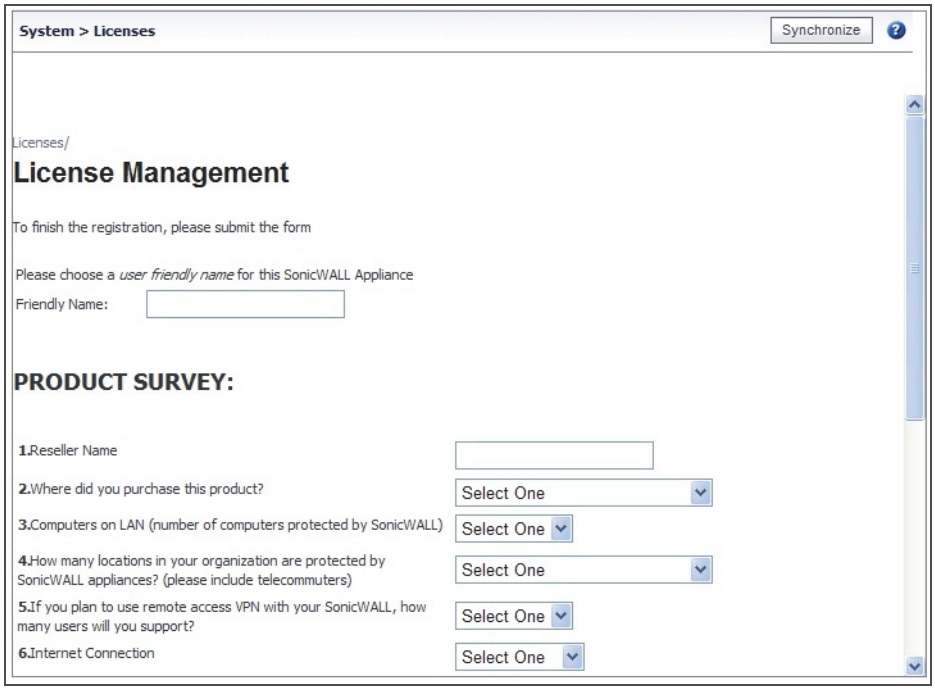
On a new SRA appliance or after upgrading to SRA 5.5 firmware from an earlier release, you can register your appliance from the **System > Licenses** page.

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

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

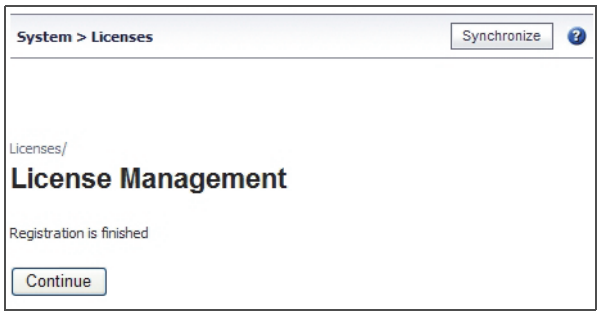



**Step 2** Enter your MySonicWALL user name and password into the fields and then click **Submit**. The display changes.



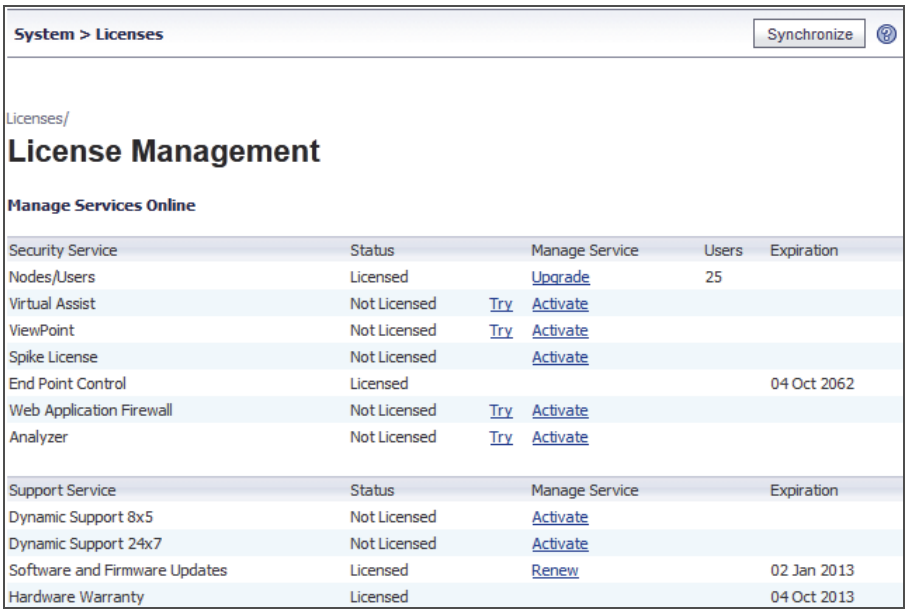

**Step 3** Enter a descriptive name for your SRA appliance in the **Friendly Name** field.

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




**Step 5** Click **Continue**.

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

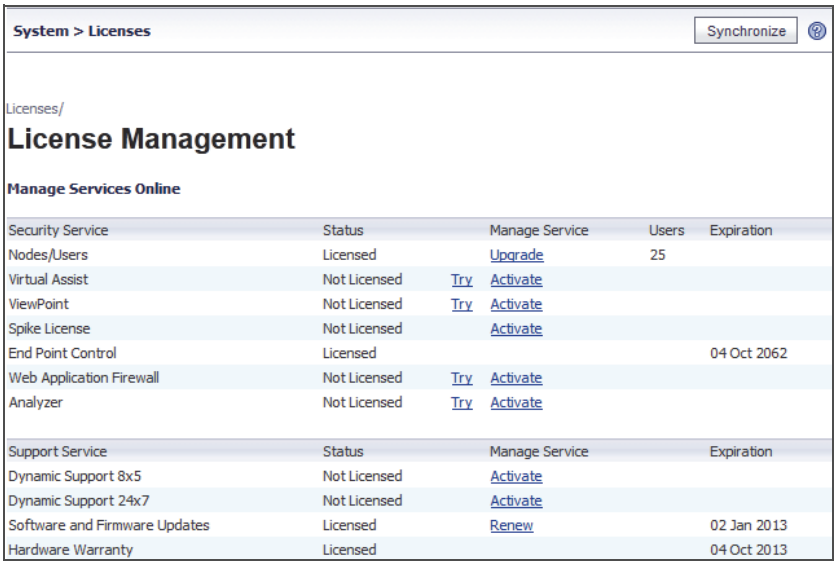



**Note** After registration, some network environments require the SRA appliance to be offline so that it is unable to connect to the Dell SonicWALL licensing server. In this mode, the appliance will still honor the valid licenses; however, timed-based licenses may not be valid.

# Activating or Upgrading Licenses

After your 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 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.

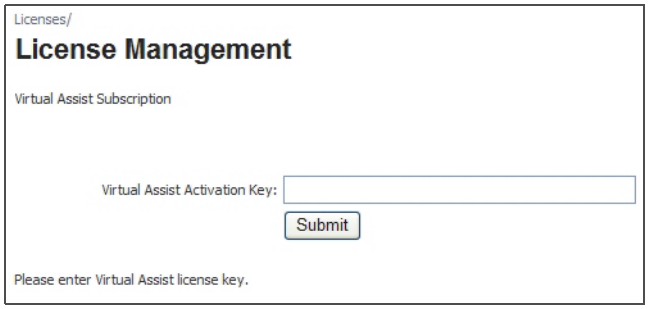
To activate or upgrade licenses or free trials on your appliance:

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

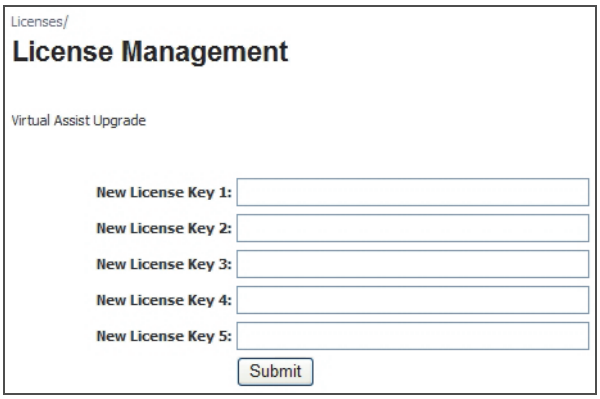
**Step 2** Enter your MySonicWALL user name and password into the fields and then click **Submit**. The display changes to show the status of your licenses. The services can have a **Try** link, an **Activate** link, or an **Upgrade** link.

**Step 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 Dell SonicWALL product subscription at any time during or after the trial. Click **Continue**, and follow the setup instructions.

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




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




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

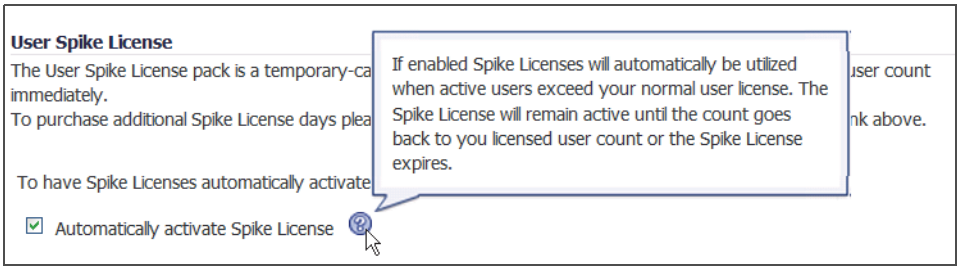
## Using a Spike License

A Spike License enables you to temporarily increase the number of remote users your appliance or 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.

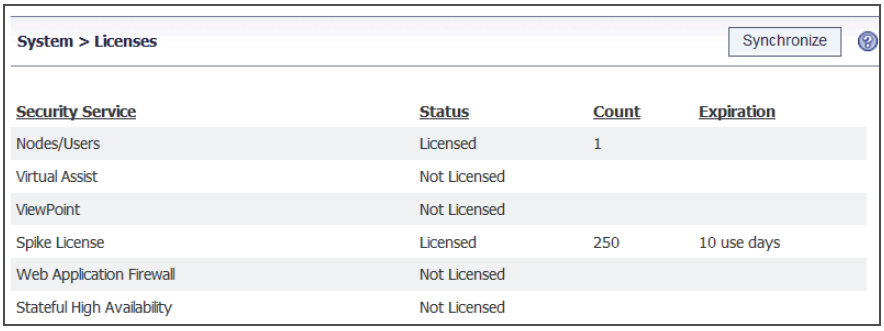
More than one Spike Licenses can be uploaded to your appliance, but only one can be active at a time.

An option is available to automatically enable and disable the license depending on the number of user connections. Select the **Automatically activate Spike License** check box to enable it. If this option is enabled, the Spike License will be 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.



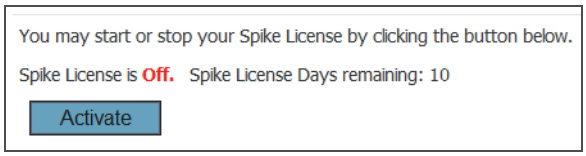
To activate or stop a Spike License, perform the following steps:

**Step 1** Purchase your Spike License from MySonicWALL and import it to the appliance, as described in Activating or Upgrading Licenses on page 100. 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.

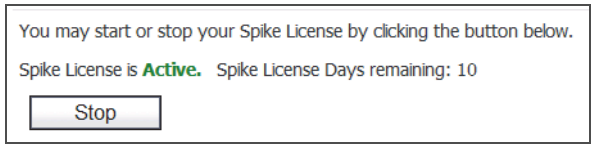



| Security Service | Status | Count | Expiration |
|---|---|---|---|
| Nodes/Users | Licensed | 1 | |
| Virtual Assist | Not Licensed | | |
| ViewPoint | Not Licensed | | |
| Spike License | Licensed | 250 | 10 use days |
| Web Application Firewall | Not Licensed | | |
| Stateful High Availability | Not Licensed | | |

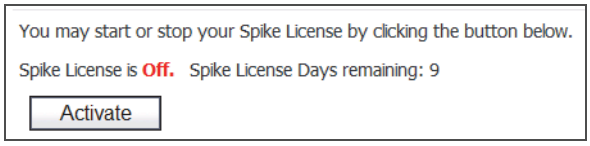
**Step 2** After reloading the page, the Spike License is listed as *Off* on the System > Licenses page.




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



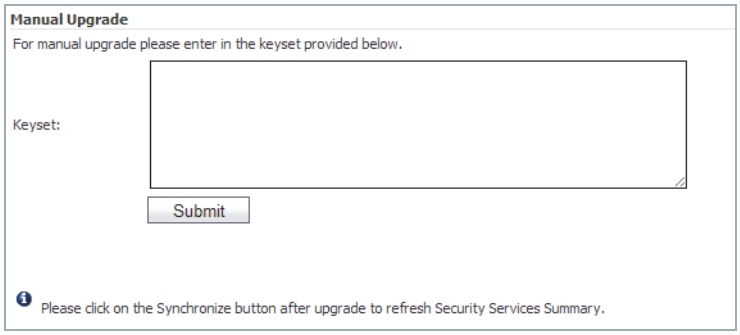

**Step 4** To stop an active Spike License, click the **Stop** button. The status goes back to *Off*, and the number of days remaining is updated.




**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 will be 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 the **Synchronize** button 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

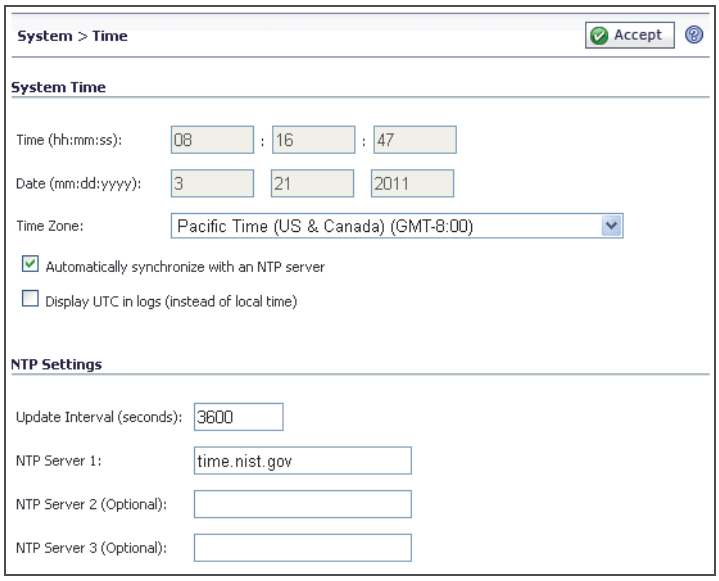
This section provides an overview of the **System > Time** page and a description of the configuration tasks available on this page.


- System > Time Overview on page 105
- Setting the Time on page 105
- Enabling Network Time Protocol on page 106

# System > Time Overview

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

***Figure 10 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 SRA appliance must have the correct time and date configured.

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

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

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

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

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

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

## Enabling Network Time Protocol

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

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

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

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

**Step 3** In the NTP Settings section, enter the time interval in seconds to synchronize time settings with the NTP server in the **Update Interval** field. If no period is defined, the appliance will select the default update interval, 3600 seconds.

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

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

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

# System > Settings

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

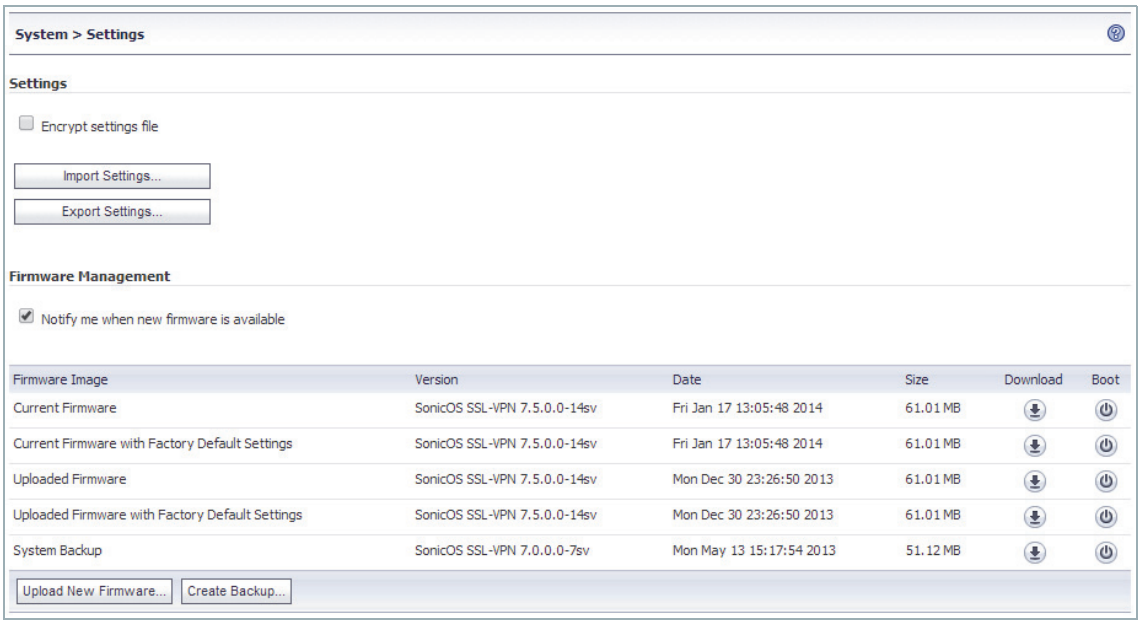

- System > Settings Overview on page 106
- Managing Configuration Files on page 108
- Managing Firmware on page 110


## System > Settings Overview

The **System** > **Settings** page allows the administrator to import and export the settings of the SRA appliance.

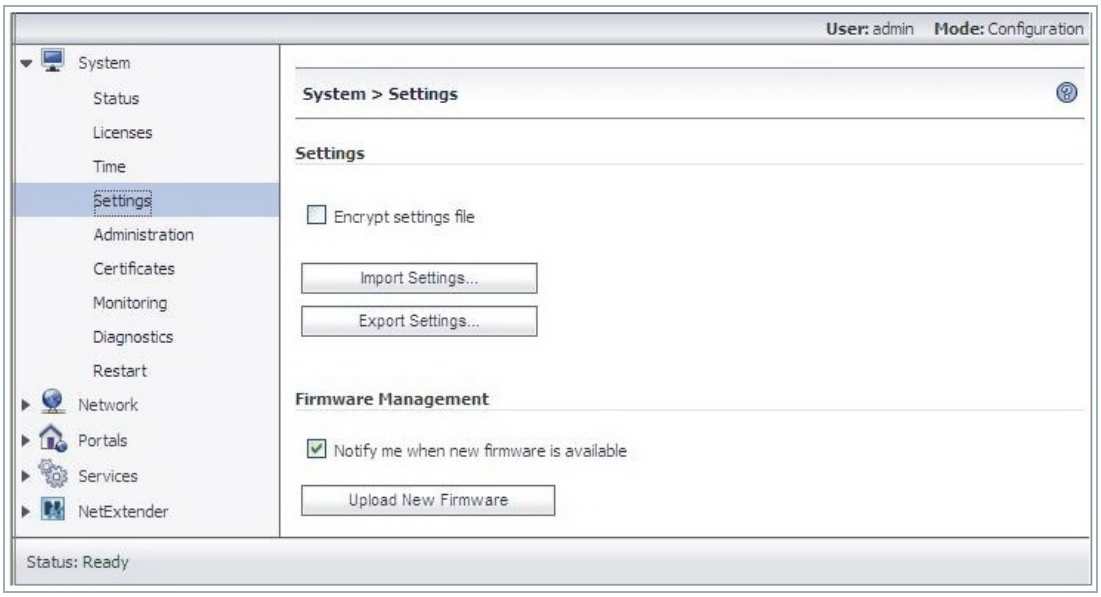
On a physical appliance, the **System** > **Settings** page provides a way to upload new firmware, and to boot either the current firmware, newly uploaded firmware, or backup firmware.

***Figure 11 System > Settings Page - Physical Appliance***




On a virtual appliance, the **System** > **Settings** page allows for settings management, but does not provide any firmware management, because the SRA Virtual Appliance is itself a software image.

***Figure 12 System > Settings Page - Virtual Appliance***




## Settings

The Settings page provides buttons to import settings and export settings, and allows the administrator to encrypt the settings file.

## Firmware Management

The Firmware Management section allows the administrator to control the firmware that is running on the 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. There is also an option to be notified when new firmware becomes available.

# Managing Configuration Files

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

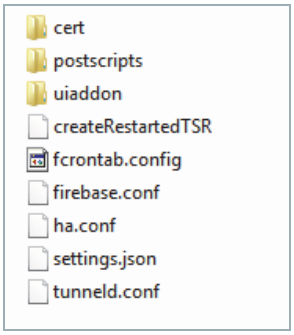
These tasks are described in the following sections:


- Exporting a Backup Configuration File on page 108
- Importing a Configuration File on page 109
- Encrypting the Configuration File on page 109


## Exporting a Backup Configuration File

Exporting a backup configuration file allows you to save a copy of your configuration settings on your local machine. You may then save the configuration settings or export them to a backup file and import the saved configuration file at a later time, if necessary. The backup file is called **sslvpnSettings-serialnumber.zip** by default, and includes the contents shown in the following figureFigure 13.

***Figure 13 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 generatd when the Schedule TSR is enabled.

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

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

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

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

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

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

## Importing a Configuration File

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

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

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

**Note** Settings can be imported between the 1200 and 1600 and between the 4200 and 4600. Due to feature differences between some platforms, importing settings from the 1200/1600 to the 4200/4600 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.

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

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

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

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

## Encrypting the Configuration File

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

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

# Managing Firmware

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

These tasks are described in the following sections:


- Setting Firmware Notification 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 the **Notify me when new firmware is available** check box.

## Creating a Backup

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

## Downloading Firmware

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

## Booting a Firmware Image

To boot a firmware image, perform the following steps:

**Step 1** Click the boot icon next to the Firmware Image version that you want to run on the SRA appliance.

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

### Uploading New Firmware

To upload new firmware, perform the following steps:

**Step 1** Login to MySonicWALL.

**Step 2** Download the latest SRA firmware version.

**Step 3** In the SRA management interface, navigate to the **System > Settings** page.

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

**Step 5** Click **Browse**.

**Step 6** Select the downloaded SRA firmware. It should have a .sig file extension.

**Step 7** Click **Open**.

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

**Step 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.

# 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 on page 111
- Configuring Login Security on page 113
- Configuring HTTP DOS Settings on page 114
- Enabling GMS Management on page 114
- Configuring Web Management Settings on page 114
- Configuring SNMP Settings on page 114

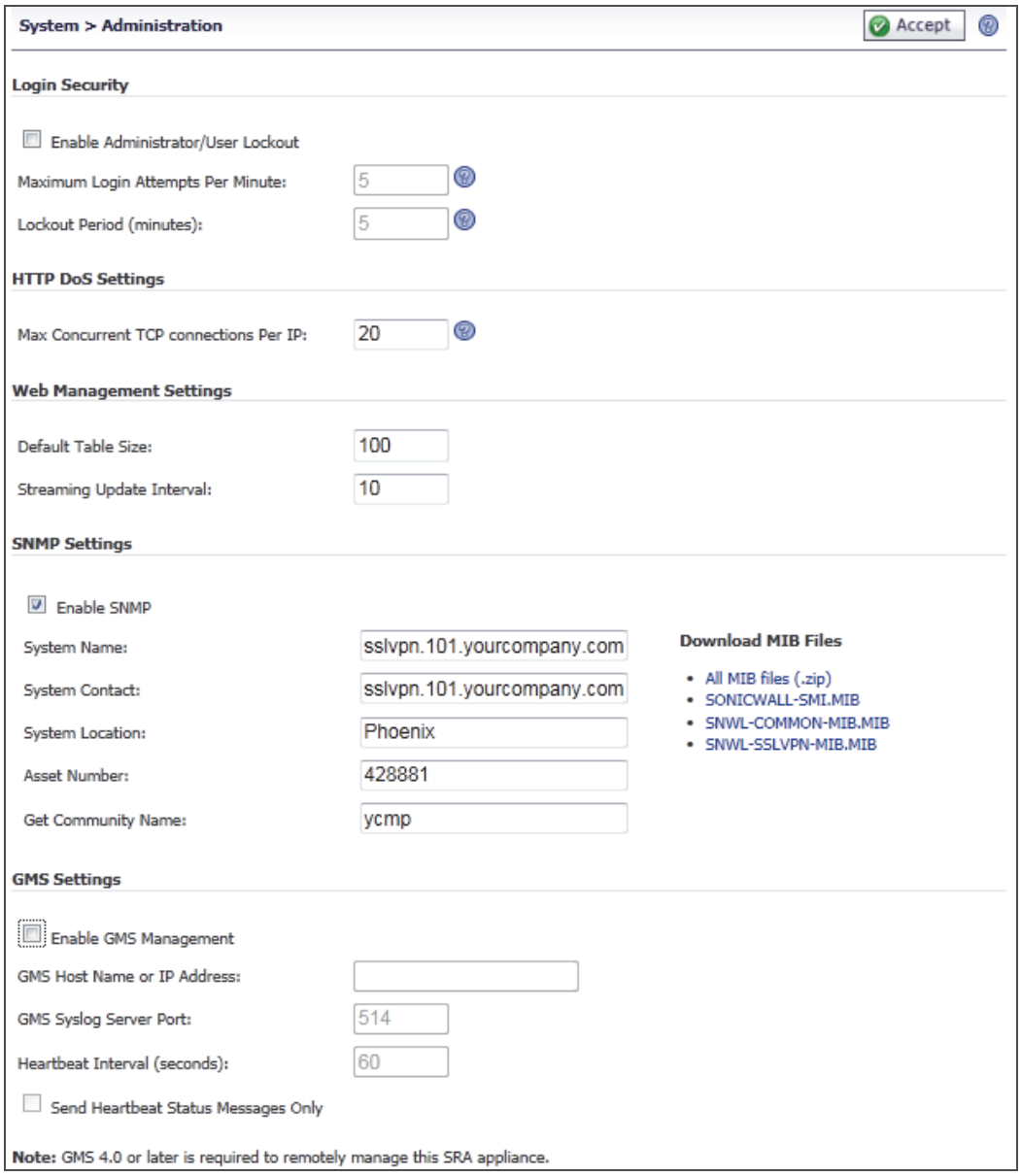

## System > Administration Overview

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

See the following sections:


- Login Security on page 112
- HTTP DOS Settings on page 112
- Web Management Settings on page 113
- SNMP Settings on page 113
- GMS Settings on page 113

*Figure 14 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 SRA web server.

## Web Management Settings

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

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

- 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 1 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

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:

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

**Step 2** Select the **Enable Administrator/User Lockout** check box.

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

**Step 4** In the **Lockout Period (minutes)** field, type a number of minutes to lockout a user that has exceeded the number of maximum login attempts. The default is 5 minutes. The maximum is 9999 minutes.

**Step 5** Click the **Accept** button 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:

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

**Step 2** In the **Max Concurrent TCP connections Per IP** field, type the maximum number of concurrent TCP connections a client can open with the SRA web server. The default is 20 attempts. 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 management interface.

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

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

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

**Step 3** Click the **Accept** button to save your changes.

# Configuring SNMP Settings

To configure the SNMP Settings fields:

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

**Step 2** Select the **Enable SNMP** check box.

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

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

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

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

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

**Step 8** Click the **Accept** button to save your changes.

# Enabling GMS Management

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

Complete the following steps to enable GMS management of your SRA appliance:

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

**Step 2** Select the **Enable GMS Management** check box.

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

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

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

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

# System > Certificates

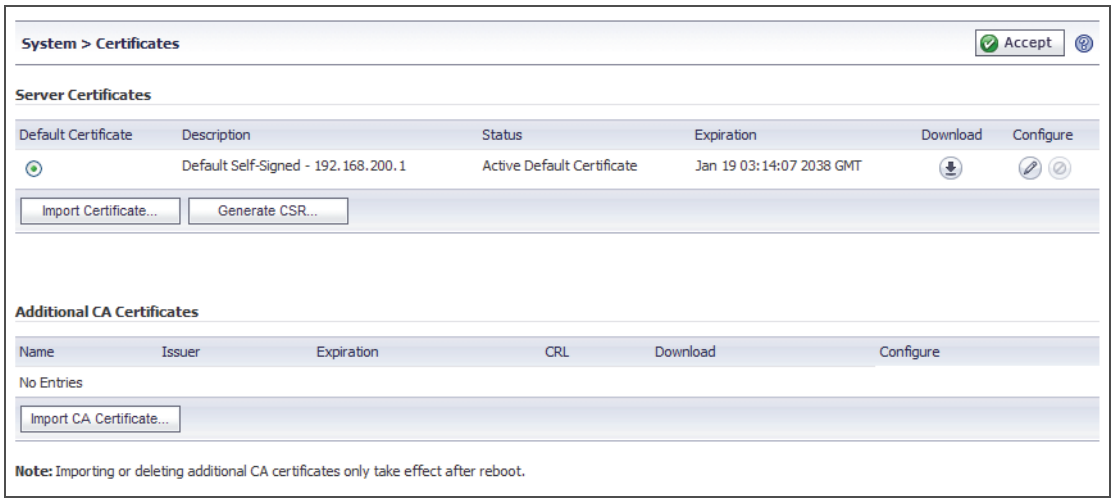
This section provides an overview of the **System > Certificates** page and a description of the configuration tasks available on this page.


- System > Certificates Overview on page 115
- Certificate Management on page 116
- Generating a Certificate Signing Request on page 117
- Viewing and Editing Certificate Information on page 118
- Importing a Certificate on page 118
- Adding Additional CA Certificates on page 119


## System > Certificates Overview

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

***Figure 15 System > Certificates Page***



## Server Certificates

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

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

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

## Additional CA Certificates

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

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

# Certificate Management

The 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 will present an "untrusted root CA certificate" security warning to users until the self-signed certificate is imported into their trusted root store. This import procedure can be performed by the user by clicking the **Import Certificate** button within the portal after authenticating.

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

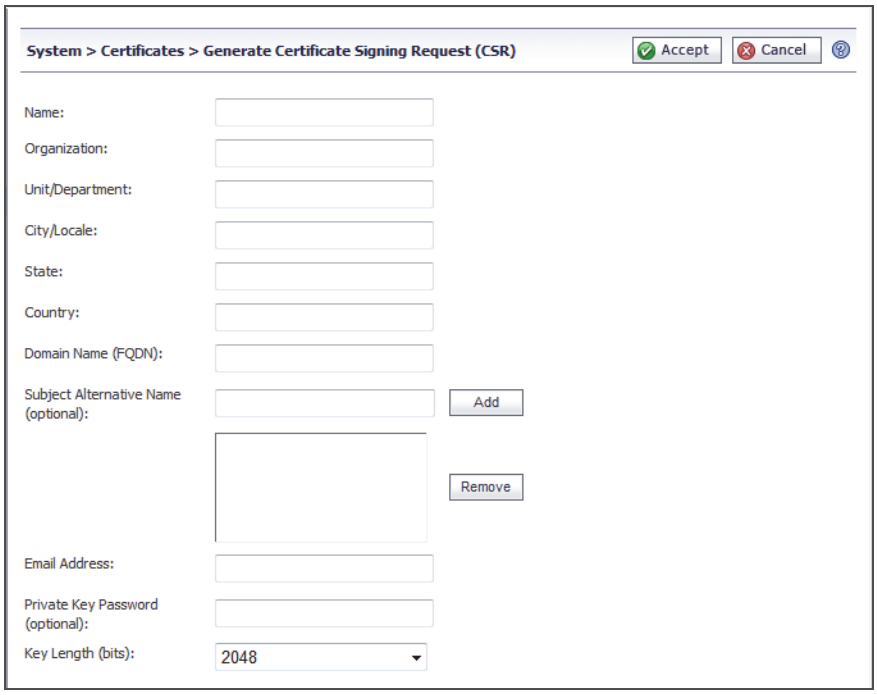
**Note** Beginning in SRA 6.0, Virtual Assist verifies the server certificate, which provides a safer environment for the appliance. If the certificate is not issued by an authorized organization, an alert message is displayed to notify the user of the risk. The user can view detailed information about the server certificate and choose to continue or 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 SRA appliance. To generate a certificate signing request, perform the following steps:

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

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




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

Note that the Subject Alternative Name (SAN)/Unified Communications Certificate (UCC) can be included in the request.

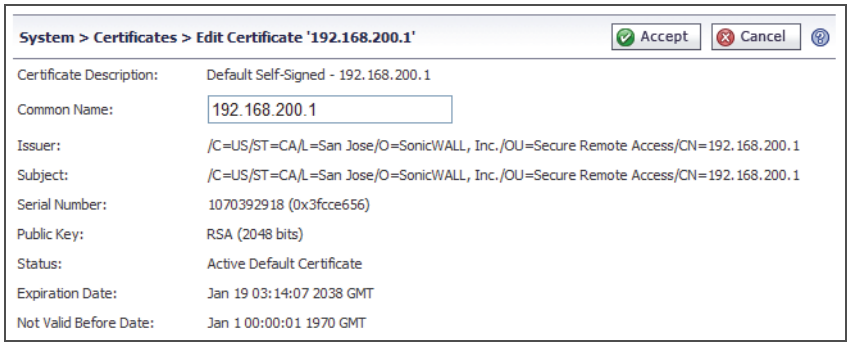
**Step 4** If all information is entered correctly, a **csr.zip** file will be created. Save this .zip file to disk. You will need to provide the contents of the server.csr file, found within this zip file, to the CA.

# 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, perform the following steps:

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




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

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

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

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

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

# Importing a Certificate

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

To import a certificate, perform the following steps:

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

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

**Step 3** Click **Browse**.

**Step 4** Locate the 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 will be accepted, but it must

have the ".zip" extension. The zipped file should contain a certificate file named **server.crt** and a certificate key file named **server.key**. The key and certificate must be at the root of the zip, or the file will not be uploaded.

**Step 5** Click **Upload**.

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

**Note** Private keys may require a password.

## Adding Additional CA Certificates

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

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

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

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

**Step 3** Click **Browse**.

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

**Step 5** Click **Upload**.

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

**Step 6** To add the new CA certificate to the Web server's active CA certificate list, the Web server must be restarted. Restart the 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 on page 119
- Setting The Monitoring Period on page 121
- Refreshing the Monitors on page 121


## System > Monitoring Overview

The 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:

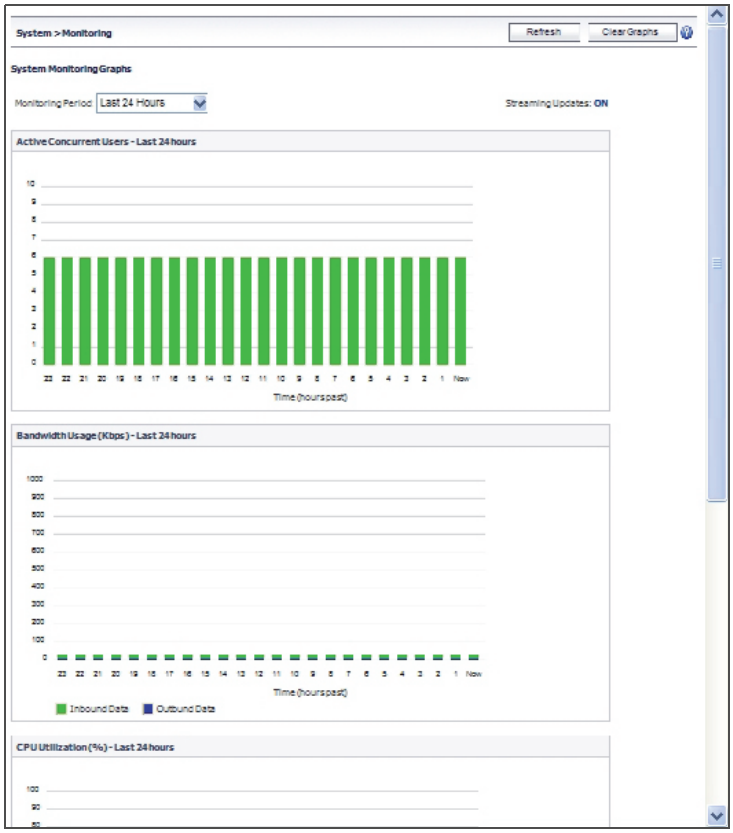
- Active Concurrent Users
- Bandwidth Usage
- CPU Utilization (%)

- 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.

Figure 16 The following figure shows the System > Monitoring page.

***Figure 16 System > Monitoring Page***




## Monitoring Graphs

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

***Table 12 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. |

| Graph | Description |
|---|---|
| CPU Utilization (%) | The amount of capacity usage on the appliance processor being used, measured over time by seconds, minutes, hours, or days. This figure is expressed as a percentage of the total capacity on the CPU. |
| Memory Utilization (%) | The amount of memory available used by the appliance, measured over time by seconds, minutes, hours, or days. This monitoring graph displays memory utilization as a percentage of the total memory available. |

## Setting The Monitoring Period

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

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

## Refreshing the Monitors

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

# System > Diagnostics

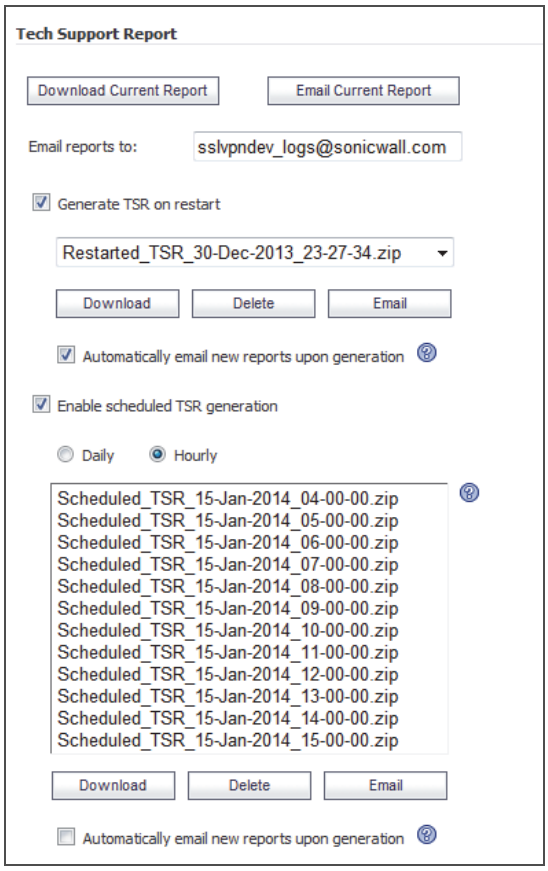
This section provides an overview of the **System > Diagnostics** page and a description of the configuration tasks available on this page.


- System > Diagnostics Overview on page 122
- Downloading & Generating the Tech Support Report on page 122
- Performing Diagnostic Tests on page 124

# System > Diagnostics Overview

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

***Figure 17 System > Diagnostics Page***




# Downloading & Generating the Tech Support Report

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

- **Download Current Report**—Clicking this button will prompt 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 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 SRA appliance will generate 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. Once enabled, you can either have them generated **Hourly** or **Daily**. Note that a maximum of 12 TSRs will be stored, with a total file size not exceeding 50 MB. Scheduled Tech Support Reports are mostly used for diagnostics or troubleshooting purposes by a Dell SonicWALL technician, if needed.

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

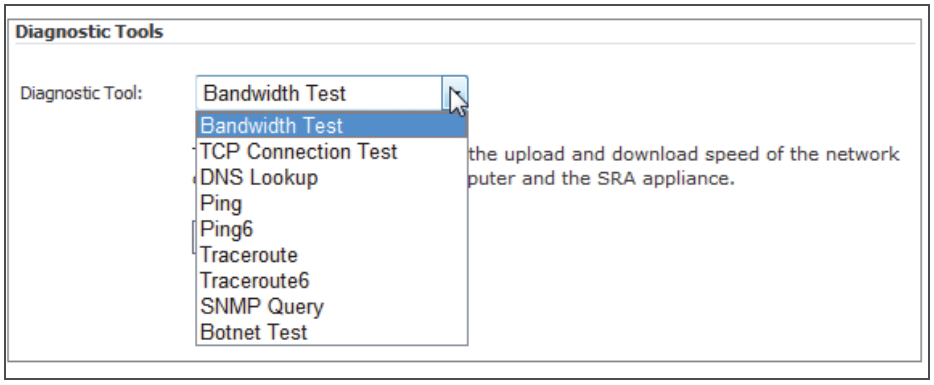
- **Download**—This button allows you to download the latest scheduled Tech Support Reports to your local system.
- **Delete**—This button allows you to delete the latest scheduled Tech Support Reports.
- **Email**—Click this button to email the latest scheduled Tech Support Reports to the values specified 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

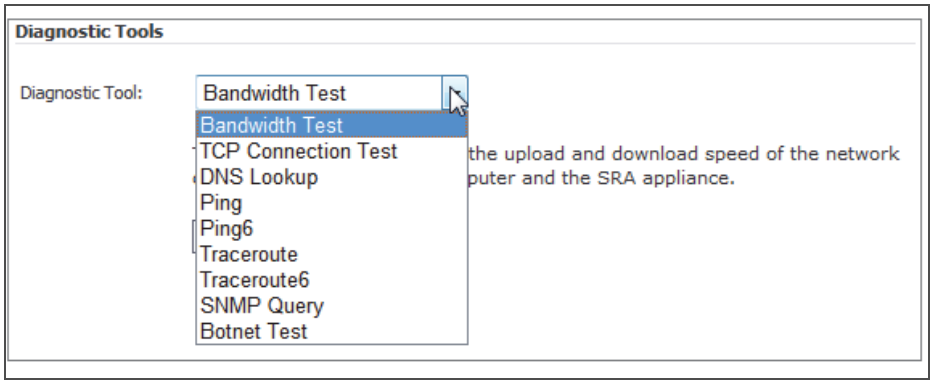
Diagnostic tools allows the administrator to test SRA connectivity by performing a ping, TCP connection test, DNS lookup, or Traceroute for a specific IP address or Web site. You can also perform a bandwidth test between the SRA appliance and your local computer, or do an SNMP query to display information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

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

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




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



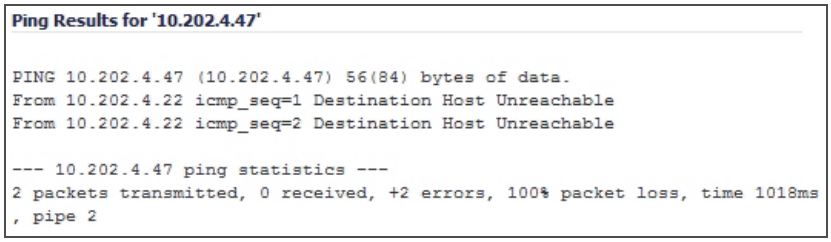
**These diagnostic tools perform the following functions:**

| Diagnostic Tool | Function |
|---|---|
| Bandwidth Test | Measures the upload and download speed of the network connection between your computer and the SRA appliance. |
| TCP Connection Test | Tests the connectivity of a port, which is specified by appending a colon and port number to the host name or IP address (e.g., 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 performed. In the **SNMP MIB** drop-down list, select the MIB for which to display the values. The SNWL-SSLVPN-MIB is the SRA specific MIB that shows device statistics and licensing information. The SNWL-COMMON-MIB is a file common to all Dell SonicWALL 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. |

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

**Step 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 126
- Restarting the SRA Appliance on page 126


## System > Restart Overview

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

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

## Restarting the SRA Appliance

To restart the SRA appliance:

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

**Step 2** Click the **Restart** button.

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

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

# Chapter 4

# Network Configuration

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

This chapter contains the following sections:


- Network > Interfaces on page 127
- Network > DNS on page 130
- Network > Routes on page 132
- Network > Host Resolution on page 135
- Network > Network Objects on page 136


## Network > Interfaces

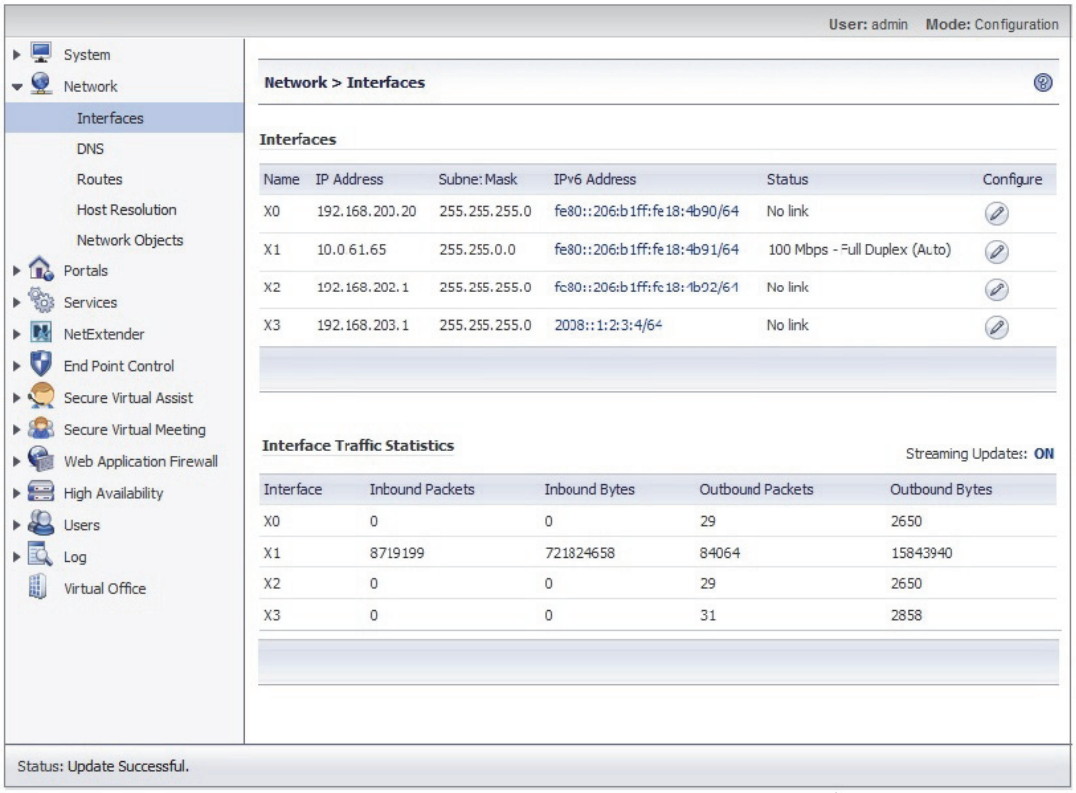
This section provides an overview of the **Network > Interfaces** page and a description of the configuration tasks available on this page.


- Network > Interfaces Overview on page 128
- Configuring Network Interfaces on page 128

# 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 SRA appliance.

***Figure 18 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 SRA appliance. For a port on your 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.

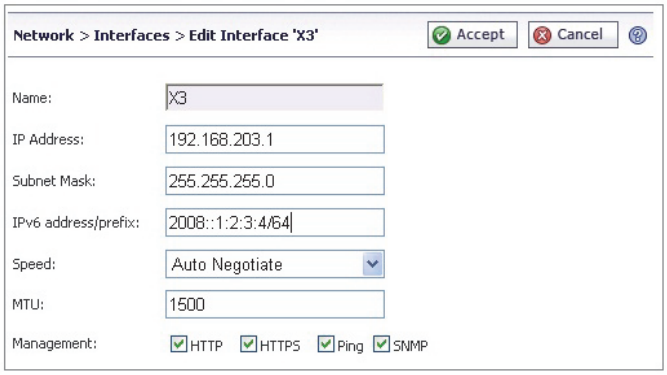
**Note** If the management interface IP address changes, the SRA services will be automatically restarted. This interrupts any existing user sessions, and users will need to reconnect to continue using the SRA appliance.

To configure these settings for an interface on the SRA appliance, perform the following steps:

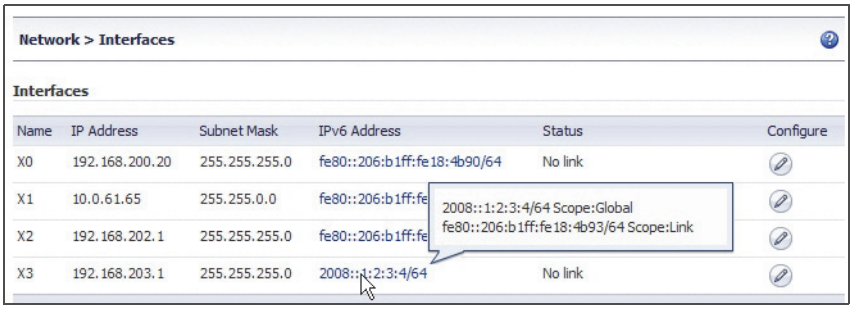
**Step 1** Navigate to the **Network > Interfaces** page and click the configure icon next to the interface you want to configure.

**Step 2** In the **Edit Interfaces** dialog box on the 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 SRA appliance is connected.

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




**Step 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.




**Step 5** In the **Speed** drop-down list, **Auto Negotiate** is selected by default to allow the 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 Dell SonicWALL security appliance as well.

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

**Step 7** Click **Accept**.

# Network > DNS

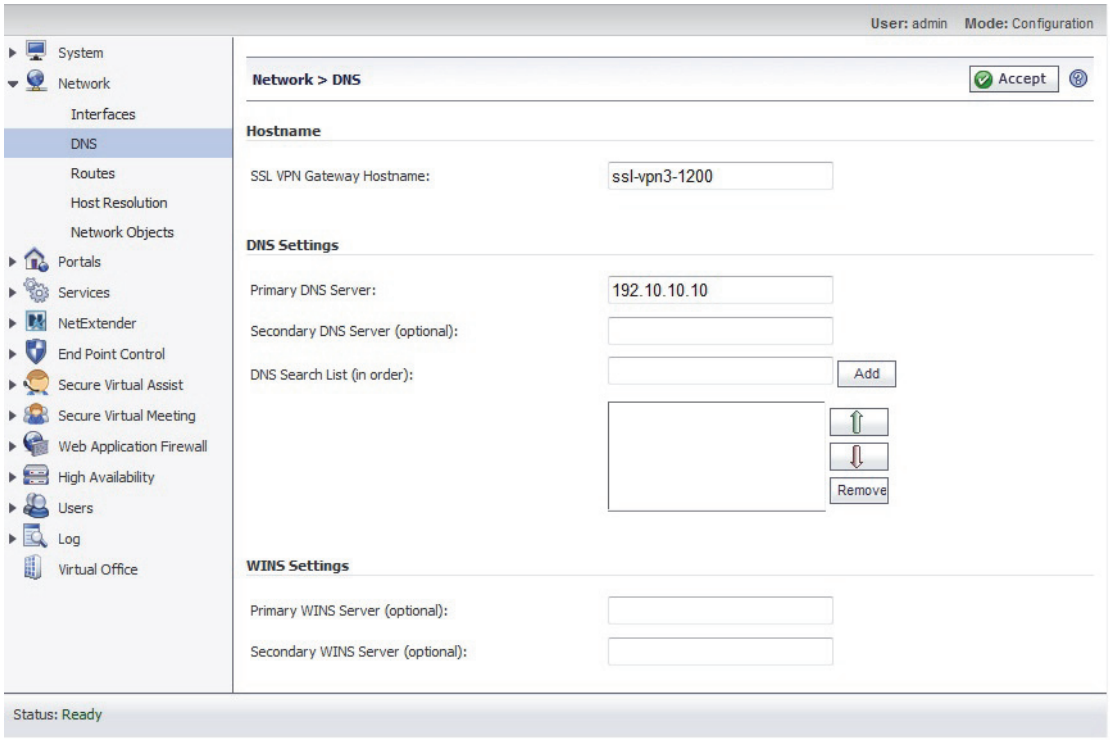
This section provides an overview of the **Network > DNS** page and a description of the configuration tasks available on this page.


- Network > DNS Overview on page 130
- Configuring Hostname Settings on page 131
- Configuring DNS Settings on page 131
- Configuring WINS Settings on page 132


## Network > DNS Overview

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

***Figure 19 Network > DNS Page***




The hostname section allows the administrator to specify the 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 SRA appliances supporting connections from Apple iPhones, iPads, or other iOS devices using Dell SonicWALL 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 DNS server is used, which will not be able to 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, perform the following steps:

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

**Step 2** In the Hostname region, type a hostname for the SRA appliance in the **SRA Gateway Hostname** field.

**Step 3** Click **Accept**.

# Configuring DNS Settings

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

To configure a DNS server, perform the following steps:

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

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

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

**Step 4** 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 will be appended with the host name to make a Fully Qualified Domain Name (FQDN), which will be 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 will be 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 will be appended to SonicPRS to make the FQDN (SonicPRS.usa.n.sonicwall.com), which will be used in name resolution. If the name is not resolved, the next suffix in the search list will be used (SonicPRS.rsc.sonicwall.com).This process continues until the name is resolved or all suffixes have been tried.

**Step 5** Click **Accept**.

**Step 6** Restart the appliance to ensure new DNS settings take effect.

## Configuring WINS Settings

WINS settings are optional. The 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, perform the following tasks:

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

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

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

**Step 4** Click **Accept**.

# Network > Routes

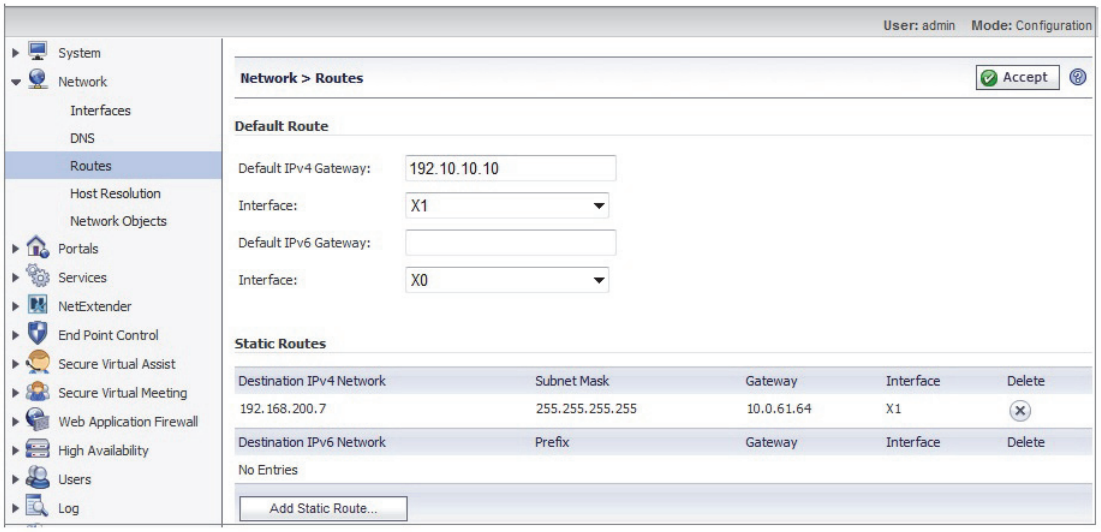
This section provides an overview of the **Network > Routes** page and a description of the configuration tasks available on this page.


- Network > Routes Overview on page 133
- Configuring a Default Route for the SRA Appliance on page 133
- Configuring Static Routes for the Appliance on page 134

# 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 *Dell SonicWALL SRA Getting Started Guide* for your appliance model.

***Figure 20 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.

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

# Configuring a Default Route for the SRA Appliance

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

To configure the default route, perform the following steps:

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

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

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

**Step 4** In the **Default IPv6 Gateway** field, type the IPv6 address of the firewall or other gateway device through which the SRA appliance connects to the network. This address will act as the default IPv6 route for the appliance.

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

**Step 6** Click **Accept**.

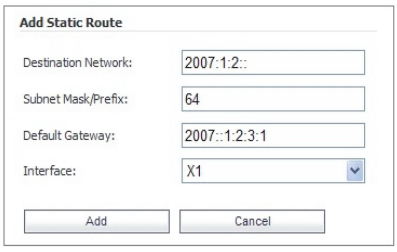
# Configuring Static Routes for the Appliance

Based on your network's topology, you might find it necessary or preferable to configure static routes to certain subnets rather than attempting to reach them through the default gateway. While the default route is the default gateway for the device, static routes can be added as needed to make other networks reachable for the 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, perform the following steps:

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

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




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

**Step 4** In the **Default Gateway** field, type the IP address of the gateway device that connects the appliance to the network.You can enter an IPv6 address.

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

**Step 6** Click **Accept**.

# Network > Host Resolution

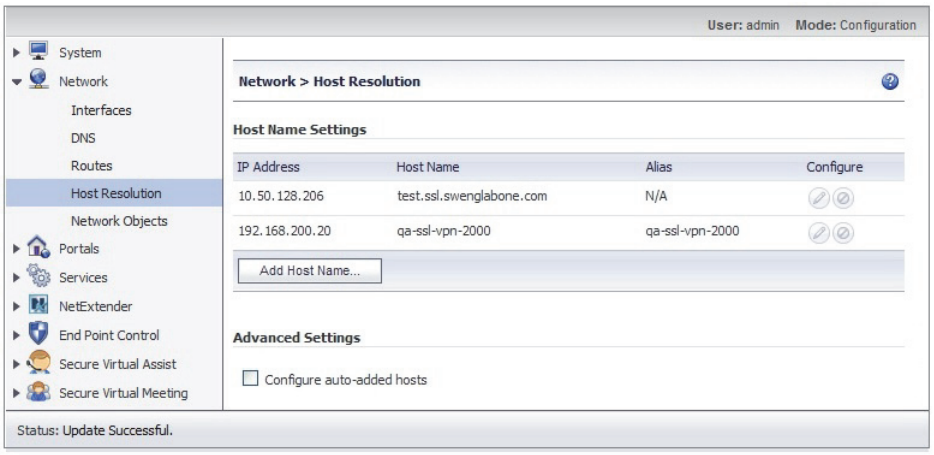
This section provides an overview of the **Network > Host Resolution** page and a description of the configuration tasks available on this page.


- Network > Host Resolution Overview on page 135
- Configuring Host Resolution on page 135


## Network > Host Resolution Overview

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

***Figure 21 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 SRA appliance itself. Do not delete it.

The 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, perform the following steps:

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

**Step 2** Click **Add Host Name**.

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

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

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

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

**Step 7** Optionally select the **Configure auto-added hosts** check box 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.

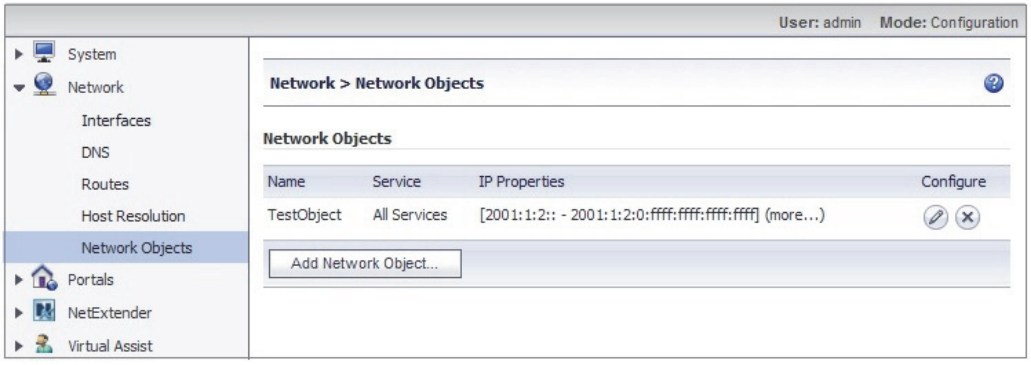

- Network > Network Objects Overview on page 136
- Adding Network Objects on page 137
- Editing Network Objects on page 138


## 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.

***Figure 22 Network > Network Objects Page***



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

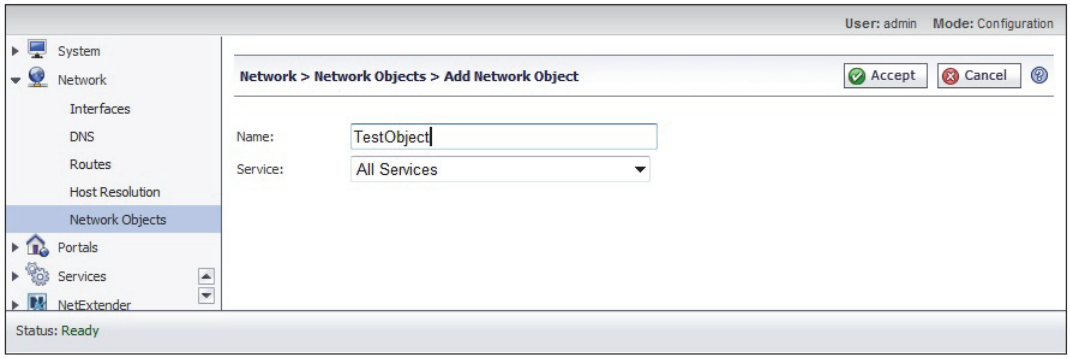
- Web (HTTP)
- Secure Web (HTTPS)
- NetExtender
- Terminal Services (RDP - Active X)
- Terminal Services (RDP - Java)
- Virtual Network Computing (VNC)
- File Transfer Protocol (FTP)
- Telnet, Secure Shell version 1 (SSHv1) / Secure Shell version 2 (SSHv2)
- File Shares (CIFS)
- Citrix Portal (Web Access)

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

# Adding Network Objects

To add a network object, perform the following steps:

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




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

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

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

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

**Step 5** Click **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 138.

# Editing Network Objects

To edit a network object, perform the following steps:

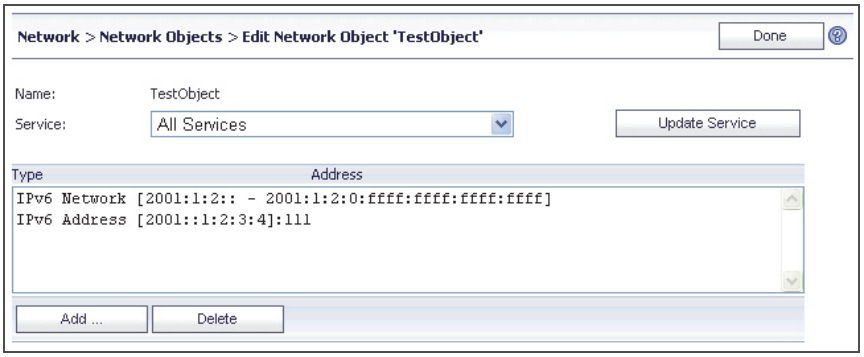
**Step 1** To edit an existing network object, navigate to the **Network** > **Network Objects** page and click the Configure icon or click the **Incomplete** link for the object you wish to edit. The **Edit Network Object** screen is displayed.

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.

**Step 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.

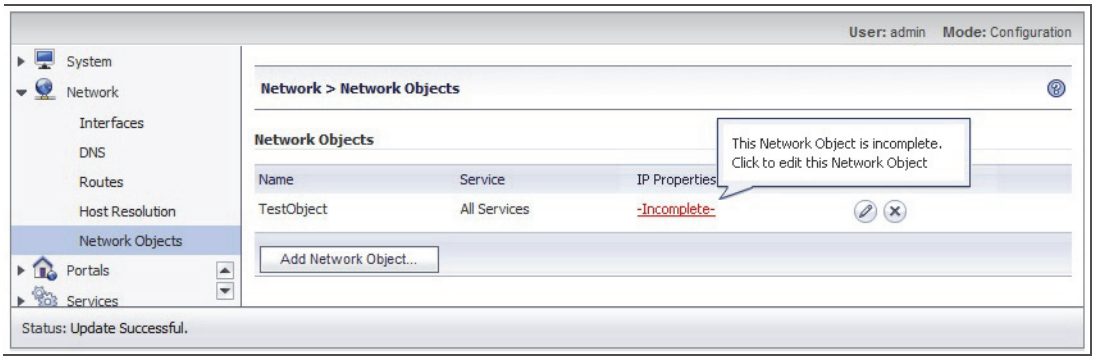
**Step 3** To add or edit **Type** and **Address** values for this Network Object, click **Add**. The **Define Object Address** page is displayed. See Defining an Object Address on page 139.




**Step 4** When finished adding addresses, click **Done** in the Edit Network Object screen.

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

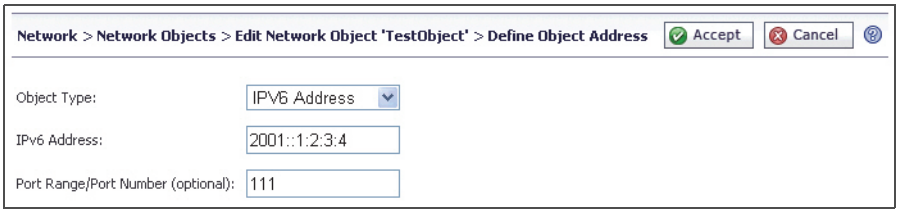
**Step 6** If the object is not fully defined with at least one IP address or network range, the status **Incomplete** will display. Click the **Incomplete** link or the Configure icon to edit the network object again, and then click **Add** to add Type and Address values for this network object. The **Define Object Address** page is displayed. See Defining an Object Address on page 139.




**Note** Policies cannot be created for incomplete network objects.

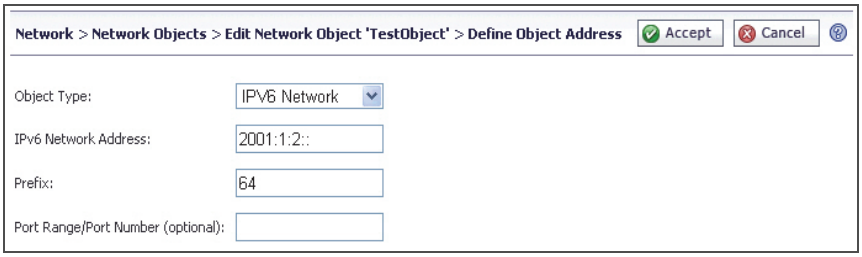
**Step 1** In the **Define Object Address** page, click on the **Object Type** drop-down list and select an object type. The four object types are:

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

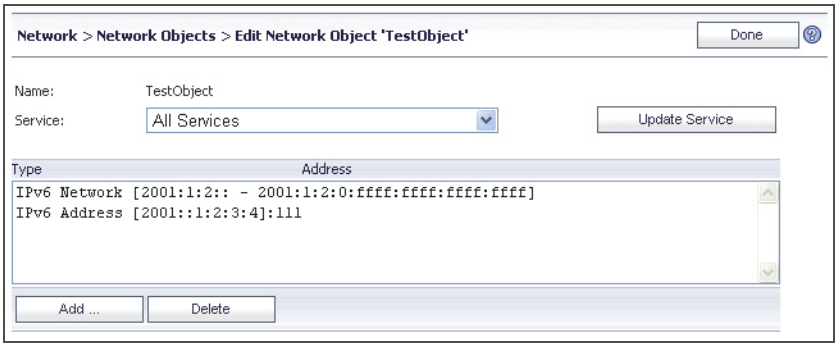



**Step 2** Type in the appropriate information pertaining to the object type you have selected.

- 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.




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



# Chapter 5

# Portals Configuration

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

This chapter contains the following sections:


- Portals > Portals on page 141
- Portals > Application Offloading on page 155
- Portals > Domains on page 162
- Portals > Custom Logo on page 187
- Portals > Load Balancing on page 187


# Portals > Portals

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

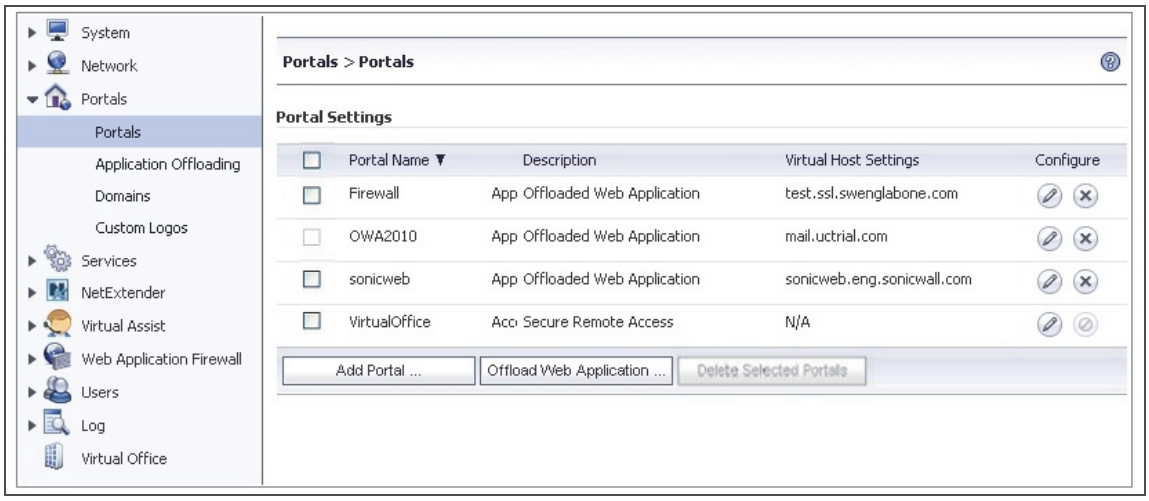

- Portals > Portals Overview on page 142
- Adding Portals on page 143
- Configuring General Portal Settings on page 144
- Enforcing Client Source Uniqueness on page 146
- Configuring Per-Portal Virtual Assist Settings on page 151
- Configuring Virtual Host Settings on page 153
- Adding a Custom Portal Logo on page 154


For information about Application Offloading and the **Offload Web Application** button, see Portals > Application Offloading on page 155.

# Portals > Portals Overview

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

***Figure 23 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.

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

## Additional Information About the Portal Home Page

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

### Modern Portals

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

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

# Adding Portals

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

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

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

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

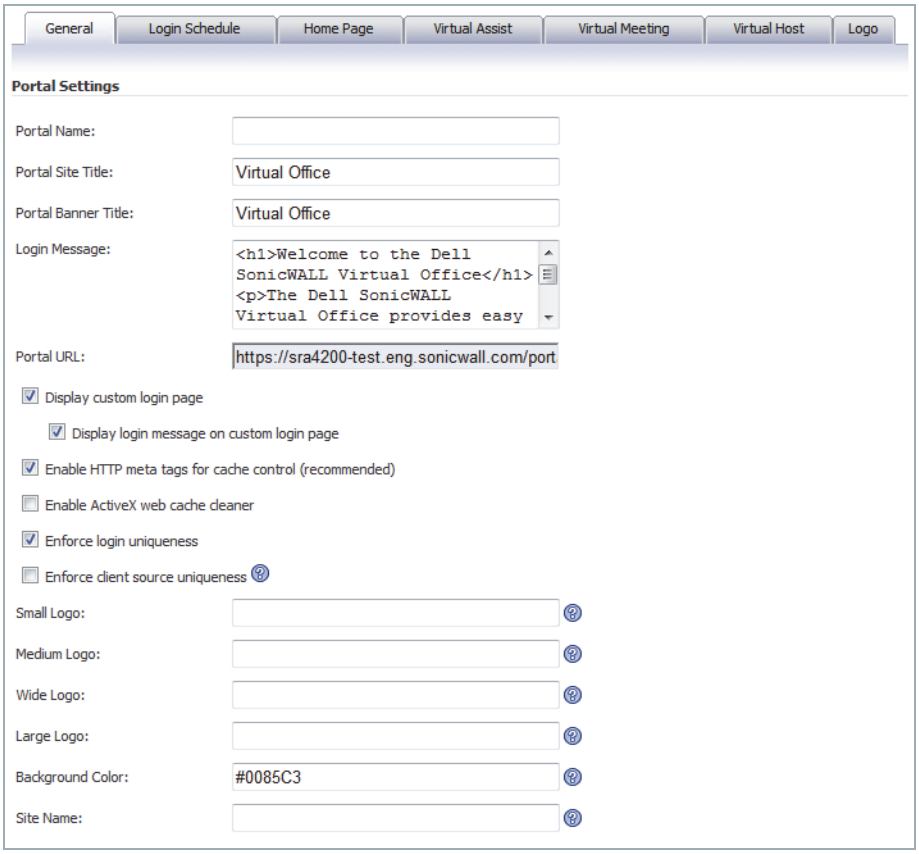


Table 13The following table provides a description of the fields you may configure on the **General** tab. Refer to Configuring General Portal Settings on page 144 for the specific steps required to configure a custom portal.

***Table 13 General Tab Fields.***

| Field | Description |
|---|---|
| Portal Name | The title used to refer to this portal. It is for internal reference only, and is not displayed to users. |
| Portal Site Title | The title that will appear on the Web browser title bar of users access this portal. |
| Portal Banner Title | The welcome text that will appear on top of the portal screen. |
| Login Message | Optional text that appears on the portal login page above the authentication area. |
| 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. |
| 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 SRA session is closed. |
| Enforce login uniqueness | If enforced, login uniqueness restricts each account to one session at a time. If not enforced, each account can have multiple simultaneous sessions. |
| 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 Dell SonicWALL client (NetExtender, Mobile Connect, Virtual Assist etc.). 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 . 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 on the General tab for a new portal, perform the following steps:

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

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

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

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

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

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

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

**Step 7** The **Portal URL** field is automatically populated based on your SRA appliance network address and Portal Name.

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

**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 154.

**Step 9** Select the **Enable HTTP meta tags for cache control** check box 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 SRA portal pages and other Web content.

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

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

**Step 11** See Enforcing Login Uniqueness on page 146.

**Step 12** See Enforcing Client Source Uniqueness on page 146.

**Step 13** Specify the link(s) for the **Small** / **Medium** / **Wide** / **Large** Logo on the Portal page.

**Step 14** Specify the **Background Color** for the on the Portal page. If no value is specified, the default color is #0085C3.

**Step 15** Specify the **Site Name**, which is the display name for the bookmark. If no value is specified, the default is your 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, perform the following steps:

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

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

**Step 3** Select the **Enforce login uniqueness** check box.

**Step 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 Dell SonicWALL 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 timeout disconnects them.

To enforce client source uniqueness, perform the following steps:

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

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

**Step 3** Select the **Enforce client source uniqueness** check box.

**Step 4** Click **Accept**.

# Configuring Login Schedules

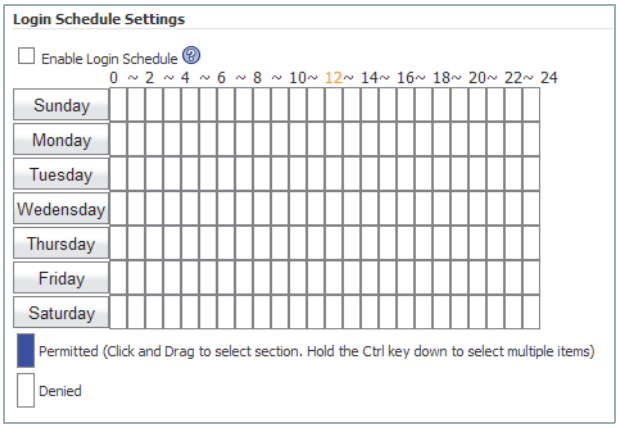
The login schedules tab allows you to restrict access to a portal based on the time specified.

To enable login schedules, perform the following steps:

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

**Step 2** Select the existing portal you want to configure.

**Step 3** Click the **Login Schedule** tab. The Login Schedule displays.




**Step 4** Click the **Enable Login Schedule** check box.

**Step 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 the Day button to select the whole day.

**Step 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 SRA appliance portal. The home page enables you to create a custom page that mobile users will see when they log into the portal. Because the home page can be customized, it provides the ideal way to communicate remote access instructions, support information, technical contact information or SRA-related updates to remote users.

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

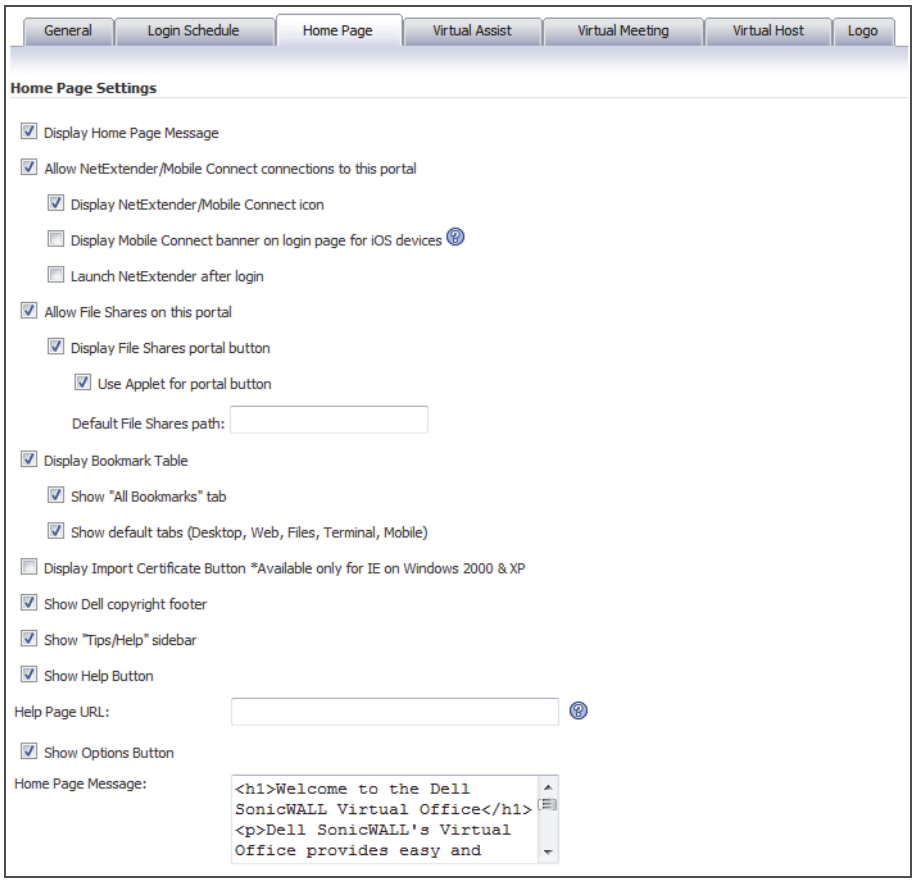
You can edit the title of the page, create a home page message that is displayed at the top of the page, show all applicable bookmarks (user, group, and global) for each user, and optionally upload an HTML file.

To configure the home page, perform the following tasks:

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

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

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




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

***Table 14 Home Page Tab Fields***

| Field | Description |
|---|---|
| Display Home Page Message | Displays the customized home page message after a user successfully authenticates to the 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 will not be 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. |
| 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. |

| Field | Description |
|---|---|
| Launch NetExtender after Login | Launches NetExtender automatically after a user successfully authenticates to the 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 will not be accessible from the portal. |
| Display File Shares portal button | Provide a button to link to the File Shares (Windows CIFS/SMB) Web interface so that authenticated SRA users may use NT file shares 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 will provide a link for the user to find all available domains. The file share will also list 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 will not be 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. Certificate import is only available for Internet Explorer on Windows 2000 and XP. |
| Show Dell SonicWALL copyright footer | Displays Dell SonicWALL copyright footer on portal. If unchecked, the footer is not shown. |
| Show “Tips/Help” sidebar | Displays a sidebar in the portal with tips and help links. This option is not available when the Legacy Look & Feel check box 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 Dell SonicWALL 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 will disable access to the DFS file shares from other domains. The SRA appliance is not a domain member and will not be able to connect to the DFS shares. DFS file shares on a stand-alone root are not affected by this Microsoft restriction.

- Some ActiveX applications, such as the ActiveX Terminal Services RDP client, will only work when connecting to a server with a certificate from a trusted root authority. If you are using the test SSL certificate that is included with the SRA appliance, then you can select the **Display Import self-signed certificate links** check box to allow Windows users to easily import a self-signed certificate.
- It is strongly recommended that you upload a valid SSL certificate from a trusted root authority such as Verisign or Thawte. If you have a valid SSL certificate, do not select the **Display Import self-signed certificate links** check box.

---

**Step 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, perform the following steps:

---

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

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

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

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

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

**Step 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, perform the following tasks:

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

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

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

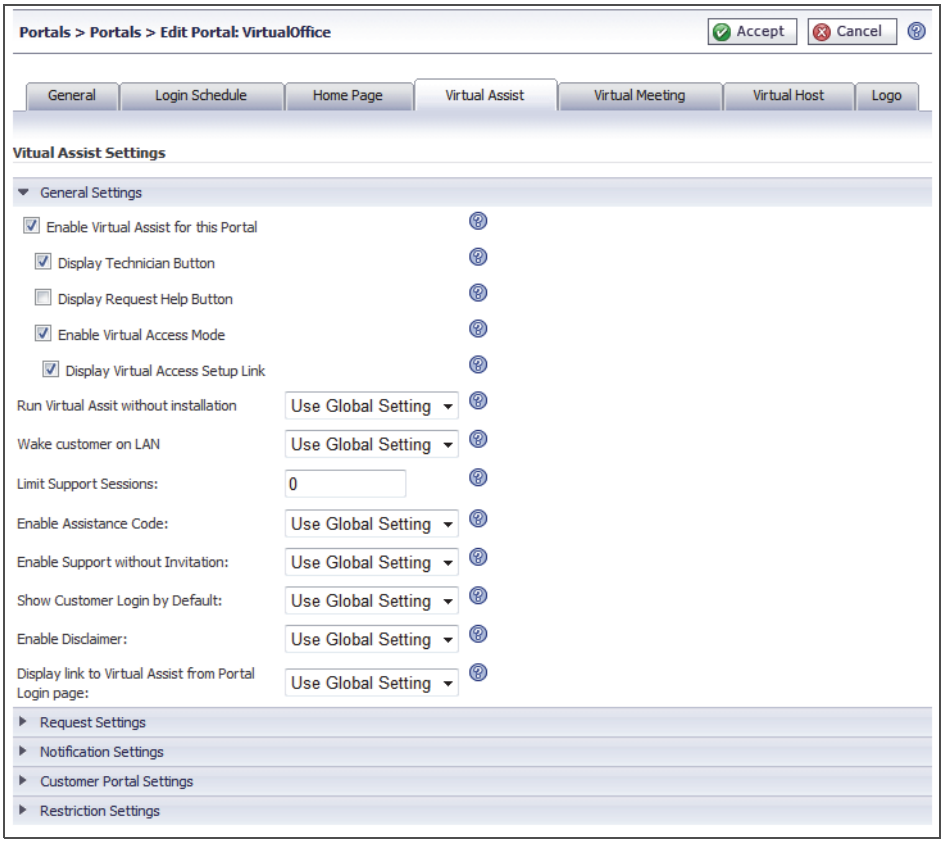
**Step 4** Select the **Display File Shares portal button** check box.

**Step 5** Select the **Use Applet for portal button** check box.

**Step 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 tab 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 this portal, perform the following steps:

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

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

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

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

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

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

**Step 7** Select the **Enable Virtual Access Mode** check box 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 the **Display Virtual Access Setup Link** check box 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.

**Step 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.

**Step 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 SRA User Guide.

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

**Step 11** Check the **Enable Assistance Code** check box 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

**Step 12** See Secure Virtual Assist > Settings on page 244 for information about all other configuration settings on the Virtual Assist tab.

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

**Step 14** Click **Accept** to save changes.

# Configuring Virtual Host Settings

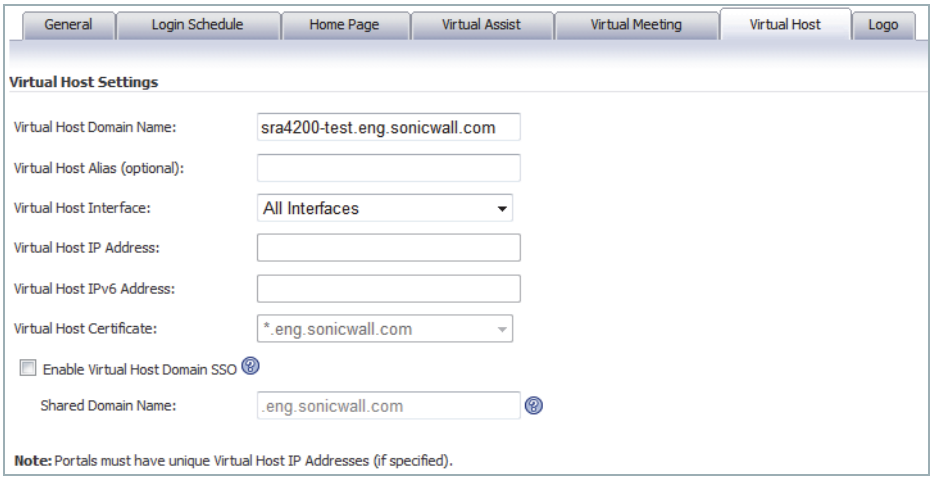
Creating a virtual host allows users to log in using a different hostname than your default URL. For example, sales members can access **https://sales.company.com** instead of the default domain, **https://vpn.company.com** that you use for administration. The Portal URL (for example, **https://vpn.company.com/portal/sales**)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

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

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

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

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




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

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

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

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

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

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

**Step 7** If you selected a specific Virtual Host Interface for this portal, you can specify an IPv6 address in the **Virtual Host IPv6 Address** field. You can use this address to access the virtual host. Enter the IPv6 address using decimal or hexadecimal numbers in the form:

2001::A987:2:3:4321

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

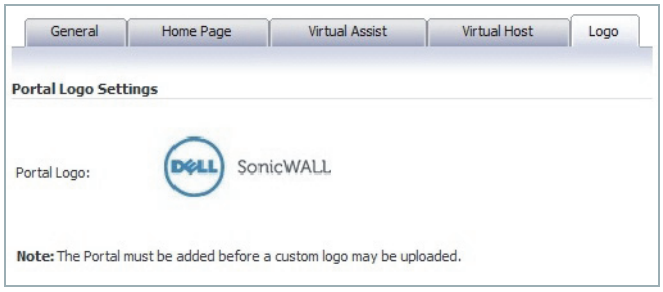
Unless you have a certificate for each virtual host domain name, or if you have purchased a *.domain SSL certificate, your users may see a **Certificate host name mismatch** warning when they log into the SRA appliance portal. The certificate hostname mismatch affects the login page, NetExtender, and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

To achieve a single point of access for users, configure External Website Bookmarks for application offloading portals by selecting the **Enable Virtual Host Domain SSO** check box 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 into application offloading portals or Web sites that share the same Virtual Host Domain.

# Adding a Custom Portal Logo

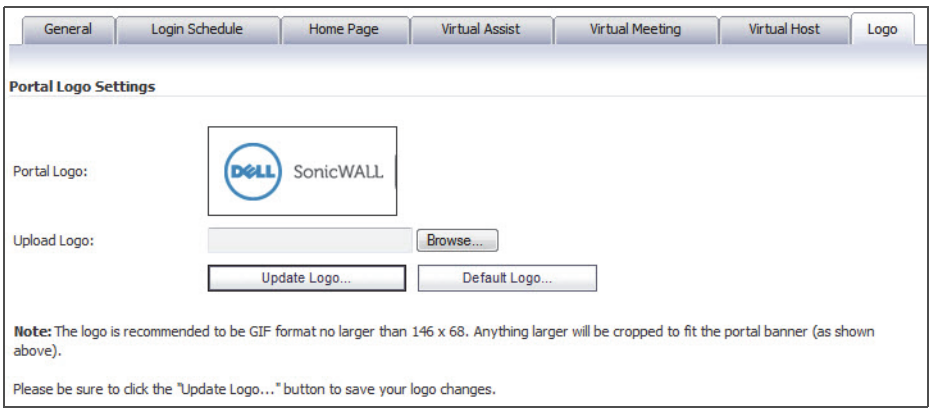
The Custom Logo Settings section allows the administrator to upload a custom portal logo and to toggle between the default Dell SonicWALL logo and a custom uploaded logo. You must add the portal before you can upload a custom logo. In the Add Portal screen, the Logo tab does not have an option to upload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




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

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

**Step 2** Click the **Logo** tab.




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

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

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

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

**Step 6** Click the **Update Logo** button to transfer the logo to the SRA appliance.

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

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

# Portals > Application Offloading

The Portals > Application Offloading page in the management interface provides an overview of the Application Offloading functionality available from the Portals > Portals page. No configuration is available on this page.

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

See the following sections:


- Application Offloading Overview on page 155
- Configuring an HTTP/HTTPS Application Offloading Portal on page 156


## Application Offloading Overview

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

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

The portal must be configured as a virtual host with a suitable SRA 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 SRA:

- 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 SRA 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 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**

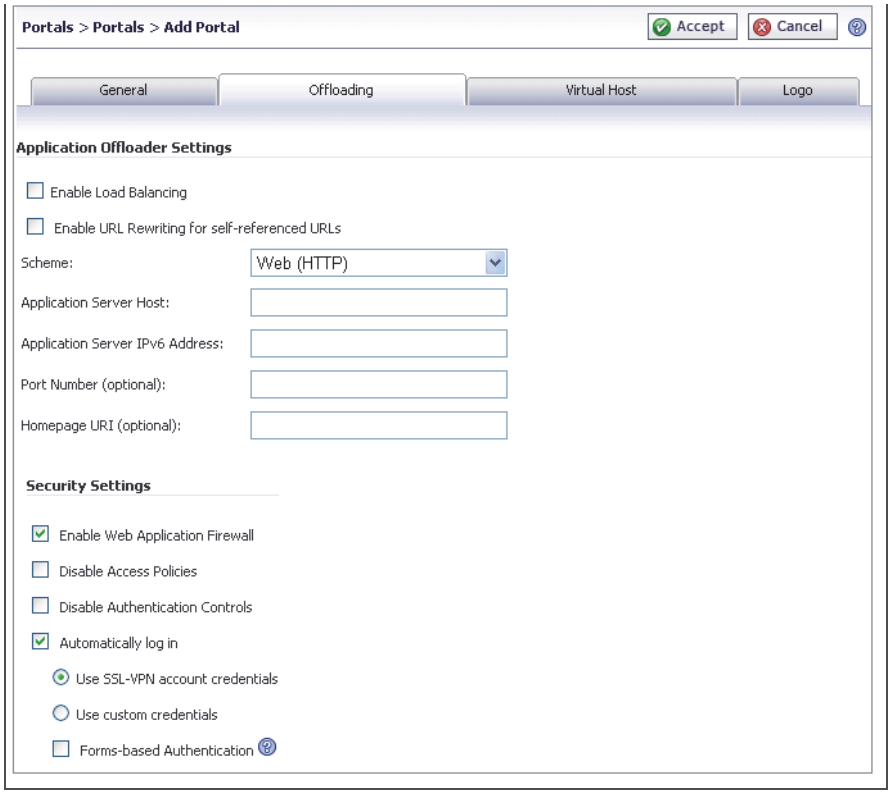
- The maximum number of users supported is limited by the number of applications being accessed and the volume of application traffic being sent.
- The Application Offloading feature will not work well if the application refers to resources within the same host using absolute URLs. In this case, you may need to convert an absolute URL reference to its relative form.
- NTLM (Microsoft NT Lan Manager) authentication and digest authentication schemes are not supported for HTTP(S) bookmarks or Application Offloading.

  Further information about configuring specific backend Web applications is available in the *Dell SonicWALL SRA 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, perform the following steps:

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




**Step 2** On the **General** tab, enter a descriptive name in the **Portal Name** field. See Configuring General Portal Settings on page 144 for more instructions for configuring the fields on this tab.

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

**Step 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), which may be insecure. Therefore, you will be prompted to click OK to enable HTTP for Virtual Host and enable Anonymous access.

- **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 Generic SSL Offloading on page 160.

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

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

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

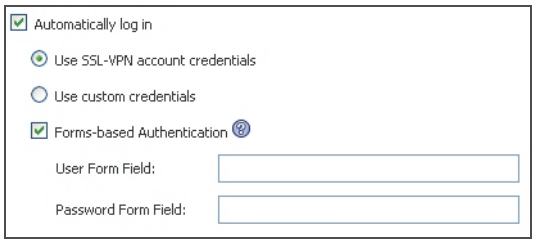
**Step 8** In the **Homepage URI (optional)** field, optionally enter a URI to a specific resource on the Web server to which the user will be forwarded the first time the user tries to access the Application Offloading Portal. This is a string in the form of:
**/exch/test.cgi?key1=value1&key2=value2**

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. Under Security Settings, select the **Enable Web Application Firewall** button to enable the feature.
12. Select the **Disable Authentication Controls, Access Policies, and CSRF Protection (if enabled)** check box if you need no authentication, access policies, or CSRF protection enforced. This is useful for publicly hosted Web sites.
13. To configure ActiveSync authentication, clear the **Disable Authentication Controls** check box to display the authentication fields. Select the **Enable ActiveSync authentication** check box 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.

**Step 9** Select the **Automatically Login** check box to configure Single Sign-On settings.




**Step 10** For automatic login 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 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:

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

**Step 11** If you selected **Automatically Login**, select the **Forms-based Authentication** check box to configure Single Sign-On for forms-based authentication.

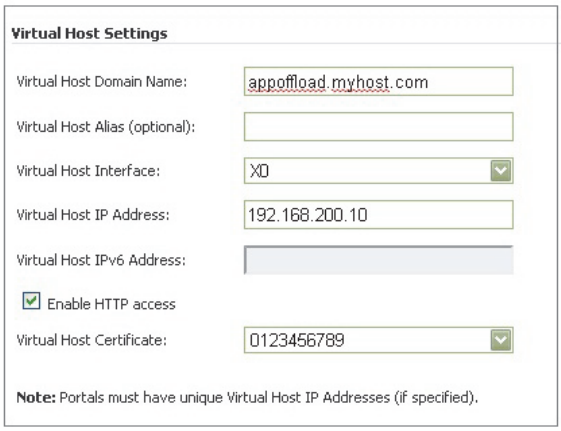
- Configure the **User Form Field** to be the same as the 'name' and 'id' attribute of the HTML element representing User Name in the Login form, for example:
  **<input type=text name='userid'>**
- Configure the **Password Form Field** to be the same as the 'name' or 'id' attribute of the HTML element representing Password in the Login form, for example:
  **<input type=password name='PASSWORD' id='PASSWORD' maxlength=128>**

**Step 12** On the **Virtual Host** tab, set a host name for the application in the **Virtual Host Domain Name** field, and optionally enter a descriptive alias in the **Virtual Host Alias** field.

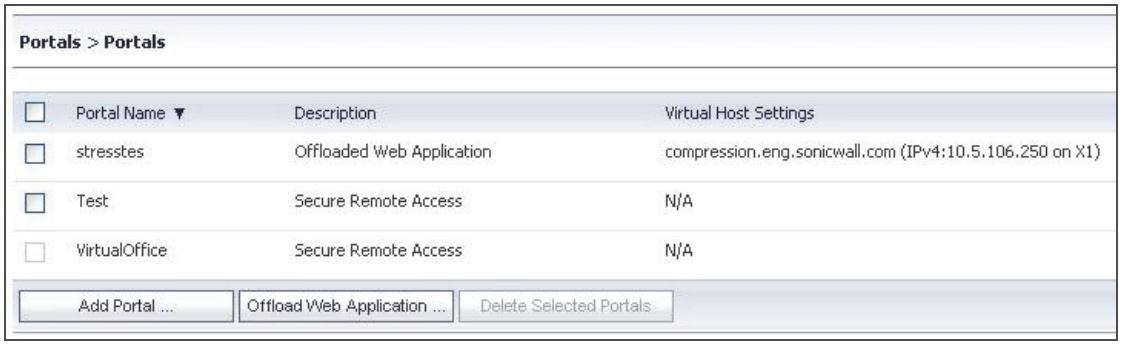
If you need to associate a certificate to this host, you should additionally set a virtual interface and import the relevant SSL certificate. You could avoid creating a virtual interface by importing a wildcard certificate for all virtual hosts on the SRA appliance.

See Configuring Virtual Host Settings on page 153 for more instructions on configuring the fields on this tab.

**Step 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.




**Step 14** 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.




**Step 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 162 for information about creating a domain.

**Step 16** Update your DNS server for this virtual host domain name and alias (if any).

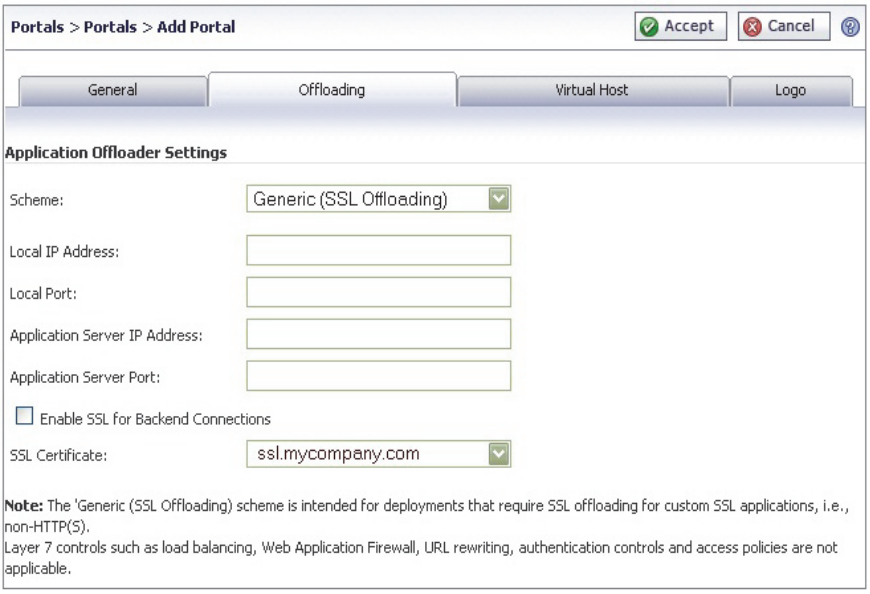
# Configuring Generic SSL Offloading

SSL Offloading portals extends the Application Offloading feature to support protocol independent SSL requests and forward them to the backend server. This feature is needed for customer client/server applications that use SSL for security.

The “Generic (SSL Offloading)” scheme is intended for deployments that require SSL offloading for custom SSL applications, i.e., *non*-HTTP(S). Layer 7 controls such as load balancing, Web Application Firewall, URL rewriting, authentication controls and access policies are not applicable when using this offloading method.

To configure generic SSL offloading:

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




**Step 2** On the **Offloading** tab, select Generic (SSL Offloading) as the **Scheme**.

**Step 3** Enter the IP address of the portal which will listen for incoming SSL requests in the **Local IP Address** field.

**Step 4** In the **Local Port** field, enter the port on which to listen for incoming SSL requests. This is often set to 443.

**Step 5** In the **Application Server IP Address** field, enter the IP Address of the backend server where SSL offloaded requests are to be proxied.

**Step 6** In the **Application Server Port** field, enter the port of the backend server where SSL offloaded requests are to be proxied. This is often set to 80 for internal HTTP communication.

**Step 7** Select the **Enable SSL for Backend Connections** check box to enable SSL encapsulation of all traffic destined for the backend application server.

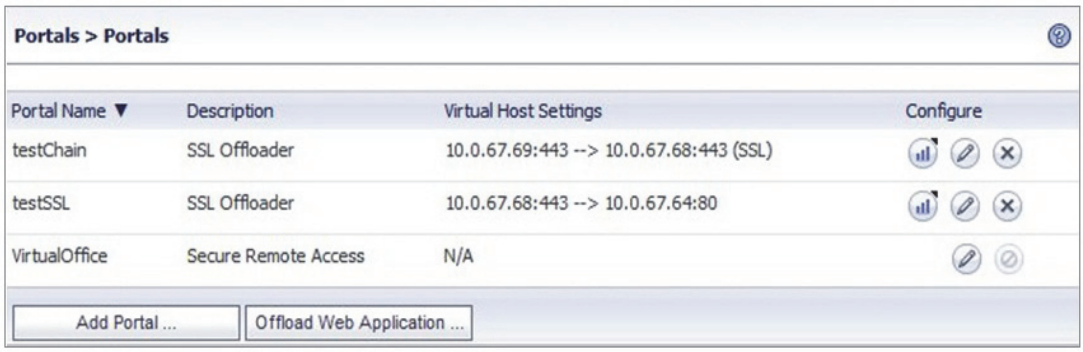
**Step 8** Select the **SSL Certificate** to use for SSL connection to the portal. This list of certificates mirrors the list of sever certificates on the System > Certificates page.

**Step 9** On the **General** tab, enter a descriptive **Portal Name** name for this portal.

**Note** Other portal options such as Virtual Host and Logo are not available when using the Generic (SSL Offloading) scheme.

**Step 10** Click the **Accept** button to add this portal.

When completed, SSL Offloading portals are displayed in the list of portals on the Portals > Portals page. Note that the Virtual Host Settings column shows the Local IP:port --> Application Server IP:port as well as (SSL) if 'Enable SSL for Backend Connections' is enabled.




### Verification and Considerations for Generic SSL Offloading

To view the SSL Offloading portal in action, point it to a backend web server and use a current Internet browser to view the SSL offloaded site, using the format <Local IP:port>

Generic (SSL Offloading) scheme is not meant for HTTP/HTTPS, and should not be used in deployments as such. Since there is no layer 7 analysis, issues such as insecure HTTP 30X redirects can occur and this is not recommended.

# Portals > Domains

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

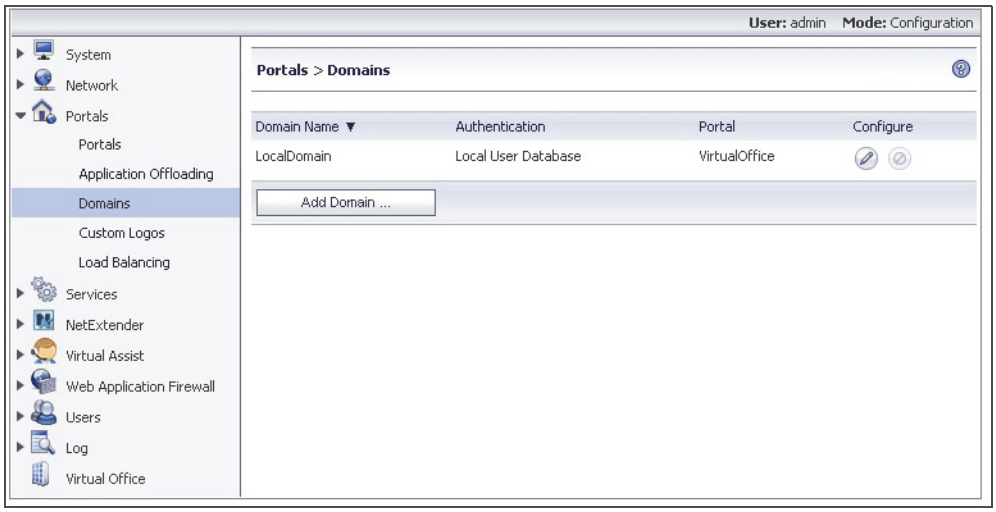

- Portals > Domains Overview on page 162
- Viewing the Domains Table on page 163
- Removing a Domain on page 163
- Adding or Editing a Domain with Local User Authentication on page 165
- Adding or Editing a Domain with Active Directory Authentication on page 167
- Adding or Editing a Domain with LDAP Authentication on page 171
- Adding or Editing a Domain with NT Domain Authentication on page 174
- Adding or Editing a Domain with RADIUS Authentication on page 175
- Configuring Two-Factor Authentication on page 178


## 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, NT Domain, 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)

*Figure 24 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, perform the following steps:

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

**Step 2** In the table, click the delete icon in the same row as the domain that you wish to delete.

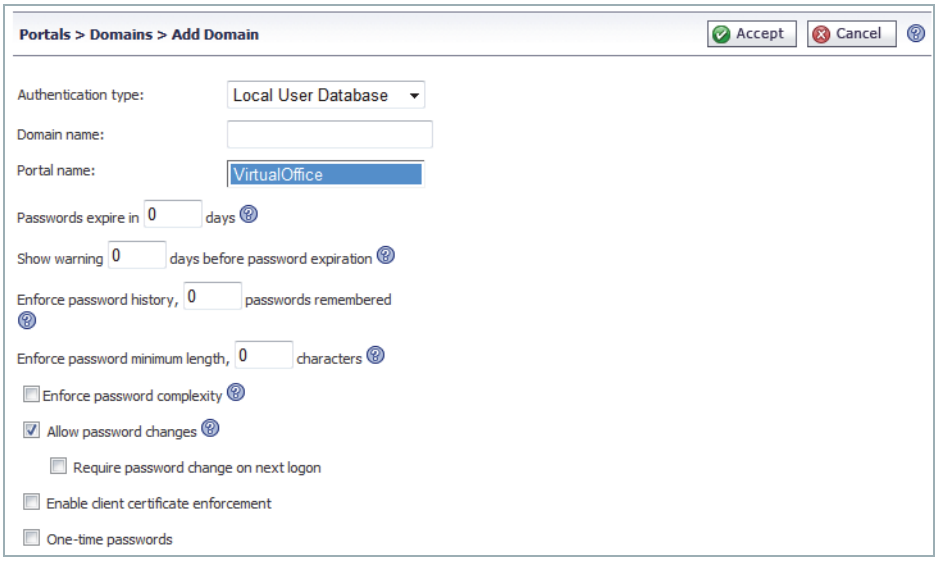
**Step 3** Click **OK** in the confirmation dialog box.

Once the SRA appliance has been updated, the deleted domain will 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 the **Add Domain** button 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 366 for instructions on configuring groups.

In order to create access policies, you must first create authentication domains. By default, the LocalDomain authentication domain is already defined. The LocalDomain domain is the internal user database. Additional domains may be created that require authentication to remote authentication servers. The SRA appliance supports RADIUS, LDAP, NT Domain, and Active Directory authentication in addition to internal user database authentication.

**Note** To apply a portal to a domain, add a new domain and select the portal from the Portal Name drop-down list in the **Add Domain** window. The selected portal will be applied to all users in the new domain. Domain choices will be displayed in the login page of the Portal that was selected. Domains are case-sensitive when logging in.

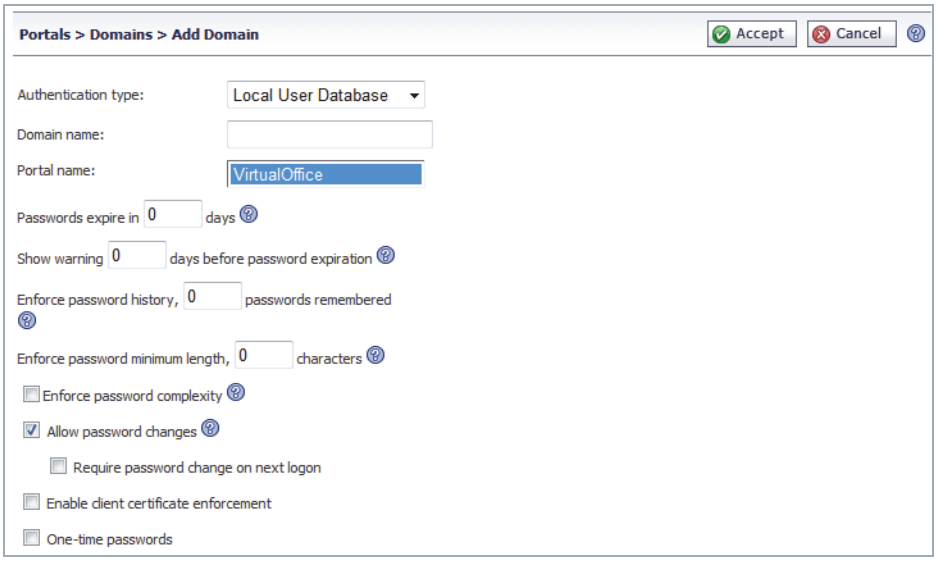
You may create multiple domains that authenticate users with user names and passwords stored on the SRA appliance to display different portals (such as a SRA portal page) to different users.

For convenient configuration of SRA appliance administrator accounts, you can create a domain that provides administrator access for all users who log into 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, perform the following steps:

**Step 1** Navigate to the **Portals > Domains** window and click the **Add Domain** button or the Configure icon for the domain to edit. The **Add Domain** or **Edit Domain** window is displayed.




**Step 2** If adding the domain, select **Local User Database** from the **Authentication Type** drop-down list.

**Step 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 will select to log into the SRA portal.

**Step 4** Select the name of the layout in the **Portal Name** field. Additional layouts may be defined in the **Portals > Portals** page.

**Step 5** 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 the **Change password at next logon** check box.

**Note** A specific local domain user can be forced to change their password. Use the General tab on the Users > Local Users > Edit page.

**Step 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 will expire. Notifications also include a link to a screen where the password can be changed.

**Step 7** Optionally add the number of unique new passwords that will be 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.

**Step 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.

**Step 9** Optionally **Enforce password complexity** by selecting the check box. 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, !, $, #, %)

**Step 10** Optionally select the **Allow password changes** check box. This allows users to change their own passwords after their account is set up.

**Step 11** Optionally select the **Enable client certificate enforcement** check box to require the use of client certificates for login. By checking this box, you require the client to present a client certificate for strong mutual authentication. Two additional fields will appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this 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 will match the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

**Step 12** Optionally select the **One-time passwords** check box to enable the One-time password feature. A drop-down list will appear, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured will use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured will not be allowed to login.
- **using domain name** - Users in the domain will use the One Time Password feature. One Time Password emails for all users in the domain will be sent to username@domain.com.

**Step 13** If you select **using domain name**, an **E-mail domain** field appears below the drop-down list. Type in the domain name where one-time password emails will be sent (for example, abc.com).

**Step 14** Click **Accept** to update the configuration. Once the domain has been added, the domain will be added to the table on the Portals > Domains page.

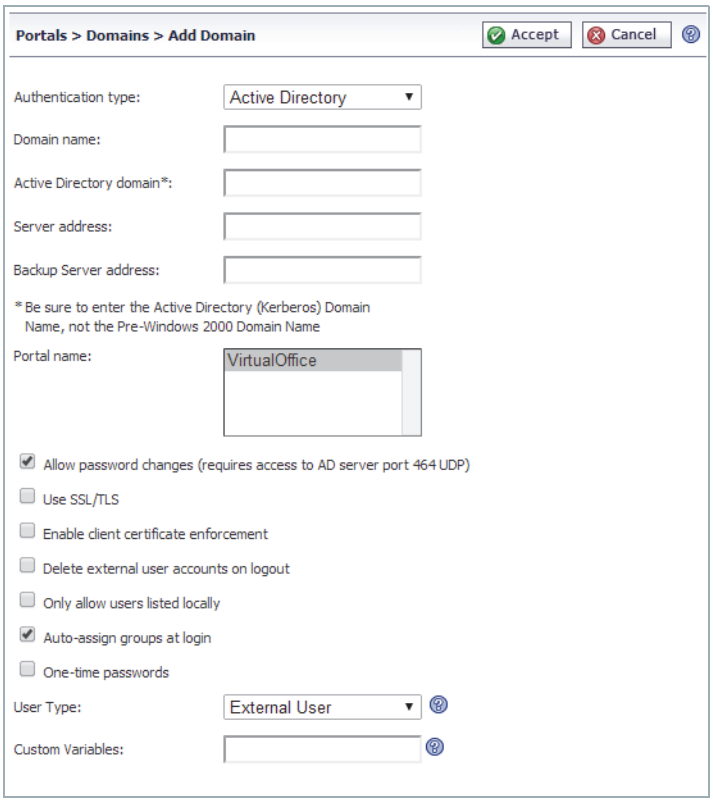
# Adding or Editing a Domain with Active Directory Authentication

To configure Windows Active Directory authentication, perform the following steps:

**Step 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 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 170.

**Step 2** If adding the domain, select **Active Directory** from the **Authentication type** drop-down list. The Active Directory configuration fields will be displayed.




**Step 3** If adding the domain, enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the 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.

**Step 4** Enter the Active Directory domain name in the **Active Directory Domain** field.

**Step 5** Enter the IP address or host and domain name of the Active Directory server in the **Server Address** field.

**Step 6** Enter the IP address or host and domain name of the back up server in the **Backup Server Address** field.

**Step 7** Enter the name of the layout in the **Portal Name** field. Additional layouts may be defined in the **Portals > Portals** page.

**Step 8** Optionally select the **Allow Password Changes** Check Box. Enabling this feature allows a user to change their password through the Virtual Office portal by selecting the **Options** button on the top of the portal page. User must submit their old password, along with a new password and a re-verification of the newly selected password.

**Step 9** Optionally select the **Use SSL/TLS** check box. 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.

**Step 10** Optionally select the **Enable client certificate enforcement** check box to require the use of client certificates for login. By checking this box, you require the client to present a client certificate for strong mutual authentication. Two additional fields will appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this 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 will match the client certificate:
  - User name: %USERNAME%

- Domain name: %USERDOMAIN%
- Active Directory user name: %ADUSERNAME%
- Wildcard: %WILDCARD%

**Step 11** Select the **Delete external user accounts on logout** check box to delete users who are not logged into a domain account after they log out.

**Step 12** Check the **Only allow users listed locally** check box to allow only users with a local record in the Active Directory to login.

**Step 13** Select the **Auto-assign groups at login** check box to assign users to a group when they log in.

Users logging into Active Directory domains are automatically assigned in real time to SRA groups based on their external AD group memberships. If a user's external group membership has changed, their SRA group membership automatically changes to match the external group membership.

**Step 14** Optionally, select the **One-time passwords** check box to enable the One Time Password feature. A drop-down list will appear, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured will use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured will not be allowed to login.
- **using domain name** - Users in the domain will use the One Time Password feature. One Time Password emails for all users in the domain will be sent to username@domain.com.

**Step 15** If you selected **if configured** or **required for all users** in the **One-time passwords** drop-down list, the Active Directory **AD e-mail attribute** drop-down list will appear, in which you can select **mail**, **mobile**, **pager**, **userPrincipalName**, or **custom**. These are defined as:

- **mail** - If your AD server is configured to store email addresses using the "mail" attribute, select **mail**.
- **mobile** or **pager** - If your AD server is configured to store mobile or pager numbers using either of these attributes, select mobile or pager, respectively. Raw numbers cannot be used, however, SMS addresses can.
- **userPrincipalName** - If your AD server is configured to store email addresses using the "userPrincipalName" attribute, select **userPrincipalName**.
- **custom** - If your AD server is configured to store email addresses using a custom attribute, select **custom**. If the specified attribute cannot be found for a user, the email address assigned in the individual user policy settings will be used. If you select **custom**, the **Custom attribute** field will appear. Type the custom attribute that your AD server uses to store email addresses. If the specified attribute cannot be found for a user, the email address will be taken from their individual policy settings.

If you select **using domain name**, an **E-mail domain** field appears below the drop-down list. Type in the domain name where one-time password emails will be sent (for example, abc.com).

**Step 16** Select the type of user from the **User Type** drop-down list. All users logging in through this domain will be 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 SRA admin credentials. These users are presented with the admin login page.

This option allows the SRA administrator to configure a domain that allows SRA admin privileges to all users logging into that domain.

Dell SonicWALL 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.

**Step 17** Click **Accept** to update the configuration. Once the domain has been added, the domain will be 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:

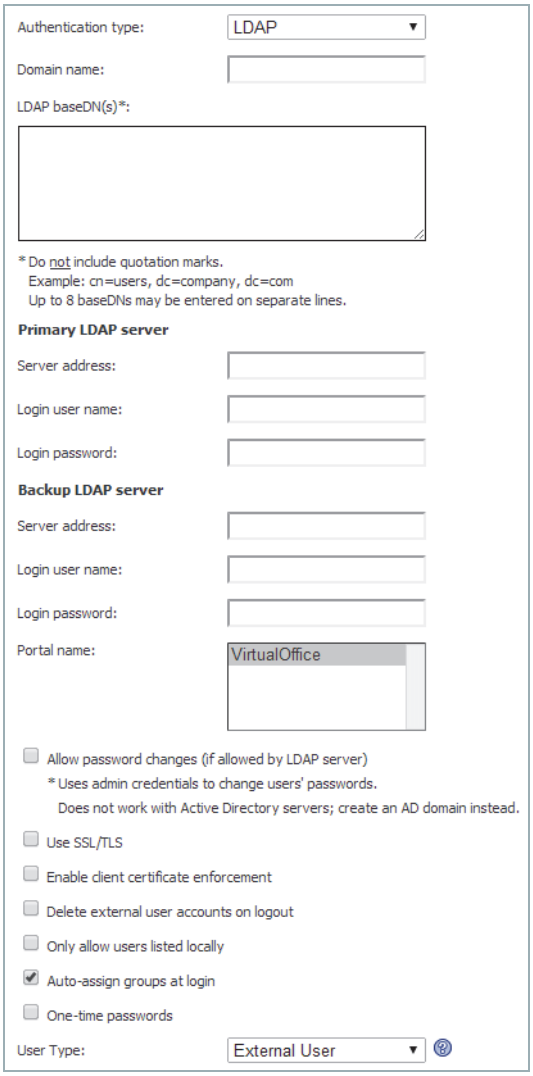
- The time settings on the Active Directory server and the SRA appliance must be synchronized. Kerberos authentication, used by Active Directory to authenticate clients, permits a maximum 15-minute time difference between the Windows server and the client (the SRA appliance). The easiest way to solve this issue is to configure Network Time Protocol on the **System > Time** page of the SRA Web-based management interface and check that the Active Directory server has the correct time settings.
- Confirm that your Windows server is configured for Active Directory authentication. If you are using Window NT4.0 server, then your server only supports NT Domain authentication. Typically, Windows 2000 and 2003 servers are also configured for NT Domain authentication to support legacy Windows clients.

# Adding or Editing a Domain with LDAP Authentication

To configure a domain with LDAP authentication, perform the following steps:

**Step 1** Click **Add Domain** or the Configure icon for the domain to edit. The **Add Domain** or **Edit Domain** window is displayed.

**Step 2** If adding the domain, select **LDAP** from the **Authentication Type** menu. The LDAP domain configuration fields are displayed.




**Step 3** If adding the domain, enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the SRA appliance user portal. It can be the same value as the Primary LDAP **Server Address** field.

**Step 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 will be automatically included when parents are added to this field.

**Note** Do not include quotes ("") in the **LDAP BaseDN** field.

**Step 5** Enter the IP address or domain name of the Primary LDAP server in the **Server Address** field.

**Step 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 SRA appliance binds to the LDAP tree with these credentials and users can log in with their sAMAccountName.

**Step 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.

**Step 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.

**Step 9** Enter the name of the layout in the **Portal Name** field. Additional layouts may be defined in the **Portals > Portals** page.

**Step 10** Optionally select the **Allow password changes (if allowed by LDAP server)** check box. This option, if allowed by your LDAP server, will enable users to change their LDAP password during an SRA session.

**Step 11** Optionally select the **Use SSL/TLS** check box. This option allows for the SSL/TLS encryption to be used for LDAP password exchanges. This option is disabled by default as not all LDAP servers are configured for SSL/TLS.

**Step 12** Optionally select the **Enable client certificate enforcement** check box to require the use of client certificates for login. By checking this box, you require the client to present a client certificate for strong mutual authentication. Two additional fields will appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this 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 will match the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

**Step 13** Select the **Auto-assign groups at login** check box to assign users to a group when they log in.

Users logging into LDAP domains are automatically assigned in real time to SRA groups based on their external LDAP attributes. If a user's external group membership has changed, their SRA group membership automatically changes to match the external group membership.

**Step 14** Optionally select the **One-time passwords** check box to enable the One Time Password feature. A drop-down list will appear, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured will use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured will not be allowed to login.
- **using domain name** - Users in the domain will use the One Time Password feature. One Time Password emails for all users in the domain will be sent to username@domain.com.

If you selected **if configured** or **required for all users** in the **One-time passwords** drop-down list, the **LDAP e-mail attribute** drop-down list will appear, in which you can select **mail**, **userPrincipalName**, or **custom**. These are defined as:

- **mail** - If your LDAP server is configured to store email addresses using the "mail" attribute, select **mail**.
- **mobile** or **pager** - If your AD server is configured to store mobile or pager numbers using either of these attributes, select mobile or pager, respectively. Raw numbers cannot be used, however, SMS addresses can.
- **userPrincipalName** - If your LDAP server is configured to store email addresses using the "userPrincipalName" attribute, select **userPrincipalName**.
- **custom** - If your LDAP server is configured to store email addresses using a custom attribute, select **custom**. If the specified attribute cannot be found for a user, the email address assigned in the individual user policy settings will be used. If you select **custom**, the **Custom attribute** field will appear. Type the custom attribute that your LDAP server uses to store email addresses. If the specified attribute cannot be found for a user, the email address will be taken from their individual policy settings.

If **using domain name** is selected in the **One-time passwords** drop-down list, the **E-mail domain** field will appear instead of the **LDAP e-mail attribute** drop-down list. Type in the domain name where one-time password emails will be sent (for example, abc.com).

**Step 15** Select the type of user from the **User Type** drop-down list. All users logging in through this domain will be 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 SRA admin credentials. These users are presented with the admin login page.

  This option allows the SRA administrator to configure a domain that allows SRA admin privileges to all users logging into that domain.

  Dell SonicWALL 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.

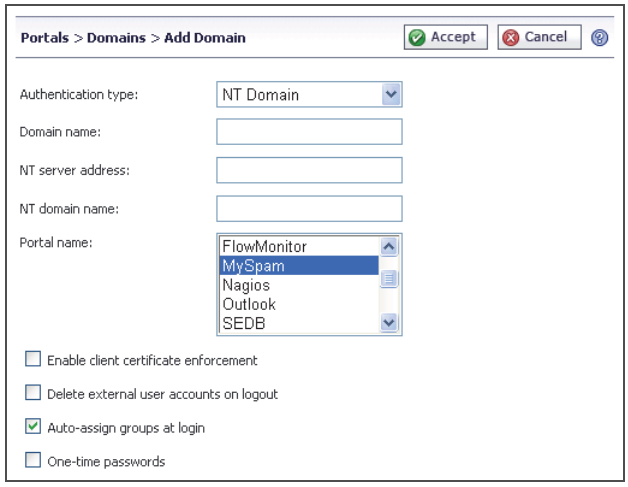
**Step 16** Click **Accept** to update the configuration. Once the domain has been added, the domain will be added to the table on the Portals > Domains page.

# Adding or Editing a Domain with NT Domain Authentication

To configure a domain with NT Domain authentication, perform the following steps:

**Step 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.

**Step 2** If adding the domain, select **NT Domain** from the **Authentication Type** menu. The NT Domain configuration fields will be displayed.




**Step 3** If adding the domain, enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name selected by users when they authenticate to the SRA appliance portal. It may be the same value as the **NT Domain Name**.

**Step 4** Enter the IP address or host and domain name of the server in the **NT Server Address** field.

**Step 5** Enter the NT authentication domain in the **NT Domain Name** field. This is the domain name configured on the Windows authentication server for network authentication.

**Step 6** Enter the name of the layout in the **Portal Name** field. Additional layouts may be defined in the **Portals > Portals** page.

**Step 7** Optionally select the **Enable client certificate enforcement** check box to require the use of client certificates for login. By checking this box, you require the client to present a client certificate for strong mutual authentication. Two additional fields will appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this 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 will match the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%

– Wildcard: %WILDCARD%

**Step 8** Select the **Delete external user accounts on logout** check box to delete users who are not logged into a domain account after they log out.

**Step 9** Select the **Auto-assign groups at login** check box to assign users to a group when they log in.

Users logging into NT domains are automatically assigned in real time to SRA groups based on their external NT group memberships. If a user's external group membership has changed, their SRA group membership automatically changes to match the external group membership.

**Step 10** Optionally select the **One-time passwords** check box to enable the One-time password feature. A drop-down list will appear, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured will use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured will not be allowed to login.
- **using domain name** - Users in the domain will use the One Time Password feature. One Time Password emails for all users in the domain will be sent to username@domain.com.

**Step 11** If you select **using domain name**, an **E-mail domain** field appears below the drop-down list. Type in the domain name where one-time password emails will be sent (for example, abc.com).

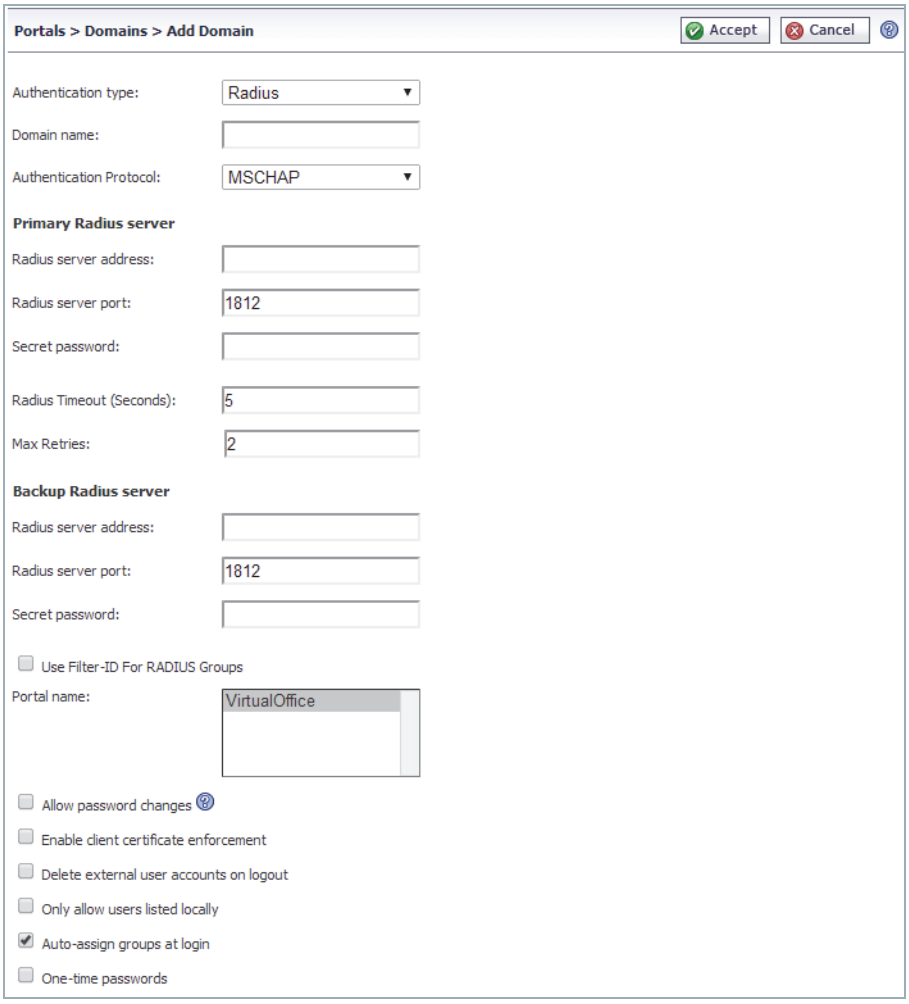
**Step 12** Click **Accept** to update the configuration. Once the domain has been added, the domain will be added to the table on the Portals > Domains page.

# Adding or Editing a Domain with RADIUS Authentication

To configure a domain with RADIUS authentication, perform the following steps:

**Step 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.

**Step 2** If adding the domain, select **RADIUS** from the **Authentication Type** menu. The **RADIUS configuration** field is displayed.




**Step 3** If adding the domain, enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the SRA appliance portal.

**Step 4** Select the proper **Authentication Protocol** for your RADIUS server. Choose from **PAP**, **CHAP**, **MSCHAP**, or **MSCHAPV2**.

**Step 5** Under **Primary Radius Server**, enter the IP address or domain name of the RADIUS server in the **RADIUS Server Address** field.

**Step 6** Enter the RADIUS server port in the **RADIUS server port** field.

**Step 7** If required by your RADIUS configuration, enter an authentication secret in the **Secret Password** field.

**Step 8** Enter a number (in seconds) for RADIUS timeout in the **RADIUS Timeout (Seconds)** field.

**Step 9** Enter the maximum number of retries in the **Max Retries** field.

**Step 10** Under **Backup Radius Server**, enter the IP address or domain name of the backup RADIUS server in the **RADIUS Server Address** field.

**Step 11** Enter the backup RADIUS server port in the **RADIUS server port** field.

**Step 12** If required by the backup RADIUS server, enter an authentication secret for the backup RADIUS server in the **Secret Password** field.

**Step 13** Optionally, if using RADIUS for group-based access, select the **Use Filter-ID for RADIUS Groups** check box.

**Step 14** Click the name of the layout in the **Portal Name** drop-down list.

**Step 15** If you selected the Authentication Protocol for your RADIUS server as MSCHAP or MSCHAPV2, you have the option to **Allow password changes** by selecting the check box. Note that if you enable password changes, you must also deploy the LAN Manager authentication.

**Step 16** Optionally select the **Enable client certificate enforcement** check box to require the use of client certificates for login. By checking this box, you require the client to present a client certificate for strong mutual authentication. Two additional fields will appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this 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 will match the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%
  - Wildcard: %WILDCARD%

**Step 17** Select the **Delete external user accounts on logout** check box to delete users who are not logged into a domain account after they log out.

**Step 18** Select the **Auto-assign groups at login** check box to assign users to a group when they log in.

Users logging into RADIUS domains are automatically assigned in real time to SRA groups based on their external RADIUS filter-IDs. If a user's external group membership has changed, their SRA group membership automatically changes to match the external group membership.

**Step 19** Optionally select the **One-time passwords** check box to enable the One-time password feature. A drop-down list will appear, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

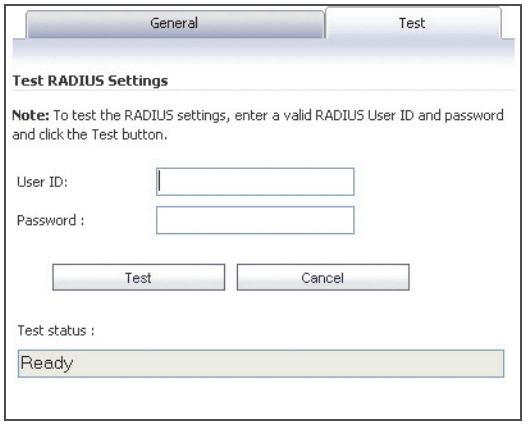
- **if configured** - Only users who have a One Time Password email address configured will use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured will not be allowed to login.

- **using domain name** - Users in the domain will use the One Time Password feature. One Time Password emails for all users in the domain will be sent to username@domain.com.

**Step 20** If you select **using domain name**, an **E-mail domain** field appears below the drop-down list. Type in the domain name where one-time password emails will be sent (for example, abc.com).

**Step 21** Click **Accept** to update the configuration. Once the domain has been added, the domain will be added to the table on the Portals > Domains page.

**Step 22** Click the configure button next to the RADIUS domain you added. The **Test** tab of the **Edit Domain** page displays.




**Step 23** Enter your RADIUS user ID in the **User ID** field and your RADIUS password in the **Password** field.

**Step 24** Click **Test**. The SRA appliance will connect to your RADIUS server.

**Step 25** 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 SRA appliance will attempt to authenticate against the specified RADIUS server using PAP authentication. It is generally required that the RADIUS server be configured to accept RADIUS client connections from the SRA appliance. Typically, these connections will appear to come from the SRA appliance X0 interface IP address. Refer to your RADIUS server documentation for configuration instructions.

# 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.

Dell SonicWALL'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 175.

The following sections describe how to configure the supported third-party authentication servers:

- Configuring the RSA Authentication Manager on page 179
- Configuring the VASCO IdentiKey Solution on page 184

## Configuring the RSA Authentication Manager

The following sections describe how to configure the RSA Authentication Manager version 6.1 to perform two-factor authentication with your SRA appliance:

- Adding an Agent Host Record for the SRA Appliance on page 179
- Adding the SRA Appliance as a RADIUS Client on page 180
- Setting the Time and Date on page 181
- Importing Tokens and Adding Users on page 182

**Note** This configuration procedure is specific to RSA Authentication Manager version 6.1. If you are using a different version of RSA Authentication Manager, the procedure will be slightly different.

If you will be using VASCO instead of RSA, see Configuring the VASCO IdentiKey Solution on page 184.

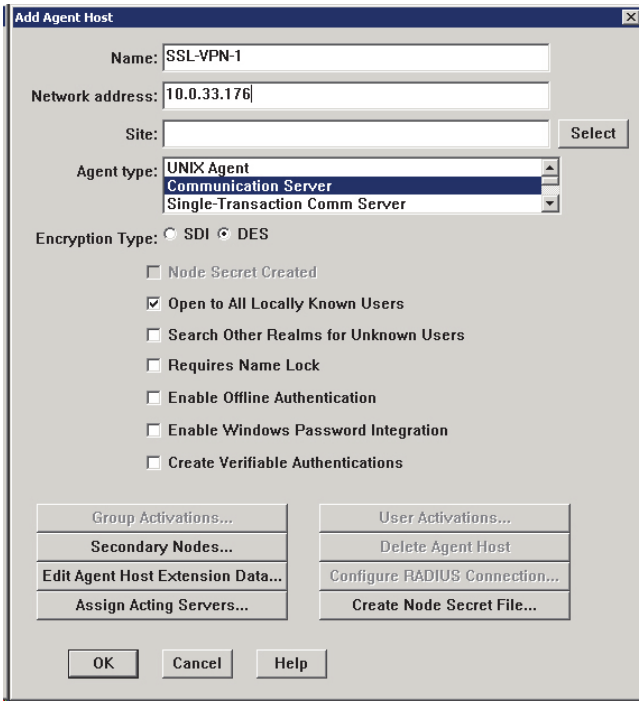
### Adding an Agent Host Record for the SRA Appliance

To establish a connection between the 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 SRA appliance within its database and contains information about communication and encryption.

To create the Agent Host record for the SRA appliance, perform the following steps:

**Step 1** Launch the RSA Authentication Manager.

**Step 2** On the **Agent Host** menu, select **Add Agent Host**. The **Add Agent Host** window displays.




**Step 3** Enter a hostname for the SRA appliance in the **Name** field.

**Step 4** Enter the IP address of the SRA appliance in the **Network address** field.

**Step 5** Select **Communication Server** in the **Agent type** window.

**Step 6** By default, the **Enable Offline Authentication** and **Enable Windows Password Integration** options are enabled. Dell SonicWALL recommends disabling all of these options except for **Open to All Locally Known Users**.

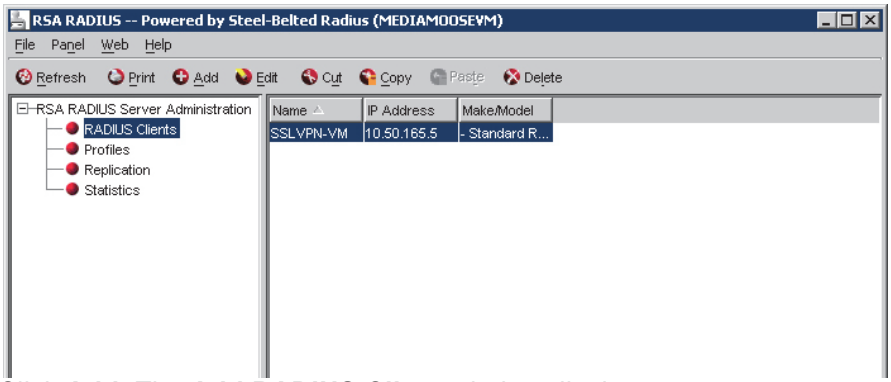
**Step 7** Click **OK**.

## Adding the SRA Appliance as a RADIUS Client

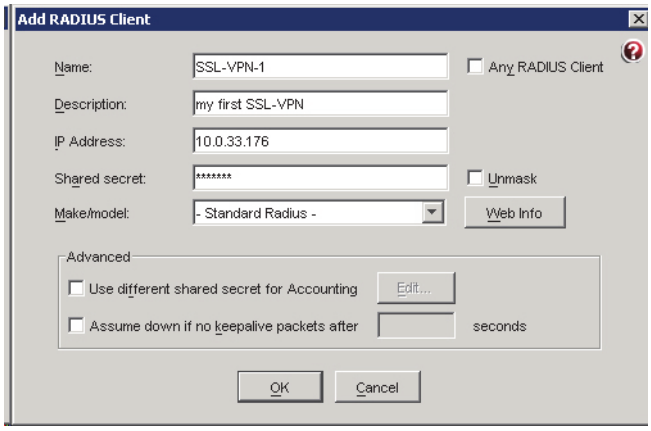
After you have created the Agent Host record, you must add the SRA appliance to the RSA Authentication Manager as a RADIUS client. To do so, perform the following steps:

**Step 1** In RSA Authentication Manager, go to the **RADIUS** menu and select **Manage RADIUS Server**. The **RSA RADIUS Manager** displays.

**Step 2** Expand the **RSA RADIUS Server Administration** tree and select **RADIUS Clients**.




**Step 3** Click **Add**. The **Add RADIUS Client** window displays.




**Step 4** Enter a descriptive name for the SRA appliance.

**Step 5** Enter the IP address of the SRA in the **IP Address** field.

**Step 6** Enter the shared secret that is configured on the SRA in the **Shared secret** field.

**Step 7** Click **OK** and close the RSA RADIUS Manager.

### Setting the Time and Date

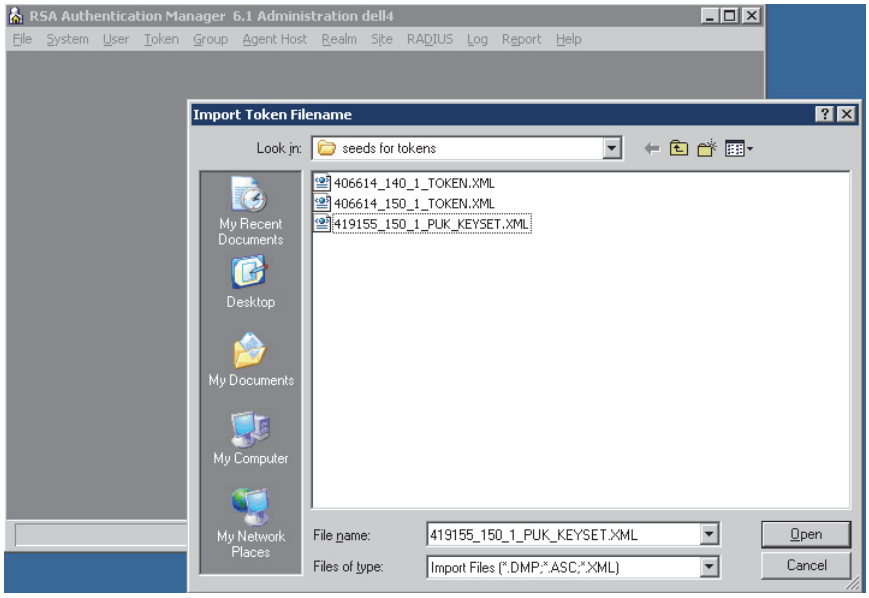
Because two-factor authentication depends on time synchronization, it is important that the internal clocks for the RSA Authentication Manager and the SRA appliance are set correctly.

## Importing Tokens and Adding Users

After you have configured the RSA Authentication Manager to communicate with the SRA appliance, you must import tokens and add users to the RSA Authentication Manager.

To import tokens and add users, perform the following steps:

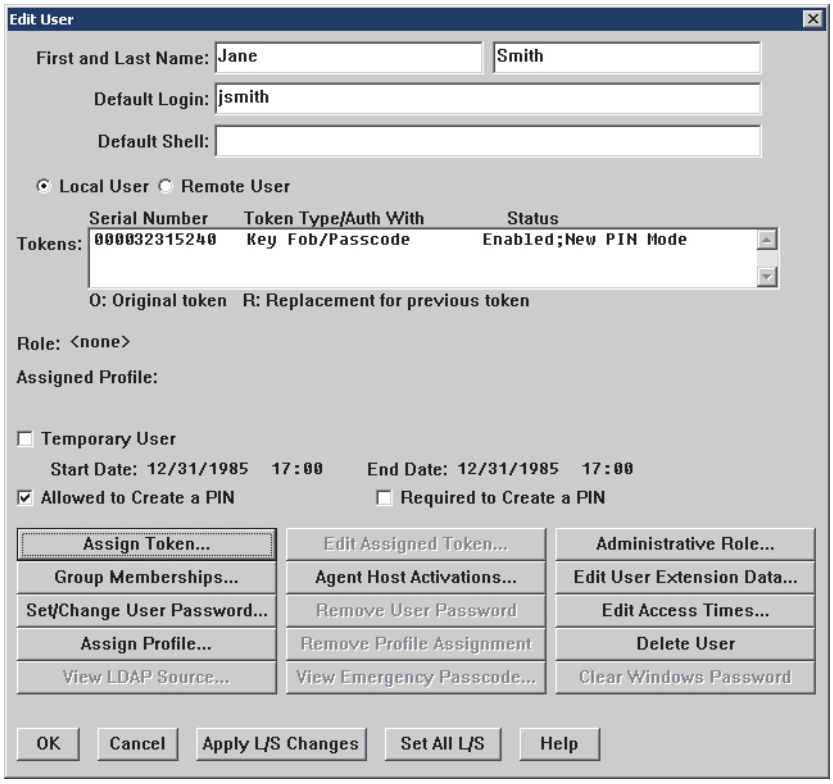
**Step 1** To import the token file, select **Token > Import Tokens**.




**Step 2** When you purchase RSA SecurID tokens, they come with an XML file that contains information on the tokens. Navigate to the token XML file and click **Open**. The token file is imported.

**Step 3** The **Import Status** window displays information on the number of tokens imported to the RSA Authentication Manager.

**Step 4** To create a user on the RSA Authentication Manager, click on **User > Add user**.

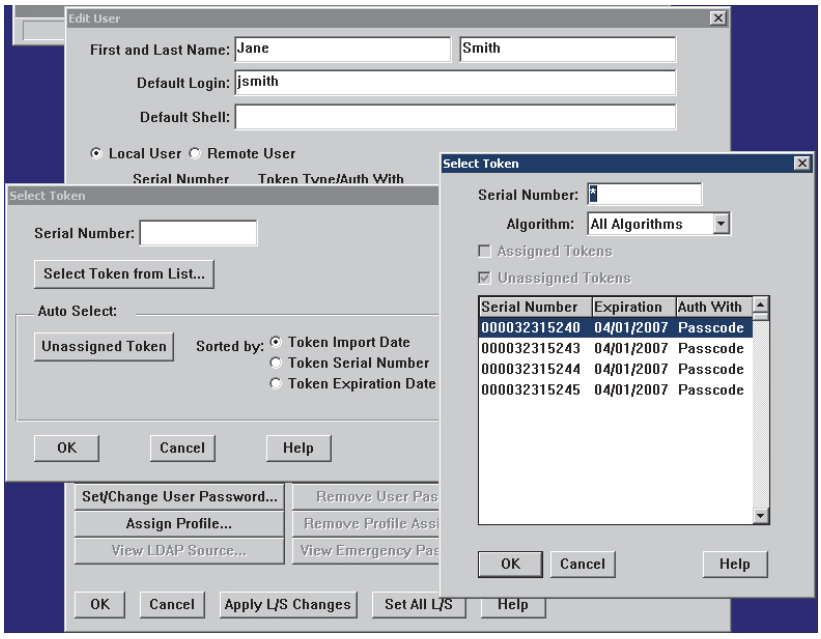



**Step 5** Enter the user's **First and Last Name**.

**Step 6** Enter the user's username in the **Default Login** field.

**Step 7** Select either **Allowed to Create a PIN** or **Required to Create a PIN**. **Allowed to Create a PIN** gives users the option of either creating their own PIN or having the system generate a random PIN. **Required to Create a PIN** requires the user to create a PIN.

**Step 8** To assign a token to the user, click on the **Assign Token** button. Click **Yes** on the confirmation window that displays. The **Select Token** window displays.




**Step 9** You can either manually select the token or automatically assign the token:

- To manually select the token for the user, click **Select Token from List**. In the window that displays, select the serial number for the token and click **OK**.
- To automatically assign the token, you can optionally select the method by which to sort the token: the token's import date, serial number, or expiration date. Then click the **Unassigned Token** button and the RSA Authentication Manager assigns a token to the user. Click **OK**.

**Step 10** Click **OK** in the **Edit User** window. The user is added to the RSA Authentication Manager.

**Step 11** Give the user their RSA SecurID Authenticator and instructions on how to log in, create a PIN, and user the RSA SecurID Authenticator. See the *Dell SonicWALL SRA User Guide* for more information.

## Configuring the VASCO IdentiKey Solution

The VASCO IdentiKey solution works with SRA 5.0 or higher. The following sections describe how to configure two-factor authentication using VASCO's IdentiKey version 3.2:


- Setting the Time on page 184
- Setting DNS and the Default Route on page 184
- Setting NetExtender Client Address Range and Route on page 185
- Creating a Portal Domain with RADIUS Authentication on page 185
- Configuring a Policy on VASCO IdentiKey on page 185
- Registering the SRA as a Client on page 186
- Configuring a VASCO IdentiKey User on page 186
- Importing DIGIPASS on page 186
- Assigning a DIGIPASS to a User on page 186
- Verifying Two-Factor Authentication on page 187


**Note** This configuration procedure is specific to VASCO IdentiKey version 3.2. If you are using a different version of VASCO IdentiKey, the procedure will be slightly different.

If you will be using RSA instead of VASCO, see Configuring the RSA Authentication Manager on page 179.

### Setting the Time

The DIGIPASS token is based on time synchronization. Since the two-factor authentication depends on time synchronization, it is important that the internal clocks for the SRA appliance and the VASCO IdentiKey are set correctly.

Navigate to System > Time on the SRA appliance to select the correct time zone.

### Setting DNS and the Default Route

The default route for the 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 SRA appliance.

To configure Domain Name Service and the default route:

**Step 1** On the SRA management interface, navigate to Network > DNS and set the correct DNS settings and/ or WINS Settings.

**Step 2** Navigate to Network > Routes and set the correct **Default Route** for the SRA **X0** interface.

### Setting NetExtender Client Address Range and Route

To configure the NetExtender client address range and route on the SRA appliance:

**Step 1** Navigate to NetExtender > Client Addresses to set the **NetExtender Client Address Range**.

Client Addresses will be assigned in the same subnet of the SRA X0 interface. Exclude the SRA appliance X0 interface and the firewall DMZ interface IP address.

**Step 2** Navigate to NetExtender > Client Routes.

Click the **Add Client Route** button to select the correct Client Routes for the authenticated remote users accessing the private networks via the SRA connection.

The client route corresponds with the subnet connected to the X0 (LAN) interface of the Dell SonicWALL NSA or TZ firewall.

### Creating a Portal Domain with RADIUS Authentication

To create a domain using RADIUS authentication on the SRA appliance:

**Step 1** Navigate to Portal > Domains and click **Add Domain**.

**Step 2** Select **Radius** from the **Authentication Type** drop-down list.

**Step 3** Enter the **Domain Name** that users will use in order to log into the SRA appliance portal.

### Configuring a Policy on VASCO IdentiKey

Follow these steps to add a new policy in the VASCO Identikey Web Administration interface:

**Step 1** Log in to the Vasco Identikey Web Administration window.

**Step 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

**Step 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 may be the same authentication service as previously used in the SRA appliance.

Use the following settings for the policy:

| | |
|---|---|
| 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 SRA as a Client

To register the SRA appliance as a VASCO client:

**Step 1** In the Vasco Identikey Web Administration window, click the **Clients** Tab and choose **Register**.

**Step 2** Select **RADIUS Client** for **Client Type**.

**Step 3** Enter the IP address of the SRA appliance.

**Step 4** In the **Policy ID** field, select your new policy.

**Step 5** Fill in the **Shared Secret** you entered for the RADIUS server properties on the SRA appliance.

**Step 6** Click **Create**.

### Configuring a VASCO IdentiKey User

To create a new user:

**Step 1** In the Vasco Identikey Web Administration window, click the **Users** tab and select **Create**.

**Step 2** Fill in the **User ID** field.

**Step 3** Select the **Domain**.

**Step 4** Select the **Organizational Unit**.

**Step 5** Click the **Create** button.

The user appears in the list of users in the Vasco Identikey Web Administration management interface.

### Importing DIGIPASS

To import a DIGIPASS:

**Step 1** In the Vasco Identikey Web Administration window, click on the **DIGIPASS** tab and select **Import**.

**Step 2** Browse for the ***.DPX** file.

**Step 3** Enter the **Transport Key**.

**Step 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.

**Step 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 the **Find** button and a list of all the available users in the same domain will appear. 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 will pop up.

### Verifying Two-Factor Authentication

To test the two-factor authentication SRA connectivity with VASCO IdentiKey:

**Step 1** Connect your PC on the WAN (X1) interface of the Dell SonicWALL firewall by pointing your browser to its IP address.

**Step 2** Login to the Local Domain as an Administrator.

**Step 3** Navigate to Portal > Domains and click **Configure** to test the RADIUS connectivity to VASCO IdentiKey.

**Step 4** If the RADIUS Authentication is successful, log out of the Administrator account and log in to the WAN (X1) interface of the Dell SonicWALL firewall with the User Name you created.

# Portals > Custom Logo

Beginning with the SRA 2.5 release, portal logos are no longer configured globally from the **Portals > Custom Logo** page. Custom logos are uploaded on a per-portal basis from the **Logo** tab in the **Portal Logo Settings** dialogue. For information related to Custom Portal Logos, refer to Adding a Custom Portal Logo on page 154.

# 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.

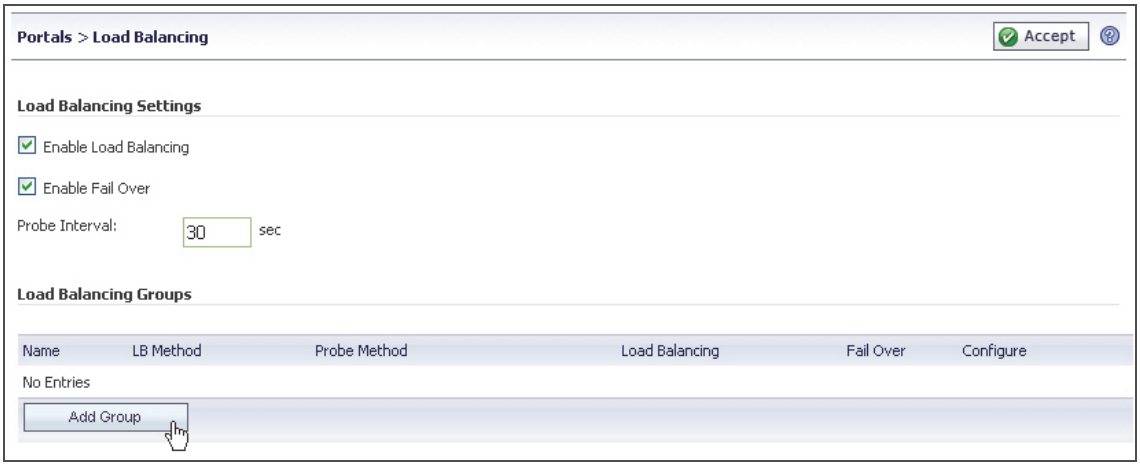

- Portals > Load Balancing Overview on page 187
- Configuring a Load Balancing Group on page 189


## 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.

***Figure 25 Portals > Load Balancing Page***




## Configuration Scenarios

Load Balancing for SRA SRA is a robust feature that has multiple uses, including:

**Balancing a Farm of Web Servers** – This is useful when the 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 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 SRA appliances.

**Load Balanced Pair** – In this scenario, the Load Balancer may 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 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 189.

| Option | Description |
|---|---|
| Enable Load Balancing | Enables the load balancing feature across all currently active groups. |
| Enable Failover | Enables/disables all probing, monitoring, and failover features. |
| Probe Interval | Determines the frequency (in seconds) at which the load balancing feature will check the status of backend nodes. |

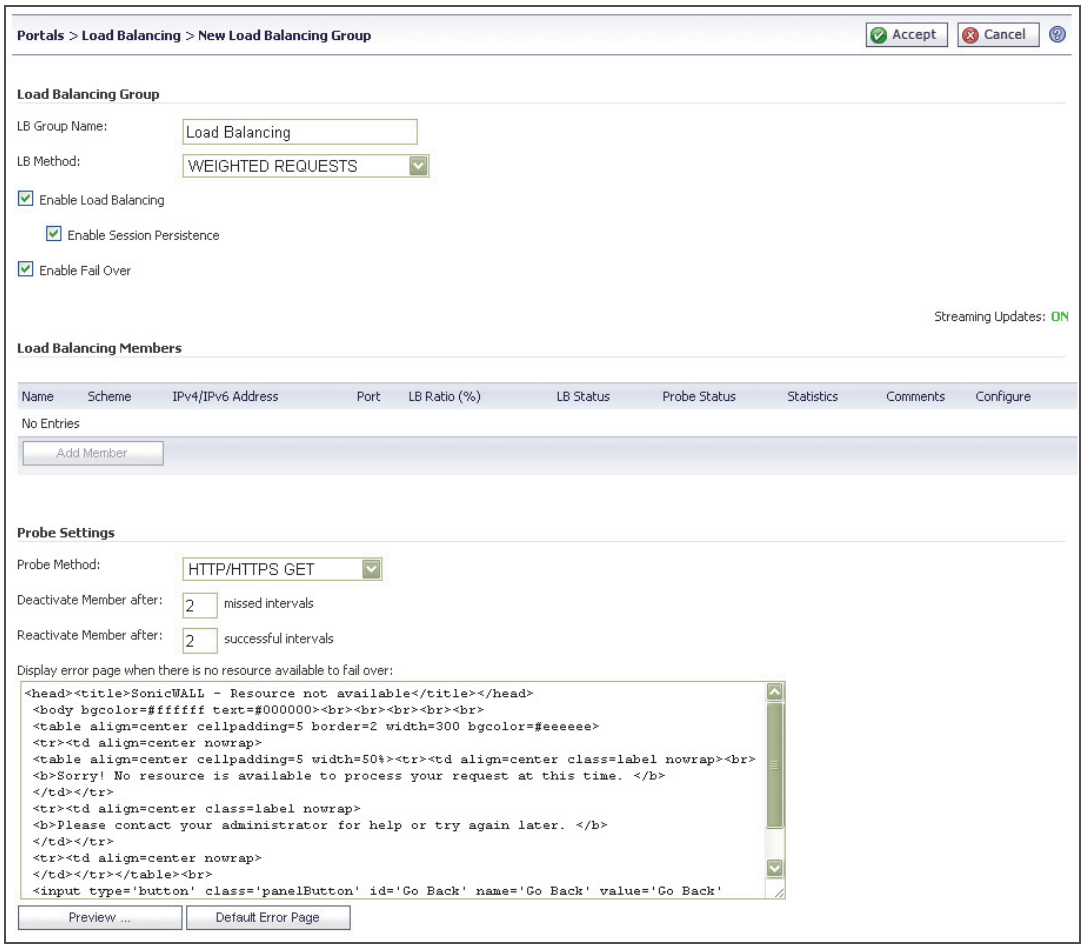
# Configuring a Load Balancing Group

This section provides configuration details for creating a new load balancing group and consists of the following sections:


- Adding a New Load Balancing Group on page 189
- Configuring Probe Settings on page 190
- Adding New Members to a Load Balancing Group on page 191


## Adding a New Load Balancing Group

**Step 1** In the **Portals > Load Balancing** page, click the **Add Group** button. The New Load Balancing Group configuration information displays.




**Step 2** Enter a friendly **LB Group Name** for this load balancing group.

**Step 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 will decide 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.

**Step 4** Select **Enable Load Balancing** to enable this group for load balancing.

**Step 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.

**Step 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 may be able to accept the session cookies of all users. In this case, the administrator may decide to turn off Session persistence. The Load Balancer will then strictly adhere to the LB method and LB factors in distributing the load.

**Step 7** To add a new member to the group, see Adding New Members to a Load Balancing Group on page 191.

## Configuring Probe Settings

To configure probe settings for this load balancing group in the **Probe Settings** section of the **Portals > Load Balancing** screen:

**Step 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.

**Step 2** In the **Deactivate Member after** field, enter the number of missed intervals required to fail the node. The default value is 2.

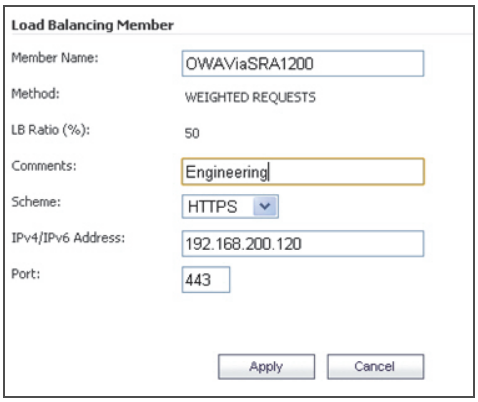
**Step 3** In the **Reactivate Member after** field, enter the number of successful intervals required to reinstate the node as functional. The default value is 2.

**Step 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

To add members to a new or existing load balancing group:

**Step 1** When editing or adding a group from the **Portals > Load Balancing** page, click the **Add Member** button. The Load Balancing Member screen displays.




**Step 2** Enter a **Member Name** to uniquely identify this member within the Load Balancing Group.

**Step 3** Enter a friendly name or description in the **Comment** field to identify this group by mousing over the group's page.

**Step 4** Select a **Scheme** to determine HTTP or HTTPS access. The default value is HTTPS.

**Step 5** Enter the back end HTTP(S) server IP address in the **IPv4/IPv6 Address** field.

**Step 6** Enter the **Port** for the back end server. The default value for an HTTPS connection is 443.

**Step 7** Click the **Accept** button to add this member to the group.

# Chapter 6

# Services Configuration

This chapter provides information and configuration tasks specific to the **Services** pages on the SRA Web-based management interface, including configuring settings, bookmarks, and policies for various application layer services, such as HTTP/HTTPS, Citrix, RDP, and VNC.

This chapter contains the following sections:

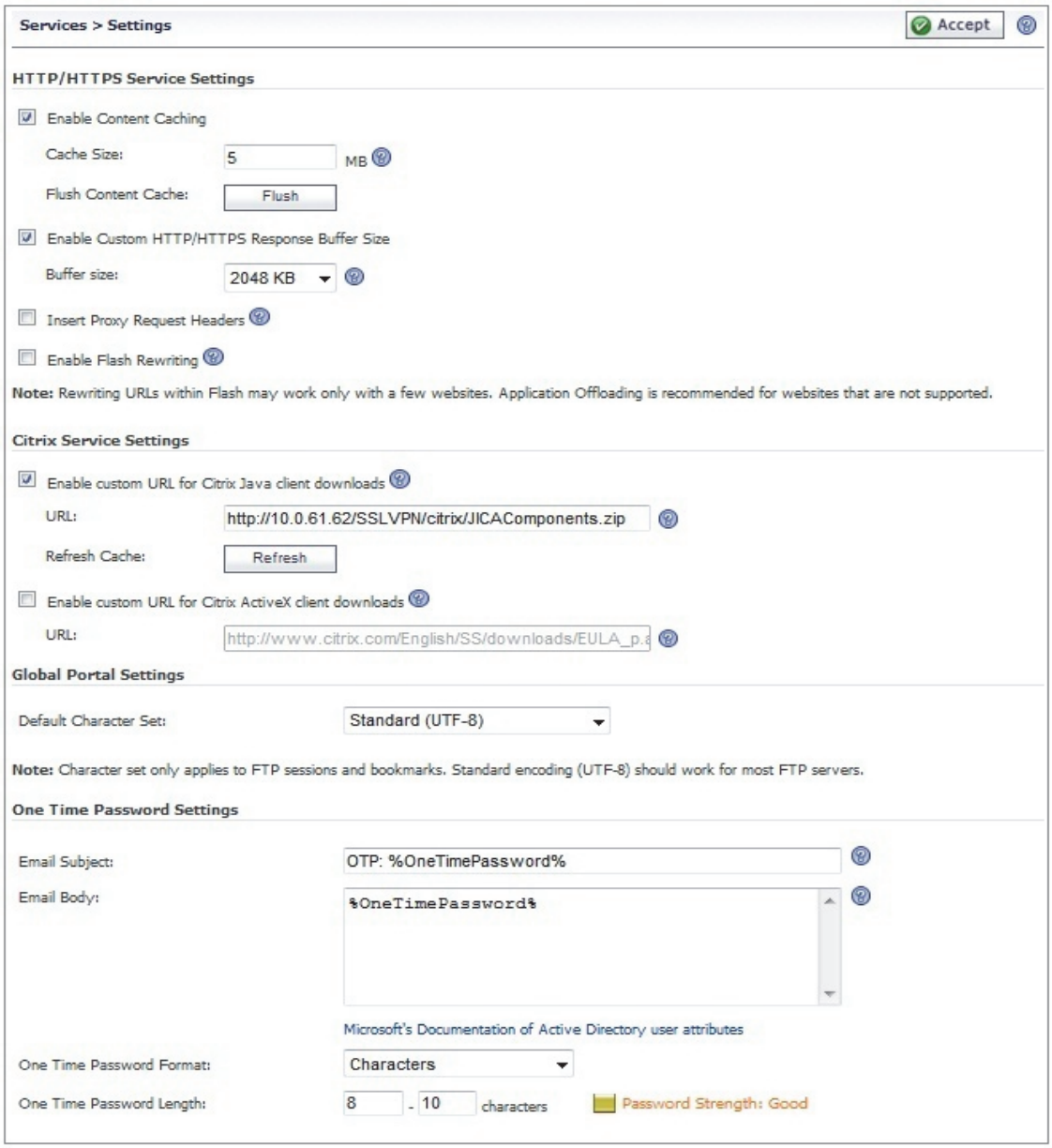

- Services > Settings on page 193
- Services > Bookmarks on page 197
- Services > Policies on page 209


## Services > Settings

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


- HTTP/HTTPS Service Settings on page 194
- Citrix Service Settings on page 195
- Global Portal Settings on page 195
- One Time Password Settings on page 195

The **Services > Settings** page allows the administrator to configure various settings related to HTTP/HTTPS, Citrix, Global Portal character sets, and one-time passwords.




## HTTP/HTTPS Service Settings

Administrators can take the following steps to configure HTTP/HTTPS Service Settings:

**Step 1** The **Enable Content Caching** check box is selected by default. Administrators may disable the check box if they choose to do so. However, changing the Enable Content Cache setting will restart SRA Services, including the web server.

In the **Cache Size** field, define the size of the desired content cache. 5 MB is the default setting, but administrators may set any size in the valid range from two to 20 MB. Select the **Flush** button to flush the content cache.

**Step 2** Check the **Enable Custom HTTP/HTTPS Response Buffer Size** check box, if you wish to establish a response buffer. Enabling this check box. Set the desired buffer size using the **Buffer size** drop-down menu. This limit is enforced for HTTP and HTTPS responses from the backend Web server for plain text, Flash, and Java applets. The default size of the buffer is 1024 KB.

**Step 3** Check the **Insert Proxy Request Headers** check box to insert these types of headers into the HTTP/HTTPS requests to the backend Web server. The following headers will be inserted:

- **X-Forwarded-For**: Specifies the client IP address of the original HTTP/HTTPS request.
- **X-Forwarded-Host**: Specifies the "Host" in the HTTP/HTTPS request from the client.
- **X-Forwarded-Server**: Specifies the host name of the SRA proxy server.

**Step 4** Check the **Enable Flash Rewriting** check box to rewrite URLs contained in Flash files. Rewriting URLs in Flash may 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 the SRA 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

Perform the following steps to configure Citrix Service Settings:

**Step 1** The Dell SonicWALL SRA appliance will always perform the Citirix client detection when using Citrix Bookmarks. Click the **Disable client detection by Citrix server** check box to disable this feature wen using Citrix Bookmarks. Note that this feature is compatible with Citrix XenAPP 5.0 or later.

**Step 2** Select the **Enable custom URL for Citrix Java client downloads** check box to use your own HTTP URL to download the Citrix Java client. Fill-in the custom URL in the **URL** field. If this option is not enabled, the default URL will be used.

**Step 3** Select the **Enable custom URL for Citrix ActiveX client downloads** check box to use your own HTTP URL to download the Citrix ActiveX client. Fill-in the custom URL in the **URL** field. If this option is not enabled, the default URL will be used.

## Global Portal Settings

**Step 1** Use the **Default Character Set** drop-down menu to set the language compatibility character set to be used with standard and non-standard FTP servers. The character set only applies to FTP sessions and bookmarks. Standard encoding (UTF-8), the default setting, should work for most FTP servers.

## One Time Password Settings

The **One Time Password Settings** section allows administrators to configure settings relating to the creation and communication of one-time passwords. One-time passwords are dynamically generated strings of characters, numbers or a combination of both. For

compatibility with mail services that allow a limited number of characters in the email subject (such as SMS), the administrator can customize the email subject to either include or exclude the one-time password. The email message body can also be configured in the same way. The administrator can also select the format (such as characters and numbers) for the password.

To configure the One Time Password email subject format, email body format, and change the default character types used when generating one time passwords, perform the following tasks:

**Step 1** In the **Email Subject** field, type the desired text for the one-time password email subject. The default subject consists of **OTP** plus the actual one-time password (represented here with the parameter placeholder **%OneTimePassword%**).

**Step 2** In the **Email Body** field, type the desired text for the one-time password email message body. The default message is simply the one-time password itself (represented here as **%OneTimePassword%**).

Variables can be used in the subject or body of a one-time password email:

- %**OneTimePassword**% - The user's one-time password. This should appear at least once in either the email subject or body.
- %**AD:mobile**% - The user's mobile phone as configured in Active Directory (AD).
- %**AD:_____**% - Any other Active Directory (AD) user attribute. See the Microsoft documentation link below the **Email Body** field for additional attributes.

**Step 3** In the **One Time Password Format** drop-down list, select one of the following three options:

- **Characters** – Only alphabetic characters will be used when generating the one-time password.
- **Characters and Numbers** – Alphabetic characters and numbers will be used when generating the one-time password.
- **Numbers** – Only numbers will be used when generating the one-time password.

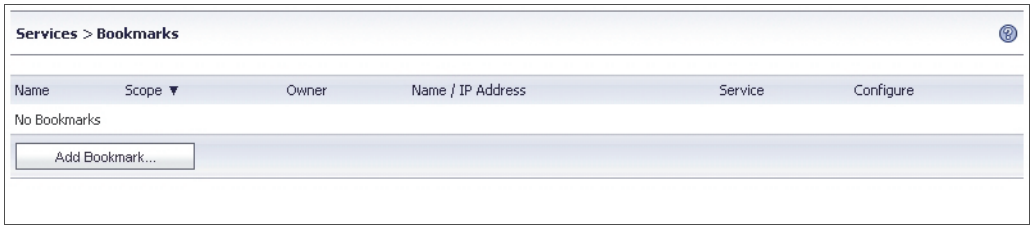
**Step 4** Use the **One Time Password Length** fields to adjust the range of characters allowed for one-time passwords.

**Step 5** Click the **Accept** button in the upper right corner of the **Services > Settings** page to save your changes.

For more information about the One Time Passwords feature, refer to One Time Password Overview on page 49.

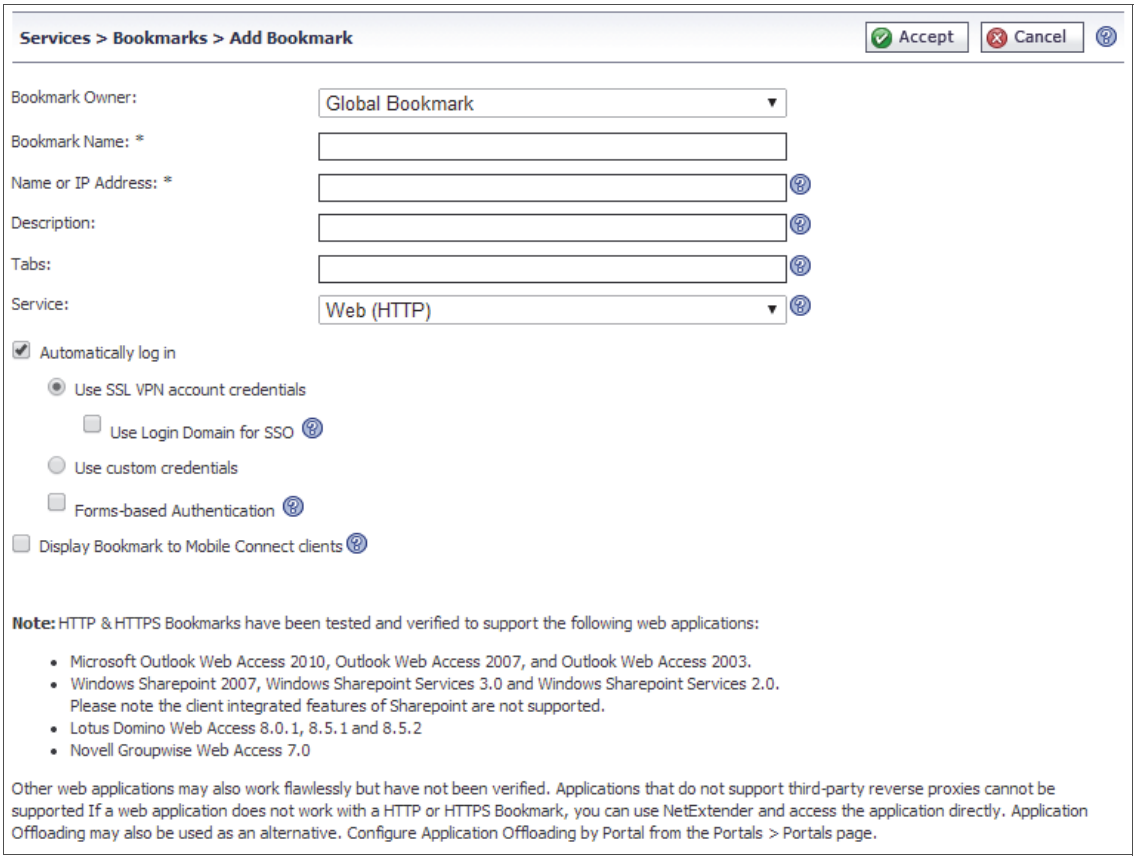
# Services > Bookmarks

The **Services > Bookmarks** page within the Web-based management interface provides a single interface for viewing bookmarks and access to configure bookmarks for users and groups.




Adding or Editing a Bookmark

To add a bookmark, navigate to the **Services > Bookmarks** screen within the management interface and select the **Add Bookmark...** button. The **Add Bookmark** window opens.




Complete the following steps to add a service bookmark:

**Step 1** Use the **Bookmark Owner** drop-down menu to select whether the bookmark is owned as a **Global Bookmark**, a **Local Domain** group bookmark, or a bookmark assigned to an individual **User**.

**Step 2** Fill-in the **Bookmark Name** field with a friendly name for the service bookmark.

**Step 3** Fill-in the **Name or IP Address** field with hostname, IP address, or IPv6 address for the desired bookmark. IPv6 addresses should begin with "[" and end with "]".

**Note** IPv6 is not supported 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 following table.

| Service Type | Format | Example for Name or IP Address Field |
|---|---|---|
| RDP - ActiveX<br>RDP - Java<br>RDP - HTML5 | IP Address<br>IPv6 Address<br>IP:Port (non-standard)<br>FQDN<br>Host name | 10.20.30.4<br>2008::1:2:3:4<br>10.20.30.4:6818<br>JBJONES-PC.sv.us.sonicwall.com<br>JBJONES-PC |
| VNC<br>VNC - HTML5 | IP Address<br>IPv6 Address<br>IP:Port (mapped to session)<br>FQDN<br>Host name<br>**Note**: Do not use session or display number instead of port. | 10.20.30.4<br>2008::1:2:3:4<br>10.20.30.4:5901 (mapped to session 1)<br>JBJONES-PC.sv.us.sonicwall.com<br>JBJONES-PC<br>**Note**: Do not use 10.20.30.4:1<br>**Tip**: For a bookmark to a Linux server, see the Tip below this table. |
| FTP | IP Address<br>IPv6 Address<br>IP:Port (non-standard)<br>FQDN<br>Host name | 10.20.30.4<br>2008::1:2:3:4<br>10.20.30.4:6818 or [2008::1:2:3:4]:6818<br>JBJONES-PC.sv.us.sonicwall.com<br>JBJONES-PC |
| Telnet | IP Address<br>IPv6 Address<br>IP:Port (non-standard)<br>FQDN<br>Host name | 10.20.30.4<br>2008::1:2:3:4<br>10.20.30.4:6818 or [2008::1:2:3:4]:6818<br>JBJONES-PC.sv.us.sonicwall.com<br>JBJONES-PC |
| SSHv1<br>SSHv2 | IP Address<br>IPv6 Address<br>IP:Port (non-standard)<br>FQDN<br>Host name | 10.20.30.4<br>2008::1:2:3:4<br>10.20.30.4:6818 or [2008::1:2:3:4]:6818<br>JBJONES-PC.sv.us.sonicwall.com<br>JBJONES-PC |
| HTTP<br>HTTPS | URL<br>IP Address of URL<br>IPv6 Address<br>URL:Path or File<br>IP:Path or File<br>URL:Port<br>IP:Port<br>URL:Port:Path or File<br>IP:Port:Path or File | www.sonicwall.com<br>204.212.170.11<br>2008::1:2:3:4<br>www.sonicwall.com/index.html<br>204.212.170.11/folder/<br>www.sonicwall.com:8080<br>204.212.170.11:8080 or [2008::1:2:3:4]:8080<br>www.sonicwall.com:8080/folder/index.html<br>204.212.170.11:8080/index.html |

| Service Type | Format | Example for Name or IP Address Field |
|---|---|---|
| File Shares | Host\Folder\<br>Host\File<br>FQDN\Folder<br>FQDN\File<br>IP\Folder\<br><br>IP\File | server-3\sharedfolder\<br>server-3\inventory.xls<br>server-3.company.net\sharedfolder\<br>server-3company.net\inventory.xls<br>10.20.30.4\sharedfolder\<br>10.20.30.4\status.doc<br>**Note**: Use backslashes even on Linux or Mac computers; these use the Windows API for file sharing. |
| Citrix<br>(Citrix Web Interface) | IP Address<br>IPv6 Address<br>IP:Port<br>IP:Path or File<br>IP:Port:Path or File<br>FQDN<br>URL:Path or File<br>URL:Port<br>URL:Port:Path or File<br>**Note**: *Port* refers to the HTTP(S) port of Citrix Web Interface, not to the Citrix client port. | 172.55.44.3<br>2008::1:2:3:4<br>172.55.44.3:8080 or [2008::1:2:3:4]:8080<br>172.55.44.3/folder/file.html<br>172.55.44.3:8080/report.pdf<br>www.citrixhost.company.net<br>www.citrixhost.net/folder/<br>www.citrixhost.company.com:8080<br>www.citrixhost.com:8080/folder/index.html |

Tip When creating a **Virtual Network Computing (VNC)** bookmark to a Linux server, you must specify the port number and server number in addition to the Linux server IP the **Name or IP Address** field in the form of **ipaddress:port:server**. For example, if the Linux server IP address is 192.168.2.2, the port number is 5901, and the server number is 1, the value for the **Name or IP Address** field would be **192.168.2.2:5901:1**.

**Step 4** Use the **Service** drop-down menu to select the desired bookmark service. Use the following information for the chosen service to complete the building of the bookmark.

**Terminal Services (RDP - ActiveX) or Terminal Services (RDP - Java)**

Note If you select **Terminal Services (RDP - ActiveX)** while using a browser other than Internet Explorer, the selection is automatically switched to **Terminal Services (RDP - Java)**. A popup dialog box notifies you of the switch.

– In the **Screen Size** drop-down list, select the default terminal services screen size to be used when users execute this bookmark.

Because different computers support different screen sizes, when you use a remote desktop application, you should select the size of the screen on the computer from which you are running a remote desktop session. Additionally, you may want to provide a path to where your application resides on your remote computer by typing the path in the **Application Path** field.

– In the **Colors** drop-down list, select the default color depth for the terminal service screen when users execute this bookmark.

– Optionally, enter the local path for this application in the **Application and Path** field.

– In the **Start in the following folder** field, optionally enter the local folder in which to execute application commands.

– Select the **Login as console/admin session** check box to allow login as console or admin. Login as admin replaces login as console in RDC 6.1 and newer.

– Select the **Enable wake-on-LAN** check box 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 the **Send WOL packet to host name or IP address** check box, which can be applied in tandem with a MAC address of another machine to wake.

– Check the **Server is TS Farm** check box if the bookmark will be 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.

– For **RDP - ActiveX** on Windows clients, expand **Show client redirect options** and select any of the redirect check boxes **Redirect Printers**, **Redirect Drives**, **Redirect Ports**, or **Redirect SmartCards** to redirect those devices on the local network for use in this bookmark session. You can hover your mouse pointer over these options to display tooltips that indicate requirements for certain actions.

  To see local printers show up on your remote machine (Start > Settings > Control Panel > Printers and Faxes), select **Redirect Ports** as well as **Redirect Printers**.

– For **RDP - Java** on Windows clients, or on Mac clients running Mac OS X 10.5 or above with RDC installed, expand **Show advance Windows options** and select the check boxes for any of the following redirect options: **Redirect Printers**, **Redirect Drives**, **Redirect Ports**, **Redirect SmartCards**, **Redirect clipboard**, or **Redirect plug and play devices** to redirect those devices or features on the local network for use in this bookmark session. You can hover your mouse pointer over the Help icon next to certain options to display tooltips that indicate requirements.

  To see local printers show up on your remote machine (Start > Settings > Control Panel > Printers and Faxes), select **Redirect Ports** as well as **Redirect Printers**.

  Select the check boxes for any of the following additional features for use in this bookmark session: **Display connection bar**, **Auto reconnection**, **Desktop background**, **Window drag**, **Menu/window animation**, **Themes**, or **Bitmap caching**.

  If the client application will be RDP 6 (Java), you can select any of the following options as well: **Dual monitors**, **Font smoothing**, **Desktop composition**, or **Remote Application**.
  **Remote Application** monitors server and client connection activity; to use it, you need to register remote applications in the Windows 2008 RemoteApp list. If **Remote Application** is selected, the Java Console will display messages regarding connectivity with the Terminal Server.

– Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current SRA session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

**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 may want to provide a path to where your application resides on your remote computer by typing the path in the **Application Path** field.

- In the **Colors** drop-down list, select the default color depth for the terminal service screen when users execute this bookmark.
- Select the **Enable wake-on-LAN** check box 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 the **Send WOL packet to host name or IP address** check box, which can be applied in tandem with a MAC address of another machine to wake.
- Select the **Login as console/admin session** check box to allow login as console or admin. Login as admin replaces login as console in RDC 6.1 and newer.
- Check the **Server is TS Farm** check box if the bookmark will be 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 checkboxes 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 SRA session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

**Terminal Services (Using Tunnel)**

- In the **Screen Size** drop-down list, select the default terminal services screen size to be used when users execute this bookmark.

Because different computers support different screen sizes, when you use a remote desktop application, you should select the size of the screen on the computer from which you are running a remote desktop session. Additionally, you may want to provide a path to where your application resides on your remote computer by typing the path in the **Application Path** field.

- In the **Colors** drop-down list, select the default color depth for the terminal service screen when users execute this bookmark.
- Select the **Enable wake-on-LAN** check box 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 the **Send WOL packet to host name or IP address** check box, which can be applied in tandem with a MAC address of another machine to wake.

– **Application and Path** — The vale entered here is a valid path of an alternate shell or an executable application.

– **Command-line arguments** — Enter the command line arguments for the RemoteApp.

– **Start in the following folder** — Enter the folder you want to start with.

– Select the **Login as console/admin session** check box to allow login as console or admin. Login as admin replaces login as console in RDC 6.1 and newer.

– Check the **Server is TS Farm** check box if the bookmark will be 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 checkboxes for the following options: **Desktop background**, **Menu/window animation**, **Show window contents while dragging/resizing**, and **View styles**. There is also an RDP6 option for **Font smoothing**.

– Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current SRA session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

**Virtual Network Computing (VNC)**

– In the **Encoding** drop-down menu, select the desired encoding transfer format.

– Optionally, if available, use the **Compression Level** drop-down menu to select the desired compression level for data.

– Optionally, if available, select the JPEG image file quality level using the **JPEG Image Quality** drop-down menu.

– In the **Cursor Shape Updates** drop-down menu, select to either Enable, Disable, or Ignore these updates.

– Enable or disable the **CopyRect** function using the associated check box.

– Enable or disable the use of only **Restricted Colors** by using the associated check box.

– Enable or disable the ability to **reverse control of mouse buttons two and three** using the associated check box.

– Enable the **View Only** check box to control to prevent taking control over VNC.

– Enable the **Share Desktop** check box to allow desktop view to be shared over VNC.

**Virtual Network Computing (VNC - HTML5)**

– Enable the **View Only** check box to control to prevent taking control over VNC.

– Enable the **Share Desktop** check box 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.

- Optionally, select **HTTPS Mode** to use HTTPS to securely access the Citrix Portal. HTTPS mode is used to encrypt communication between the SRA device and the Citrix server using the SSL protocol.
- Optionally, select **Always use Java in Internet Explorer** to use Java to access the Citrix Portal when using Internet Explorer. Without this setting, a Citrix ActiveX client or plugin must be used with IE. This setting lets users avoid installing a Citrix client or plugin specifically for IE browsers. Java is used with Citrix by default on other browsers and also works with IE. Enabling this check box leverages this portability.
- 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.

**Web (HTTP)**

- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current SRA session for login to the Web server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

**Secure Web (HTTPS)**

- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current SRA session for login to the secure Web server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

**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 checkbox 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.

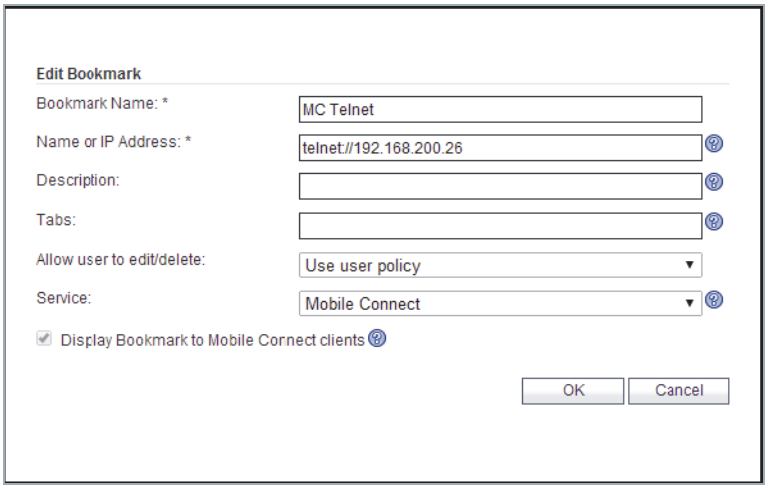
**Mobile Connect**

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.

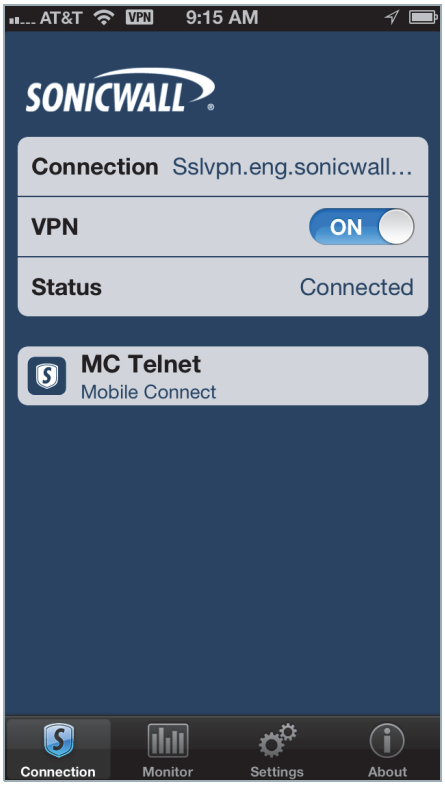
**Note** The Mobile Connect bookmark may also be used for 'http://' or 'https://' URL schemes, however, Dell SonicWALL recommends using HTTP or HTTPS bookmarks for these schemes.

- Enter the **Bookmark Name** and the **Name or IP Address**. The Name or IP Address field is the custom URL scheme.

– Enable the **Display Bookmark to Mobile Connect clients** check box to send bookmark information to Mobile Connect clients.

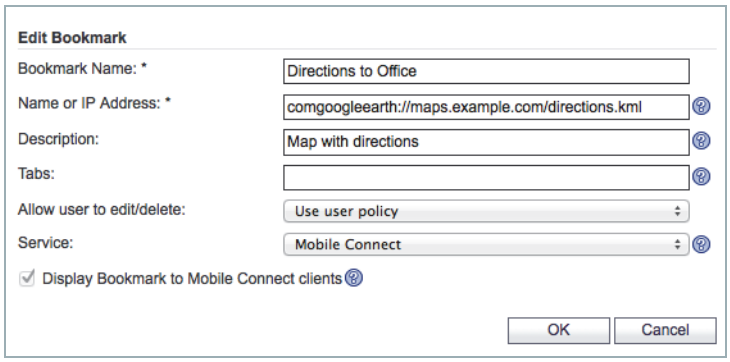



Once the Mobile Connect bookmark on the SRA is successfully configured, the bookmark will display on your mobile device:

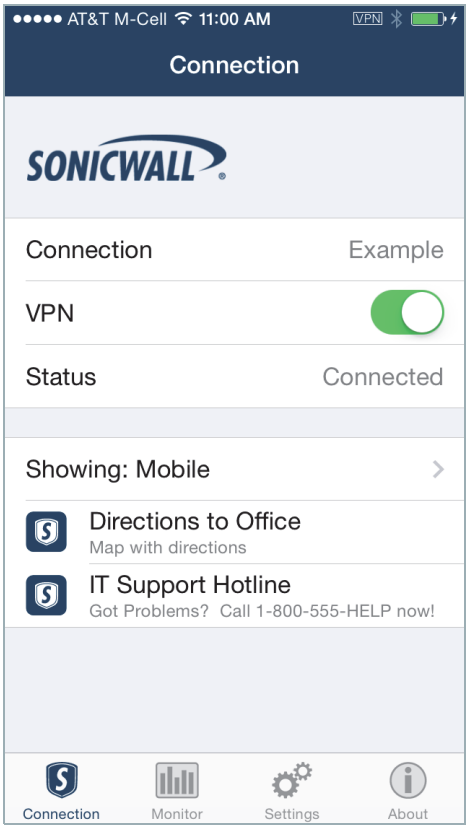



The following example of a Mobile Connect bookmark shows how a user can create a bookmark using Google Earth to display a map with specific directions.

First, the user must create the bookmark with the URL scheme:

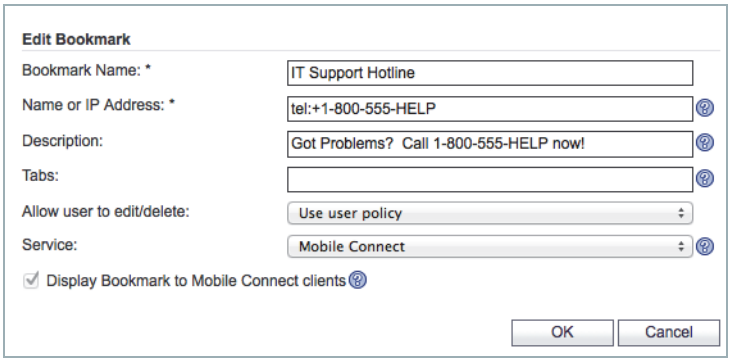



This bookmark is now available to access from your mobile device.

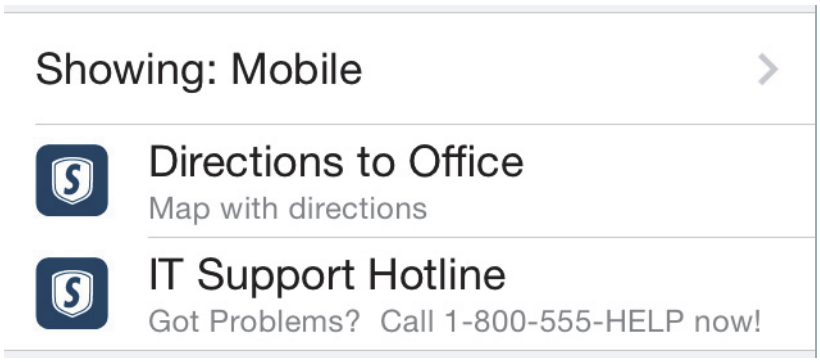


Click the newly added bookmark. For the “Directions to Office” bookmark, a Google Map displays:

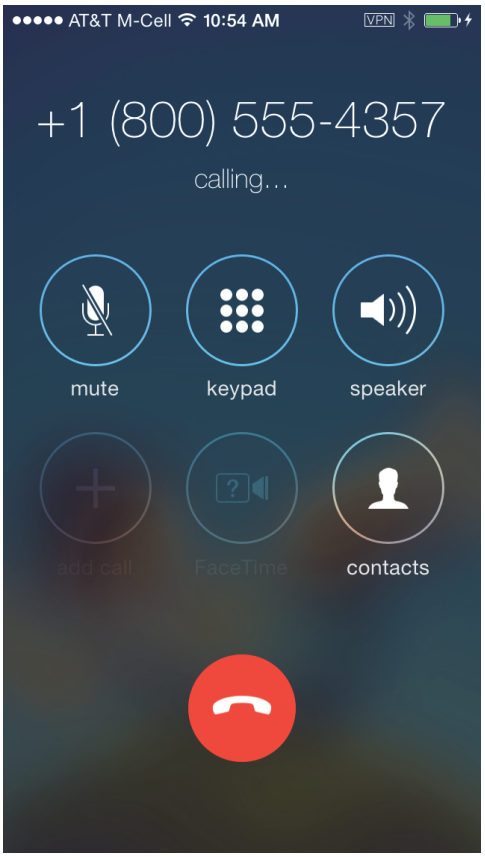
The following example shows another way to use the Mobile Connect bookmark. In this example, the user adds a bookmark that launches the Phone app on iOS to make a call to the IT Support Hotline.



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)**

- To allow users to use a Java Applet for File Shares that mimics Windows functionality, select the **Use File Shares Java Applet** check box.
- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current SRA session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

When creating a File Share, do not configure a Distributed File System (DFS) server on a Windows Domain Root system. Because the Domain Root allows access only to Windows computers in the domain, doing so will disable access to the DFS file shares from other domains. The SRA appliance is not a domain member and will not be able to connect to the DFS shares.

DFS file shares on a stand-alone root are not affected by this Microsoft restriction.

**File Transfer Protocol (FTP)**

- Expand **Show advanced server configuration** to select an alternate value in the **Character Encoding** drop-down list. The default is **Standard (UTF-8)**.
- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current SRA session for login to the FTP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

**Telnet**

- No additional fields

**Secure Shell version 1 (SSHv1)**

- No additional fields

**Secure Shell version 2 (SSHv2)**

- Optionally select the **Automatically accept host key** check box.
- If using an SSHv2 server without authentication, such as a Dell SonicWALL firewall, you can select the **Bypass username** check box.

**Step 5** To display the bookmark (Desktop, Web, and Terminal services only) on mobile devices using Mobile Connect 2.0 or higher, check the **Display Bookmark to Mobile Connect clients** check box.

**Note** Support varies by device and third party applications on the mobile device.

**Step 6** Click **OK** to update the configuration. Once the configuration has been updated, the new user bookmark will be displayed in the **Services >Bookmarks** window.

Editing a Bookmark

To edit a service bookmark, navigate to the **Services > Bookmarks** screen. Click on the **pencil icon** in the **Configure** column. A new **Edit Bookmark** window will open with the bookmark's current configuration. Make all desired adjustments and select **OK**. The edited bookmark will still display in the **Services > Bookmarks** window.

Deleting a Bookmark

To delete a configured bookmark, navigate to the **Services > Bookmarks** screen. Click on the "**X**" icon in the **Configure** column. A dialog box will open and ask if you are sure you want to delete the specified bookmark. Click **OK** to delete the bookmark. The bookmark will no longer appear in the Services > Bookmarks screen.

# Services > Policies

The **Services > Policies** page within the Web-based management interface provides a single interface for viewing service policies and access to configure policies for users and groups.

# Adding a Policy

To add a policy, navigate to the **Services > Policies** screen within the management interface and select the **Add Policy...** button. The **Add Policy** window opens.

Administrators can follow the following steps to add a service policy:

**Step 1** Use the **Policy Owner** drop-down menu to select whether the policy is owned as a **Global Policy**, a **Local Domain** group policy, or a policy assigned to an individual **User**.

**Step 2** In the **Apply Policy To** drop-down menu, select whether the policy will be applied to an individual host, a range of addresses, all addresses, a network object, a server path, or a URL object. 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 SRA policies apply to the destination address(es) of the SRA connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the 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 364.

**Step 3** Follow the appropriate step below depending on your selection in the **Apply Policy To** menu.

- **IP Address** - If your policy applies to a specific host, enter the IP address of the local host machine in the **IP Address** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field. See Adding a Policy for an IP Address on page 348.
- **IP Address Range** - If your policy applies to a range of addresses, enter the beginning IP address in the **IP Network Address** field and the subnet mask that defines the IP address range in the **Subnet Mask** field. Optionally, enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field. See Adding a Policy for an IP Address Range on page 348.
- **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 348.
- **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 137
- **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 348.
- **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 350.
- **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 351.
- **IPv6 Address Range** - If your policy applies to a range of addresses, enter the beginning IPv6 address in the **IPv6 Network Address** field and the prefix that defines the IPv6 address range in the **IPv6 Prefix** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field. See Adding a Policy for an IPv6 Address Range on page 352.
- **All IPv6 Address** - If your policy applies to all IPv6 addresses, you do not need to enter any IP address information. See Adding a Policy for All IPv6 Addresses on page 352.

**Step 4** Select the service type in the **Service** drop-down list. If you are applying a policy to a network object, the service type is defined in the network object.

**Step 5** Select **ALLOW** or **DENY** from the **Status** drop-down list to either allow or deny 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.

**Step 6** Click **Accept** to update the configuration. Once the configuration has been updated, the new policy will be displayed in the **Services > Policies** window.

# Editing a Policy

To edit a service-related policy, navigate to the **Services > Policies** screen. Click on the **pencil icon** in the **Configure** column. A new **Edit Policy** window will open with the bookmark's current configuration. Make all desired adjustments and select **Accept**. The edited bookmark will still display in the **Services > Policies** window.

# Deleting a Policy

To delete a configured policy, navigate to the **Services > Policies** screen. Click on the "**X**" icon in the **Configure** column. A dialog box will open and ask if you are sure you want to delete the specified policy. Click **OK** to delete the policy. The policy will no longer appear in the **Services > Policies** screen.

# Chapter 7

# NetExtender Configuration

This chapter provides information and configuration tasks specific to the NetExtender pages on the SRA Web-based management interface.

NetExtender is an SRA client for Windows, Mac, Linux, or Android smartphone users that is downloaded transparently and allows you to run any application securely on the company's network. It uses Point-to-Point Protocol (PPP). NetExtender allows remote clients to have seamless access to resources on your local network.

Users can access NetExtender two ways: Using the Net Extender button on the SRA user portal, or by using the NetExtender standalone client, which is installed by clicking on the NetExtender button in the SRA 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 pathname or from the shortcut bar on Linux systems, and with the icon on Android smartphones.

On Windows systems, NetExtender supports establishing a VPN session before logging in to Windows.

The standalone NetExtender Mobile client is available for devices running Windows Mobile 5 PocketPC and Windows Mobile 6 Professional/Classic.

The SRA appliance supports client certificates in both the standalone Windows NetExtender client and the NetExtender Mobile client.

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 42. For information about using or installing the NetExtender, NetExtender Mobile, or NetExtender Android clients, see the latest *Dell SonicWALL SRA User's Guide*, available on the Secure Remote Access pages of the Dell SonicWALL Support Web site at: http://www.sonicwall.com/us/Support.html

This chapter contains the following sections:


- NetExtender > Status on page 214
- NetExtender > Client Settings on page 215
- NetExtender > Client Routes on page 219
- NetExtender > Advanced Settings on page 221
- NetExtender > Client Downloads on page 222
- admin_netextenderlog on page 222
- NetExtender User and Group Settings on page 223

# NetExtender > Status

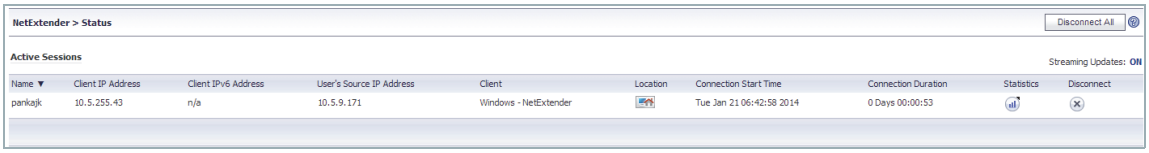
This section provides an overview of the **NetExtender > Status** page and a description of the configuration tasks available on this page.


- NetExtender > Status Overview on page 214
- Viewing NetExtender Status on page 214


## NetExtender > Status Overview

The **NetExtender > Status** page allows the administrator to view active NetExtender sessions, including the name, IP address, login time, length of time logged in and logout time.

***Figure 26 NetExtender > Status***




## Viewing NetExtender Status

The **NetExtender > Status** page allows the administrator to view active NetExtender sessions, including the name, IP address, login time, length of time logged in and administrative logout control. Table 15, “NetExtender Status,” on page 214 provides a description of the status items.

***Table 15 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 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 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

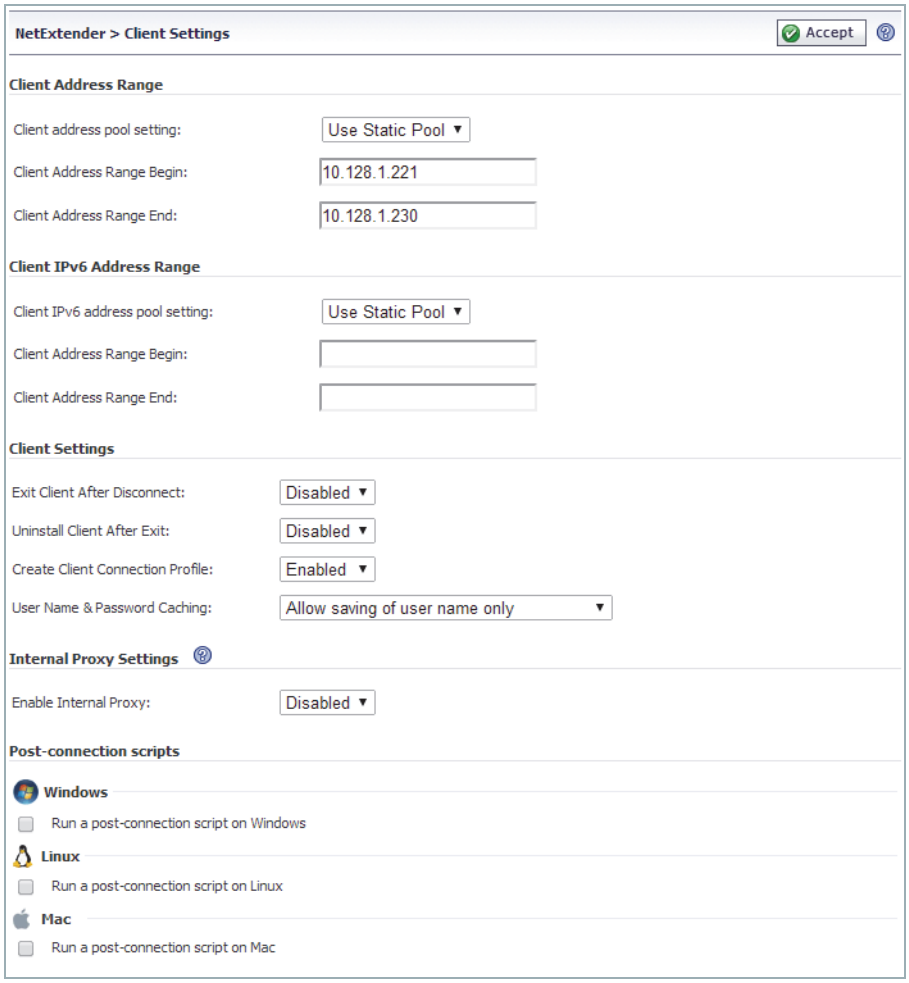
This section provides an overview of the **NetExtender > Client Settings** page and a description of the configuration tasks available on this page.


- NetExtender > Client Settings Overview on page 215
- Configuring the Global NetExtender IP Address Range on page 215
- Configuring Global NetExtender Settings on page 217


## NetExtender > Client Settings Overview

The **NetExtender > Client Settings** page allows the administrator to specify the client address range.

***Figure 27 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 will be assigned to remote users during NetExtender sessions. The range needs to be large enough to accommodate the maximum number of concurrent NetExtender users you wish to support plus one (for example, the range for 15 users requires 16 addresses, such as 192.168.200.100 to 192.168.200.115).

The range should fall within the same subnet as the interface to which the SRA appliance is connected, and in cases where there are other hosts on the same segment as the 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 may leave the NetExtender range at the default (192.168.200.100 to 192.168.200.200).
- Select a range that falls within your existing DMZ subnet. For example, if your DMZ uses the 192.168.50.0/24 subnet, and you want to support up to 30 concurrent NetExtender sessions, you could use 192.168.50.220 to 192.168.50.250, providing they are not already in use.
- Select a range that falls within your existing LAN subnet. For example, if your LAN uses the 192.168.168.0/24 subnet, and you want to support up to 10 concurrent NetExtender sessions, you could use 192.168.168.240 to 192.168.168.250, providing they are not already in use.

To specify your global NetExtender address range using a Static IP, perform the following steps:

**Step 1** Navigate to the **NetExtender** > **Client Settings** page.

**Step 2** Under **NetExtender Client Address Range**, select **Use Static Pool** from the drop down list.

**Step 3** Supply a beginning client IPv4 address in the **Client Address Range Begin** field.

**Step 4** Supply an ending client IPv4 address in the **Client Address Range End** field.

**Step 5** Under **NetExtender Client IPv6 Address Range**, optionally select **Use Static Pool** from the drop down list.

**Step 6** Supply a beginning client IPv6 address in the **Client Address Range Begin** field.

**Step 7** If using IPv6, supply an ending client IPv6 address in the **Client Address Range End** field.

**Step 8** Click **Accept**.

**Step 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, perform the following steps:

**Step 1** Navigate to the **NetExtender** > **Client Settings** page.

**Step 2** Under **NetExtender Client Address Range**, select **Use DHCP** from the drop down list.

**Step 3** Under **Select Interface**, use the drop down list to select the interface to use for DHCP.

**Step 4** Supply the **DHCP Server** in the field provided.

**Step 5** Under **NetExtender Client IPv6 Address Range**, optionally select **Use DHCP** from the drop down list.

**Step 6** Under **Select Interface**, use the drop down list to select the interface to use for DHCPv6.

**Step 7** Supply the **DHCPv6 Server** in the field provided.

**Step 8** Click **Accept**.

**Step 9** The **Status** message displays **Update Successful. Restart for current clients to obtain new addresses.**

# Configuring Global NetExtender Settings

The SRA appliance provides several settings to customize the behavior of NetExtender when users connect and disconnect. To configure global NetExtender client settings, perform the following steps:

**Step 1** Navigate to the **NetExtender** > **Client Settings** page.

1. 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 SRA server. To reconnect, users will have to either return to the SRA portal or launch NetExtender from their Programs menu. This option applies to all supported platforms except Android smartphones.
- **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 will have to return to the SRA portal and select NetExtender to reinstall it. This option only applies to Windows clients. It does not apply to Windows Mobile, Android, Mac, or Linux clients.
- **Create Client Connection Profile** - The NetExtender client will create a connection profile recording the SRA Server name, the Domain name and optionally the username and password.

**Step 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.

**Step 3** 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 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, perform the following steps:

**Step 1** Navigate to the **NetExtender** > **Client Settings** page.

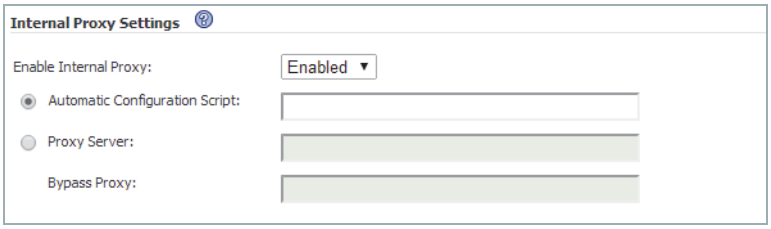
**Step 2** Under **Internal Proxy Settings**, select **Enabled** for Enable Internal Proxy.

**Step 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 which will be bypassed to the proxy server.

**Step 4** Click **Accept** to save all changes.

***Figure 28 NetExtender > Client Settings > Internal Proxy Settings***




# Configuring Post-Connection Scripts

To run post-connection scripts for a Windows, Linux, or Mac system, follow the steps listed below:

**Step 1** Navigate to the **NetExtender** > **Client Settings** page.

**Step 2** Under **Post-Connection Scripts**, find the operating system you want to run post-connection scripts to. Then, select the **Run a post-connection script** check box for that operating system.

**Step 3** Select the **Run Local File** radio button 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.

**Step 4** For local files, set the script path on the **Run this file** field.

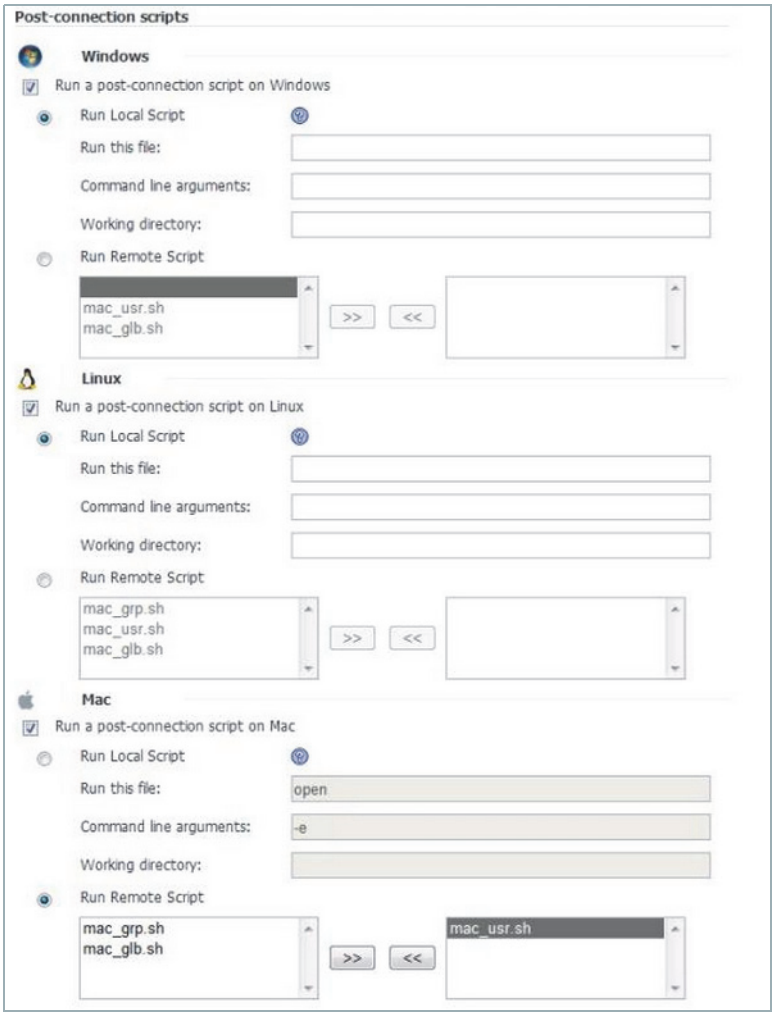
**Step 5** For local files, set the **Command line arguments**.

**Step 6** For local files, set the directory in the **Working directory** field.

**Step 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 will run after the client is connected.

**Step 8** Click **Accept** to save settings.

*Figure 29 NetExtender > Client Settings > Post-Connection Scripts*




# NetExtender > Client Routes

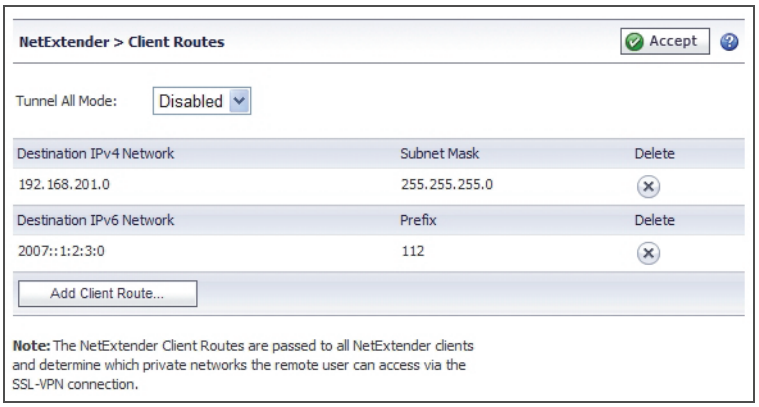
This section provides an overview of the **NetExtender > Client Routes** page and a description of the configuration tasks available on this page.

- NetExtender > Client Routes Overview on page 220
- Adding NetExtender Client Routes on page 220

# NetExtender > Client Routes Overview

The **NetExtender > Client Routes** page allows the administrator to add and configure client routes.

***Figure 30 NetExtender > Client Routes***




# Adding NetExtender Client Routes

The NetExtender client routes are passed to all NetExtender clients and are used to govern which private networks and resources remote user can access via the SRA 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 NX 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 Dell SonicWALL Unified Threat Management (UTM) appliances, where all inbound traffic is denied by default. If you do not create policies for your SRA appliance, then all NetExtender users may be able to access all resources on your internal network(s).

Additional allow and deny policies may be created by destination address or address range and by service type.

**Note** The most specific policy will take precedence over less specific policies. For example, a policy that applies to only one IP address will have priority over a policy that applies to a range of IP addresses. If there are two policies that apply to a single IP address, then a policy for a specific service (for example RDP) will take precedence over a policy that applies to all services.
User policies take precedence over group policies and group policies take precedence over global policies, regardless of the policy definition. A user policy that allows access to all IP addresses will take precedence over a group policy that denies access to a single IP address.

To add NetExtender client routes, perform the following steps:

**Step 1** Navigate to the **NetExtender** > **Client Routes** page.

**Step 2** Select **Enabled** from the **Tunnel All Mode** drop-down list to force all traffic for this user—including traffic destined to the remote users' local network—over the SRA NetExtender tunnel.

**Step 3** Click the **Add Client Route** button. The **Add Client Route** dialog box displays.

**Step 4** In the **Add Client Route** dialog box, in the **Destination Network** field, type the IP address of the trusted network to which you would like to provide access with NetExtender. For example, if you are connecting to an existing DMZ with the network 192.168.50.0/24 and you want to provide access to your LAN network 192.168.168.0/24, you would enter 192.168.168.0.

You can enter an IPv6 route in the **Destination Network** field, in the form 2007::1:2:3:0.

**Step 5** For an IPv4 destination network, type the subnet mask in the **Subnet Mask/Prefix** field using decimal format (255.0.0.0, 255.255.0.0, or 255.255.255.0). For an IPv6 destination network, type the prefix, such as 112.

**Step 6** Click **Add**.

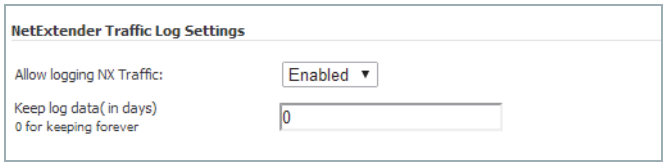
**Step 7** Repeat this procedure for all necessary routes.

# NetExtender > Advanced Settings

The **NetExtender > Advanced Settings** page allows you to set traffic log settings and upload post connection script files.

## 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.

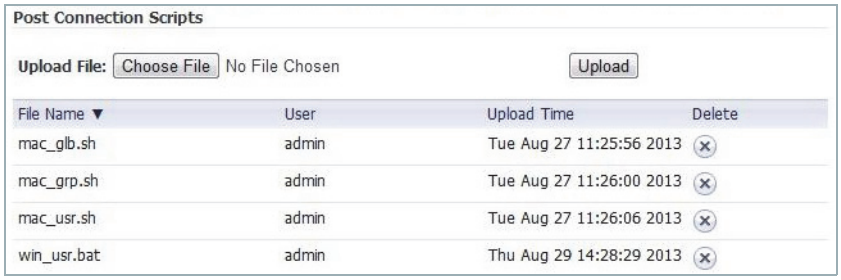



## Post Connection Scripts

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 the **Choose File** button to upload a file from your local system. Then, click **Upload**. Once 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. The following systems/mobile devices are supported:

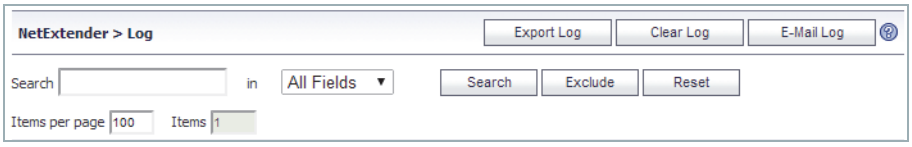
- Windows
- Mac OS X
- Linux 32-bit
- Linux 64-bit
- Android
- Apple iOS

*admin_netextenderlog*

# 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 will be 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 the **Search** button. 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 223
- Configuring Group-Level NetExtender Settings on page 227


## Configuring User-Level NetExtender Settings

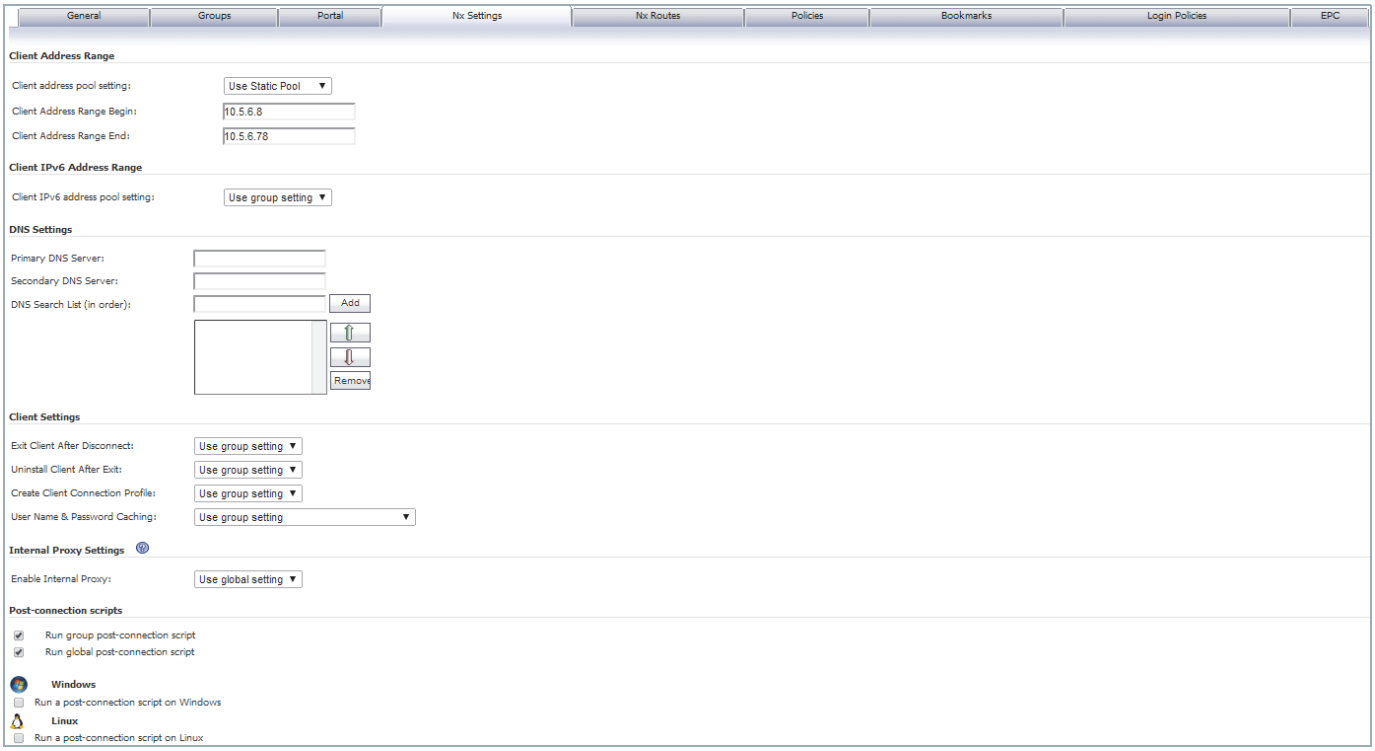
All of the global settings for NetExtender (IP address ranges, DNS settings, client routes, and client connection settings) can be configured at the user and group levels. Multiple range and route support for NetExtender enables network administrators to easily segment groups and users without the need 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, perform the following steps:

**Step 1** Navigate to the **Users > Local Users** page.

**Step 2** Click on the configure icon for the user you want to edit. The **Edit User** window is launched.

**Step 3** Click on the **Nx Settings** tab.




## *Configuring User Client IP Address Range*

To configure a user client IP address range:

**Step 1** To configure an IPv4 address range for this user, enter the beginning of the range in the **Client Address Range Begin** field and the end of the range in the **Client Address Range End** field.

**Step 2** To give this user the same IP address every time the user connects, enter the IP address in both fields.

**Step 3** 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 will be using the same username, which is not recommended, there is no need to configure more than one IP address for the user client IP address range.

**Step 4** Click **Accept**.

### *Configuring User DNS Settings*

To configure custom NetExtender DNS settings for a user:

**Step 1** In the **Primary DNS Server** field, type in the IP address of the main DNS server.

**Step 2** In the **Secondary DNS Server** field, optionally type the IP address of the backup DNS server.

**Step 3** In the **DNS Domain** field, type the domain for the DNS servers.

**Step 4** Click **Accept**.

### *Configuring User NetExtender Settings*

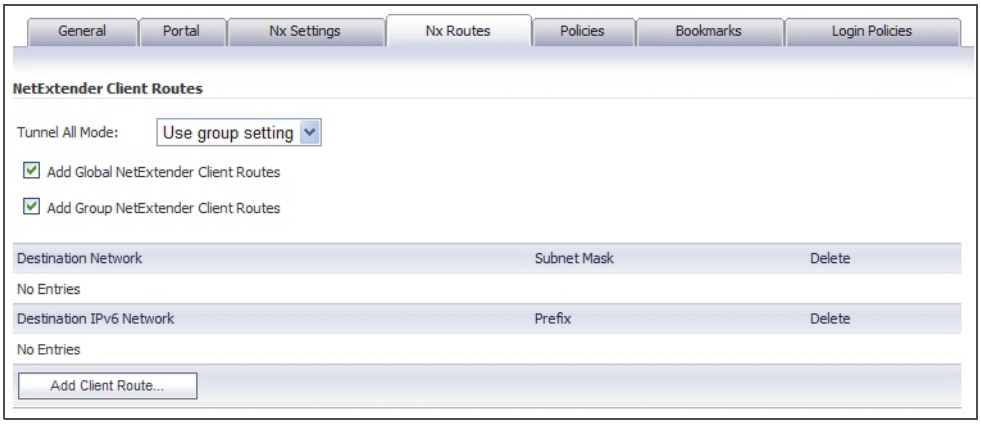
The following NetExtender settings can be configured for the user:

- **Exit Client After Disconnect** - The NetExtender client exits when it becomes disconnected from the SRA server. To reconnect, users will have to either return to the SRA 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 will have to return to the SRA portal and click NetExtender. This option only applies to Windows clients. It does not apply to Windows Mobile, Android, Mac, or Linux clients.
- **Create Client Connection Profile** - The NetExtender client will create a connection profile recording the 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.

To have the user inherit the NetExtender settings from the group it belongs to (or from the global NetExtender settings if the user does not belong to a group), select **Use Group Settings** for any of the above options.

To configure user NetExtender routes:

**Step 1** To add a NetExtender client route that will only be added to this user, click the **Nx Routes** tab in the **Edit User Settings** window.




**Step 2** **Add Client Route** button.

**Step 3** Type the IPv4 or IPv6 address of the trusted network to which you would like to provide access with NetExtender in the **Destination Network** field.

**Step 4** For an IPv4 client route, type the subnet mask in the **Subnet Mask/Prefix** field. For an IPv6 client route, type the prefix in this field.

**Step 5** Click **Add**.

**Step 6** Repeat steps 1 through 5 for all necessary routes.

**Step 7** Select **Enabled** from the **Tunnel All Mode** drop-down list to force all traffic for this user—including traffic destined to the remote users' local network—over the SRA NetExtender tunnel.

**Step 8** To also add the global NetExtender client routes (which are configured on **NetExtender** > **Client Routes** page) to the user, select the **Add Global NetExtender Client Routes** check box.

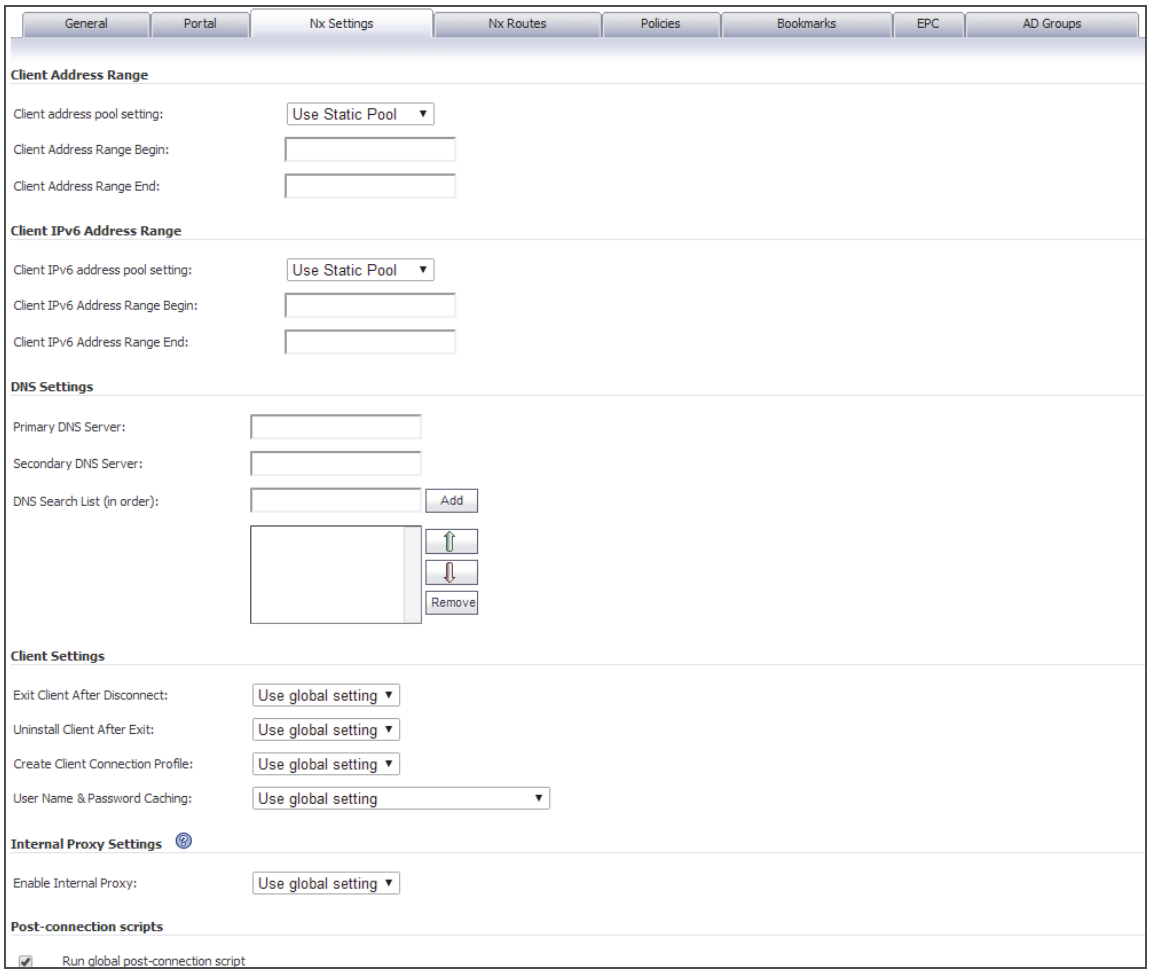
**Step 9** To also add the group NetExtender client routes for the group the user belongs to, select the **Add Group NetExtender Client Routes** check box. Group NetExtender routes are configured on the **NetExtender** tab of the **Edit Group** window, which is accessed through the **Users > Local Groups** page.

**Step 10** Click **Accept**.

**Note** When using an external authentication server, local usernames are not typically configured on the 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, perform the following steps:

**Step 1** Navigate to the **Users > Local Groups** page.

**Step 2** Click on the configure icon for the group you want to edit. The **Edit Group Settings** window is launched.

**Step 3** Click on the **Nx Settings** tab.

### *Configuring Group Client IP Address Range*

To configure group-level NetExtender address ranges:

**Step 1** To configure an IPv4 address range for this group, enter the beginning of the range in the **Client Address Range Begin** field and the end of the range in the **Client Address Range End** field.

**Step 2** To configure an IPv6 address range for this group, enter the beginning of the range in the **Client IPv6 Address Range Begin** field and the end of the range in the **Client IPv6 Address Range End** field. IPv6 configuration is optional.

**Step 3** Click **Accept**.

### *Configuring Group DNS Settings*

To configure custom NetExtender DNS settings for a group:

**Step 1** In the **Primary DNS Server** field, type in the IP address of the main DNS server.

**Step 2** In the **Secondary DNS Server** field, optionally type the IP address of the backup DNS server.

**Step 3** In the **DNS Domain** field, type the domain for the DNS servers.

**Step 4** Click **Accept**.

### *Configuring Group NetExtender Settings*

The following NetExtender settings can be configured for the group:

- **Exit Client After Disconnect** - The NetExtender client exit when it becomes disconnected from the SRA server. To reconnect, users in the group will have to either return to the SRA 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 will have to return to the SRA portal and click NetExtender. This option only applies to Windows clients. It does not apply to Windows Mobile, Android, Mac, or Linux clients.
- **Create Client Connection Profile** - The NetExtender client will create a connection profile recording the 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.

To have the user inherent the NetExtender settings from the global NetExtender settings, select **Use Global Settings** for any of the above options.

*Configuring Group NetExtender Routes*

To configure NetExtender client routes:

**Step 1** To add a NetExtender client route that will only be added to this user, click the **Nx Routes** tab in the **Edit User Settings** window.

**Step 2** To add a NetExtender client route that will only be added to users in this group, click the **Add Client Route** button.

**Step 3** Type the IPv4 or IPv6 address of the trusted network to which you would like to provide access with NetExtender in the **Destination Network** field.

**Step 4** For an IPv4 route, type the subnet mask in the **Subnet Mask/Prefix** field. For an IPv6 route, type the prefix in the **Subnet Mask/Prefix** field.

**Step 5** Click **Add**. Repeat this procedure for all necessary routes.

**Step 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 SRA NetExtender tunnel.

**Step 7** To also add the global NetExtender client routes (which are configured on **NetExtender** > **Client Routes** page) to users in this group, select the **Add Global NetExtender Client Routes** check box.

**Step 8** Click **Accept**.

# Chapter 8

# End Point Control

This chapter provides information and configuration tasks specific to the **End Point Control** pages on the Dell SonicWALL SRA Web-based management interface.

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 SRA appliance provides secure access from any Web-enabled system, including devices in untrusted environments.Starting in version 6.0, SRA supports End Point Control (EPC), a default service available on SRA 4600/4200/1600/1200 and Virtual Appliances.

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 SRA.

EPC is checked when users log into the web portal from a web browser, which blocks any access to the private network from untrusted sites. The EPC portal checking process uses the browser plug-ins on your system.

In SRA 7.5 and higher firmware versions, 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 SSL VPN from threats originating from client devices participating in the SSL VPN. For more information on Mobile Connect, refer to the *Mobile Connect User Guides*.

The SRA appliance provides these end point security controls by performing 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. Dell SonicWALL end point security controls are tightly integrated with access control to analyze the client system and apply access controls based on the results.

Currently, EPC supports the Windows, Linux, and Mac NetExtender client. EPC enhancements are supported on the Dell SonicWALL SRA 4600/4200/1600/1200 and Virtual Appliance platforms.

**Note** When the EPC feature is active other features may run slower due to the increased traffic handled by the appliance.

Perform the following tasks to configure EPC:

**Step 1** Image the appliance with the latest SRA firmware, as explained in the *Dell SonicWALL SRA Getting Started Guide*.

**Step 2** Configure Device Profiles that allow or deny user authentication based on various global, group, or user attributes. See "End Point Control > Device Profiles" section on page 232.

**Step 3** Add and configure groups and users to allow or deny End Point Control profiles. See "End Point Control > Settings" section on page 240.

**Step 4** Configure users to inherit their group profiles. See "Users > Local Groups > Edit EPC Settings" section on page 234.

**Step 5** Enable End Point Control. See "End Point Control > Settings" section on page 240.

**Step 6** Connect to NetExtender and monitor the End Point Control log. See "End Point Control > Log" section on page 240.

# 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 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.

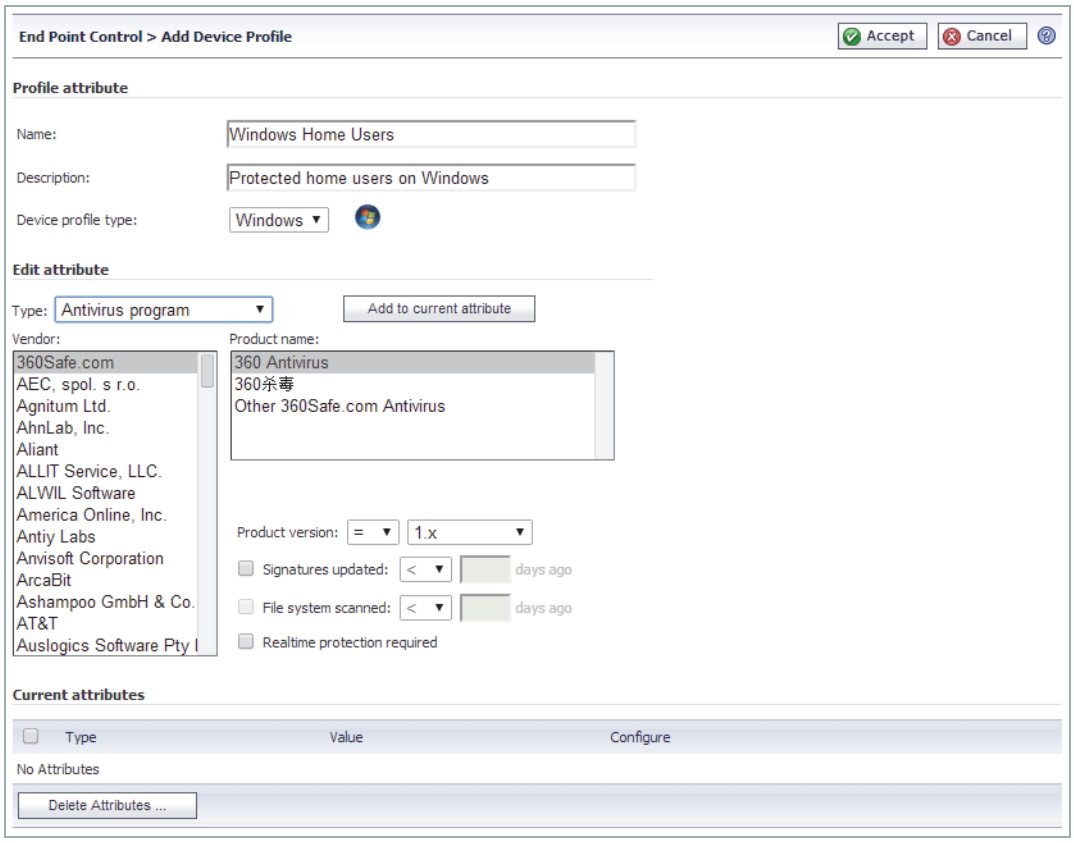
***Figure 31 End Point Control > Device Profiles***

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:

**Step 1** On the **End Point Control > Device Profiles** page, click the **Add Device Profile** button. The Add Device Profile page is displayed.

***Figure 32 End Point Control > Add Device Profile***




**Step 2** In the **Name** field, type the name that will be used to identify the profile.

**Step 3** In the **Description** field, optionally type a brief description of the profile that will help identify the profile.

**Step 4** Select whether the profile is being created for **Windows**, **Mac**, **Linux**, **iOS**, or **Android** clients.

**Step 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.

**Step 6** Click the **Add to current attribute** button.

**Step 7** Repeat Step 5 and Step 6 for each attribute that should be included in the profile.

**Step 8** To complete the profile, click the **Accept** button at the upper right of the page.

# Users > Local Groups > Edit EPC Settings

After creating device profiles, assign them to the local groups that will use 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 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 tab 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, so NetExtender must be installed. EPC is checked when users log into the web portal from a web browser, which blocks any access to the private network from untrusted sites.

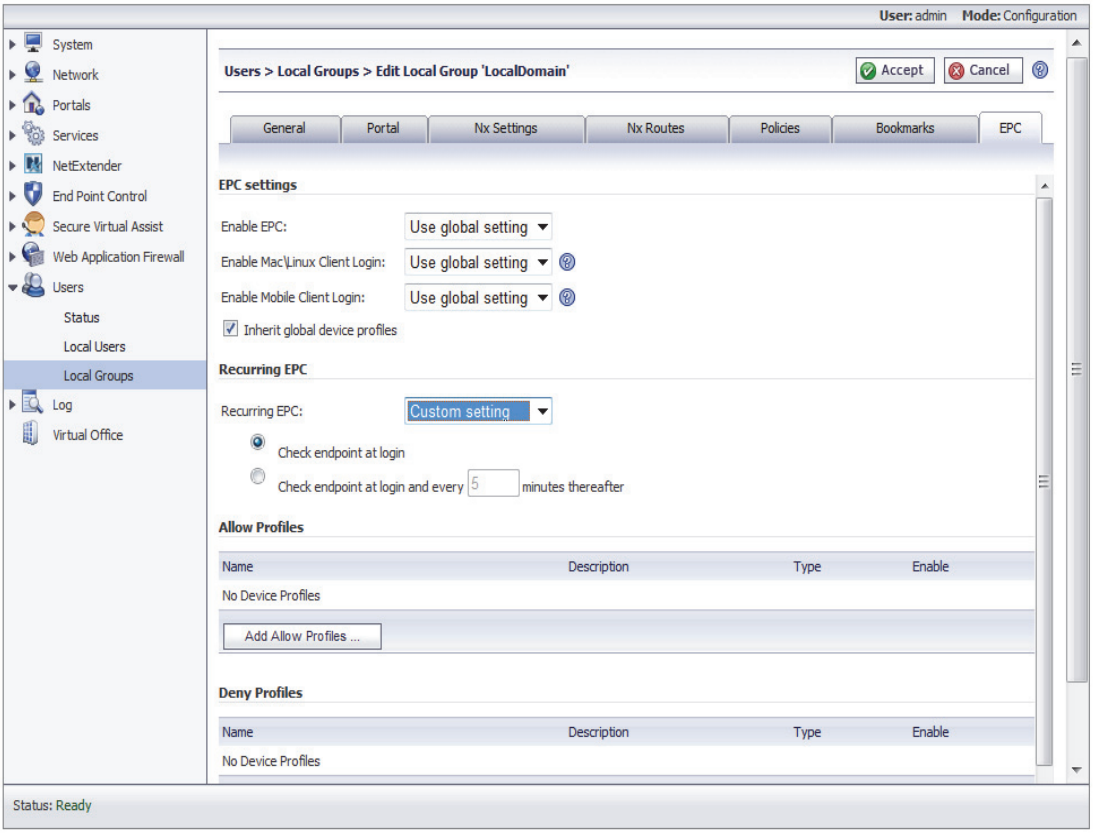
**Note** Before SRA 7.0, this feature was available on Windows only.

To configure device profiles to be used when authenticating users in a local group:

**Step 1** Navigate to the Users > Local Groups page and click the **Edit** button for the Global group or a local group to be configured for EPC.

**Step 2** When the Edit Local Group page appears, click the **EPC** tab. Use the EPC tab to enable or disable EPC for the group, select how to handle authentication requests from unsupported clients, and to add or remove device profiles.

*Figure 33 End Point Control Settings for a Local Group*




**Step 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.

**Step 4** In the **Enable Mac/Linux Client Login** field, set the default action to **Enabled** to allow or **Disabled** to block logins from these clients when EPC is enabled.

**Step 5** In SRA 7.5 and newer, 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.

**Step 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 perform EPC checks only when users login, or select **Check endpoint at login and every *x* minutes thereafter** to also perform EPC checks at set intervals. For example, to perform 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.

**Step 7** Either select the **Inherit global device profiles** check box 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 the **Add Allow Profiles** button.

**b.** In the Edit EPC page, select the profiles from the **All Profiles** list that you want to add to the group and click the **Add selected profiles** button. Selected profiles are then moved to the **In Use Profiles** list on the page, which lists all device profiles that will be used for the group.

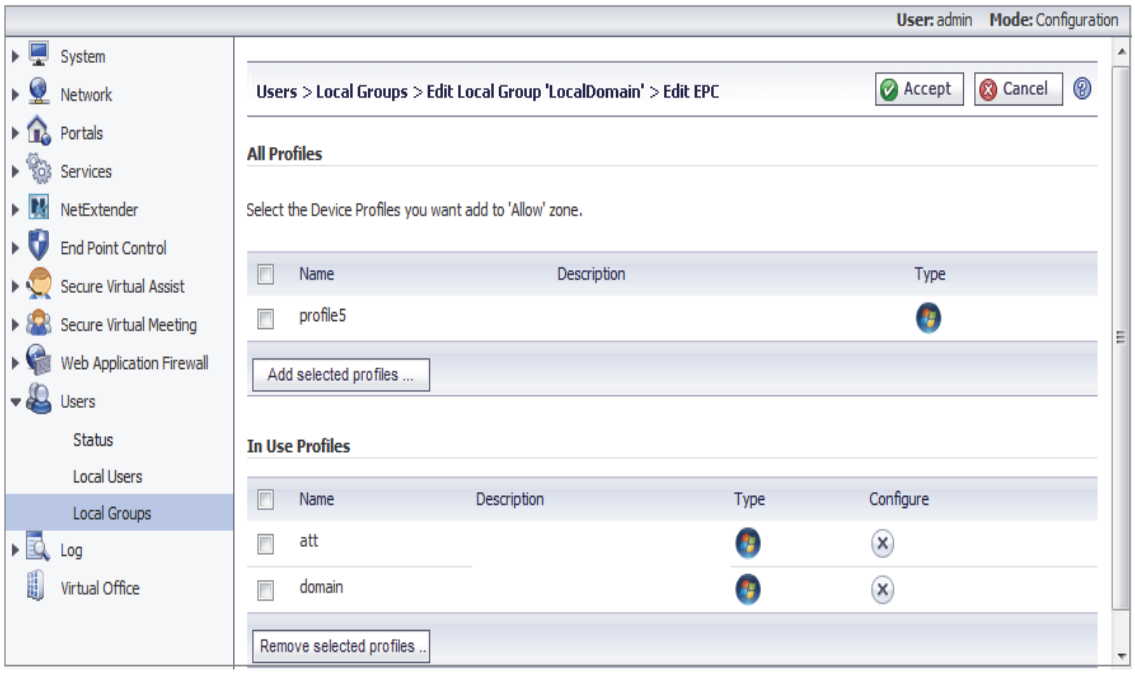
**c.** To disable a profile without deleting it, clear the **Enabled** check box next to the profile. O enable a profile, select the Enabled check box. This allows you to selectively enable or disable a profile that is used periodically.

**d.** To remove an Allow profile from the group, select the profile from the **In Use Profile**s list and click the **Remove selected profiles** button.

**e.** To add or remove a Deny profile for the group, click the **Add Deny Profiles** button and follow the preceding steps b and d.

**Step 8** Click the **Accept** button to save your changes.

***Figure 34 End Point Control - Add or Remove Device Profiles for Local Group***



# 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 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 tab 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.

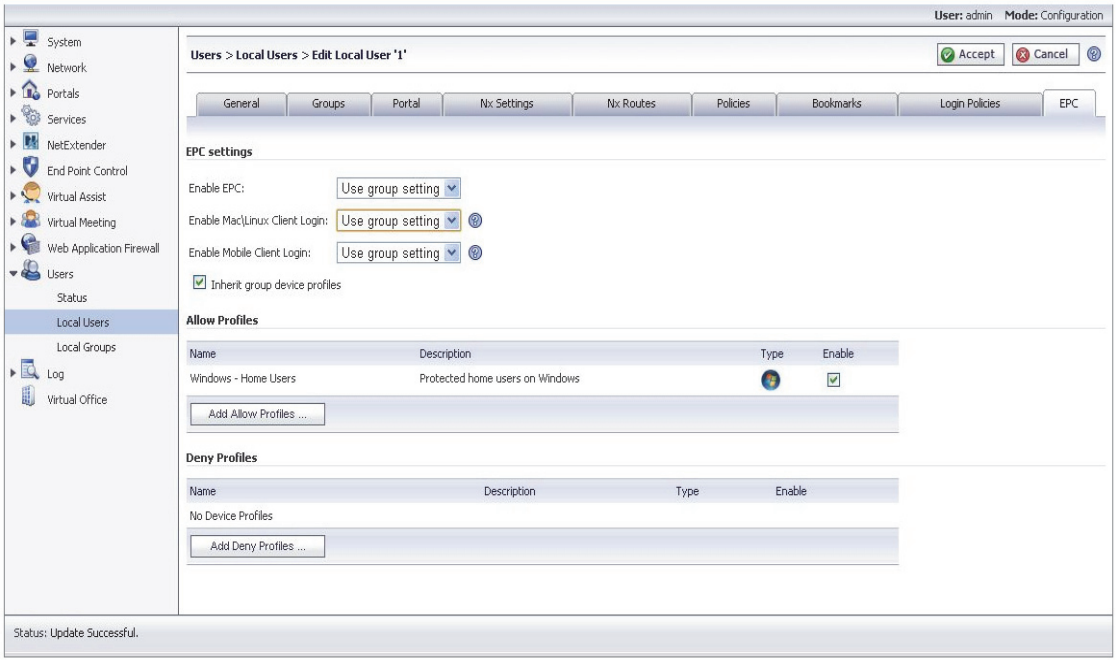
**Note** Before SRA 7.5, EPC checking was available on Windows only.

To configure device profiles to be used when authenticating a local user:

**Step 1** Navigate to the Users > Local Users page and click the **Edit** button for the user to be configured for EPC.

**Step 2** When the Edit Local User page appears, click the **EPC** tab. Use the EPC tab to enable or disable EPC for the user, select how to handle authentication requests from unsupported clients, and to add or remove device profiles.

*Figure 35 End Point Control Settings for a Local User*




**Step 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.

**Step 4** In the **Enable Mac/Linux Client Login** field, set the default action to **Enabled** to allow or **Disabled** to block logins when EPC is enabled.

**Step 5** In SRA 7.5 or newer, 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

**Step 6** In the **Recurring EPC** section, configure when EPC checks should be conducted. Select **Check endpoint at login** to perform EPC checks only when users login, or select **Check endpoint at login and every *x* minutes thereafter** to also perform EPC checks at set intervals. For example, to perform 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.

**Step 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 perform EPC checks only when users login, or select **Check endpoint at login and every *x* minutes thereafter** to also perform EPC checks at set intervals. For example, to perform 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.

**Step 8** Either select the **Inherit group device profiles** check box 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 the **Add Allow Profiles** button.

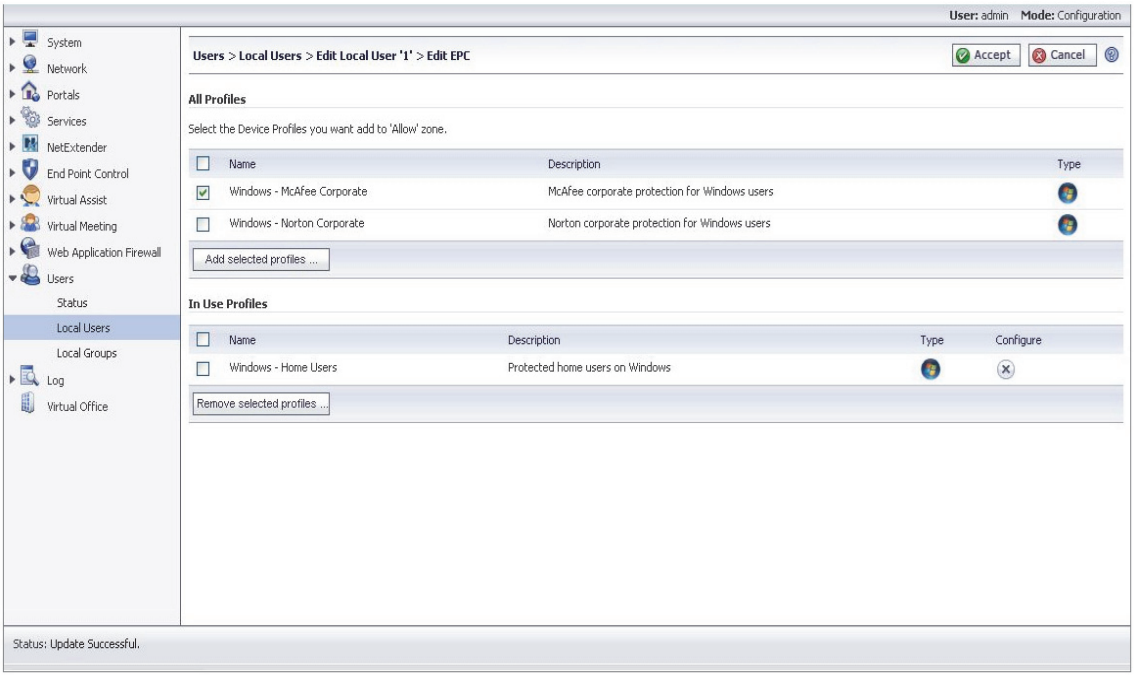
**b.** In the Edit EPC page, select the profiles from the **All Profiles** list that you want to add for the user and click the **Add selected profiles** button. Selected profiles are then moved to the **In Use Profiles** list on the page, which lists all device profiles that will be used for the user.

**c.** To remove an Allow profile for the user, select the profile from the **In Use Profile**s list and click the **Remove selected profiles** button.

**d.** To add or remove a Deny profile for the user, click the **Add Deny Profiles** button and follow the preceding steps b and d.

**Step 9** Click the **Accept** button to save your changes.

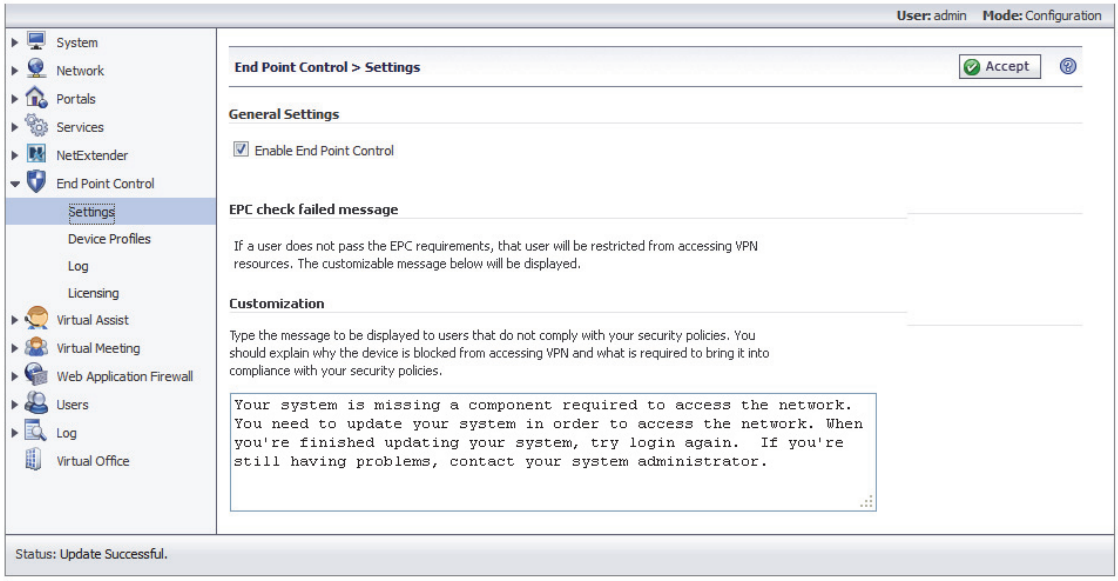
***Figure 36 End Point Control - Add or Remove Device Profiles for Local User***



# 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.

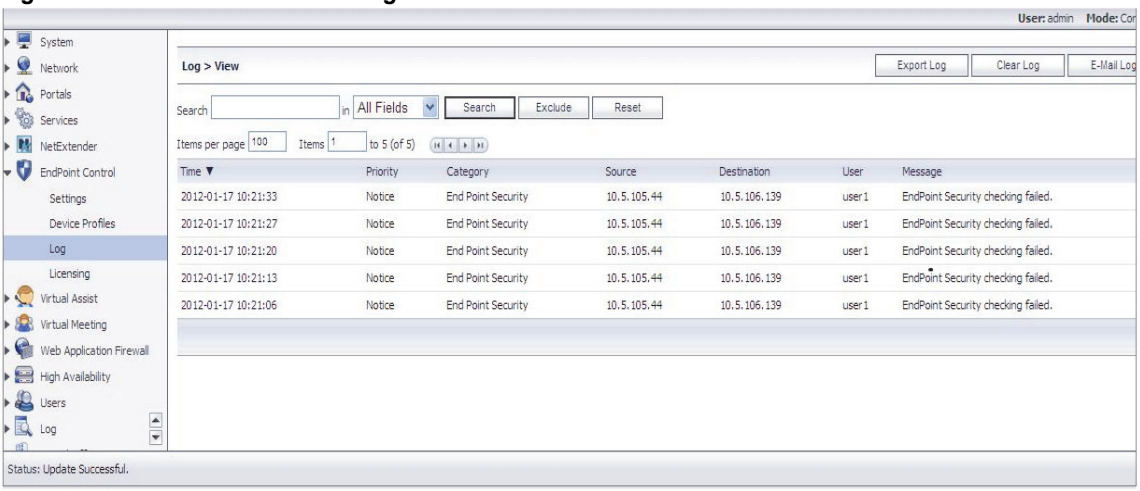
***Figure 37 End Point Control > Settings***




# 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.

***Figure 38 End Point Control Log***




Use this page to perform 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.

# Chapter 9

# Secure Virtual Assist Configuration

This chapter provides information and configuration tasks specific to the **Secure Virtual Assist** pages on the Dell SonicWALL SRA Web-based management interface.

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

For more information on Secure Virtual Assist concepts, see Secure Virtual Assist Overview on page 52.

This chapter contains the following sections:


- Secure Virtual Assist > Status on page 243
- Secure Virtual Assist > Settings on page 244
- Secure Virtual Assist > Log on page 251
- Secure Virtual Assist > Licensing on page 252


# 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.

# Secure Virtual Assist > Status

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.

On the right side of the screen, **Streaming Updates** indicates that changes to the status of customers will be dynamically updated. Click **ON/OFF** to enable/disable Streaming Updates, respectively.

Click the **Logout** button to remove a customer from the queue. If the customer is currently in a session, both the customer and technician are disconnected.

For information about using Virtual Assist as a technician, see the following sections:

- Launching a Secure Virtual Assist Technician Session on page 55
- Performing Secure Virtual Assist Technician Tasks on page 58

# Secure Virtual Assist > Settings

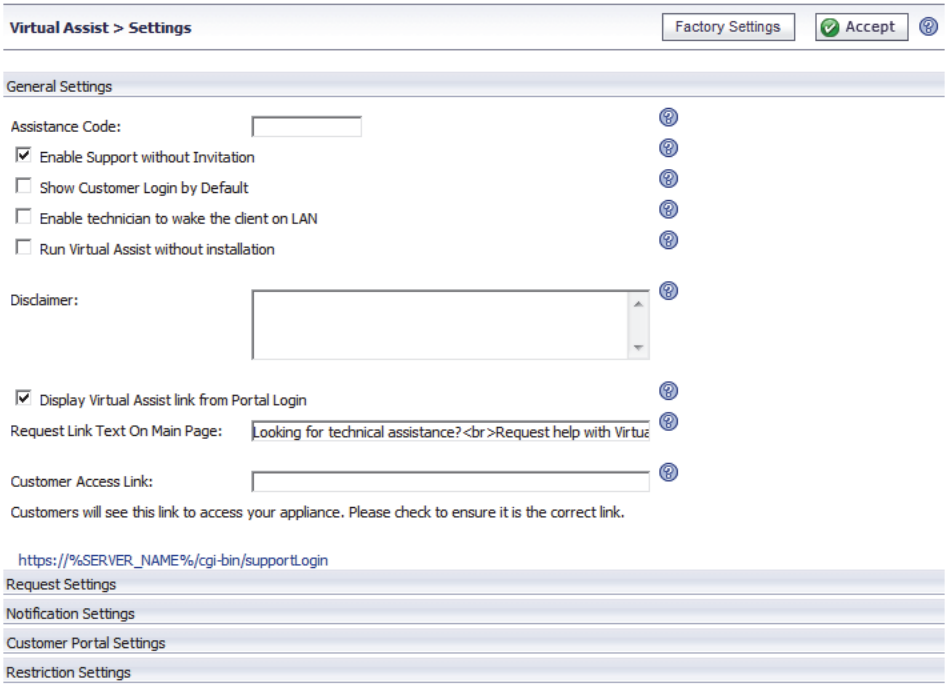
This section describes the **Secure Virtual Assist > Settings** page and the configuration tasks available on this page. The Virtual Assist options are divided into the following tabs:

- General Settings on page 245
- Request Settings on page 247
- Notification Settings on page 248
- Customer Portal Settings on page 249
- Restriction Settings on page 250

# General Settings

To configure Virtual Assist general settings, perform the following tasks:

**Step 1** Navigate to the **Secure Virtual Assist > Settings** page.




**Step 2** To require customers to enter a password before being allowed to access Virtual Assist, enter the password in the **Assistance Code** window.

**Step 3** (Optional) Select **Enable Support without Invitation** to allow customers who have not received an email invitation to request assistance. If this is disabled, customers can receive assistance only if they are explicitly invited by a technician.

**Step 4** (Optional) Select **Show Customer Login by Default** to have the default landing page be the customer login screen instead of the standard user login page.

**Step 5** (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.

**Step 6** (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.

**Step 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 will be presented with the disclaimer and required to click “Accept” before beginning a Virtual Assist session.

**Step 8** (Optional) To change the URL that customers use to access Virtual Assist, enter it in the **Customer Access Link** field. This may be necessary if your SRA appliance requires a different access URL when outside the network.

The default URL is **https://***server-name***/cgi-bin/supportLogin**. When entering a URL, the **https://** will be automatically prepended to your entry, and **/cgi-bin/supportLogin** will be automatically appended.

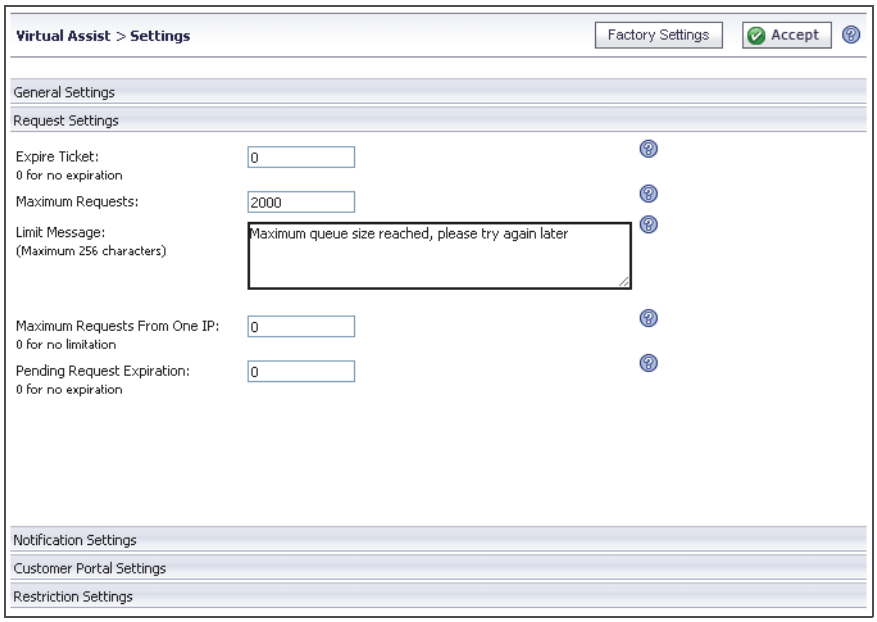
For example, if you enter **test.com/virtual_assist** in the **Customer Access Link** field, the URL will be **https://test.com/virtual_assist/cgi-bin/supportLogin**.

**Step 9** To include a link to Virtual Assist on the portal login page, select the **Display Virtual Assist link from Portal Login** check box. Customers can then click on a link to go directly to the Virtual Assist portal login page without having to login to the Virtual Office.

# Request Settings

To configure Virtual Assist request settings, perform the following tasks:

**Step 1** On the **Secure Virtual Assist > Settings** page, click the **Request Settings** tab at the bottom of the page.




**Step 2** To have Virtual Assist requests timeout after a certain amount of time, enter a value in the **Expire Ticket** field. The default is **0**, which means there is no expiration. After the timeout duration has passed, customers will have to reinitiate their Virtual Assist request.

**Step 3** To limit the number of customers allowed in the Virtual Assist queue, enter a value in the **Maximum Request** field.

**Step 4** Optionally you can customize the message that is displayed to customers when the queue is full in the **Limit Message** field. The message is limited to 256 characters.

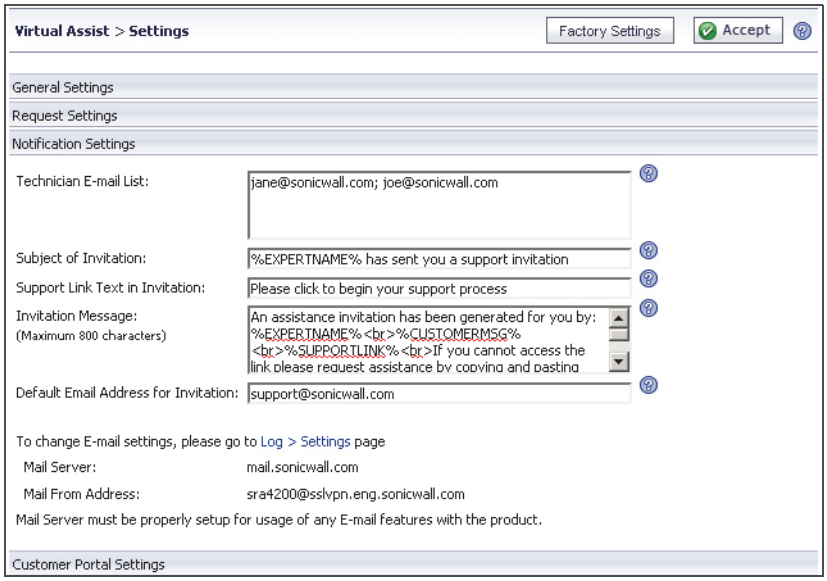
**Step 5** Entering a value in the **Maximum requests From One IP** field can be useful if individual customers are repeatedly requesting help. However, this may cause problems for customers using DHCP behind a single IP address. The default **0** does not limit request from individual IP addresses.

**Step 6** Enter a value in the **Pending Request Expired** field to have customers automatically removed from the queue if they are not assisted within the specified number of minutes. The default **0** does not remove unassisted customers.

# Notification Settings

To configure Virtual Assist notification settings, perform the following tasks:

**Step 1** On the **Secure Virtual Assist > Settings** page, click the **Notification Settings** tab at the bottom of the page.




**Step 2** To automatically email support technicians when a customer logs in to the Virtual Assist queue, enter the technicians' emails in the **Technician Email List**. Separate multiple emails with semi-colons (the ; symbol).

**Step 3** The next three fields allow you to customize the email invitation:

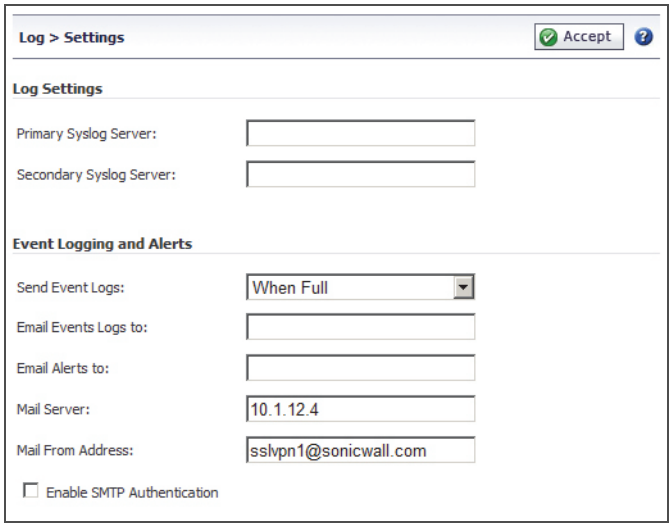
- **Subject of Invitation** - The email subject line.
- **Support Link Text in Invitation** - Text that introduces the link to the URL for accessing Virtual Assist.
- **Invitation Message** - The body of the invitation email message.
- **Default Email Address for Invitation** - The default source email.

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** tab.
- %SUPPORTLINK% - The URL for accessing Virtual Assist.
- %ACCESSLINK% - The URL for accessing the SRA 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

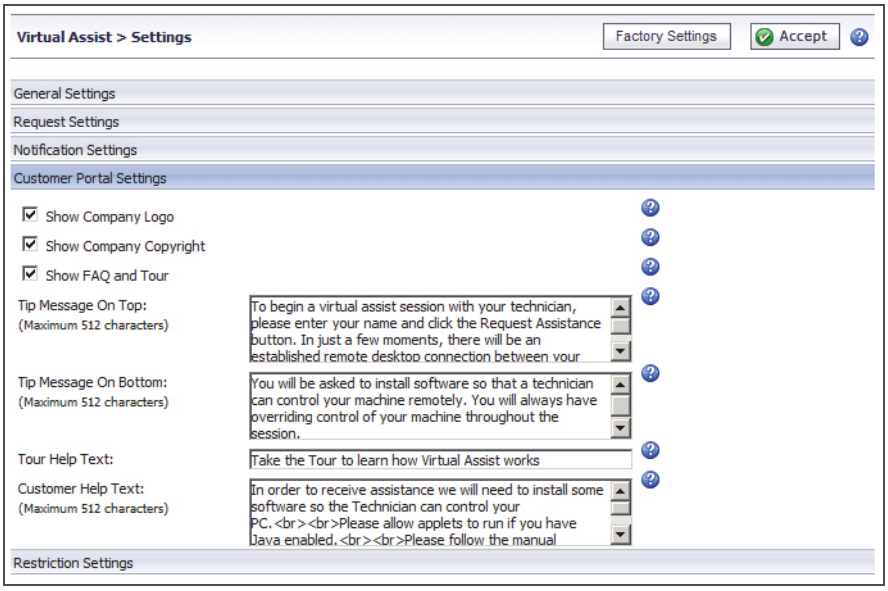
**Log > Settings** page. An accurate technician email address will also allow blocked email notification to the technician in deployments where a third-party email filter may block emails sent to the customer without providing an error to the Virtual Assist client.




# Customer Portal Settings

To customize the appearance of the Virtual Assist customer portal, perform the following tasks:

**Step 1** On the **Secure Virtual Assist > Settings** page, click the **Customer Portal Settings** tab at the bottom of the page.




**Step 2** Configure the following options to customize the appearance of the customer portal

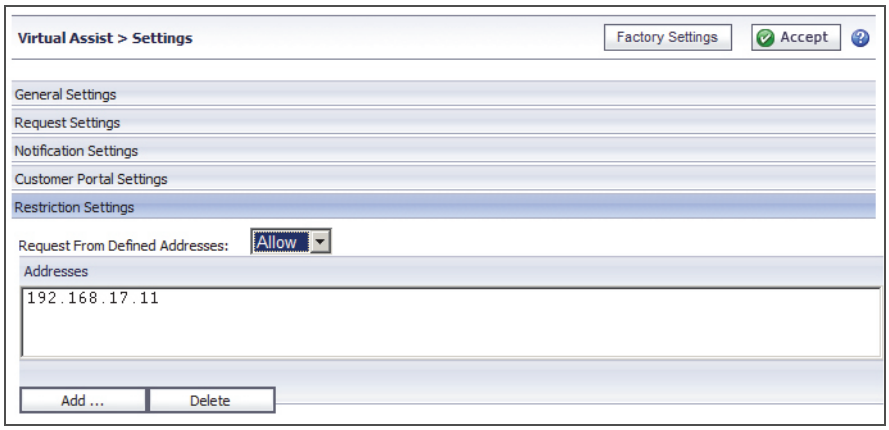
- **Show Company Logo** - Displays the company logo that is configured on the **Logo** tab of the **Edit Portal** window.
- **Show Company Copyright** - Displays the copyright at the bottom of the page.

- **Show FAQ and Tour** - Displays links to the Secure Virtual Assist FAQ and tour on the customer request page.
- **Tip Message On Top** - Customizes the text that is displayed above the Secure Virtual Assist link.
- **Tip Message On Bottom** - Customizes the text that is displayed below the Secure Virtual Assist link.
- **Tour Help Text** - Customizes the text that is displayed above the link for the Secure Virtual Assist tour.
- **Customer Help Text** - Customizes the text that is displayed after the customer clicks the Secure Virtual Assist link.

# Restriction Settings

To configure Virtual Assist restriction settings, perform the following tasks:

**Step 1** On the **Secure Virtual Assist > Settings** page, click the **Restriction Settings** tab at the bottom of the page.




**Step 2** To deny Virtual Assist requests from specific IP addresses or networks, select **Deny** from the **Request From Defined Addresses** drop-down menu.

**Step 3** To allow Virtual Assist requests only from specific IP addresses or networks, select **Allow** from the **Request From Defined Addresses** drop-down menu.

**Step 4** To add an IP address or network to the Deny or Allow list, click the **Add ...** button. The **Admin Addresses** window displays. See Adding an Address to Restriction Settings on page 251.

**Step 5** To delete a configured restriction setting, select the desired address in the **Addresses** field and click **Delete**. The address will be removed from the field.

## Adding an Address to Restriction Settings

To add an IP address or network to the Deny or Allow list for Virtual Assist restriction settings, perform the following tasks:

**Step 1** On the **Secure Virtual Assist > Settings** page, click the **Restriction Settings** tab at the bottom of the page.

**Step 2** Click the **Add ...** button. The **Admin Addresses** window displays.

**Step 3** In the **Source Address Type** drop-down menu, select which of the following you want to specify:

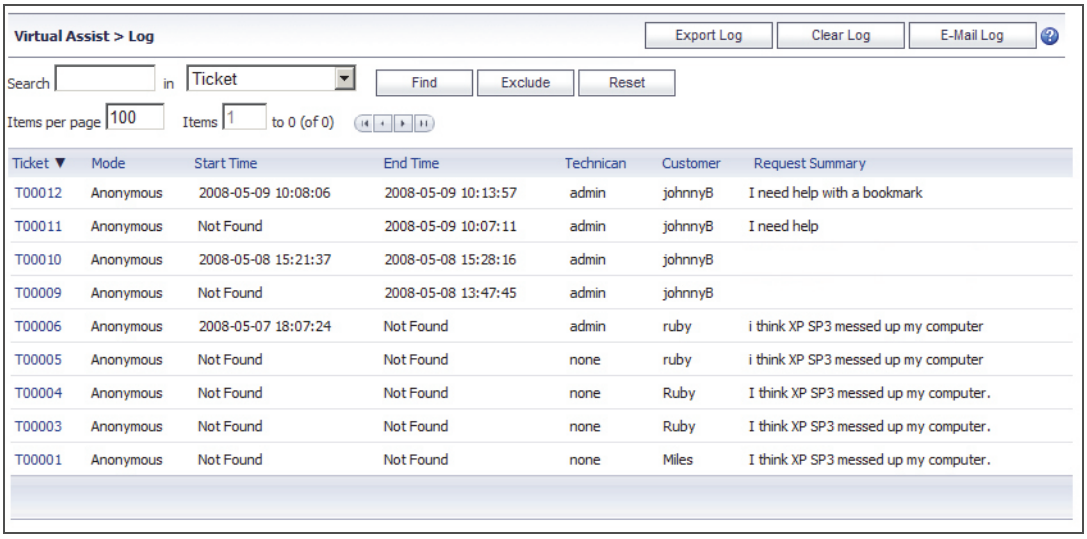
- IP Address
- IP Network
- IPv6 Address
- IPv6 Network

**Step 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.




| Ticket ▼ | Mode | Start Time | End Time | Technican | Customer | Request Summary |
|---|---|---|---|---|---|---|
| T00012 | Anonymous | 2008-05-09 10:08:06 | 2008-05-09 10:13:57 | admin | johnnyB | I need help with a bookmark |
| T00011 | Anonymous | Not Found | 2008-05-09 10:07:11 | admin | johnnyB | I need help |
| T00010 | Anonymous | 2008-05-08 15:21:37 | 2008-05-08 15:28:16 | admin | johnnyB | |
| T00009 | Anonymous | Not Found | 2008-05-08 13:47:45 | admin | johnnyB | |
| T00006 | Anonymous | 2008-05-07 18:07:24 | Not Found | admin | ruby | i think XP SP3 messed up my computer |
| T00005 | Anonymous | Not Found | Not Found | none | ruby | i think XP SP3 messed up my computer |
| T00004 | Anonymous | Not Found | Not Found | none | Ruby | I think XP SP3 messed up my computer. |
| T00003 | Anonymous | Not Found | Not Found | none | Ruby | I think XP SP3 messed up my computer. |
| T00001 | Anonymous | Not Found | Not Found | none | Miles | I think XP SP3 messed up my computer. |

Click on the **Ticket Number** to view details about a session, or ticket. The **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.

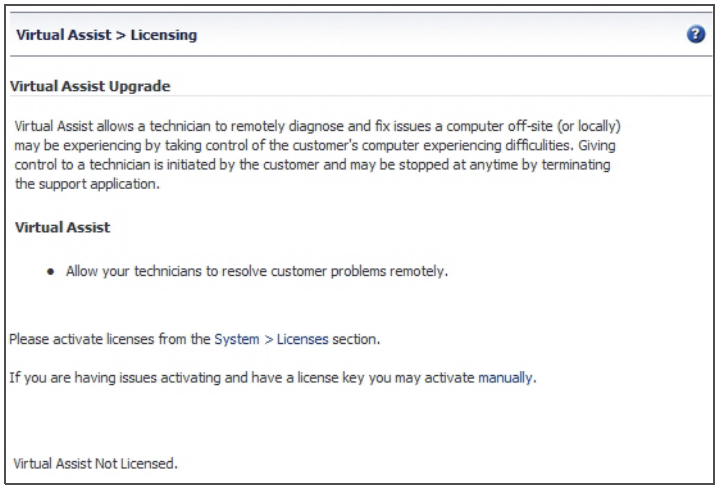
# Secure Virtual Assist > Licensing

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 252
- Enabling Secure Virtual Assist on page 252


# 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 may be necessary, but full installation is not necessary to use the service. Secure Virtual Access or unattended mode requires admin rights.

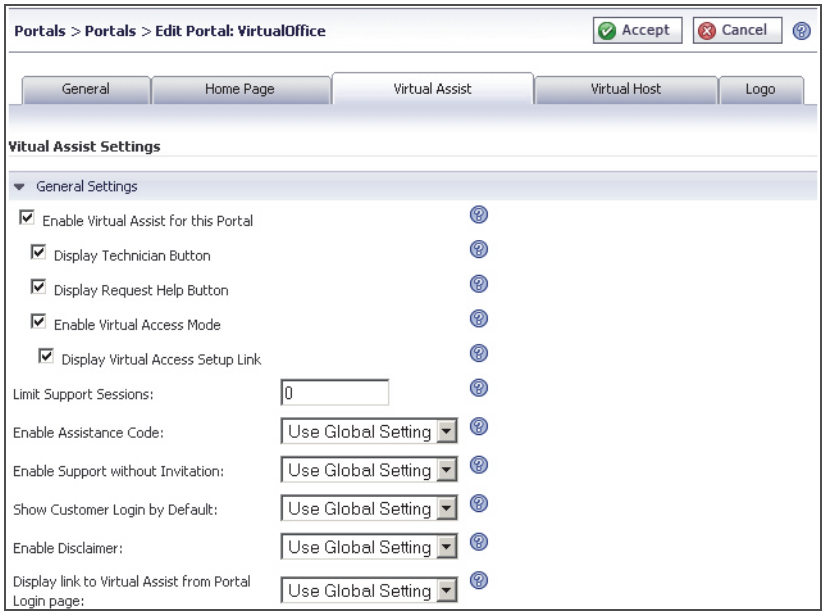
To configure Virtual Assist, perform the following tasks:

**Step 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 96.

**Step 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 the **Add Portal** button. See Portals > Portals on page 141.

**Step 3** In the **Edit Portal** window that displays, click the **Virtual Assist** tab.




**Step 4** Click on the **Enable Virtual Assist for this Portal** check box and click **Accept**. Virtual Assist is now enabled and ready to use. SRA users will now see the Virtual Assist icon on the Virtual Office page.

**Step 5** Clear the **Display Technician Button** check box to hide the technician button on the Virtual Office window and require technicians to login directly through the client.

**Step 6** Select the **Display Request Help Button** check box to display the help button on the Virtual Office for users to launch Virtual Assist.

**Step 7** Select the **Enable Virtual Access Mode** check box to allow Secure Virtual Access connections to be made to this portal. This must be enabled for Virtual Assist to function on this portal.

**Step 8** Select the **Display Virtual Access Setup Link** check box to display the Secure Virtual Access Setup link on the Virtual Office.

**Step 9** 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. SRA users will now see the **Virtual Assist** icon on the Virtual Office page.

# Chapter 10

# Secure Virtual Meeting

This chapter provides information and configuration tasks specific to the **Secure Virtual Meeting** pages on the SRA Web-based management interface and a description of the configuration tasks available for Virtual Meeting.

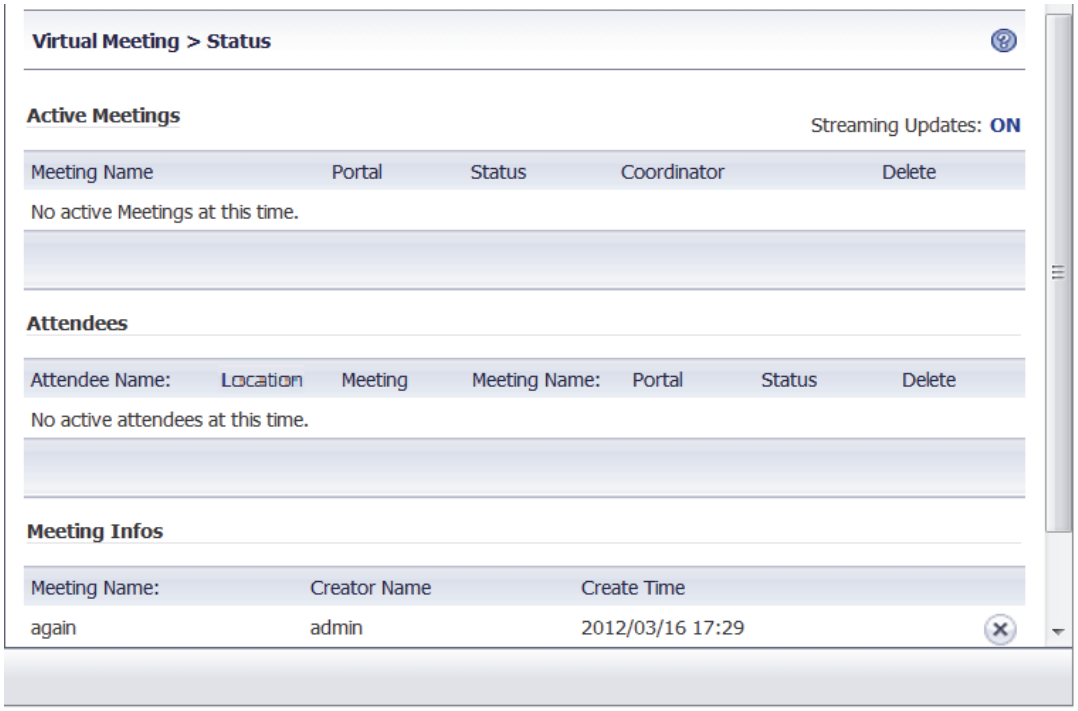
This chapter contains the following sections:


- Secure Virtual Meeting > Status on page 255
- Secure Virtual Meeting > Settings on page 256
- Secure Virtual Meeting > Log on page 258
- Secure Virtual Meeting > Licensing on page 258


For information about using Virtual Meeting, see the *Dell SonicWALL SRA 7.5 User Guide*.

## Secure Virtual Meeting > Status

The **Secure Virtual Meeting > Status** page displays a summary of current active meetings and attendees, in addition to upcoming meetings.




On the right side of the screen, **Streaming Updates** indicates that changes to the status of customers will be dynamically updated. Click **ON/OFF** to enable/disable Streaming Updates, respectively.

Click the **Logout** button next to a meeting in the Meeting Infos section to delete an upcoming meeting.

# Secure Virtual Meeting > Settings

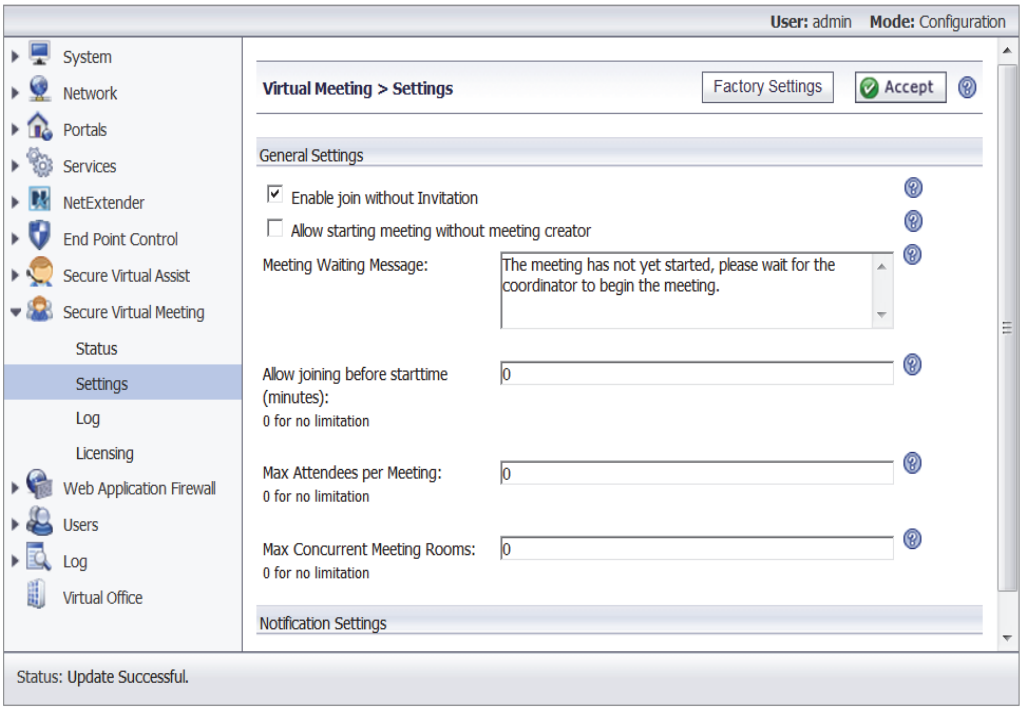
This section describes the **Secure Virtual Meeting > Settings** page and the configuration tasks available for Virtual Meeting. The Virtual Meeting settings are divided into the following tabs:


- General Settings on page 256
- Notification Settings on page 257


## General Settings

Use the General Settings page to configure general Virtual Meeting settings. To configure Virtual Meeting general settings, perform the following steps:

**Step 1** Navigate to the **Secure Virtual Meeting > Settings** page.




**Step 2** Select the **Enable join without Invitation** check box 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.

**Step 3** Select the **Allow starting meeting without meeting creator** check box 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 will be 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.

**Step 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.

**Step 5** In the **Allow joining before start time** field, select the number of minutes that Participants will be allowed to join a meeting before it starts. Select 0 if Participants will be allowed to join a meeting at any time, but you may want to consider that a license is in use from the time a Participant enters the lobby. See Licensing Overview on page 259 for additional licensing information.

**Step 6** In the **Max Attendees per Meeting** field, select the maximum number of attendees that may 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.

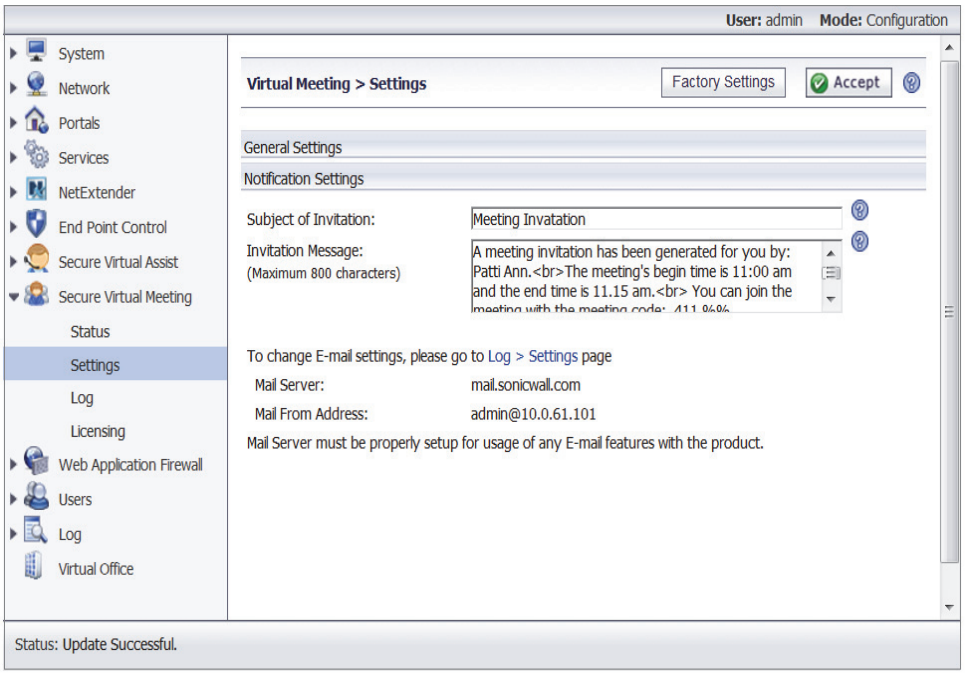
**Step 7** In the **Max Concurrent Meeting Rooms** field, select the maximum number of meetings that can take place simultaneously on the appliance.

For example, your company has 5 Secure Virtual Assist technician licenses and 2 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).

# Notification Settings

To configure Virtual Meeting notification settings, perform the following steps:

**Step 1** On the **Secure Virtual Meeting > Settings** page, click the **Notification Settings** tab at the bottom of the page.



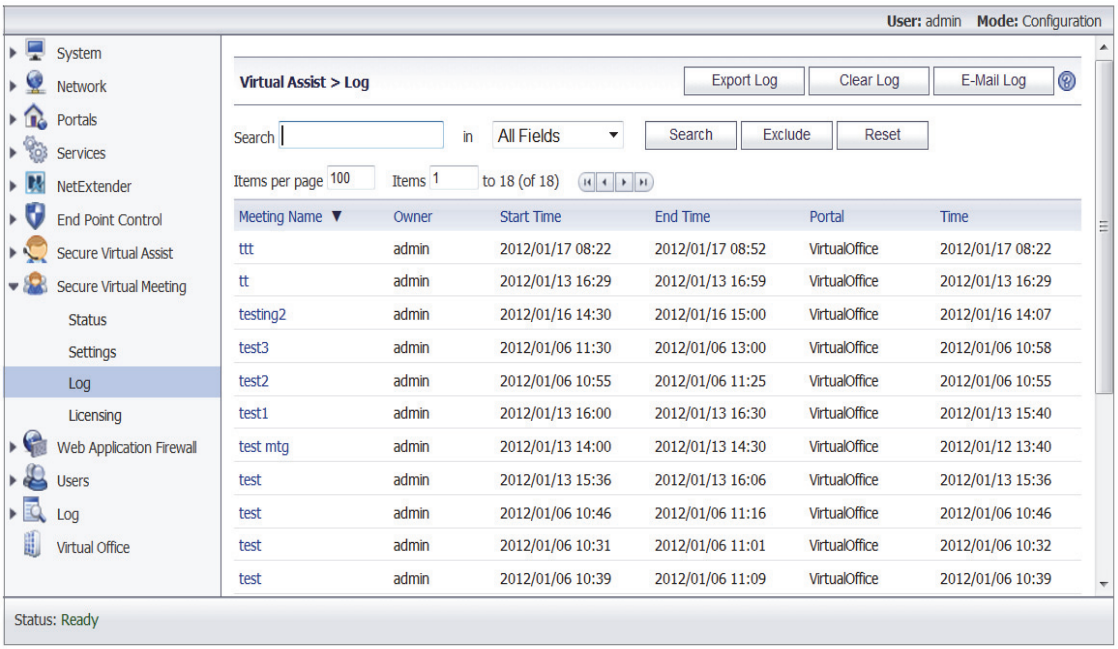

**Step 2** In the **Subject of Invitation** field type the subject used for Virtual Meeting e-mail invitations sent to Participants. The subject may include variables such as %MEETINGNAME%. Move the mouse pointer over the icon to the right of this field to display possible variables.

**Step 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 may 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, which 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

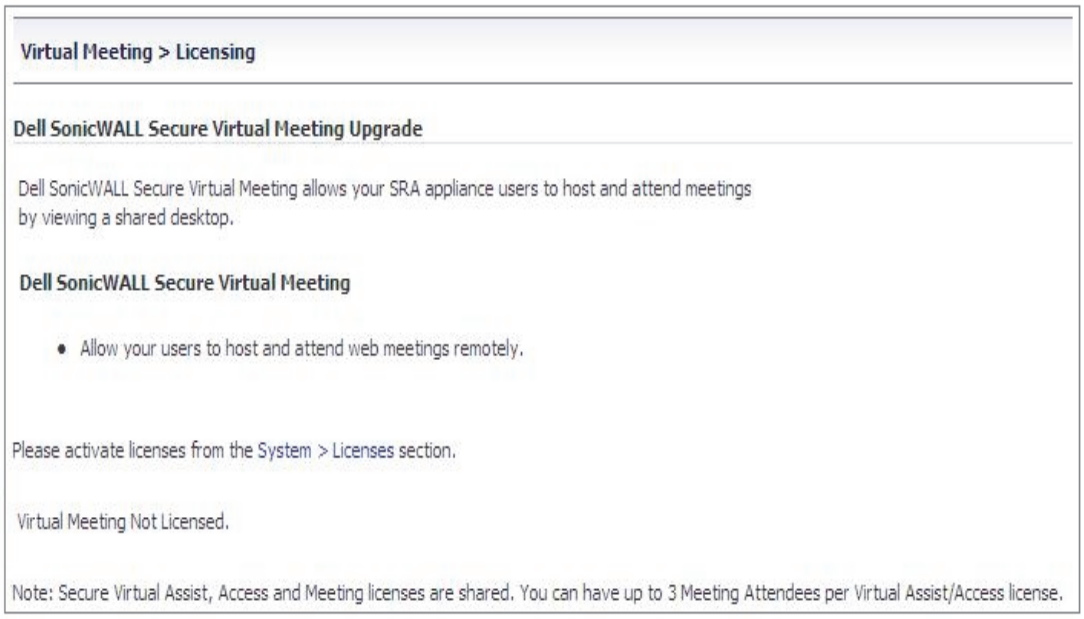
Secure Virtual Meeting is part of the Secure Virtual Assist package. Multiple Virtual Meetings and Virtual Assist sessions can occur simultaneously. However, one Virtual Assist technician license is required for every three active Virtual Meeting users. For example, your company has 5 Virtual Assist technician licenses and 2 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, which is also displayed on the System > Licenses page. See Licensing Overview on page 259 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.

***Figure 39 Secure Virtual Meeting Licensing***



# Chapter 11

# High Availability Configuration

This chapter provides information and configuration tasks specific to the **High Availability** page on the Dell SonicWALL SRA management interface.

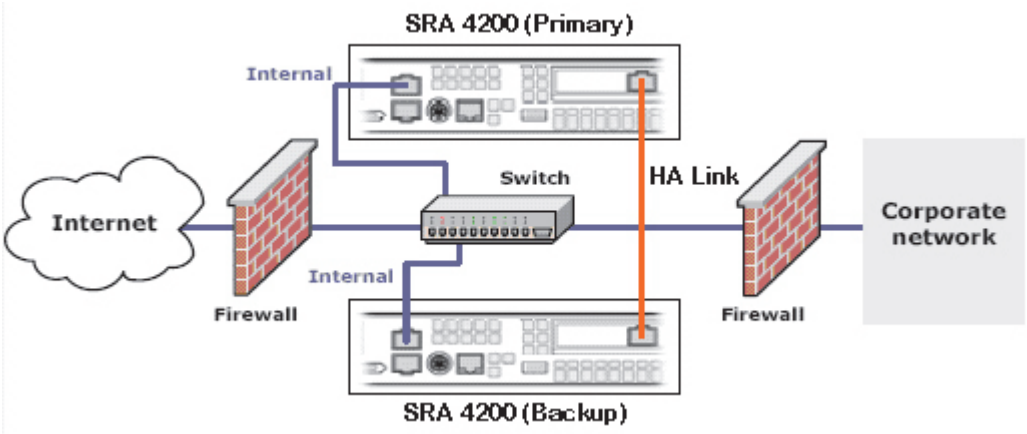
High Availability allows two identical SRA appliances or virtual appliances to provide a reliable, continuous connection to the public Internet. The two SRA appliances are deployed at the same time and connected together, and are called a High Availability Pair (HA Pair).

This chapter contains the following sections:


- High Availability Overview on page 261
- Configuring High Availability on page 262
- Technical FAQ on page 269


## High Availability Overview

High Availability requires one SRA appliance configured as the primary device, and an identical SRA configured as the backup device.




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.

### Supported Platforms

High Availability is supported in SRA 5.0 or higher on the SRA 4200, in SRA 6.0.0.6 or higher on the SRA 4600, and in SRA 7.5 or higher on the SRA Virtual Machine.

# Configuring High Availability

High Availability (HA) requires one SRA 4200, SRA 4600, or SRA Virtual Appliance configured as a primary device and an identical SRA configured as a backup device. The HA connection between two SRA appliances is in an Active/Passive state.

See the following sections for configuration information:


- Physical Connectivity on page 262
- Preparing for High Availability on page 262
- Configuring High Availability Settings on a 4200 and 4600 on page 263
- Enabling Interface Monitoring on page 266
- Configuring Network Monitoring Addresses on page 267
- Configuring Management Settings for Idle Unit on page 267
- Synchronizing Firmware on page 268
- Synchronizing Settings on page 268
- Synchronizing Licenses on page 268


## Physical Connectivity

You can select the interface to use for HA control traffic. The HA link should connect the identical ports of the 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:

**Step 1** Configure both SRA appliances as separate devices with independent IP addresses on your subnet.

**Note** SRA appliances in an HA pair cannot be deployed behind a proxy.

**Step 2** Upload the latest SRA firmware to both devices. High Availability will not work unless both devices have the same firmware version installed.

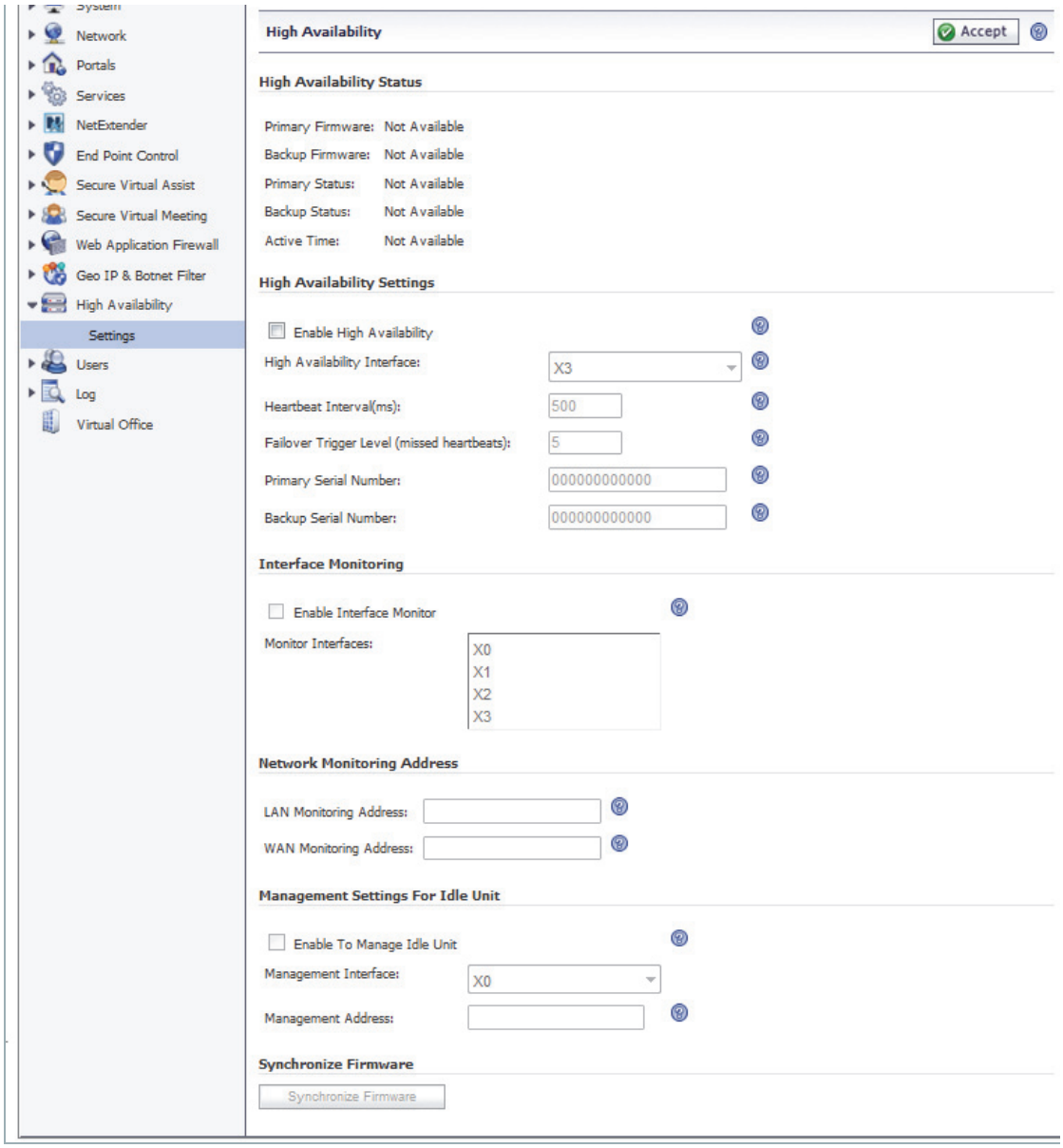
**Step 3** Connect the X3 interfaces of the two appliances together with a CAT 5E or better cable to ensure a gigabit connection.

**Note** Dell SonicWALL recommends that you backup and download the settings for both SRA devices at this stage.

**Step 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**, which should show **1000 Mbps Full Duplex**.

# Configuring High Availability Settings on a 4200 and 4600

The High Availability > Settings page provides settings for configuring High Availability.




**Note** The contents of this page vary slightly for a Virtual Machine, as explained in Configuring High Availability Settings on a Virtual Machine on page 265.

To enable High Availability and configure the options in the High Availability Settings section, perform the following steps:

**Step 1** In a browser, log in to the primary unit and navigate to the **High Availability > Settings** page.

**Step 2** Select the **Enable High Availability** check box.

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.

**Step 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.

**Step 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 (5 minutes).

**Step 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 4, and the maximum is 99.

**Step 6** In the **Primary Serial Number** field, type in the serial number of the primary device. The maximum length is 12 characters.

**Step 7** In the **Backup Serial Number** field, type in the serial number of the backup device. The maximum length is 12 characters.

**Step 8** Click **Accept**.

**Step 9** In the browser, open a new tab and point it to the IP address of the backup unit. Log in to the backup.

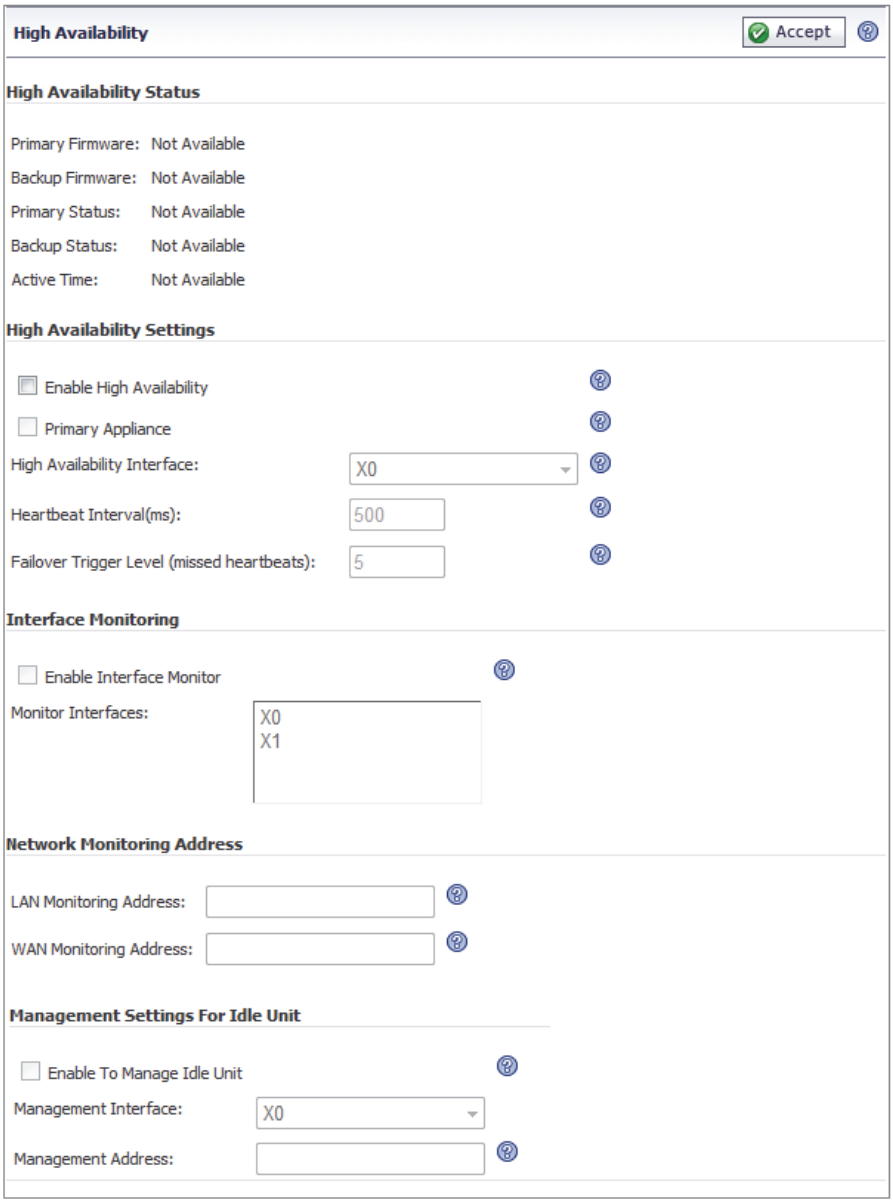
**Step 10** Repeat Step 1 through Step 8 on the backup unit.

When you click the **Accept** button, the backup device will become IDLE and you will no longer be 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 will become Active with the same settings as the primary.

# Configuring High Availability Settings on a Virtual Machine

The High Availability > Settings page provides settings for configuring High Availability.




To enable High Availability for a Virtual Machine and configure the options in the High Availability Settings section, perform the following steps:

**Step 1** In a browser, log in to the primary unit and navigate to the **High Availability > Settings** page.

**Step 2** Select the **Enable High Availability** check box.

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.

**Step 3** Select the **Primary Appliance** check box if this Virtual Machine is the primary appliance in the HA pair.

**Step 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.

**Step 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 (5 minutes).

**Step 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 4, and the maximum is 99.

**Step 7** Click **Accept**.

**Step 8** In the browser, open a new tab and point it to the IP address of the backup unit. Log in to the backup.

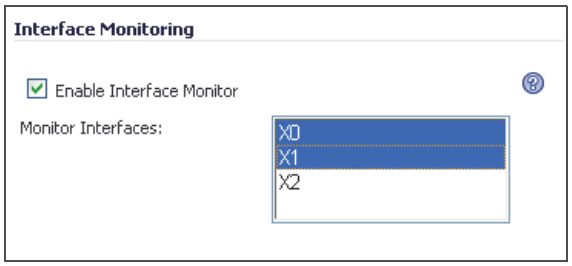
**Step 9** Configure High Availability on the backup unit.

When you click the **Accept** button, the backup device will become IDLE and you will no longer be 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 will become 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:

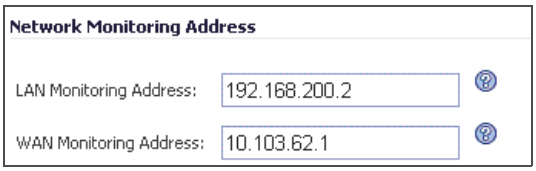
**Step 1** On the High Availability > Settings page under Interface Monitoring, select the **Enable Interface Monitor** check box.

**Step 2** In the **Monitor Interfaces** list, select the interfaces that you want to monitor.

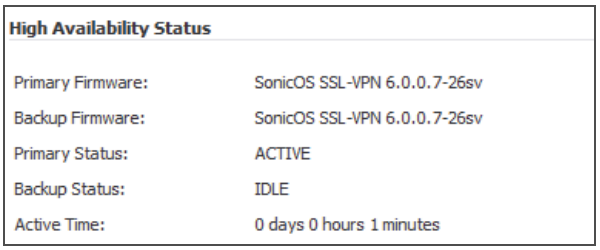
**Step 3** Click **Accept**.

# 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:

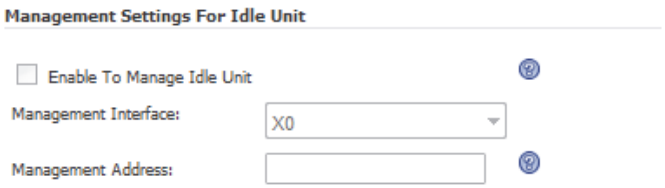
**Step 1** On the High Availability > Settings page under Network Monitoring Address, type the LAN IP address into the LAN Monitoring Address field.

**Step 2** Type the WAN IP address into the WAN Monitoring Address field.

**Step 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 virtual appliances. Use the High Availability > Settings page to enable High Availability on the virtual appliance, designate it as the primary or secondary unit, and select the interface. Note the following limitations when configuring management settings for a virtual appliance:

- High Availability is not supported on a virtual appliance in Single Network Interface mode.
- The Synchronize Firmware function is not supported for a virtual appliance.

To configure management settings for the idle unit:

**Step 1** On the High Availability > Settings page under Management Settings for Idle Unit, check the **Enable To Manage Idle Unit** check box.

**Step 2** Select the **Management Interface** using the drop-down list.

**Step 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. Please enter the management IP address of the idle unit if you wish to view the status of it.

**Step 4** Click **Accept**.

# Synchronizing Firmware

You can synchronize firmware from the active unit to the idle unit in the HA pair by clicking the **Synchronize Firmware** button.

This allows you to synchronize firmware between the units after upgrading the active unit to a different version.

**Note** Synchronizing firmware on a Virtual Appliance is currently not supported.

# Synchronizing Settings

Synchronize settings by clicking the **Accept** button. 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 will become Active with the same settings as the primary.

# Synchronizing Licenses

To synchronize licenses between two SRA appliances in an HA pair, login to MySonicWALL.com and bind the two SRA appliances together. Both appliances will share the primary unit's license information.

**Note** There is no function in the SRA management interface to synchronize licenses between the two units in the HA pair, all license synchronization is controlled via MySonicWALL.

# Technical FAQ

1. Once HA is enabled, can the idle device be used separately?

   No. Once HA is configured, only one device can be in use at any one time. During failover the Idle device will become Active. Two devices in HA mode cannot be used as separate SRA appliances.

2. What will happen 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 will cause an IP conflict, as both the primary and backup devices have the same IP configuration.

3. Can the HA interface settings be amended, once HA is enabled?

   When HA is configured, the 'Edit' button for the HA interface is grayed out and disabled. So the HA interface setting cannot be changed once the devices are in HA mode.

4. Can the X0, X1 and X2 interface settings be amended once HA mode is set up?

   Yes, the X0, X1 and X2 interface settings can be amended on the primary device and these new settings will be copied to the backup device.

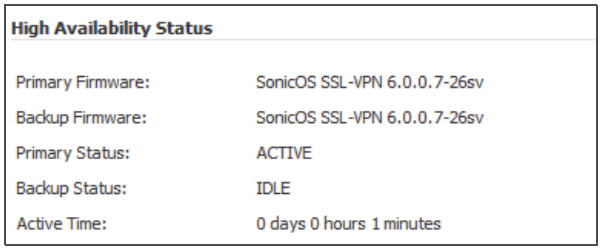
5. Can the synchronization status between the devices be viewed in the management interface?

   Yes. These can be viewed on the Active SRA in the Log > View page. The log message: "Finish synchronizing all data", will appear.

6. Is there any provision to make sure that the backup device is working correctly?

   Yes. There will be 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 will be IDLE, as indicated in the image below:




   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 the Accept button synchronizes settings.

8. Does the HA configuration for SRA 4200 or 4600 devices differ from the HA configuration of Dell SonicWALL 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 SRA devices 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 the **Accept** button. 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 will display as “Not Available”.

12. Can I deploy an HA pair behind a proxy?

    No, SRA appliances in an HA pair cannot be deployed behind a proxy. They communicate with the backend servers directly to download signatures etc.

# Chapter 12

# Web Application Firewall Configuration

This chapter provides information and configuration tasks specific to the **Web Application Firewall** pages on the Dell SonicWALL SRA Web-based management interface.

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

For more information on Web Application Firewall concepts, see Web Application Firewall Overview on page 69.

This chapter contains the following sections:


- Licensing Web Application Firewall on page 271
- Configuring Web Application Firewall on page 275
- Verifying and Troubleshooting Web Application Firewall on page 321

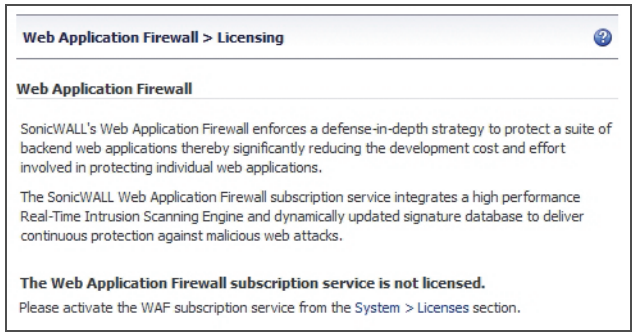

## Licensing Web Application Firewall

Dell SonicWALL SRA Web Application Firewall must be licensed before you can begin using it. You can access the MySonicWALL Web site directly from the SRA management interface to obtain a license.

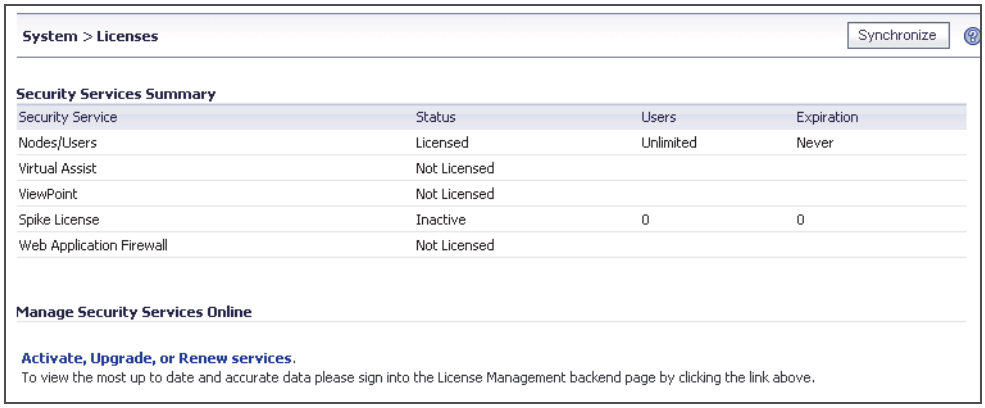
The Web Application Firewall > Licensing page in the Dell SonicWALL SRA management interface provides a link to the System > Licenses page, where you can connect to MySonicWALL and purchase the license or start a free trial. You can view all system licenses on the System > Licenses page of the management interface.

To view license details and obtain a license on MySonicWALL for Web Application Firewall, perform the following steps:

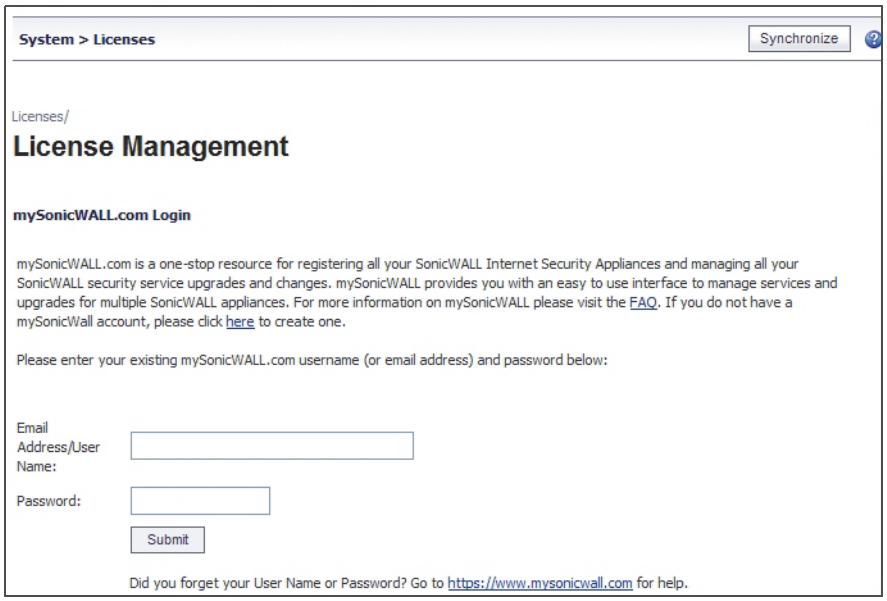
**Step 1** Log in to your Dell SonicWALL SRA appliance and navigate to **Web Application Firewall > Licensing**.



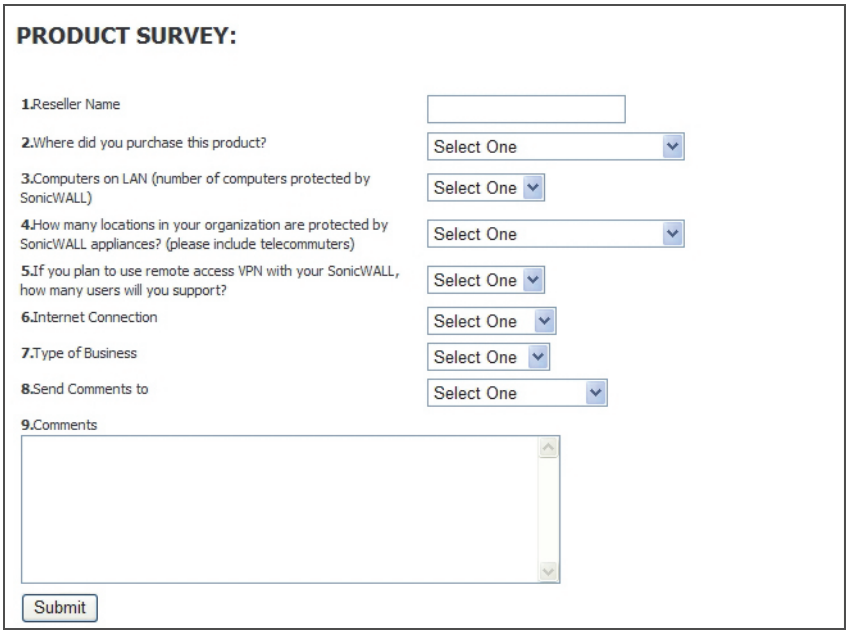

**Step 2** If Web Application Firewall is not licensed, click the **System > Licenses** link. The System > Licenses page is displayed.



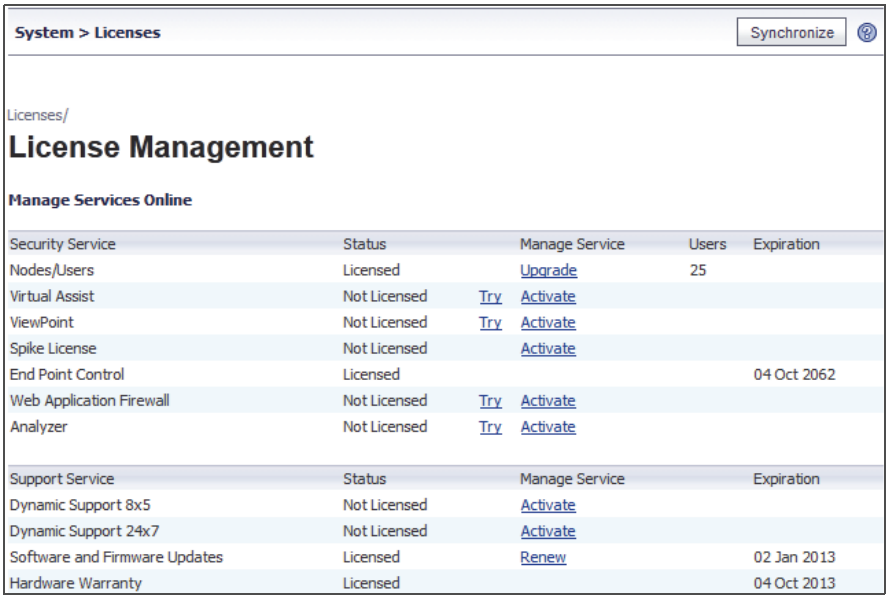

**Step 3** Under Manage Security Services Online, click the **Activate, Upgrade, or Renew services** link. The MySonicWALL Login page is displayed.



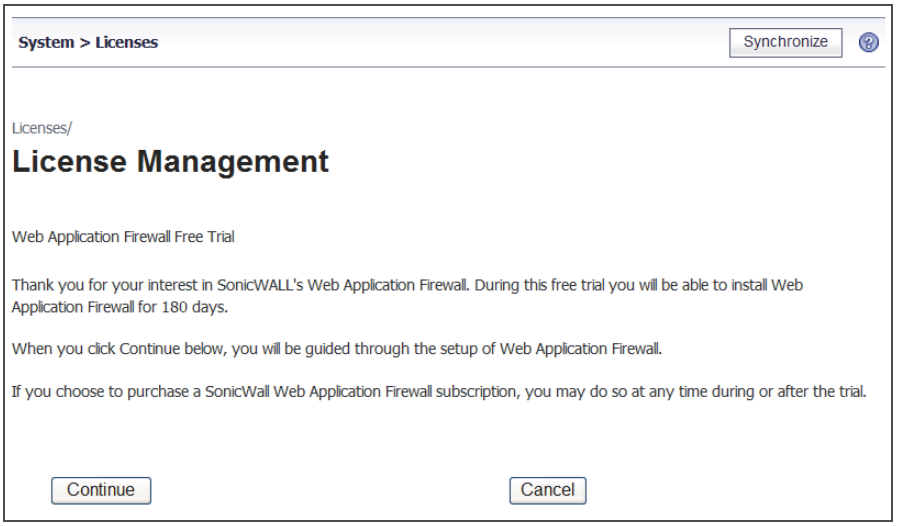
**Step 4** Type your MySonicWALL credentials into the fields, and then click **Submit**. The Product Survey page is displayed.



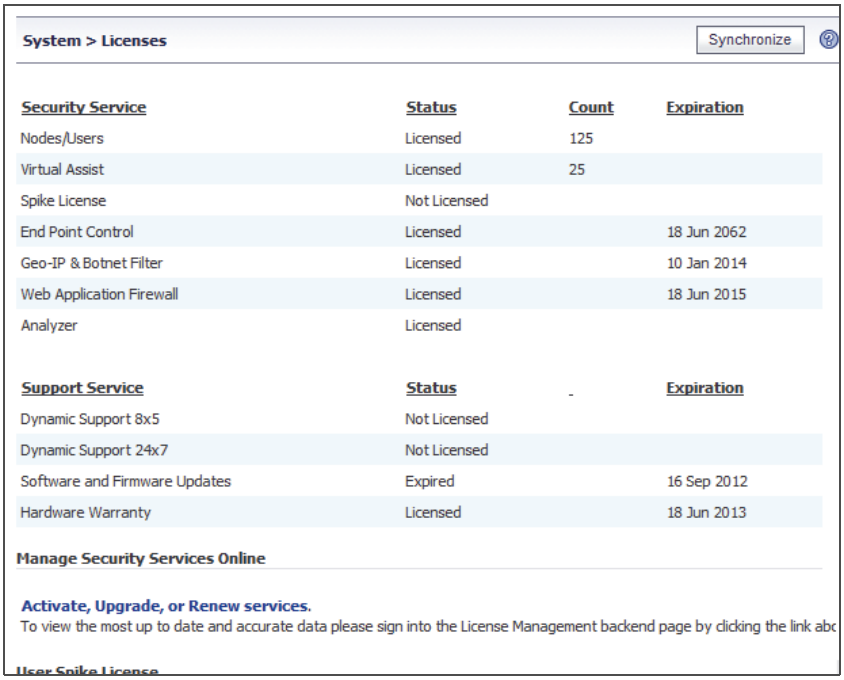

**Step 5** Fill out the survey and then click **Submit**. The System > Licenses page is displayed.




**Step 6** Click **Try** to start a 30 day free trial, or click **Activate** to subscribe to the service for 1 year. The screen below is displayed after selecting the free trial.




**Step 7** Click **Synchronize** to view the license on the System > Licenses page.




Web Application Firewall is now licensed on your 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

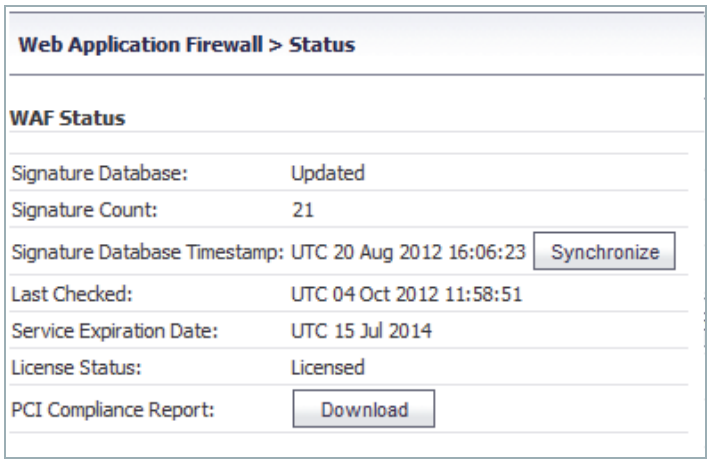
**Note** Web Application Firewall requires the purchase of an additional license.

To configure the Web Application Firewall feature, see the following sections:


- Viewing and Updating Web Application Firewall Status on page 275
- Configuring Web Application Firewall Settings on page 277
- Configuring Web Application Firewall Signature Actions on page 287
- Determining the Host Entry for Exclusions on page 291
- Configuring Custom Rules and Application Profiling on page 293
- Using Web Application Firewall Monitoring on page 311
- Using Web Application Firewall Logs on page 319


# 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. The **Synchronize** button allows you to download the latest signatures from the Dell SonicWALL online database. You can use the **Download** button to generate and download a PCI compliance report file.



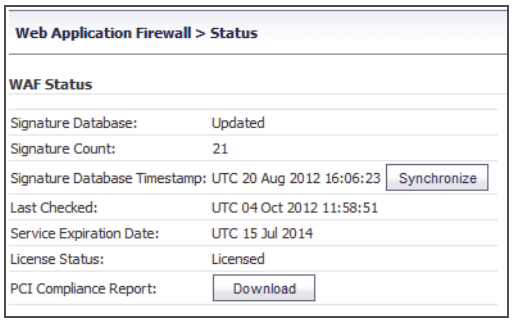

## Viewing Status and Synchronizing Signatures

To view the status of the signature database and Web Application Firewall service license, and synchronize the signature database, perform the following steps in the appliance management interface:

**Step 1** Navigate to **Web Application Firewall > Status**. The WAF Status section displays the following information:

- Status of updates to the signature database
- Timestamp of the signature database
- Time that the system last checked for available updates to the signature database

- Expiration date of the Web Application Firewall subscription service
- Status of the Web Application Firewall license




**Step 2** If updates are available for the signature database, the **Apply** button is displayed. Click **Apply** to download the updates.

You can select an option to update and apply new signatures automatically on the Web Application Firewall > Settings page. If this automatic update option is enabled, the **Apply** button disappears from the Web Application Firewall > Status screen as soon as the new signatures are automatically applied.

**Step 3** To synchronize the signature database with the Dell SonicWALL online database server, click **Synchronize**. The timestamp is updated.

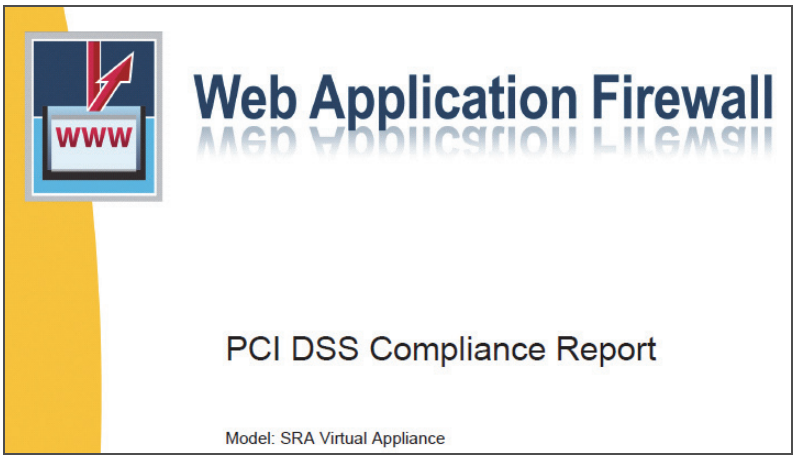
## Downloading a PCI Compliance Report

To download a PCI DSS 6.5/6.6 compliance report, perform the following steps:

**Step 1** Navigate to Web Application Firewall > Status.

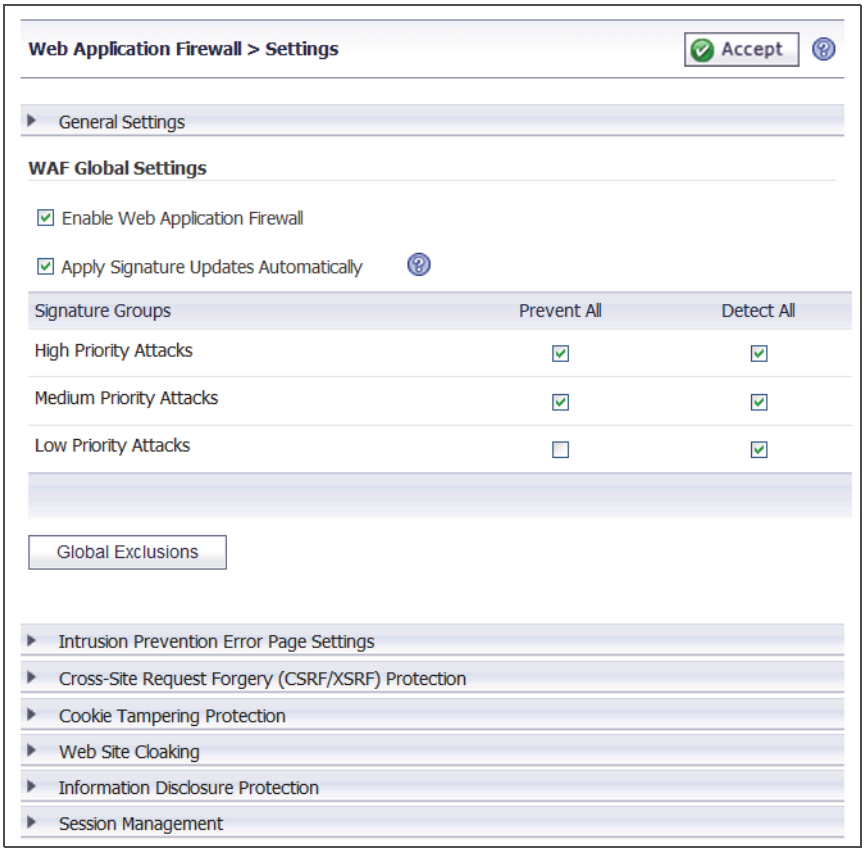
**Step 2** Click the **Download** button.

**Step 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 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 on page 277
- Configuring Global Exclusions on page 278
- Configuring Intrusion Prevention Error Page Settings on page 280
- Configuring Cross-Site Request Forgery Protection Settings on page 280
- Configuring Cookie Tampering Protection Settings on page 283
- Configuring Web Site Cloaking on page 284
- Configuring Information Disclosure Protection on page 285
- Configuring Session Management Settings on page 287

## 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 the global **Enable Web Application Firewall** check box 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 WAF > 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, perform the following steps:

**Step 1** On the Web Application Firewall > Settings page, expand the **General Settings** section.

**Step 2** Select the **Enable Web Application Firewall** check box.

**Step 3** A warning dialog box is displayed if none of the signature groups have **Prevent All** already selected. Click **OK** in the dialog box to set all signature groups to **Prevent All**, or click **Cancel** to leave the settings as they are or to manually continue the configuration.

**Step 4** Select the **Apply Signature Updates Automatically** check box to enable new signatures to be automatically downloaded and applied when available. You do not have to click the **Apply** button on the Web Application Firewall > Status page to apply the new signatures.

**Step 5** Select the desired level of protection for **High Priority Attacks** in the Signature Groups table. Select one of the following options:

- Select the **Prevent All** check box to block access to a resource when an attack is detected. Selecting **Prevent All** automatically selects **Detect All**, turning on logging.
- Clear the **Prevent All** check box and select the **Detect All** check box 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.

**Step 6** Select the desired level of protection for **Medium Priority Attacks** in the Signature Groups table.

**Step 7** Select the desired level of protection for **Low Priority Attacks** in the Signature Groups table.

**Step 8** 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.

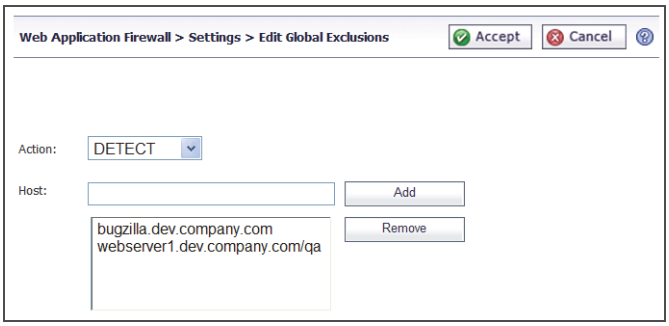
To configure global exclusions, perform the following steps:

**Step 1** On the Web Application Firewall > Settings page, expand the **General Settings** section.

**Step 2** Click the **Global Exclusions** button.

**Step 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.




**Step 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 291.

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.

**Step 5** Click **Add** to move the host name into the list box.

**Step 6** Repeat Step 4 and Step 5 to add more hosts to this exclusion.

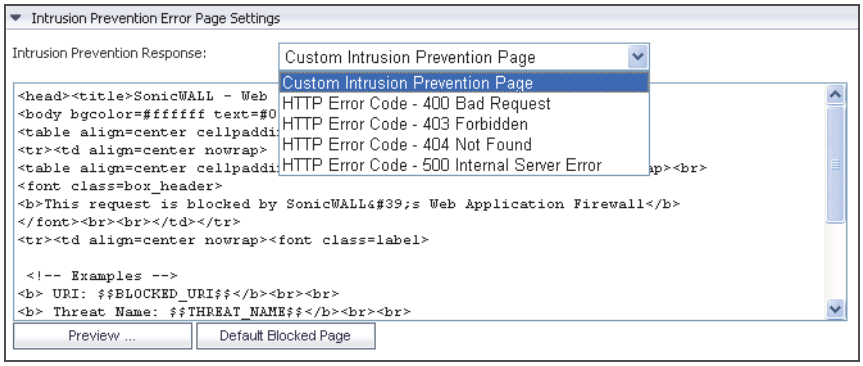
**Step 7** When finished, click **Accept**.

## Configuring Intrusion Prevention Error Page Settings

To configure the error page to use when intrusions are detected, perform the following steps:

**Step 1** Expand the **Intrusion Prevention Error Page Settings** section.

**Step 2** In the **Intrusion Prevention Response** drop-down list, select the type of error page to be displayed when blocking an intrusion attempt.




**Step 3** To create a custom page, select **Custom Intrusion Prevention Page** and modify the sample HTML in the text box.

**Step 4** To view the resulting page, click the **Preview** button.

**Step 5** To reset the current customized error page to the default error page, click the **Default Blocked Page** button and then click **OK** in the confirmation dialog box.

**Step 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

**Step 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, which 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, perform the following steps:

**Step 1** Expand the **Cross-Site Request Forgery (CSRF/XSRF) Protection** section.

**Step 2** In the **Portals** drop down list, select the Portal to which these CSRF protection settings will apply. To make these CSRF settings the default for all portals, select **Global**.

**Step 3** Select **URL Rewrite-based Protection** from the **Protection Method** drop down list.

**Step 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.

**Step 5** When finished, click **Accept**.

To configure the settings for CSRF protection with the Form-based Protection Method, perform the following steps:

**Step 1** Expand the **Cross-Site Request Forgery (CSRF/XSRF) Protection** section.

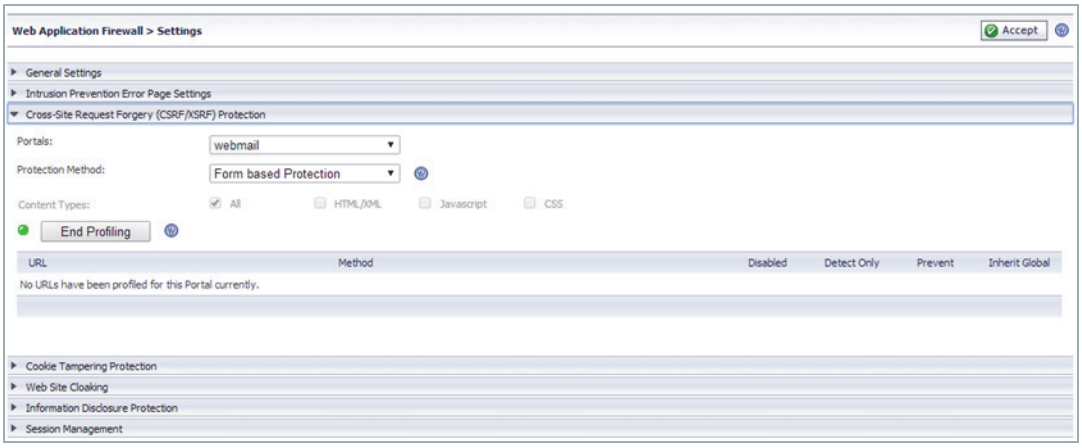
**Step 2** In the **Portals** drop down list, select the Portal to which these CSRF protection settings will apply. To make these CSRF settings the default for all portals, select **Global**.

**Step 3** Select **Form-based Protection** from the **Protection Method** drop down list.

**Step 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**.

**Step 5** Click the **Begin Profiling** button to start the CSRF Form-based Protection. If you wish to stop profiling, click **End Profiling**.

**Step 6** When finished, click **Accept**.

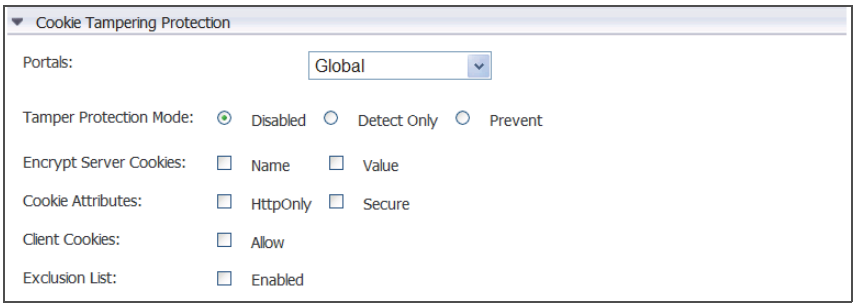



**Note** If you are upgrading from a previous firmware version and switch the Protection Method to **Form-based Protection**, the controls may appear grayed and disabled. Simply click the **Accept** button to activate the controls.

## Configuring Cookie Tampering Protection Settings

Cookie tampering protection is configured independently for each Application Offloading portal. To configure the settings for cookie tampering protection, perform the following steps:

**Step 1** Expand the **Cookie Tampering Protection** section.




**Step 2** In the **Portals** drop-down list, select the Application Offloading portal to which these cookie tampering protection settings will apply. To make these cookie tampering settings the default for all portals, select **Global**.

**Step 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.

**Step 4** For **Encrypt Server Cookies**, select the **Name** check box to encrypt cookie names, and/or select the **Value** check box 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.

**Step 5** For **Cookie Attributes**, select the **HttpOnly** check box to append the *HttpOnly* attribute to server-side cookies, and/or select the **Secure** check box to append the *Secure* attribute to server-side cookies. The attribute *HttpOnly* prevents the client-side scripts from accessing the cookies, which 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.

**Step 6** For **Client Cookies**, select the **Allow** check box 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.

**Step 7** For the **Exclusion List**, select the **Enabled** check box to display additional fields for configuration.

**Step 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 the **Add >** button.

**Step 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 the **< Add** button to add them to the **Exclusion List**.

**Step 10** To remove cookies from the **Exclusion List**, select the cookies to be removed and then click the **Remove** button.

**Step 11** To clear the **Detected Cookies** list, click the **Clear** button.

**Step 12** When finished, click **Accept**.

## Configuring Web Site Cloaking

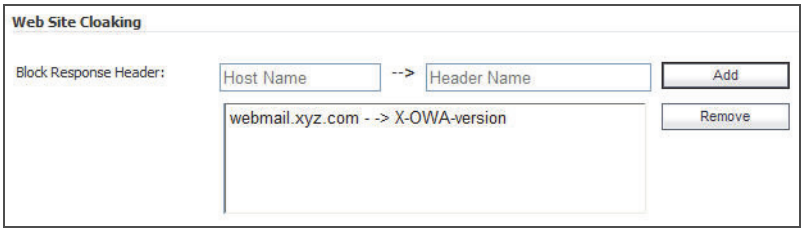
Under **Web Site Cloaking**, you can filter out headers in response messages that could provide information to clients about the backend Web server, which could possibly be used to find a vulnerability.

To configure Web site cloaking:

---

**Step 1** Expand the **Web Site Cloaking** section.

**Step 2** In the **Block Response Header** fields, 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” will be blocked. In general, listed headers will not be sent to the client if an HTTP/HTTPS bookmark or offloaded 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 will not occur for headers such as Content-Type that are critical to the HTTP protocol.

**Step 3** To remove a host/header pair from the list to be blocked, select the pair in the text box and then click the **Remove** button.

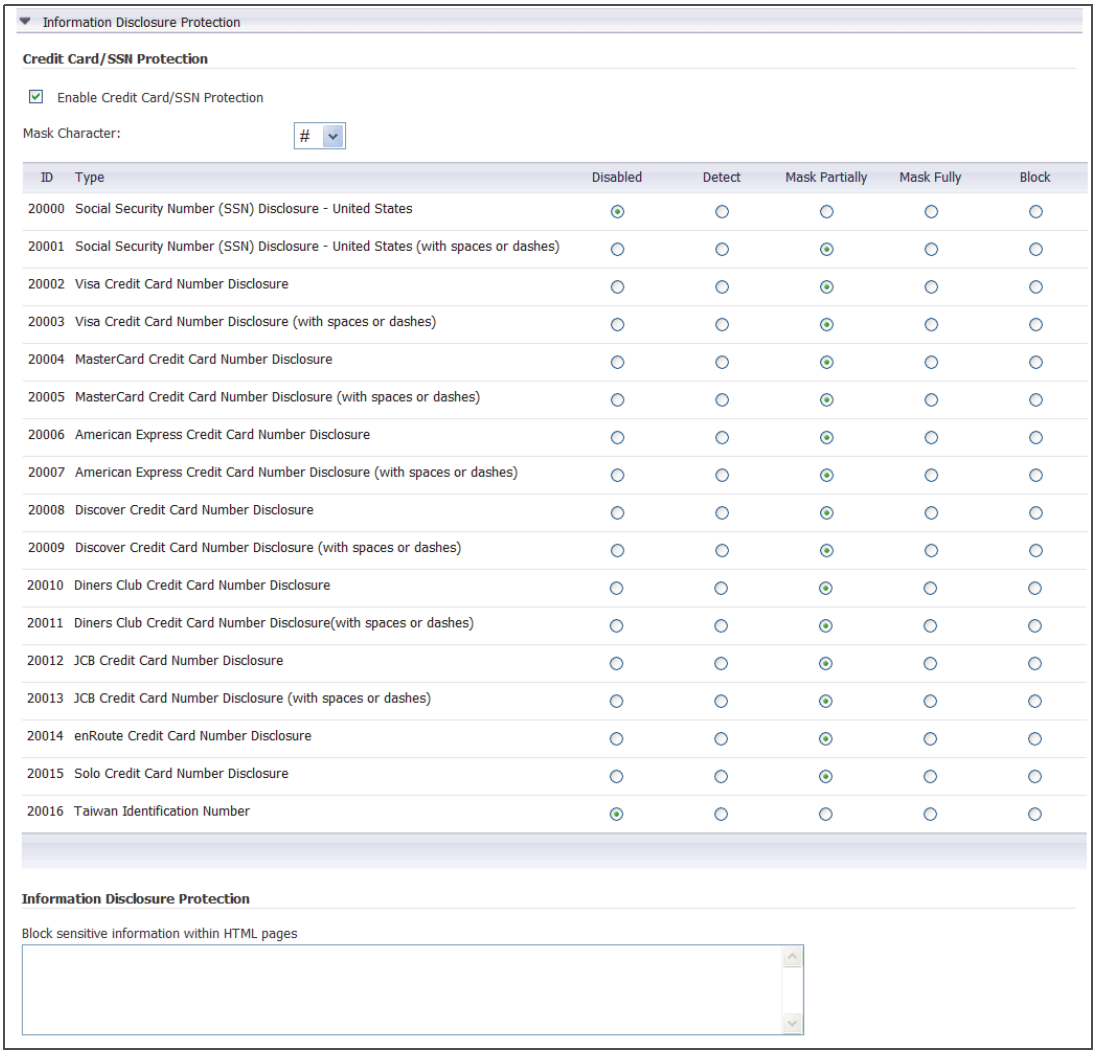
**Step 4** When finished, click **Accept**.

## 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:

**Step 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.




**Step 2** Select the **Enable Credit Card/SSN Protection** check box.

**Step 3** In the **Mask Character** drop-down list, select the character to be substituted when masking the SSN or credit card number.

**Step 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 performed.
- **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.

**Step 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.

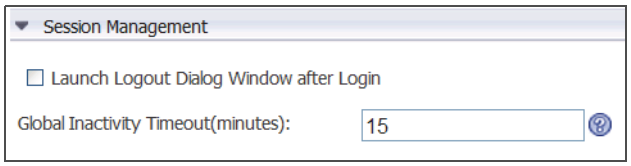
**Step 6** When finished, click **Accept**.

## 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:

**Step 1** Expand the **Session Management** section.




**Step 2** Select the **Launch Logout Dialog Window after Login** check box to display the session logout popup dialog box when the user portal is launched or when a user logs into an application offloaded portal.

**Step 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.

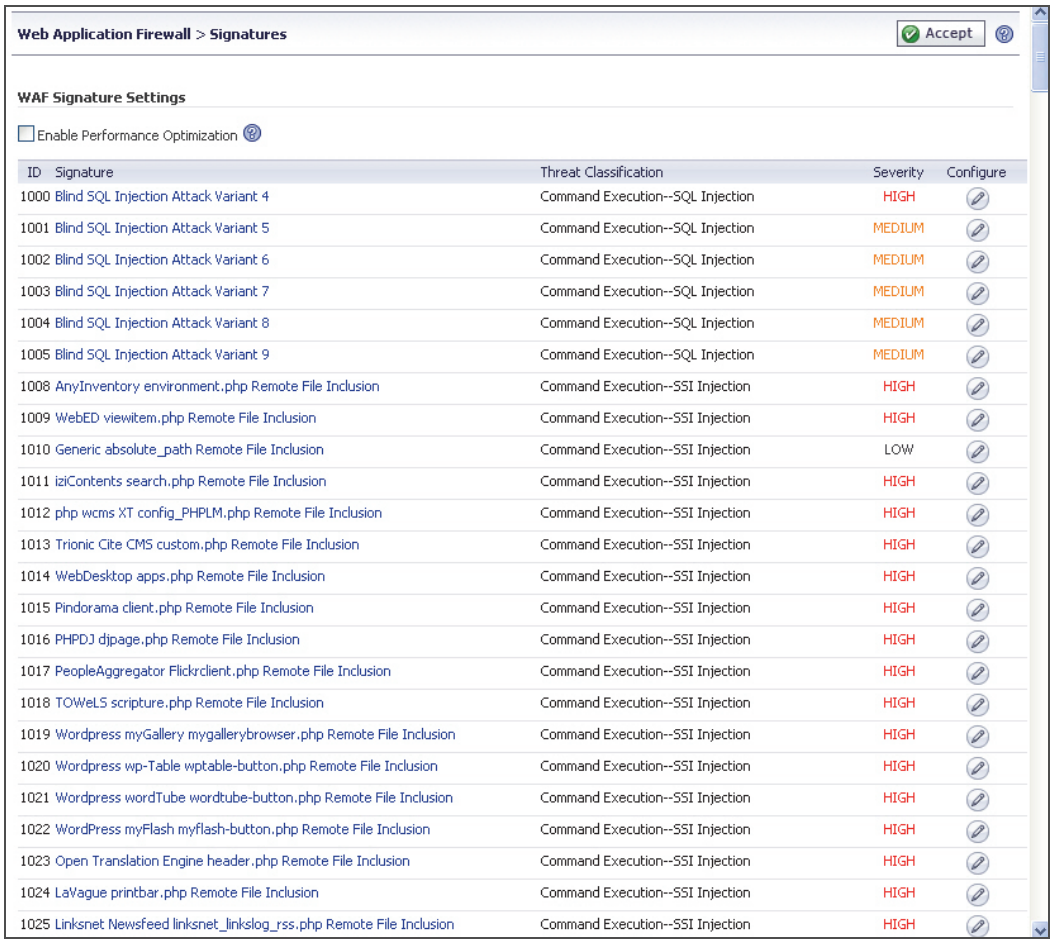
**Note** To mitigate CSRF attacks, it is important to keep a low idle timeout value for user sessions, such as 10 minutes.

**Step 4** When finished, click **Accept**.

# Configuring Web Application Firewall Signature Actions

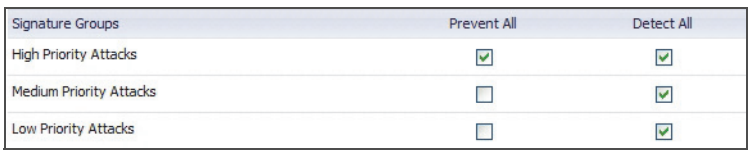
The Web Application Firewall > Signatures page allows you to configure custom handling or exclusion of certain hosts on a per-signature basis. You can use signature-based exclusions to apply exclusions for all hosts for each signature.

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.




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 277.




See the following sections:

- Enabling Performance Optimization on page 289
- Configuring Signature Based Custom Handling and Exclusions on page 289
- Reverting a Signature to Global Settings on page 291

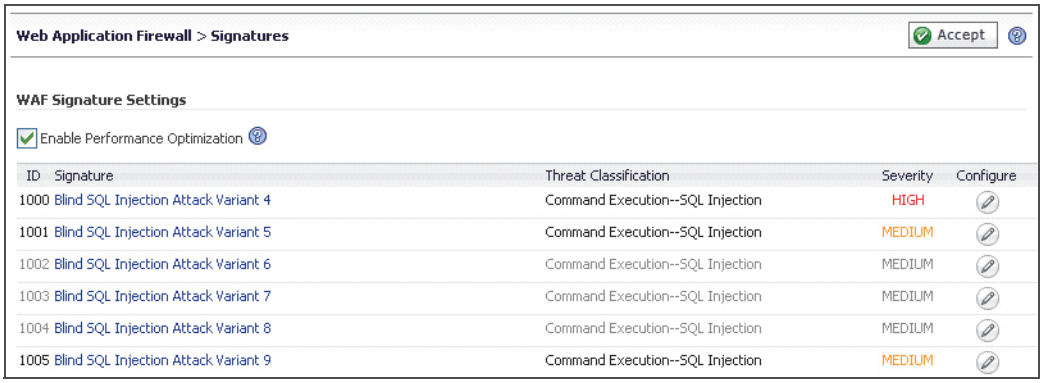
- Removing a Host from a Per-Signature Exclusion on page 291

## 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 Dell SonicWALL signature team and the list is pushed out to SRA appliances. When you select the **Enable Performance Optimization** check box, 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 Figure 40.

***Figure 40 Enabling Performance Optimization***



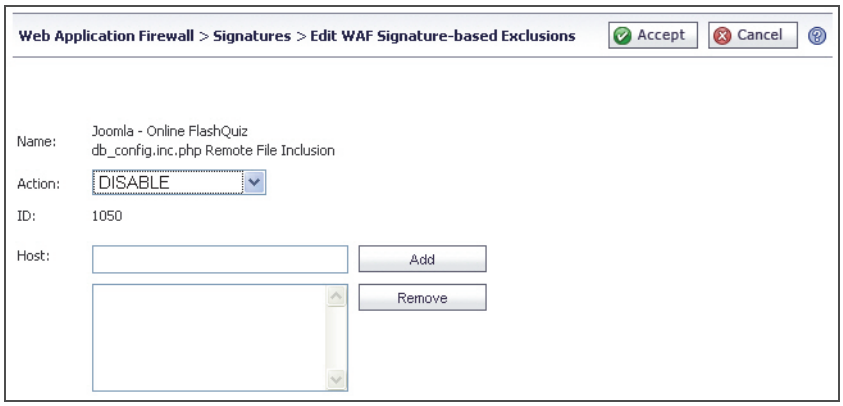

## Configuring Signature Based Custom Handling and Exclusions

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 will block access to a host when the attack signature is detected. Similarly, you can lower the level of protection to Detect if the associated signature group is globally set to Prevent All.

**Note** For signature based customization to take effect, the signature group of the modified signature must be globally enabled for either prevention or detection on the Web Application Firewall > Settings page.

To configure one or more hosts with an exclusion from inspection for a signature, or to configure custom handling when Web Application Firewall detects a specific signature for one or more hosts, perform the following steps:

**Step 1** On the Web Application Firewall > Signatures page, click the **Configure** button for the signature that you wish to change. The **Edit WAF Signature-based Exclusions** screen displays.




**Step 2** In the Edit WAF Signature-based Exclusions screen, select one of the following actions from the **Action** drop-down list:

- **DISABLE** – Disable Web Application Firewall inspections for this signature in traffic from hosts listed in this exclusion
- **DETECT** – Detect and log threats matching this signature from hosts listed in this exclusion, but do not block access to the host
- **PREVENT** – Log and block host access for threats matching this signature from hosts listed in this exclusion

**Step 3** To apply this action globally to all hosts, leave the **Host** field blank. To apply this action to an individual host, type the host entry as it appears in the bookmark or offloaded application into the **Host** field. This can be a host name or an IP address. To determine the correct host entry for this exclusion, see Determining the Host Entry for Exclusions on page 291.

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.

**Step 4** If you specified a host, click **Add** to move the host name into the list box.

**Step 5** If you want to apply this action to additional individual hosts, repeat Step 3 and Step 4 to add more hosts to this exclusion.

**Step 6** Click **Accept**. If the Host list contains host entries, SonicOS SRA verifies that each host entry is valid. If no hosts were specified, a dialog box confirms that this is a global action to be applied to the signature itself.

**Step 7** Click **OK** in the confirmation dialog box.

**Step 8** Click **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 will continue to use the old settings until they are terminated.

## Reverting a Signature to Global Settings

You can revert to using global signature group settings for a signature that was previously configured with an exclusion, without losing the configuration. This allows you to leave the host names in place in case you need to re-enable the exclusion.

To revert to using global signature group settings for a signature, perform the following steps:

**Step 1** On the Web Application Firewall > Signatures page, click the **Configure** button for the signature that you wish to change.

**Step 2** In the Edit WAF Signature-based Exclusions screen, select **INHERIT GLOBAL** from the **Action** drop-down list.

**Step 3** The **Host** field may be blank if global settings were previously applied to this signature. To revert to global signature settings for all hosts, leave the **Host** field blank. To apply this action to one or more individual hosts, leave these host entries in the **Host** field and remove any host entries that are not to be reverted.

**Step 4** Click **Accept**. SonicOS SRA verifies that each host entry is valid.

**Step 5** Click **OK** in the confirmation dialog box.

**Step 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 will continue to use the old settings until they are terminated.

## Removing a Host from a Per-Signature Exclusion

To remove a host from a configured exclusion for a signature, perform the following steps:

**Step 1** On the Web Application Firewall > Signatures page, click the **Configure** button for the signature that you wish to change.

**Step 2** Select the host entry in the list box under the Host field, and then click **Remove**.

**Step 3** Repeat Step 2 to remove other listed hosts, if desired.

**Step 4** Click **Accept**. SonicOS SRA verifies that each host entry is valid.

**Step 5** Click **OK** in the confirmation dialog box.

**Step 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 will continue to use the old settings until they are terminated.

# Determining the Host Entry for Exclusions

When configuring an exclusion, either globally or per-signature, you must provide the host name or IP address. The affected hosts must match the host names used in your HTTP(S) bookmarks and Citrix bookmarks, and the virtual host domain name configured for an offloaded Web application.

For a description of how to determine the correct host name, see the following sections:

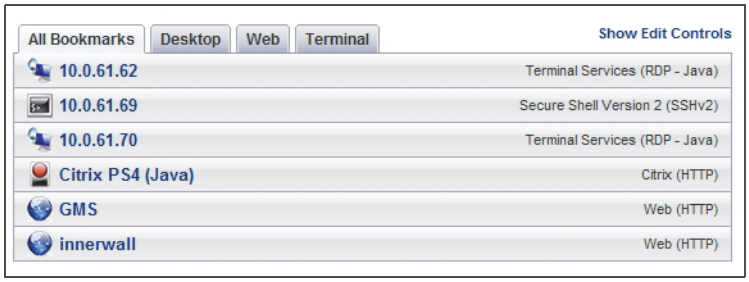
- Viewing the Host Entry in a Bookmark on page 292
- Viewing the Host Entry in an Offloaded Application on page 292

## Viewing the Host Entry in a Bookmark

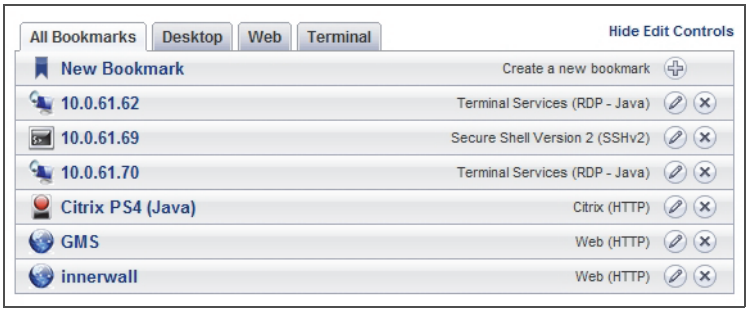
You can determine exactly what host name to enter in your exclusion by viewing the configuration details of the bookmark.

To view the host entry in a bookmark, perform the following steps:

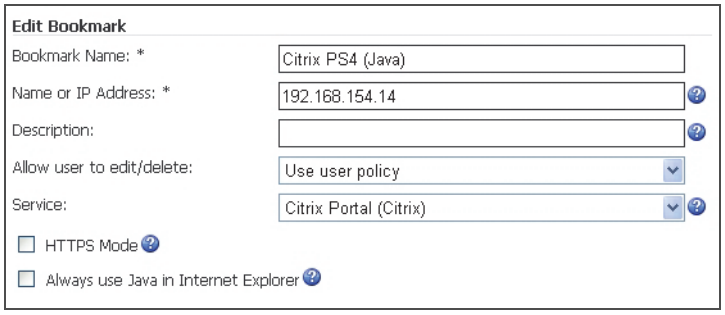
**Step 1** Navigate to the Virtual Office page, and click **Show Edit Controls** above the list of bookmarks.




**Step 2** Click the Edit button for the bookmark.




**Step 3** In the Edit Bookmark screen, view the host entry in the **Name or IP Address** field.



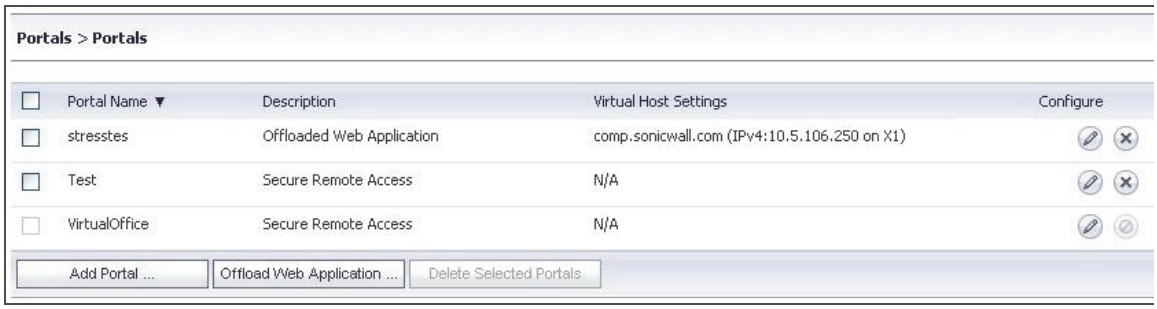

**Step 4** Click **Cancel**.

## Viewing the Host Entry in an Offloaded Application

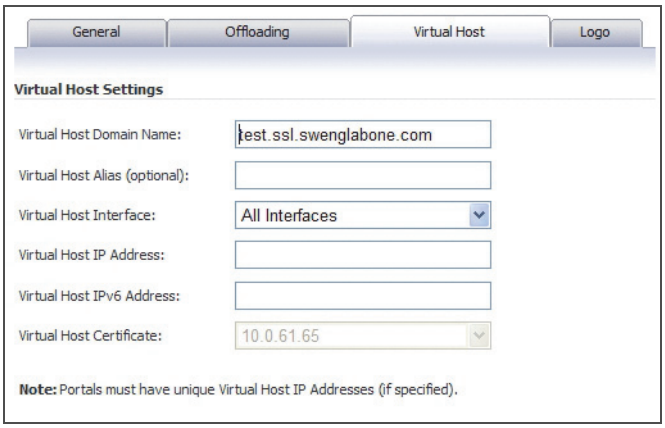
You can determine exactly what host name to enter in your exclusion by viewing the configuration details of the offloaded application. In an offloaded application, you will use the virtual host domain name.

To view the virtual host domain name in an offloaded application, perform the following steps:

**Step 1** Navigate to the Portals > Portals page and click the Configure button next to the offloaded application.




**Step 2** In the Edit Portal screen, click the **Virtual Host** tab.




**Step 3** View the host entry for your exclusion in the **Virtual Host Domain Name** field.

**Step 4** Click **Cancel**.

# Configuring Custom Rules and Application Profiling

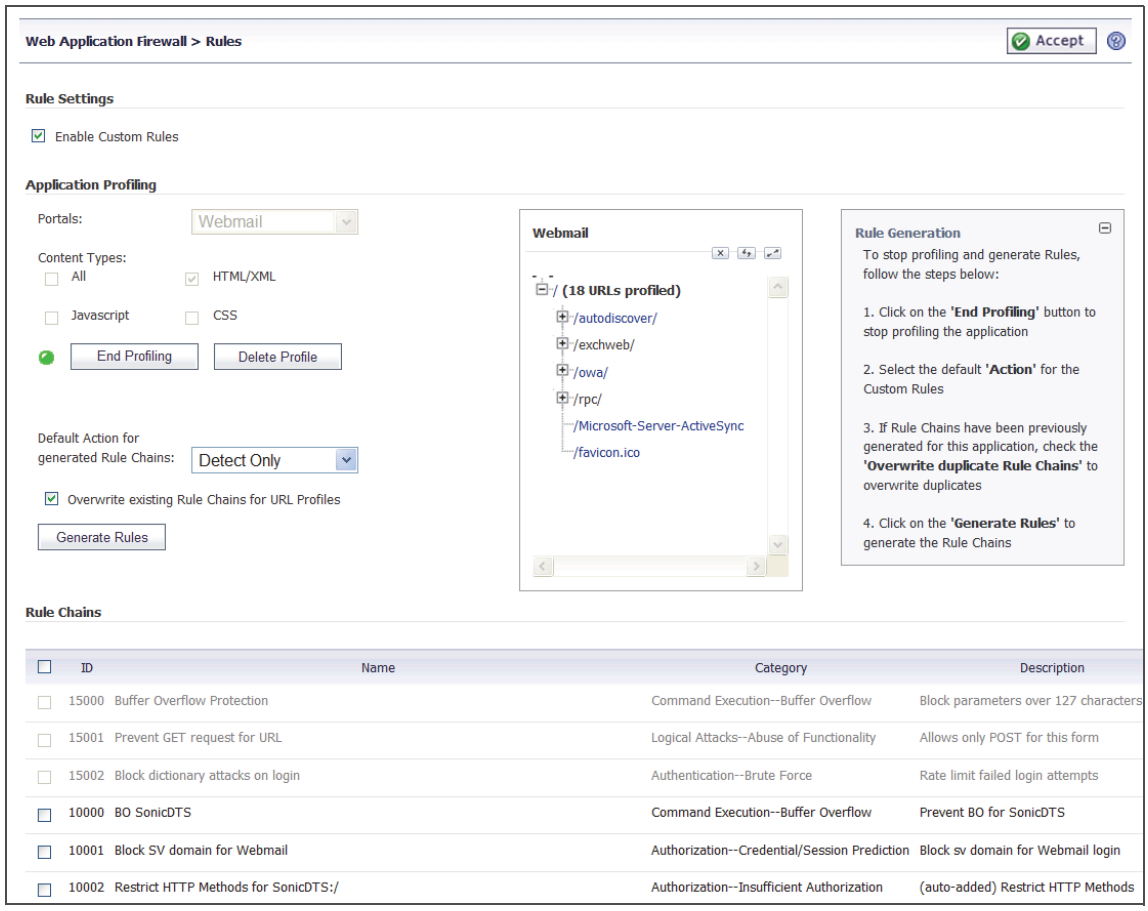
The Web Application Firewall > Rules page allows you to configure custom rules and application profiling.

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 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 79.

**Note** Application profiling is supported only on the SRA 4600, 4200, and Virtual Appliance.

Custom rules created on this page have all the same properties as the signatures that Dell SonicWALL pushes out to Web Application Firewall-enabled appliances. Figure 41 shows the Rules page.

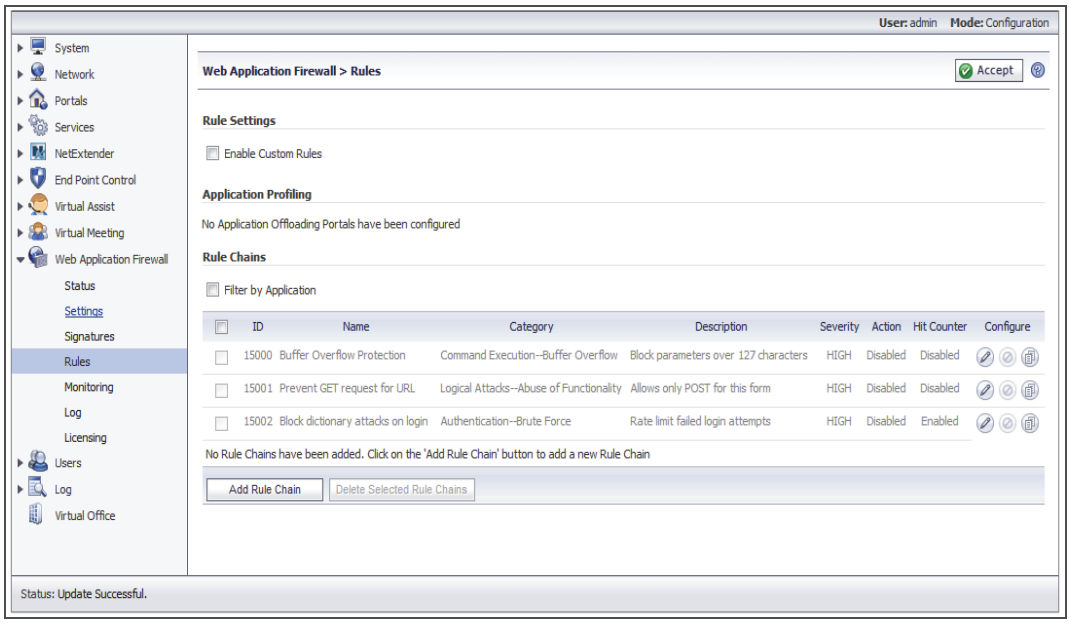
***Figure 41 Web Application Firewall > Rules Page***




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. Figure 42 shows all rule chain fields.

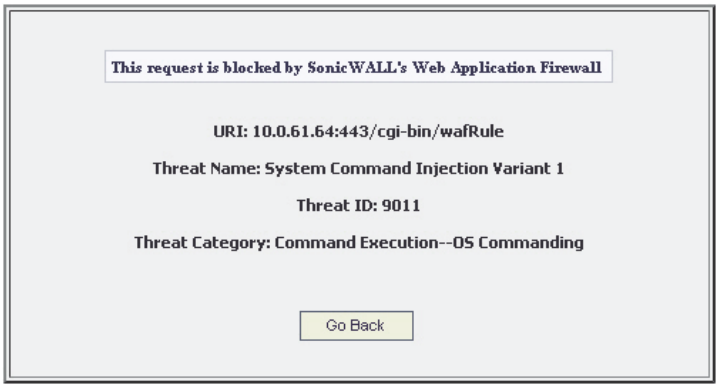
Rules in the Web Application Firewall > Rules page can be divided into pages and filtered by searching for a key word. To display only rules containing a key word in all fields or a specific field, type the key word in the Search field, select **All Fields** or a specific field to search, and click **Search**. 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.

***Figure 42 Rule Chains***



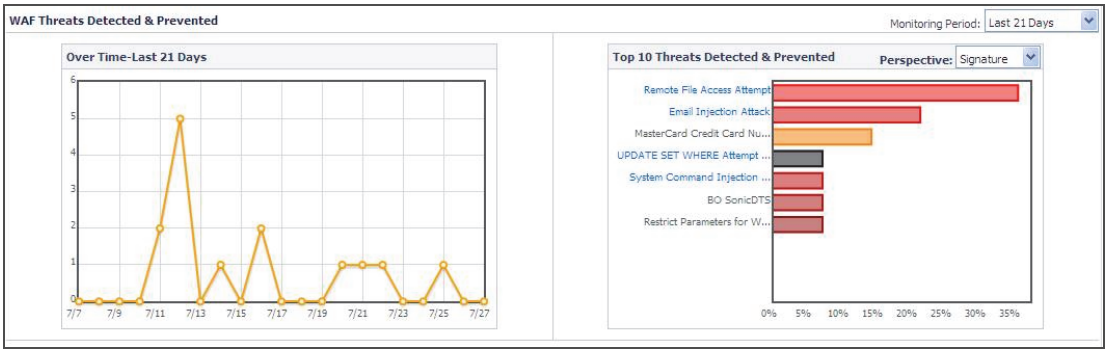

Custom rules and rule chains can be used to distinguish between legitimate and illegitimate traffic as defined by a Web application that is using a certain URI or running on a certain portal. One rule in the chain is configured to match the URI or portal host name, while another rule is created that 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 performed 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 Figure 43.

***Figure 43 Block Page***



The Web Application Firewall > Monitoring page also shows the activity in the graphs. Figure 44 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 311.

***Figure 44 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 performed. 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

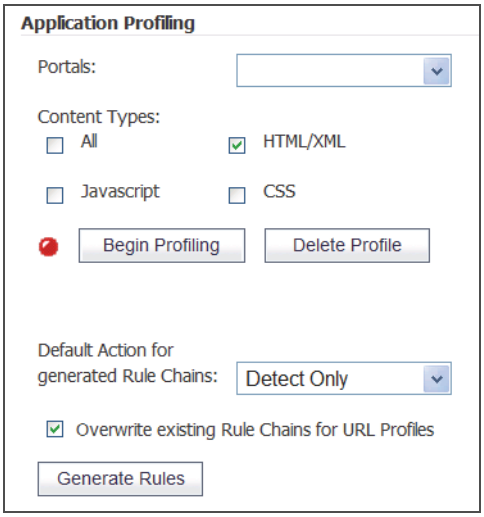
You can create URL profiles by putting the SRA appliance into learning mode while applications are in use by trusted users, and then use those URL profiles to generate rule chains that prevent malicious misuse of the applications.

**Note** Application profiling is supported only on the SRA 4600, 4200, and Virtual Appliance.

To configure application profiling and automatically generate rules:

**Step 1** Navigate to the Web Application Firewall > Rules page.

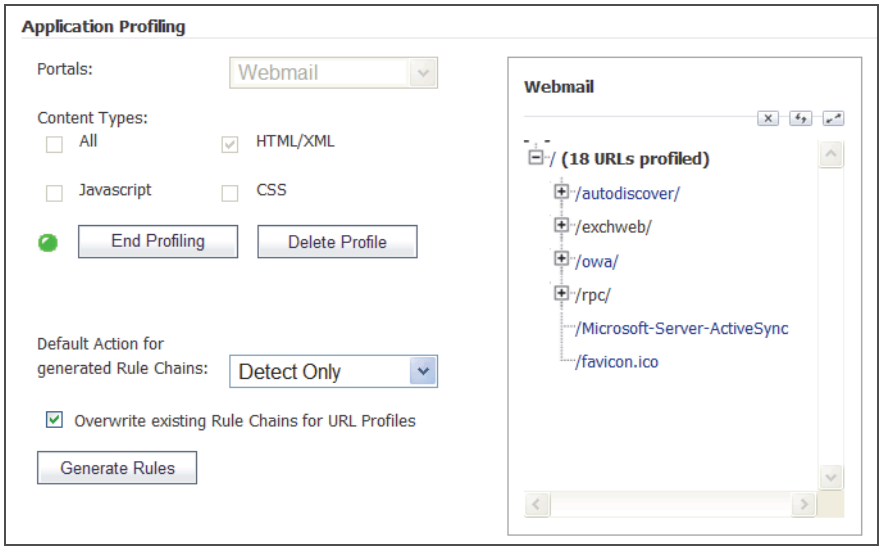
**Step 2** Under **Application Profiling**, select one or more portals with the application(s) to be profiled from the **Portals** drop-down list. Use Shift+click or CTRL+click to select multiple portals.




**Step 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.

**Step 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. The **Begin Profiling** button changes to **End Profiling**. Profiling continues until you click **End Profiling**.

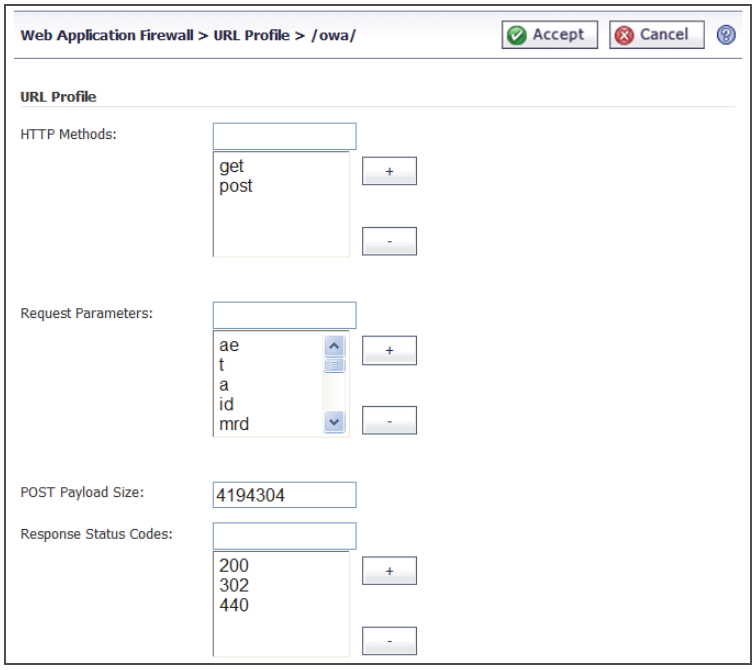


During profiling, the SRA records inputs and stores them as URL profiles. The URL profiles are listed as a tree structure on the Web Application Firewall > Rules page in the Application Profiling section.

**Step 5** After a period of time adequate to record inputs from normal application use, click **End Profiling** to stop the profiling process.

**Step 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.




**Step 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.

**Step 8** Click **Accept** when finished editing. Repeat for other URLs as needed.

**Step 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 will be disabled rather than active.
- **Detect Only** – Content triggering the generated rule will be detected and logged.
- **Prevent** – Content triggering the generated rule will be blocked and logged.

**Step 10** Select the **Overwrite existing Rule Chains for URL Profiles** check box to overwrite rule chains that have already been generated from a URL profile.

**Step 11** Click the **Generate Rules** button 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.

**Step 12** If you do not want to accept the generated rule chains, click the **Delete Selected Rule Chains** button, which is available below the rule chain list. All of the automatically added rule chains are pre-selected right after generation for easy deletion of the group.

**Step 13** Click **Accept** to apply the generated rule chains to the SRA 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 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.

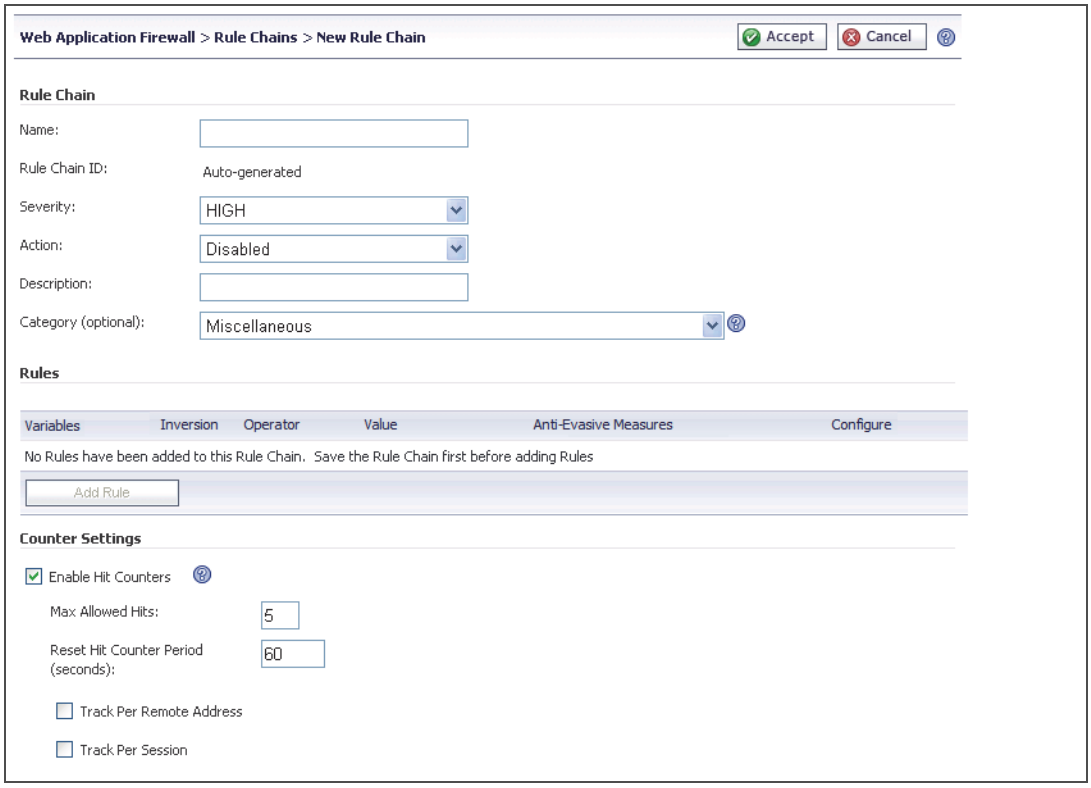
### Adding or Editing a Rule Chain

To add or edit a rule chain, perform the following steps:

**Step 1** On the Web Application Firewall > Rules page, click the **Add Rule Chain** button 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.




**Step 2** On the New Rule Chain page, type a descriptive name for the rule chain in the **Name** field.

**Step 3** Select a threat level from the **Severity** drop-down list. You can select **HIGH**, **MEDIUM**, or **LOW**.

**Step 4** Select **Prevent**, **Detect Only**, or **Disabled** from the **Action** drop-down list.

- **Prevent** – Block traffic that matches the rule and log it.
- **Detect** – Allow the traffic, but log it.
- **Disabled** – The rule chain should not take effect.

The **Disabled** option allows you to temporarily deactivate a rule chain without deleting its configuration.

**Step 5** In the **Description** field, type a short description of what the rule chain will match or other information.

**Step 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.

**Step 7** Under **Counter Settings**, to enable tracking the rate at which the rule chain is being matched and to configure rate limiting, select the **Enable Hit Counters** check box. Additional fields are displayed.

**Step 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.

**Step 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.

**Step 10** Select the **Track Per Remote Address** check box 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 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.

**Step 11** Select the **Track Per Session** check box 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.

**Step 12** Click **Accept** to save the rule chain. A **Rule Chain ID** is automatically generated.

**Step 13** Next, add one or more rules to the rule chain. See Configuring Rules in a Rule Chain on page 302 for detailed information.

### Cloning a Rule Chain

To clone a rule chain:

**Step 1** On the Web Application Firewall > Rules page, click its Clone Rule Chain icon under **Configure**.

**Step 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 299.

### Deleting a Rule Chain

**Note** Deleting a rule chain also deletes all the associated rules.

To delete a rule chain:

**Step 1** On the Web Application Firewall > Rules page, click the Delete Rule Chain icon  under **Configure** for the rule chain you want to delete.

**Step 2** Click **OK** in the confirmation dialog box.

**Step 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 will 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 will see the Web Application Firewall block page (as configured on the Web Application Firewall > Settings page). If not, there will be 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 SRA appliance. For example, the admin may 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 will mean 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, which 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 SRA appliance will be denied, because the Web management interface depends on the GET method.

To fix a misconfigured rule chain, perform the following tasks:

**Step 1** Point your browser to https://<SRA IP>/cgi-bin/welcome.

If you try to reach the welcome page by simply using the URL https://<SRA IP>/, the usual redirect to https://<SRA IP>/cgi-bin/welcome may not work. To repair misconfigured rules, you need to explicitly go to https://<SRA IP>/cgi-bin/welcome, where <SRA IP> is the host name or IP address of your SRA appliance.

**Step 2** Log in as **admin**.

**Step 3** Navigate to the Web Application Firewall > Rules page.

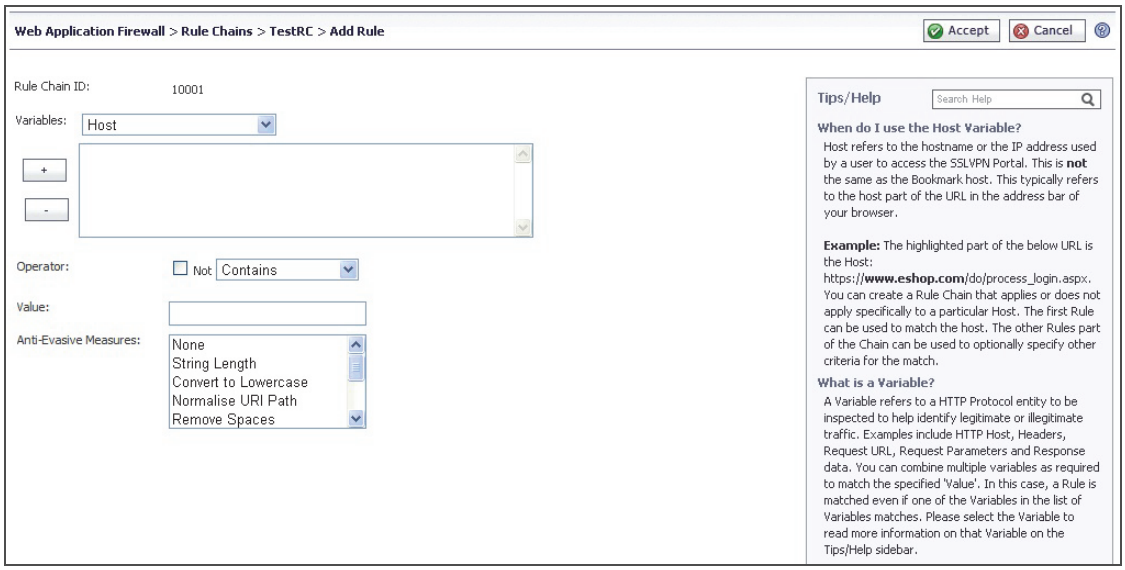
**Step 4** Edit or delete the bad rules.

**Step 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. Figure 45 shows the Add Rule page.

***Figure 45 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 303 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 305 for more information about the operators.
- **Value** – This entity can be a number, literal string, or a regular expression, which 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 305 for more information about these measures.

The following sections provide detailed information about rules:


- About the Tips/Help Sidebar on page 303
- About Variables on page 303

- About Operators on page 305
- About Anti-Evasive Measures on page 305
- Example Use Cases for Rules on page 307
- Deleting a Rule on page 310
- Cloning a Rule on page 310
- Adding or Editing a Rule on page 310


### 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**.

Table 16 on page 303 describes the available variables.

***Table 16 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. |

| Variable Name | Collection | Description |
|---|---|---|
| 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.<br>To match against some aspect of the entire list of parameter values, such as the number of parameter values, leave the selection field empty.<br>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.<br>To match against some aspect of the entire list of parameter names, leave the selection field empty.<br>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.<br>To match against some aspect of the entire list of request header values, leave the selection field empty.<br>To match against a particular header value, specify the name of the header in the selection field to the right of the colon.<br>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. |
| Request Header Names | Yes | Refers to the collection of all HTTP(S) request header names for the current request.<br>To match against some aspect of the entire list of request header names, leave the selection field empty.<br>To match against a particular header name, specify the name of the header in the selection field to the right of the colon.<br>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.<br>To match against some aspect of the entire list of response header values, leave the selection field empty.<br>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.<br>To match against some aspect of the entire list of response header names, leave the selection field empty.<br>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. |

| Variable Name | Collection | Description |
|---|---|---|
| Portal Hostname | No | Refers to the virtual host name of the SRA portal which accepts the request from the client.<br>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 SRA 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, which 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**.

Table 17 describes the available operators for use with rules.

***Table 17 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. Table 18 describes the anti-evasive measures available for use with rules.

***Table 18 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. |
| 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.<br>This is an anti-evasive measure to prevent hackers from changing case to bypass the rule. |
| Normalise URI Path | Use the **Normalise 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.<br>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.<br>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.<br>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.<br>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.<br>This is an anti-evasive measure to prevent hackers from using hexadecimal encoding of their input to bypass the rule. |

| Measure | Description |
|---|---|
| URL Decode<br>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.<br>**NOTE**: Do not use these measures against an input that has been decoded already.<br>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.<br>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.<br>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.

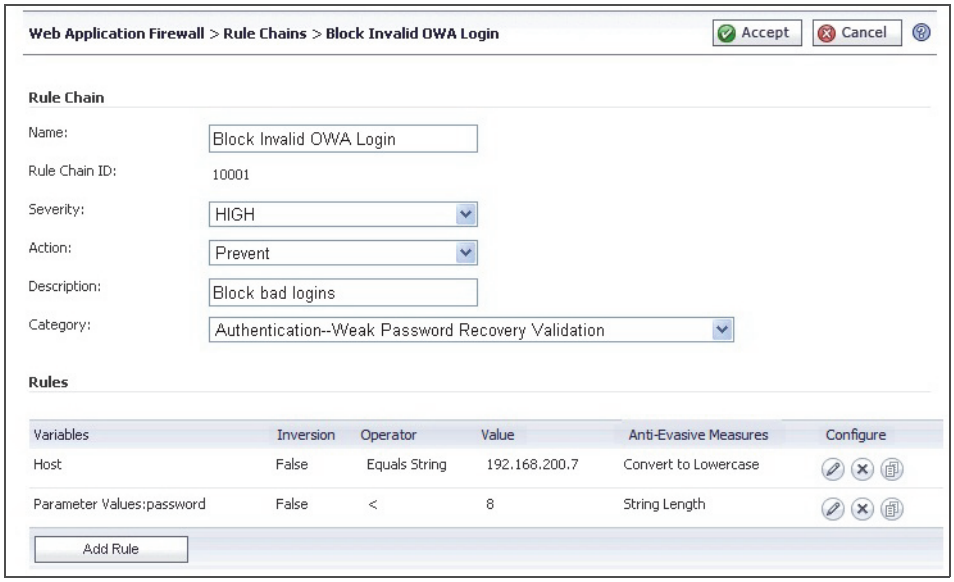
### Example – Positive Security Model: Blocking Bad Logins

To prevent login 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**. Figure 46 shows the rule chain for this example.

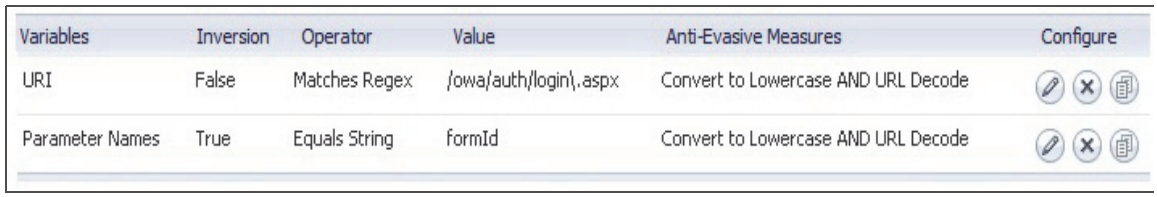
***Figure 46 Example Rule Chain – Blocking Bad Logins***




**Example – Positive Security Model: Blocking a Form Submission with Unwanted Parameters**

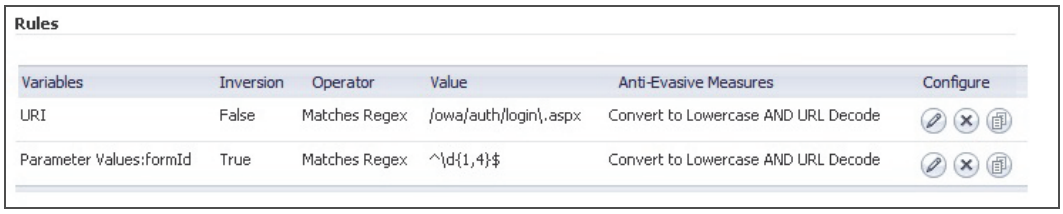
This rule chain blocks a form submission if the form has a request parameter other than **formId** or if the value of **formId** contains more than 4 digits. To accomplish this, you would need two rule chains:

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.

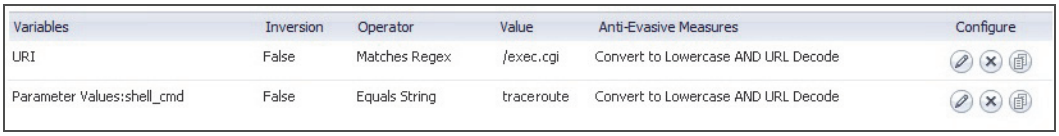
– The second rule checks if the value contained by the **Parameter Value: formId** variable matches the regular expression **^\d{1,4}$** which matches anything that consists of 1 to 4 digits. The **Not** inversion check box is selected to change the rule to match anything that does not consist of 1 to 4 digits.




### 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**.




### 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 may attempt to sneak those characters into the request by performing URL encoding on the characters before adding them to the request. The URI will then contain **%0D** and **%0A** characters, which 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, which 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 310.

## Adding or Editing a Rule

To add or edit a rule in a rule chain, perform the following steps:

**Step 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.

**Step 2** Click the **Add Rule** button to add a new rule, or click the Edit icon under **Configure** for the rule you want to edit.

**Step 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 303 for information about the available variables.

**Step 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).

**Step 5** Click the Plus button + 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 the Minus button [ - ].

**Step 6** Select a string or arithmetic operator from the **Operators** drop-down list. To perform the inverse operation, select the **Not** check box.

**Step 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 will be compared individually.

**Step 8** Select one or more measures from the **Anti-Evasive Measures** list. Hold the **Ctrl** button on your keyboard while clicking to select multiple measures.

**Step 9** Click the **Accept** button when finished.

# Using Web Application Firewall Monitoring

The Web Application Firewall > Monitoring page provides two tabs: **Local** and **Global**. The pages for both tabs display statistics and graphs for detected/prevented threats over time and top 10 threats. The Local tab 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 tab are explained in the following sections:

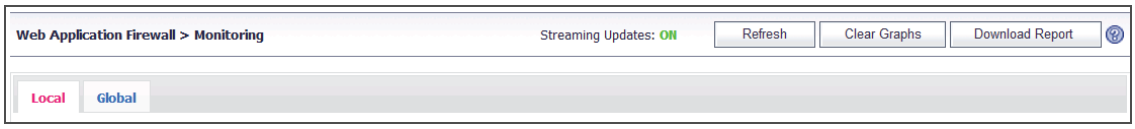
- Monitoring on the Local Tab on page 311
- Monitoring on the Global Tab on page 317

## Monitoring on the Local Tab

The Local tab 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 tab, 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:

**Step 1** Select the **Local** tab. The active tab name is displayed in red or pink, while the inactive tab name is blue. The control buttons act on the page that is currently displayed.

**Step 2** To turn streaming on or off, click the **ON** or **OFF** indicator next to **Streaming Updates**.

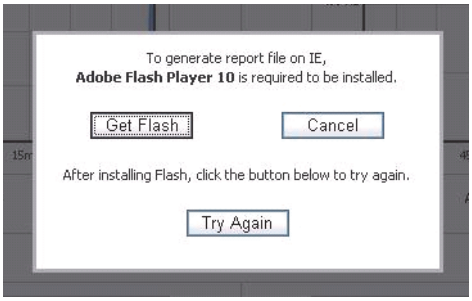
**Step 3** To refresh the display, click the **Refresh** button.

**Step 4** To clear all Web Application Firewall statistics from the graphs and list, click the **Clear Graphs** button.

**Step 5** To generate a PDF report containing Web Application Firewall statistics, click the **Download Report** button.

**Note** Internet Explorer requires Adobe Flash Player version 10 or higher to generate the report.

**Step 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** tab, 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 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** tab 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

Figure 47 shows a 24 hour period of Web server activity.

***Figure 47 Web Server Status For Last 24 Hours***

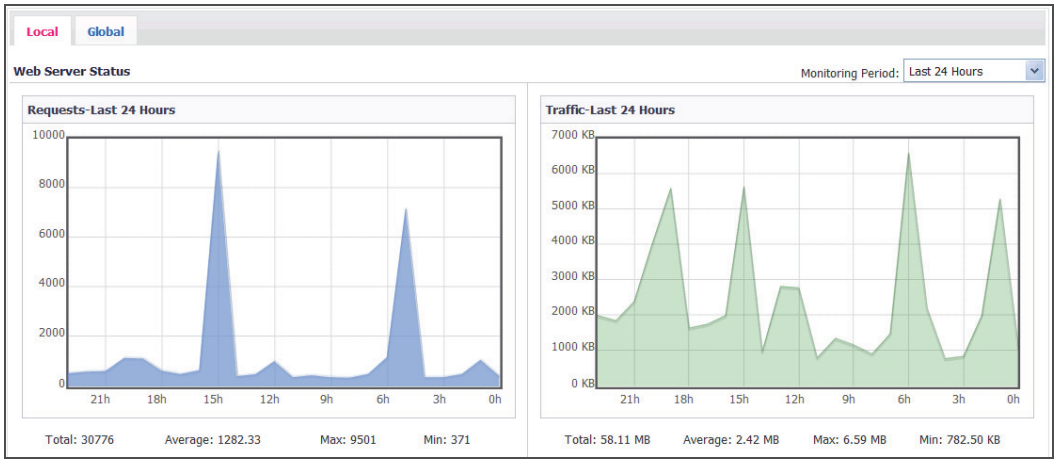
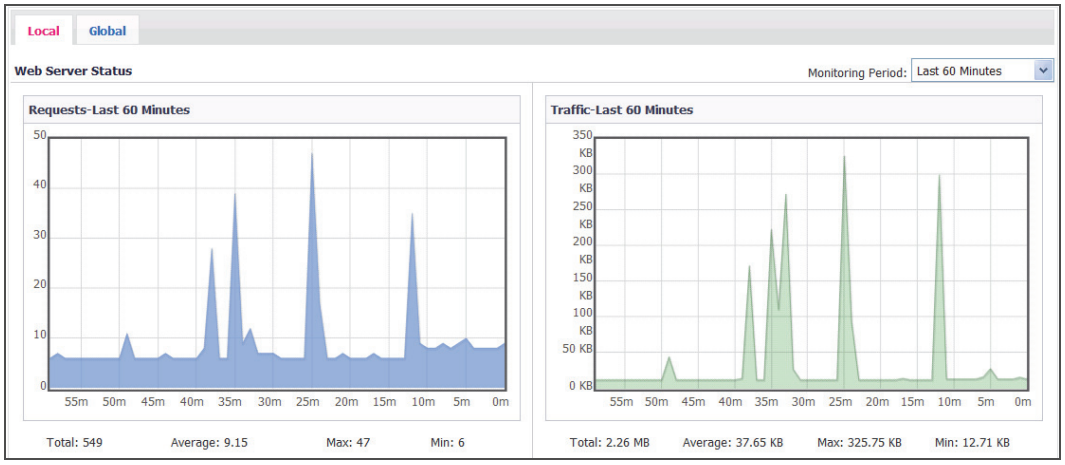



Figure 48 shows a 60 minute period of Web server activity.

***Figure 48 Web Server Status For Last 60 Minutes***




## Monitoring Detected and Prevented Threats

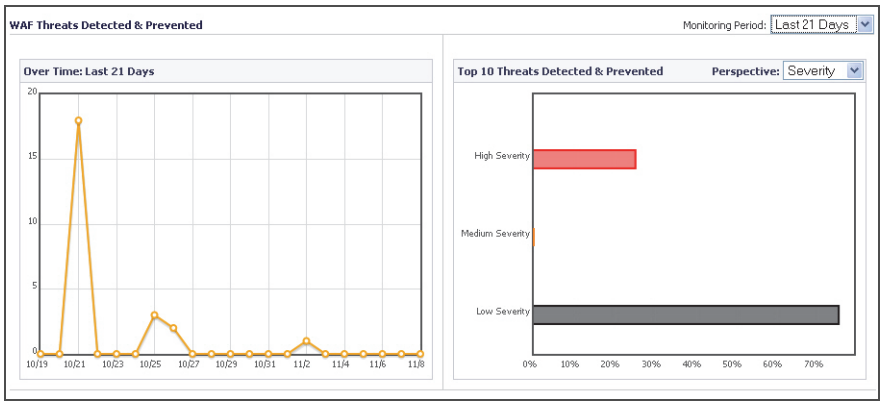
On the **Local** tab below the Web server status graphs, the Web Application Firewall > Monitoring page displays graphs indicating the number of detected and prevented threats. Two graphs are presented, one showing the number of threats over time, and the other showing the top ten threats that were detected 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

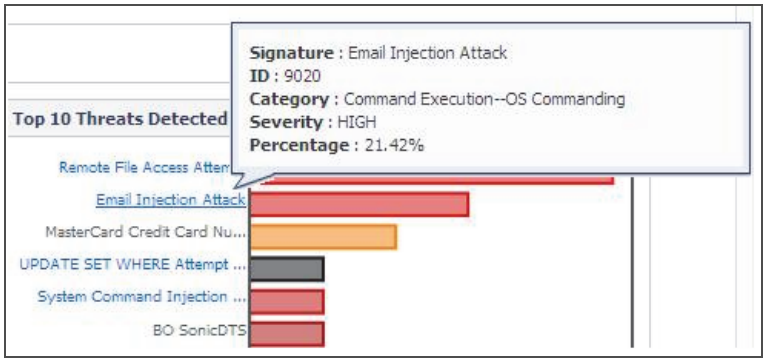
Figure 49 shows the number and severities of threats detected and prevented over the last 21 days.

***Figure 49 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.

***Figure 50 Threat Details Tooltip***




## Viewing Threats in List Format

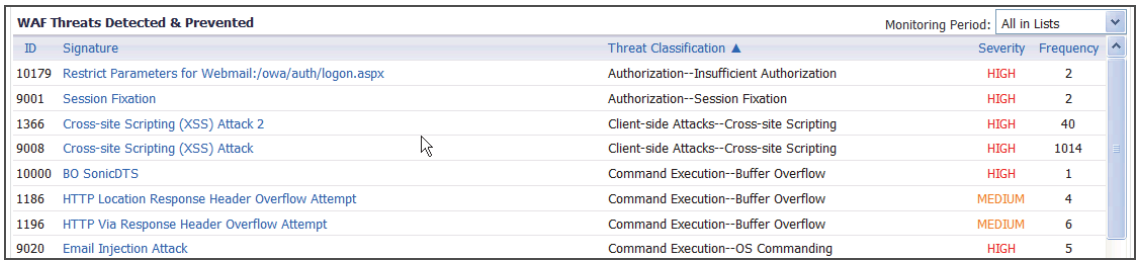
To see the threats in list format rather than as a graph, select **All in Lists** from the **Monitoring Period** drop-down list. Figure 51 shows the list format.

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.

***Figure 51 Threats in List Format***

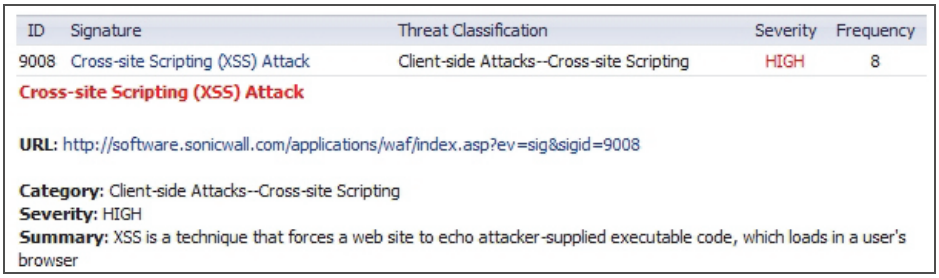



To view and hide threat details, perform the following steps:

**Step 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.

**Step 2** To display details about a threat, click on the threat. The details include the following:

- **URL** – The URL to the Dell SonicWALL knowledge base for this threat
- **Category** – The category of the threat
- **Severity** – The severity of the threat, either high, medium, or low
- **Summary** – A short description of how the threat behaves

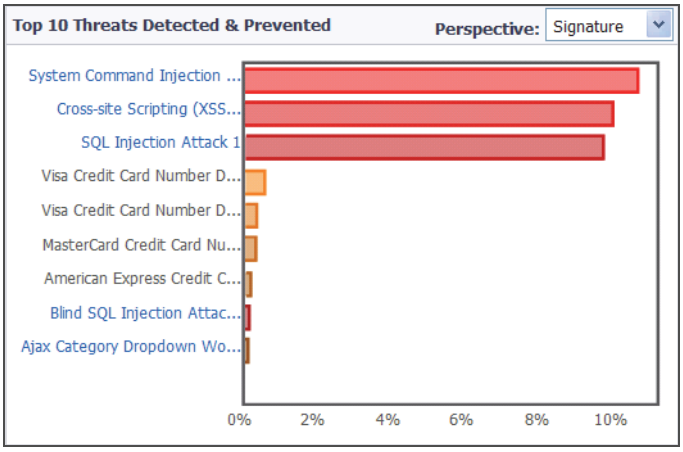



**Step 3** To collapse the threat details, click the threat link again.

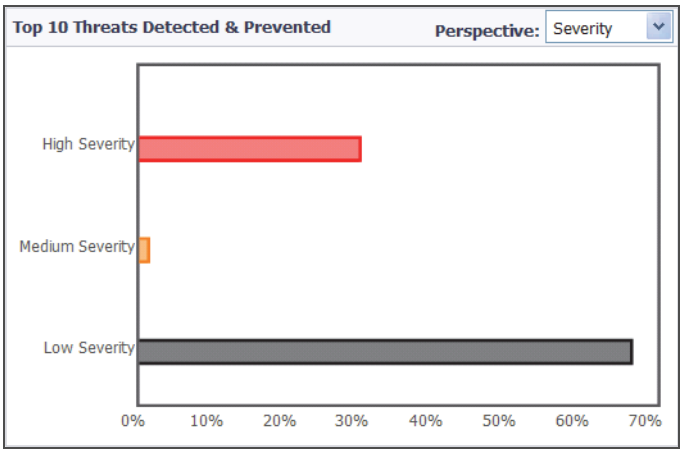
### Changing Perspective

For the Top 10 Threats graph, you can select the following display options from the **Perspective** drop-down list:

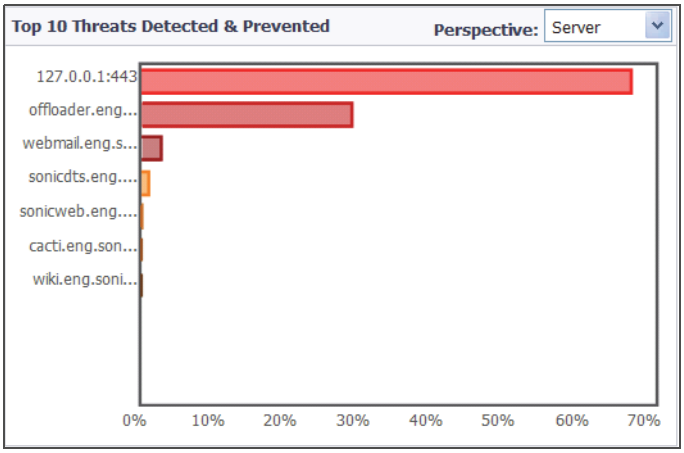
- Signature – The name of each threat shown is listed at the left side of the graph.




- 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 Tab

The **Global** tab displays statistics and graphs for threats reported by all 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 tab, 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:

**Step 1** Select the **Global** tab. The active tab name is displayed in red or pink, while the inactive tab name is blue. The control buttons act on the page that is currently displayed.

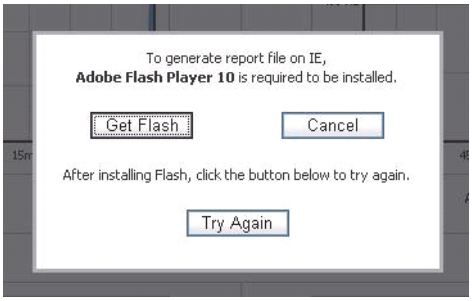
**Step 2** To turn streaming on or off, click the **ON** or **OFF** indicator next to **Streaming Updates**.

**Step 3** To refresh the display, click the **Refresh** button.

**Step 4** To generate a PDF report containing Web Application Firewall statistics, click the **Download Report** button.

**Note** Internet Explorer requires Adobe Flash Player version 10 or higher to generate the report.

**Step 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

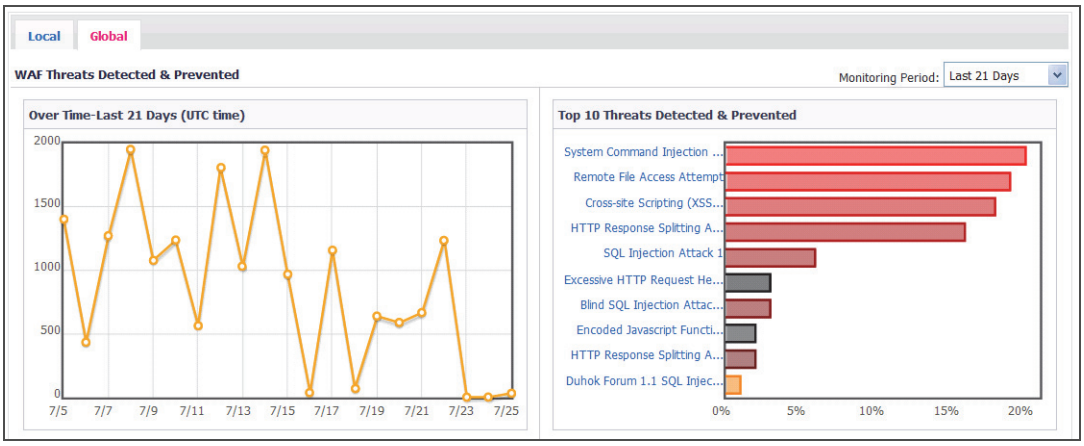
At the top of the **Global** tab, the Web Application Firewall > Monitoring page displays graphs indicating the number of detected and prevented threats. Two graphs are presented, one showing the number of threats over time, and the other showing the top ten threats that were detected and prevented during 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

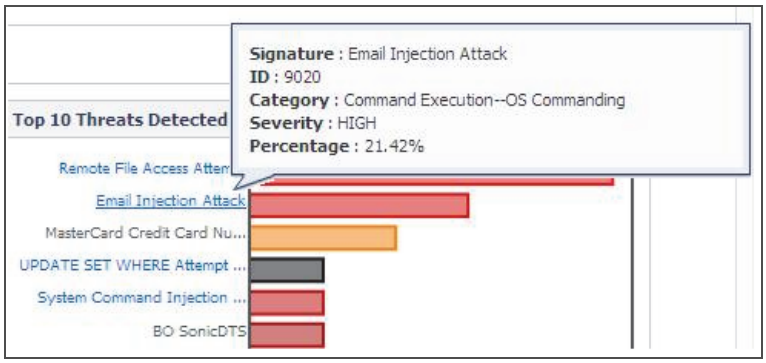
Figure 52 shows the number and severities of threats detected and prevented over the last 21 days.

***Figure 52 Threats Over Last 21 Days***




Hovering your mouse pointer over the signature ID causes a tooltip to appear with details about the threat.

***Figure 53 Threat Details Tooltip***

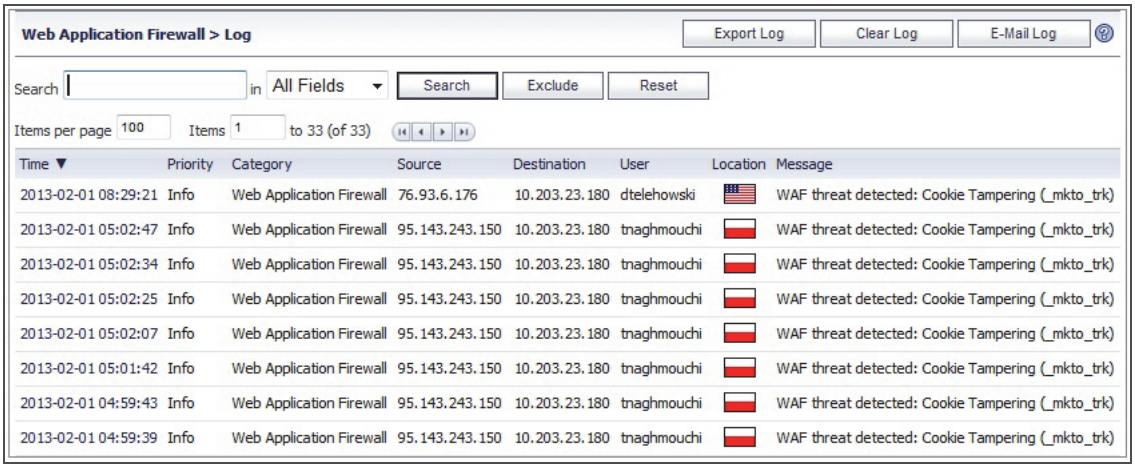



The local signature database on the appliance is accessed to get detailed threat information, but if the database is not up-to-date, some detailed information for the Top 10 Threats might not be available. In this case, the threat color in the graph is light grey, and the severity is displayed as unknown 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. Please 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 319
- Controlling the Log Pagination on page 320
- Viewing Log Entry Details on page 320
- Exporting and Emailing Log Files on page 320
- Clearing the Log on page 321


## Searching the Log

You can search for a value contained in a certain column of the log table, and can also search for log entries that do **not** contain the specified value.

To view and search Web Application Firewall log files, perform the following steps:

---

**Step 1** On the Web Application Firewall > Log page, type the value to search for into the **Search** field.

**Step 2** Select the column in which to search from the drop-down list to the right of the Search field.

**Step 3** Do one of the following:

- To start searching for log entries containing the search value, click **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, perform the following steps:

**Step 1** On the Web Application Firewall > Log page, enter the number of log entries that you want on each page into the **Items per Page** field. The Log page display changes to show the new number of entries.

**Step 2** To view the log entries beginning at a certain number, type the starting number into the **Item** field and press **Enter** on your keyboard.

**Step 3** To view the first page of log entries, click the left-most button in the arrow control pad.

**Step 4** To view the previous page of log entries, click the left arrow in the arrow control pad.

**Step 5** To view the next page of log entries, click the right arrow in the arrow control pad.

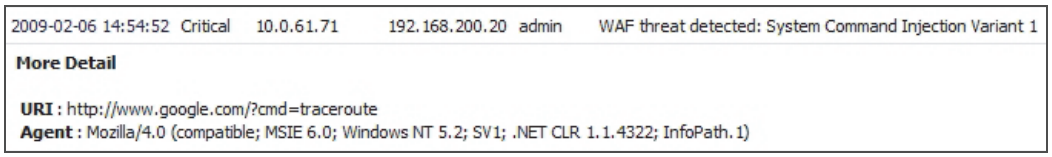
**Step 6** To view the last page of log entries, click the right-most button in the arrow control pad.

## Viewing Log Entry Details

The log entry details vary with the type of log entry. The URI (Uniform Resource Indicator) is provided along with the command for detected threats. Information about the agent that caused the event is also displayed. For an explanation of the rather cryptic Agent string, the following Wikipedia page provides a description and links to external sites that can analyze any user agent string: http://en.wikipedia.org/wiki/User_agent

To view more details about an individual log entry, perform the following steps:

**Step 1** On the Web Application Firewall > Log page, click anywhere on the log entry that you want to view. The details are displayed directly beneath the entry.



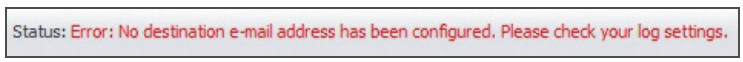

**Step 2** To collapse the details for a log entry, click again on the entry.

## Exporting and Emailing Log Files

You can export the current contents of the Web Application Firewall log to a file, or email the log contents by using the buttons in the top right corner of the Web Application Firewall > Log page.

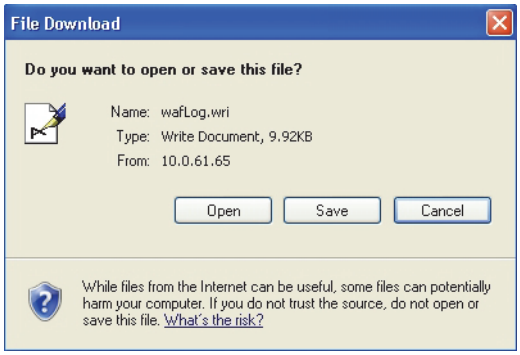
Exported files are saved with a **.wri** file name extension, and open with Wordpad, by default.

Emailed files are automatically sent to the address configured on the Log > Settings page of the SRA management interface. If no address is configured, the Status line at the bottom of the browser will display an error message when you click the **E-Mail Log** button on the Web Application Firewall > Log page.



To export or email the log, perform the following steps:

**Step 1** To export the log contents, click the **Export** button in the top right corner of the Web Application Firewall > Log page. The File Download dialog box is displayed.



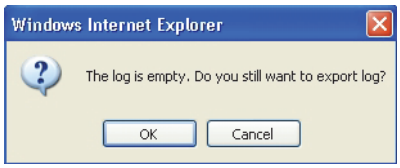

**Step 2** In the File Download dialog box, do one of the following:

- To open the file, click **Open**.
- To save the file, click **Save**, then browse to the folder where you want to save the file and click **Save**.

**Step 3** To email the log contents, click the **E-Mail Log** button in the top right corner of the Web Application Firewall > Log page. The log contents are emailed to the address specified in the Log > Settings page.

## Clearing the Log

You can remove all entries from the Web Application Firewall log on the Web Application Firewall > Log page. The entries on the page are removed, and any attempt to export or email the log file while it is still empty will cause a confirmation dialog box to display.




To clear the Web Application Firewall log, perform the following:

**Step 1** On the top right corner of the Web Application Firewall > Log page, click **Clear**.

**Step 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** tab 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 - Restart appliance may be necessary

  Test the connectivity to **licensemanager.sonicwall.com** from the System > Diagnostics page using the **Ping** and **DNS Lookup** diagnostic utilities to ensure that there is connectivity to the backend server.
- License Manager Failed to resolve host. Check DNS.

  Test the connectivity to **licensemanager.sonicwall.com** from the System > Diagnostics page using the **Ping** and **DNS Lookup** diagnostic utilities to ensure that there is connectivity to the backend server.
- License Manager Peer Identity failed - Check certs and time

  The License Manager server or the signature database server may not have a valid SSL Certificate.
- License Manager Reset called

  The device licenses have been reset. Navigate to the System > Licenses page to activate, upgrade or renew licenses.

**Web Application Firewall > Log and Log > View Messages**

The following messages can be viewed from the Web Application Firewall > Log page and the Log > View page:

- WAF signature database update failed: No signatures were found in the update

  The download for the database update completed, but no suitable signatures were found in the database.
- WAF signature database update failed: Old signature timestamp found in the update

  The timestamp found in the database update from the License Manager is older than what was originally advertised before the download for the update started.
- WAF signature database update failed: Error occurred while processing the update

  There was a general error in downloading and processing the database update. This is possible if the data in the update does not conform to the signature parser schema.
- WAF signature database update failed: Error occurred while downloading the WAF signature database update

  There was a general error in downloading and processing the database update. This is possible if the data in the update does not conform to the signature parser schema.
- WAF signature database update was downloaded successfully. The new database contains <num> rules

  Signature database download was successful. The new database contains <num> number of rules. A rule is an internal property which will be used by Dell SonicWALL to determine how many signatures were downloaded.

**Note** You can select the **Apply Signature Updates Automatically** option on the Web Application Firewall > Settings page to apply new signatures automatically. If this option is not selected, you must click the **Apply** button that appears on the Web Application Firewall > Status page after a successful download. After the database has been successfully applied, all of the signatures within the new database can be found on the Web Application Firewall > Signatures page.

- WAF signature database has been updatesd

  The signature database update was applied after the administrator clicked on the **Apply** button on the Web Application Firewall > Status page.

- WAF engine is being started with the factory default signature database

  The Web Application Firewall engine will be using the factory default signature database for traffic inspection. This may imply that no new signatures were found since the firmware update. If an attempt to download is revealed in the logs earlier, then this message could also imply that the update could not be processed successfully due to database errors and as a precautionary measure the factory default database has been used.

# Chapter 13

# Geo IP and Botnet Filter

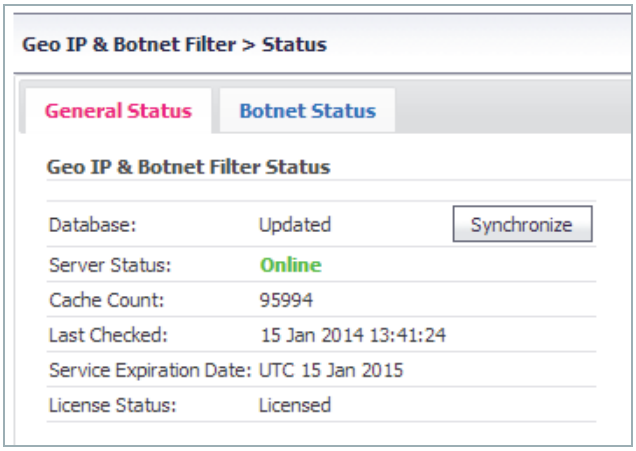
This chapter provides information and configuration tasks specific to the Geo IP and Botnet Filter page on the Dell SonicWALL SRA management interface. The Geo IP feature enables administrators to monitor and enforce policies effectively based on the geographical locations of remote users. The Botnet Filter feature enforces a strong and anti-evasive defense against any rogue activity from Botnets using a dynamically updated database maintained by Dell SonicWALL. Botnets pose huge security risks such as DoS and Data Leakage. They are hard to identify and control due to the transient nature of their origins. These features are disabled by default.

This chapter contains the following sections:


- Status on page 325
- Settings on page 327
- Access Policies on page 329
- Log on page 331
- Licensing on page 334


## Status

The **Geo IP & Botnet Filter > Status** page contains two tabs of information: General Status and Botnet Status.



# General Status

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

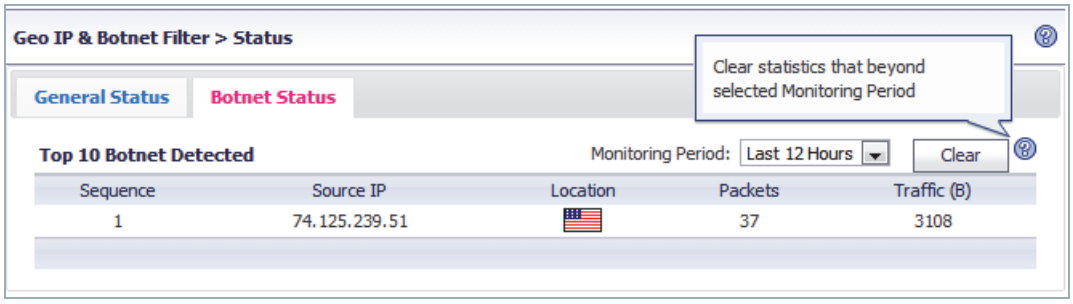
- **Database** shows the update status and provides a **Synchronize** button to manually synchronize updates. When the **Synchronize** button is clicked, the server immediately checks for new updates on the backend server.
- **Server Status** shows whether the backend server is connected. Offline status may indicate the network settings may 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, which includes a free trial that expires one year after the SRA 7.5 release date.

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

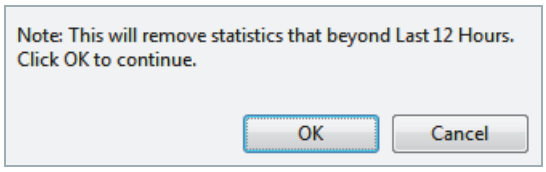
The **Botnet Status** tab shows traffic statistics for Botnet IP addresses for the current reporting period. Statistics are shown for the top 10 IP addresses detected by the Botnet Filter during the selected period.

**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 the **Clear** button to clear statistics that are beyond the selected Monitoring Period. Before clearing, a popup window displays to confirm the clear action:




**Tip** The Clear button 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

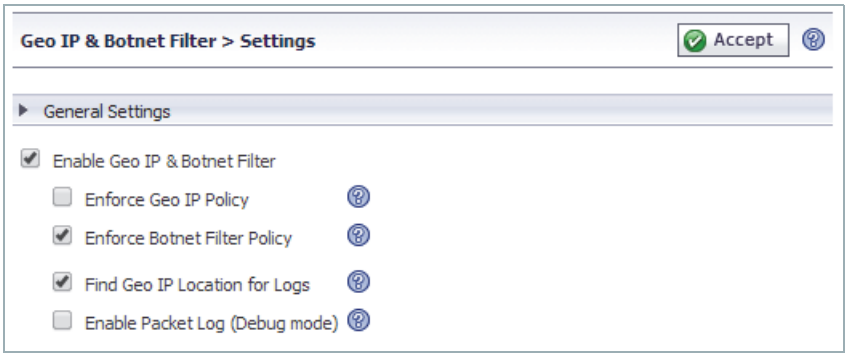
The **Geo IP & Botnet Filter > Settings** page is used to enable/disable the Geo IP and Botnet Filter and configure Remediation Settings. The Geo IP & Botnet Filter > Settings page contains these tabs:

- General Settings on page 327
- Remediation Settings on page 328

## 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, which 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. Check the **Enable Geo IP & Botnet Filter** check box to 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**.

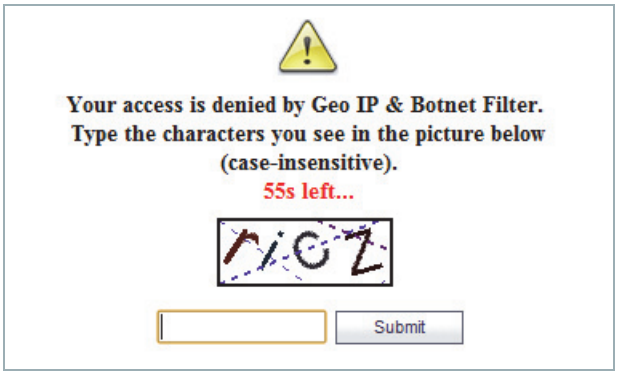
When this feature is enabled, the General Settings section displays four sub-features that can be individually enabled or disabled:

- **Enforce Geo IP Policy** — Select this option to enforce Geo IP polices.
- **Enforce Botnet Filter Policy** — Select this option to enforce Botnet Filter policies. If this is disabled, Botnet IPs will not be blocked, however they will still be 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 will make logs increase rapidly if the log level is set to Debug.

# Remediation Settings

Access to an SRA appliance from aggressive IP addresses are denied directly when Geo IP & Botnet Filter is enabled. Remediation provides valid users an opportunity to process the access from the aggressive IP addresses.

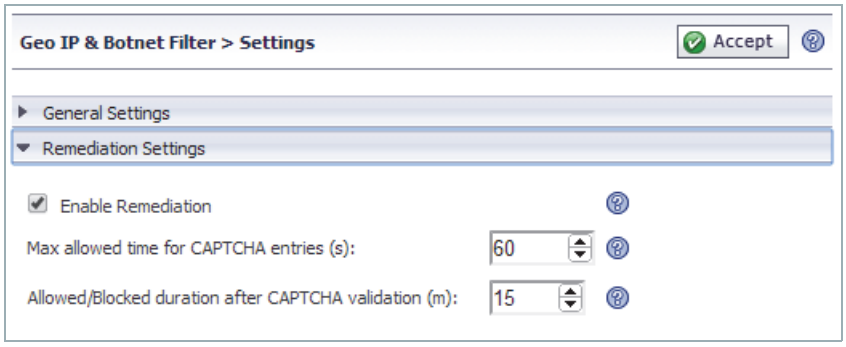
For web access, user are redirected to the CAPTCHA page, as shown below. A countdown timer tells the time that remained for user to perform remediation. The user must finish remediation within limited time, otherwise user IP address is added to the block list and all access from the aggressive IP address is blocked for a period of time.




If remediation is successful within the Verification Time, the user is directed to corresponding page that was requested. 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 goes to expired status. If the user is still in login status, access is not interrupted, but after the user login session is expired the CAPTCHA session is deleted and remediation is required again.

To enable Remediation and configure the settings, perform the following:

**Step 1** Click **Remediation Settings**.



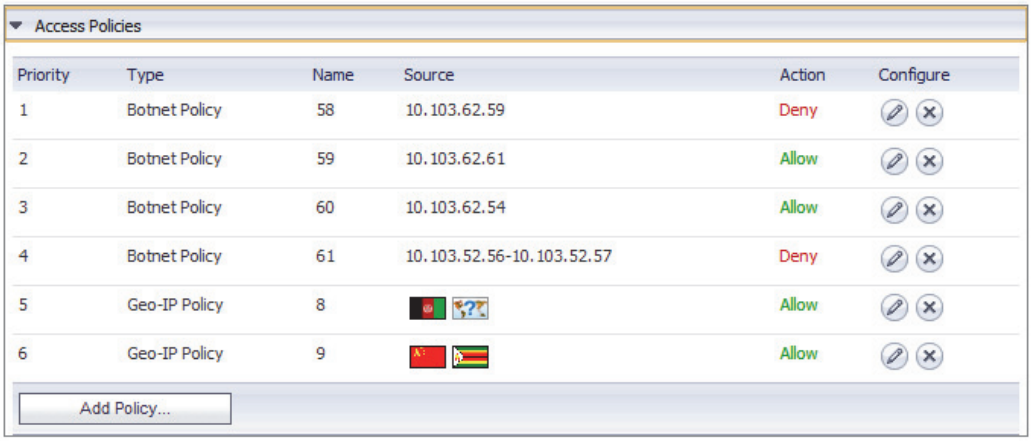

**Step 2** Click the **Enable Remediation** checkbox.

**Step 3** In the **Max allowed time for CAPTCHA entries (s)** field, select the maximum amount of time (in seconds) that the user will have perform Remediation. The minimum/maximum range is 30-300 seconds, with default value for this field being 60 seconds.

**Step 4** In the **Allowed/Blocked duration after CAPTCHA validation (m)** filed, select the duration of time (in minutes) that the user is allowed/blocked after performing the CAPTCHA validation. The minimum value is 5 minutes and the maximum is 30, with the default value being 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 they are listed on the Settings page.

- Botnet Filter policies have a higher priority than Geo IP policies. Geo IP policies are prioritized by 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 polices are enforced first, which means if an IP address is listed in the SonicWALL Botnet Filter database, but admin defines an allow policy for this IP, then access from this IP will be allowed.

A policy can be modified by clicking the button, but a policy name cannot be modified.

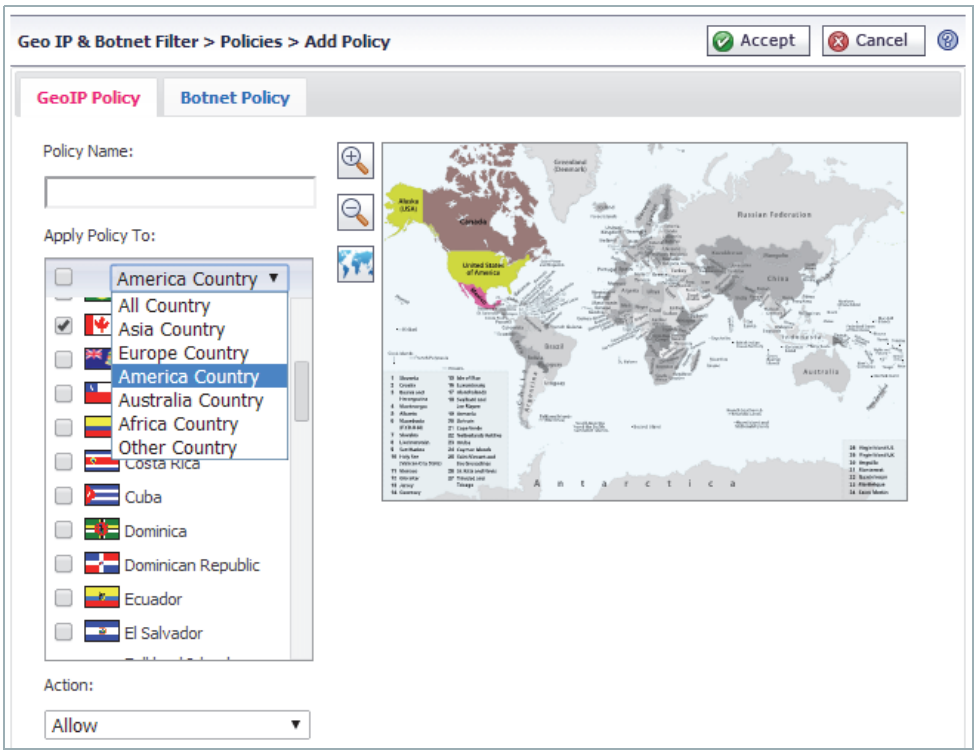
A policy can be deleted by clicking the button.

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, all the countries within that continent will display in the **Apply Policy To** list. You can also select countries directly from the map.

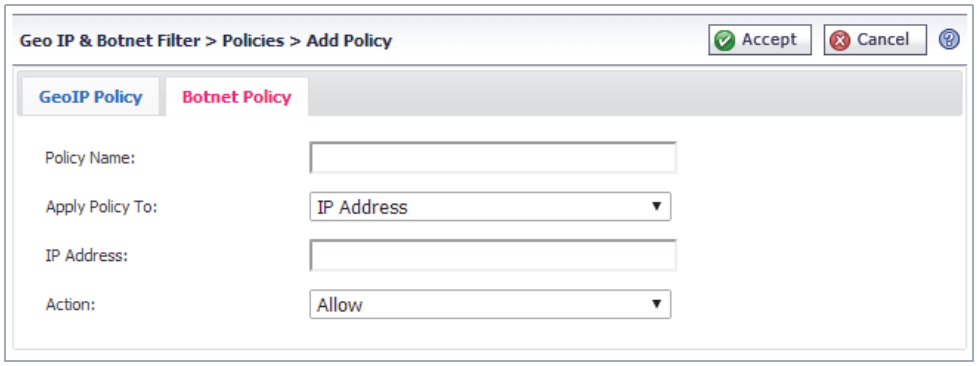
  The map displays selected/unselected countries by color. The unselected countries display gray, while the selected countries display in color. Mouse over a country in the **Apply Policy To** list and the corresponding country will blink on map. Use the Zoom tool to zoom in or out on the map. If you do not wish to use the map, hide it by clicking the Map button.

**Note** If using Internet Explorer 7 or 8, the flash player 10+ will be launched or required installing; otherwise the page displays without 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.

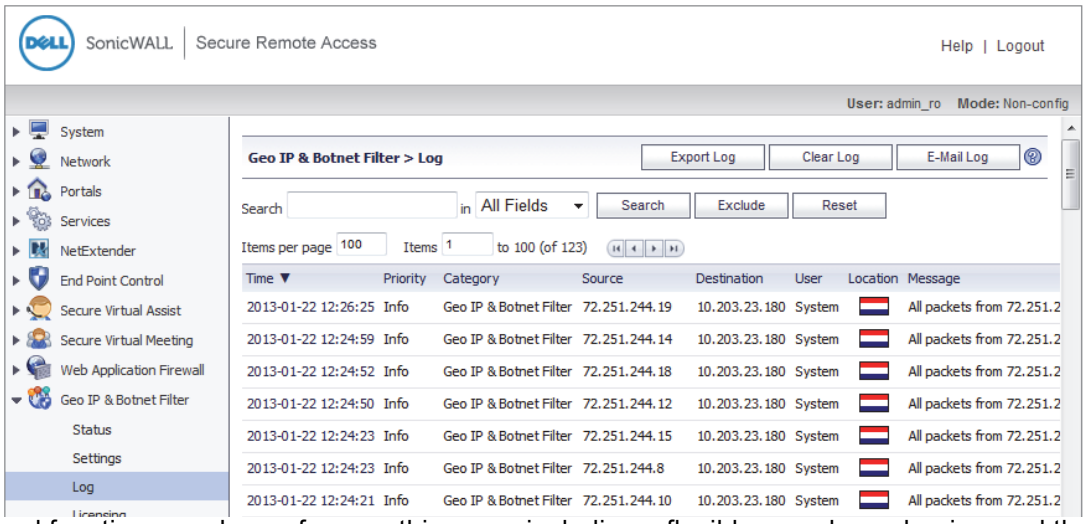



# Log

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 SRA 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 once for each second, no matter if it's denied or allowed.




Several functions can be perform on this page, including a flexible search mechanism and the ability to export the log to a file or email it. Following are instruction for using these functions.

- Clicking on a log entry displays more information about the event, if available.
- Click 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, perform the following steps:

**Step 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.

**Step 2** Select the column in which to search from the drop-down list to the right of the Search field.

**Step 3** Do one of the following:

- To start searching for log entries containing the search value, click **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, perform the following steps:

**Step 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.

**Step 2** To view the log entries beginning at a certain number, type the starting number into the **Item** field and press **Enter** on your keyboard.

**Step 3** To view the first page of log entries, click the left-most button in the arrow control pad.

**Step 4** To view the previous page of log entries, click the left arrow in the arrow control pad.

**Step 5** To view the next page of log entries, click the right arrow in the arrow control pad.

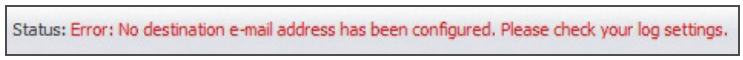
**Step 6** To view the last page of log entries, click the right-most button in the arrow control pad.

## 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.

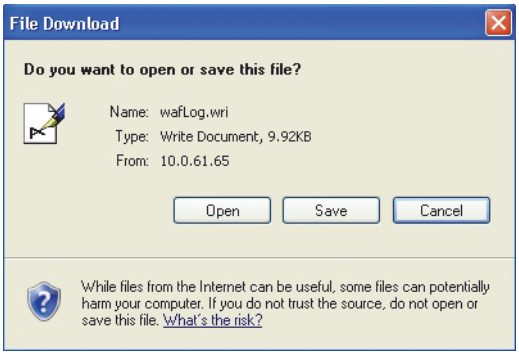
Exported files are saved with a **.wri** file name extension, and open with WordPad, by default.

Emailed files are automatically sent to the address configured on the Log > Settings page of the SSL-VPN management interface. If no address is configured, the Status line at the bottom of the browser will display an error message when you click the **E-Mail Log** button.



To export or email the log, perform the following steps:

**Step 1** To export the log contents, click the **Export** button in the top right corner of the Geo IP & Botnet Filter > Log page. The File Download dialog box is displayed.



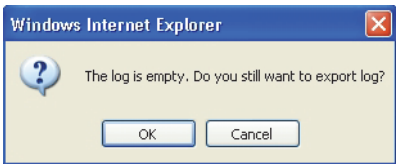

**Step 2** In the File Download dialog box, do one of the following:

- To open the file, click **Open**.
- To save the file, click **Save**, then browse to the folder where you want to save the file and click **Save**.

**Step 3** To email the log contents, click the **E-Mail Log** button in the top right corner of the 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 will cause a confirmation dialog box to display.



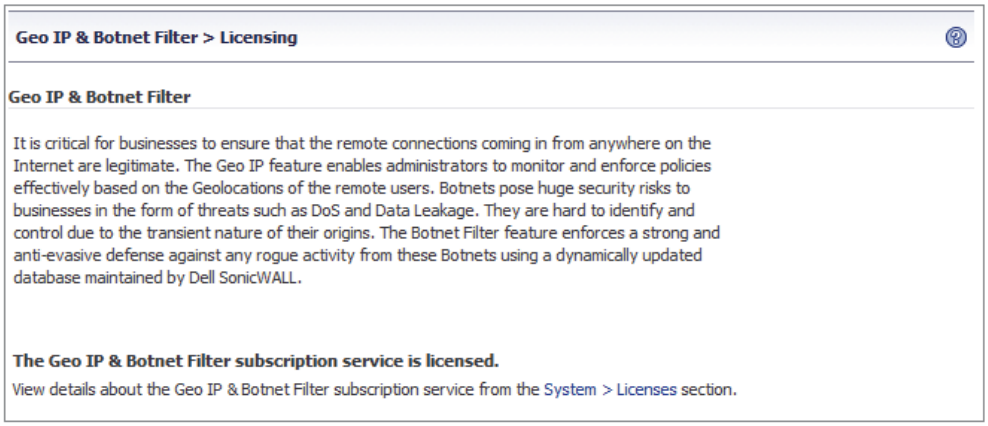

To clear the log, perform the following:

**Step 1** On the top right corner of the Geo IP & Botnet Filter > Log page, click **Clear**.

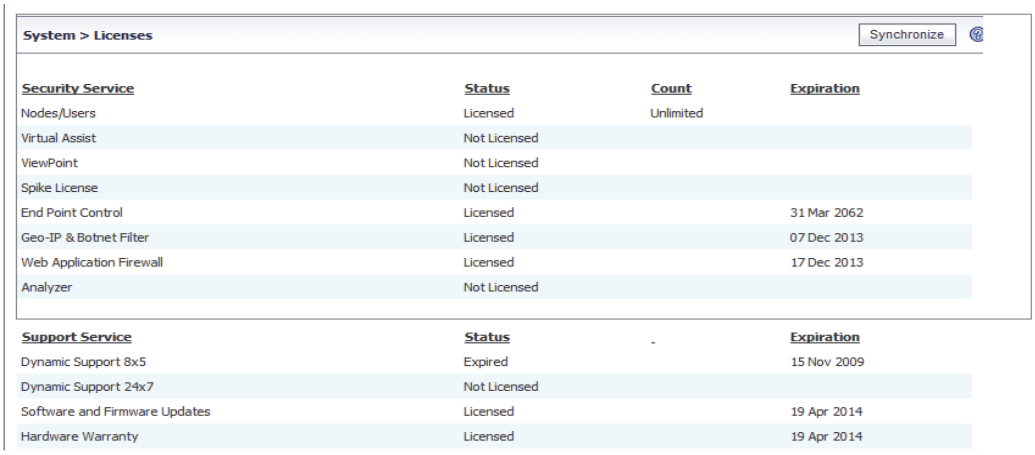
**Step 2** Click **OK** in the confirmation dialog box.

# Licensing

Geo IP & Botnet Filter is a subscription service, which includes a free trial that expires one year after the SRA 7.5 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.



# Chapter 14

# Users Configuration

This chapter provides information and configuration tasks specific to the **Users** pages on the Dell SonicWALL SRA 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 SRA appliance. This chapter contains the following sections:


- Users > Status on page 335
- Users > Local Users on page 337
- Users > Local Groups on page 366
- Global Configuration on page 389

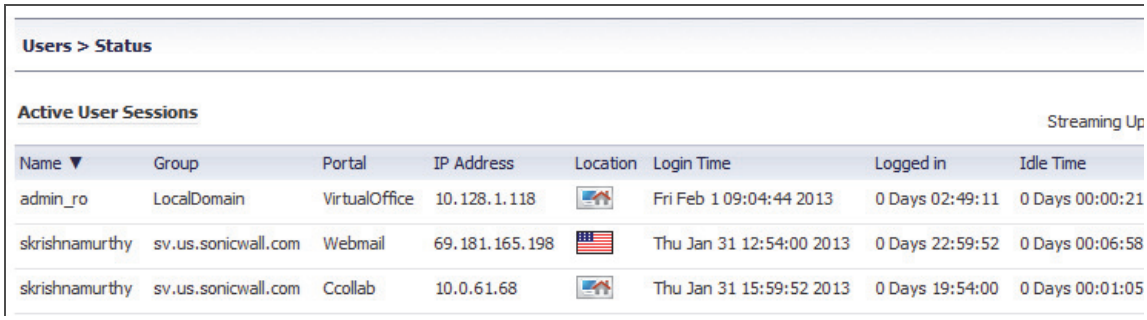

# Users > Status

The **Users > Status** page provides information about users and administrators who are currently logged into the SRA appliance. This section provides general information about how the SRA appliance manages users through a set of hierarchical policies.

This section contains the following sub-sections:


- Access Policies Concepts on page 336
- Access Policy Hierarchy on page 336


***Figure 54 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 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 may terminate a user session and log the user out by clicking the Logout icon at the right of the user row. The **Active User Session** table includes the following information:

***Table 19 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 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 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 SRA appliance. |
| Logout | Displays an icon that enables the administrator to log the user out of the appliance. |

# Access Policies Concepts

The Dell SonicWALL SRA Web-based management interface provides granular control of access to the SRA appliance. Access policies provide different levels of access to the various network resources that are accessible using the 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 SRA services. Certain policies take precedence.

The Dell SonicWALL SRA 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, which resolves to 10.0.1.3.

Assuming that no conflicting user or group policies have been configured, if a user attempted to access:

- An FTP server at 10.0.0.1, the user would be blocked by Policy 1
- An FTP server at 10.0.1.5, the user would be blocked by Policy 2
- An FTP server at 10.0.0.10, the user would be granted access by Policy 3. The IP address range 10.0.0.5 - 10.0.0.20 is more specific than the IP address range defined in Policy 1.
- An FTP server at ftp.company.com, the user would be granted access by Policy 3. A single host name is more specific than the IP address range configured in Policy 2.

**Note** In this example, the user would not be able to access ftp.company.com using its IP address 10.0.1.3. The SRA 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

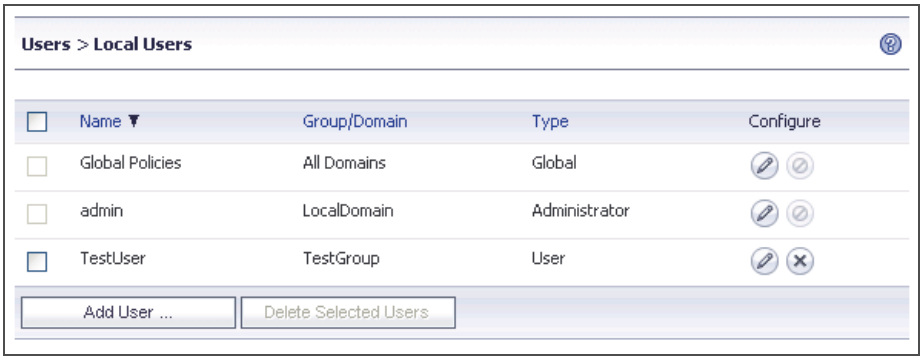
This section provides an overview of the **Users > Local Users** page and a description of the configuration tasks available on this page.


- Users > Local Users Overview on page 337
- Removing a User on page 338
- Adding a Local User on page 338
- Editing User Settings on page 340


For global configuration settings, see Global Configuration on page 389.

## Users > Local Users Overview

The **Users > Local Users** page allows the administrator to add and configure users.



## Local Users

The Local Users section 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, NT Domain or Active Directory authentication do not require passwords because the external authentication server will validate user names and passwords.

**Tip** When a user is authenticated using RADIUS and Active Directory, an External User within the Local User database is created, however, the administrator will not be able to change the group for this user. If you want to specify different policies for different user groups when using RADIUS or Active Directory, the administrator will need to create the user manually in the Local User database.

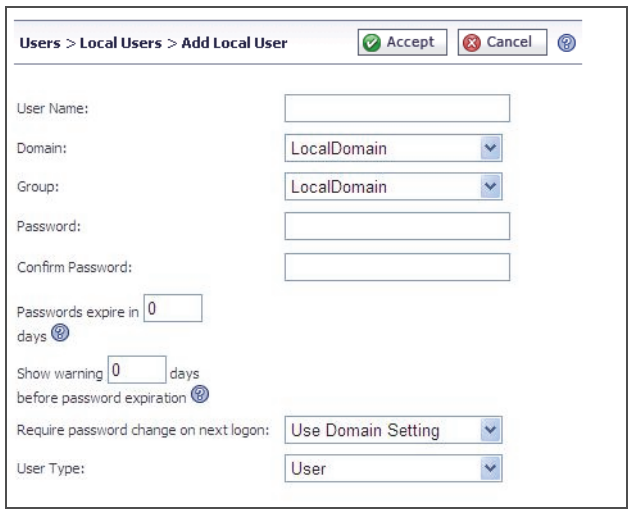
# Removing a User

To remove a user, navigate to **Users > Local Users** and click the delete icon next to the name of the user that you wish to remove. Once deleted, the user will be removed from the **Local Users** window.

# Adding a Local User

To create a new local user, perform the following steps:

**Step 1** Navigate to the **Users** > **Local Users** page and click **Add User**. The **Add Local User** window is displayed.




**Step 2** In the **Add Local User** window, enter the username for the user in the **User Name** field. This will be the name the user will enter in order to log into the SRA user portal.

**Step 3** Select the name of the domain to which the user belongs in the **Domain** drop-down list.

**Step 4** Select the name of the group to which the user belongs in the **Group** drop-down list.

**Step 5** Type the user password in the **Password** field.

**Step 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.

**Step 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.

**Step 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 will expire. Notifications also include a link to a screen where the password can be changed.

**Step 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.

**Step 10** 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, NT Domain or LDAP, then the **Add User** window will close and the new user will be added to the **Local Users** list.

**Step 11** Click **Accept** to update the configuration. Once the user has been added, the new user will be displayed on the **Local Users** window.

**Note** Entering RADIUS, LDAP, NT and Active Directory user names is only necessary if you wish to define specific policies or bookmarks per user. If users are not defined in the SRA appliance, then global policies and bookmarks will apply to users authenticating to an external authentication server. When working with external (non-LocalDomain) users, a local user entity must exist so that any user-created (personal) bookmarks can be stored within the SRA configuration files. Bookmarks must be stored on the SRA appliance because LDAP, RADIUS, and NT Authentication external domains do not provide a direct facility to store such information as bookmarks. Rather than requiring administrators to manually create local users for external domain users wishing to use personal bookmarks, the SRA appliance will automatically create a corresponding local user entity when an external domain user creates a personal bookmark so that it may store the bookmark information.

# 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 tabs as described in the following table:

| Tab | Description |
|---|---|
| General | Enables you to create a password and an inactivity timeout, and specify Single Sign-On settings for automatic login to bookmarks for this user. |
| 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. |
| Nx Settings | Enables you to specify a NetExtender client address range, including for IPv6, and to configure client settings. |
| Nx 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. |
| 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 will not be shown. The password field is not configurable because the authentication server validates the password. The user type is not configurable because the SRA appliance only allows users that authenticate to the internal user database to have administrative privileges. Also, the user type **External** will be used to identify the local user instances that are auto-created to correspond to externally authenticating users.

See the following sections for a description of the configuration options on each tab of the **Edit User Settings** window:


- Modifying General User Settings on page 340
- Modifying Group Settings on page 342
- Modifying Portal Settings on page 343
- Modifying User NetExtender Settings on page 344
- Modifying NetExtender Client Routes on page 346
- Adding User Policies on page 346
- Adding or Editing User Bookmarks on page 352
- Configuring Login Policies on page 364


## Modifying General User Settings

The **General** tab provides configuration options for a user's password, inactivity timeout value, and bookmark single sign-on (SSO) control. Table 20 The following table provides detailed information about application-specific support of SSO, global/group/user policies and bookmark policies.

*Table 20 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) | No | Yes | Yes |
| Virtual Network Computing (VNC - HTML5) | No | Yes | Yes |
| File Transfer Protocol (FTP) | Yes | Yes | Yes |
| Telnet | No | 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 |

Single sign-on (SSO) in the SRA appliance supports the following applications:

- RDP - Active X
- RDP - Java
- RDP - HTML5
- FTP
- HTTP
- HTTPS
- CIFS

**Note** SSO cannot be used in tandem with two-factor authentication methods.

To modify general user settings, perform the following tasks:

**Step 1** In the left-hand column, navigate to the **Users** > **Local Users**.

**Step 2** Click the configure icon next to the user you want to configure. The **General** tab of the **Edit User Settings** window displays. The **General** tab displays the following non-configurable fields: **User Name**, **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 338 and add the user again.

**Step 3** To set or change the user password, type the password in the **Password** field. Re-type it in the **Confirm Password** field.

**Step 4** 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 the **Change password at next logon** check box.

**Note** A specific local domain user can be forced to change their password. Use the General tab on the Users > Local Users > Edit page.

**Step 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 will expire. Notifications also include a link to a screen where the password can be changed.

**Step 6** To set the inactivity timeout for the user, meaning that they will be signed out of the Virtual Office after the specified time period, enter the number of minutes of inactivity to allow in the **Inactivity Timeout** field. The timeout value also controls the number of minutes that a one-time password remains valid, when One Time Passwords are configured for a user.

The inactivity timeout can be set at the user, group and global level. If one or more timeouts are configured for an individual user, the user timeout setting will take precedence over the group timeout and the group timeout will take precedence over the global timeout. Setting the global settings timeout to 0 disables the inactivity timeout for users that do not have a group or user timeout configured.

**Step 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.

**Step 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.

**Step 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 may be expecting the username to be prefixed by the domain name. In this instance, SSO will fail and the user will have to login with the domain-prefixed username. In some instances, a default domain name can be configured at the server to allow SSO to succeed.

**Step 10** Click **Accept** to save the configuration changes

## Modifying Group Settings

On the **Groups** tab, 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 SRA 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 SRA group membership automatically changes to match the external group membership.

To configure settings on the **Groups** tab:

**Step 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.

**Step 2** To add a group of which users will be a member, click **Add Group**. The group must be already configured from Users > Local Groups.

**Step 3** Select the desired group from the drop-down list.

**Step 4** Select the **Make primary group** check box to make this the primary group membership for users.

**Step 5** Click **Add Group** to add the selected group to the **Group Memberships** list.

**Step 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.

**Step 7** Click **Accept**.

## Modifying Portal Settings

The **Portal** tab provides configuration options for portal settings for this user.

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

**Step 1** On the **Portal** tab under **Portal Settings**, select one of the following portal settings for this user:

- **Use group setting** – The setting defined in the group to which this user belongs will be used to determine if the portal feature is enabled or disabled. Group settings are defined by configuring the group in the Users > Local Groups page.
- **Enabled** – Enable this portal feature for this user.
- **Disabled** – Disable this portal feature for this user.

You can configure one of the above settings for each of the following portal features:

- **NetExtender** – 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.

**Step 2** Click **Accept**.

## Modifying User NetExtender Settings

This feature is for external users, who will inherit the settings from their assigned group upon login. NetExtender client settings can be specified for the user, or use the group settings. For information about configuring group settings, see Editing Group Settings on page 368.

To enable NetExtender ranges and configure Static client settings for a user, perform the following steps:

**Step 1** Navigate to **Users > Local Users**.

**Step 2** Click the configure icon next to the user you want to configure.

**Step 3** In the **Edit Local User** page, select the **NxSettings** tab.

3. Under **NetExtender Client Address Range**, select **Use Static Pool** from the drop down list.
4. Supply a beginning client IPv4 address in the **Client Address Range Begin** field.
5. Supply an ending client IPv4 address in the **Client Address Range End** field.
6. Under **NetExtender Client IPv6 Address Range**, optionally select **Use Static Pool** from the drop down list.
7. Supply a beginning client IPv6 address in the **Client Address Range Begin** field.
8. If using IPv6, supply an ending client IPv6 address in the **Client Address Range End** field.

**Step 4** Under **NetExtender 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 368.
- **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.

**Step 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 368.
- **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.

**Step 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 368.
- **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.

**Step 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 368.
- **Allow saving of user name only** - Allow caching of the user name. The user will only need 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 will be 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 will be required to enter both user name and password when starting NetExtender. Overrides the group setting.

**Step 8** 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 215 for more information.

**Step 9** Click **Accept**.

To enable NetExtender ranges and configure DHCP client settings for a user, perform the following steps:

---

**Step 1** Navigate to **Users > Local Users**.

**Step 2** Click the configure icon next to the user you want to configure.

**Step 3** In the **Edit Local User** page, select the **NxSettings** tab.

**9.** Under **NetExtender Client Address Range**, select **Use DHCP** from the drop down list.

**10.** Under **Select Interface**, use the drop down list to select the interface to use for DHCP.

**11.** Supply the **DHCP Server** in the field provided.

**12.** Under **NetExtender Client IPv6 Address Range**, optionally select **Use DHCP** from the drop down list.

**13.** Under **Select Interface**, use the drop down list to select the interface to use for DHCPv6.

**14.** Supply the **DHCPv6 Server** in the field provided.

**Step 4** Under **NetExtender 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 368.
- **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.

**Step 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 368.
- **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.

**Step 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 368.
- **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.

**Step 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 368.
- **Allow saving of user name only** - Allow caching of the user name. The user will only need 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 will be 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 will be required to enter both user name and password when starting NetExtender. Overrides the group setting.

**Step 8** 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 215 for more information.

**Step 9** Click **Accept**.

## Modifying NetExtender Client Routes

The **Nx Routes** tab provides configuration options for NetExtender client routes. For procedures on modifying NetExtender client route settings, see NetExtender > Client Routes on page 219.

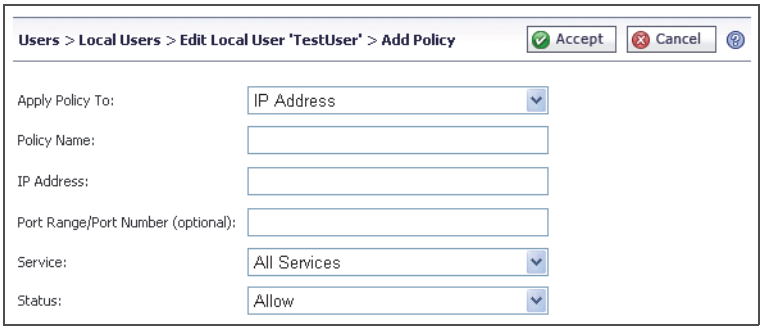
## Adding User Policies

The **Policies** tab 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, perform the following steps:

**Step 1** On the **Policies** tab, click **Add Policy**. The **Add Policy** window is displayed.




**Step 2** In the **Apply Policy To** drop-down list, select whether the policy will be applied to an individual host, a range of addresses, all addresses, a network object, a server path, or a URL object. 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 SRA policies apply to the destination address(es) of the SRA connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the 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 364.

- **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 348.

- **IP Address Range** - If your policy applies to a range of addresses, enter the beginning IP address in the **IP Network Address** field and the subnet mask that defines the IP address range in the **Subnet Mask** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field. See Adding a Policy for an IP Address Range on page 348.
- **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 348.
- **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 137
- **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 348.
- **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 350.
- **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 351.
- **IPv6 Address Range** - If your policy applies to a range of addresses, enter the beginning IPv6 address in the **IPv6 Network Address** field and the prefix that defines the IPv6 address range in the **IPv6 Prefix** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field. See Adding a Policy for an IPv6 Address Range on page 352.
- **All IPv6 Address** - If your policy applies to all IPv6 addresses, you do not need to enter any IP address information. See Adding a Policy for All IPv6 Addresses on page 352.

**Step 3** Select the service type in the **Service** drop-down list. If you are applying a policy to a network object, the service type is defined in the network object.

**Step 4** Select **Allow** or **Deny** from the **Status** drop-down list to either permit or deny SRA connections for the specified service and host machine.

When using Citrix bookmarks, in order to restrict proxy access to a host, a **Deny** rule must be configured for both Citrix and HTTP services.

**Step 5** Click **Accept** to update the configuration. Once the configuration has been updated, the new policy will be 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

**Step 1** Navigate to **Users > Local Users**.

**Step 2** Click the configure icon next to the user you want to configure.

**Step 3** Select the **Policies** tab.

**Step 4** Click **Add Policy...**

**Step 5** In the **Apply Policy to** field, click the IP Address option.

**Step 6** Define a name for the policy in the **Policy Name** field.

**Step 7** Type an IP address in the **IP Address** field.

**Step 8** In the **Port Range/Port Number** field, optionally enter a port range or an individual port.

**Step 9** In the **Service** drop-down list, click on a service object.

**Step 10** In the **Status** drop-down list, click on an access action, either **Allow** or **Deny**.

**Step 11** Click **Accept**.

### Adding a Policy for an IP Address Range

**Step 1** In the **Apply Policy to** field, click the IP Address Range option.

**Step 2** Define a name for the policy in the **Policy Name** field.

**Step 3** Type a starting IP address in the **IP Network Address** field.

**Step 4** Type a subnet mask value in the **Subnet Mask** field in the form 255.255.255.0.

**Step 5** In the **Port Range/Port Number** field, optionally enter a port range or an individual port.

**Step 6** In the **Service** drop-down list, click on a service option.

**Step 7** In the **Status** drop-down list, click on an access action, either **Allow** or **Deny**.

**Step 8** Click **Accept**.

### Adding a Policy for All Addresses

**Step 1** In the **Apply Policy to** field, select the **All Addresses** option.

**Step 2** Define a name for the policy in the **Policy Name** field.

**Step 3** The **IP Address Range** field is read-only, specifying All IP Addresses.

**Step 4** In the **Service** drop-down list, click on a service option.

**Step 5** In the **Status** drop-down list, click on an access action, either **Allow** or **Deny**.

**Step 6** Click **Accept**.

### Setting File Shares Access Policies

To set file share access policies, perform the following steps:

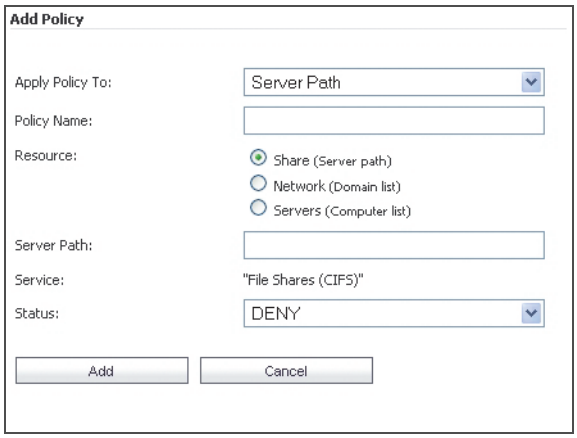
**Step 1** Navigate to **Users > Local Users**.

**Step 2** Click the configure icon next to the user you want to configure.

**Step 3** Select the **Policies** tab.

**Step 4** Click **Add Policy**.

**Step 5** Select **Server Path** from the **Apply Policy To** drop-down list.




**Step 6** Type a name for the policy in the **Policy Name** field.

**Step 7** Select the **Share** radio button in the **Resource** field.

**Step 8** Type the server path in the **Server Path** field.

**Step 9** From the **Status** drop-down list, select **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 349.

**Step 10** Click **Accept**.

## Adding a Policy for a File Share

To add a file share access policy, perform the following steps:

**Step 1** Navigate to **Users > Local Users**.

**Step 2** Click the configure icon next to the user you want to configure.

**Step 3** Select the **Policies** tab.

**Step 4** Click **Add Policy...**

**Step 5** Select **Server Path** from the **Apply Policy To** drop-down list.

**Step 6** Type a name for the policy in the **Policy Name** field.

**Step 7** In the **Server Path** field, enter the server path in the format *servername/share/path* or *servername\share\path*. The prefixes \\, //, \ and / are acceptable.

**Note** Share and path provide more granular control over a policy. Both are optional.

**Step 8** Select **Allow** or **Deny** from the **Status** drop-down list.

**Step 9** Click **Accept**.

### Adding a Policy for a URL Object

To create object-based HTTP or HTTPS user policies, perform the following steps:

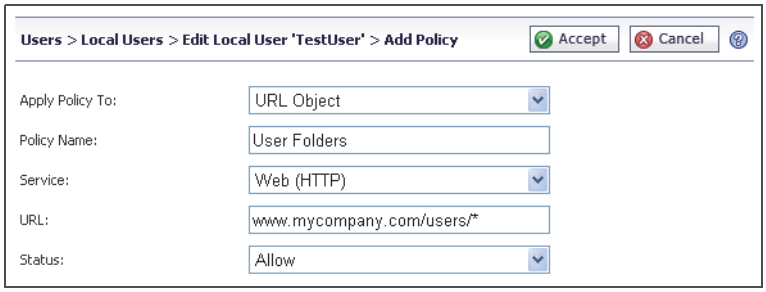
**Step 1** Navigate to **Users > Local Users**.

**Step 2** Click the configure icon next to the user you want to configure.

**Step 3** Select the **Policies** tab.

**Step 4** Click **Add Policy**.

**Step 5** In the **Apply Policy To** drop-down menu, select the **URL Object** option.




**Step 6** Define a name for the policy in the **Policy Name** field.

**Step 7** In the **Service** drop-down list, choose either **Web (HTTP)** or **Secure Web (HTTPS)**.

**Step 8** In the **URL** field, add the URL string to be enforced in this policy.

**Note** In addition to standard URL elements, the administrator may enter port, path and wildcard elements to the URL field. For more information on using these additional elements, see Policy URL Object Field Elements on page 351.

If a path is specified, the URL policy is recursive and applies to all subdirectories. If, for example “www.mycompany.com/users/*” is specified, the user is permitted access to any folder or file under the “www.mycompany.com/users/” folder.

**Step 9** In the **Status** drop-down list, click on an access action, either **Allow** or **Deny**.

**Step 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 may enter port, path and wildcard elements to this field. The following chart provides an overview of standard URL field elements:

| Element | Usage |
|---|---|
| Host | Can be a hostname that should be resolved or an IP address. Host information has to be present. |
| Port | If port is not mentioned, then all ports for that host are matched. Specify a specific port or port range using digits [0-9], and/or wildcard elements. Zero “0” must not be used as the first digit in this field. The least possible number matching the wildcard expression should fall within the range of valid port numbers i.e. [1-65535]. |
| Path | This is the file path of the URL along with the query string. A URL Path is made of parts delimited by the file path separator ‘/’. Each part may contain wildcard characters. The scope of the wildcard characters is limited only to the specific part contained between file path separators. |
| Usernames | %USERNAME% is a variable that matches the username appearing in a URL requested by a user with a valid session. Especially useful if the policy is a group or a global policy. |
| Wildcard Characters | The following wildcard characters are used to match one or more characters within a port or path specification.<br>***** – Matches one or more characters in that position.<br>**^** – Matches exactly one character in the position.<br>**[!<character set>]** – Matches any character in that position not listed in character set. E.g. **[!acd]**, **[!8a0]**<br>**[<range>]** – Matches any character falling within the specified ASCII range. Can be an alphanumeric character. E.g.) **[a-d]**, **[3-5]**, **[H-X]** |

**Note** Entries in the URL field can not contain (“http://”, “https://”) elements. Entries can also not contain fragment delimiters such as “#”.

### Adding a Policy for an IPv6 Address

To add a policy for an IPv6 address, perform the following steps:

**Step 1** Navigate to **Users > Local Users**.

**Step 2** Click the configure icon next to the user you want to configure.

**Step 3** Select the **Policies** tab.

**Step 4** Click **Add Policy...**

**Step 5** In the **Apply Policy To** field, click the **IPv6 Address** option.

**Step 6** Define a name for the policy in the **Policy Name** field.

**Step 7** Type an IPv6 address in the **IPv6 Address** field in the form 2001::1:2:3:4.

**Step 8** In the **Port Range/Port Number** field, optionally enter a port range or an individual port.

**Step 9** In the **Service** drop-down list, click on a service object.

**Step 10** In the **Status** drop-down list, click on an access action, either **Allow** or **Deny**.

**Step 11** Click **Accept**.

### Adding a Policy for an IPv6 Address Range

To add a policy for an IPv6 address range, perform the following steps:

**Step 1** In the **Apply Policy To** field, click the **IPv6 Address Range** option.

**Step 2** Define a name for the policy in the **Policy Name** field.

**Step 3** Type a starting IPv6 address in the **IPv6 Network Address** field.

**Step 4** Type a prefix value in the **IPv6 Prefix** field, such as 64 or 112.

**Step 5** In the **Port Range/Port Number** field, optionally enter a port range or an individual port.

**Step 6** In the **Service** drop-down list, click on a service option.

**Step 7** In the **Status** drop-down list, click on an access action, either **Allow** or **Deny**.

**Step 8** Click **Accept**.

### Adding a Policy for All IPv6 Addresses

To add a policy for all IPv6 addresses, perform the following steps:

**Step 1** In the **Apply Policy To** field, select the **All IPv6 Address** option.

**Step 2** Define a name for the policy in the **Policy Name** field.

**Step 3** The **IPv6 Address Range** field is read-only, specifying all IPv6 addresses.

**Step 4** In the **Service** drop-down list, click on a service option.

**Step 5** In the **Status** drop-down list, click on an access action, either **Allow** or **Deny**.

**Step 6** Click **Accept**.

## Adding or Editing User Bookmarks

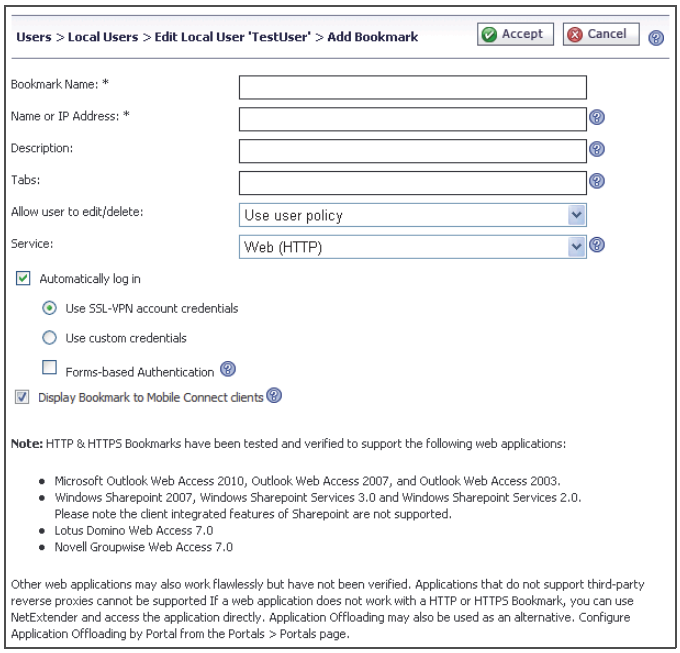
The **Bookmarks** tab provides configuration options to add and edit user bookmarks. In addition to the main procedure below, see the following:

- Creating a Citrix Bookmark for a Local User on page 361
- Creating Bookmarks with Custom SSO Credentials on page 362

To define user bookmarks, perform the following steps:

**Step 1** In the E**dit User Settings** window, click the **Bookmarks** tab.

**Step 2** Click **Add Bookmark**. The **Add Bookmark** window displays.




When user bookmarks are defined, the user will see the defined bookmarks from the SRA Virtual Office home page.

**Step 1** Type a descriptive name for the bookmark in the **Bookmark Name** field.

**Step 2** Enter the fully qualified domain name (FQDN) or the IPv4 or 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 Table 21the following table.

***Table 21 Bookmark Name or IP Address Formats by Service Type***

| Service Type | Format | Example for Name or IP Address Field |
|---|---|---|
| RDP - ActiveX<br>RDP - Java<br>RDP - HTML5 | IP Address<br>IPv6 Address<br>IP:Port (non-standard)<br>FQDN<br>Host name | 10.20.30.4<br>2008::1:2:3:4<br>10.20.30.4:6818<br>JBJONES-PC.sv.us.sonicwall.com<br>JBJONES-PC |
| VNC<br>VNC - HTML5 | IP Address<br>IPv6 Address<br>IP:Port (mapped to session)<br>FQDN<br>Host name<br>**Note**: Do not use session or display number instead of port. | 10.20.30.4<br>2008::1:2:3:4<br>10.20.30.4:5901 (mapped to session 1)<br>JBJONES-PC.sv.us.sonicwall.com<br>JBJONES-PC<br>**Note**: Do not use 10.20.30.4:1<br>**Tip**: For a bookmark to a Linux server, see the Tip below this table. |
| FTP | IP Address<br>IPv6 Address<br>IP:Port (non-standard)<br>FQDN<br>Host name | 10.20.30.4<br>2008::1:2:3:4<br>10.20.30.4:6818 or [2008::1:2:3:4]:6818<br>JBJONES-PC.sv.us.sonicwall.com<br>JBJONES-PC |
| Telnet | IP Address<br>IPv6 Address<br>IP:Port (non-standard)<br>FQDN<br>Host name | 10.20.30.4<br>2008::1:2:3:4<br>10.20.30.4:6818 or [2008::1:2:3:4]:6818<br>JBJONES-PC.sv.us.sonicwall.com<br>JBJONES-PC |
| SSHv1<br>SSHv2 | IP Address<br>IPv6 Address<br>IP:Port (non-standard)<br>FQDN<br>Host name | 10.20.30.4<br>2008::1:2:3:4<br>10.20.30.4:6818 or [2008::1:2:3:4]:6818<br>JBJONES-PC.sv.us.sonicwall.com<br>JBJONES-PC |
| HTTP<br>HTTPS | URL<br>IP Address of URL<br>IPv6 Address<br>URL:Path or File<br>IP:Path or File<br>URL:Port<br>IP:Port<br>URL:Port:Path or File<br>IP:Port:Path or File | www.sonicwall.com<br>204.212.170.11<br>2008::1:2:3:4<br>www.sonicwall.com/index.html<br>204.212.170.11/folder/<br>www.sonicwall.com:8080<br>204.212.170.11:8080 or [2008::1:2:3:4]:8080<br>www.sonicwall.com:8080/folder/index.html<br>204.212.170.11:8080/index.html |

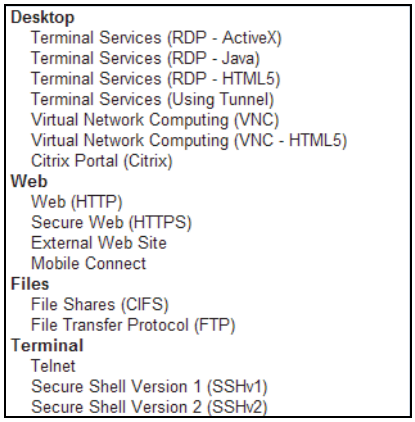
| Service Type | Format | Example for Name or IP Address Field |
|---|---|---|
| File Shares | Host\Folder\<br>Host\File<br>FQDN\Folder<br>FQDN\File<br>IP\Folder\<br>IP\File | server-3\sharedfolder\<br>server-3\inventory.xls<br>server-3.company.net\sharedfolder\<br>server-3company.net\inventory.xls<br>10.20.30.4\sharedfolder\<br>10.20.30.4\status.doc<br>**Note**: Use backslashes even on Linux or Mac computers; these use the Windows API for file sharing. |
| Citrix<br>(Citrix Web Interface) | IP Address<br>IPv6 Address<br>IP:Port<br>IP:Path or File<br>IP:Port:Path or File<br>FQDN<br>URL:Path or File<br>URL:Port<br>URL:Port:Path or File<br>**Note**: *Port* refers to the HTTP(S) port of Citrix Web Interface, not to the Citrix client port. | 172.55.44.3<br>2008::1:2:3:4<br>172.55.44.3:8080 or [2008::1:2:3:4]:8080<br>172.55.44.3/folder/file.html<br>172.55.44.3:8080/report.pdf<br>www.citrixhost.company.net<br>www.citrixhost.net/folder/<br>www.citrixhost.company.com:8080<br>www.citrixhost.com:8080/folder/index.html |

When creating a **Virtual Network Computing (VNC)** bookmark to a Linux server, you must specify the port number and server number in addition to the Linux server IP the **Name or IP Address** field in the form of **ipaddress:port:server**. For example, if the Linux server IP address is 192.168.2.2, the port number is 5901, and the server number is 1, the value for the **Name or IP Address** field would be **192.168.2.2:5901:1**.

**Step 3** Optionally, you can enter a friendly description to be displayed in the bookmark table by filling in the **Description** field.

**Step 4** Set whether users are can edit or delete bookmarks from the Virtual Office portal by making a selection for **Allow user to edit/delete**. You can select to **Allow**, **Deny**, or to **Use the user policy** setting.

**Step 5** 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 may appear. Use the following information for the chosen service to complete the building of the bookmark:

**Terminal Services (RDP - ActiveX)**, **Terminal Services (RDP - Java)**, or **Terminal Services (RDP - HTML5)**

**Note** If you create a bookmark using the **Terminal Services (RDP - ActiveX)** service type, then when you click on that bookmark while using a browser other than Internet Explorer, the service is automatically switched to **Terminal Services (RDP - Java)**. A popup window notifies you of the switch.

- In the **Screen Size** drop-down list, select the default terminal services screen size to be used when users execute this bookmark. *(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 may want to provide a path to where your application resides on your remote computer by typing the path in the **Application Path** field.

- In the **Colors** drop-down list, select the default color depth for the terminal service screen when users execute this bookmark. *(Option available for all Terminal Services.)*
- Select the **Enable wake-on-LAN** check box 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 the **Send WOL packet to host name or IP address** check box, which 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. *(Option available for ActiveX or Java only.)*
- 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 the **Login as console/admin session** check box 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** checkbox if users are connecting to a TS Farm or Load Balanced server. By default, the bookmark only connects to the provided name and IP address. If you enable this feature, the SRA appliance will obtain the redirected address and connect the user to the correct server. Note that Interactive Login may need to be disabled for this feature to work properly. *(Option is available for ActiveX or Java only.)*
  - For *RDP - HTML5* bookmarks, you will have the option to list the TS Farm servers. If a list is provided, the client is redirected and connected to the servers in the list. If no list is provided, any server will be connected.

– For *RDP - Java* bookmarks, select the **Force Java Client Usage** check box to force the use of the Java RDP client rather than the locally installed RDP client if it exists. If this option is selected, no Windows Advanced options are supported.

– For Windows clients or on Mac clients running Mac OS X 10.5 or above with RDC installed, expand **Show advanced Windows options** and select the check boxes for to redirect the following features on the local network for use in this bookmark: (*Options available for ActiveX or Java only)*

  - **Redirect Printers**
  - **Redirect Ports**
  - **Redirect Drives**
  - **Redirect Ports**
  - **Redirect SmartCards**
  - **Redirect Clipboard**
  - **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**
  - **Auto-reconnection**
  - **Desktop background**
  - **Bitmap caching**
  - **Menu/window animation**
  - **Visual styles**
  - **Show window contents while dragging/resizing**.
  - **Remote Audio -** This drop down list allows you to select **Play on this computer**, **Play on remote computer**, or **Do not play**.

**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**
  - **Visual Styles**
  - **Show window contents while dragging/resizing**
  - **Enable Compression**

– If the client application will be RDP6 for *RDP - ActiveX or Java*, you can select any of the following options:

  - **Dual monitors**
  - **Font smoothing**
  - **Desktop composition**

- **Remote Application - Remote Application** monitors server and client connection activity; to use it, you need to register remote applications in the Windows 2008 RemoteApp list. If **Remote Application** is selected, the Java Console will display messages regarding connectivity with the Terminal Server.
- **Spam Monitors**
- **Desktop Composition**

– If the client application will be RDP6 for *RDP - HTML5*, you can select the **Font Smoothing** option.

– Select the **Connection Speed** from the drop down list for optimized performance. (*Option available for all Terminal Services.*)

– Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current SRA session for login 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 may 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 362.

– Select the **Display Bookmark to Mobile Connect clients** check box to display the bookmark on mobile devices. *(Option available for all Terminal Services.)*

**Virtual Network Computing (VNC)**

– 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** if the user will not be making any changes on the remote system.
- Select **Share Desktop** to allow multiple users to view and use the same VNC desktop.
- Check the **Display Bookmark to Mobile Connect clients** check box to display the bookmark on mobile devices.

**Virtual Network Computing (VNC - HTML5)**

- Select the **View Only** check box to disable keyboard and mouse events in the desktop window.
- Select the **Share Desktop** check box to enable desktop sharing between clients.
- Select the **Display Bookmark to Mobile Connect clients** check box to enable bookmark viewing on Mobile Connect clients. Mobile Connect must be running version 2.0 or newer to view and access this bookmark.

**Note** Support will vary by device and may 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.
- Optionally select **HTTPS Mode** to use HTTPS to securely access the Citrix Portal.
- Optionally, select **Always use Java in Internet Explorer** to use Java to access the Citrix Portal when using Internet Explorer. Without this setting, a Citrix ActiveX client or plugin must be used with IE. This setting lets users avoid installing a Citrix client or plugin specifically for IE browsers. Java is used with Citrix by default on other browsers and also works with IE. Enabling this check box leverages this portability.
- 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.
- Check the **Display Bookmark to Mobile Connect clients** check box 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 SRA session for login to the Web server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

  Select the **Forms-based Authentication** check box 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>.

– Check the **Display Bookmark to Mobile Connect clients** check box 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 SRA session for login to the secure Web server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

  Select the **Forms-based Authentication** check box 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>.

– Check the **Display Bookmark to Mobile Connect clients** check box to display the bookmark on mobile devices.

**External Web Site**

– Select the **HTTPS Mode** check box to use SSL to encrypt communications with this Web site.

– Select the **Disable Security Warning** check box 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.

– Check the **Display Bookmark to Mobile Connect clients** check box to display the bookmark on mobile devices.

**Mobile Connect**

– Check the **Display Bookmark to Mobile Connect clients** check box to display the bookmark on mobile devices.

**File Shares (CIFS)**

– To allow users to use a Java Applet for File Shares that mimics Windows functionality, select the **Use File Shares Java Applet** check box.

– Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current SRA session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

  When creating a File Share, do not configure a Distributed File System (DFS) server on a Windows Domain Root system. Because the Domain Root allows access only to Windows computers in the domain, doing so will disable access to the DFS file shares from other domains. The SRA appliance is not a domain member and will not be able to connect to the DFS shares.

  DFS file shares on a stand-alone root are not affected by this Microsoft restriction.

**File Transfer Protocol (FTP)**

- Expand **Show advanced server configuration** to select an alternate value in the **Character Encoding** drop-down list. The default is **Standard (UTF-8)**.
- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current SRA session for login to the FTP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

**Telnet**

- Check the **Display Bookmark to Mobile Connect clients** check box to display the bookmark on mobile devices.

**Secure Shell version 1 (SSHv1)**

- Check the **Display Bookmark to Mobile Connect clients** check box to display the bookmark on mobile devices.

**Secure Shell version 2 (SSHv2)**

- Optionally select the **Automatically accept host key** check box.
- If using an SSHv2 server without authentication, such as a Dell SonicWALL firewall, you can select the **Bypass username** check box.
- Check the **Display Bookmark to Mobile Connect clients** check box to display the bookmark on mobile devices.

**Step 6** Click **Accept** to update the configuration. Once the configuration has been updated, the new user bookmark will be displayed in the **Edit Local User** window.

### Creating a Citrix Bookmark for a Local User

Citrix support requires Internet connectivity in order to download the ActiveX or Java client from the Citrix Web site. Citrix is accessed from Internet Explorer using ActiveX by default, or from other browsers using Java. Java can be used with IE by selecting an option in the Bookmark configuration. The server will automatically decide which Citrix client version to use. For browsers requiring Java to run Citrix, you must have Java 10.1 or higher.

When using the Java applet, the local printers are available in the Citrix client. However, under some circumstances it might be necessary to change the Universal Printer Driver to PCL mode.

To configure a Citrix bookmark for a user, perform the following tasks:

---

**Step 1** Navigate to **Users > Local Users** and click the configure icon next to the user.

**Step 2** In the **Edit Local User** page, select the **Bookmarks** tab.

**Step 3** Click **Add Bookmark...**

**Step 4** Enter a name for the bookmark in the **Bookmark Name** field.

**Step 5** Enter the name or IP address of the bookmark in the **Name or IP Address** field.

**Note** HTTPS, HTTP, Citrix, SSHv2, SSHv1, Telnet, and VNC will all take a port option :portnum. HTTP, HTTPS, and Fileshares can also have the path specified to a directory or file.

**Step 6** From the **Service** drop-down list, select **Citrix Portal (Citrix)**. The display will change.

**Step 7** Select the box next to **HTTPS Mode** to enable HTTPS mode.

**Step 8** Optionally select the **Always use Java in Internet Explorer** check box to use Java to access the Citrix Portal when using Internet Explorer. Without this setting, a Citrix ICA client or XenApp plugin (an ActiveX client) must be used with IE. This setting lets users avoid installing a Citrix ICA client or XenApp plugin specifically for IE browsers. Java is used with Citrix by default on other browsers and also works with IE. Enabling this check box leverages this portability.

**Step 9** 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.

**Step 10** Click **Accept**.

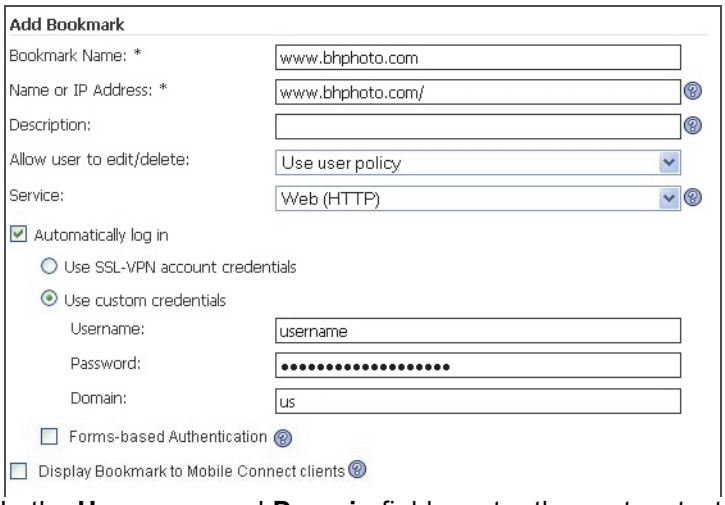
### Creating Bookmarks with Custom SSO Credentials

The administrator can configure custom Single Sign On (SSO) credentials for each user, group, or globally in HTTP(S), RDP (Java or ActiveX), File Shares (CIFS), and FTP bookmarks. This feature is used to access resources such as HTTP, RDP and FTP servers that need a domain prefix for SSO authentication. Users can log into the SRA appliance as *username*, and click a customized bookmark to access a server with *domain**username*. Either straight textual parameters or dynamic variables may be used for 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), perform the following steps:

**Step 1** Create or edit a HTTP(S), RDP, File Shares (CIFS), or FTP bookmark as described in Adding or Editing User Bookmarks on page 352.

**Step 2** In the **Bookmarks** tab, select the **Use Custom Credentials** option



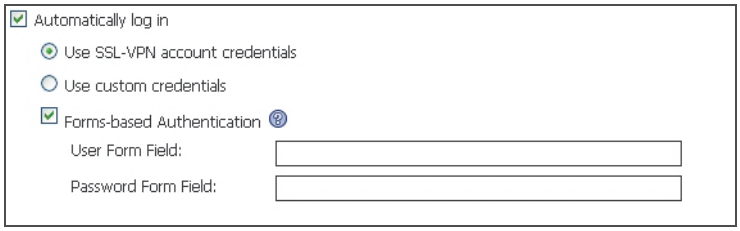

**Step 3** In the **Username** and **Domain** fields, enter the custom text to be passed to the bookmark, or use dynamic variables, as follows:

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

**Step 4** 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.

**Step 5** Select the **Forms-based Authentication** check box to configure Single Sign-On for Forms-based authentication.

- **User Form Field** - This should be the same as the 'name' and 'ID' attribute of the HTML element representing the User Name in the login form, for example:
  **<input type=text name='userid'>**
- **Password Form Field** - This should be the same as the 'name' or the 'ID' attribute of the HTML element representing Password in the login form, for example:
  **<input type=password name='PASSWORD' id='PASSWORD' maxlength=128>**




**Step 6** Check the **Display Bookmark to Mobile Connect** clients check box to display the bookmark on mobile devices.

**Step 7** Click **Accept**.

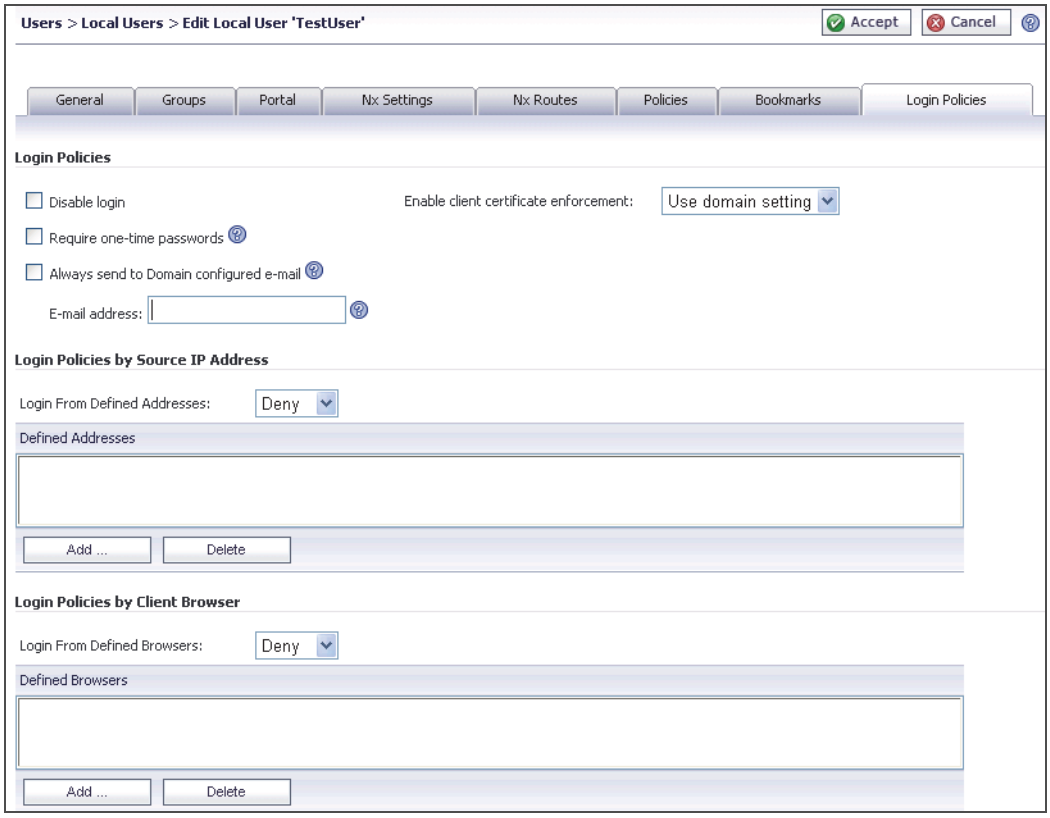
## Configuring Login Policies

The **Login Policies** tab provides configuration options for policies that allow or deny users with specific IP addresses from having login privileges to the SRA appliance. To allow or deny specific users from logging into the appliance, perform the following steps:

**Step 1** Navigate to the **Users > Local Users** page.

**Step 2** Click the configure icon for the user you want to configure. The **Edit Local User** page is displayed.

**Step 3** Click the **Login Policies** tab. The **Edit Local User** - **Login Policies** tab is displayed.




**Step 4** To block the specified user or users from logging into the appliance, select the **Disable login** check box.

**Step 5** Optionally select the **Enable client certificate enforcement** check box to require the use of client certificates for login. By checking this box, you require the client to present a client certificate for strong mutual authentication. Two additional fields will appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this 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 will match the client certificate:
  - User name: %USERNAME%
  - Domain name: %USERDOMAIN%
  - Active Directory user name: %ADUSERNAME%

– Wildcard: %WILDCARD%

**Step 6** To require the use of one-time passwords for the specified user to log into the appliance, select the **Require one-time passwords** check box.

**Step 7** Enter the user's email address into the **E-mail address** field to override any address provided by the domain. For more information about one-time passwords, see 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 SRA appliance and that domain.

**Step 8** To apply the policy you selected to a source IP address, select an access policy (**Allow** or **Deny**) in the **Login From Defined Addresses** drop-down list under **Login Policies by Source IP Address**, and then click **Add** under the list box. The **Define Address** window is displayed.

**Step 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.

**Step 10** Provide appropriate IP address(es) for the source address type you selected.

- **IP Address** - Type a single IP address in the **IP Address** field.
- **IP Network** - Type an IP address in the **Network Address** field and then supply a subnet mask value that specifies a range of addresses in the **Subnet Mask** field.
- **IPv6 Address** - 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**.

**Step 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 will now be applied to addresses in this range.

**Step 12** To apply the policy you selected to a client browser, select an access policy (**Allow** or **Deny**) in the **Login From Defined Browsers** drop-down list under **Login Policies by Client Browser**, and then click **Add** under the list. The **Define Browser** window is displayed.

**Step 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, Internet Explorer and Netscape is: javascript:document:writeln(navigator.userAgent)

**Step 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, perform the following steps:

**Step 1** Navigate to the **Users** > **Local Users** page.

**Step 2** Click the configure icon next to the user to be configured for EPC. The **Edit Local User** window is displayed.

**Step 3** Click the EPC tab. The **EPC** window is displayed.

**Step 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.


- Users > Local Groups Overview on page 366
- Deleting a Group on page 367
- Adding a New Group on page 367
- Editing Group Settings on page 368
- Group Configuration for LDAP Authentication Domains on page 382
- Group Configuration for Active Directory, NT and RADIUS Domains on page 386
- Creating a Citrix Bookmark for a Local Group on page 388
- Creating a Citrix Bookmark for a Local Group on page 388

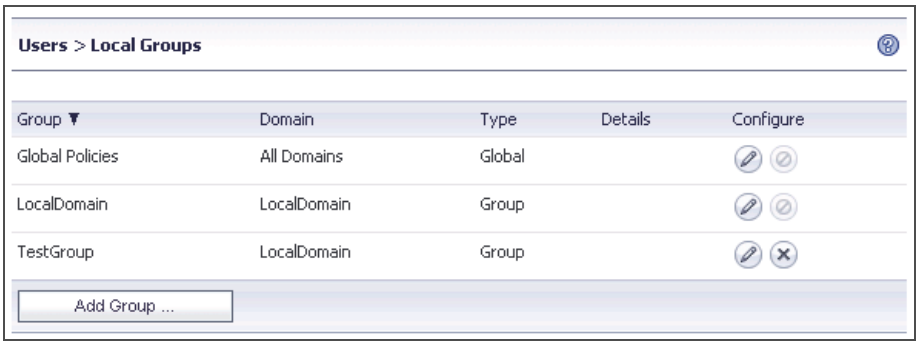

For a description of global settings for local groups, see Global Configuration on page 389.

# Users > Local Groups Overview

The **Users > Local Groups** page allows the administrator to add and configure groups for granular control of user access by specifying a group name and domain.

Note that a group is automatically created when you create a domain. You can create domains in the **Portals > Domains** page. You can also create a group directly from the **Users** > **Local Groups** page.

***Figure 55 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, may come from primary or additional groups.

**Additional Groups** - Multiple additional groups may be assigned, but in the case of conflicting policies, the primary group will take 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 will no longer appear in the list of defined groups.

**Note** A group cannot be deleted if users have been added to the group or if the group is the default group created for an authentication domain. To delete a group that is the default group for an authentication domain, delete the corresponding domain (you cannot delete the group in the **Edit Group Settings** window). If the group is not the default group for an authentication domain, first delete all users in the group. Then you will be able to delete the group on the **Edit Group Settings** page.

# Adding a New Group

Note that a group is automatically created when you create a domain. You can create domains in the **Portals > Domains** page. You can also create a group directly from the **Users** > **Local Groups** page.

The **Users** > **Local Groups** window contains two default objects:

- **Global Policies** - Contains access policies for all nodes in the organization.
- **LocalDomain** - The LocalDomain group is automatically created to correspond to the default LocalDomain authentication domain. This is the default group to which local users will be added, unless otherwise specified.

To create a new group, perform the following steps:

**Step 1** Click **Add Group**. The **Add Local Group** window is displayed.

**Step 2** In the **Add Local Group** window, enter a descriptive name for the group in the **Group Name** field.

**Step 3** Select the appropriate domain from the **Domain** drop-down list. The domain is mapped to the group.

**Step 4** Click **Accept** to update the configuration. Once the group has been added, the new group will be added to the **Local Groups** window.

All of the configured groups are displayed in the **Users > Local Groups** page, listed in alphabetical order.

# Editing Group Settings

To edit the settings for a group, click the configure icon in the row for the group that you wish to edit in the Local Groups table on the **Users > Local Groups** page. The Edit Group Settings window contains six tabs: **General**, **Portal**, **NxSettings**, **NxRoutes**, **Policies**, and **Bookmarks**.

See the following sections for information about configuring settings:

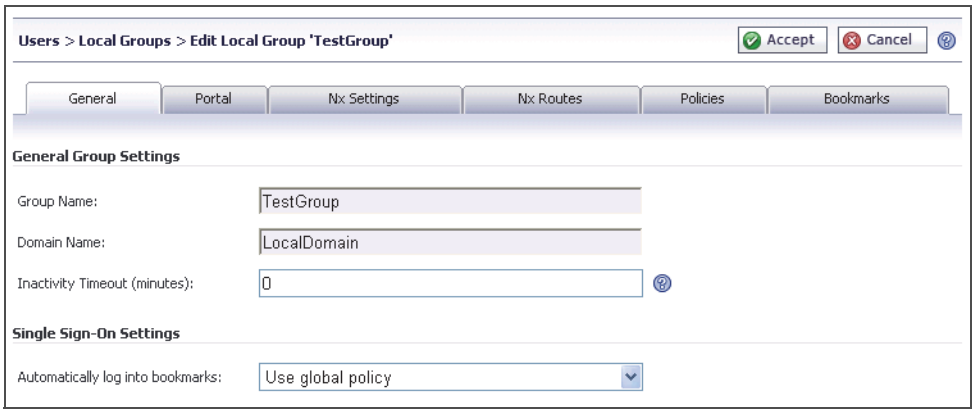

- Editing General Group Settings on page 368
- Modifying Group Portal Settings on page 369
- Enabling Group NetExtender Settings on page 371
- Enabling NetExtender Routes for Groups on page 372
- Adding Group Policies on page 374
- Editing a Policy for a File Share on page 376
- Configuring Group Bookmarks on page 377


## Editing General Group Settings

The **General** tab provides configuration options for a group's inactivity timeout value and single sign-on settings. To modify the general user settings, perform the following steps:

**Step 1** In the left-hand column, navigate to the **Users** > **Local Groups**.

**Step 2** Click the configure icon next to the group you want to configure. The **General** tab of the **Edit Group Settings** window displays. The **General** tab displays the following non-configurable fields: **Group Name** and **Domain Name**.




**Step 3** To set the inactivity timeout for the group, meaning that users will be signed out of the Virtual Office after 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 will take precedence over the group timeout and the group timeout will take precedence over the global timeout. Setting the global settings timeout to 0 disables the inactivity timeout for users that do not have a group or user timeout configured.

**Step 4** 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 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.

**Step 5** Click **Accept** to save the configuration changes.

## Modifying Group Portal Settings

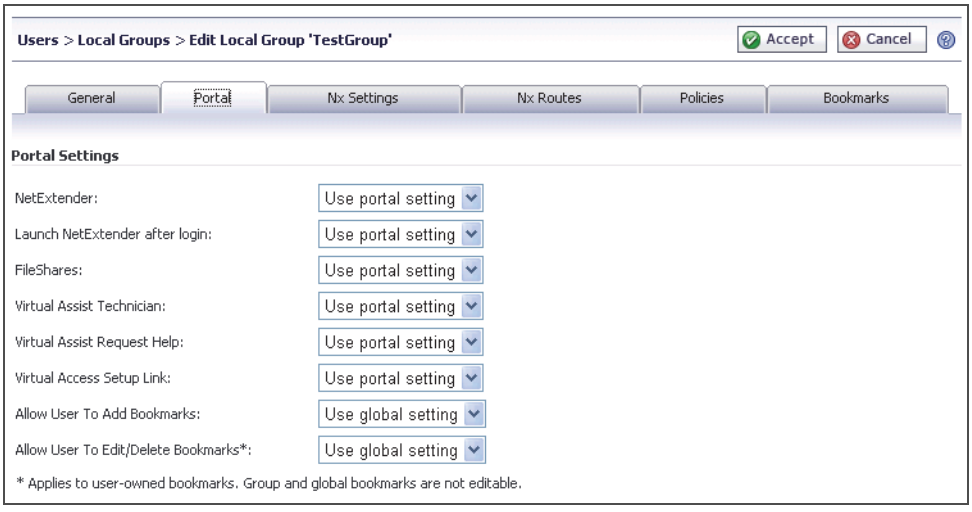
The **Portal** tab provides configuration options for portal settings for this group.

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

**Step 1** In the left-hand column, navigate to the **Users** > **Local Groups**.

**Step 2** Click the configure icon next to the group you want to configure.

**Step 3** In the **Edit Local Group** page, click the **Portal** tab.



**Step 4** On the **Portal** tab under **Portal Settings**, 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 setting defined in the main portal settings will be used to determine if the portal feature is enabled or disabled. The main portal settings are defined by configuring the portal in the Portals > Portals page, on the Home tab of the Edit Portal screen.
- Enabled – Enable this portal feature for this 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.

**Step 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 390 for information about global settings.

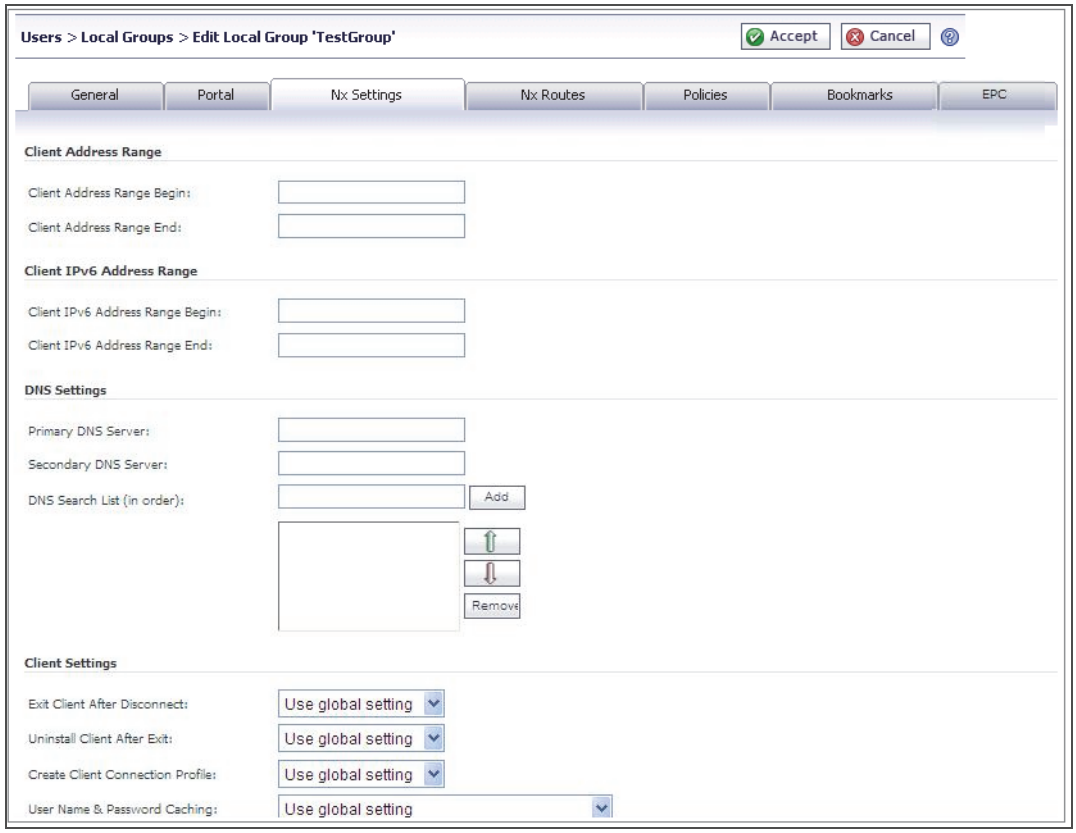
**Step 6** To allow users to edit or delete user-owned bookmarks, select **Allow** from the **Allow user to edit/delete bookmarks** drop-down menu. To prevent users from editing or deleting user-owned bookmarks, select **Deny**. To use the setting defined globally, select **Use global setting**.

**Note** The **Allow User to Edit/Delete Bookmarks** setting applies to user-owned bookmarks only. Users cannot edit or delete group and global bookmarks.

**Step 7** Click **Accept**.

## Enabling Group NetExtender Settings

This feature is for external users, who will inherit the settings from their assigned group upon login. NetExtender client settings can be specified for the group, or use the global settings. For information about configuring global settings, see Edit Global Settings on page 390.




To enable NetExtender ranges and configure DNS and client settings for a group, perform the following steps:

**Step 1** Navigate to **Users > Local Groups**.

**Step 2** Click the configure icon next to the group you want to configure.

**Step 3** In the **Edit Local Group** page, select the **NxSettings** tab.

**Step 4** Enter a beginning IPv4 address in the **Client Address Range Begin** field.

**Step 5** Enter an ending IPv4 address in the **Client Address Range End** field.

**Step 6** Enter a beginning IPv6 address in the **Client IPv6 Address Range Begin** field.

**Step 7** Enter an ending IPv6 address in the **Client IPv6 Address Range End** field.

**Step 8** Under **DNS Settings**, type the address of the primary DNS server in the **Primary DNS Server** field.

**Step 9** Optionally type the IP address of the secondary server in the **Secondary DNS Server** field.

**Step 10** 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 SRA appliances supporting connections from Apple iPhones, iPads, or other iOS devices using Dell SonicWALL 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 DNS server is used, which will not be able to resolve hosts within the company intranet.

**Step 11** 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 390.
- **Enabled** - Enable this action for all members of the group. Overrides the global setting.
- **Disabled** - Disable this action for all members of the group. Overrides the global setting.

**Step 12** 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 390.
- **Enabled** - Enable this action for all members of the group. Overrides the global setting.
- **Disabled** - Disable this action for all members of the group. Overrides the global setting.

**Step 13** 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 390.
- **Enabled** - Enable this action for all members of the group. Overrides the global setting.
- **Disabled** - Disable this action for all members of the group. Overrides the global setting.

**Step 14** 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 390.
- **Allow saving of user name only** - Allow caching of the user name for members of the group. Group members will only need to enter their password when starting NetExtender. Overrides the global setting.
- **Allow saving of user name & password** - Allow caching of the user name and password for members of the group. Group members will be automatically logged in when starting NetExtender. Overrides the global setting.
- **Prohibit saving of user name & password** - Do not allow caching of the user name and password for members of the group. Group members will be required to enter both user name and password when starting NetExtender. Overrides the global setting.

**Step 15** Click **Accept**.

## Enabling NetExtender Routes for Groups

The **Nx Routes** tab allows the administrator to add and configure client routes. IPv6 client routes are supported on SRA appliances.

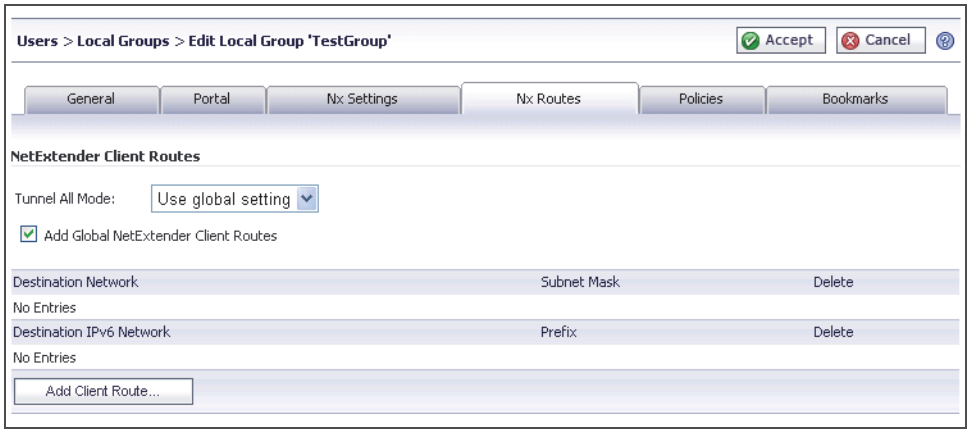
To enable multiple NetExtender routes for a group, perform the following steps:

---

**Step 1** Navigate to **Users > Local Groups.**

**Step 2** Click the configure icon next to the group you want to configure.

**Step 3** In the **Edit Local Group** page, select the **Nx Routes** tab.




**Step 4** In the **Tunnel All Mode** drop-down list, select one of the following:

- **Use global setting** - Take the action specified by the global setting. See Edit Global Settings on page 390.
- **Enabled** - Force all traffic for this user, including traffic destined to the remote users' local network, over the SRA NetExtender tunnel. Affects all members of the group. Overrides the global setting.
- **Disabled** - Disable this action for all members of the group. Overrides the global setting.

**Step 5** To add globally defined NetExtender client routes for members of this group, select the **Add Global NetExtender Client Routes** check box.

**Step 6** To configure NetExtender client routes specifically for members of this group, click **Add Client Route**.

**Step 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.

**Step 8** For an IPv4 destination network, type the subnet mask in the **Subnet Mask/Prefix** field using decimal format (255.0.0.0, 255.255.0.0, or 255.255.255.0). For an IPv6 destination network, type the prefix, such as 112.

**Step 9** On the **Add Client Route** screen, click **Accept**.

**Step 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, perform the following steps:

**Step 1** Navigate to **Users > Local Groups**.

**Step 2** Click the configure icon next to the group you want to configure.

**Step 3** In the **Edit Local Group** page, select the **Nx Routes** tab.

**Step 4** Select the **Add Global NetExtender Client Routes** check box.

**Step 5** Click **Accept**.

### Enabling Tunnel All Mode for Local Groups

This feature is for external users, who will inherit the settings from their assigned group upon login. Tunnel all mode ensures that all network communications are tunneled securely through the SRA tunnel. To enable tunnel all mode, perform the following tasks:

**Step 1** Navigate to **Users > Local Groups**.

**Step 2** Click the configure icon next to the group you want to configure.

**Step 3** In the **Edit Local Group** page, select the **Nx Routes** tab.

**Step 4** Select **Enable** from the **Tunnel All Mode** drop-down list.

**Step 5** Click **Accept**.

**Note** You can optionally tunnel-all SRA 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 may be created by destination address or address range and by service type.

The most specific policy will take precedence over less specific policies. For example, a policy that applies to only one IP address will have priority over a policy that applies to a range of IP addresses. If there are two policies that apply to a single IP address, then a policy for a specific service (for example RDP) will take precedence over a policy that applies to all services.

User policies take precedence over group policies and group policies take precedence over global policies, regardless of the policy definition. A user policy that allows access to all IP addresses will take precedence over a group policy that denies access to a single IP address.

**Note** Within the group policy scheme, the primary group policy is always enforced over any additional group policies.

To define group access policies, perform the following steps:

**Step 1** Navigate to **Users > Local Groups**.

**Step 2** Click the configure icon next to the group you want to configure.

**Step 3** In the **Edit Local Group** page, select the **Policies** tab.

**Step 4** On the **Policies** tab, click **Add Policy**. The **Add Policy** screen is displayed.

**Step 5** Define a name for the policy in the **Policy Name** field.

**Step 6** In the **Apply Policy To** drop-down list, select whether the policy will be applied to an individual host, a range of addresses, all addresses, a network object, a server path, or a URL object. 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 SRA policies apply to the destination address(es) of the SRA connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the 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 364.

- **IP Address** - If your policy applies to a specific host, enter the IP address of the local host machine in the **IP Address** field. Optionally enter a port range (80-443) or a single port number into the **Port Range/Port Number** field.
- **IP Address Range** - If your policy applies to a range of addresses, enter the beginning IP address in the **IP Network Address** field and the subnet mask that defines the IP address range in the **Subnet Mask** field. Optionally enter a port range (4100-4200) or a single port number into the **Port Range/Port Number** field.
- **Network Object -** If your policy applies to a predefined network object, select the name of the object from the **Network Object** drop-down list. A port or port range can be specified when defining a Network Object. See Adding Network Objects on page 137.
- **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 376.
- **URL Object** - If your policy applies to a predefined URL object, type the URL into the **URL** field.

- **IPv6 Address** - If your policy applies to a specific host, enter the IPv6 address of the local host machine in the **IPv6 Address** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field.
- **IPv6 Address Range** - If your policy applies to a range of addresses, enter the beginning IPv6 address in the **IPv6 Network Address** field and the prefix that defines the IPv6 address range in the **IPv6 Prefix** field. Optionally enter a port range (for example, 4100-4200) or a single port number into the **Port Range/Port Number** field.
- **All IPv6 Address** - If your policy applies to all IPv6 addresses, you do not need to enter any IP address information.

**Step 7** Select the service type in the **Service** menu. If you are applying a policy to a network object, the service type is defined in the network object.

**Step 8** Select **Allow** or **Deny** from the **Status** drop-down list to either permit or deny SRA connections for the specified service and host machine.

**Step 9** Click **Accept** to update the configuration. Once the configuration has been updated, the new group policy will be 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, perform the following steps:

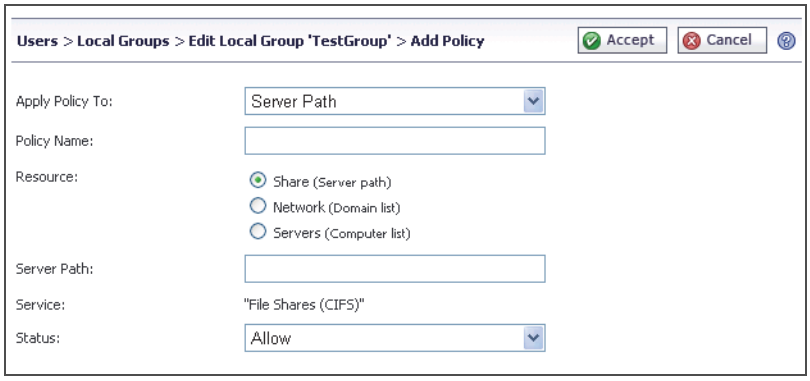
**Step 1** Navigate to **Users > Local Groups**.

**Step 2** Click the configure icon next to the group you want to configure.

**Step 3** Select the **Policies** tab.

**Step 4** Click **Add Policy...**

**Step 5** Select **Server Path** from the **Apply Policy To** drop-down list.




**Step 6** Type a name for the policy in the **Policy Name** field.

**Step 7** For **Resource**, select **Share (Server path)** for the resource type.

**Step 8** In the **Server Path** field, enter the server path in the format *servername/share/path* or *servername* *share**path*. The prefixes \\, //, \ and / are acceptable.

**Note** Share and path provide more granular control over a policy. Both are optional.

**Step 9** Select **Allow** or **Deny** from the **Status** drop-down list.

**Step 10** Click **Accept**.

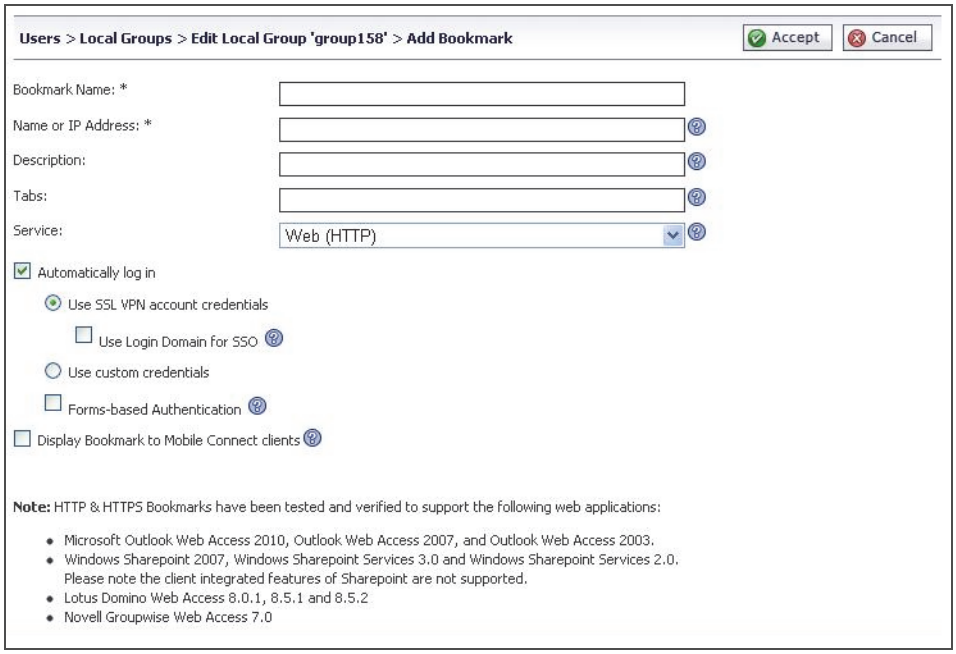
## Configuring Group Bookmarks

SRA appliance bookmarks provide a convenient way for SRA users to access computers on the local area network that they will connect to frequently. Group bookmarks will apply to all members of a specific group. To define group bookmarks, perform the following steps:

**Step 1** Navigate to the **Users** > **Local Groups** window.

**Step 2** Click the configure icon for the group for which you want to create a bookmark. The **Edit Local Group** page is displayed.

**Step 3** On the **Bookmarks** tab, click **Add Bookmark**. The **Add Bookmark** screen is displayed.




**Note** When group bookmarks are defined, all group members will see the defined bookmarks from the SRA user portal. Individual group members will not be able to delete or modify group bookmarks.

**Step 4** Enter a string that will be the name of the bookmark in the **Bookmark Name** field.

**Step 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 RDP - ActiveX, RDP - Java, 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.

**Step 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 may appear. Use the following information for the chosen service to complete the building of the bookmark:

**Terminal Services (RDP - ActiveX) or Terminal Services (RDP - Java)**

**Note** If you create a bookmark using the **Terminal Services (RDP - ActiveX)** service type, then when you click on that bookmark while using a browser other than Internet Explorer, the service is automatically switched to **Terminal Services (RDP - Java)**. A popup window notifies you of the switch.

- In the **Screen Size** drop-down menu, select the default terminal services screen size to be used when users execute this bookmark.

  Because different computers support different screen sizes, when you use a remote desktop application, you should select the size of the screen on the computer from which you are running a remote desktop session. Additionally, you may want to provide a path to where your application resides on your remote computer by typing the path in the **Application Path** field.
- In the **Colors** drop-down list, select the default color depth for the terminal service screen when users execute this bookmark.
- Optionally enter the local path for this application in the **Application and Path (optional)** field.
- In the **Start in the following folder** field, optionally enter the local folder in which to execute application commands.
- Select the **Login as console/admin session** check box to allow login as console or admin. Login as admin replaces login as console in RDC 6.1 and newer.
- Select the **Enable wake-on-LAN** check box 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 the **Send WOL packet to host name or IP address** check box, which can be applied in tandem with a MAC address of another machine to wake.
  - For Terminal Server Farm or Load Balancing support with **RDP - Java** bookmarks, select the **Server is TS Farm** check box to enable a proper connection. Note that only the pure Java RDP client supports this feature and some advanced options will not be available in this mode.

- For **RDP - Java** bookmarks, select the **Force Java Client Usage** check box to force the use of the Java RDP client rather than the locally installed RDP client if it exists. If this option is selected, no Windows Advanced options are supported.
- For Windows clients or on Mac clients running Mac OS X 10.5 or above with RDC installed, expand **Show advanced Windows options** and select the check boxes for any of the following redirect options: **Redirect Printers**, **Redirect Drives**, **Redirect Ports**, **Redirect SmartCards**, **Redirect clipboard**, or **Redirect plug and play devices** to redirect those devices or features on the local network for use in this bookmark session. You can hover your mouse pointer over the Help icon next to certain options to display tooltips that indicate requirements.

  To see local printers show up on your remote machine (Start > Settings > Control Panel > Printers and Faxes), select **Redirect Ports** as well as **Redirect Printers**.

  Select the check boxes for any of the following additional features for use in this bookmark session: **Display connection bar**, **Auto reconnection**, **Desktop background**, **Bitmap caching**, **Menu/window animation**, **Visual styles**, or **Show window contents while dragging/resizing**.
  In the **Remote Audio** drop-down list, select **Play on this computer**, **Play on remote computer**, or **Do not play**.
  If the client application will be RDP 6 (Java), you can select any of the following options as well: **Dual monitors**, **Font smoothing**, **Desktop composition**, or **Remote Application**.
  **Remote Application** monitors server and client connection activity; to use it, you need to register remote applications in the Windows 2008 RemoteApp list. If **Remote Application** is selected, the Java Console will display messages regarding connectivity with the Terminal Server.
- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current SRA session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

**Virtual Network Computing (VNC)**

- 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** if the user will not be making any changes on the remote system.
- Select **Share Desktop** to allow multiple users to view and use the same VNC desktop.

**Citrix Portal (Citrix)**

- Optionally select **HTTPS Mode** to use HTTPS to securely access the Citrix Portal.
- Optionally, select **Always use Java in Internet Explorer** to use Java to access the Citrix Portal when using Internet Explorer. Without this setting, a Citrix ActiveX client or plugin must be used with IE. This setting lets users avoid installing a Citrix client or plugin specifically for IE browsers. Java is used with Citrix by default on other browsers and also works with IE. Enabling this check box leverages this portability.
- 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.

**Web (HTTP)**

- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current SRA session for login to the Web server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

  Select the **Forms-based Authentication** check box 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>.

**Secure Web (HTTPS)**

- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current SRA session for login to the secure Web server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

  Select the **Forms-based Authentication** check box 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>.

**External Web Site**

- Select the **HTTPS Mode** check box to use SSL to encrypt communications with this Web site.
- Select the **Disable Security Warning** check box 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.

**File Shares (CIFS)**

- To allow users to use a Java Applet for File Shares that mimics Windows functionality, select the **Use File Shares Java Applet** check box.
- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current SRA session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

  When creating a File Share, do not configure a Distributed File System (DFS) server on a Windows Domain Root system. Because the Domain Root allows access only to Windows computers in the domain, doing so will disable access to the DFS file shares from other domains. The SRA appliance is not a domain member and will not be able to connect to the DFS shares.

  DFS file shares on a stand-alone root are not affected by this Microsoft restriction.

**File Transfer Protocol (FTP)**

- Expand **Show advanced server configuration** to select an alternate value in the **Character Encoding** drop-down list. The default is **Standard (UTF-8)**.
- Optionally select **Automatically log in** and select **Use SSL-VPN account credentials** to forward credentials from the current SRA session for login to the FTP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials on page 362.

**Telnet**

- No additional fields

**Secure Shell version 1 (SSHv1)**

- No additional fields

**Secure Shell version 2 (SSHv2)**

- Optionally select the **Automatically accept host key** check box.
- If using an SSHv2 server without authentication, such as a Dell SonicWALL firewall, you can select the **Bypass username** check box.

**Step 7** Check the **Display Bookmark to Mobile Connect** clients check box to display the bookmark on mobile devices.

**Step 8** Click **Accept** to update the configuration. Once the configuration has been updated, the new group bookmark will display in the **Edit Local Group** page.

## Configuring Group End Point Control

To configure the End Point Control profiles used by local groups, perform the following steps:

**Step 1** Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** page.

**Step 2** Click the configure icon next to the group to be configured for EPC. The **Edit Local Group** window is displayed.

**Step 3** Click the EPC tab. The **EPC** window is displayed.

**Step 4** Configure EPC group settings and add or remove device profiles, as explained in Users > Local Groups on page 366.

# Group Configuration for LDAP Authentication Domains

**Note** The Microsoft Active Directory database uses an LDAP organization schema. The Active Directory database may be queried using Kerberos authentication (the standard authentication type; this is labeled “Active Directory” domain authentication in the Dell SonicWALL SRA management interface), NTLM authentication (labeled NT Domain authentication in the SRA management interface), or using LDAP database queries. An LDAP domain configured in the SRA management interface can authenticate to an Active Directory server.

LDAP (Lightweight Directory Access Protocol) is a standard for querying and updating a directory. Since LDAP supports a multilevel hierarchy (for example, groups or organizational units), the SRA appliance can query this information and provide specific group policies or bookmarks based on LDAP attributes. By configuring LDAP attributes, the 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 SRA appliance.

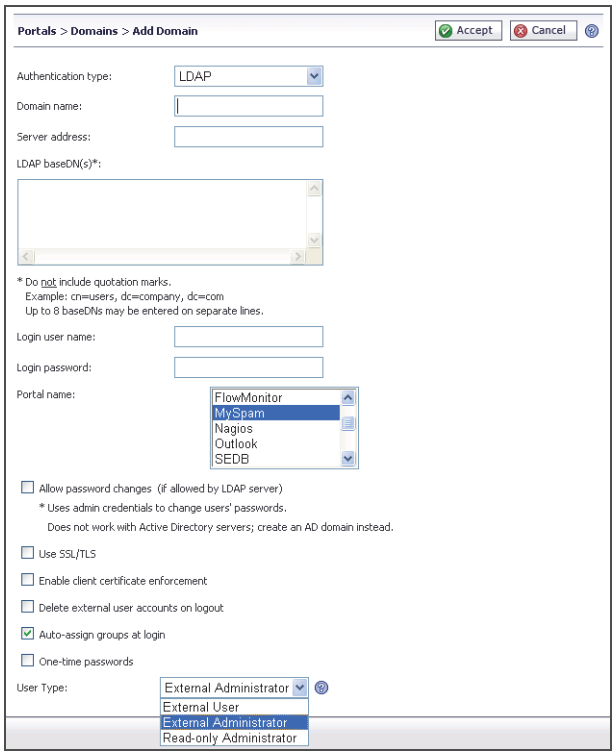
Once an LDAP authentication domain is created, a default LDAP group will be created with the same name as the LDAP domain name. Although additional groups may be added or deleted from this domain, the default LDAP group may not be deleted. If the user for which you created LDAP attributes enters the Virtual Office home page, the bookmark you created for the group the user is in will display in the Bookmarks Table.

For an LDAP group, you may define LDAP attributes. For example, you can specify that users in an LDAP group must be members of a certain group or organizational unit defined on the LDAP server. Or you can specify a unique LDAP distinguished name.

To add an LDAP attribute for a group so that a user will have a bookmark assigned when entering the Virtual Office environment, perform the following steps:

**Step 1** Navigate to the **Portals > Domains** page and click **Add Domain** to display the **Add New Domain** window.

**Step 2** Select LDAP from the **Authentication Type** menu. The LDAP domain configuration fields will be displayed.




**Step 3** Enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the SRA user portal. It can be the same value as the **Server address** field.

**Step 4** Enter the IP address or domain name of the server in the **Server address** field.

**Step 5** Enter the search base for LDAP queries in the **LDAP baseDN** field. An example of a search base string is **CN=Users,DC=yourdomain,DC=com**.

**Tip** It is possible for multiple OUs to be configured for a single domain by entering each OU on a separate line in the **LDAP baseDN** field. In addition, any sub-OUs will be automatically included when parents are added to this field.

**Note** Do not include quotes (“”) in the **LDAP BaseDN** field.

**Step 6** Enter the common name of a user that has been delegated control of the container that user will be in along with the corresponding password in the **Login user name** and **Login password** fields.

**Note** When entering **Login user name** and **Login password**, remember that the SRA appliance binds to the LDAP tree with these credentials and users can log in with their sAMAccountName.

**Step 7** Enter the name of the portal in the **Portal name** field. Additional layouts may be defined in the **Portals > Portals** page.

**Step 8** Select the **Allow password changes (if allowed by LDAP server)** check box if you want to be able to change user's passwords. The admin account must be used when changing user passwords.

**Step 9** Select the **Delete external user accounts on logout** check box to delete users who are not logged into a domain account after they log out.

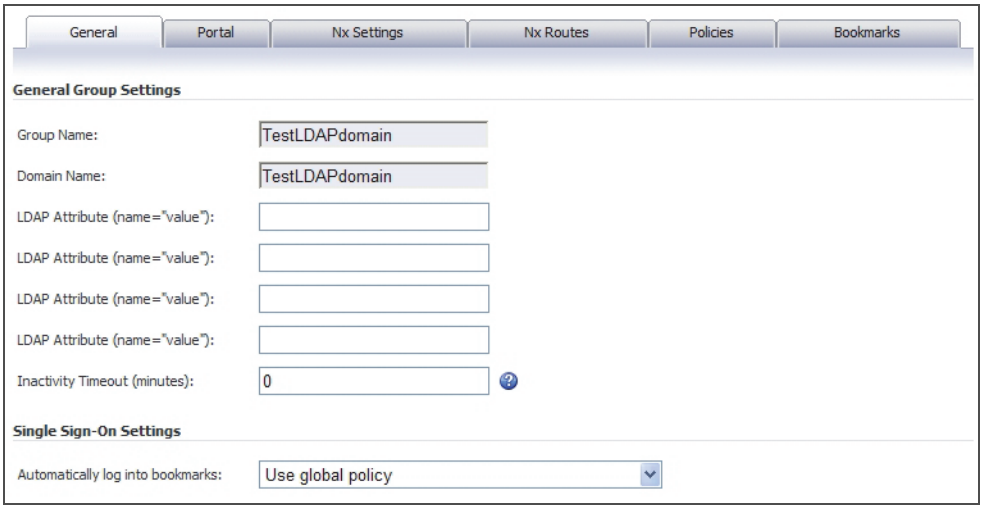
**Step 10** Optionally select the **One-time passwords** check box to enable the One-time password feature. A drop-down list will appear, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured will use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured will not be allowed to login.
- **using domain name** - Users in the domain will use the One Time Password feature. One Time Password emails for all users in the domain will be sent to username@domain.com.

**Step 11** If you select **One-time passwords**, an **LDAP e-mail attribute** drop-down list appears. Select one of the following:

- **mail** - Select **mail** if this is the name of your LDAP email attribute.
- **userPrincipalName** - Select **userPrincipalName** if this is the name of your LDAP email attribute.
- **custom** - Select **custom** to enter any other LDAP email attribute. Enter the attribute name into the **Custom attribute** field that appears.

**Step 12** Navigate to the **Users > Local Groups** page and click the configure icon. The **Edit Group Settings** page is displayed, with fields for LDAP attributes on the **General** tab.




**Step 13** On the **General** tab, you may optionally fill out one or multiple **LDAP Attribute** fields with the appropriate names where **name=value** is the convention for adding a series of LDAP attributes. To see a full list of LDAP attributes, refer to the *Dell SonicWALL LDAP Attribute document*.

As a common example, fill out an attribute field with the memberOf= attribute which can bundle the following common variable types:

CN= - the common name. DN= - the distinguished name. DC= - the domain component.

You need to provide quote delimiters around the variables you bundle in the memberOf line. You separate the variables by commas. An example of the syntax using the **CN** and **DC** variables would be:

memberOf="CN=<string>, DC=<string>"

An example of a line you might enter into the **LDAP Attribute** field, using the **CN** and **DC** variables would be:

memberOf="CN=Terminal Server Computers,CN=Users,DC=sonicwall,DC=net"

**Step 14** Type an inactivity timeout value (in minutes) in the **Inactivity Timeout** field. Enter **0** (zero) to use the global inactivity timeout setting.

**Step 15** Under **Single Sign-On Settings**, in the **Automatically log into bookmarks list**, select one of the following:

- **Use global policy** – Use the global policy for using SSO to login to bookmarks.
- **User-controlled (enabled by default for new users)** – Enable SSO to login to bookmarks for new users, and allow users to change this setting.
- **User-controlled (disabled by default for new users)** – Disable SSO to login to bookmarks for new users, and allow users to change this setting.
- **Enabled** – Enable SSO to login to bookmarks
- **Disabled** – Disable SSO to login to bookmarks

**Step 16** Click **Accept** when done.

## LDAP Attribute Information

When configuring LDAP attributes, the following information may be helpful:

- If multiple attributes are defined for a group, all attributes must be met by LDAP users.
- LDAP authentication binds to the LDAP tree using the same credentials as are supplied for authentication. When used against Active Directory, this requires that the login credentials provided match the CN (common name) attribute of the user rather than samAccountName (login name). For example, if your NT/Active Directory login name is **gkam** and your full name is **guitar kam,** when logging into the 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 will login with the sAMAccountName.
- If no attributes are defined, then any user authorized by the LDAP server can be a member of the group.
- If multiple groups are defined and a user meets all the LDAP attributes for two groups, then the user will be considered part of the group with the most LDAP attributes defined. If the matching LDAP groups have an equal number of attributes, then the user will be considered a member of the group based on the alphabetical order of the groups.
- If an LDAP user fails to meet the LDAP attributes for all LDAP groups configured on the SRA appliance, then the user will not be able to log into the portal. So the LDAP attributes feature not only allows the administrator to create individual rules based on the LDAP group or organization, it also allows the administrator to only allow certain LDAP users to log into the portal.

### Example of LDAP Users and Attributes

If a user is manually added to a LDAP group, then the user setting will take precedence over LDAP attributes.

For example, an LDAP attribute **objectClass="Person"** is defined for group Group1 and an LDAP attribute **memberOf="CN=WINS Users,DC=sonicwall,DC=net"** is defined for Group2.

If user Jane is defined by an LDAP server as a member of the Person object class, but is not a member of the WINS Users group, Jane will be a member of SRA appliance Group1.

But if the administrator manually adds the user Jane to SRA appliance Group2, then the LDAP attributes will be ignored and Jane will be a member of Group2.

### Sample LDAP Attributes

You may enter up to four LDAP attributes per group. The following are some example LDAP attributes of Active Directory LDAP users:

```
name="Administrator"
memberOf="CN=Terminal Server Computers,CN=Users,DC=sonicwall,DC=net"
objectClass="user"
msNPAllowDialin="FALSE"
```

## Querying an LDAP Server

If you would like to query your LDAP or Active Directory server to find out the LDAP attributes of your users, there are several different methods. From a machine with 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 will be 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, NT and RADIUS Domains

For authentication to RADIUS, Microsoft NT domain or Active Directory servers (using Kerberos), you can individually define AAA users and groups. This is not required, but it enables you to create separate policies or bookmarks for individual AAA users.

When a user logs in, the SRA appliance will validate with the appropriate Active Directory, RADIUS, or NT server that the user is authorized to login. If the user is authorized, the SRA appliance will check to see if a user exists in the SRA appliance database for users and groups. If the user is defined, then the policies and bookmarks defined for the user will apply.

For example, if you create a RADIUS domain in the 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 login to the portal, policies, bookmarks and other user settings will apply to the users. If the AAA user does not exist in the SRA appliance, then only the global settings, policies and bookmarks will apply to the user.

This section contains the following subsections:


- Bookmark Support for External (Non-Local) Users on page 387
- Adding a RADIUS Group on page 387
- Adding an Active Directory Group on page 388


## Bookmark Support for External (Non-Local) Users

The Virtual Office bookmark system allows bookmarks to be created at both the group and user levels. The administrator can create both group and user bookmarks which will be propagated to applicable users, while individual users can create only personal bookmarks.

Since bookmarks are stored within the 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, NT, LDAP) groups, the correlation is automated since creating an external domain creates a corresponding local group.

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

Rather than requiring administrators to manually create local users for external domain users to use personal bookmarks, the 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 SRA appliance, the moment jdoe adds a personal bookmark, a local user called jdoe will be created on the SRA appliance as type External, and can then be managed like any other local user by the administrator. The external local user will remain until deleted by the administrator.

## Adding a RADIUS Group

**Note** Before configuring RADIUS groups, ensure that the RADIUS Filter-Id option is enabled for the RADIUS Domain to which your group is associated. This option is configured in the **Portals > Domains** page.

The **RADIUS Groups** tab allows the administrator to enable user access to the SRA appliance based on existing RADIUS group memberships. By adding one or more RADIUS groups to an SRA group, only users associated with specified RADIUS group(s) are allowed to login. To add a RADIUS group, perform the following steps:

**Step 1** In the **Users > Local Groups** page, click the configure button for the RADIUS group you want to configure.

**Step 2** In the **RADIUS Groups** tab and click the **Add Group...** button. The Add RADIUS Group page displays.

**Step 3** Enter the **RADIUS Group** name in the corresponding field. The group name must match the RADIUS Filter-Id exactly.

**Step 4** Click the **Accept** button. The group displays in the RADIUS Groups section.

## Adding an Active Directory Group

The **AD Groups** tab allows the administrator to enable user access to the SRA appliance based on existing AD group memberships. By adding one or more AD groups to an SRA 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, perform the following steps:

**Step 1** In the **Users > Local Groups** page, click the configure button for the AD group you want to configure.

**Step 2** In the **AD Groups** tab and click the **Add Group...** button. The Add Active Directory Group page displays.

**Step 3** Enter the **Active Directory Group** name in the corresponding field.

**Step 4** Optionally, select the **Associate with AD group** check box if you wish to associate the SRA group with your AD group. This step can also be completed at a later time in the **Edit Group** page under the **AD Groups** tab.

**Step 5** Click the **Accept** button. The group displays in the Active Directory Groups section. The process of adding a group may take several moments. Do not click the Add button more than once during this process.

# Creating a Citrix Bookmark for a Local Group

To configure a Citrix bookmark for a user, perform the following tasks:

**Step 1** Navigate to **Users > Local Groups**.

**Step 2** Click the configure icon next to the group you want to configure.

**Step 3** In the **Edit Group Settings** window, select the **Bookmarks** tab.

**Step 4** Click **Add Bookmark...**

**Step 5** Enter a name for the bookmark in the **Bookmark Name** field.

**Step 6** Enter the name or IP address of the bookmark in the **Name or IP Address** field.

**Step 7** From the **Service** drop-down list, select **Citrix Portal (Citrix)**. A check box for **HTTPS Mode** displays.

**Step 8** Optionally select the **HTTPS Mode** check box to enable HTTPS mode.

**Step 9** Optionally, select **Always use Java in Internet Explorer** to use Java to access the Citrix Portal when using Internet Explorer. Without this setting, an ActiveX Citrix client or plugin must be used with IE.

**Step 10** 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.

**Step 11** Click **Accept**.

# Global Configuration

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:

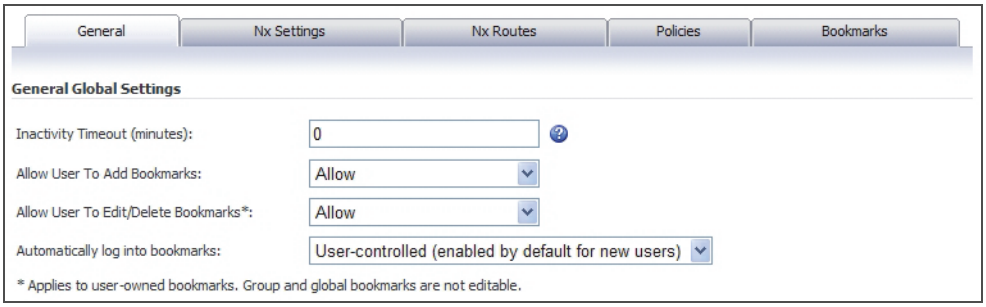

- Edit Global Settings on page 390
- Edit Global Policies on page 392
- Edit Global Bookmarks on page 394

# Edit Global Settings

To edit global settings, perform the following steps:

**Step 1** Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** window.

**Step 2** Click the configure icon next to **Global Policies**. The **Edit Global Settings** window is displayed.




**Step 3** On the **General** tab, to set the inactivity timeout for all users or groups, meaning that users will be signed out of the Virtual Office after the specified time period, enter the number of minutes of inactivity to allow in the **Inactivity Timeout** field.

**Note** The inactivity timeout can be set at the user, group and global level. If one or more timeouts are configured for an individual user, the user timeout setting will take precedence over the group timeout and the group timeout will take precedence over the global timeout. Setting the global settings timeout to 0 disables the inactivity timeout for users that do not have a group or user timeout configured.

**Step 4** To allow users to add new bookmarks, select **Allow** from the **Allow User to Add Bookmarks** drop-down menu. To prevent users from adding new bookmarks, select **Deny**.

**Step 5** To allow users to edit or delete user-owned bookmarks, select **Allow** from the **Allow User to Edit/Delete Bookmarks** drop-down menu. To prevent users from editing or deleting user-owned bookmarks, select **Deny**.

**Note** Users cannot edit or delete group and global bookmarks.

**Step 6** In the **Automatically log into bookmarks** drop-down list, select one of the following options:

- **User-controlled (enabled by default for new users)**: Select this option to allow users to enable or disable single sign-on (SSO) automatic login for bookmarks. This setting enables automatic login by default for new users.
- **User-controlled (disabled by default for new users)**: Select this option to allow users to enable or disable single sign-on (SSO) automatic login for bookmarks. This setting disables automatic login by default for new users.
- **Enabled**: Select this option to enable automatic login for bookmarks.

- **Disabled**: Select this option to disable automatic login for bookmarks.

**Step 7** Click **Accept** to save the configuration changes.

**Step 8** Navigate to the **Nx Settings** tab.

**Step 9** To set a client address range, enter a beginning address in the **Client Address Range Begin** field and an ending address in the **Client Address Range End** field.

**Step 10** To set a client IPv6 address range, enter a beginning IPv6 address in the **Client IPv6 Address Range Begin** field and an ending IPv6 address in the **Client IPv6 Address Range End** field.

**Step 11** In the **Exit Client After Disconnect** drop-down list, select **Enabled** or **Disabled**.

**Step 12** In the **Uninstall Client After Exit** drop-down list, select **Enabled** or **Disabled**.

**Step 13** In the **Create Client Connection Profile** drop-down list, select **Enabled** or **Disabled**.

**Step 14** In the **User Name & Password Caching** drop-down list, select one of the following:

- **Allow saving of user name only** - Allow caching of the user name on the client. Users will only need to enter their password when starting NetExtender.
- **Allow saving of user name & password** - Allow caching of the user name and password on the client. Users will be automatically logged in when starting NetExtender, after the first login.
- **Prohibit saving of user name & password** - Do not allow caching of the user name and password on the client. Users will be required to enter both user name and password when starting NetExtender.

**Step 15** Navigate to the **Nx Routes** tab.

**Step 16** In the **Tunnel All Mode** drop-down list, select **Enabled** to force all traffic for the user, including traffic destined to the remote user's local network, over the SRA NetExtender tunnel. **Tunnel All Mode** is disabled by default.

**Step 17** To add a client route, click **Add Client Route...**

**Step 18** In the **Add Client Route** 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.

**Step 19** For an IPv4 destination network, type the subnet mask in the **Subnet Mask/Prefix** field using decimal format (255.0.0.0, 255.255.0.0, or 255.255.255.0). For an IPv6 destination network, type the prefix, such as 112.

**Step 20** Click **Add**.

**Step 21** Click **Accept** to save the configuration changes.

**Step 22** Navigate to the **Policies** tab.

**Step 23** To add a policy, click **Add Policy...**

**Step 24** In the **Apply Policy To** drop-down list, select one of the following: **IP Address**, **IP Address Range**, **All Addresses**, **Network Object**, **Server Path**, **URL Object**, **All IPv6 Address**, **IPv6 Address**, or **IPv6 Address Range**.

**Step 25** Enter a name for the policy in the **Policy Name** field.

**Step 26** In the fields that appear based on your **Apply Policy To** settings, fill in the appropriate information. For example, if you select **IP Address** in the **Apply Policy To** drop-down list, you will need to supply the IP Address in the **IP Address** field and the service in the **Service** drop-down list. If you select **IPv6 Address Range**, enter the beginning IPv6 address in the **IPv6 Network Address** field and the prefix that defines the IPv6 address range in the **IPv6 Prefix**

field. Optionally enter a port range (80-443) or a single port number into the **Port Range/Port Number** field. This field is available when you select **IP Address**, **IP Address Range**, **IPv6 Address**, or **IPv6 Address Range** in the **Apply Policy To** drop-down list.

**Step 27** Click **Accept** to save the configuration changes.

**Step 28** Click the **Bookmarks** tab.

**Step 29** To add a bookmark, click **Add Bookmark...**

**Step 30** Enter a bookmark name in the **Bookmark Name** field.

**Step 31** Enter the bookmark name or IP address in the **Name or IP Address** field.

**Step 32** Select one of the following services from the **Service** drop-down list: **Terminal Services (RDP - ActiveX)**, **Terminal Services (RDP - Java)**, **Virtual Network Computing (VNC)**, **Citrix Portal (Citrix)**, **Web (HTTP)**, **Secure Web (HTTPS)**, **File Shares (CIFS)**, **File Transfer Protocol (FTP)**, **Telnet, Secure Shell Version 1 (SSHv1)**, or **Secure Shell Version 2(SSHv2)**.

**Note** IPv6 is not supported on File Shares bookmarks.

**Step 33** In the fields that appear based on your **Service** settings, fill in the appropriate information. For example, if you select **Terminal Services (RDP - ActiveX)**, you will need to select the desired screen size from the **Screen Size** drop-down list.

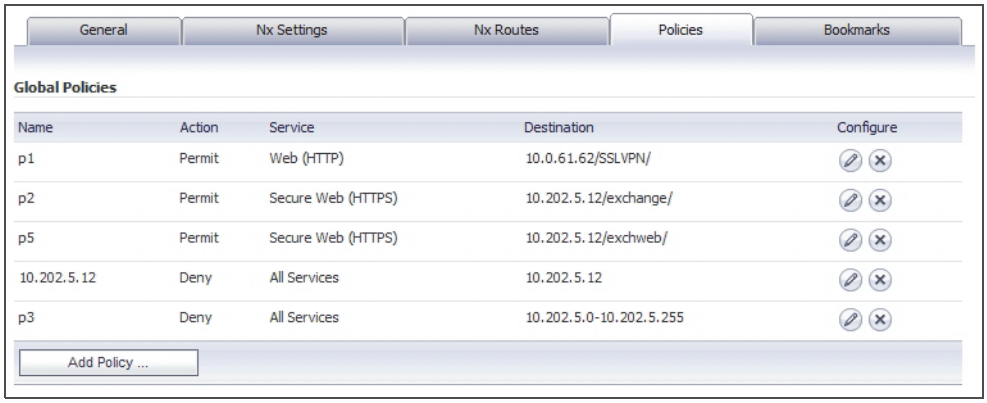
**Step 34** Click **Accept** to save the configuration changes.

# Edit Global Policies

To define global access policies, perform the following steps:

**Step 1** Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** window.

**Step 2** Click the configure icon next to **Global Policies**. The **Edit Global Settings** window is displayed.




**Step 3** On the **Policies** tab, click **Add Policy**. The **Add Policy** window is displayed.

**Note** User and group access policies will take precedence over global policies.

**Step 4** In the **Apply Policy To** drop-down list, select one of the following: **IP Address**, **IP Address Range**, **All Addresses**, **Network Object**, **Server Path**, **URL Object**, **All IPv6 Address**, **IPv6 Address**, or **IPv6 Address Range**.

**Step 5** Type a name for the policy in the **Policy Name** field.

**Note** SRA appliance policies apply to the destination address(es) of the SRA connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to the 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 Address Range** option from the **Apply Policy To** drop-down list and enter the IPv4 network address in the **IP Network Address** field and the subnet mask in the **Subnet Mask** field.
- If your policy applies to a specific IPv6 host, select the **IPv6 Address** option from the **Apply Policy To** drop-down list and enter the IPv6 address of the local host machine in the **IPv6 Address** field.
- If your policy applies to a range of IPv6 addresses, select the **IPv6 Address Range** option from the **Apply Policy To** drop-down list and enter the IPv6 network address in the **IPv6 Network Address** field and the IPv6 prefix in the **IPv6 Prefix** field.

**Step 6** Optionally enter a port range (80-443) or a single port number into the **Port Range/Port Number** field. This field is available when you select **IP Address**, **IP Address Range**, **IPv6 Address**, or **IPv6 Address Range** in the **Apply Policy To** drop-down list.

**Step 7** Select the service type in the **Service** drop-down list. If you are applying a policy to a network object, the service type is defined in the network object.

**Step 8** Select **ALLOW** or **DENY** from the **Status** drop-down list to either permit or deny SRA connections for the specified service and host machine.

**Step 9** Click **Accept** to update the configuration. Once the configuration has been updated, the new policy will be displayed in the **Edit Global Settings** window. The global policies will be displayed in the policy list in the **Edit Global Settings** window in the order of priority, from the highest priority policy to the lowest priority policy.

## Edit a Policy for a File Share

To edit file share access policies, perform the following steps:

**Step 1** Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** window.

**Step 2** Click the configure icon next to **Global Policies**. The **Edit Global Settings** window will be displayed.

**Step 3** Select the **Policies** tab.

**Step 4** Click **Add Policy**.

**Step 5** Select **Server Path** from the **Apply Policy To** drop-down list.

**Step 6** Type a name for the policy in the **Policy Name** field.

**Step 7** In the **Resource** field, select one of the following radio buttons for the type of resource:

- Share (Server path)
- Network (Domain list)
- Servers (Computer list)

**Step 8** In the **Server Path** field, enter the server path in the format *servername/share/path* or *servername\share\path*. The prefixes \\, //, \ and / are acceptable.

**Note** Share and path provide more granular control over a policy. Both are optional.

**Step 9** Select **PERMIT** or **DENY** from the **Status** drop-down list.

**Step 10** Click **Accept**.

# Edit Global Bookmarks

To edit global bookmarks, perform the following steps:

**Step 1** Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** page.

**Step 2** Click the configure icon next to **Global Policies**. The **Edit Global Policies** window is displayed.

**Step 3** Click **Add Bookmark**. An **Add Bookmark** window will be displayed.

**Note** When global bookmarks are defined, all users will see the defined bookmarks from the SRA user portal. Individual users will not be able to delete or modify global bookmarks.

**Step 4** To edit a bookmark, enter a descriptive name in the **Bookmark Name** field.

**Step 5** Enter the domain name or the IP address of a host machine on the LAN in the **Name or IP Address** field.

**Step 6** Select the service type in the **Service** drop-down list.

**Note** Depending on the service you select from the **Service** drop-down list, additional fields may appear. Fill in the information based on the service you select. For example, if you select **RDP - ActiveX** or **RDP - Java**, a **Screen Size** drop-down list and other additional fields are displayed.

**Step 7** Click **Accept** to update the configuration. Once the configuration has been updated, the new global bookmark will be displayed in the bookmarks list in the **Edit Global Settings** window.

# Edit EPC Settings

To configure global End Point Control profiles for local groups or users, perform the following steps:

**Step 1** Navigate to either the **Users** > **Local Users** or **Users** > **Local Groups** page.

**Step 2** Click the configure icon next to **Global Policies**. The **Edit Global Policies** window is displayed.

**Step 3** Click the EPC tab. The **EPC** window is displayed.

**Step 4** Configure EPC global settings and add or remove device profiles, as explained in Users > Local Groups on page 366 and Users > Local Groups on page 366.

# Chapter 15
# Log Configuration

This chapter provides information and configuration tasks specific to the **Log** pages on the SRA Web-based management interface.

This chapter contains the following sections:


- Log > View on page 397
- Log > Settings on page 400
- Log > Categories on page 404
- Log > ViewPoint on page 404
- Log > Analyzer on page 405


## Log > View

The SRA appliance supports Web-based logging, syslog logging and email alert messages. In addition, The SRA appliance may be configured to email the event log file to the SRA administrator before the log file is cleared.

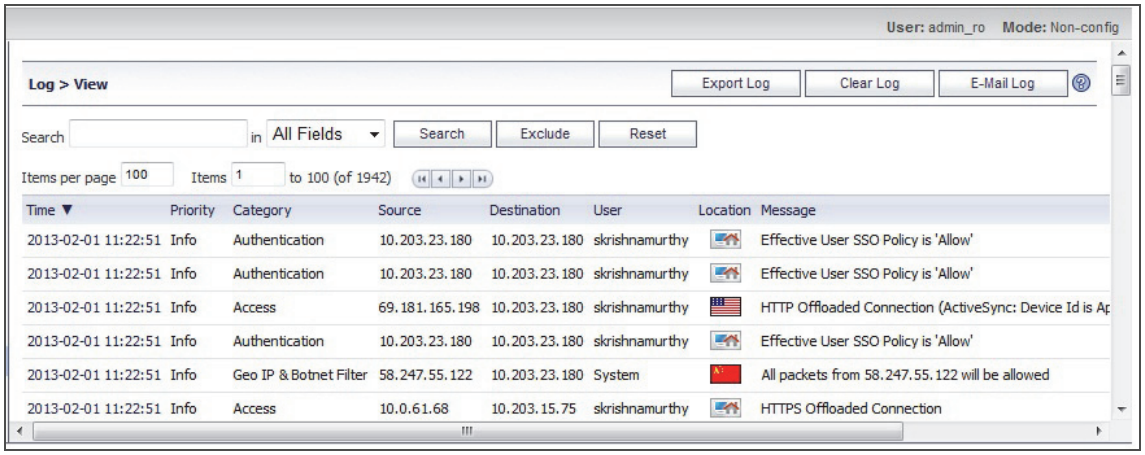
This section provides an overview of the **Log > View** page and a description of the configuration tasks available on this page.


- Log > View Overview on page 398
- Viewing Logs on page 399
- Emailing Logs on page 400

# Log > View Overview

The **Log > View** page allows the administrator to view the SRA event log. The event log can also be automatically sent to an email address for convenience and archiving.

***Figure 56 Log > View***




The **Log > View** page displays log messages in a sortable, searchable table. The SRA appliance can store 250 Kilobytes of log data or approximately 1,000 log messages. Each log entry contains the date and time of the event and a brief message describing the event. Once the log file reaches the log size limit, the log entry is cleared and optionally emailed to the SRA administrator.

The log table size can be specified on the **System > Administration** page under **Default Table Size**.

## Column Views

Each log entry displays the following information:

***Table 22 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 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 may not be displayed for certain events, such as system errors. |
| Destination | The Destination IP address shows the name or IP address of the server or service associated with the event. For example, if a user accessed an intranet Web site through the SRA 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. |

| Column | Description |
|---|---|
| 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:

***Table 23 Log Table Navigation Facilities***

| Navigation Button | Description |
|---|---|
| Find | Enables you to search for a log containing a specified setting based on a criteria type you select in the criteria list. Criteria includes Time, Priority, Source, Destination, and User. Search results list out the results in various orders depending upon the criteria type. |
| Exclude | Enables you to display all log entries but the type specified in the criteria list. |
| Reset | Resets the listing of log entries to their default sequence after you have displayed them in an alternate way, using search buttons. |

## Log > View Buttons

The **Log > View** page also contains options that allow the administrator to send, save log files for external viewing or processing.

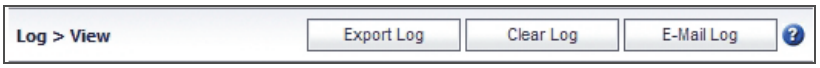



***Table 24 Log rendering options***

| 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 SRA event log. The 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 SRA appliance can store 250 Kilobytes of log data or approximately 1,000 log messages. 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, either to an email address or to an email pager. Each log entry contains the date and time of the event and a brief message describing the event. Once the log file reaches the log size limit, the log entry is cleared and optionally emailed to the SRA administrator.

Each log entry displays the following information:

***Table 25 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 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 may not be displayed for certain events, such as system errors. |
| Destination | Displays the name or IP address of the server or service associated with the event. For example, if a user accessed an Internet Web site through the SRA 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 SRA event log. This feature is useful archiving email and in testing email configuration and email filters for multiple SRA units. To use the **E-mail Log** feature, perform the following tasks:

**Step 1** Navigate to **Log > View**.

**Step 2** Click the **E-mail Log** button.

**Step 3** You will see the message **Log has been successfully sent**.

**Note** If you receive an error message, verify that the administrator email and mail server information has been specified in the **Email Logging and Alerts** section of the **Log > Settings** page. For instructions on configuring the administrator email, refer to Configuring Log Settings on page 402.

# Log > Settings

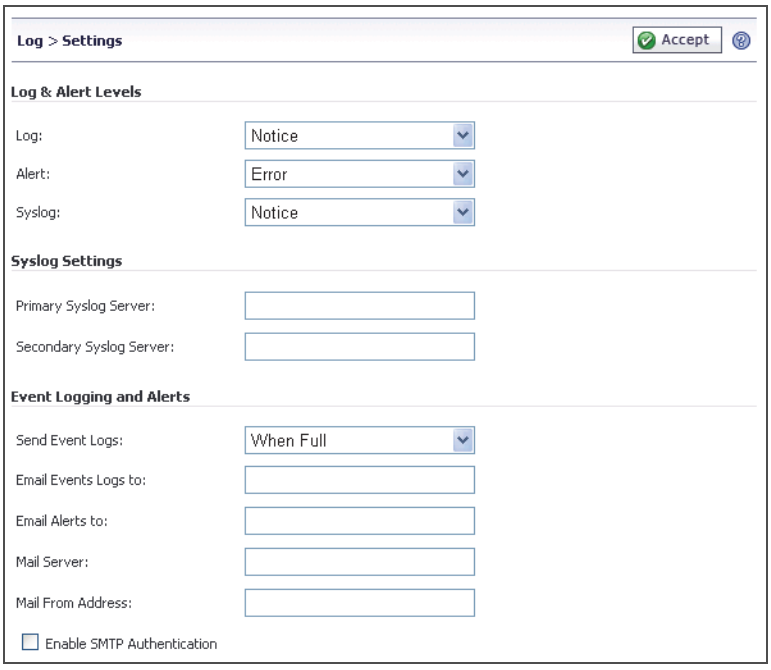
This section provides an overview of the **Log > Settings** page and a description of the configuration tasks available on this page.


- Log > Settings Overview on page 401
- Configuring Log Settings on page 402
- Configuring the Mail Server on page 403

# Log > Settings Overview

The **Log > Settings** page allows the administrator to configure log alert and syslog server settings. Syslog is an industry-standard logging protocol that records system and networking activity. The syslog messages are sent in WELF (WebTrends Enhanced Log Format), so most standard firewalls and networking reporting products can accept and interpret the log files. The syslog service transmits syslog messages to external syslog server(s) listening on UDP port 514.

***Figure 57 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:

**Step 1** To begin configuring event log, syslog and alert settings, navigate to the **Log > Settings** page.

**Step 2** In the **Log & Alert Levels** section, define the severity level of log messages that will be 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 will be logged. For example, if the Error level is selected for the Log service, then all Emergency, Alert, Critical, and Error events will be stored in the internal log file.

**Step 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.

**Step 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.

**Step 5** Designate when log files will be cleared and emailed to an administrator in the **Send Event Logs** field. If the option **When Full** is selected, the event log will be emailed and then cleared from when the log file is full. If **Daily** is selected, select the hour at which to email the event log. If **Weekly** is selected, select the day of the week and the hour. If **Daily** or **Weekly** are chosen, the log file will still be sent if the log file is full before the end of the period. In the **Log > View** page, you can click the **Clear Log** button to delete the current event log. The event log will not be emailed in this case.

**Step 6** To receive event log files via email, enter your full email address (username@domain.com) in the **Email Event Logs to** field in the Event Logging and Alerts region. The event log file will be emailed to the specified email address before the event log is cleared. If this field is left blank, log files will not be emailed.

**Step 7** To receive alert messages via email, enter your full email address (username@domain.com) or an email pager address in the **Email Alerts to** field. An email will be sent to the email address specified if an alert event occurs. If this field is left blank, alert messages will not be emailed.

**Note** Define the type of events that will generate alert messages on the **Log > Categories** page.

**Step 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 will not be emailed.

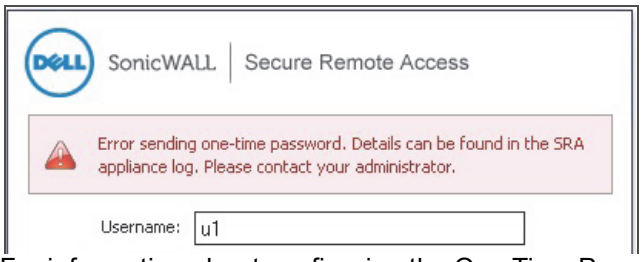
**Step 9** Specify a **Mail From Address** in the corresponding field. This address appears in the from field of all log and alerts emails.

**Step 10** To use SMTP authentication when sending log files, select the **Enable SMTP Authentication** check box. The display will change to expose related fields. Enter the user name, password, and the SMTP port to use. The default port is 25.

**Step 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, perform the following steps:

**Step 1** Log in to the SRA management interface using administrator credentials.

**Step 2** Navigate to **Log > Settings**.

**Step 3** Type the email address where you want logs sent to in the **Email Events Logs to** field.

**Step 4** Type the email address where you want alerts sent to in the **Email Alerts to** field.

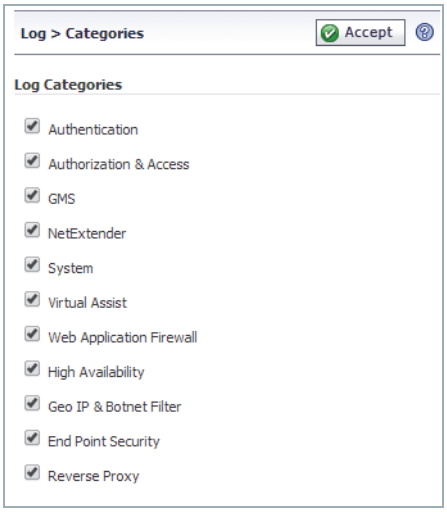
**Step 5** Type the IP address for the mail server you will be using in the **Mail Server** field.

**Step 6** Type the email address for outgoing mail from your SRA appliance in the **Mail From Address** field.

**Step 7** Click **Accept** in the upper right-hand corner.

# Log > Categories

This section provides an overview of the **Log > Categories** page and a description of the various categories of event messages that can be viewed in the log. This page allows for each category to be enabled or disabled by the administrator. This capability can be particularly helpful when used to filter the log during the debug process.




Administrators can enable or disable check boxes for each of the following log categories:

- Authentication
- Authorization & Access
- GMS
- NetExtender
- System
- Virtual Assist
- Web Application Firewall
- High Availability (SRA 4600 and 4200 only)
- Geo IP & Botnet Filter
- End Point Security
- Reverse Proxy

Once all selections have been made, click **Accept** in the upper right corner of the screen to finish configuring the desired categories.

# Log > ViewPoint

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


- Log > ViewPoint Overview on page 405
- Adding a ViewPoint Server on page 405

# Log > ViewPoint Overview

The **Log > ViewPoint** page allows the administrator to add the SRA appliance to a ViewPoint server for installations that have Dell SonicWALL ViewPoint available, or are managed by the Dell SonicWALL 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 SRA appliance and remote access activity
- Generates both real-time and historical reports to provide a complete view of activity through your SRA Appliance
- Enables remote access monitoring
- Enhances network security
- Helps you to anticipate future bandwidth needs

For more information about monitoring your Dell SonicWALL 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 SRA appliance to a ViewPoint server and enable ViewPoint reporting on your SRA appliance, complete the following steps:

**Step 1** Navigate to the **Log > ViewPoint** page in the SRA Web management interface.

If you are using ViewPoint for the first time on this appliance or if you do not have a valid license, the page directs you to the **System > Licenses** page to activate your license.

**Step 2** In the ViewPoint Settings section, click the **Add** button. The Add ViewPoint Server screen displays.

**Step 3** In the Add ViewPoint Server screen, enter the **Hostname or IP Address** of your ViewPoint server.

**Step 4** Enter the **Port** which your ViewPoint server communicates with managed devices.

**Step 5** Click **Accept** at the top of the page to add this server.

**Step 6** To start ViewPoint report logging for the server you just added, select the **Enable ViewPoint** check box.

# 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 406
- Adding an Analyzer Server on page 406

# Log > Analyzer Overview

The **Log > Analyzer** page allows the administrator to add the SRA appliance to an Analyzer server for installations that have Dell SonicWALL Analyzer available, or are managed by the Dell SonicWALL Global Management System (GMS) version 7.0 or higher appliance management software. This feature requires an Analyzer license key.

Dell SonicWALL 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 Dell SonicWALL 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 Dell SonicWALL 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 SRA appliance to an Analyzer server and enable Analyzer reporting on your SRA appliance, complete the following steps:

**Step 1** Navigate to the **Log > Analyzer** page in the SRA Web 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.

**Step 2** In the Analyzer Settings section, click the **Add** button. The Add Analyzer Server screen displays.

**Step 3** In the Add Analyzer Server screen, enter the **Hostname or IP Address** of your Analyzer server.

**Step 4** Enter the **Port** which your Analyzer server communicates with managed devices. The default is 514.

**Step 5** Click **Accept** at the top of the page to add this server.

**Step 6** To start Analyzer report logging for the server you just added, select the **Enable Analyzer** check box.

# Chapter 16

# Virtual Office Configuration

This chapter provides information and configuration tasks specific to the **Virtual Office** page on the Dell SonicWALL SRA Web-based management interface.

# Virtual Office

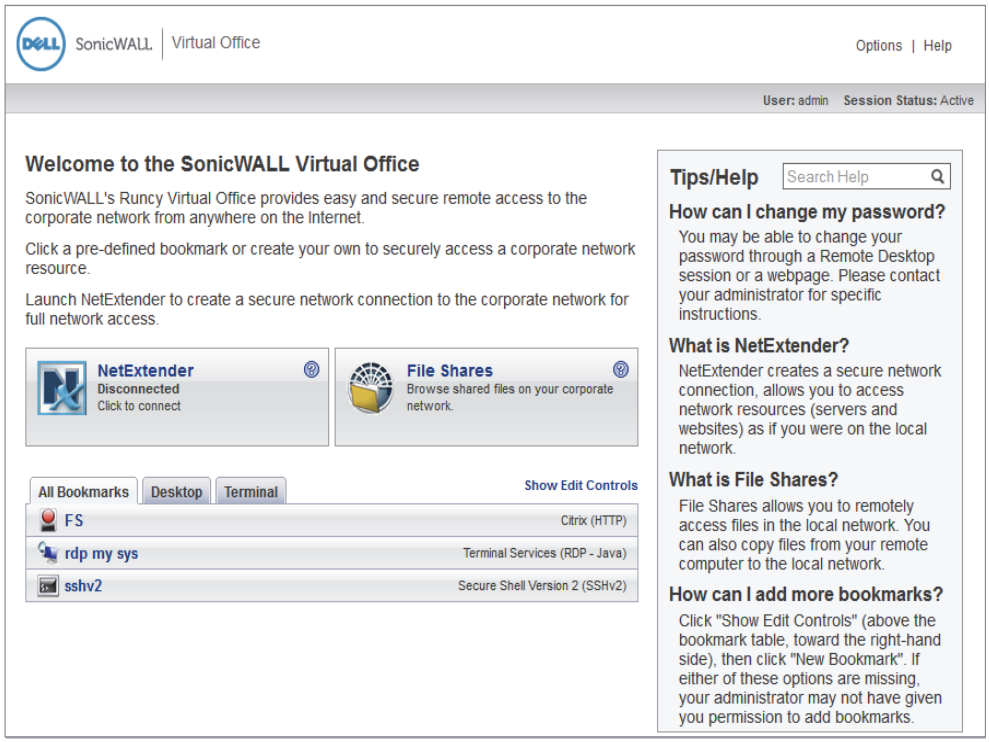
This section provides an overview of the **Virtual Office** page and a description of the configuration tasks available on this page.


- Virtual Office Overview on page 407
- Using the Virtual Office on page 408


## Virtual Office Overview

The **Virtual Office** option is located in the navigation bar of the SRA 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, perform the following tasks:

**Step 1** From the SRA Web-based management interface, click **Virtual Office** in the navigation bar.

**Step 2** A new browser window opens to the Virtual Office home page.

**Note** When you launch the Virtual Office from the Web-based management interface, you will be automatically logged in with your administrator credentials.

The **Logout** button will not appear in the Virtual Office when you are logged on as an administrator. To log out, you must close the browser window.

**Step 3** From the Virtual Office home page, you can:

- Launch and install NetExtender
- Use File Shares
- Launch a Virtual Assist session
- Add and configure bookmarks
- Add and configure bookmarks for offloaded portals
- Follow bookmark links
- Import certificates
- Get Virtual Office help
- Configure a system for 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 Dell SonicWALL SRA User's Guide, available on the Secure Remote Access pages of the Dell SonicWALL support Web site at http://www.sonicwall.com/us/Support.html.

# Appendix A

# Online Help

This appendix describes how to use the **Online Help** on the Dell SonicWALL SRA Web-based management interface. This appendix also contains information about context-sensitive help.

# Online Help Button

The **Online Help** button is located in upper right corner of the SRA management interface.

The **Online Help** button launches the online help in a separate Web browser. The **Online Help** button links to the main page of the online help document.

## Using Context Sensitive Help

Context-sensitive help is available on most pages of the SRA 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 SRA 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 management interface. When you hover your mouse cursor over one of these help icons, a tooltip is displayed containing important information about configuring the associated option.

# Appendix B

# Configuring the SRA Appliance with a Third-Party Gateway

This appendix shows methods for configuring various third-party firewalls for deployment with a SRA appliance.

This appendix contains the following sections:


- Cisco PIX Configuration for SRA Appliance Deployment on page 411
- Linksys WRT54GS on page 417
- WatchGuard Firebox X Edge on page 418
- NetGear FVS318 on page 420
- Netgear Wireless Router MR814 SSL configuration on page 422
- Check Point AIR 55 on page 423


# Cisco PIX Configuration for SRA Appliance Deployment

## Before you Begin

Make sure you have a management connection to the PIX's console port, or the ability to Telnet/SSH into one of the PIX's interfaces. You will need to know the PIX's global and enable-level passwords in order to access the device and issue changes to the configuration. If you do not have these, contact your network administrator before continuing.

Dell SonicWALL recommends updating the PIX's OS to the most recent version if your PIX can support it. This document was validated on a Cisco PIX 515e running PIX OS 6.3.5 and is the recommended version for interoperation with a SRA appliance. You will need a valid Cisco SmartNET maintenance contract for your Cisco PIX and a CCO login to obtain newer versions of the PIX OS.

**Note** The WAN/DMZ/LAN IP addresses used in the deployment method examples below are not valid and will need to be modified to reflect your networking environment.

## Management Considerations for the Cisco Pix

Both deployment methods described below use the PIX's WAN interface IP address as the means of external connectivity to the internal SRA appliance. The PIX has the ability to be managed via HTTP/S, but cannot have their default management ports (80,443) reassigned in the recommended PIX OS version. Because of this, the HTTP/S management interface must be deactivated. To deactivate the HTTP/S management interface, issue the command 'clear http'.

**Note** If you have a separate static WAN IP address to assign to the SRA appliance, you do not have to deactivate the HTTP/S management interface on the PIX.

# Method One – SRA Appliance on LAN Interface

**Step 1** From a management system, log into the SRA appliance's management interface. By default the management interface is X0 and the default IP address is 192.168.200.1.

**Step 2** Navigate to the **Network > Interfaces** page and click on the configure icon for the X0 interface. On the pop-up that appears, change the X0 address to **192.168.100.2** with a mask of **255.255.255.0**. When done, click on the **OK** button to save and activate the change.

**Step 3** Navigate to the **Network > Routes** page and change the Default Gateway to **192.168.100.1** When done, click on the **Accept** button in the upper-right-hand corner to save and activate the change.

**Step 4** Navigate to the **NetExtender > Client Addresses** page. You will need to enter a range of IP addresses for the 192.168.100.0/24 network that are not in use on your internal LAN network; if your network has an existing DHCP server or the PIX is running a DHCP server on its internal interface, you will need to make sure not to conflict with these addresses. For example: enter

**192.168.100.201** in the field next to **Client Address Range Begin:**, and enter **192.168.100.249** in the field next to **Client Address Range End:**. When done, click on the **Accept** button in the upper-right-hand corner to save and activate the change.

**Step 5** Navigate to the **NetExtender > Client Routes** page. Add a client route for **192.168.100.0**. If there is an entry for **192.168.200.0**, delete it.

**Step 6** Navigate to the **Network > DNS** page and enter your internal network's DNS addresses, internal domain name, and WINS server addresses. These are critical for NetExtender to function correctly. When done, click on the **Accept** button in the upper-right-hand corner to save and activate the change.

**Step 7** Navigate to the **System > Restart** page and click on the **Restart…** button.

**Step 8** Install the SRA appliance's X0 interface on the LAN network of the PIX. Do not hook any of the appliance's other interfaces up.

**Step 9** Connect to the PIX's management CLI via console port, telnet, or SSH and enter configure mode.

**Step 10** Issue the command **'clear http'** to shut off the PIX's HTTP/S management interface.

**Step 11** Issue the command '**access-list sslvpn permit tcp any host x.x.x.x eq www'** (replace x.x.x.x with the WAN IP address of your PIX)

**Step 12** Issue the command **'access-list sslvpn permit tcp any host x.x.x.x eq https'** (replace x.x.x.x with the WAN IP address of your PIX)

**Step 13** Issue the command '**static (inside,outside) tcp x.x.x.x www 192.168.100.2 www netmask 255.255.255.255 0 0'** (replace x.x.x.x with the WAN IP address of your PIX)

**Step 14** Issue the command **'static (inside,outside) tcp x.x.x.x https 192.168.100.2 https netmask 255.255.255.255 0 0'** (replace x.x.x.x with the WAN IP address of your PIX)

**Step 15** Issue the command **'access-group sslvpn in interface outside'**

**Step 16** Exit config mode and issue the command **'wr mem'** to save and activate the changes.

**Step 17** From an external system, attempt to connect to the SRA appliance using both HTTP and HTTPS. If you cannot access the SRA appliance, check all steps above and test again.

**Final Config Sample – Relevant Programming in Bold:**

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security4
enable password SqjOo0II7Q4T90ap encrypted
passwd SqjOo0II7Q4T90ap encrypted
hostname tenaya
domain-name vpntestlab.com
clock timezone PDT -8
clock summer-time PDT recurring
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
```

```
fixup protocol tftp 69
names
access-list sslvpn permit tcp any host 64.41.140.167 eq www
access-list sslvpn permit tcp any host 64.41.140.167 eq https
pager lines 24
logging on
logging timestamp
logging buffered warnings
logging history warnings
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 64.41.140.167 255.255.255.224
ip address inside 192.168.100.1 255.255.255.0
no ip address dmz
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0 0 0
static (inside,outside) tcp 64.41.140.167 www 192.168.100.2 www netmask
255.255.255.255 0 0
static (inside,outside) tcp 64.41.140.167 https 192.168.100.2 https netmask
255.255.255.255 0 0
access-group sslvpn in interface outside
route outside 0.0.0.0 0.0.0.0 64.41.140.166 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
ntp server 192.43.244.18 source outside prefer
no snmp-server location
no snmp-server contact
snmp-server community SF*&^SDG
no snmp-server enable traps
floodguard enable
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 15
ssh 0.0.0.0 0.0.0.0 outside
ssh 0.0.0.0 0.0.0.0 inside
ssh timeout 15
console timeout 20
dhcpd address 192.168.100.101-192.168.100.199 inside
dhcpd dns 192.168.100.10
dhcpd lease 600
dhcpd ping_timeout 750
dhcpd domain vpntestlab.com
dhcpd enable inside
terminal width 80
banner motd Restricted Access. Please log in to continue.
Cryptochecksum:422aa5f321418858125b4896d1e51b89
: end
tenaya#
```

# Method Two – 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 will be using the default numbering scheme of the SRA appliance.

---

**Step 1** From a management system, log into the SRA appliance's management interface. By default the management interface is X0 and the default IP address is 192.168.200.1.

**Step 2** Navigate to the **Network > Routes** page and make sure the Default Gateway is set to 192.168.200.2 When done, click on the **Accept** button in the upper-right-hand corner to save and activate the change.

**Step 3** Navigate to the **NetExtender > Client Addresses** page. Enter **192.168.200.201** in the field next to **Client Address Range Begin**:, and enter **192.168.200.249** in the field next to **Client Address Range End**:'. When done, click on the **Accept** button in the upper-right-hand corner to save and activate the change.

**Step 4** Navigate to the **NetExtender > Client Routes** page. Add a client route for **192.168.100.0** and **192.168.200.0**.

**Step 5** Navigate to the **Network > DNS** page and enter your internal network's DNS addresses, internal domain name, and WINS server addresses. These are critical for NetExtender to function correctly. When done, click on the **Accept** button in the upper-right-hand corner to save and activate the change.

**Step 6** Navigate to the **System > Restart** page and click on the **Restart…** button.

**Step 7** Install the SRA appliance's X0 interface on the unused DMZ network of the PIX. Do not hook any of the appliance's other interfaces up.

**Step 8** Connect to the PIX's management CLI via console port, telnet, or SSH and enter configure mode.

**Step 9** Issue the command **'clear http'** to shut off the PIX's HTTP/S management interface.

**Step 10** Issue the command '**interface ethernet2 auto'** (or whatever interface you will be using)

**Step 11** Issue the command '**nameif ethernet2 dmz security4'** (or whatever interface you will be using)

**Step 12** Issue the command '**ip address dmz 192.168.200.2 255.255.255.0'**

**Step 13** Issue the command **'nat (dmz) 1 192.168.200.0 255.255.255.0 0 0'**

**Step 14** Issue the command '**access-list sslvpn permit tcp any host x.x.x.x eq www'** (replace x.x.x.x with the WAN IP address of your PIX)

**Step 15** Issue the command **'access-list sslvpn permit tcp any host x.x.x.x eq https'** (replace x.x.x.x with the WAN IP address of your PIX)

**Step 16** Issue the command '**access-list dmz-to-inside permit ip 192.168.200.0 255.255.255.0 192.168.100.0 255.255.255.0'**

**Step 17** Issue the command '**access-list dmz-to-inside permit ip host 192.168.200.1 any'**

**Step 18** Issue the command **'static (dmz,outside) tcp x.x.x.x www 192.168.200.1 www netmask 255.255.255.255 0 0'** (replace x.x.x.x with the WAN IP address of your PIX)

**Step 19** Issue the command **'static (dmz,outside) tcp x.x.x.x https 192.168.200.1 https netmask 255.255.255.255 0 0'** (replace x.x.x.x with the WAN IP address of your PIX)

**Step 20** Issue the command **'static (inside,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0 0 0'**

**Step 21** Issue the command **'access-group sslvpn in interface outside'**

**Step 22** Issue the command **'access-group dmz-to-inside in interface dmz'**

**Step 23** Exit config mode and issue the command **'wr mem'** to save and activate the changes.

**Step 24** From an external system, attempt to connect to the SRA appliance using both HTTP and HTTPS. If you cannot access the SRA appliance, check all steps above and test again.

**Final Config Sample – Relevant Programming in Bold:**

PIX Version 6.3(5)

```
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security4
enable password SqjOo0II7Q4T90ap encrypted
passwd SqjOo0II7Q4T90ap encrypted
hostname tenaya
domain-name vpntestlab.com
clock timezone PDT -8
clock summer-time PDT recurring
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list sslvpn permit tcp any host 64.41.140.167 eq www
access-list sslvpn permit tcp any host 64.41.140.167 eq https
access-list dmz-to-inside permit ip 192.168.200.0 255.255.255.0 192.168.100.0
255.255.255.0
access-list dmz-to-inside permit ip host 192.168.200.1 any
pager lines 24
logging on
logging timestamp
logging buffered warnings
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 64.41.140.167 255.255.255.224
ip address inside 192.168.100.1 255.255.255.0
ip address dmz 192.168.200.2 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0 0 0
nat (dmz) 1 192.168.200.0 255.255.255.0 0 0
static (dmz,outside) tcp 64.41.140.167 www 192.168.200.1 www netmask 255.255.255.255 0
0
static (dmz,outside) tcp 64.41.140.167 https 192.168.200.1 https netmask
255.255.255.255 0 0
static (inside,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0 0 0
access-group sslvpn in interface outside
access-group dmz-to-inside in interface dmz
route outside 0.0.0.0 0.0.0.0 64.41.140.166 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
```

```
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
ntp server 192.43.244.18 source outside prefer
floodguard enable
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 15
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 15
console timeout 20
dhcpd address 192.168.100.101-192.168.100.199 inside
dhcpd dns 192.168.100.10
dhcpd lease 600
dhcpd ping_timeout 750
dhcpd domain vpntestlab.com
dhcpd enable inside
terminal width 80
banner motd Restricted Access. Please log in to continue.
Cryptochecksum:81330e717bdbfdc16a140402cb503a77
: end
```

# Linksys WRT54GS

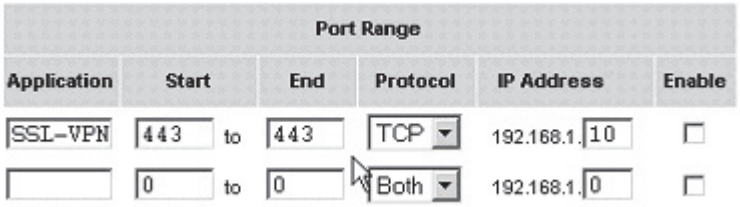
The SRA appliance should be configured on the LAN switch of the Linksys wireless router. This guide assumes that your Linksys is assigned a single WAN IP, via DHCP by the cable ISP and is using the default LAN IP address scheme of 192.168.1.0/24.

**Note** Version 2.07.1 Firmware or newer is recommended for this setup.

To configure your Linksys for operation with the SRA appliance, you must forward the SSL (443) port to the IP address of the SRA appliance.

**Step 1** Login to the Linksys device.

**Step 2** Navigate to the **Applications & Gaming** tab.




**Step 3** Enter the following information:

| | | |
|---|---|---|
| Application | 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 Dell SonicWALL SRA application uses TCP |
| IP Address | 192.168.1.10 | The IP address assigned to the SRA appliance. |
| Enable | Checked | Select the check box to enable the SSL port forwarding |

**Step 4** With the configuration complete, click the **Save Settings** button on the bottom of the page.

The Linksys is now ready for operations with the SRA appliance.

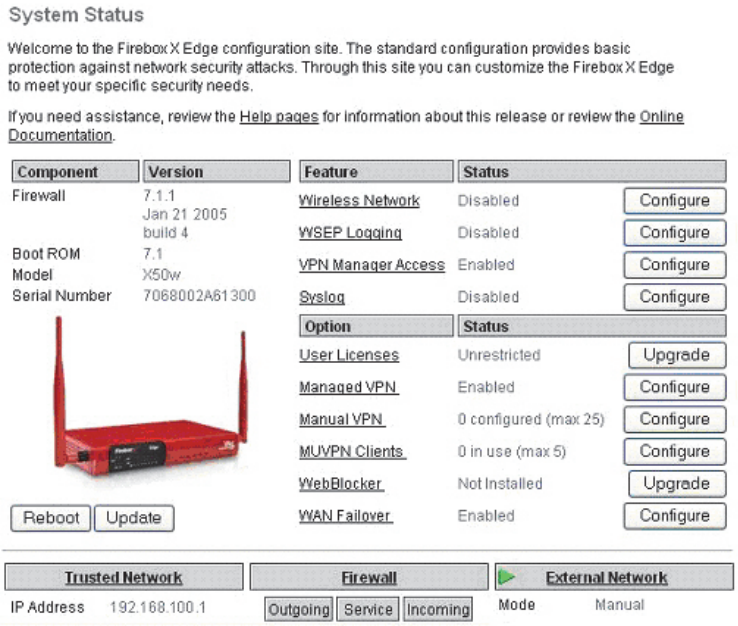
# WatchGuard Firebox X Edge

This guide assumes that your WatchGuard Firebox X Gateway is configured with an IP of 192.168.100.1 and your SRA appliance is configured with an IP of 192.168.100.2.

**Note** The steps below are similar for WatchGuard SOHO6 series firewall.

Before you get started, take note of which port the WatchGuard is using for management. If the WatchGuard is not being managed on HTTPS (443), perform the following steps. If the WatchGuard is being managed on HTTPS (443) you'll need to first review the notes within this guide.

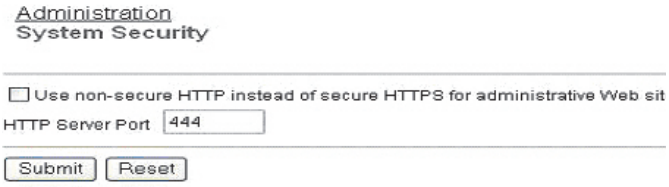
**Step 1** Open browser and enter the IP address of the WatchGuard Firebox X Edge appliance (i.e. 192.168.100.1). Once successful, you'll be brought to the "System Status" page (below).




**Step 2** If the WatchGuard's management interface is already configured to accept HTTPS on port 443 you will need to change the port in order to be able to manage both the Dell SonicWALL SRA and WatchGuard appliances.

**Step 3** Navigate to **Administration > System Security**.

***Figure 1 WatchGuard Administration > System Security Dialog Box***

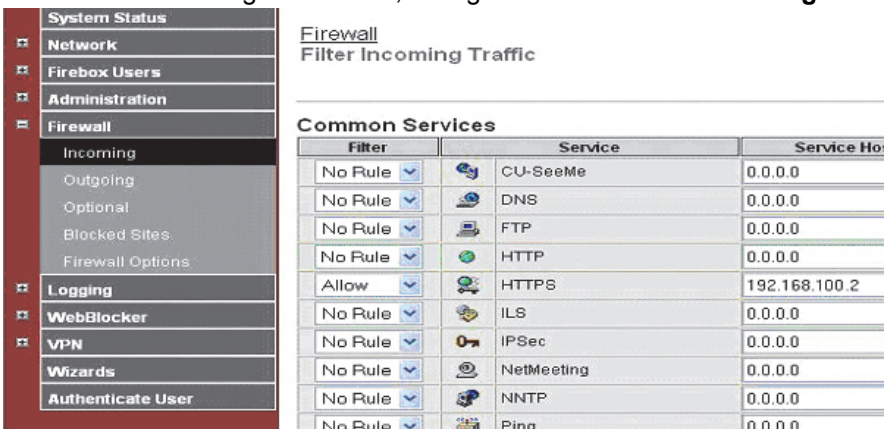



**Step 4** Clear the **Use non-secure HTTP instead of secure HTTPS for administrative Web site** check box.

**Step 5** Change the **HTTP Server Port** to 444 and click the **Submit** button.

The WatchGuard will now be managed from the WAN on port 444. It should be accessed as follows: https://<watchguard wan ip>:444

**Step 6** In the left-hand navigation menu, Navigate to **Firewall > Incoming**.




**Step 7** For the **HTTPS Service**, set **Filter** to Allow and enter the WAN IP of the SRA appliance (192.168.100.2) in the **Service Host** field.

**Step 8** Click the Submit button at the bottom of the page.

Your Watchguard Firebox X Edge is now ready for operations with the SRA appliance.

# NetGear FVS318

This guide assumes that your NetGear FVS318 Gateway is configured with an IP of 192.168.100.1 and your SRA appliance is configured with an IP of 192.168.100.2.

---

**Step 1** Click **Remote Management** from the left-hand index of your Netgear management interface.

In order for the SRA appliance to function with your Netgear gateway device, you must verify that the NetGear's management port will not conflict with the management port used by the SRA appliance.

**Step 2** Clear the **Allow Remote Management** box.

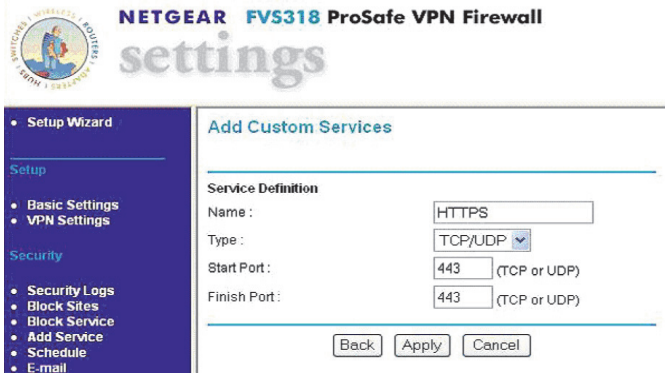
**Step 3** Click the **Accept** button to save changes.

**Note** If Remote Management of the NetGear is desired, you must leave the box checked and change the default port (8080 is recommended)

**Step 4** Navigate to **Add Service** in the left-hand navigation.

**Step 5** Click the **Add Custom Service** button.

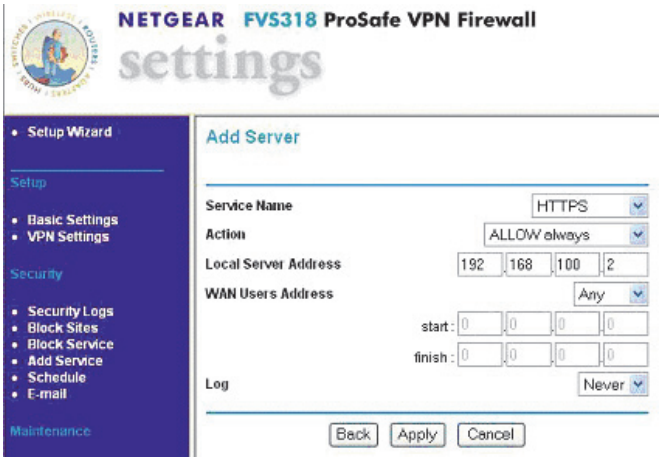
**Step 6** To create a service definition, enter the following information:




| | |
|---|---|
| Name | HTTPS |
| Type | TCP/UDP |
| Start Port | 443 |
| Finish Port | 443 |

**Step 7** Navigate to **Ports** in the left-hand navigation.

**Step 8** Click the **Add** button.




**Step 9** Select HTTPS from the **Service Name** drop-down list.

**Step 10** Select ALLOW always in the **Action** drop-down list.

**Step 11** Enter the WAN IP address of the SRA appliance (ex.192.168.100.2) in the **Local Server Address** field.

**Step 12** Click Accept to save changes.

Your Netgear gateway device is now ready for operations with the SRA appliance.

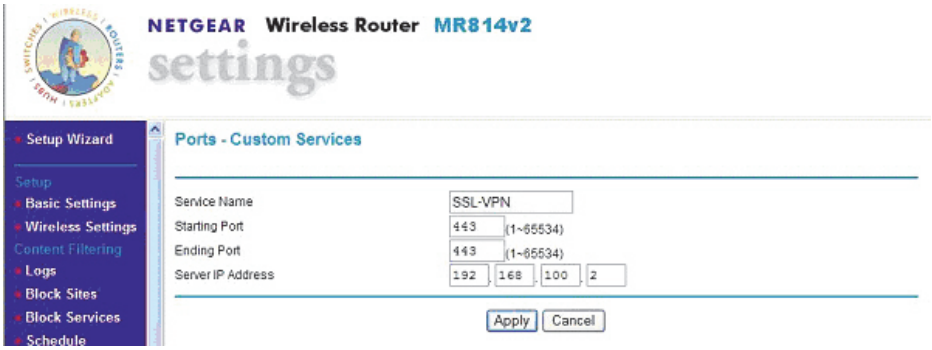
# Netgear Wireless Router MR814 SSL configuration

This guide assumes that your NetGear Wireless Router is configured with an IP of 192.168.100.1 and your SRA appliance is configured with an IP of 192.168.100.2.

**Step 1** Navigate to **Advanced > Port Management** in the left-hand index of your Netgear management interface.

**Step 2** Click the **Add Custom Service** button in the middle of the page.

**Step 3** Enter a service name in the **Service Name** field (ex. SRA)




**Step 4** Enter **443** in the **Starting Port** field.

**Step 5** Enter **443** in the **Ending Port** field.

**Step 6** Enter the WAN IP address of the SRA appliance (ex.192.168.100.2) in the **Local Server Address** field.

**Step 7** Click the **Accept** button

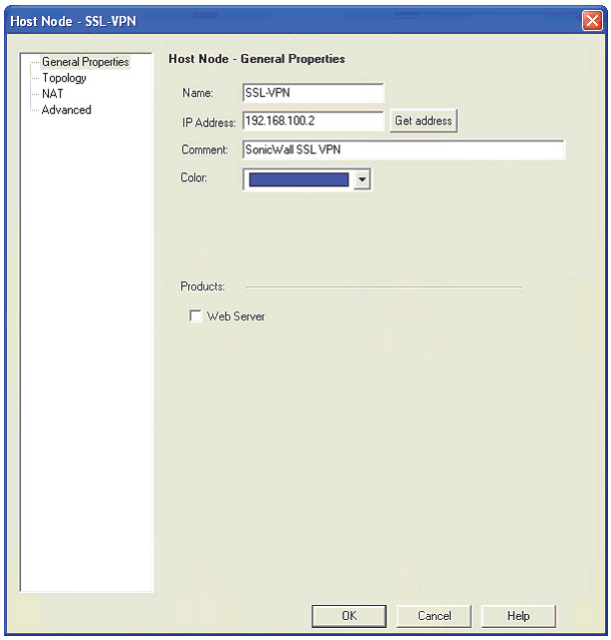
Your Netgear wireless router is now ready for operations with the SRA appliance.

# Check Point AIR 55

## Setting up an 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”.

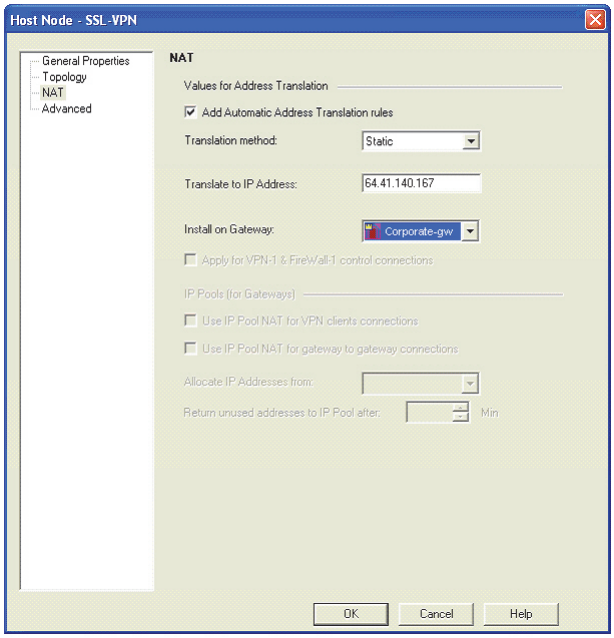
***Figure 58 Check Point Host Node Object Dialog Box***




**Note** The object is defined as existing on the internal network. Should you decide to locate the SRA appliance on a secure segment (sometimes known as a demilitarized zone) then subsequent firewall rules will have to pass the necessary traffic from the secure segment to the internal network.

Next, select the **NAT** tab for the object you have created.

***Figure 59 Check Point NAT Properties Dialog Box***




Here you will enter the external IP address (if it is not the existing external IP address of the firewall). The translation method to be selected is **static**. Clicking **OK** will automatically create the necessary NAT rule shown below.

***Figure 60 Check Point NAT Rule Window***

# Static Route

Most installations of Check Point AIR55 require a static route. This route will send all traffic from the public IP address for the 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 will automatically add an ARP entry for a secondary external IP address (the public IP address of the 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 SRA appliance.

***Figure 61 Check Point Policy Rule Window***

Again, should the SRA appliance be located on a secure segment of the Check Point firewall, a second rule allowing the relevant traffic to flow from the SRA appliance to the internal network will be necessary.

# Appendix C

# Use Cases

This appendix provides the following use cases:


- Importing CA Certificates on Windows on page 427
- Creating Unique Access Policies for AD Groups on page 431


# Importing CA Certificates on Windows

Two certificates are imported in this use case, a goDaddy certificate and a server certificate. See the following sections:

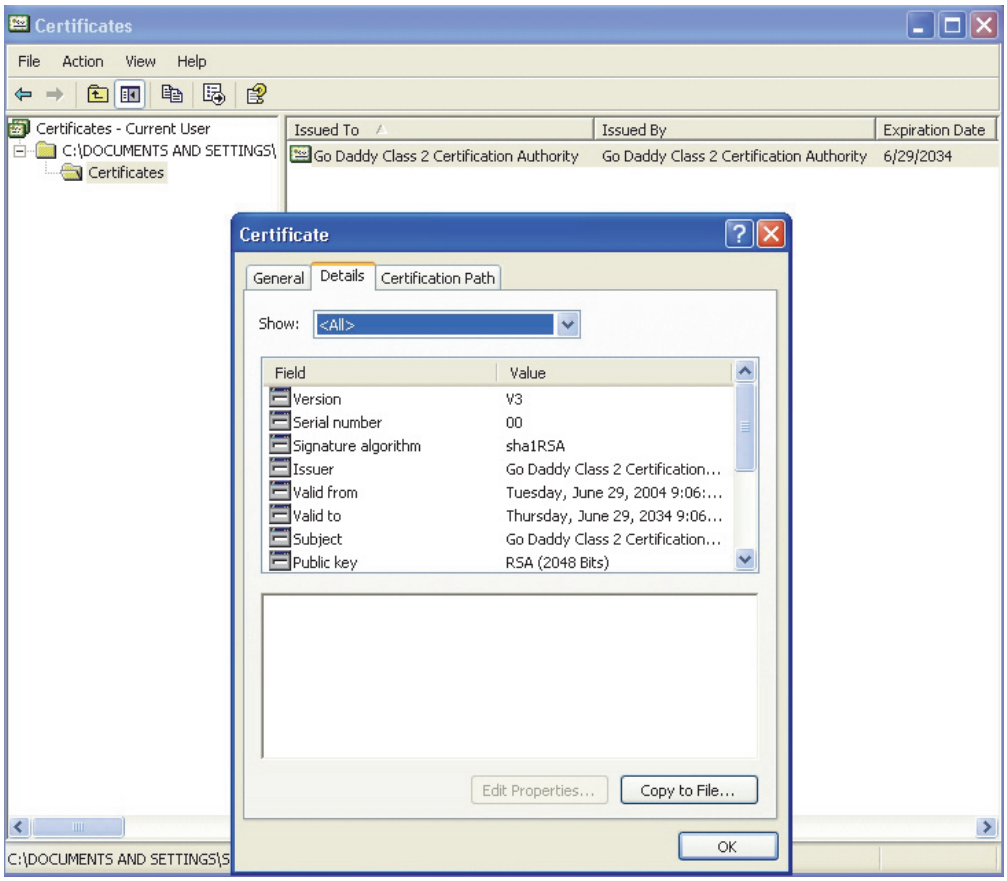

- Importing a goDaddy Certificate on Windows on page 427
- Importing a Server Certificate on Windows on page 430


## 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 SRA appliance.

**Step 1** Double-click on the **goDaddy.p7b** file to open the Certificates window, and navigate to the goDaddy certificate.
The .p7b format is a PKCS#7 format certificate file, a very common certificate format.

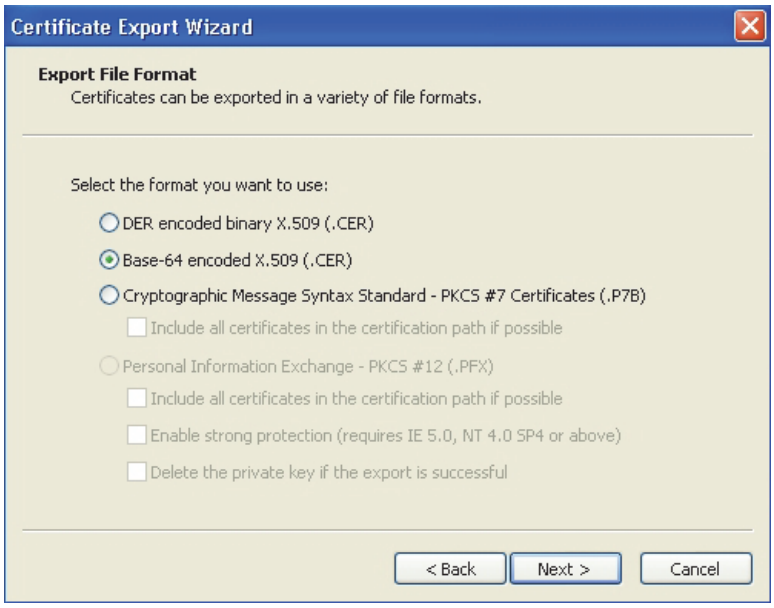
**Step 2** Double-click the certificate file and select the **Details** tab.




**Step 3** Click **Copy to File**. The Certificate Export Wizard launches.

**Step 4** In the Certificate Export Wizard, click **Next**.

**Step 5** Select **Base-64 encoded X.509 (.CER)** and then click **Next**.




**Step 6** In the File to Export screen, type the file name in as **goDaddy.cer** and then click **Next**.

**Step 7** In the Completing the Certificate Export Wizard screen, verify the path and format and then click **Finish**.

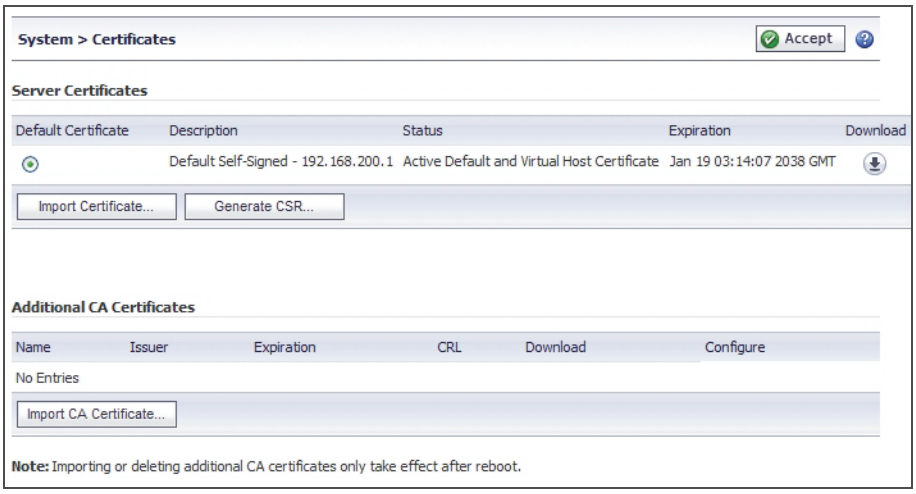
**Step 8** Click **OK** in the confirmation dialog box.

The certificate is exported in base-64 encoded format. You can view it in a text editor.

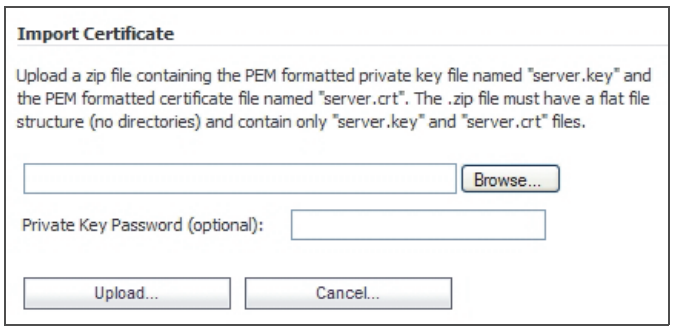
goDaddy.cer

```
-----BEGIN CERTIFICATE-----
MIIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEh
MB8GA1UEChMYVGhlIEdvIERhZGR5IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBE
YWRkeSBDbGFzcyAyIEN1cnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTA0MDYyOTE3
MDYyMFoXDTM0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRo
ZSBHbyBEYWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3Mg
MiBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTCCASAwDQYJKoZIhvcNAQEBBQADggEN
ADCCAQgCggEBAN6d1+pXGEmhW+vXX0iG6r7d/+TvZxz0ZWizV3GgXne77ZtJ6XCA
PVYYYwhv2vLM0D9/AlQiVBDYsoHUwHU9S3/Hd8M+eKsaA7Ugay9qK7HFiH7Eux6w
wdhFJ2+qN1j3hybX2C32qRe3H3I2TqYXP2WYktsqbl2i/ojgC95/5Y0V4evLOtXi
EqITLdiOr18SPaAIBQi2XKVlOARFmR6jYGB0xUGlcmIbYsUfb18aQr4CUWWoriMY
avx4A6lNf4DD+qta/KFApMoZFv6yyO9ecw3ud72a9nmYvLEHZ6IVDd2gWMZEewo+
YihfukEHU1jPEX44dMX4/7VpkI+EdOqXG68CAQOjgcAwgb0wHQYDVR0OBBYEFNLE
sNKR1EwRcbNhyz2h/t2oatTjMIGNBgNVHSMEgYUwgYKAFNLEsNKR1EwRcbNhyz2h
/t2oatTjoWekZTBjMQswCQYDVQQGEwJVUzEhMB8GA1UEChMYVGhlIEdvIERhZGR5
IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBEYWRkeSBDbGFzcyAyIEN1cnRpZmlj
YXRpb24gQXV0aG9yaXR5ggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQAD
ggEBADJL87LKPpH8EsahB4yOd6AzBhRckB4Y9wimPQoZ+YeAEW5p5JYXMP80kWNy
OO7MHAGjHZQopDH2esRU1/blMVgDoszOYtuURXO1v0XJJLXVggKtI3lpjbi2Tc7P
TMozI+gciKqdi0FuFskg5YmezTvacPd+mSYgFFQlq25zheabIZ0KbIIOqPjCDPoQ
HmyW74cNxA9hi63ugyuV+I6ShHI56yDqg+2DzZduCLzrTia2cyvk0/ZM/iZx4mER
dEr/VxqHD3VILs9RaRegAhJhldXRQLIQTO7ErBBDpqWeCtWVYpoNz4iCxTIM5Cuf
ReYNnyicsbkqWletNw+vHX/bvZ8=
-----END CERTIFICATE-----
```

**Step 9** In the SRA management interface, navigate to **System > Certificates**.

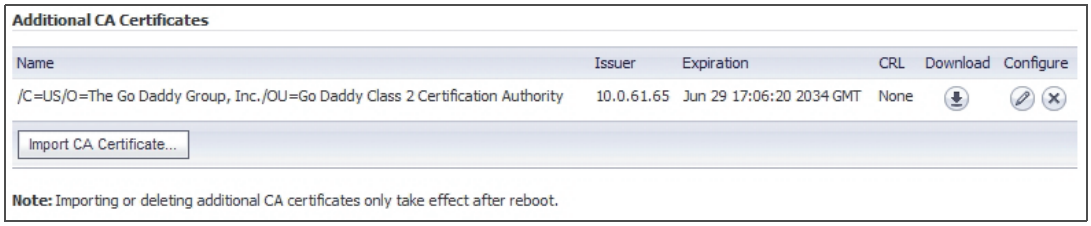



**Step 10** In the **Additional CA Certificates** section, click **Import CA Certificate**. The Import Certificate window appears.




**Step 11** In the Import Certificate window, click **Browse** and navigate to the **goDaddy.cer** file on your Windows system and double-click it.

**Step 12** Click **Upload**. The certificate will be listed in the **Additional CA Certificates** table.




**Step 13** Navigate to **System > Restart** and restart the SRA appliance for the CA certificate to take effect.

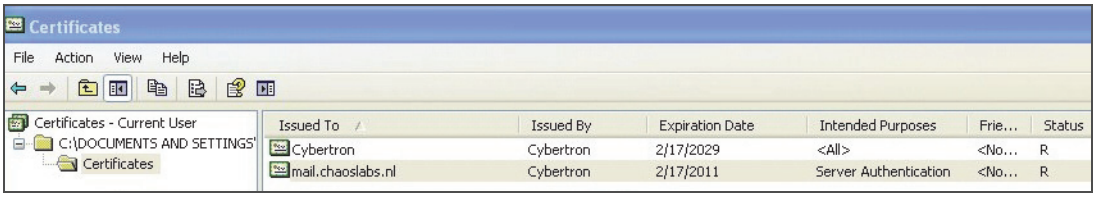
# Importing a Server Certificate on Windows

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.

**Step 1** Double-click on the **mail.chaoslabs.nl.pb7** file and navigate to the certificate.




**Step 2** Double-click the certificate file and select the **Details** tab.

**Step 3** Click **Copy to File**.

**Step 4** In the Certificate Export Wizard, select **Base-64 encoded X.509 (.CER)**.

**Step 5** Click **Next** and save the file as **server.crt** on your Windows system.

The certificate is exported in base-64 encoded format.

**Step 6** Add the server.crt file to a .zip file.

**Step 7** Separately save the private key in base-64 format as **server.key**.

**Step 8** Add the **server.key** file to the .zip file that contains **server.crt**.

**Step 9** Upload the .zip file to the server as a Server Certificate.

# Creating Unique Access Policies for AD Groups

In this use case, we add Outlook Web Access (OWA) resources to the 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 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.

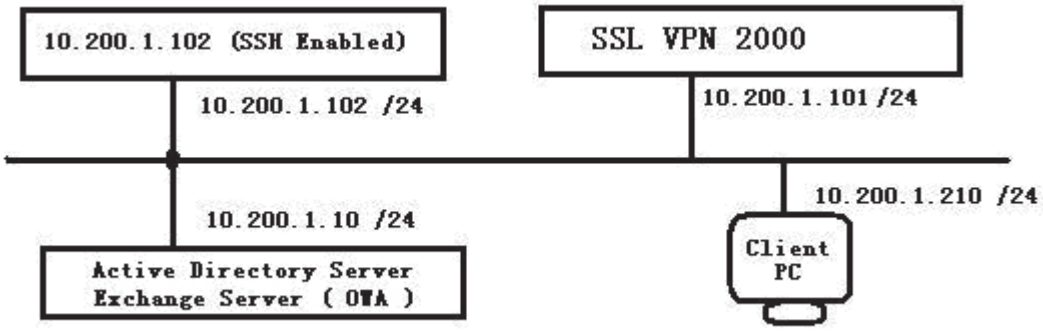
When importing a user from AD, the user will be placed into the local SRA group with which they have the most AD groups in common. For example: Bob belongs to the Users, Administrators, and Engineering AD groups. If one SRA group is associated with Users, and another is associated with both Administrators and Engineering, Bob will be assigned to the SRA 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 Dell SonicWALL SRA firmware supports group-based access policies by configuring the following:

- Allow Acme Group in Active Directory to access the 10.200.1.102 server using SSH
- Allow Mega Group in Active Directory to access Outlook Web Access (OWA) at 10.200.1.10
- Allow IT Group in Active Directory to access both SSH and OWA resources defined above
- Deny access to these resources to all other groups

This example configuration is provided courtesy of Vincent Cai, June 2008.

**Figure C:1 Network Topology**




Perform the tasks in order of the following sections:

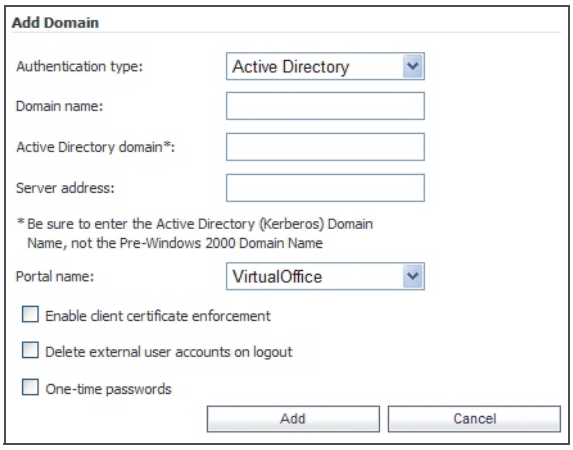
- Creating the Active Directory Domain on page 432
- Adding a Global Deny All Policy on page 433
- Creating Local Groups on page 434
- Adding the SSHv2 PERMIT Policy on page 437
- Adding the OWA PERMIT Policies on page 437
- Verifying the Access Policy Configuration on page 439

# Creating the Active Directory Domain

This section describes how to create the SRA Local Domain, SNWL_AD. SNWL_AD is associated with the Active Directory domain of the OWA server.

**Step 1** Log in to the SRA management interface and navigate to the **Portals > Domains** page.

**Step 2** Click **Add Domain**. The Add Domain window appears.




**Step 3** In the **Authentication type** drop-down list, select **Active Directory**.

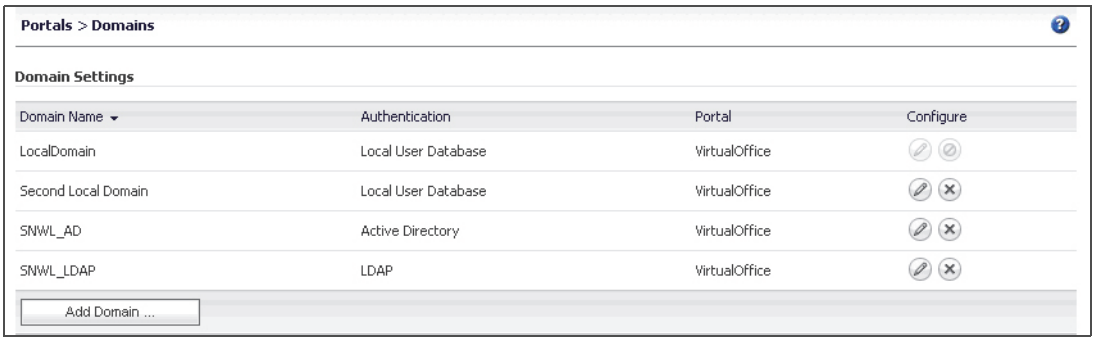
**Step 4** In the **Domain name** field, type **SNWL_AD**.

**Step 5** In the **Active Directory domain** field, type the AD domain name, **in.loraxmfg.com**.

**Step 6** In the **Server address** field, type the IP address of the OWA server, **10.200.1.10**.

**Step 7** Click **Add**.

**Step 8** View the new domain in the **Portals > Domains** page.

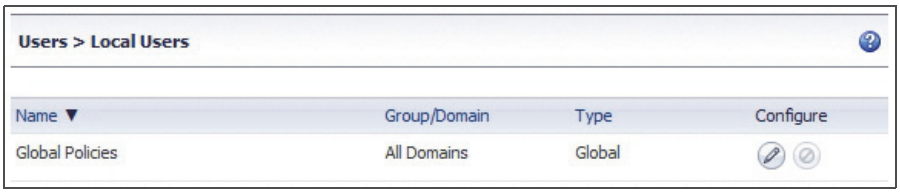



# Adding a Global Deny All Policy

This procedure creates a policy that denies access to the OWA resources to all groups, except groups configured with an explicit Permit policy.

The SRA default policy is **Allow All**. In order to have more granular control, we add a **Deny All** policy here. Later, we can add **Permit** policies for each group, one at a time.

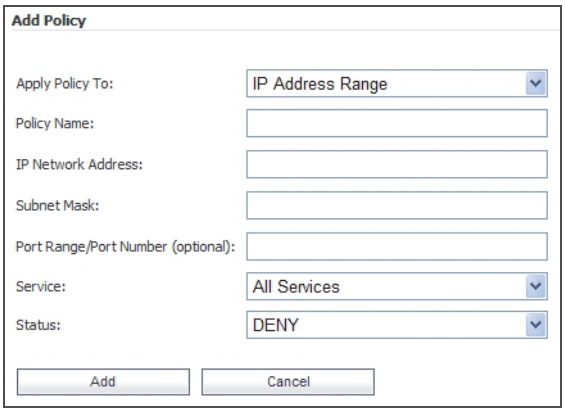
**Step 1** Navigate to the **Users > Local Users** page.




**Step 2** Click the **Configure** button in the **Global Policies** row. The **Edit Global Policies** window appears.

**Step 3** In the **Edit Global Policies** window, click the **Policies** tab.

**Step 4** Click **Add Policy**. The Add Policy window appears.




**Step 5** Select **IP Address Range** from the **Apply Policy To** drop-down list.

**Step 6** In the **Policy Name** field, type the descriptive name **Deny All**.

**Step 7** In the **IP Network Address** field, type the network address, **10.200.1.0**.

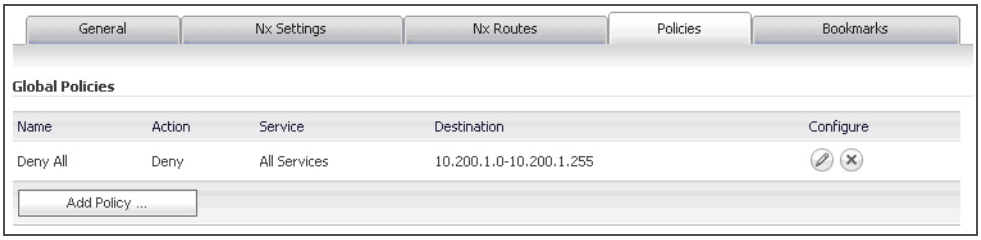
**Step 8** In the **Subnet Mask** field, type the mask in decimal format, **255.255.255.0**.

**Step 9** In the **Service** drop-down list, select **All Services**.

**Step 10** In the **Status** drop-down list, select **DENY**.

**Step 11** Click **Add**.

**Step 12** In the **Edit Global Policies** window, verify the **Deny All** policy settings and then click **OK**.

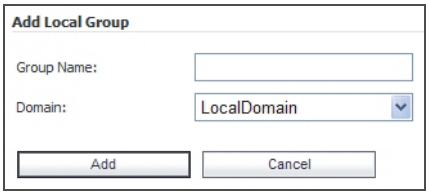



# Creating Local Groups

This procedure creates Local Groups that belong to the SNWL_AD domain on the SRA appliance. We create one local group for each Active Directory group.

## Adding the Local Groups

**Step 1** Navigate to the **Users > Local Groups** page and click **Add Group**. The **Add Local Group** window appears. We will add three local groups, corresponding to our Active Directory groups.




**Step 2** In the **Add Local Group** window, type **Acme_Group** into the **Group Name** field.

**Step 3** Select **SNWL_AD** from the **Domain** drop-down list.

**Step 4** Click **Add**.

**Step 5** On the **Users > Local Groups** page, click **Add Group** to add the second local group.

**Step 6** In the Add Local Group window, type **Mega_Group** into the **Group Name** field.

**Step 7** Select **SNWL_AD** from the **Domain** drop-down list.

**Step 8** Click **Add**.

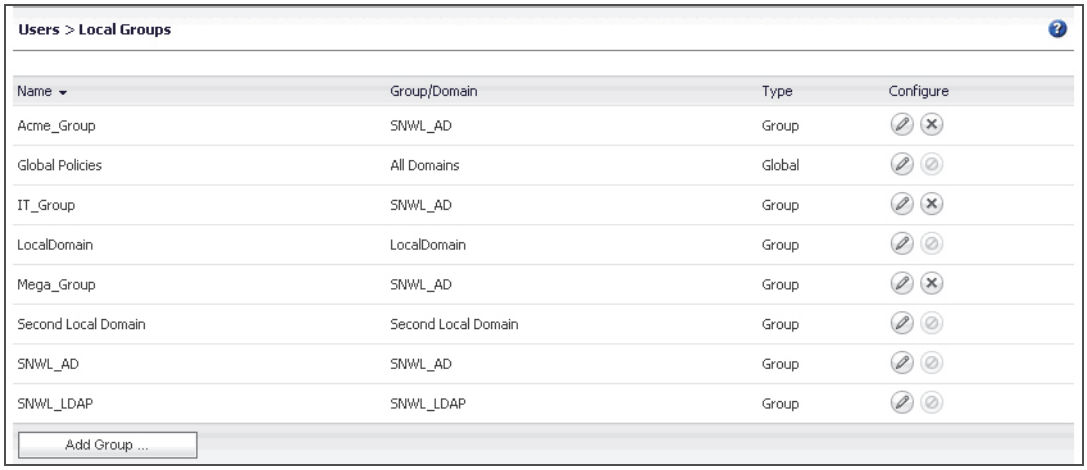
**Step 9** On the **Users > Local Groups** page, click **Add Group** to add the second local group.

**Step 10** In the Add Local Group window, type **IT_Group** into the **Group Name** field.

**Step 11** Select **SNWL_AD** from the **Domain** drop-down list.

**Step 12** Click **Add**.

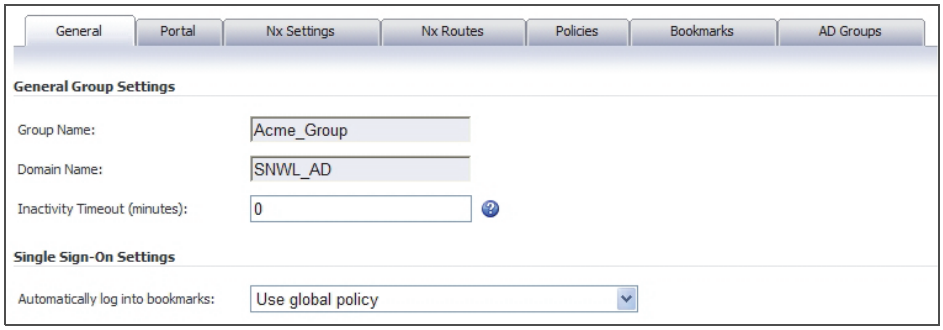
**Step 13** View the added groups on the **Users > Local Groups** page.




## Configuring the Local Groups

In this procedure we will edit each new local group and associate it with the corresponding Active Directory Group.

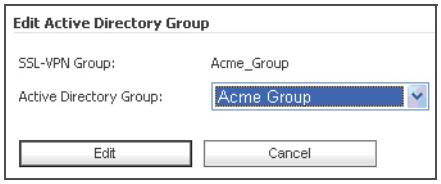
**Step 1** Click the **Configure** button in the **Acme_Group** row. The **Edit Group Settings** window appears.




**Step 2** In the **Edit Group Settings** window, click the **AD Groups** tab.

**Step 3** On the **AD Groups** tab, click the **Add Group** button.

**Step 4** In the **Edit Active Directory Group** window, select **Acme Group** from the **Active Directory Group** drop-down list.




**Step 5** Click **Edit**.
**Acme Group** is listed in the **Active Directory Groups** table on the **AD Groups** tab.

**Step 6** In the **Edit Group Settings** window, click **OK**.

**Step 7** On the **Users > Local Groups** page, click the **Configure** button in the **Mega_Group** row. The **Edit Group Settings** window appears.

**Step 8** In the **Edit Group Settings** window, click the **AD Groups** tab and then click the **Add Group** button.

**Step 9** In the **Edit Active Directory Group** window, select **Mega Group** from the **Active Directory Group** drop-down list and then click **Edit**.
**Mega Group** is listed in the **Active Directory Groups** table on the **AD Groups** tab.

**Step 10** In the **Edit Group Settings** window, click **OK**.

**Step 11** On the **Users > Local Groups** page, click the **Configure** button in the **IT_Group** row. The **Edit Group Settings** window appears.

**Step 12** In the **Edit Group Settings** window, click the **AD Groups** tab and then click the **Add Group** button.

**Step 13** In the **Edit Active Directory Group** window, select **IT Group** from the **Active Directory Group** drop-down list and then click **Edit**.
**IT Group** is listed in the **Active Directory Groups** table on the **AD Groups** tab.

**Step 14** In the **Edit Group Settings** window, click **OK**.

At this point, we have created the three Local Groups and associated each with its Active Directory Group.

# Adding the SSHv2 PERMIT Policy

In this section, we will add the SSHv2 PERMIT policy for both **Acme_Group** and **IT_Group** to access the 10.200.1.102 server using SSH.

This procedure creates a policy for the SRA Local Group, **Acme_Group**, and results in SSH access for members of the Active Directory group, Acme Group.

Repeat this procedure for **IT_Group** to provide SSH access to the server for members of the Active Directory group, IT Group.

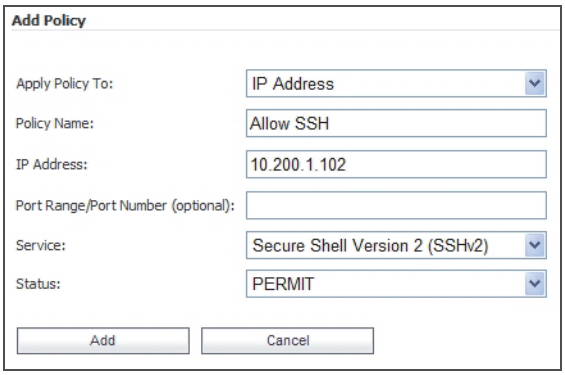
---

**Step 1** On the **Users > Local Groups** page, click the **Configure** button in the **Acme_Group** row. The **Edit Group Settings** window appears.

**Step 2** In the **Edit Group Settings** window, click the **Policies** tab.

**Step 3** On the **Policies** tab, click **Add Policy**.

**Step 4** In the **Add Policy** window, select **IP Address** in the **Apply Policy To** drop-down list.




**Step 5** In the **Policy Name** field, enter the descriptive name, **Allow SSH**.

**Step 6** In the **IP Address** field, enter the IP address of the target server, **10.202.1.102**.

**Step 7** In the **Services** drop-down list, select **Secure Shell Version 2 (SSHv2)**.

**Step 8** In the **Status** drop-down list, select **PERMIT**, and then click **Add**.

**Step 9** In the **Edit Group Settings** window, click **OK**.

# Adding the OWA PERMIT Policies

In this section, we will add two OWA PERMIT policies for both **Mega_Group** and **IT_Group** to access the OWA service using Secure Web (HTTPS).

This procedure creates a policy for the SRA Local Group, **Mega_Group**, and results in OWA access for members of the Active Directory group, Mega Group.

To access the Exchange server, adding a PERMIT policy to the **10.200.1.10/exchange** URL Object itself is not enough. Another URL Object policy is needed that permits access to **10.200.1.10/exchweb**, because some OWA Web contents are located in the **exchweb** directory.

Repeat this procedure for **IT_Group** to provide OWA access for members of the Active Directory group, IT Group.

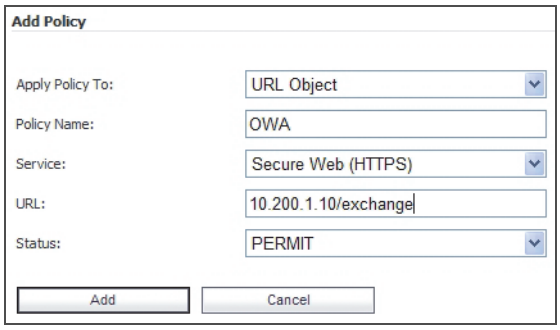
**Note** In this configuration, members of IT_Group and Mega_Group are denied access to the https://owa-server/public folder, because these groups have access only to the /exchange and /exchweb subfolders.

The OWA policies are applied to Exchange server URL Objects rather than server IP addresses since OWA is a Web service.

**Step 1** In the **Users > Local Groups** page, click the **Configure** button in the **Mega_Group** row. We will create **two** PERMIT policies for Mega_Group to allow access to the OWA Exchange server.

**Step 2** In the **Edit Group Settings** window, click the **Policies** tab, and then click **Add Policy**.

**Step 3** In the **Add Policy** window, select **URL Object** in the **Apply Policy To** drop-down list.




**Step 4** In the **Policy Name** field, enter the descriptive name, **OWA**.

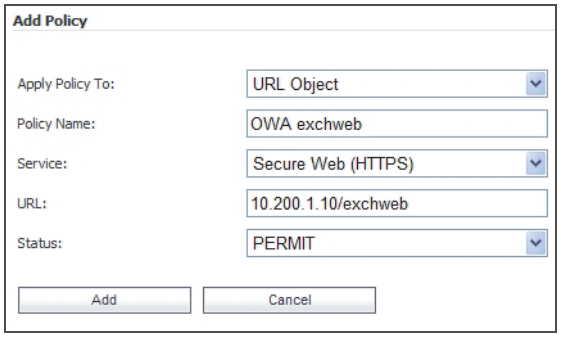
**Step 5** In the **Service** drop-down list, select **Secure Web (HTTPS)**.

**Step 6** In the **URL** field, enter the URL of the target application, **10.200.1.10/exchange**.

**Step 7** In the **Status** drop-down list, select **PERMIT**, and then click **Add**.

**Step 8** In the **Edit Group Settings** window on the **Policies** tab, click **Add Policy**.

**Step 9** In the **Add Policy** window, select **URL Object** in the **Apply Policy To** drop-down list.



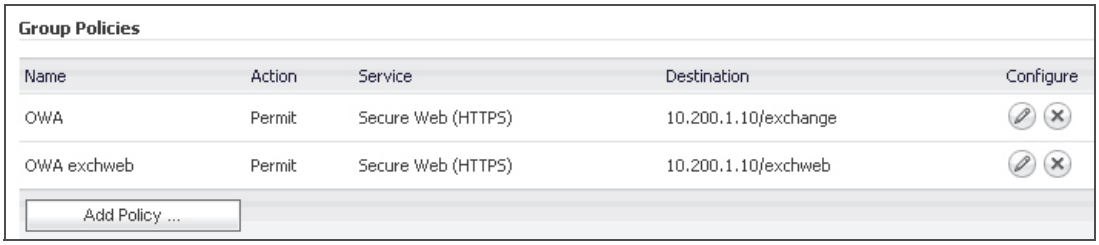

**Step 10** In the **Policy Name** field, enter the descriptive name, **OWA exchweb**.

**Step 11** In the **Service** drop-down list, select **Secure Web (HTTPS)**.

**Step 12** In the **URL** field, enter the URL of the target application, **10.200.1.10/exchweb**.

**Step 13** In the **Status** drop-down list, select **PERMIT**, and then click **Add**.

**Step 14** In the **Edit Group Settings** window, click **OK**. We are finished with the policies for Mega_Group. Repeat this procedure for IT_Group to provide OWA access for members of the Active Directory group, IT Group.




# Verifying the Access Policy Configuration

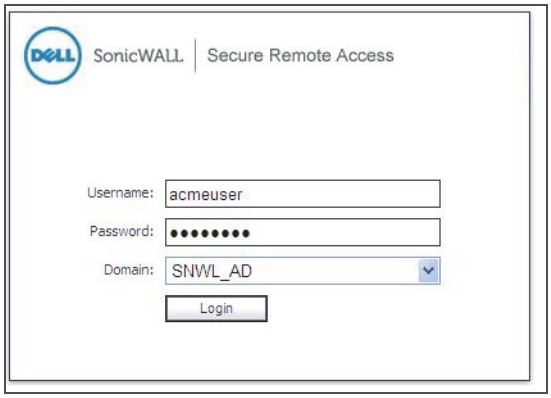
At this point:

- Acme_Group users are allowed to access SSH to 10.200.1.102
- Mega_Group users are allowed to access OWA at 10.200.1.10
- IT_Groups users are allowed to access both SSH and OWA as defined above

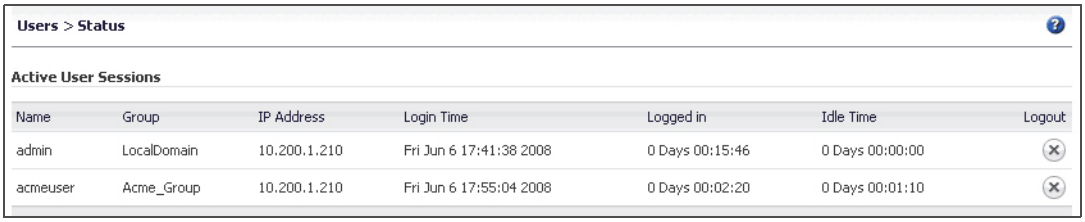
The configuration can be verified by logging in as different AD group members to the SNWL_AD domain on the SRA appliance, and attempting to access the resources.

## Test Result: Try Acmeuser Access

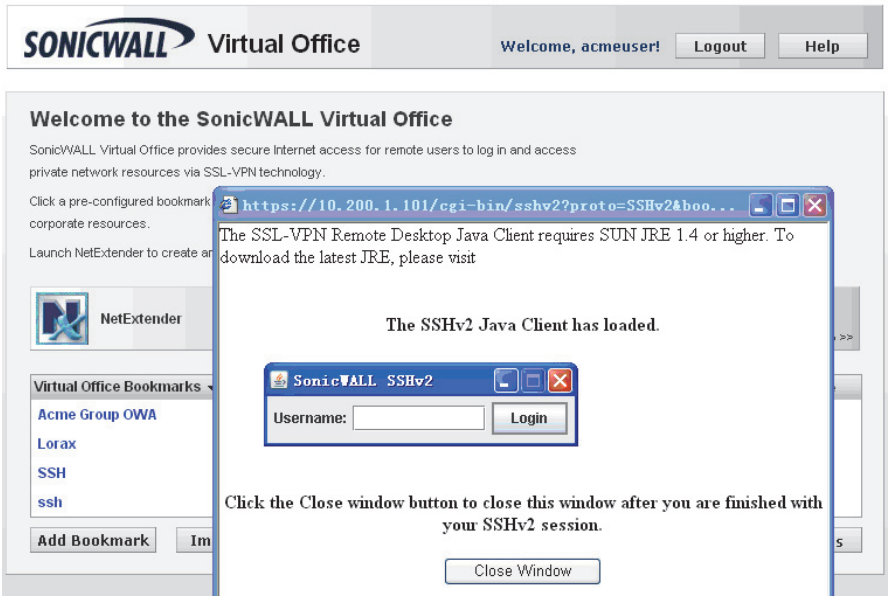
**Acmeuser** logs into the **SNWL_AD** domain.



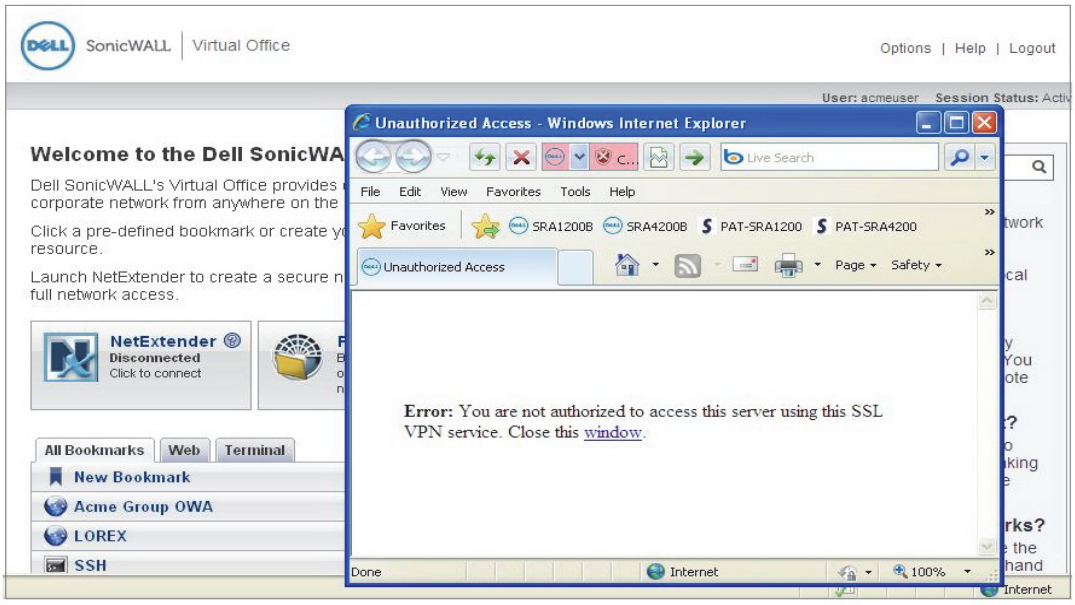

The **Users > Status** page shows that **acmeuser** is a member of the local group, **Acme_Group**.



**Acmeuser** can access SSH, as expected.

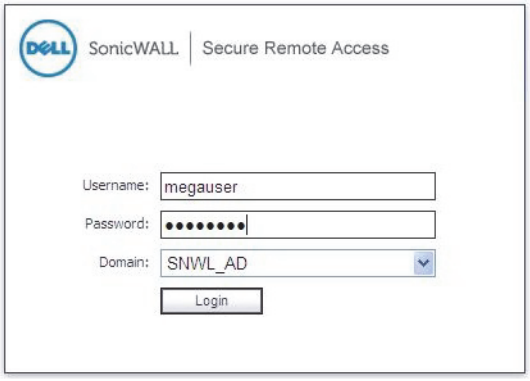



**Acmeuser** tries to access to other resources like OWA 10.200.1.10, but is denied, as expected.

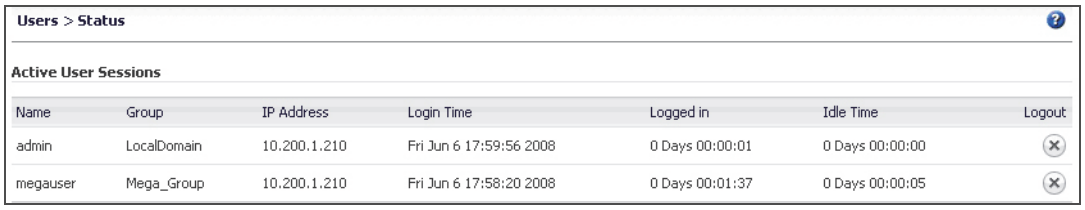


## Test Result: Try Megauser Access

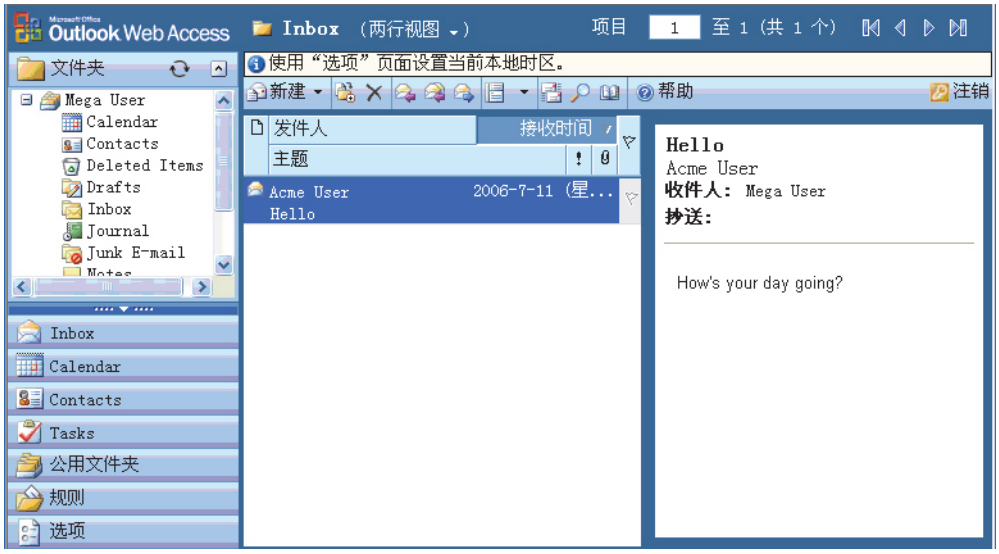
**Megauser** logs into the **SNWL_AD** domain.



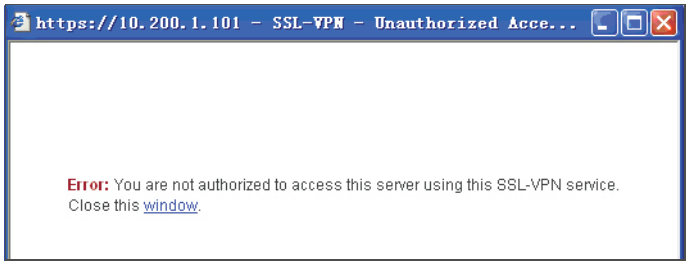

The **Users > Status** page shows that **megauser** is a member of the local group, **Mega_Group**.




**Megauser** can access OWA resources, as expected.

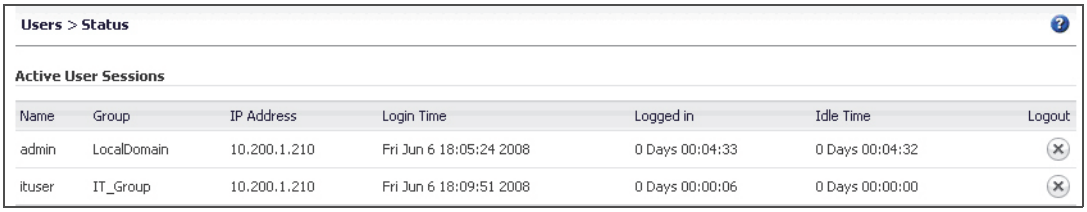


**Megauser** tries to access SSH, but is denied, as expected.

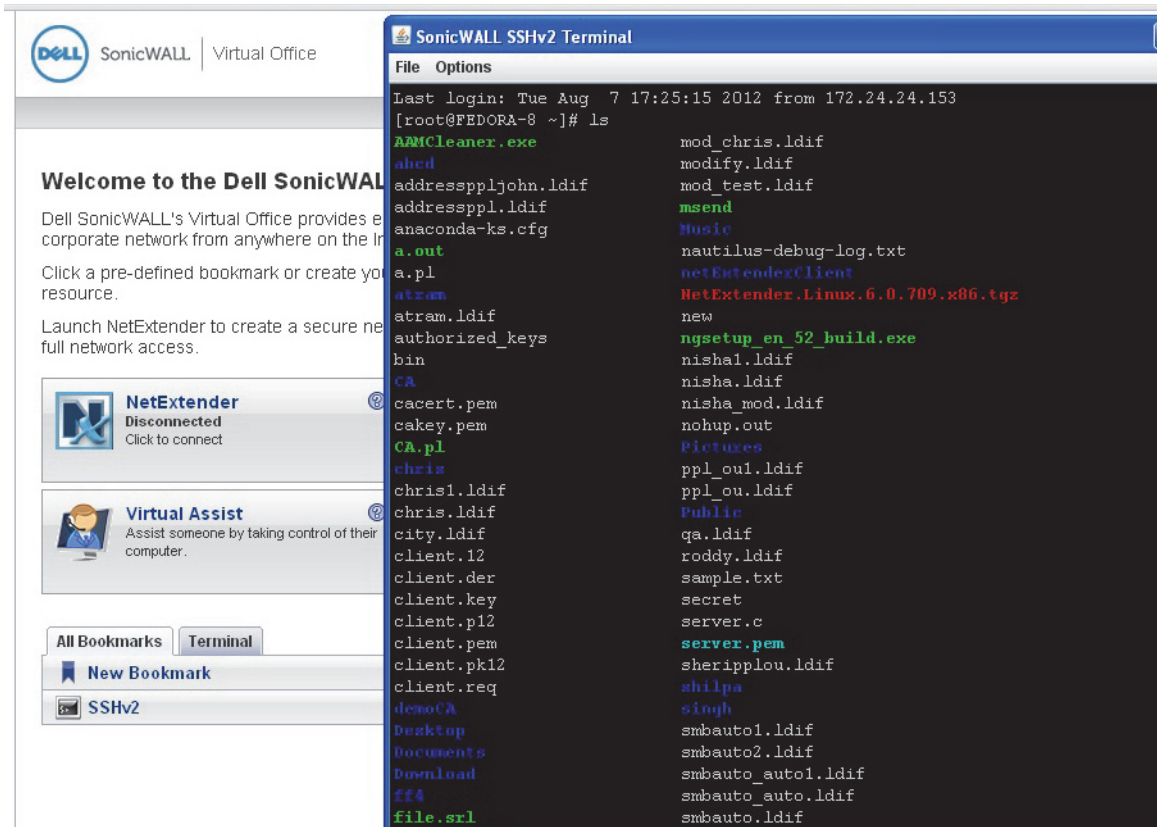



## Test Result: Try Ituser Access

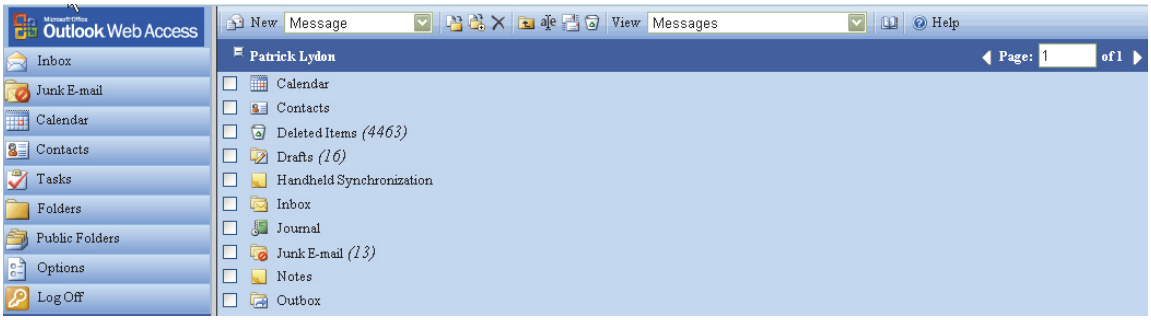
**Ituser** logs into the **SNWL_AD** domain. The **Users > Status** page shows that **ituser** is a member of the local group, **IT_Group**.




**Ituser** can access SSH to 10.200.1.102, as expected.



**ltuser** can access OWA resources, as expected.



# Appendix D

# NetExtender Troubleshooting

See the following tables with troubleshooting information for the Dell SonicWALL SRA NetExtender utility.

*Table 26 NetExtender Cannot Be Installed*

| Problem | Solution |
|---|---|
| **NetExtender cannot be installed.** | 1. Check your OS Version, NetExtender only supports Win2000 or above, Mac OS X 10.5 or above with Apple Java 1.6.0_10 or above, and Linux OpenSUSE in addition to Fedora Core and Ubuntu. An i386-compatible Linux distribution is required, along with Sun Java 1.6.0_10+.<br>2. Check that the user has administrator privilege, NetExtender can only install/work under the user account with administrator privileges.<br>3. Check if ActiveX has been blocked by Internet Explorer or third-party blockers.<br>4. If the problem still exists, obtain the following information and send to support:<br>– The version of Dell SonicWALL SRA NetExtender Adapter from Device Manager.<br>– The log file located at **C:\Program files\SonicWALL\SRA\NetExtender.dbg.**<br>– The event logs in the **Event Viewer** found under the Windows Control Panel **Administrator Tools** folder. Select Applications and System events and use the **Action /Save Log File as…** menu to save the events in a log file. |

*Table 27 NetExtender Connection Entry Cannot Be Created*

| Problem | Solution |
|---|---|
| NetExtender connection entry cannot be created. | 1. Navigate to Device Manager and check if the Dell SonicWALL SRA NetExtender Adapter has been installed successfully. If not, delete the adapter from the device list, reboot the machine and install NetExtender again.<br>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.<br>3. Check if there is another dial-up connection in use. If so, disconnect the connection, reboot the machine and install NetExtender again.<br>4. If problem still exists, obtain the following information and send them to support:<br>– The version of Dell SonicWALL SRA NetExtender Adapter from Device Manager.<br>– The log file located at **C:\Program files\SonicWALL\SRA\NetExtender.dbg**.<br>– The event logs in **Control Panel** > **Administrator Tools** > **Event Viewer**. Select **Applications and System** events and use the **Action /Save Log File as…** menu to save the events in a log file. |

*Table 28 NetExtender Cannot Connect*

| Problem | Solution |
|---|---|
| NetExtender cannot connect. | 1. Navigate to Device Manager and check if the Dell SonicWALL SRA NetExtender Adapter has been installed successfully. If not, delete the adapter from the device list, reboot the machine and install NetExtender again.<br>2. Navigate to Network connections to check if the Dell SonicWALL SRA NetExtender Dialup entry has been created. If not, reboot the machine and install NetExtender again.<br>3. Check if there is another dial-up connection in use, if so, disconnect the connection and reboot the machine and connect NetExtender again.<br>4. If problem still exists, obtain the following information and send them to support:<br>– The version of Dell SonicWALL SRA NetExtender Adapter from Device Manager.<br>– The log file located at **C:\Program files\SonicWALL\SRA\NetExtender.dbg**.<br>– The event logs in **Control Panel > Administrator Tools > Event Viewer**. Select **Applications and System** events and use the **Action /Save Log File as…** menu to save the events in a log file. |

*Table 29 NetExtender BSOD After Connected*

| Problem | Solution |
|---|---|
| NetExtender BSOD after connected. | 1. Uninstall NetExtender, reboot machine, reinstall the latest version NetExtender.<br>2. Obtain the following information and send them to support:<br>– The version of Dell SonicWALL SRA NetExtender Adapter from Device Manager.<br>– The log file located at **C:\Program files\SonicWALL\SRA\NetExtender.dbg**.<br>– Windows memory dump file located at **C:\Windows\MEMORY.DMP**. If you can not find this file, then you will need to open System Properties, click the **Startup and Recovery Settings** button under the **Advanced** tab. Select **Complete Memory Dump**, **Kernel Memory Dump** or **Small Memory Dump** in the **Write Debugging Information** drop-down list. Of course, you will also need to reproduce the BSOD to get the dump file.<br>– The event logs in **Control Panel > Administrator Tools > Event Viewer**. Select **Applications and System Events** and use the **Action /Save Log File as…** menu to save the events in a log file. |

# Appendix E

# FAQs

This appendix contains FAQs about the SRA appliance.

This appendix contains the following sections:


- Hardware FAQ on page 452
  - What are the hardware specs for the SRA 1600 and SRA 4600? on page 452
  - What are the hardware specs for the SRA 1200 and SRA 4200? on page 453
  - What are the SRA virtual appliance virtualized environment requirements? on page 455
  - Do the SRA appliances have hardware-based SSL acceleration onboard? on page 455
  - What operating system do the SRA appliances run? on page 455
  - Can I put multiple SRA appliances behind a load-balancer? on page 455
- Digital Certificates and Certificate Authorities FAQ on page 456
  - What do I do if when I log in to the SRA appliance my browser gives me an error, or if my Java components give me an error?
  - I get this message below when I log into my SRA appliance – what do I do? on page 456
  - I get this message below when I log into my SRA appliance using Firefox 3.0 – what do I do? on page 457
  - I get the warning below when I log into my SRA using Firefox 3.5 – what do I do? on page 458
  - When I launch any of the Java components it gives me an error – what should I do? on page 459
  - Do I have to purchase a SSL certificate? on page 459
  - What format is used for the digital certificates? on page 459
  - Are wild card certificates supported? on page 460
  - What CA's certificates can I use with the SRA appliance? on page 460
  - Does the SRA appliance support chained certificates? on page 460
  - Any other tips when I purchase the certificate for the SRA appliance? on page 460
  - Can I use certificates generated from a Microsoft Certificate Server? on page 460
  - Why can't I import my new certificate and private key? on page 460
  - Why do I see the status "pending" after importing a new certificate and private key? on page 460
  - Can I have more than one certificate active if I have multiple virtual hosts? on page 460
  - 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? on page 461
  - Can I store the key and certificate? on page 461
  - Are PKCS#7 (chained certs) or PKCS#12 (key and cert PFX container) supported on the SRA appliance? on page 461
  - Does the SRA appliance support client-side digital certificates? on page 461

  - When client authentication is required my clients cannot connect even though a CA certificate has been loaded. Why? on page 461
- NetExtender FAQ on page 462
  - Does NetExtender work on other operating systems than Windows? on page 462
  - Which versions of Windows does NetExtender support? on page 462
  - I tried to run NetExtender but it says I must have admin rights – why? on page 462
  - Can I block communication between NetExtender clients? on page 462
  - Can NetExtender run as a Windows service? on page 462
  - What range do I use for NetExtender IP client address range? on page 462
  - What do I enter for NetExtender client routes? on page 463
  - What does the 'Tunnel All Mode' option do? on page 463
  - Is there any way to see what routes the SRA appliance is sending NetExtender? on page 463
  - Once I install the NetExtender is it uninstalled when I leave my session? on page 463
  - How do I get new versions of NetExtender? on page 463
  - How is NetExtender different from a traditional IPSec VPN client, such as Dell SonicWALL's Global VPN Client (GVC)? on page 463
  - Is NetExtender encrypted? on page 463
  - Is there a way to secure clear text traffic between the SRA appliance and the server? on page 464
  - What is the PPP adapter that is installed when I use the NetExtender? on page 464
  - What are the advantages of using the NetExtender instead of a Proxy Application? on page 464
  - Does performance change when using NetExtender instead of proxy? on page 464
  - The SRA appliance is application dependent; how can I address non-standard applications? on page 464
  - What applications are supported using Application Offloading? on page 464
  - Speaking of SSH, is SSHv2 supported? on page 465
  - Why is it required that an ActiveX component be installed? on page 465
  - Does NetExtender support desktop security enforcement, such as AV signature file checking, or Windows registry checking? on page 465
  - Does NetExtender work with the 64-bit version of Microsoft Windows? on page 465
  - Does NetExtender work 32-bit and 64-bit version of Microsoft Windows 7? on page 465
  - Does NetExtender support client-side certificates? on page 465
  - My firewall is dropping NetExtender connections from my SonicWALL SRA as being spoofs. Why? on page 465
- General FAQ on page 465
  - Is the SRA appliance a true reverse proxy? on page 465
  - What browser and version do I need to successfully connect to the SRA appliance? on page 465
  - What needs to be activated on the browser for me to successfully connect to the SRA appliance? on page 465

- What version of Java do I need? on page 466
- What operating systems are supported? on page 466
- Why does the 'File Shares' component not recognize my server names? on page 466
- Does the SRA appliance have a SPI firewall? on page 466
- Can I access the SRA appliance using HTTP? on page 466
- What is the most common deployment of the SRA appliances? on page 466
- Why is it recommended to install the SRA appliance in one-port mode with a Dell SonicWALL security appliance? on page 466
- Is there an installation scenario where you would use more than one interface or install the appliance in two-port mode? on page 467
- Can I cascade multiple SRA appliances to support more concurrent connections? on page 467
- Why can't I log into the management interface of the SRA appliance? on page 467
- Can I create site-to-site VPN tunnels with the SRA appliance? on page 467
- Can the Dell SonicWALL Global VPN Client (or any other third-party VPN client) connect to the SRA appliance? on page 467
- Can I connect to the SRA appliance over a modem connection? on page 467
- What SSL ciphers are supported by the SRA appliance? on page 467
- Is AES supported in the SRA appliance? on page 467
- Can I expect similar performance (speed, latency, and throughput) as my IPSec VPN? on page 467
- Is Two-factor authentication (RSA SecurID, etc) supported? on page 467
- Does the SRA appliance support VoIP? on page 467
- Is Syslog supported? on page 467
- Does NetExtender support multicast? on page 467
- Are SNMP and Syslog supported? on page 468
- Does the SRA appliance have a Command Line Interface (CLI)? on page 468
- Can I Telnet or SSH into the SRA appliance? on page 468
- When controlling user access, can I apply permissions on both a domain as well as a Forest basis? on page 468
- What does the Web cache cleaner do? on page 468
- Why didn't the Web cache cleaner work when I exited the Web browser? on page 468
- What does the 'encrypt settings file' check box do? on page 468
- What does the 'store settings' button do? on page 468
- What does the 'create backup' button do? on page 468
- What is 'SafeMode'? on page 468
- How do I access the SafeMode menu? on page 469
- Can I change the colors of the portal pages? on page 469
- What authentication methods are supported? on page 469
- I configured my SRA appliance to use Active Directory as the authentication method, but it fails with a very strange error message. Why? on page 469

- My Windows XPSP2 system cannot use the RDP-based connectors. Why? on page 469
- I created a FTP bookmark, but when I access it, the filenames are garbled – why? on page 469
- Where can I get a VNC client? on page 469
- Are the SRA 4600/4200/1600/1200 appliances fully supported by GMS or Analyzer? on page 469
- Does the SRA appliance support printer mapping? on page 469
- Can I integrate the SRA appliance with wireless? on page 469
- Can I manage the appliance on any interface IP address of the SRA appliance? on page 470
- Can I allow only certain Active Directory users access to log into the SRA appliance? on page 470
- Does the HTTP(S) proxy support the full version of Outlook Web Access (OWA Premium)? on page 470
- Why are my RDP sessions dropping frequently? on page 470
- Can I create my own services for bookmarks rather than the services provided in the bookmarks section? on page 470
- Why can't I see all the servers on my network with the File Shares component? on page 470
- What port is the SRA appliance using for the Radius traffic? on page 470
- Do the SRA appliances support the ability for the same user account to login simultaneously? on page 470
- Does the SRA appliance support NT LAN Manager (NTLM) Authentication? on page 470
- 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 SRA, which currently supports only basic and digest authentication schemes. Please contact the administrator for further assistance.' - why? on page 471
- Why do Java Services, such as Telnet or SSH, not work through a proxy server? on page 471
- Why won't the SSH client connect to my SSH server? on page 471
- How are the F1-F12 keys handled in the Java-based SSHv1 and Telnet proxies? on page 471
- There is no port option for the service bookmarks – what if these are on a different port than the default? on page 471
- What if I want a bookmark to point to a directory on a Web server? on page 471
- What versions of Citrix are supported? on page 472


# Hardware FAQ

1. What are the hardware specs for the SRA 1600 and SRA 4600?

   **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, ICES Class A, CE, C-Tick, VCCI Class A, KCC, ANATEL, BSMI, NOM, UL, cUL, TUV/GS, CB

**Environment**:

Temperature:

SRA 1600/4600: 32-105ª F, 0-40ª C

Relative Humidity:

SRA 1600/4600: 5-95% RH non-condensing

MTBF

SRA 1600: 18.3 years

SRA 4600: 17.8 years

2. What are the hardware specs for the SRA 1200 and SRA 4200?

**Answer**:

Interfaces

SRA 1200: (2) 10/100/1000 Ethernet, (1) RJ-45 Serial port (115200 Baud)

SRA 4200: (4) 10/100/1000 Ethernet, (1) RJ-45 Serial port (115200 Baud)

Processors

SRA 1200: 1.5 GHz Via C7 x86 processor

SRA 4200: 1.8 GHz Via C7 x86 processor, cryptographic accelerator

Memory (RAM)

SRA 1200: 1 GB

SRA 4200: 2 GB

Flash Memory

SRA 1200: 1 GB

SRA 4200: 1 GB

Power Supply

SRA 1200: Internal

SRA 4200: Internal

Max Power Consumption

SRA 1200: 53 W

SRA 4200: 75 W

Total Heat Dissipation

SRA 1200: 181 BTU

SRA 4200: 256 BTU

Dimensions

SRA 1200: 17.00 x 10.125 x 1.75 in (43.18 x 25.70 x 4.45 cm)

SRA 4200: 17.00 x 10.125 x 1.75 in (43.18 x 25.70 x 4.45 cm)

Weight

SRA 1200: 8.7 lbs (3.95 kg)

SRA 4200: 9.5 lbs (4.31 kg)

Major Regulatory Compliance

SRA 1200/4200:

FCC Class A, ICES Class A, CE, C-Tick, VCCI Class A, MIC, NOM, UL, cUL, TUV/GS, CB, WEEE, RoHS (Europe), RoHS (China)

FIPS: Mechanically Designed for FIPS 140-2 Level 2

**Environment**

Temperature:

SRA 1200/4200: 32-105ª F, 0-40ª C

Relative Humidity:

SRA 1200/4200: 5-95% non-condensing

MTBF

SRA 1200: 13 years

SRA 4200: 8.3 years

3. What are the SRA virtual appliance virtualized environment requirements?

   Hypervisor: VMWare ESXi and ESX (version 4.0 and newer)

   Appliance size (on disk): 2 GB

   Allocated memory: 2 GB

4. Do the SRA appliances have hardware-based SSL acceleration onboard?

   **Answer**: The SRA 4200 has a hardware-based SSL accelerator onboard. The SRA 1200 does not have a hardware-based SSL accelerator processor. The SRA 1600 and SRA 4600 do not have a hardware-based SSL accelerator processor.

5. What operating system do the SRA appliances run?

   **Answer:** The appliance runs Dell SonicWALL's own hardened Linux distribution.

6. Can I put multiple 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.

***Table 30 SRA Max Count Table***

| Type | Max Supported on 1200/1600 | Max Supported on 4200/4600 | Max Supported on Virtual Appliance |
|---|---|---|---|
| Portal entries | 32 | 64 | 64 |
| Domain entries | 32 | 64 | 64 |
| Group entries | 512 | 512 | 512 |
| User entries | 1,000 | 2,000 | 2,000 |
| NetExtender global client routes | 100 | 100 | 100 |
| NetExtender group client routes | 100 | 100 | 100 |
| NetExtender user client routes | 100 | 100 | 100 |
| Maximum concurrent users | 200 | 1024 | 1024 |
| Maximum concurrent Nx connections | 50 | 500 | 500 |
| Route entries | 32 | 32 | 32 |
| Host entries | 32 | 32 | 32 |
| Bookmark entries | 500 | 500 | 500 |
| User Policy entries | 64 | 64 | 64 |
| Group Policy entries | 64 | 64 | 64 |
| Global Policy entries | 64 | 64 | 64 |
| Policy address entries | 32 | 32 | 32 |
| Network Objects | 128 | 128 | 128 |
| 'Address' Network Objects | 32 | 32 | 32 |
| 'Network' Network Objects | 64 | 64 | 64 |
| 'Service' Network Objects | 64 | 64 | 64 |
| SMB shares | 1,024 | 1,024 | 1,024 |
| SMB nodes | 1,024 | 1,024 | 1,024 |
| SMB workgroups | 8 | 8 | 8 |
| Concurrent FTP sessions | 8 | 8 | 8 |
| Log size | 250 KB | 250 KB | 250 KB |

# Digital Certificates and Certificate Authorities FAQ

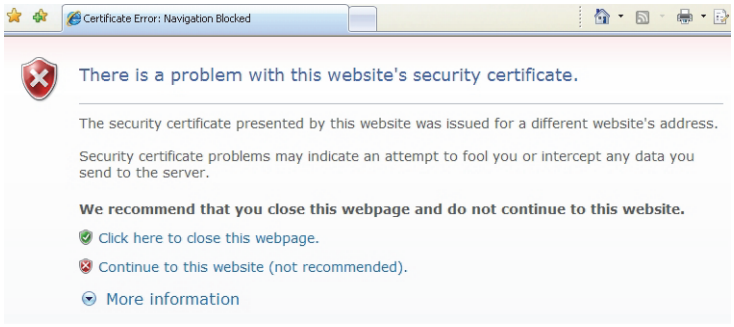
1. What do I do if when I log in to the SRA appliance my browser gives me an error, or if my Java components give me an error?

   **Answer:** These errors can be caused by any combination of the following three factors:

   - The certificate in the SRA appliance is not trusted by the browser
   - The certificate in the SRA appliance may be expired.
   - The site requested by the client Web browser does not match the site name embedded in the certificate.

   Web browsers are programmed to issue a warning if the above three conditions are not met precisely. This security mechanism is intended to ensure end-to-end security, but often confuses people into thinking something is broken. If you are using the default self-signed certificate, this error will appear every time a Web browser connects to the 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 will need to purchase and install a trusted SSL certificate onto the SRA appliance.

2. I get this message below when I log into my SRA appliance – what do I do?

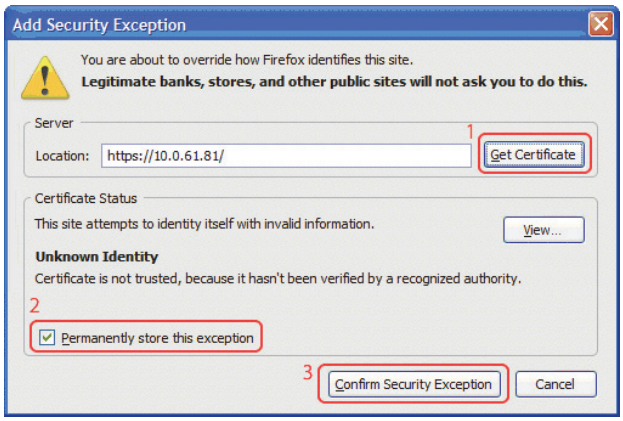



   **Answer**: It's the same problem as noted in the previous topic, but this is the new "improved" security warning screen in Microsoft Internet Explorer 8.0. Whereas before IE5.x and IE6.x presented a pop-up that listed the reasons why the certificate is not trusted, IE8.0 simply returns a generic error 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 SRA appliances, going forward, have a trusted digital certificate installed.

3. I get this message below when I log into my SRA appliance using Firefox 3.0 – what do I do?

   **Answer**: Much like the errors shown above for Internet Explorer, Firefox 3.0 has a unique error message when any certificate problem is detected. The conditions for this error are the same as for the above Internet Explorer errors.

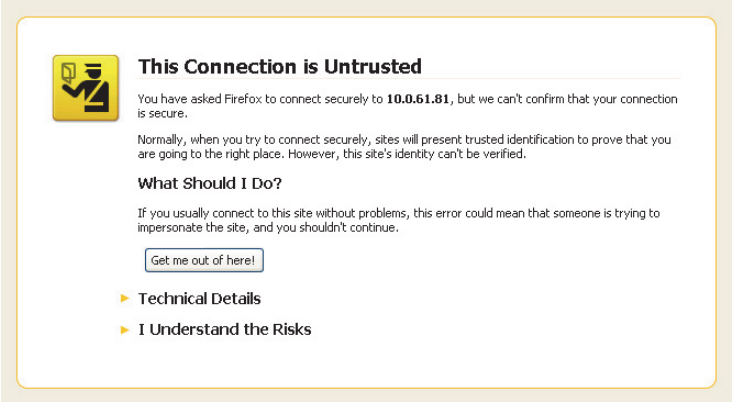
   To get past this screen, click the **Or you can add an exception** link at the bottom, then click the **Add Exception** button that appears. In the Add Security Exception window that opens, click the **Get Certificate** button, ensure that **Permanently store this exception** is checked, and finally, click the **Confirm Security Exception** button. See below:



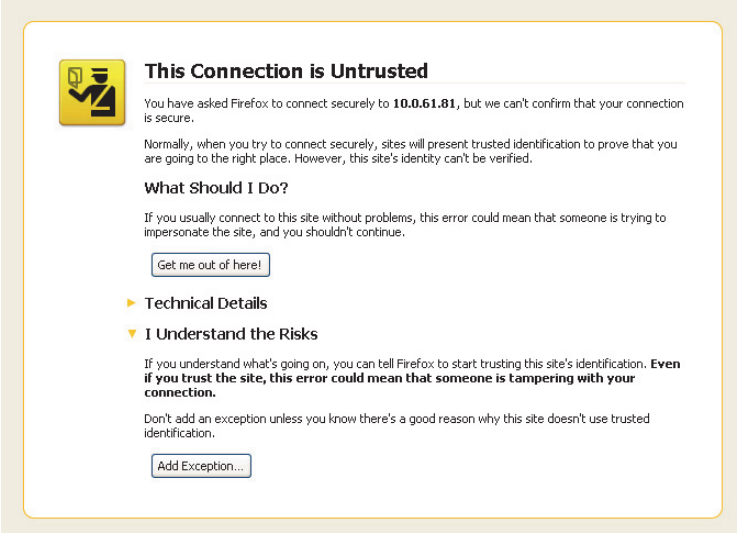

To avoid this inconvenience, it is strongly recommended that all SRA appliances, going forward, have a trusted digital certificate installed.

4. I get the warning below when I log into my SRA using Firefox 3.5 – what do I do?

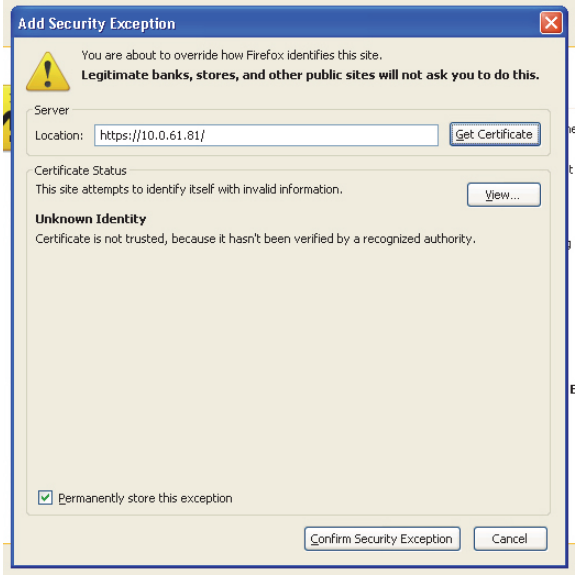
   **Answer**: This is the Firefox 3.5 warning message when any certificate problem is detected. The conditions for this error are the same as for the above Internet Explorer errors.




   To get past this screen, click the arrow next to **I Understand the Risks** to expand the section, then click the **Add Exception** button that appears.



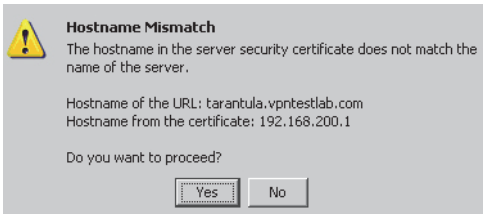
In the Add Security Exception window that opens, click the **Get Certificate** button, ensure that **Permanently store this exception** is checked, and finally, click the **Confirm Security Exception** button. See below:




To avoid this inconvenience, it is strongly recommended that all SRA appliances, going forward, have a trusted digital certificate installed.

5. 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 SRA appliance during the SSL handshake process. This error can be safely ignored.




6. Do I have to purchase a SSL certificate?

   **Answer**: No, you can simply ignore the security warnings, which are a message to users that the certificate is not trusted or contains mismatched information. Accepting a non-trusted certificate does not have anything to do with the level of encryption negotiated during the SSL handshake. However, Dell SonicWALL tested digital certificates from www.rapidssl.com, which are inexpensive, work fine in the SRA appliance, and do not require the background check that other Certificate Authorities require during the purchase process. You can find a white paper on how to purchase and install a certificate online at: http://www.sonicwall.com/us/support/3165.html.

7. What format is used for the digital certificates?

   **Answer**: X509v3.

8. Are wild card certificates supported?

   **Answer**: Yes.

9. What CA's certificates can I use with the SRA appliance?

   **Answer**: Any CA certificate should work if the certificate is in X509v3 format, including Verisign, Thawte, Baltimore, RSA, etc.

10. Does the SRA appliance support chained certificates?

    **Answer**: Yes, it does. On the System > Certificates page, do the following:

    – Under "Server Certificates", click Import Certificate and upload the SSL server certificate and key together in a .zip file. The certificate should be named 'server.crt'. The private key should be named 'server.key'.

    – Under "Additional CA Certificates", click Import Certificate button and upload the intermediate CA certificate(s). The certificate should be PEM encoded in a text file.

    After uploading any intermediate CA certificates, the system should be restarted. The web server needs to be restarted with the new certificate included in the CA certificate bundle.

11. Any other tips when I purchase the certificate for the 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 will connect to the SRA appliance run Windows Update (also known as Microsoft Update) and install the 'Root Certificates' update.

12. Can I use certificates generated from a Microsoft Certificate Server?

    **Answer**: Yes, but to avoid a browser warning, you will need to install the Microsoft CA's root certificate into all Web browsers that will connect to the appliance.

13. Why can't I import my new certificate and private key?

    **Answer**: Be sure that you upload a .zip file containing the PEM formatted private key file named "server.key" and the PEM formatted certificate file named "server.crt". The .zip file must have a flat file structure (no directories) and contain only "server.key" and "server.crt" files. The key and the certificate must also match, otherwise the import will fail.

14. Why do I see the status "pending" after importing a new certificate and private key?

    **Answer:** Click the 'configure' icon next to the new certificate and enter the password you specified when creating the Certificate Signing Request (CSR) to finalize the import of the certificate. Once this is done, you can successfully activate the certificate on the SRA appliance.

15. Can I have more than one certificate active if I have multiple virtual hosts?

    **Answer:** Prior to 2.5 firmware: No, only one can be active, other virtual sites with names that do not match the name embedded on the SRA appliance's certificate will show security warnings to any Web browser connecting to them.

    With 2.5 firmware or later, it is possible to select a certificate for each Portal under the Portals > Portals: Edit Portal - Virtual Host tab. The portal Virtual Host Settings fields allow you to specify separate IP address, and certificate per portal. If the administrator has configured multiple portals, it is possible to associate a different certificate with each portal. For example, **sslvpn.test.sonicwall.com** might also be reached by pointing the browser to **virtualassist.test.sonicwall.com**. Each of those portal names can have its own certificate. This is useful to prevent the browser from displaying a certificate mismatch warning, such as "This server is abc, but the certificate is xyz, are you sure you want to continue?".

16. 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'.

17. 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 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.

18. Are PKCS#7 (chained certs) or PKCS#12 (key and cert PFX container) supported on the SRA appliance?

    **Answer:** No, neither one is currently supported. Dell SonicWALL is investigating supporting these in a future release.

19. Does the 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%

    **Note** Firmware prior to 3.5 required the client certificate CN field to be the username (CN=username) entered to login to the appliance.

    – Support for Microsoft CA Subject Names where CN=<Full user name>, e.g. CN=John Doe. Client certificate authentication attempts for users in Active Directory domains will have the CN compared against the user's full name in AD.

    – Detailed client certificate authentication failure messages and log messages are available in the Log > View page.

    – Certificate Revocation List (CRL) Support. Each CA Certificate now supports an optional CRL via file import or periodic import via URL.

      The client certificate must be loaded into the client's browser. Also, remember that any certificates in the trust chain of the client certificates must be installed onto the SRA appliance.

20. 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 SRA appliance must be rebooted before it is used for client authentication. Failures to validate the client certificate will also cause failures to logon. Among the most common are certificate is not yet valid, certificate has expired, login name does not match common name of the certificate, certificate not sent.

# NetExtender FAQ

1. Does NetExtender work on other operating systems than Windows?

   **Answer**: Yes. Version 2.5 firmware added support for Mac and Linux platforms.

   Mac Requirements:

   - Mac OS X 10.6.8+
   - 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:

   - Windows XP Service Pack 3 (SP3)
   - Vista SP2
   - Windows 7

3. I tried to run NetExtender but it says I must have admin rights – why?

   **Answer**: If your SRA appliance is running 1.0 firmware, then on Windows 2000, XP, 2003, Vista, and Windows 7 systems the logged-in user must have administrative rights to be able to install ActiveX-based components such as NetExtender, and it will not be possible to run NetExtender on systems where you do not have administrative rights (this often is seen in kiosk or public computer environments, where the OS is locked down to prevent this sort of behavior). If your SRA appliance is running firmware 1.5 firmware or newer, a user can run NetExtender provided that a user with administrative rights previously installed NetExtender onto the system.

4. Can I block communication between NetExtender clients?

   **Answer:** Yes, this can be achieved with the User/Group/Global Policies by adding a ‘deny’ policy for the NetExtender IP range.

5. Can NetExtender run as a Windows service?

   **Answer**: The Windows version of NetExtender found in the 1.5 firmware release and newer can be installed and configured to run as a Windows service, which will allow systems to login to domains across the NetExtender client.

6. What range do I use for NetExtender IP client address range?

   **Answer**: This range is the pool that incoming NetExtender clients will be assigned – NetExtender clients actually appear as though they are on the internal network – much like the Virtual Adapter capability found in Dell SonicWALL’s Global VPN Client. You will need to dedicate one IP address for each active NetExtender session, so if you expect 20 simultaneous NetExtender sessions to be the maximum, create a range of 20 open IP addresses. Make sure that these IP addresses are open and are not used by other network appliances or contained within the scope of other DHCP servers. For example, if your 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. In the 1.5 firmware release, you can create multiple unique pools on a per-group or per-user basis.

7. What do I enter for NetExtender client routes?

   **Answer:** These are the networks that will be sent to remote NetExtender clients and should contain all networks that you wish to give your NetExtender clients access to. For example, if your SRA appliance was in one-port mode, attached to a Dell SonicWALL NSA 3500 appliance on a DMZ using 192.168.200.0/24 as the subnet for that DMZ, and the Dell SonicWALL NSA 3500 had two LAN subnets of 192.168.168.0/24 and 192.168.170.0/24, you would enter those two LAN subnets as the client routes to provide NetExtender clients access to network resources on both of those LAN subnets.

8. What does the 'Tunnel All Mode' option do?

   **Answer:** Activating this feature will cause the SRA appliance to push down two default routes that tell the active NetExtender client to send all traffic through the SRA appliance. This feature is useful in environments where the SRA appliance is deployed in tandem with a Dell SonicWALL security appliance running all UTM services, as it will allow you to scan all incoming and outgoing NetExtender user traffic for viruses, spyware, intrusion attempts, and content filtering.

9. Is there any way to see what routes the 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.

10. Once I install the NetExtender is it uninstalled when I leave my session?

    **Answer:** By default, when NetExtender is installed for the first time it stays resident on the system, although this can be controlled by selecting the **Uninstall On Browser Exit** > **Yes** option from the NetExtender icon in the taskbar while it is running. If this option is checked, NetExtender will remove itself when it is closed. It can also be uninstalled from the "Add/ Remove Program Files" in Control Panel. NetExtender remains on the system by default to speed up subsequent login times.

11. How do I get new versions of NetExtender?

    **Answer:** New versions of NetExtender are included in each Dell SonicWALL SRA firmware release and have version control information contained within. If the SRA appliance has been upgraded with new software, and a connection is made from a system using a previous, older version of NetExtender, it will automatically be upgraded to the new version.

    There is one exception to the automatic upgrading feature: it is not supported for the MSI version of NetExtender. If NetExtender was installed with the MSI package, it must be upgraded with a new MSI package. The MSI package is designed for the administrator to deploy NetExtender through Active Directory, allowing full version control through Active Directory.

12. How is NetExtender different from a traditional IPSec VPN client, such as Dell SonicWALL's Global VPN Client (GVC)?

    **Answer:** NetExtender is designed as an extremely lightweight client that is installed via a Web browser connection, and utilizes the security transforms of the browser to create a secure, encrypted tunnel between the client and the SRA appliance.

13. Is NetExtender encrypted?

    **Answer:** Yes, it uses whatever cipher the NetExtender client and SRA appliance negotiate during the SSL connection.

14. Is there a way to secure clear text traffic between the 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.

15. What is the PPP adapter that is installed when I use the NetExtender?

    **Answer:** This is the transport method NetExtender uses. It also uses compression (MPPC). You can elect to have it removed during disconnection by selecting this from the NetExtender menu.

16. What are the advantages of using the NetExtender instead of a Proxy Application?

    **Answer:** NetExtender allows full connectivity over an encrypted, compressed PPP connection allowing the user to directly to connect to internal network resources. For example, a remote user could launch NetExtender to directly connect to file shares on a corporate network.

17. Does performance change when using NetExtender instead of proxy?

    **Answer:** Yes. NetExtender connections put minimal load on the SRA appliances, whereas many proxy-based connections may put substantial strain on the SRA appliance. Note that HTTP proxy connections use compression to reduce the load and increase performance. Content received by the SRA from the local Web server is compressed using gzip before sending it over the Internet to the remote client. Compressing content sent from the SRA saves bandwidth and results in higher throughput. Furthermore, only compressed content is cached, saving nearly 40-50% of the required memory. Note that gzip compression is not available on the local (clear text side) of the SRA appliance, or for HTTPS requests from the remote client.

18. The 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, RDP4 (firmware 1.0 only), ActiveX-based RDP, Java-based RDP (firmware 1.5 and newer), Telnet, and SSHv1. With 3.5 firmware and later, Application Offloading can be used for web applications. In this way, the SRA appliance functions similar to an SSL offloader and will proxy web applications pages without the need for URL rewriting.

19. What applications are supported using Application Offloading?

    **Answer**: Application Offloading should support any application using HTTP/HTTPS. 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. Since 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 Offloading will need 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 Offloading Portal, but all the URLs may not be rewritten, depending on how the Web application has been developed. (This limitation is usually the same for other WAF/SRA vendors employing reverse proxy mode.*)*

20. Speaking of SSH, is SSHv2 supported?

    **Answer**: Yes, this is supported in firmware 2.0 and newer.

21. Why is it required that an ActiveX component be installed?

    **Answer:** NetExtender is installed via an ActiveX-based plug-in from Internet Explorer. Users using Firefox browsers may install NetExtender via an XPI installer. NetExtender may also be installed via an MSI installer. Download the NetExtender MSI installer from mysonicwall.com.

22. 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.

23. Does NetExtender work with the 64-bit version of Microsoft Windows?

    **Answer**: Yes, starting with 3.0 firmware, NetExtender supports 64-bit Windows 7, Vista and XP.

24. Does NetExtender work 32-bit and 64-bit version of Microsoft Windows 7?

    **Answer**: Yes, starting with 3.0.0.9-20sv and later firmware, NetExtender supports 32-bit and 64-bit Windows 7.

25. Does NetExtender support client-side certificates?

    **Answer**: Yes, in 3.5 and up the Windows NetExtender client supports client certificate authentication from the stand-alone client. Users can also authenticate to the SRA portal and then launch NetExtender.

26. My firewall is dropping NetExtender connections from my SonicWALL 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 SRA appliance.

# General FAQ

1. Is the 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 - ActiveX, RDP - Java, SSHv1 and Telnet use browser-delivered Java or ActiveX clients. NetExtender on Windows uses a browser-delivered client.

2. What browser and version do I need to successfully connect to the SRA appliance?

   **Answer**: Currently supported browsers and versions are listed in Browser Requirements for the SRA Administrator on page 24 and Browser Requirements for the SRA End User on page 24.

3. What needs to be activated on the browser for me to successfully connect to the SRA appliance?

   **Answer**:

   - SSLv2, SSLv3, or TLS – recommend disabling SSLv2 if possible
   - Enable cookies
   - Enable pop-ups for the site

- Enable Java
- Enable Javascript
- Enable ActiveX

4. What version of Java do I need?

   **Answer:** You will need to install SUN's JRE 1.6.0_10 or higher (available at http://www.java.com) to use some of the features on the SRA appliance. On Google Chrome, you will need Java 1.6.0 update 10 or higher.

5. What operating systems are supported?

   **Answer**:

   - Microsoft Windows 2000 Professional SP4 and newer
   - Microsoft XP, SP2 and newer
   - Microsoft Vista
   - Microsoft Windows 7
   - Apple OSX 10.6.8 and newer
   - Linux kernel 2.4.x and newer

6. Why does the 'File Shares' component not recognize my server names?

   **Answer**: If you cannot reach your server by its NetBIOS name, there might be a problem with name resolution. Check your DNS and WINS settings on the 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, e.g. \\192.168.100.100\sharefolder.

   Also, if you get an authentication loop or an error, is this File Share a DFS server on a Windows domain root? When creating a File Share, do not configure a Distributed File System (DFS) server on a Windows Domain Root system. Because the Domain Root allows access only to Windows computers in the domain, doing so will disable access to the DFS file shares from other domains. The SRA appliance is not a domain member and will not be able to connect to the DFS shares.DFS file shares on a stand-alone root are not affected by this Microsoft restriction.

7. Does the SRA appliance have a SPI firewall?

   **Answer:** No. It must be combined with a Dell SonicWALL security appliance or other third-party firewall/VPN device.

8. Can I access the SRA appliance using HTTP?

   **Answer:** No, it requires HTTPS. HTTP connections are immediately redirected to HTTPS. You may wish to open both 80 and 443, as many people forget to type https: and instead type
   http://. If you block 80, it will not get redirected.

9. What is the most common deployment of the 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 Dell SonicWALL security appliance, such as the Dell SonicWALL TZ 180, or the Dell SonicWALL NSA appliance.

10. Why is it recommended to install the SRA appliance in one-port mode with a Dell SonicWALL security appliance?

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

11. Is there an installation scenario where you would use more than one interface or install the appliance in two-port mode?

    **Answer:** Yes, when it would be necessary to bypass a firewall/VPN device that may not have an available third interface, or a device where integrating the SRA appliance may be difficult or impossible.

12. Can I cascade multiple SRA appliances to support more concurrent connections?

    **Answer:** No, this is not supported.

13. Why can't I log into the management interface of the 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 into the 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 SRA appliance?

    **Answer:** No, it is only a client-access appliance. If you require this, you will need a Dell SonicWALL TZ series or NSA series security appliance.

15. Can the Dell SonicWALL Global VPN Client (or any other third-party VPN client) connect to the SRA appliance?

    **Answer:** No, only NetExtender and proxy sessions are supported.

16. Can I connect to the SRA appliance over a modem connection?

    **Answer:** Yes, although performance will be slow, even over a 56K connection it is usable.

17. What SSL ciphers are supported by the SRA appliance?

    **Answer:** Starting with 4.0 firmware, Dell SonicWALL only uses HIGH security ciphers with SSLv3 and TLSv1:

    - AES256-SHA
    - DES-CBC3-SHA
    - DHE-RSA-AES256-SHA
    - EDH-RSA-DES-CBC3-SHA

18. Is AES supported in the 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 may 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 in the 2.0 firmware release and newer.

21. Does the 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 SRA appliance have a Command Line Interface (CLI)?

    **Answer:** Yes, the SRA 4600, 4200, 1600, and 1200 have a simple CLI when connected to the console port. The SRA Virtual Appliance is also configurable with the CLI. The Dell SonicWALL SRA 6.0 CLI allows configuration of only the X0 interface on the Dell SonicWALL SRA appliances or SRA Virtual Appliance.

26. Can I Telnet or SSH into the SRA appliance?

    **Answer**: No, neither Telnet or SSH are supported in the current release of the SRA appliance software as a means of management (this is not to be confused with the Telnet and SSH proxies, which the appliance does support).

27. When controlling user access, can I apply permissions on both a domain as well as a Forest basis?

    **Answer:** Yes, using the LDAP connector.

28. What does the Web cache cleaner do?

    **Answer:** The Web cache cleaner is an ActiveX-based applet that removes all temporary files generated during the session, removes any history bookmarks, and removes all cookies generated during the session. It will only run on Internet Explorer 8.0 or newer.

29. Why didn't the Web cache cleaner work when I exited the Web browser?

    **Answer:** In order for the Web cache cleaner to run, you must click on the **Logout** button. If you close the Web browser using any other means, the Web cache cleaner cannot run.

30. What does the 'encrypt settings file' check box do?

    **Answer:** This setting will encrypt the settings file so that if it is exported it cannot be read by unauthorized sources. Although it is encrypted, it can be loaded back onto the 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.

31. What does the 'store settings' button do?

    **Answer:** By default, the settings are automatically stored on a 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 will be lost. This feature is most useful when you are unsure of making a change that may result in the box locking up or dropping off the network. If the setting is not immediately saved, you can power-cycle the box and it will return to the previous state before the change was made.

32. What does the 'create backup' button do?

    **Answer:** This feature allows you to create a backup snapshot of the firmware and settings into a special file that can be reverted to from the management interface or from SafeMode. Dell SonicWALL strongly recommends creating system backup right before loading new software, or making significant changes to the programming of the appliance.

33. What is 'SafeMode'?

    **Answer:** SafeMode is a feature of the 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 will boot into a special interface mode that allows the administrator to choose which version to boot, or load a new version of the software image.

34. How do I access the SafeMode menu?

    **Answer:** In emergency situations, you can access the SafeMode menu by holding in the Reset button on the SRA appliance (the small pinhole button located on the front of the SRA appliances) for 12-14 seconds until the 'Test' LED begins quickly flashing yellow. Once the 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 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 will be able to boot the appliance using a previously saved backup snapshot, or you can upload a new version of software with the **Upload New Software image** button.

35. Can I change the colors of the portal pages?

    **Answer**: This is not supported in the current releases, but is planned for a future software release.

36. What authentication methods are supported?

    **Answer:** Local database, RADIUS, Active Directory, NT4, and LDAP.

37. I configured my 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 will fail. Ensure that the SRA appliance and the Active Directory server are both using NTP to keep their internal clocks synchronized.

38. My Windows XPSP2 system cannot use the RDP-based connectors. Why?

    **Answer:** You will need to download and install a patch from Microsoft for this to work correctly. The patch can be found at the following site:

    http://www.microsoft.com/downloads/details.aspx?FamilyID=17d997d2-5034-4bbb-b74dad8430a1f7c8&DisplayLang=en.

    You will need to reboot your system after installing the patch.

39. I created a FTP bookmark, but when I access it, the filenames are garbled – why?

    **Answer**: If you are using a Windows-based FTP server, you will need to change the directory listing style to 'UNIX' instead of 'MS-DOS'.

40. Where can I get a VNC client?

    **Answer:** Dell SonicWALL has done extensive testing with RealVNC. It can be downloaded at:

    http://www.realvnc.com/download.html

41. Are the SRA 4600/4200/1600/1200 appliances fully supported by GMS or Analyzer?

    **Answer**: You need SonicOS SRA 1.5.0.3 or higher for basic management by Dell SonicWALL GMS; SonicOS SRA 2.1 or higher is required for SRA Reporting in Dell SonicWALL GMS or ViewPoint.

42. Does the 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 may need to install the correct printer driver software on the Terminal Server you are accessing.

43. Can I integrate the SRA appliance with wireless?

    **Answer:** Yes, refer to the *Dell SonicWALL Secure Wireless Networks Integrated Solutions Guide*, available through Elsevier, http://www.elsevierdirect.com/.

44. Can I manage the appliance on any interface IP address of the SRA appliance?

    **Answer:** Prior to 2.5 firmware: No, the appliance can only by managed using the X0's IP address. With 2.5 firmware and later, yes, you can manage on any of the interface IP addresses.

45. Can I allow only certain Active Directory users access to log into the 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.

46. Does the HTTP(S) proxy support the full version of Outlook Web Access (OWA Premium)?

    **Answer**: Yes.

47. Why are my RDP sessions dropping frequently?

    **Answer:** Try adjusting the session and connection timeouts on both the SRA appliance and any appliance that sits between the endpoint client and the destination server. If the SRA appliance is behind a firewall, adjust the TCP timeout upwards and enable fragmentation.

48. Can I create my own services for bookmarks rather than the services provided in the bookmarks section?

    **Answer**: This is not supported in the current release of software but may be supported in a future software release.

49. Why can't I see all the servers on my network with the File Shares component?

    **Answer**: The CIFS browsing protocol is limited by the server's buffer size for browse lists. These browse lists contain the names of the hosts in a workgroup or the shares exported by a host. The buffer size depends on the server software. Windows personal firewall has been known to cause some issues with file sharing even when it is stated to allow such access. If possible, try disabling such software on either side and then test again.

50. What port is the SRA appliance using for the Radius traffic?

    **Answer**: It uses port 1812.

51. Do the SRA appliances support the ability for the same user account to login simultaneously?

    **Answer:** Yes, this is supported on 1.5 and newer firmware releases. On the portal layout, you can enable or disable 'Enforce login uniqueness' option. If this box is unchecked, users can log in simultaneously with the same username and password.

52. Does the SRA appliance support NT LAN Manager (NTLM) Authentication?

    **Answer**: Yes, in SRA 5.0 and later releases, backend Web servers using NTLM or Windows Integrated Authentication are supported. Single Sign-On with NTLM is also supported. NTLM support is specific to Application Offloading and/or reverse-proxy bookmarks.

    SRA 3.5 and earlier do not support NTLM authentication. As a work around, the administrator can turn on basic or digest authentication. Basic authentication specifies the username and password in clear text, but the security outside the intranet is not compromised because the SRA uses HTTPS. However, the intranet is required to be "trusted". Digest authentication works better in this case, because the password is not sent in clear text and only a MD5 checksum that incorporates the password is sent.

53. I cannot connect to a web server when Windows Authentication is enabled. I get the following error message when I try that: 'It appears that the target web server is using an unsupported HTTP(S) authentication scheme through the SRA, which currently supports only basic and digest authentication schemes. Please 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 anonymous or basic authentication is supported.

54. Why do Java Services, such as Telnet or SSH, not work through a proxy server?

    **Answer**: When the Java Service is started it does not use the proxy server. Transactions are done directly to the SRA appliance.

55. Why won't the SSH client connect to my SSH server?

    **Answer**: Check the version of SSH you have enabled on your server, and check the firmware release on the SRA appliance. SSHv2 support was not added until firmware 2.0 and newer. It's possible that there is a mismatch between the two.

56. How are the F1-F12 keys handled in the Java-based SSHv1 and Telnet proxies?

    **Answer**: The Telnet server must support function keys. If it does, the keyboard used is relevant. Currently, the Telnet proxy uses vt320 and the SSHv1 proxy uses vt100 key codes. This is the default and the SRA appliance does not support other types such as SCO-ANSI yet. This may be supported in a future firmware release.

57. 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.

58. 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/.

59. When I access Microsoft Telnet Server using a telnet bookmark it does not allow me to enter a user name -- why?

    **Answer:** This is not currently supported on the appliance.

**60.** What versions of Citrix are supported?

**Answer**: Citrix Portal Bookmarks have been tested and verified to support the following Citrix Application Virtualization platforms through the Citrix Web Interface:

Servers:

- Citrix XenApp 6.5
- Citrix XenApp 6.0
- XenApp 5.0
- XenApp 4.5
- XenApp Server 4.5
- Presentation Server 4.0

Clients:

- Receiver for Windows 3.0 client, for Citrix ActiveX bookmarks
- Receiver for Java 10.1 client for Citrix Java bookmarks
- XenApp Plugin version 12.0.3 or earlier
- Java client version 10 or earlier

For browsers requiring Java to run Citrix, you must have Sun Java 1.6.0_10 or above.

# Appendix F

# 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 perform specific tasks. It is a critical part of the deployment of the SRA Virtual Appliance, where basic networking needs to be configured from the console. The CLI is also supported on the SRA 4600, 4200, 1600, and 1200 appliances.

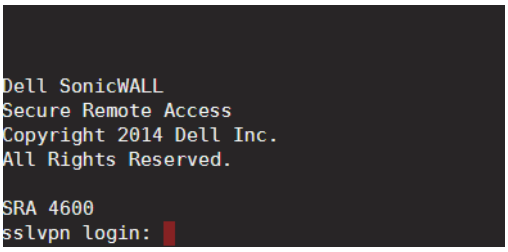
While the SRA physical appliance products have a default IP address and network configuration that requires a client's network settings to be reconfigured to connect, the network settings in an existing VMware virtual environment might conflict with the SRA appliance defaults. The CLI utility remedies this by allowing basic configuration of the network settings when deploying the SRA Virtual Appliance.

**Note** The Dell SonicWALL SRA 6.0 CLI allows configuration of only the X0 interface on the SRA 4600/4200/1600/1200 or SRA Virtual Appliance.

For the 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

For the SRA 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 example below:

```
System Information
Model:               SRA 4200
Serial Number:       0017C54172D4
Version:             SonicOS SSL-VPN 5.5.0.0-11sv
CPU (Utilization):   1.8 GHz Via C7 Processor (2%)
```

```
Total Memory:        2 GB RAM, 1 GB Flash
System Time:         2011/08/18 13:39:51
Up Time:             0 Days 00:40:51
X0 IP Address:       192.168.200.1
X0 Subnet mask:      255.255.255.0
Default Gateway:     192.168.200.2
Primary DNS:         10.50.128.52
Secondary DNS:       n/a
Hostname:            sslvpn


Main Menu
1. Setup Wizard
2. Reboot
3. Restart SSL-VPN Services
4. Logout


Press <Ctrl-c> at any time to cancel changes and logout.
Select a number (1-4):
```

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): SRA4200


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:            SRA4200


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:

```
System Information
Model:                SRA 4200
Serial Number:        0017C54172D4
Version:              SonicOS SSL-VPN 5.5.0.0-11sv
CPU (Utilization):    1.8 GHz Via C7 Processor (2%)
Total Memory:         2 GB RAM, 1 GB Flash
System Time:          2011/08/18 13:39:51
Up Time:              0 Days 00:40:51
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:             SRA4200


Main Menu
1. Setup Wizard
2. Reboot
3. Restart SSL-VPN Services
4. Logout


Press <Ctrl-c> at any time to cancel changes and logout.
Select a number (1-4):
```

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 may be a delay of up to 5 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 SRA 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.

# Appendix G

# SMS Email Formats

This section provides a list of SMS (Short Message Service) formats for worldwide cellular carriers. Find the correct format for your carrier from the list below, using your own phone number before the @ sign.

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

| Carrier | SMS Format |
|---|---|
| 3River Wireless | 4085551212@sms.3rivers.net |
| AirTel | 4085551212@airtelmail.com |
| AT&T Wireless | 4085551212@mobile.att.net |
| Andhra Pradesh Airtel | 4085551212@airtelap.com |
| Andhra Pradesh Idea Cellular | 4085551212@ideacellular.net |
| Alltel PC | 4085551212@message.alltel.com |
| Alltel | 4085551212@alltelmessage.com |
| Arch Wireless | 4085551212@archwireless.net |
| BeeLine GSM | 4085551212@sms.beemail.ru |
| BeeLine (Moscow) | 4085551212@sms.gate.ru |
| Bell Canada | 4085551212@txt.bellmobility.ca |
| Bell Canada | 4085551212@bellmobility.ca |
| Bell Atlantic | 4085551212@message.bam.com |
| Bell South | 4085551212@sms.bellsouth.com |
| Bell South | 4085551212@wireless.bellsouth.com |
| Bell South | 4085551212@blsdcs.net |
| Bite GSM (Lithuania) | 4085551212@sms.bite.lt |
| Bluegrass Cellular | 4085551212@sms.bluecell.com |
| BPL mobile | 4085551212@bplmobile.com |
| Celcom (Malaysia) | 4085551212@sms.celcom.com.my |
| Cellular One | 4085551212@mobile.celloneusa.com |
| Cellular One East Cost | 4085551212@phone.cellone.net |
| Cellular One South West | 4085551212@swmsg.com |
| Cellular One | 4085551212@mobile.celloneusa.com |
| Cellular One | 4085551212@cellularone.txtmsg.com |
| Cellular One | 4085551212@cellularone.textmsg.com |
| Cellular South | 4085551212@csouth1.com |
| CenturyTel | 4085551212@messaging.centurytel.net |
| Cingular | 4085551212@mobile.mycingular.net |
| Cingular Wireless | 4085551212@mycingular.textmsg.com |
| Comcast | 4085551212@comcastpcs.textmsg.com |
| CZECH EuroTel | 4085551212@sms.eurotel.cz |
| CZECH Paegas | 4085551212@sms.paegas.cz |

| Carrier | SMS Format |
|---|---|
| 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 |
| 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 |

| Carrier | SMS Format |
|---|---|
| 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 |
| 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 |

| Carrier | SMS Format |
|---|---|
| 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 |
| Swisscom | 4085551212@bluemail.ch |
| Telecom Italia Mobile (Italy) | 4085551212@posta.tim.it |
| Telenor Mobil Norway | 4085551212@mobilpost.com |
| Telecel (Portugal) | 4085551212@sms.telecel.pt |
| Tele2 | 4085551212@sms.tele2.lv |
| Tele Danmark Mobil | 4085551212@sms.tdk.dk |
| Telus | 4085551212@msg.telus.com |
| Telenor | 4085551212@mobilpost.no |
| Telia Denmark | 4085551212@gsm1800.telia.dk |
| TIM | 4085551212 @timnet.com |
| TMN (Portugal) | 4085551212@mail.tmn.pt |
| T-Mobile Austria | 4085551212@sms.t-mobile.at |
| T-Mobile Germany | 4085551212@t-d1-sms.de |
| T-Mobile UK | 4085551212@t-mobile.uk.net |
| T-Mobile USA | 4085551212@tmomail.net |
| Triton | 4085551212@tms.suncom.com |
| Tamil Nadu Aircel | 4085551212@airsms.com |
| Tamil Nadu BPL Mobile | 4085551212 @bplmobile.com |
| UMC GSM | 4085551212@sms.umc.com.ua |
| Unicel | 4085551212@utext.com |
| Uraltel | 4085551212@sms.uraltel.ru |
| US Cellular | 4085551212@email.uscc.net |
| US West | 4085551212@uswestdatamail.com |
| Uttar Pradesh (West) Escotel | 4085551212@escotelmobile.com |
| Verizon | 4085551212@vtext.com |
| Verizon PCS | 4085551212@myvzw.com |
| Virgin Mobile | 4085551212@vmobl.com |
| Vodafone Omnitel (Italy) | 4085551212@vizzavi.it |
| Vodafone Italy | 4085551212@sms.vodafone.it |
| Vodafone Japan | 4085551212@pc.vodafone.ne.j |
| Vodafone Japan | 4085551212@h.vodafone.ne.jp |

| Carrier | SMS Format |
|---|---|
| Vodafone Japan | 4085551212@t.vodafone.ne.jp |
| Vodafone Spain | 4085551212@vodafone.es |
| Vodafone UK | 4085551212@vodafone.net |
| West Central Wireless | 4085551212@sms.wcc.net |
| Western Wireless | 4085551212@cellularonewest.com |

# Appendix H

# Support Information

This appendix contains the following sections:


- Contact Information on page 483
- Limited Hardware Warranty on page 483
- GNU General Public License (GPL) Source Code on page 484
- End User Licensing Agreement on page 484


# Contact Information

For timely resolution of technical support questions and the latest technical support telephone numbers, visit Dell SonicWALL on the Internet.

Support Contact Information:

Contact Support Page - http://www.sonicwall.com/us/support/contact.html

Contact Dell SonicWALL Page - http://www.sonicwall.com/us/company/286.html

# Limited Hardware Warranty

All Dell SonicWALL appliances come with a 1-year Limited Hardware Warranty which provides delivery of critical replacement parts for defective parts under warranty. In addition, for 90 days from the warranty start date, Dell SonicWALL SRA 4600/1600 appliances are entitled to a Limited Software Warranty which provides bug fixes, updates and any maintenance releases that occur during the coverage term. Visit the Warranty Information page for details on your product's warranty:
http://www.sonicwall.com/us/support/Services.html#tab=warranty

Dell SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by Dell SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. Dell SonicWALL and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At Dell SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. Dell SonicWALL's obligations under this warranty are contingent upon the return of the defective product according to the terms of Dell SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of Dell SonicWALL.

**DISCLAIMER OF WARRANTY**. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

**DISCLAIMER OF LIABILITY.** DELL SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL DELL 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 DELL SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Dell 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.

# GNU General Public License (GPL) Source Code

Dell SonicWALL will provide a machine-readable copy of the GPL open source on a CD. To obtain a complete machine-readable copy, send your written request, along with a certified check or money order in the amount of US $25.00 payable to "Dell SonicWALL, Inc." to:

General Public License Source Code Request
Dell SonicWALL, Inc. Attn: Jennifer Anderson
2001 Logic Drive
San Jose, CA 95124-3452

# End User Licensing Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SONICWALL PRODUCT. BY INSTALLING OR USING THE SONICWALL PRODUCT, YOU (AS THE CUSTOMER, OR IF NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) INDICATE ACCEPTANCE OF AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT FOR AND ON BEHALF OF THE CUSTOMER. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, THEN DO NOT USE THE PRODUCT AND RETURN IT TO THE PLACE OF PURCHASE WITH PROOF OF PURCHASE WITHIN THIRTY (30) DAYS OF PURCHASE FOR A REFUND. IF YOU DO PROCEED TO INSTALL OR USE THE SONICWALL PRODUCT, YOU WILL HAVE INDICATED

ACCEPTANCE AND AGREEMENT WITH THE TERMS AND CONDITIONS HEREIN. NOTWITHSTANDING THE FOREGOING, THIS AGREEMENT SHALL NOT SUPERSEDE ANY OTHER SIGNED AGREEMENT BETWEEN YOU AND SONICWALL THAT EXPRESSLY GOVERNS THE SONICWALL PRODUCT.

"Product" means the SonicWALL labeled hardware and related documentation ("Hardware") and/or proprietary SonicWALL labeled software, firmware and related documentation ("Software") purchased by the end user of the product either directly from SonicWALL or a Reseller (“Customer”). “Services” means the Support Services described below and any other services provided with or for the Products directly by SonicWALL or its agents. “Reseller” shall mean those entities to which SonicWALL or SonicWALL’s authorized distributors distribute the Products for resale to end users. Except as otherwise agreed upon by the parties, this Agreement will also cover any updates and upgrades to the Products provided to Customer by SonicWALL directly or through a Reseller (except as may be otherwise indicated, such updates and upgrades shall be deemed Products).

## 1. LICENSE(S) AND RESTRICTIONS

(a) Licenses. Subject to the terms and conditions of this Agreement, SonicWALL grants to Customer, and Customer accepts from SonicWALL, a nonexclusive, nontransferable (except as otherwise set forth herein) and nonsublicensable license (“License”) to:

(i) execute and use the Software on the Hardware with which the Software is provided (pre-installed) in accordance with the applicable Documentation; and,

(ii) for Software provided in standalone form (without Hardware), install, execute and use the Software on the Hardware or hardware device(s) on which it is intended to be used in accordance with the applicable Documentation and the License purchased. If Customer purchased multiple copies of standalone Software, Customer’s License to such standalone Software includes the right to install, use and execute up to the number of copies of Software Licenses purchased.

In addition, the License includes the right to (x) make a reasonable number of additional copies of the Software to be used solely for non-productive archival purposes, and (y) make and use copies of the end user documentation for Hardware and/or Software provided with the Products (“Documentation”) as reasonably necessary to support Customer’s authorized users in their use of the Products.

(b) License Limitations. Order acknowledgments, Documentation and/or the particular type of the Products/ Licenses purchased by Customer may specify limits on Customer’s use of the Software, and which limits apply to the License(s) granted hereunder for such Software. Such limits may consist of limiting the term of the License, or the number or amount of nodes, storage space, sessions, calls, users, subscribers, clusters, devices, ports, bandwidth, throughput or other elements, and/or or require the purchase of separate Licenses to use or obtain particular features, functionalities, services, applications or other items. Use of the Software shall be subject to all such limitations.

(c) For Customer’s Internal Business. Each License shall be used by Customer solely to manage its own internal business operations as well as the business operations of its Affiliates. Notwithstanding the foregoing, if Customer is in the regular business of providing firewall, VPN or Security management for a fee to entities that are not its Affiliates (“MSP Customers”), Customer may use the Products for its MSP Customers provided that either (i) Customer, and not MSP Customers, maintain control and possession of the Products, or (ii) if MSP Customers have possession and/or control of Products in whole or in part, this Agreement must be provided to MSP Customers and they must agree that their use of the Products is subject to the terms and conditions of this Agreement. Customer agrees to indemnify and hold SonicWALL harmless from and against any claims by MSP Customers against SonicWALL relating to the

Products and/or Customer's services for MSP Customers. "Affiliate" means any legal entity controlling, controlled by, or under common control with a party to this Agreement, but only for so long as such control relationship exists.

(d) Evaluation License. If the Software is provided by SonicWALL or a Reseller at no charge for evaluation purposes, then Section 1(a) above shall not apply to such Software and instead Customer is granted a nonproduction License to use such Software and the associated documentation solely for Customer's own internal evaluation purposes for an evaluation period of up to thirty (30) days from the date of delivery of the Software, plus any extensions granted by SonicWALL in writing (the "Evaluation Period"). There is no fee for Customer's use of the Software for nonproduction evaluation purposes 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. Notwithstanding anything otherwise set forth in this Agreement, Customer understands and agrees that evaluation Software is provided "AS IS" and that SonicWALL does not provide a warranty or maintenance services for evaluation Licenses.

(e) Restrictions. Customer may not (i) modify, translate, localize, adapt, rent, lease, loan, create or prepare derivative works of, or create a patent based on the Software or any part thereof, (ii) make copies except as expressly authorized under this Agreement, (iii) copy the Software onto any public or distributed network, (iv) modify or resell the Software, use the Software in connection with the operation of any nuclear facilities, or use for purposes which are competitive to SonicWALL, or (v) except as expressly authorized in Section 2(c) above, operate the Software for use in any time-sharing, outsourcing, service bureau or application service provider type environment. Unless and except to the extent authorized in the applicable Documentation, Software provided with and/or as the Product, in part or whole, is licensed for use only in accordance with the Documentation as part of the Product: Software components making up a Product may not be separated from, nor used on a separate or standalone basis from the Product. 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. Any Software provided in object code form is licensed hereunder only in object code form. Except to the extent allowed by applicable law if located in the European Union, and then only with prior written notice to SonicWALL, Customer shall not disassemble or reverse engineer the Software in whole or in part or authorize others to do so. Customer agrees not to use the Software to perform comparisons or other "benchmarking" activities, either alone or in connection with any other software or service, without SonicWALL's written permission; or publish any such performance information or comparisons.

(f) Third Party Software. There may be certain third party owned software provided along with, or incorporated within, the Products ("Third Party Software"). Except as set forth below, such Third Party Software shall be considered Software governed by the terms and conditions of this Agreement. However, some Products may contain other Third Party Software that is provided with a separate license agreement, in which case such Third Party Software will be governed exclusively by such separate license agreement ("Third Party License") and not this Agreement. Any such Third Party Software that is governed by a Third Party License, and not this Agreement, will be identified on the applicable Product page on SonicWALL's website and/or in a file provided with the Product. Except as SonicWALL may otherwise inform Customer in writing, the Third Party License gives Customer at least the license rights granted above, and may provide additional license rights as to the Third Party Software, but only with respect to the particular Third Party Software to which the Third Party License applies. SUCH THIRD PARTY SOFTWARE UNDER A THIRD PARTY LICENSE IS PROVIDED WITHOUT ANY WARRANTY FROM SONICWALL AND ITS SUPPLIERS, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. Notwithstanding the foregoing, SonicWALL shall honor its warranty,

maintenance and support obligations in respect to the SonicWALL Products regardless of whether the warranty, maintenance or support issue is caused in whole or in part by the Third Party Software provided by SonicWALL with the Product.

(g) Updates/Upgrades. If Customer purchases or otherwise is eligible to receive a SOFTWARE update or upgrade, you must be properly licensed to use the Product identified by SonicWALL as being eligible for the update/ upgrade in order to install and use the SOFTWARE update/ upgrade. A SOFTWARE update/ upgrade replaces and/or supplements the Software Product that formed the basis for your eligibility for the update/upgrade, and does not provide you an additional License (copy) of the Software to use separately from the Software Product to be updated/ upgraded. You may use the resulting updated/upgraded Product only in accordance with the terms of this Agreement.

(h) Activation Keys May Expire. Certain Products, including Security Services that provide regular ongoing updates for Software (e.g., Security Service consisting of anti-virus signature updates), may come with an activation key or license key (a key that must be entered to activate the Product, “Activation Key”). If the Activation Key for a Product is not activated within five (5) years from the date of issuance by SonicWALL, such Activation Key(s) may expire and no longer activate the Product. Products that come with an expiring Activation Key will operate for the contracted term of the License (or purchased Security Service), so long as the Activation Key is activated within five (5) years from SonicWALL’s date of issuance.

## 2. OWNERSHIP

SonicWALL and its licensors are the sole and exclusive owners of the Software, and all underlying intellectual property rights in the Hardware. All rights not expressly granted to Customer are reserved by SonicWALL and its licensors.

## 3. TERMINATION OF LICENSE(S)

All licenses to the Software hereunder shall terminate if Customer fails to comply with any of the provisions of this Agreement and does not remedy such breach within thirty (30) days after receiving written notice from SonicWALL. Customer agrees upon termination to immediately cease using the Software and to destroy all copies of the Software which may have been provided or created hereunder.

## 4. SUPPORT SERVICES

SonicWALL’s current Support Service offerings (“Support Services”) and the terms and conditions applicable to such Support Services are set forth in SonicWALL’s Support Services Terms located http://www.sonicwall.com/us/support/ Services.html and are incorporated herein by reference. Support Services may require an additional fee. Unless otherwise agreed to in writing, SonicWALL’s Support Services are subject to SonicWALL’s Support Services Terms which are in effect at the time the Support Services are purchased by Customer, and these terms and conditions will be incorporated herein by reference at that time. SonicWALL reserves the right to change the Support Services Terms from time to time by posting such changes on its website, which shall apply to any Support Services purchased on or after the date of such posting.

## 5. SONICWALL WARRANTY

(a) Warranty. SonicWALL warrants to Customer (original purchaser Customer only) that for the applicable warranty period (“Warranty Period”) the Hardware will be free from any material defects in materials or workmanship and the Software, if any, will substantially conform to the

Documentation applicable to the Software and the License purchased (“Limited Warranty”). Except as may indicated otherwise in writing by SonicWALL, the Warranty Period for Hardware is one year from the date of registration of the Hardware Product (or if sooner, seven days after initial delivery of the Hardware Product to Customer), and the applicable warranty period for Software is ninety days from the date of registration of the Software Product (or if sooner, seven days after initial delivery/download) of the Software Product to/by Customer. SonicWALL does not warrant that use of the Product(s) will be uninterrupted or error free nor that SonicWALL will correct all errors. The Limited Warranty shall not apply to any non-conformance (i) that SonicWALL cannot recreate after exercising commercially reasonable efforts to attempt to do so; (ii) caused by misuse of the Product or by using the Product in a manner that is inconsistent with this Agreement or the Documentation; (iii) arising from the modification of the Products by anyone other than SonicWALL; or (iv) caused by any problem or error in third party software or hardware not provided by SonicWALL with the Product regardless of whether or not the SonicWALL Product is designed to operate with such third party software or hardware. SonicWALL's sole obligation and Customer's sole and exclusive remedy under any express or implied warranties hereunder shall be for SonicWALL to use commercially reasonable efforts to provide error corrections and/or, if applicable, repair or replace parts in accordance with SonicWALL’s Support Services Terms. Customer shall have no rights or remedies under this Limited Warranty unless SonicWALL receives Customer’s detailed written warranty claim within the applicable warranty period.

(b) Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH ABOVE, TO MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW SONICWALL HEREBY DISCLAIMS ON BEHALF OF ITSELF, ITS SUPPLIERS, DISTRIBUTORS AND RESELLERS ALL WARRANTIES, EXPRESS, STATUTORY AND IMPLIED, APPLICABLE TO THE PRODUCTS, SERVICES AND/OR THE SUBJECT MATTER OF THIS AGREEMENT, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE.

## 6. LIMITATION OF LIABILITY

The Products are not designed, manufactured, authorized or warranted to be suitable for use in any system where a failure of such system could result in a situation that threatens the safety of human life, including without limitation any such medical, life support, aviation or nuclear applications. Any such use and subsequent liabilities that may arise from such use are totally the responsibility of Customer, and all liability of SonicWALL, whether in contract, tort (including without limitation negligence) or otherwise in relation to the same is excluded. Customer shall be responsible for mirroring its data, for backing it up frequently and regularly, and for taking all reasonable precautions to prevent data loss or corruption. SonicWALL shall not be responsible for any system downtime, loss or corruption of data or loss of production. NOTWITHSTANDING ANYTHING ELSE IN THIS AGREEMENT OR OTHERWISE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SONICWALL, ITS SUPPLIERS, DISTRIBUTORS OR RESELLERS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, LOST OR CORRUPTED DATA, LOST PROFITS OR SAVINGS, LOSS OF BUSINESS OR OTHER ECONOMIC LOSS OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, ARISING OUT OF OR RELATED TO THIS AGREEMENT, THE PRODUCTS OR THE SERVICES, WHETHER OR NOT BASED ON TORT, CONTRACT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND WHETHER OR NOT SONICWALL HAS BEEN ADVISED OR KNEW OF THE POSSIBILITY OF SUCH DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, SONICWALL'S MAXIMUM LIABILITY TO CUSTOMER ARISING FROM OR RELATING TO THIS AGREEMENT SHALL BE LIMITED TO THE AMOUNTS RECEIVED BY SONICWALL FOR THE PRODUCTS AND THE SERVICES PURCHASED BY CUSTOMER, PROVIDED THAT WHERE ANY CLAIM AGAINST SONICWALL RELATES TO PARTICULAR PRODUCT AND/OR SERVICES, SONICWALL’S MAXIMUM LIABILITY SHALL BE LIMITED TO THE

AGGREGATE AMOUNT RECIEVED BY SONICWALL IN RESPECT OF THE PRODUCTS AND/OR SERVICES PURCHASED BY CUSTOMER AFFECTED BY THE MATTER GIVING RISE TO THE CLAIM. (FOR MAINTENANCE SERVICES OR A PRODUCT SUBJECT TO RECURRING FEES, THE LIABILITY SHALL NOT EXCEED THE AMOUNT RECEIVED BY SONICWALL FOR SUCH MAINTENANCE SERVICE OR PRODUCT PURCHASED BY CUSTOMER DURING THE TWELVE (12) MONTHS PRECEDING THE CLAIM). CUSTOMER EXPRESSLY AGREES TO THE ALLOCATION OF LIABILITY SET FORTH IN THIS SECTION, AND ACKNOWLEDGES THAT WITHOUT ITS AGREEMENT TO THESE LIMITATIONS, THE PRICES CHARGED FOR THE PRODUCTS AND SERVICES WOULD BE HIGHER.

## 7. GOVERNMENT RESTRICTIONS

Customer agrees that it will not export or re-export the Products without SonicWALL's prior written consent, and then only in compliance with all requirements of applicable law, including but not limited to U.S. export control regulations. Customer has the responsibility to obtain any required licenses to export, reexport or import the Products. Customer shall defend, indemnify and hold SonicWALL and its suppliers harmless from any claims arising out of Customer’s violation of any export control laws relating to any exporting of the Products. By accepting this Agreement and receiving the Products, Customer confirms that it and its employees and agents who may access the Products are not listed on any governmental export exclusion lists and will not export or re-export the Products to any country embargoed by the U.S. or to any specially denied national (SDN) or denied entity identified by the U.S. Applicable export restrictions and exclusions are available at the official web site of the U.S. Department of Commerce Bureau of Industry and Security (www.bis.doc.gov). For purchase by U.S. governmental entities, the technical data and computer software in the Products are commercial technical data and commercial computer software as subject to FAR Sections 12.211, 12.212, 27.405-3 and DFARS Section 227.7202. The rights to use the Products and the underlying commercial technical date and computer software is limited to those rights customarily provided to the public purchasers as set forth in this Agreement. The Software and accompanying Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

## 8. 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. 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. Any action seeking enforcement of this Agreement or any provision hereof shall be brought exclusively in the state or federal courts located in the County of Santa Clara, State of California, United States of America. Each party hereby agrees to submit to the jurisdiction of such courts. Notwithstanding the foregoing, SonicWALL is entitled to seek immediate injunctive relief in any jurisdiction in the event of any alleged breach of Section 1 and/or to otherwise protect its intellectual property.

b) Assignment. Except as otherwise set forth herein, Customer shall not, in whole or part, assign or transfer any part of this Agreement or any rights hereunder without the prior written consent of SonicWALL. Any attempted transfer or assignment by Customer that is not permitted by this Agreement shall be null and void. Any transfer/assignment of a License that is permitted

hereunder shall require the assignment/transfer of all copies of the applicable Software along with a copy of this Agreement, the assignee must agree to all terms and conditions of this Agreement as a condition of the assignment/transfer, and the License(s) held by the transferor Customer shall terminate upon any such transfer/assignment.

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 and the remaining provisions of this Agreement will remain in full force and effect.

d) Privacy Policy. Customer hereby acknowledges and agrees that SonicWALL's performance of this Agreement may require SonicWALL to process or store personal data of Customer, its employees and Affiliates, and to transmit such data within SonicWALL or to SonicWALL Affiliates, partners and/or agents. Such processing, storage, and transmission may be used for the purpose of enabling SonicWALL to perform its obligations under this Agreement, and as described in SonicWALL's Privacy Policy (www.SonicWALL.com/us/Privacy_Policy.html, "Privacy Policy") and may take place in any of the countries in which SonicWALL and its Affiliates conduct business, including countries outside of the European Economic Area. SonicWALL reserves the right to change the Privacy Policy from time to time as described in the Privacy Policy.

e) Notices. All notices provided hereunder shall be in writing, delivered personally, or sent by internationally recognized express courier service (e.g., Federal Express), addressed to the legal department of the respective party or to such other address as may be specified in writing by either of the parties to the other in accordance with this Section.

f) Disclosure of Customer Status. SonicWALL may include Customer in its listing of customers and, upon written consent by Customer, announce Customer's selection of SonicWALL 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) 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.

i) Audit. Customer shall maintain accurate records to verify compliance with this Agreement. Upon request by SonicWALL, Customer shall furnish (a copy of) such records to SonicWALL and certify its compliance with this Agreement.

j) 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."

k) Entire Agreement. This Agreement is intended by the parties as a final expression of their agreement with respect to the subject matter hereof 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 judicial proceeding that may involve the Agreement. This Agreement represents the complete agreement and understanding of the parties with respect to the subject matter herein. This Agreement may be modified only through a written instrument signed by both parties.

# Appendix I

# Glossary

**Active Directory (AD)** - A centralized directory service system produced by Microsoft that automates network management of user data, security and resources, and enables interoperation with other directories. Active Directory is designed especially for distributed networking environments.

**Common Internet File System (CIFS)** - a protocol that defines a standard for remote file access, allowing users with different platforms and computers to share files without installing special software.

**File Shares** - Dell SonicWALL's network file browsing feature on the SRA appliance. This uses the Web browser to browse shared files on the network.

**Lightweight Directory Access Protocol (LDAP)** - An Internet protocol that email and other programs use to retrieve data from a server.

**One-time Password** - A randomly-generated, single-use password. One-time Password may be used to refer to a particular instance of a password, or to the feature as a whole.

**Simple Mail Transfer Protocol (SMTP)** - A protocol for sending email messages between servers.

**Secure Socket Layer Virtual Private Network (SRA**) - A remote access tool that utilizes a Web browser to provide clientless access to private applications.

**Virtual Office** - The user interface of the SRA appliance.

**Windows Internet Naming Service (WINS)** - A system that determines the IP address associated with a network computer.