



Single Sign-On in SonicOS Enhanced 5.6

Document Scope

This document describes how to install and configure the Single Sign-On feature in the SonicOS Enhanced 5.6 release.

This document contains the following sections:

- [“Single Sign-On Overview” section on page 1](#)
- [“Installing the SonicWALL SSO Agent” section on page 11](#)
- [“Installing the SonicWALL Terminal Services Agent” section on page 16](#)
- [“Configuring the SonicWALL SSO Agent” section on page 18](#)
- [“Configuring the SonicWALL Terminal Services Agent” section on page 25](#)
- [“Using NDConnector with SonicWALL SSO” section on page 27](#)
- [“Configuring Your SonicWALL Security Appliance” section on page 32](#)
- [“Glossary” section on page 61](#)

Single Sign-On Overview

This section provides an introduction to the SonicWALL Single Sign-On feature. This section contains the following subsections:

- [“What Is Single Sign-On?” section on page 1](#)
- [“Benefits of SonicWALL SSO” section on page 3](#)
- [“Platforms and Supported Standards” section on page 3](#)
- [“How Does Single Sign-On Work?” section on page 5](#)
- [“How Does SonicWALL SSO Agent Work?” section on page 6](#)
- [“How Does SonicWALL Terminal Services Agent Work?” section on page 9](#)

What Is Single Sign-On?

Single Sign-On (SSO) is a transparent user authentication mechanism that provides privileged access to multiple network resources with a single login to the domain from a workstation or through a Windows Terminal Services or Citrix server. SonicWALL security appliances provide SSO functionality using the SonicWALL Single Sign-On Agent (SSO Agent) and SonicWALL Terminal Services Agent (TSA) to identify

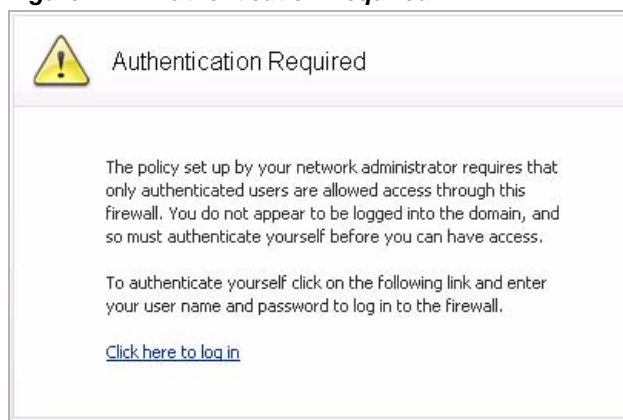
user activity. The SonicWALL Single Sign-On Agent (SSO Agent) identifies users based on workstation IP address. The SonicWALL TSA identifies users through a combination of server IP address, user name, and domain.

SonicWALL SSO is configured in the **Users > Settings** page of the SonicOS management interface. SSO is separate from the **Authentication method for login** settings, which can be used at the same time for authentication of VPN/L2TP client users or administrative users.

SonicWALL SSO Agent and TSA use a protocol compatible with SonicWALL ADConnector and NDConnector, and automatically determine when a user has logged out to prevent unauthorized access. Based on data from SonicWALL SSO Agent or TSA, the SonicWALL security appliance queries LDAP or the local database to determine group membership. Memberships are optionally checked by firewall policies to control who is given access, and can be used in selecting policies for Content Filtering and Application Firewall to control what they are allowed to access. User names learned via SSO are reported in logs of traffic and events from the users. The configured inactivity timer applies with SSO but the session limit does not, though users who are logged out are automatically and transparently logged back in when they send further traffic.

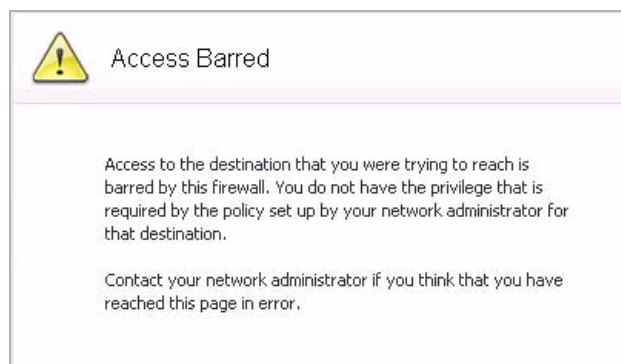
Users logged into a workstation or Terminal Services/Citrix server directly, but not logged into the domain will not be authenticated by default (although they can optionally be authenticated for limited access). For users that are not authenticated by SonicWALL SSO, the following screen will display, indicating that a manual login will be required for further authentication.

Figure 1 Authentication Required



Users that are identified but lack the group memberships required by the configured policy rules are redirected to the Access Barred page.

Figure 2 Access Barred



Benefits of SonicWALL SSO

SonicWALL SSO is a reliable and time-saving feature that utilizes a single login to provide access to multiple network resources based on administrator-configured group memberships and policy matching. SonicWALL SSO is transparent to end users and requires minimal administrator configuration.

By automatically determining when users have logged in or out based on workstation IP address traffic, or, for Terminal Services or Citrix, traffic from a particular user at the server IP address, SonicWALL SSO is secure and hands-free. SSO authentication is designed to operate with any external agent that can return the identity of a user at a workstation or Terminal Services/Citrix server IP address using a SonicWALL ADConnector-compatible protocol.

SonicWALL SSO works for any service on the SonicWALL security appliances that uses user-level authentication, including Content Filtering Service (CFS), Firewall Access Rules, group membership and inheritance, and security services (IPS, GAV, SPY and Application Firewall) inclusion/exclusion lists.

Other benefits of SonicWALL SSO include:

- Ease of use — Users only need to sign in once to gain automatic access to multiple resources.
- Improved user experience — Windows domain credentials can be used to authenticate a user for any traffic type without logging in using a Web browser.
- Transparency to users — Users are not required to re-enter user name and password for authentication.
- Secure communication — Shared key encryption for data transmission protection.
- SonicWALL SSO Agent can be installed on any Windows server on the LAN, and TSA can be installed on any terminal server.
- Multiple SSO Agents — Up to 8 agents are supported to provide capacity for large installations.
- Multiple TSAs — Multiple terminal services agents (one per terminal server) are supported. The number depends on the SonicWALL UTM appliance model and ranges from 4 to 256.
- Login mechanism works with any protocol, not just HTTP.

Platforms and Supported Standards

SonicWALL SSO is available on SonicWALL NSA Series appliances running SonicOS Enhanced 5.0 or higher, and SonicWALL PRO security appliances running SonicOS Enhanced 4.0 or higher. The SonicWALL SSO Agent is compatible with all versions of SonicOS Enhanced that support SonicWALL SSO. The SonicWALL TSA is supported on SonicOS Enhanced 5.6 and higher, running on SonicWALL NSA Series and TZ 210 Series appliances.

The SonicWALL SSO feature supports LDAP and local database protocols. SonicWALL SSO supports SonicWALL Directory Connector. SonicWALL SSO can also interwork with ADConnector in an installation that includes a SonicWALL CSM, but Directory Connector is recommended. For all features of SonicWALL SSO and the SSO Agent to work properly, SonicOS Enhanced 5.5 or higher should be used with Directory Connector 3.1.7 or higher. To use SonicWALL SSO with Windows Terminal Services or Citrix, SonicOS Enhanced 5.6 or higher is required, and SonicWALL TSA must be installed on the server.

SonicWALL SSO on SonicOS Enhanced 5.5 and higher is compatible with SonicWALL NDConnector for interoperability with Novell users. NDConnector is also available as part of Directory Connector.

To use SonicWALL SSO, it is required that the SonicWALL SSO Agent be installed on a server within your Windows domain that can reach clients and can be reached from the appliance, either directly or through a VPN path, and/or SonicWALL TSA be installed on any terminal servers in the domain.

SSO Agent Supported Platforms

The following requirements must be met in order to run the SonicWALL SSO Agent:

- UDP port 2258 (by default) must be open; the firewall uses UDP port 2258 by default to communicate with SonicWALL SSO Agent; if a custom port is configured instead of 2258, then this requirement applies to the custom port
- Windows Server, with latest service pack:
 - Windows Server 2008, 32-bit and 64-bit
 - Windows Server 2003, 32-bit and 64-bit
 - Windows 2000 Server, 32-bit and 64-bit
- .NET Framework:
 - .NET Framework 3.5
 - .NET Framework 3.0
 - .NET Framework 2.0
- Net API or WMI

**Note**

The following Microsoft Windows operating systems and service packs are **not** supported as platforms on which SonicWALL SSO Agent can be installed:

- Windows 7 – All versions
- Windows Vista – All versions
- Windows XP – All versions
- Windows 2000 – All non-server versions

**Note**

Mac and Linux PCs do not support the Windows networking requests that are used by the SonicWALL SSO Agent, and hence do not work with SonicWALL SSO. Mac and Linux users can still get access, but will need to log in to do so. They can be redirected to the login prompt if policy rules are set to require authentication. For more information, see [“Accommodating Mac and Linux Users” on page 55](#).

TSA Supported Platforms

The following requirements must be met in order to run the SonicWALL TSA:

- UDP port 2259 (by default) must be open on all terminal servers on which TSA is installed; the firewall uses UDP port 2259 by default to communicate with SonicWALL TSA; if a custom port is configured instead of 2259, then this requirement applies to the custom port
- Windows Server, with latest service pack:
 - Windows Server 2008, 32-bit and 64-bit
 - Windows Server 2003, 32-bit and 64-bit
- Windows Terminal Services or the following Citrix version installed on the Windows Server system(s):
 - Citrix XenApp 5.0

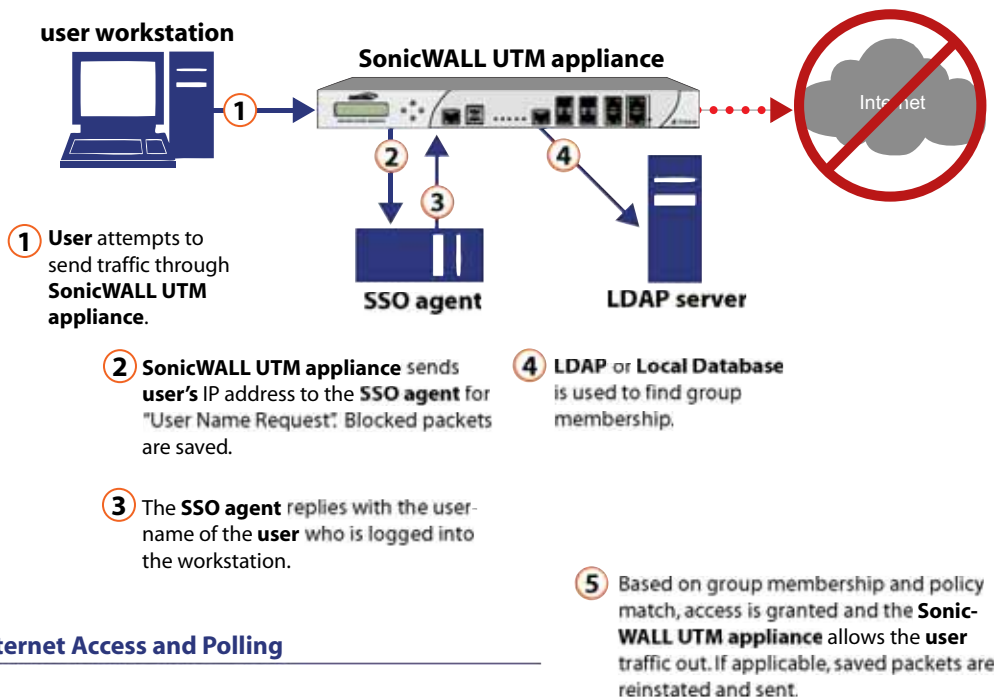
How Does Single Sign-On Work?

SonicWALL SSO requires minimal administrator configuration and is transparent to the user.

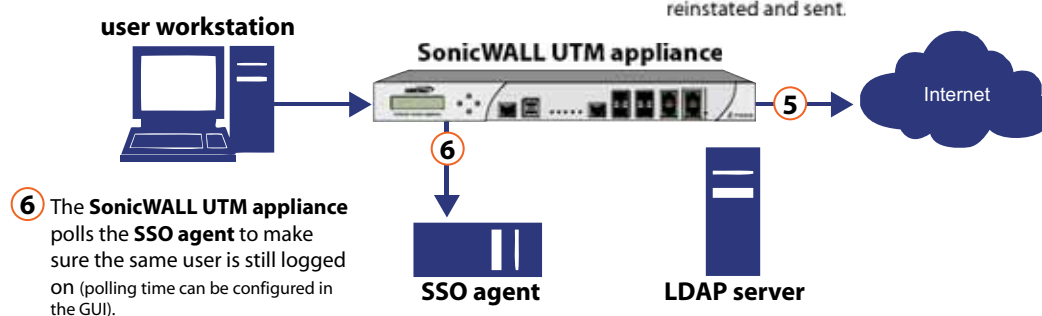
For users on individual workstations, the SSO Agent handles the authentication requests from the SonicWALL UTM appliance. There are six steps involved in SonicWALL SSO authentication, as illustrated in Figure 3.

Figure 3 SonicWALL Single Sign-On Process Using the SSO Agent

User Login Authorization



Internet Access and Polling



The SonicWALL SSO authentication process is initiated when user traffic passes through a SonicWALL security appliance, for example, when a user accesses the Internet. The sent packets are temporarily blocked and saved while the SonicWALL security appliance sends a "User Name" request and workstation IP address to the authorization agent running the SSO Agent.

The authorization agent running the SSO Agent provides the SonicWALL security appliance with the username currently logged into the workstation. A User IP Table entry is created for the logged in user, similarly to RADIUS and LDAP.

For users logged in from a Terminal Services or Citrix server, the SonicWALL TSA takes the place of the SSO Agent in the authentication process. The process is different in several ways:

- The TSA runs on the same server that the user is logged into, and includes the user name and domain along with the server IP address in the initial notification to the SonicWALL UTM appliance.
- Users are identified by a user number as well as the IP address (for non-Terminal Services users, there is only one user at any IP address and so no user number is used). A non-zero user number is displayed in the SonicOS management interface using the format "x.x.x.x user n", where x.x.x.x is the server IP address and n is the user number.
- The TSA sends a close notification to the UTM when the user logs out, so no polling occurs.

Once a user has been identified, the SonicWALL security appliance queries LDAP or a local database (based on administrator configuration) to find user group memberships, match the memberships against policy, and grant or restrict access to the user accordingly. Upon successful completion of the login sequence, the saved packets are sent on. If packets are received from the same source address before the sequence is completed, only the most recent packet will be saved.

User names are returned from the authorization agent running the SSO Agent in the format <domain>/<user-name>. For locally configured user groups, the user name can be configured to be the full name returned from the authorization agent running the SSO Agent (configuring the names in the SonicWALL security appliance local user database to match) or a simple user name with the domain component stripped off (default).

For the LDAP protocol, the <domain>/<user-name> format is converted to an LDAP distinguished name by creating an LDAP search for an object of class "domain" with a "dc" (domain component) attribute that matches the domain name. If one is found, then its distinguished name will be used as the directory sub-tree to search for the user's object. For example, if the user name is returned as "SV/bob" then a search for an object with "objectClass=domain" and "dc=SV" will be performed. If that returns an object with distinguished name "dc=sv,dc=us,dc=sonicwall,dc=com," then a search under that directory sub-tree will be created for (in the Active Directory case) an object with "objectClass=user" and "sAMAccountName=bob". If no domain object is found, then the search for the user object will be made from the top of the directory tree.

Once a domain object has been found, the information is saved to avoid searching for the same object. If an attempt to locate a user in a saved domain fails, the saved domain information will be deleted and another search for the domain object will be made.

User logout is handled slightly differently by SonicWALL SSO using the SSO Agent as compared to SSO with the TSA. The SonicWALL security appliance polls the authorization agent running the SSO Agent at a configurable rate to determine when a user has logged out. Upon user logout, the authentication agent running the SSO Agent sends a User Logged Out response to the SonicWALL security appliance, confirming that the user has been logged out and terminating the SSO session. Rather than being polled by the SonicWALL UTM appliance, the TSA itself monitors the Terminal Services / Citrix server for logout events and notifies the SonicWALL UTM appliance as they occur, terminating the SSO session. For both agents, configurable inactivity timers can be set, and for the SSO Agent the user name request polling rate can be configured (set a short poll time for quick detection of logouts, or a longer polling time for less overhead on the system).

How Does SonicWALL SSO Agent Work?

The SonicWALL SSO Agent can be installed on any workstation with a Windows domain that can communicate with clients and the SonicWALL security appliance directly using the IP address or using a path, such as VPN. For installation instructions for the SonicWALL SSO Agent, refer to the ["Installing the SonicWALL SSO Agent" section on page 11](#).

Multiple SSO agents are supported to accommodate large installations with thousands of users. You can configure up to eight SSO agents, each running on a dedicated, high-performance PC in your network. Note that one SSO agent on a fast PC can support up to 2500 users.

The SonicWALL SSO Agent only communicates with clients and the SonicWALL security appliance. SonicWALL SSO Agent uses a shared key for encryption of messages between the SSO Agent and the SonicWALL security appliance.

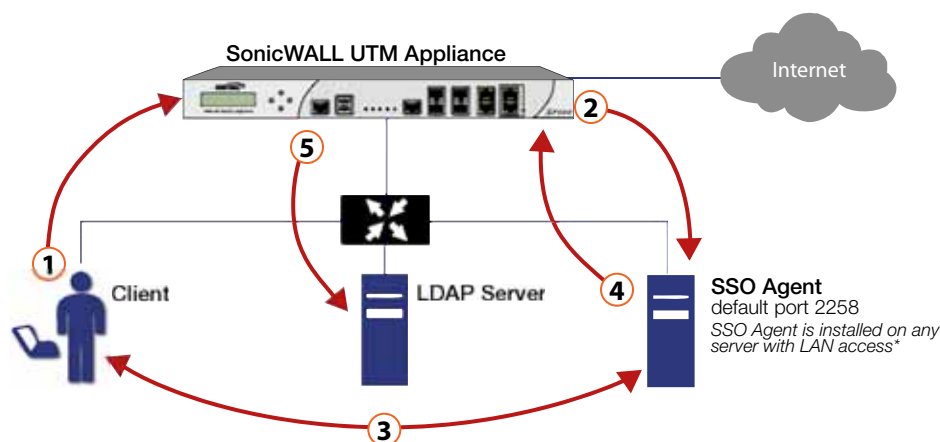


Note

The shared key is generated in the SSO Agent and the key entered in the SonicWALL security appliance during SSO configuration must match the SSO Agent-generated key exactly.

Figure 4 SonicWALL SSO Agent Process

SonicWALL SSO with SSO Agent



- 1 A client logs into the network and attempts to access the Internet or other network resources.
- 2 The SSO module on the SonicWALL UTM appliance queries the SonicWALL SSO Agent (default port 2258) for the client ID.
- 3 The SonicWALL SSO Agent forwards the request to the client and the client responds with its client ID.
- 4 Client ID information is passed back from the SonicWALL SSO Agent to the SonicWALL UTM appliance.
- 5 Based on the client ID, the SonicWALL UTM appliance checks with the LDAP server to determine group membership and permissions.

Steps 2 3 4

Communication in these steps (between the SSO Agent and client / firewall) is encrypted using a shared key which is generated by the SSO Agent.

The SonicWALL security appliance queries the SonicWALL SSO Agent over the default port 2258. The SSO Agent then communicates between the client and the SonicWALL security appliance to determine the client's user ID. The SonicWALL SSO Agent is polled, at a rate that is configurable by the administrator, by the SonicWALL security appliance to continually confirm a user's login status.

Logging

The SonicWALL SSO Agent sends log event messages to the Windows Event Log based on administrator-selected logging levels.

The SonicWALL security appliance also logs SSO Agent-specific events in its event log. The following is a list of SSO Agent-specific log event messages from the SonicWALL security appliance:

- **User login denied - not allowed by policy rule** – The user has been identified and does not belong to any user groups allowed by the policy blocking the user's traffic.
- **User login denied - not found locally** – The user has not been found locally, and **Allow only users listed locally** is selected in the SonicWALL security appliance.
- **User login denied - SSO Agent agent timeout** – Attempts to contact the SonicWALL SSO Agent have timed out.
- **User login denied - SSO Agent configuration error** – The SSO Agent is not properly configured to allow access for this user.
- **User login denied - SSO Agent communication problem** – There is a problem communicating with the workstation running the SonicWALL SSO Agent.
- **User login denied - SSO Agent agent name resolution failed** – The SonicWALL SSO Agent is unable to resolve the user name.
- **SSO Agent returned user name too long** – The user name is too long.
- **SSO Agent returned domain name too long** – The domain name is too long.



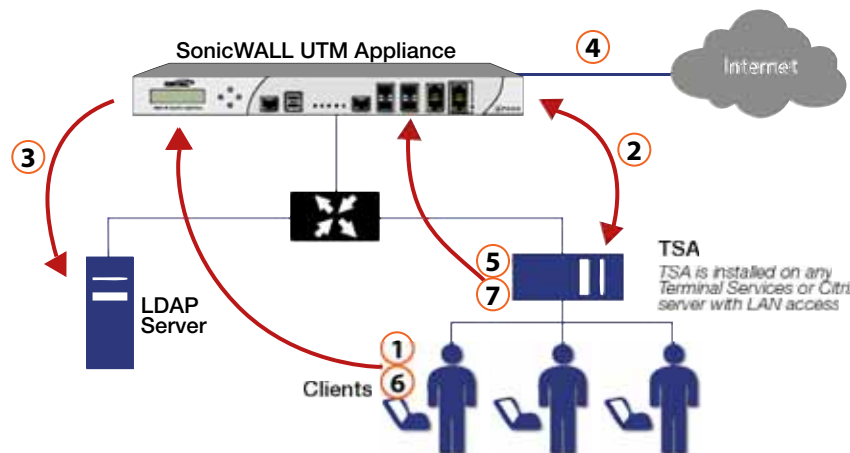
Note

The notes field of log messages specific to the SSO Agent will contain the text **<domain/user-name>, authentication by SSO Agent.**

How Does SonicWALL Terminal Services Agent Work?

The SonicWALL TSA can be installed on any Windows Server machine with Terminal Services or Citrix installed. The server must belong to a Windows domain that can communicate with the SonicWALL security appliance directly using the IP address or using a path, such as VPN.

SonicWALL SSO with Terminal Services Agent



Steps 2 3

Communication in these steps is encrypted when the user name and domain are included, using a shared key which is generated by the TSA.

For installation instructions for the SonicWALL TSA, refer to the [“Installing the SonicWALL Terminal Services Agent”](#) section on page 16.

See the following sections for information about the SonicWALL TSA:

- [“Multiple TSA Support”](#) on page 10
- [“Encryption of TSA Messages and Use of Session IDs”](#) on page 10
- [“Connections to Local Subnets”](#) on page 10
- [“Non-Domain User Traffic from the Terminal Server”](#) on page 10
- [“Non-User Traffic from the Terminal Server”](#) on page 11

Multiple TSA Support

To accommodate large installations with thousands of users, SonicWALL UTM appliances are configurable for operation with multiple terminal services agents (one per terminal server). The number of agents supported depends on the model, as shown in [Table 1](#).

Table 1 *Multiple TSA Support per Model*

SonicWALL UTM Model	TS Agents Supported
NSA E7500	256
NSA E6500	128
NSA E5500	64
NSA 5000	32
NSA 4500	16
NSA 3500	16
NSA 2400	8
NSA 240	4
TZ 210 Series	4
TZ 200 Series	Not supported
TZ 100 Series	Not supported

For all SonicWALL UTM models, a maximum of 32 IP addresses is supported per terminal server.

Encryption of TSA Messages and Use of Session IDs

SonicWALL TSA uses a shared key for encryption of messages between the TSA and the SonicWALL UTM appliance when the user name and domain are contained in the message. The first open notification for a user is always encrypted, because the TSA includes the user name and domain.



Note

The shared key is created in the TSA, and the key entered in the SonicWALL UTM appliance during SSO configuration must match the TSA key exactly.

The TSA includes a user session ID in all notifications rather than including the user name and domain every time. This is efficient, secure, and allows the TSA to re-synchronize with Terminal Services users after the agent restarts.

Connections to Local Subnets

The TSA dynamically learns network topology based on information returned from the appliance and, once learned, it will not send notifications to the appliance for subsequent user connections that do not go through the appliance. As there is no mechanism for the TSA to “unlearn” these local destinations, the TSA should be restarted if a subnet is moved between interfaces on the appliance.

Non-Domain User Traffic from the Terminal Server

The SonicWALL UTM appliance has the **Allow limited access for non-domain users** setting for optionally giving limited access to non-domain users (users logged into their local machine and not into the domain), and this works for terminal services users as it does for other SSO users.

Non-User Traffic from the Terminal Server

Non-user connections are opened from the Terminal Server for Windows updates and anti-virus updates. The TSA can identify a connection from a logged-in service as being a non-user connection, and indicates this in the notification to the appliance.

To control handling of these non-user connections, an **Allow Terminal Server non-user traffic to bypass user authentication in access rules** checkbox is available in the TSA configuration on the appliance. When selected, these connections are allowed. If this checkbox is not selected, then the services are treated as local users and can be given access by selecting the **Allow limited access for non-domain users** setting and creating user accounts on the appliance with the corresponding service names.

Installing the SonicWALL SSO Agent

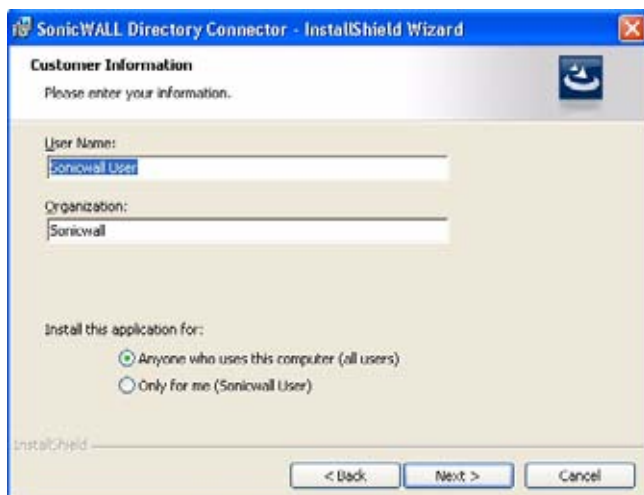
Install the SonicWALL SSO Agent on at least one, and up to eight, servers on your network within the Windows domain that have access to the Active Directory server using VPN or IP. The SonicWALL SSO Agent must have access to your SonicWALL UTM security appliance.

SonicWALL SSO Agent is available as part of SonicWALL Directory Services Connector 3.1.1 or higher, which you can download without charge from MySonicWALL. For best results, download the most recent version. To install the SonicWALL SSO Agent, perform the following steps:

-
- Step 1** Download one of the following installation programs, depending on your computer:
- **SonicWALL Directory Connector (32-bit) 3.1.x.exe**
 - **SonicWALL Directory Connector (64-bit) 3.1.x.exe**
- You can find these on <http://www.mysonicwall.com> under **Directory Services Connector**.
- Step 2** Double-click the installation program to begin installation. If prompted, install the Microsoft .NET framework.
- Step 3** On the Welcome page, click **Next** to continue.
- Step 4** The License Agreement displays. Select **I accept the terms in the license agreement** and click **Next** to continue.




- Step 5** On the Customer Information page, enter your name in the **User Name** field and your organization name in the **Organization** field. Select to install the application for **Anyone who uses this computer (all users)** or **Only for me**. Click **Next** to continue.



- Step 6** Select the destination folder. To use the default folder, C:\Program Files\SonicWALL\DCON, click **Next**. To specify a custom location, click **Change**, select the folder, and click **Next**.

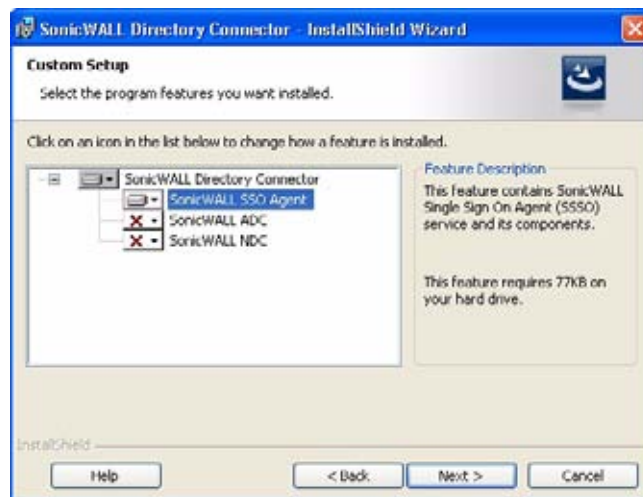


- Step 7** On the Custom Setup page, the installation icon  is displayed by default next to the **SonicWALL SSO Agent** feature.

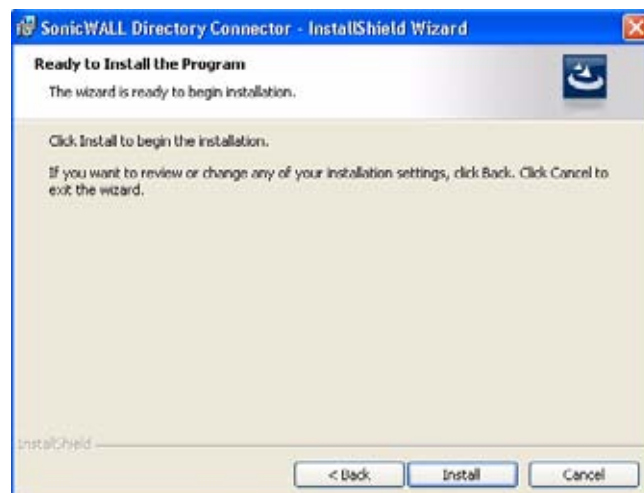
Optionally, you can select **SonicWALL NDC** to enable SonicWALL SSO to work with Novell users if this server has network access to the eDirectory server. For information about installing SonicWALL NDC, see [“Installing NDConnector for Use with a SonicWALL UTM” on page 28](#).

Optionally, you can also select **SonicWALL ADC** if this server belongs to an Active Directory domain, and will be used to communicate with a SonicWALL CSM appliance. For more information, see the *SonicOS CF 2.6 Administrator's Guide*, available on <http://www.sonicwall.com/us/Support.html>

Click **Next**.



Step 8 On the Ready to Install the Program page, click **Install** to install the SonicWALL SSO Agent.



- Step 9** To configure a common service account that the SonicWALL SSO Agent will use to log into a specified Windows domain, enter the username of an account with administrative privileges in the **Username** field, the password for the account in the **Password** field, and the domain name of the account in the **Domain Name** field. Click **Next**.



Note This section can be configured at a later time. To skip this step and configure it later, click **Skip**.

- Step 10** Enter the IP address of your SonicWALL security appliance in the **SonicWALL Appliance IP** field. Type the port number for the same appliance in the **SonicWALL Appliance Port** field. Enter a shared key (a hexadecimal number from 1 to 16 digits in length) in the **Shared Key** field. Click **Next** to continue.



Note This information can be configured at a later time. To skip this step and configure it later, leave the fields blank and click **Next**.

- Step 11** If you selected either **SonicWALL ADC** or **SonicWALL NDC** in addition to **SonicWALL SSO Agent** in the Custom Setup screen (Step 7), the Default CSM Appliance Configuration screen is displayed next. Enter the IP address and port number for your SonicWALL CSM appliance and enter the 16 digit shared key for communicating securely with the SonicWALL CSM, and then click **Next**.



- Step 12** Wait while the SonicWALL SSO Agent installs. The progress bar indicates the status.
- Step 13** When installation is complete, optionally select the **Launch SonicWALL Directory Connector** checkbox to launch the SonicWALL Directory Connector Configurator, and then click **Finish**. If you selected the **Launch SonicWALL Directory Connector** checkbox, the SonicWALL Directory Connector Configurator will display.



Installing the SonicWALL Terminal Services Agent

Install the SonicWALL TSA on one or more terminal servers on your network within the Windows domain. The SonicWALL TSA must have access to your SonicWALL UTM security appliance, and the appliance must have access to the TSA. If you have a software firewall running on the terminal server, you may need to open up the UDP port number for incoming messages from the appliance.

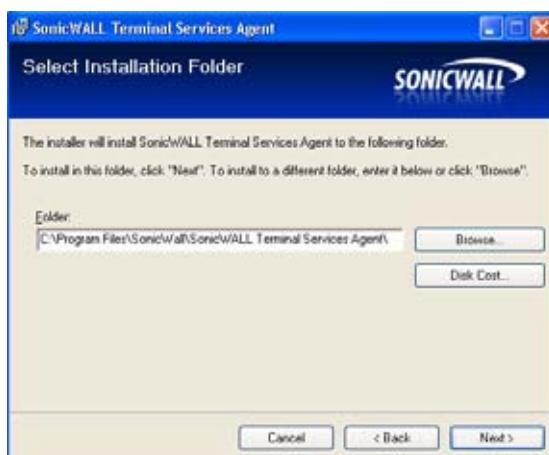
SonicWALL TSA is available for download without charge from MySonicWALL. To install the SonicWALL TSA, perform the following steps:

- Step 1** On a Windows Terminal Server system, download one of the following installation programs, depending on your computer:
 - **SonicWALL TSAInstaller32.msi** (32 bit, version 3.0.28.1001 or higher)
 - **SonicWALL TSAInstaller64.msi** (64 bit, version 3.0.28.1001 or higher)

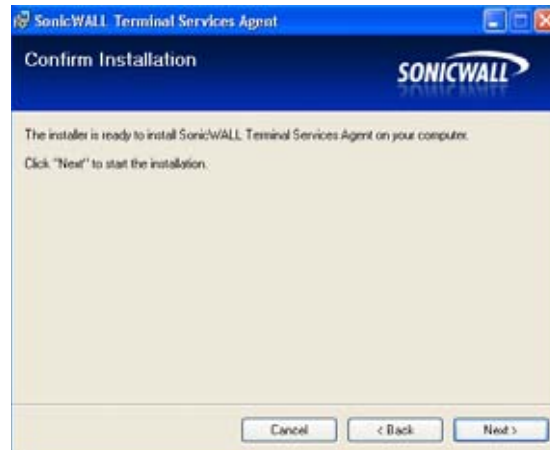
You can find these on <http://www.mysonicwall.com>.
- Step 2** Double-click the installation program to begin installation.
- Step 3** On the Welcome page, click **Next** to continue.
- Step 4** The License Agreement displays. Select **I agree** and click **Next** to continue.



- Step 5** On the Select Installation Folder window, select the destination folder. To use the default folder, C:\Program Files\SonicWALL\SonicWALL Terminal Services Agent\, click **Next**. To specify a custom location, click **Browse**, select the folder, and click **Next**.

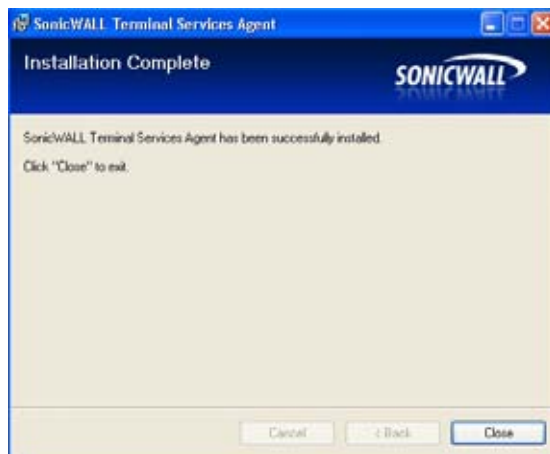


Step 6 On the Confirm Installation window, click **Next** to start the installation.

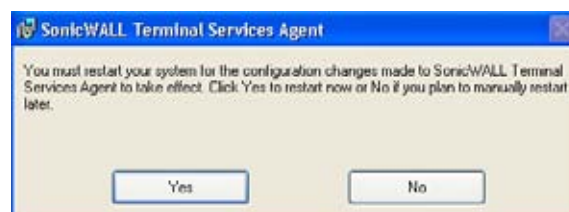


Step 7 Wait while the SonicWALL Terminal Services Agent installs. The progress bar indicates the status.

Step 8 When installation is complete, click **Close** to exit the installer.



Step 9 You must restart your system before starting the SonicWALL Terminal Services Agent. To restart immediately, click **Yes** in the dialog box. To restart later, click **No**.



Configuring the SonicWALL SSO Agent

The SonicWALL SSO Agent communicates with workstations using NetAPI or WMI, which both provide information about users that are logged into a workstation, including domain users, local users, and Windows services. WMI is pre-installed on Windows Server 2008, Windows Server 2003, Windows XP¹, Windows ME, and Windows 2000. For other Windows versions, visit www.microsoft.com to download WMI. Verify that WMI or NetAPI is installed prior to configuring the SonicWALL SSO Agent.

The .NET Framework 2.0 must be installed prior to configuring the SonicWALL SSO Agent. The .NET Framework can be downloaded from Microsoft at www.microsoft.com.

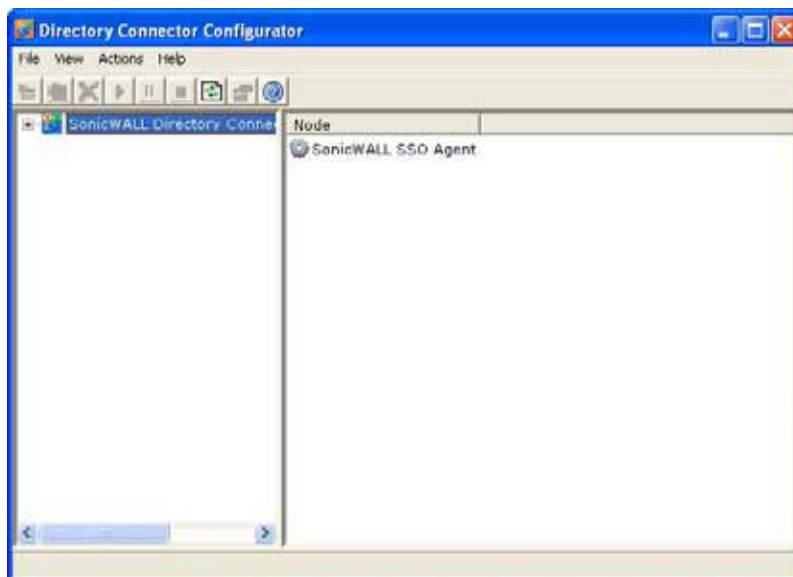
See the following sections:

- “Configuring Communication Properties” on page 18
- “Adding a SonicWALL Security Appliance” on page 22
- “Editing Appliances in SonicWALL SSO Agent” on page 24
- “Deleting Appliances in SonicWALL SSO Agent” on page 24
- “Modifying Services in SonicWALL SSO Agent” on page 24

Configuring Communication Properties

To configure the communication properties of the SonicWALL SSO Agent, perform the following tasks:

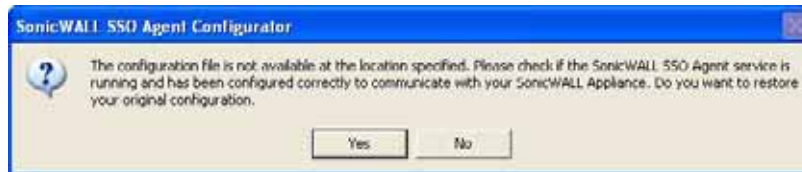
- Step 1** Launch the SonicWALL Configuration Tool by double-clicking the desktop shortcut or by navigating to **Start > All Programs > SonicWALL > SonicWALL Directory Connector > SonicWALL Configuration Tool**.



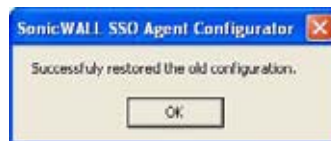
1. Windows XP with Service Pack 2 has a limitation that can affect the SonicWALL SSO Agent, and so is not recommended.

**Note**

If the IP address for a default SonicWALL security appliance was not configured, or if it was configured incorrectly, a pop up will display. Click **Yes** to use the default IP address (192.168.168.168) or click **No** to use the current configuration.




If you clicked **Yes**, the message **Successfully restored the old configuration** will display. Click **OK**.

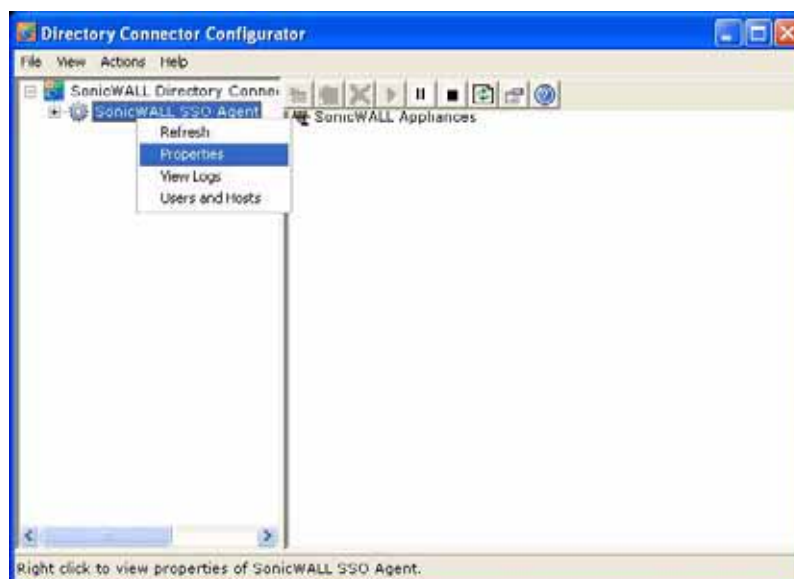


If you clicked **No**, or if you clicked **Yes** but the default configuration is incorrect, the message **SonicWALL SSO Agent service is not running. Please check the configuration and start the service.** will display. Click **OK**.



If the message **SonicWALL SSO Agent service is not running. Please check the configuration and start the service** displays, the SSO Agent service will be disabled by default. To enable the service, expand the SonicWALL Directory Connector Configuration Tool in the left navigation panel by clicking the + icon, highlight the SonicWALL SSO Agent underneath it, and click the  button.

- Step 2** In the left-hand navigation panel, expand the SonicWALL Directory Connector Configuration Tool by clicking the + icon. Right click the **SonicWALL SSO Agent** and select **Properties**.



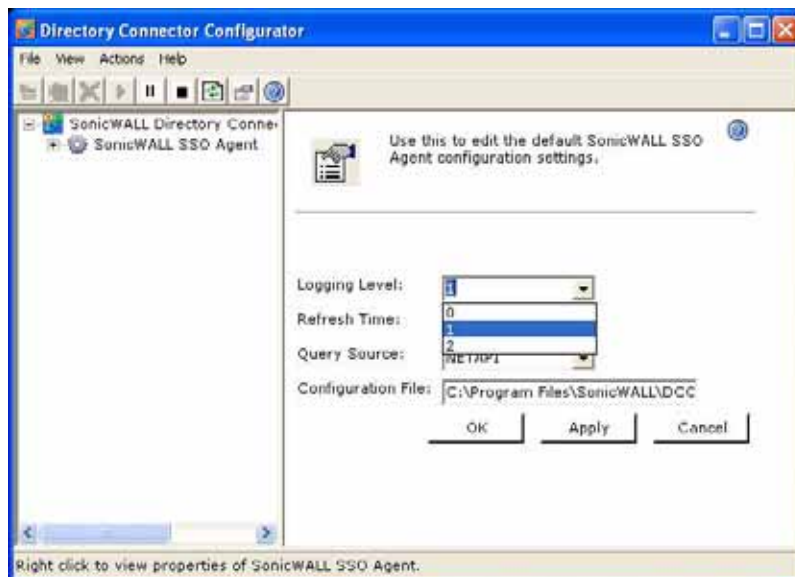
Step 3 From the **Logging Level** pull-down menu, select the level of events to be logged in the Windows Event Log. The default logging level is 1. Select one of the following levels:

- **Logging Level 0** - Only critical events are logged.
- **Logging Level 1** - Critical and significantly severe events are logged.
- **Logging Level 2** - All requests from the appliance are logged, using the debug level of severity.

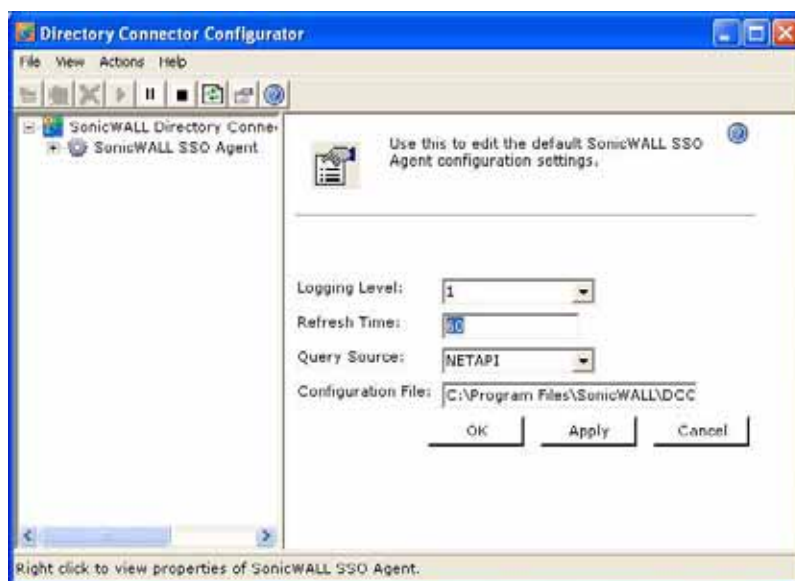


Note

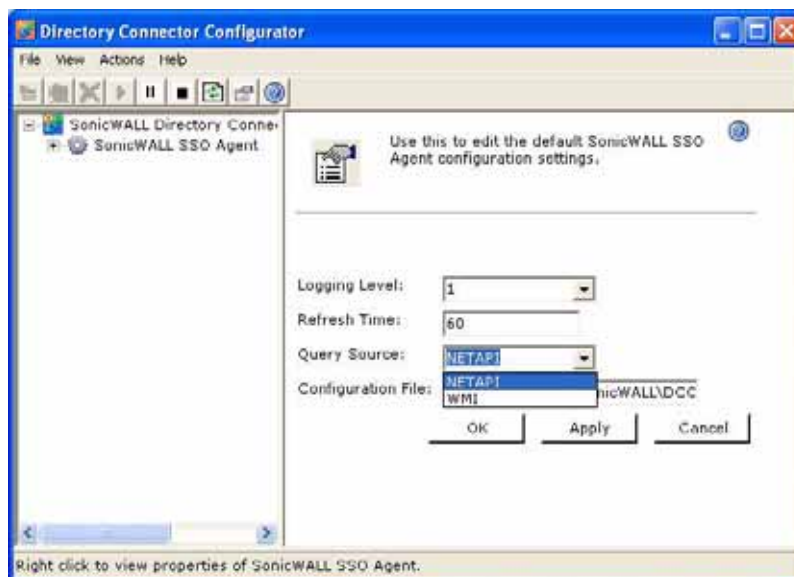
When Logging Level 2 is selected, the SSO Agent service will terminate if the Windows event log reaches its maximum capacity.



Step 4 In the **Refresh Time** field, enter the frequency, in seconds, that the SSO Agent will refresh user log in status. The default is 60 seconds.



- Step 5** From the **Query Source** pull-down menu, select the protocol that the SSO Agent will use to communicate with workstations, either **NETAPI** or **WMI**.

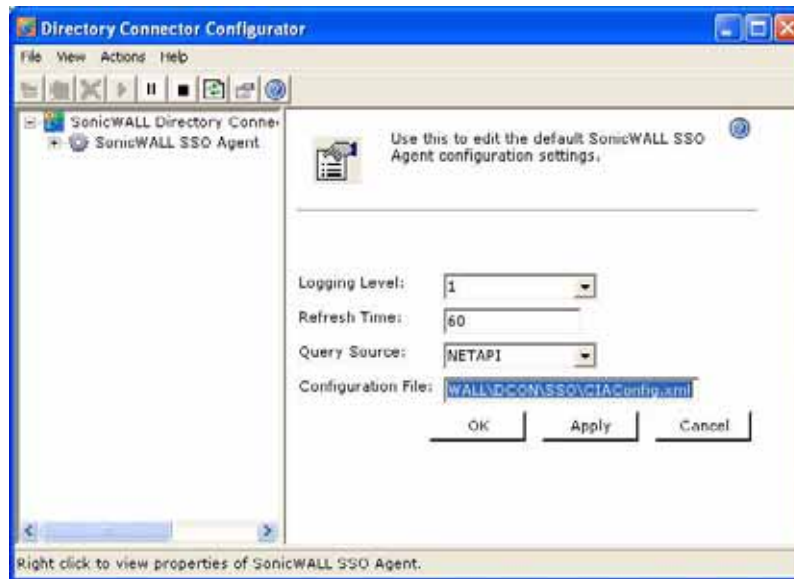
**Note**

NetAPI will provide faster, though possibly slightly less accurate, performance. WMI will provide slower, though possibly more accurate, performance. With NetAPI, Windows reports the last login to the workstation whether or not the user is still logged in. This means that after a user logs out from his computer, the appliance will still show the user as logged in when NetAPI is used. If another user logs onto the same computer, then at that point the previous user is logged out from the SonicWALL.

WMI is pre-installed on Windows Server 2008, Windows Server 2003, Windows XP¹, Windows Me, and Windows 2000. Both NetAPI and WMI can be manually downloaded and installed. NetAPI and WMI provide information about users that are logged into a workstation, including domain users, local users, and Windows services.

1. Windows XP with Service Pack 2 has a limitation that can affect the SonicWALL SSO Agent, and so is not recommended.

- Step 6** In the **Configuration File** field, enter the path for the configuration file. The default path is **C:\Program Files\SonicWALL\DCON\SSO\CIAConfig.xml**.



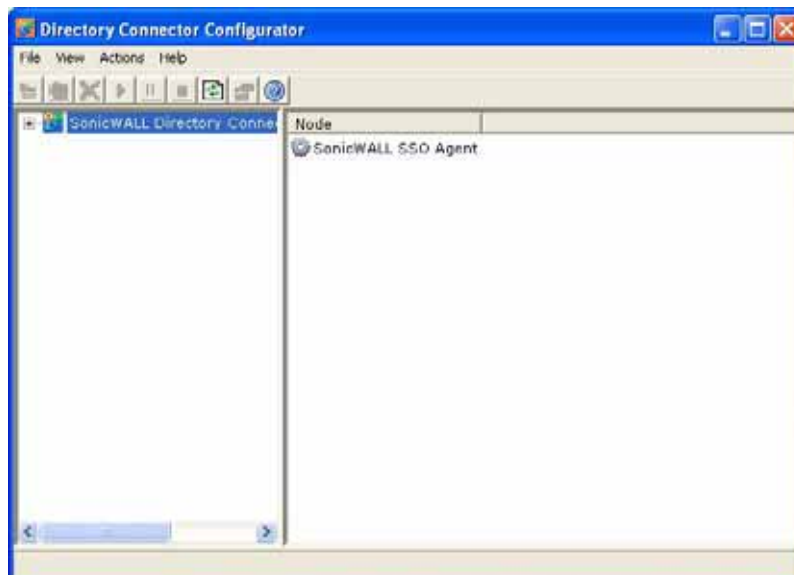
- Step 7** Click **Apply**.

- Step 8** Click **OK**.

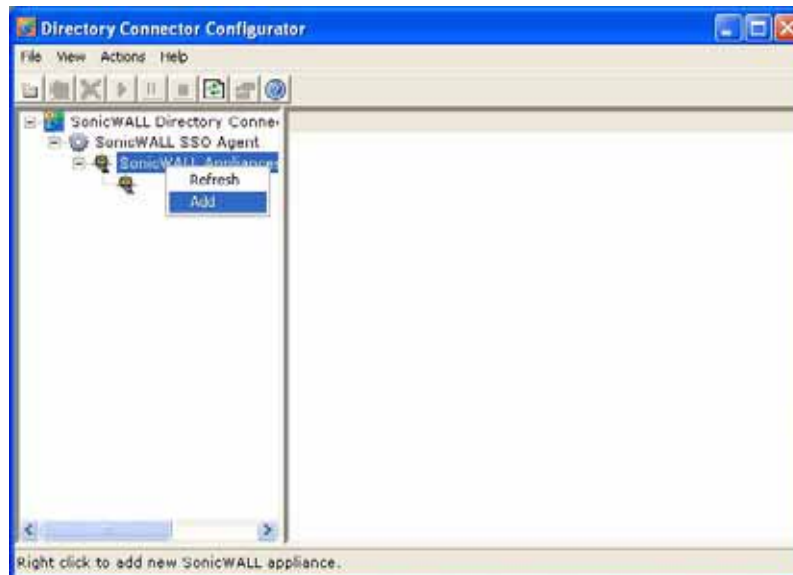
Adding a SonicWALL Security Appliance

Use these instructions to manually add a SonicWALL security appliance if you did not add one during installation, or to add additional SonicWALL security appliances. To add a SonicWALL security appliance, perform the following steps:

- Step 1** Launch the SonicWALL SSO Agent Configurator.



- Step 2** Expand the SonicWALL Directory Connector and SonicWALL SSO Agent trees in the left column by clicking the + button. Right click **SonicWALL Appliances** and select **Add**.




- Step 3** Enter the appliance IP address for your SonicWALL security appliance in the **Appliance IP** field. Enter the port for the same appliance in the **Appliance Port** field. The default port is 2258. Give your appliance a friendly name in the **Friendly Name** field. Enter a shared key in the **Shared Key** field or click **Generate Key**. When you are finished, click **OK**.




Your appliance will display in the left-hand navigation panel under the **SonicWALL Appliances** tree.






Editing Appliances in SonicWALL SSO Agent

You can edit all settings on SonicWALL security appliances previously added in SonicWALL SSO Agent, including IP address, port number, friendly name, and shared key. To edit a SonicWALL security appliance in SonicWALL SSO Agent, select the appliance from the left-hand navigation panel and click the edit icon  above the left-hand navigation panel. You can also click the **Edit** tab at the bottom of the right-hand window.

Deleting Appliances in SonicWALL SSO Agent

To delete a SonicWALL security appliance you previously added in SonicWALL SSO Agent, select the appliance from the left-hand navigation panel and click the delete icon  above the left-hand navigation panel.

Modifying Services in SonicWALL SSO Agent

You can start, stop, and pause SonicWALL SSO Agent services to SonicWALL security appliances. To pause services for an appliance, select the appliance from the left-hand navigation panel and click the pause button . To stop services for an appliance, select the appliance from the left-hand navigation panel and click the stop button . To resume services, click the start button .



Note

You may be prompted to restart services after making configuration changes to a SonicWALL security appliance in the SonicWALL SSO Agent. To restart services, press the stop button then press the start button.

Configuring the SonicWALL Terminal Services Agent

After installing the SonicWALL TSA and restarting your Windows Server system, you can double-click the SonicWALL TSA desktop icon created by the installer to launch it for configuration, to generate a trouble shooting report (TSR), or to see the status and version information.



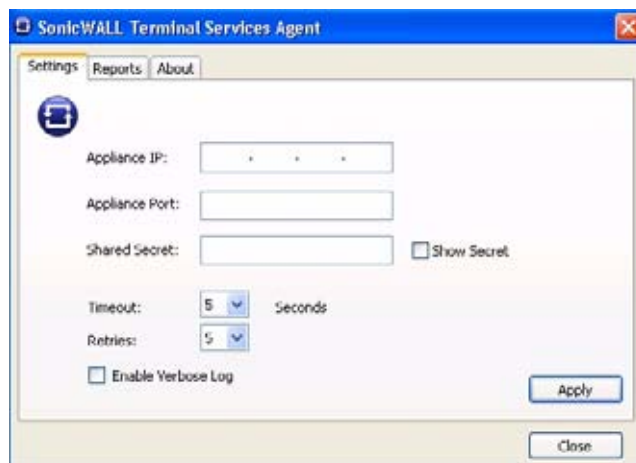
See the following sections:

- “Adding a SonicWALL UTM Appliance to SonicWALL TSA Settings” on page 25
- “Creating a SonicWALL TSA Trouble Shooting Report” on page 26
- “Viewing SonicWALL TSA Status and Version” on page 26

Adding a SonicWALL UTM Appliance to SonicWALL TSA Settings

Perform the following steps to add a SonicWALL UTM appliance to the SonicWALL TSA:

- Step 1** Double-click the SonicWALL TSA desktop icon.
- Step 2** The SonicWALL Terminal Services Agent window displays. On the **Settings** tab, type the IP address of the SonicWALL UTM appliance into the **Appliance IP** field.



- Step 3** Type the communication port into the **Appliance Port** field. The default port is 2259, but a custom port can be used instead. This port must be open on the Windows Server system.
- Step 4** Type the encryption key into the **Shared Secret** field. Select the **Show Secret** checkbox to view the characters and verify correctness. The same shared secret must be configured on the SonicWALL UTM appliance.
- Step 5** In the **Timeout** drop-down list, select the number of seconds that the agent will wait for a reply from the appliance before retrying the notification. The range is 5 to 10 seconds, and the default is 5 seconds.
- Step 6** In the **Retries** drop-down list, select the number of times the agent will retry sending a notification to the appliance when it does not receive a reply. The range is 3 to 10 retries, and the default is 5.

- Step 7** To enable full details in log messages, select the **Enable Verbose Log** checkbox. Do this only to provide extra, detailed information in a trouble shooting report. Avoid leaving this enabled at other times because it may impact performance.
- Step 8** Click **Apply**. A dialog box indicates that the SonicWALL TSA service has restarted with the new settings.

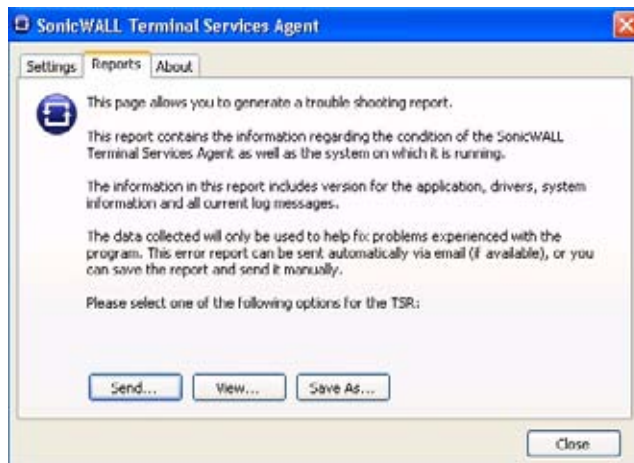


- Step 9** Click **OK**.

Creating a SonicWALL TSA Trouble Shooting Report

You can create a trouble shooting report (TSR) containing all current log messages and information about the agent, driver, and system settings to examine or to send to SonicWALL Technical Support for assistance. Perform the following steps to create a TSR for the SonicWALL TSA:

- Step 1** Double-click the SonicWALL TSA desktop icon.
- Step 2** The SonicWALL Terminal Services Agent window displays. Click the **Reports** tab.



- Step 3** To generate the TSR and automatically email it to SonicWALL Technical Support, click **Send**.
- Step 4** To generate the TSR and examine it in your default text editor, click **View**.
- Step 5** To generate the TSR and save it as a text file, click **Save As**.
- Step 6** When finished, click **Close**.

Viewing SonicWALL TSA Status and Version

To display the current status of the SonicWALL TSA service on your Windows Server system, or to view the version number of the SonicWALL TSA, perform the following steps:

- Step 1** Double-click the SonicWALL TSA desktop icon.

Step 2 The SonicWALL Terminal Services Agent window displays. Click the **About** tab.

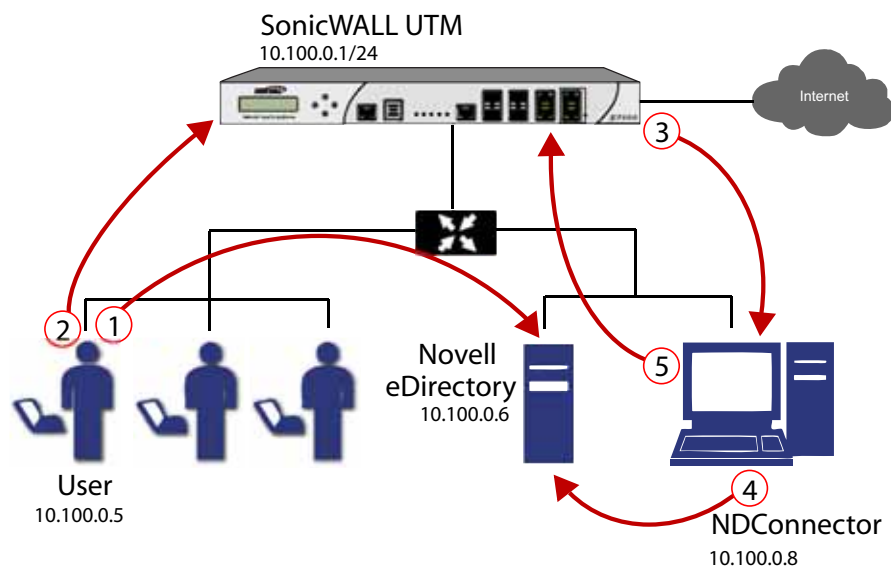


Step 3 Click **Close**.

Using NDConnector with SonicWALL SSO

Prior to SonicOS Enhanced 5.5, SonicWALL SSO was only available for Novell users with the SonicWALL CSM appliance and its NDConnector Novell agent. In SonicOS Enhanced 5.5 and higher, operability with NDConnector is available for the SonicWALL UTM appliance, enabling SonicWALL SSO to work with Novell users. Initially, the Novell agent will continue to refer to the SonicWALL CSM, but many CSM-labelled fields also apply to the SonicWALL UTM. An enhanced Novell agent is under development for a future release.

Figure 5 SonicWALL NDConnector and SonicWALL UTM



1. A Novell client logs into the network.
2. The client attempts to access the Internet or other network resources.
3. The SonicWALL UTM appliance queries the SonicWALL NDConnector for the client ID.

4. The SonicWALL NDConnector passes on the request to the Novell eDirectory server which responds with the client ID.
5. Client ID information is passed back from the SonicWALL NDConnector to the SonicWALL UTM. Based on the client ID, the SonicWALL UTM checks with the LDAP server to determine group membership and permissions, and allows or denies access.

Because NDConnector uses LDAP to query user login status with the Novell eDirectory server, it scales well as the number of SSO users increases. For information about using LDAP authentication with Novell's eDirectory LDAP server, such as configuring LDAP for user group look ups after SSO authentication, see the following document:

http://www.sonicwall.com/downloads/LDAP_Integration_Feature_Module.pdf

See the following sections for information about installing and using NDConnector with a SonicWALL UTM:

- “Installing NDConnector for Use with a SonicWALL UTM” on page 28
- “Configuring NDConnector for Use with a SonicWALL UTM” on page 30
- “Configuring SonicOS for Use with NDConnector” on page 31

Installing NDConnector for Use with a SonicWALL UTM

NDConnector can be installed on any Windows Server machine that has network access to the eDirectory server. It does not need to be run on a machine with Novell Client installed.

The NDConnector is installed from the same setup program as Directory Connector for Windows. To install it, perform the following steps:

-
- Step 1** Double-click one of the following installation programs to begin installation, depending on your computer:
 - **SonicWALL Directory Connector (32-bit) 3.1.x.exe**
 - **SonicWALL Directory Connector (64-bit) 3.1.x.exe**
 - Step 2** On the Welcome page, click **Next** to continue.
 - Step 3** The License Agreement displays. Select **I accept the terms in the license agreement** and click **Next** to continue.
 - Step 4** On the Customer Information page, enter your name in the **User Name** field and your organization name in the **Organization** field. Select to install the application for **Anyone who uses this computer (all users)** or **Only for me**. Click **Next** to continue.
 - Step 5** On the Destination Folder page, select the destination folder. To use the default folder, C:\Program Files\SonicWALL\DCON, click **Next**. To specify a custom location, click **Change**, select the folder, and click **Next**.

Step 6 On the Custom Setup page, de-select **SonicWALL SSO Agent** and select **SonicWALL NDC**.



Step 7 Click **Next**.

Step 8 On the Ready to Install the Program page, click **Install** to install SonicWALL NDC.

Step 9 On the Default CSM Appliance Configuration page, ignore the references to CSM.



Enter the SonicWALL UTM information into the fields, as follows:

- **CSM Appliance IP** – Type in the SonicWALL UTM appliance IP address.
- **CSM Appliance Port** – Type in the port used by NDC to communicate with the SonicWALL UTM appliance. The default port is 2261.
- **Shared Key** – Type in a hexadecimal number of up to 16 characters to use as the key for encrypting messages between NDC and the SonicWALL UTM appliance. You must also enter the same key when configuring the appliance to use SonicWALL NDC.

Step 10 Click **Next**.

- Step 11** On the Novell eDirectory Admin User Configuration page, type the eDirectory server IP address into the **Server IP Address** field.

- Step 12** In the **Server Port** field, enter the LDAP port number of the eDirectory server, normally 389.
- Step 13** In the **Login Username** field, enter the user name to use for logging into the eDirectory server.
- Step 14** In the **Password** field, enter the password for the eDirectory user account.
- Step 15** In the **Context** field, enter the LDAP distinguished name (DN) of the location in the eDirectory tree where the given user account is located.

**Note**

These same settings can later be modified by right-clicking on eDirectory in the Directory Connector Configurator.

- Step 16** Click **Next**.
- Step 17** When finished, click **Close** to exit the installer.

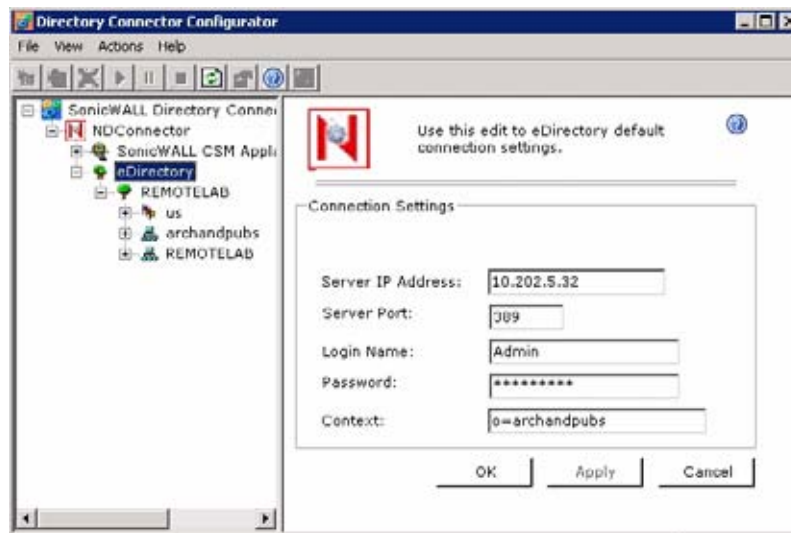
Configuring NDConnector for Use with a SonicWALL UTM

The SonicWALL Directory Connector Configurator is used to configure NDConnector to operate with a SonicWALL UTM appliance. References to the SonicWALL CSM appear in the configuration tool, but most fields also apply to SonicWALL UTM appliances. Those that do not are mentioned in the following procedure.

To configure SonicWALL NDC, perform the following steps:

- Step 1** Launch the SonicWALL Configuration Tool by double-clicking the desktop shortcut or by navigating to **Start > All Programs > SonicWALL > SonicWALL Directory Connector > SonicWALL Configuration Tool**.
- Step 2** When first launched, a dialog box displays the message “Novell eDirectory attributes have not been set to store User, Group, Computer, and OU object Policies. Please click OK to continue.” This does not apply to configuration for SonicWALL UTM. Click **Cancel**.
- Step 3** Expand **SonicWALL Directory Connector** in the left pane, and right-click **NDConnector** to display a popup menu. All the menu choices except **Search Policy** are valid for the SonicWALL UTM.
- Step 4** Click **Properties** in the popup menu.

- Step 5** On the Properties page in the right pane, none of the four **Policy** fields apply when using a SonicWALL UTM. You can configure the remaining fields, and then click **Apply**:
- **Logging Level** – The default is 2.
 - **Refresh Time** – The default is 60 seconds.
 - **Network Type** – The default is TCP.
 - **Configuration File** – The default is the Directory Connector Configurator.
- Step 6** To view settings for the SonicWALL UTM appliance, click the appliance in the left pane. You can view the settings in the right pane. To edit the settings, click the **Edit** button. The **Policies** button does not apply for SonicWALL UTM appliances.
- Step 7** To edit settings for the eDirectory server, expand **NDConnector** in the left pane and click on **eDirectory** under it.



Configuring SonicOS for Use with NDConnector

You can configure the SonicWALL UTM appliance to use SonicWALL NDConnector with the same procedures used to add an SSO Agent. The NDConnector agent is configured on the SSO settings page in the same way as the Windows agents (SSO Agent or ADConnector). The main differences in the configuration are the following:

- The **Probe users for NetAPI/WMI** setting must be disabled if using NDConnector.
- The **User names used by Windows services** setting has no effect if using NDConnector.

Configuring Your SonicWALL Security Appliance

Your SonicWALL security appliance must be configured to use SonicWALL SSO Agent as the SSO method. This is also the correct method to select when configuring the appliance to use the SonicWALL TSA. After selecting the SonicWALL SSO Agent, there are several configuration screens. See the following sections for information about configuring your SonicWALL security appliance to use SonicWALL SSO Agent or SonicWALL TSA:

- [“Selecting the Single Sign-On Method” on page 33](#)
- [“Adding an SSO Agent” on page 34](#)
- [“Editing the Settings of Existing Agents” on page 35](#)
- [“Configuring the Users Settings” on page 37](#)
- [“Configuring the Security Services Settings” on page 39](#)
- [“Adding and Configuring a Terminal Services Agent” on page 40](#)
- [“Testing the Authentication Agent Settings” on page 41](#)
- [“Advanced LDAP Configuration” on page 43](#)
- [“Tuning Single Sign-On Advanced Settings” on page 52](#)
- [“Configuring Firewall Access Rules” on page 54](#)
- [“Managing SonicOS with HTTP Login from a Terminal Server” on page 56](#)
- [“Viewing SSO Statistics and Tooltips” on page 57](#)
- [“Viewing User Status” on page 59](#)
- [“Configuring Additional User Settings” on page 59](#)
- [“Viewing SSO and LDAP Messages with Packet Monitor” on page 59](#)

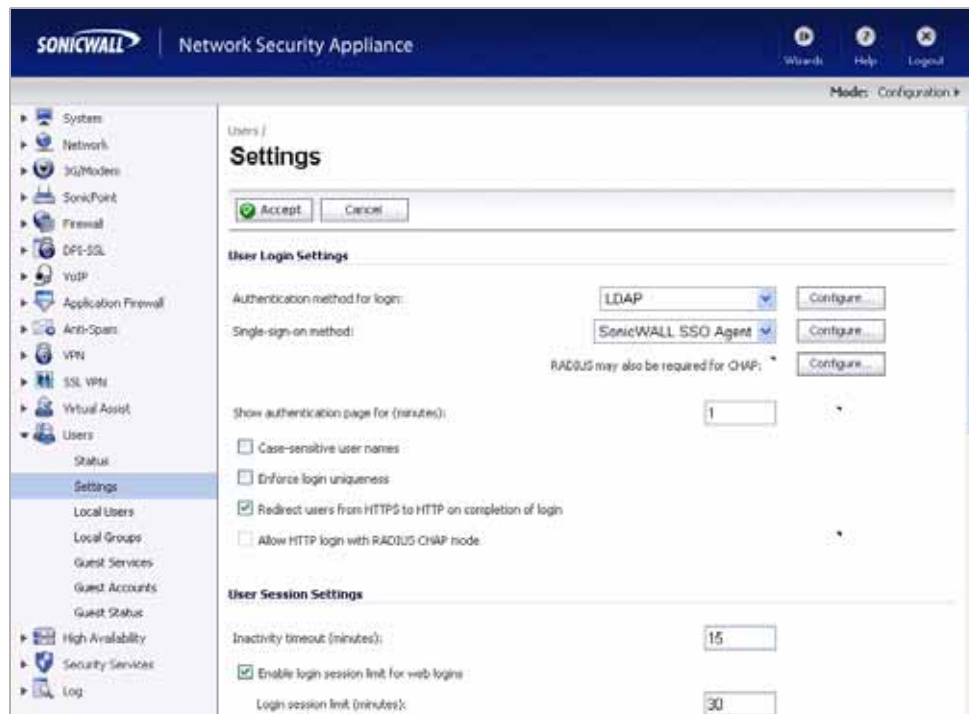
**Note**

Depending on the deployment, all procedures may not be required.

Selecting the Single Sign-On Method

To select the SonicWALL SSO Agent or TSA as the SSO method and access the configuration screen, perform the following steps:

- Step 1** Login to your SonicWALL security appliance as an administrator.
- Step 2** Navigate to **Users > Settings**.
- Step 3** In the **Single sign on method** drop-down menu, select **SonicWALL SSO Agent**. Use this choice to add and configure a TSA as well as an SSO Agent for the SSO method.



- Step 4** Click **Configure**. The Authentication Agent Settings page displays, showing any Authentication Agents already configured. The green LED next to the Agent's IP address indicates that the agent is currently up and running. A red LED would indicate that the agent is down. The LEDs are dynamically updated using AJAX.



Continue the configuration by performing the procedures described in the sections that follow.

- Step 5** When you are finished with all Authentication Agent configuration, click **OK**.

Adding an SSO Agent

Authentication agents, in this case SSO agents, are added one at a time. When configuring multiple agents, the host name / IP address, port number, timeout period, number of retries, and maximum requests to send at a time are all configured separately for each agent.

To access the page on which you can add an SSO Agent, follow the procedure described in the [“Selecting the Single Sign-On Method”](#) section on page 33.

To add an SSO Agent, perform the following steps:

- Step 1** On the Authentication Agent Settings page, click the **Add** button. The page is updated to display a new row in the table at the top, and two new tabs and their input fields in the lower half of the page.

SONICWALL Network Security Appliance

Settings Users Security Services Terminal Services Test

Authentication Agent Settings

#	Status	Host Name/IP Address	Port	Timeout	Retries	Max Rqsts	Enable
1	●	192.168.168.3	2258	5	3	32	<input checked="" type="checkbox"/>
2	●	0.0.0.0	2258	10	6	32	<input checked="" type="checkbox"/>

Add...

Settings Advanced ?

Host Name or IP Address: 0.0.0.0 Port: 2258

Shared Key:

Confirm Shared Key:

Timeout (seconds): 10 Retries: 6

Ready

OK Cancel Apply Help

- Step 2** On the **Settings** tab in the lower half of the page, in the **Host Name or IP Address** field, enter the name or IP Address of the workstation on which SonicWALL SSO Agent is installed. As you type in values for the fields, the row at the top is updated in red to highlight the new information.


The screenshot shows the 'Authentication Agent Settings' window. At the top, there are tabs: Settings, Users, Security Services, Terminal Services, and Test. The 'Settings' tab is active. Below the tabs is a table titled 'Authentication Agent Settings' with columns: #, Status, Host Name/IP Address, Port, Timeout, Retries, Max Rights, and Enable. There are two rows. Row 1 has a green status icon, Host Name/IP Address 192.168.168.3, Port 2258, Timeout 5, Retries 3, Max Rights 32, and an enabled checkbox. Row 2 has a red status icon, Host Name/IP Address 10.202.77, Port 2258, Timeout 10, Retries 6, Max Rights 32, and an enabled checkbox. Below the table is an 'Add...' button. At the bottom, there are tabs: Settings and Advanced. The 'Advanced' tab is selected. It contains fields for: Host Name or IP Address (10.202.77), Port (2258), Shared Key, Confirm Shared Key, Timeout (seconds) (10), and Retries (6). At the very bottom, there are buttons: OK, Cancel, Apply, and Help.

- Step 3** In the **Port** field, enter the port number of the workstation on which SonicWALL SSO Agent is installed. The default port is 2258. Note that agents at different IP addresses can have the same port number.
- Step 4** In the **Shared Key** field, enter the shared key that you created or generated in the SonicWALL SSO Agent. The shared key must match exactly. Re-enter the shared key in the **Confirm Shared Key** field.
- Step 5** In the **Timeout (seconds)** field, enter a number of seconds before the authentication attempt times out. This field is automatically populated with the default of 10 seconds.
- Step 6** In the **Retries** field, enter the number of authentication attempts.
- Step 7** Click the **Advanced** tab in the lower half of the page.
- Step 8** In the **Maximum requests to send at a time** field, enter the maximum number of requests to send from the appliance to the agent at one time. The default is 32.
- The agent processes multiple requests concurrently, spawning a separate thread in the agent PC to handle each. Sending too many requests at a time can overload the PC. On the other hand, if the number of requests to be sent from the appliance exceeds the maximum, then some requests will wait on an internal “ring buffer” queue. Too many requests waiting could lead to slow response times in Single Sign On authentication. For more information, see [“Tuning Single Sign-On Advanced Settings” on page 52](#).
- Step 9** To apply your changes without exiting the configuration window, click **Apply**. If you are finished with all Authentication Agent configuration, click **OK**.
- Step 10** Proceed with configuration on the **Users** tab. See [“Configuring the Users Settings” on page 37](#).

Editing the Settings of Existing Agents

You can edit the settings for configured agents (SSO Agent or TSA) by clicking the Configure icon or by clicking the settings directly in the table row of the Authentication Agents Settings page. Certain settings, such as **Shared Key**, are not available for direct editing in the table row.

To edit the settings of previously configured agents:

- Step 1** For access to all the settings of an existing agent for editing, click the Configure icon  on the right side of the row.



- Step 2** The settings are displayed in the lower half of the page. Make the desired changes and then click **Apply**.

- Step 3** To edit a setting directly in the table row, click on the value in the row that you want to change.



- Step 4** When clicked, the field changes to an editable text box.



Make the desired change and then click anywhere else in the window to exit from editing mode.

- Step 5** To apply your changes without exiting the configuration window, click **Apply**. If you are finished with all Authentication Agent configuration, click **OK**.

Configuring the Users Settings

The Users tab provides a way to configure user authentication settings and the rates for polling user login status and retrying authentication requests.

To configure the Users settings, perform the following steps:

- Step 1** Click the **Users** tab. The User Settings page displays.

- Step 2** Check the box next to **Allow only users listed locally** to allow only users listed locally on the appliance to be authenticated.
- Step 3** Check the box next to **Simple user names in local database** to use simple user names. When selected, the domain component of a user name will be ignored. User names returned from the authentication agent typically include a domain component, for example, domain1/user1. If this box is not checked, user names in the local database must match exactly the full names returned from the agent, including the domain component.
- Step 4** Check the box next to **Allow limited access for non-domain users** to allow limited access to users who are logged in to a computer but not into a domain. These users will not be given membership in the Trusted Users user group, even when set locally, and so will not get any access set in policies for Trusted Users. They will be given access through policies that apply to Everyone or to their specific user names. They are identified in logs as *computer-name/user-name*. When using the local user database to authenticate users, and the **Simple user names in local database** option is disabled, user names must be configured in the local database using the full *computer-name/user-name* identification.
- Step 5** If your network includes non-Windows devices or Windows computers with personal firewalls running, check the box next to **Probe user for** and select the radio button for either **NetAPI** or **WMI** depending on which is configured for the SSO Agent. This causes the SonicWALL UTM appliance to probe for a response

on the NetAPI/WMI port before requesting that the SSO Agent identify a user. If no response occurs, these devices will fail SSO immediately. Such devices do not respond to, or may block, the Windows networking messages used by the SSO Agent to identify a user.

- Step 6** To use LDAP to retrieve user information, select the **Use LDAP to retrieve user group information** radio button. Click **Configure** to configure the LDAP settings. The LDAP Configuration page displays. For LDAP configuration information, refer to the [“Advanced LDAP Configuration” section on page 43](#).
- Step 7** To use locally configured user group settings, select the **Local configuration** radio button.
- Step 8** In the **Polling rate (minutes)** field, enter a polling interval, in minutes, that the security appliance will poll the workstation running SSO Agent to verify that users are still logged on. The default is 1.
- Step 9** In the **Hold time after failure (minutes)** field, enter a time, in minutes, that the security appliance will wait before trying again to identify an IP address as a user after a previous failure to do so. This feature rate-limits requests to the agent. The default is 1.
- Step 10** To populate the **User names used by Windows services** list, click the **Add** button. In the Service User name dialog box, type the service login name (the simple name only, without the domain or PC name) into the **Enter the name of a user account used by a Windows service** field and then click **OK**.

The purpose of this list is to distinguish the login names used by Windows services from real user logins. When the SSO agent queries Windows to find the user logged into a computer, Windows actually returns a list of user accounts that are/have been logged in to the computer and does not distinguish user logins from service logins, hence giving the SSO agent no way to determine that a login name belongs to a service. This may result in the SSO agent incorrectly reporting a service name instead of the actual user name.

You can enter up to 64 login names here that may be used by services on end-user computers. The SSO agent will ignore any logins using these names.

If, when using Single Sign On, you see unexpected user names shown on the Users > Status page, or logs of user login or user login failure with unexpected user names, those may be due to Windows service logins and those user names should be configured here so that the SSO agent will know to ignore them.

In cases where there are multiple SonicWALL appliances communicating with an SSO agent, the list of service account names should be configured on only one of them. The effect of configuring multiple lists on different appliances is undefined.

To edit a service account name, select the name, click **Edit**, make the desired changes in the Service User name dialog box, and then click **OK**.

To remove service account names, select one or more names and then click **Remove**.

- Step 11** To apply your changes without exiting the configuration window, click **Apply**. If you are finished with all Authentication Agent configuration, click **OK**.

Step 12 Proceed with configuration on one of the following tabs:

- **Security Services** – see [“Configuring the Security Services Settings” on page 39](#)
The **Security Services** tab is only visible if security services such as SonicWALL Premium Content Filtering Service (CFS), Intrusion Prevention (IPS), Anti-Spyware, or Application Firewall are enabled on the appliance.
- **Terminal Services** – see [“Adding and Configuring a Terminal Services Agent” on page 40](#)
- **Test** – see [“Testing the Authentication Agent Settings” on page 41](#)

Configuring the Security Services Settings

The **Security Services** tab is only visible if security services such as SonicWALL Premium Content Filtering Service (CFS), Intrusion Prevention (IPS), Anti-Spyware, or Application Firewall are enabled on the appliance.

Step 1 Click on the **Security Services** tab if you are using the SonicWALL security services and there is an internal proxy server in your network (such as a Web server).



Step 2 To bypass SSO for security services traffic and apply the default content filtering policy to the traffic, select the appropriate address object or address group from the drop-down list.

This setting should be used where traffic that would be subject to security services screening can emanate from a device other than a user's workstation (such as an internal proxy Web server). It prevents the SonicWALL from attempting to identify such a device as a network user in order to select the content filtering policy to apply. The default content filtering policy will be used for all traffic from the selected IP addresses.

- Step 3** To apply your changes without exiting the configuration window, click **Apply**. If you are finished with all Authentication Agent configuration, click **OK**.
- Step 4** Proceed with configuration on one of the following tabs:
- **Terminal Services** – see [“Adding and Configuring a Terminal Services Agent” on page 40](#)
 - **Test** – see [“Testing the Authentication Agent Settings” on page 41](#)

Adding and Configuring a Terminal Services Agent

Terminal Services agents (TSAs) are added one at a time. When configuring multiple agents, the host name and IP address are configured separately for each agent.

For existing agents, a green LED-style icon next to an agent indicates that the agent is up and running. A red LED icon indicates that the agent is down. A yellow LED icon means that the TSA is idle and the appliance has not heard anything from it for 5 minutes or more. Because TSA sends notifications to the appliance rather than the appliance sending requests to the agent, a lack of notifications could mean that there is a problem, but more likely means simply that no user on the terminal server is currently doing anything.

To access the page on which you can add a TSA, follow the procedure described in the [“Selecting the Single Sign-On Method” section on page 33](#).

To add and configure a TSA, perform the following steps:

- Step 1** Click the **Terminal Services** tab. The Terminal Services Agent Settings page displays.
- Step 2** Within this page, on the **Terminal Services Agents** tab, click the **Add** button. The page is updated to display a new row in the table at the top, and new input fields in the lower half of the page.

SONICWALL | Network Security Appliance

Settings Users Security Services **Terminal Services** Test

Terminal Services Agent Settings

Terminal Services Agents General Settings

# Active	Host Name/IP Address(es)	Port	Enable
1	192.168.168.94	2259	<input checked="" type="checkbox"/>
2	0.0.0.0	2259	<input checked="" type="checkbox"/>

Add...

Host Name or IP Address(es): 0.0.0.0 Port: 2259

Shared Key:

Confirm Shared Key:

Ready

OK Cancel Apply Help

- Step 3** In the **Host Name or IP Address(es)** field, enter the name or IP address of the terminal server on which SonicWALL TSA is installed. If the terminal server is multi-homed (has multiple IP addresses) and you are identifying the host by IP address rather than DNS name, enter all the IP addresses as a comma-separated list.
- As you type in values for the fields, the row at the top is updated in red to highlight the new information.
- Step 4** In the **Port** field, enter the port number of the workstation on which SonicWALL TSA is installed. The default port is 2259. Note that agents at different IP addresses can have the same port number.
- Step 5** In the **Shared Key** field, enter the shared key that you created or generated in the SonicWALL TSA. The shared key must match exactly. Re-enter the shared key in the **Confirm Shared Key** field.
- Step 6** Click the **General Settings** tab.
- Step 7** The **Allow traffic from services on the terminal server to bypass user authentication in access rules** checkbox is selected by default. This allows traffic such as Windows updates or anti-virus updates, which is not associated with any user login session, to pass without authentication. If you clear this checkbox, traffic from services can be blocked if firewall access rules require user authentication. In this case, you can add rules to allow access for “All” to the services traffic destinations, or configure the destinations as HTTP URLs that can bypass user authentication in access rules.
- Step 8** To apply your changes without exiting the configuration window, click **Apply**. If you are finished with all Authentication Agent configuration, click **OK**.
- Step 9** Proceed with configuration on the following tab:
- **Test** – see [“Testing the Authentication Agent Settings” on page 41](#)

Testing the Authentication Agent Settings

The Test tab provides a way to test the connectivity between the appliance and an SSO agent or TSA. You can also test whether the SSO agent is properly configured to identify a user logged into a workstation.



Note

Performing tests on this page applies any changes that have been made.

To test agent settings, perform the following steps:

- Step 1** Click the **Test** tab. The Test Authentication Agent Settings page displays.

- Step 2** If you have multiple agents configured, select the SSO agent or TSA to test from the **Select agent to test** drop-down list. The drop-down list includes SSO agents at the top, and TSA's at the end under the heading **--Terminal Server Agents--**.

- Step 3** Select the **Check agent connectivity** radio button and then click the **Test** button. This will test communication with the authentication agent. If the SonicWALL security appliance can connect to the SSO agent, you will see the message **Agent is ready**. If testing a TSA, the **Test Status** field displays the message, and the version and server IP address are displayed in the **Information returned from the agent** field.

SONICWALL Network Security Appliance

Settings Users Security Services Terminal Services **Test**

Test Authentication Agent Settings

To test that communication can be established with the authentication agent, select "Check agent connectivity" and click the Test button.

To test that the agent is properly configured to identify the user logged into a workstation, select "Check user", enter the IP address of the workstation, and click the Test button.

Note that this will apply any changes that have been made.

Select agent to test: 192.168.168.94

Test: ☒ Check agent connectivity ☐ Check user Workstation IP address:

Test

Test Status: **Agent responded**

Information returned from the agent:

Version: 3.0.28.1001
Terminal server IP address: 192.168.168.94

Ready

OK Cancel Apply Help

- Step 4** For SSO agents only, select the **Check user** radio button, enter the IP address of a workstation in the **Workstation IP address** field, and then click **Test**. This will test if the SSO agent is properly configured to identify the user logged into a workstation.

**Tip**

If you receive the messages **Agent is not responding** or **Configuration error**, check your settings and perform these tests again.

- Step 5** When you are finished with all Authentication Agent configuration, click **OK**.

Advanced LDAP Configuration

If you selected **Use LDAP to retrieve user group information** on the **Users** tab in step 6 of "Configuring the Users Settings" on page 37, you must configure your LDAP settings. To configure LDAP settings, perform the following steps:

- Step 1** On the **Users** tab in the SSO Configure window, click the **Configure** button next to the **Use LDAP to retrieve user group information** option.

- Step 2** The **Settings** tab displays. In the **Name or IP address** field, enter the name or IP address of your LDAP server.

- Step 3** In the **Port Number** field, enter the port number of your LDAP server. The default LDAP ports are:
- Default LDAP port – 389
 - Default LDAP over TLS port – 636
- Step 4** In the **Server timeout (seconds)** field, enter a number of seconds the SonicWALL security appliance will wait for a response from the LDAP server before the attempt times out. Allowable values are 1 to 99999. The default is 10 seconds.
- Step 5** In the **Overall operation timeout (minutes)** field, enter a number of minutes the SonicWALL security appliance will spend on any automatic operation before timing out. Allowable values are 1 to 99999. The default is 5 minutes.
- Step 6** Select the **Anonymous login** radio button to login anonymously. Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (MS AD generally does not), you may select this option.
- Select **Give login name / location in tree** to access the tree with the login name.
- Select **Give bind distinguished name** to access the tree with the distinguished name.
- Step 7** To login with a user's name and password, enter the user's name in the **Login user name** field and the password in the **Login password** field. The login name will automatically be presented to the LDAP server in full 'dn' notation.

**Note**

Use the user's name in the **Login user name** field, not a username or login ID. For example, John Doe would login as John Doe, not jdoe.

- Step 8** Select the LDAP version from the **Protocol version** drop-down menu, either **LDAP version 2** or **LDAP version 3**. Most implementations of LDAP, including AD, employ LDAP version 3.
- Step 9** Select the **Use TLS (SSL)** checkbox to use Transport Layer Security (SSL) to login to the LDAP server. It is strongly recommended to use TLS to protect the username and password information that will be sent across the network. Most implementations of LDAP server, including AD, support TLS.
- Step 10** Select the **Send LDAP 'Start TLS' request** checkbox to allow the LDAP server to operate in TLS and non-TLS mode on the same TCP port. Some LDAP server implementations support the Start TLS directive rather than using native LDAP over TLS. This allows the LDAP server to listen on one port (normally 389) for LDAP connections, and to switch to TLS as directed by the client. AD does not use this option, and it should only be selected if required by your LDAP server.



Note Only check the **Send LDAP 'Start TLS' request** box if your LDAP server uses the same port number for TLS and non-TLS.

- Step 11** Select the **Require valid certificate from server** checkbox to require a valid certificate from the server. Validates the certificate presented by the server during the TLS exchange, matching the name specified above to the name on the certificate. Deselecting this default option will present an alert, but exchanges between the SonicWALL security appliance and the LDAP server will still use TLS – only without issuance validation.
- Step 12** Select a local certificate from the **Local certificate for TLS** drop-down menu. This is optional, to be used only if the LDAP server requires a client certificate for connections. This feature is useful for LDAP server implementations that return passwords to ensure the identity of the LDAP client (AD does not return passwords). This setting is not required for AD.
- Step 13** Click **Apply**.
- Step 14** Click the **Schema** tab.

The screenshot shows the SonicWALL Network Security Appliance configuration interface, specifically the **Schema** tab. The window has a title bar with the SonicWALL logo and the text "Network Security Appliance". Below the title bar are several tabs: **Settings**, **Schema** (selected), **Directory**, **Referrals**, **LDAP Users**, **LDAP Relay**, and **Test**.

The main content area is titled **LDAP Schema** and contains the following sections:

- LDAP Schema:** A dropdown menu showing "Microsoft Active Directory".
- User Objects:**
 - Object class:
 - Login name attribute:
 - Qualified login name attribute:
 - User group membership attributes:
 - Framed IP address attribute:
- User Group Objects:**
 - Object class:
 - Member attribute: is: ☒ Distinguished name ☐ User ID

At the bottom right of the main content area is a button labeled **Read from server**.

At the bottom of the window is a status bar with the text **Ready** and four buttons: **OK**, **Cancel**, **Apply**, and **Help**.

- Step 15** From the **LDAP Schema** drop-down menu, select one of the following LDAP schemas. Selecting any of the predefined schemas will automatically populate the fields used by that schema with their correct values. Selecting 'user-defined' will allow you to specify your own values – use this only if you have a specific or proprietary LDAP schema configuration.
- Microsoft Active Directory
 - RFC2798 InetOrgPerson
 - RFC2307 Network Information Service
 - Samba SMB
 - Novell eDirectory
 - User defined
- Step 16** The **Object class** field defines which attribute represents the individual user account to which the next two fields apply. This will not be modifiable unless you select **User defined**.
- Step 17** The **Login name attribute** field defines which attribute is used for login authentication. This will not be modifiable unless you select **User defined**.
- Step 18** If the **Qualified login name attribute** field is not empty, it specifies an attribute of a user object that sets an alternative login name for the user in *name@domain* format. This may be needed with multiple domains in particular, where the simple login name may not be unique across domains. This is set to **mail** for Microsoft Active Directory and RFC2798 inetOrgPerson.
- Step 19** The **User group membership attribute** field contains the information in the user object of which groups it belongs to. This is **memberOf** in Microsoft Active Directory. The other pre-defined schemas store group membership information in the group object rather than the user object, and therefore do not use this field.
- Step 20** The **Framed IP address attribute** field can be used to retrieve a static IP address that is assigned to a user in the directory. Currently it is only used for a user connecting using L2TP with the SonicWALL security appliance L2TP server. In future releases, this may also be supported for the SonicWALL Global VPN Client (GVC). In Active Director, the static IP address is configured on the Dial-in tab of a user's properties.
- Step 21** The **Object class** field defines the type of entries that an LDAP directory may contain. A sample object class, as used by AD, would be 'user' or 'group'.
- Step 22** The **Member attribute** field defines which attribute is used for login authentication.

Step 23 Select the **Directory** tab.

Step 24 In the **Primary Domain** field, specify the user domain used by your LDAP implementation. For AD, this will be the Active Directory domain name, such as *yourADdomain.com*. Changes to this field will, optionally, automatically update the tree information in the rest of the page. This is set to **mydomain.com** by default for all schemas except Novell eDirectory, for which it is set to **o=mydomain**.

Step 25 In the **User tree for login to server** field, specify the tree in which the user specified in the 'Settings' tab resides. For example, in AD the 'administrator' account's default tree is the same as the user tree.

Step 26 In the **Trees containing users** field, specify the trees where users commonly reside in the LDAP directory. One default value is provided that can be edited, a maximum of 64 DN values may be provided, and the SonicWALL security appliance searches the directory until a match is found, or the list is exhausted. If you have created other user containers within your LDAP or AD directory, you should specify them here.

Step 27 In the **Trees containing user groups** specify the trees where user groups commonly reside in the LDAP directory. A maximum of 32 DN values may be provided. These are only applicable when there is no user group membership attribute in the schema's user object, and are not used with AD.

The above-mentioned trees are normally given in URL format but can alternatively be specified as distinguished names (for example, "myDom.com/Sales/Users" could alternatively be given as the DN "ou=Users,ou=Sales,dc=myDom,dc=com"). The latter form will be necessary if the DN does not conform to the normal formatting rules as per that example. In Active Directory the URL corresponding to the distinguished name for a tree is displayed on the Object tab in the properties of the container at the top of the tree.



Note

AD has some built-in containers that do not conform (for example, the DN for the top level Users container is formatted as "cn=Users,dc=...", using 'cn' rather than 'ou') but the SonicWALL knows about and deals with these, so they can be entered in the simpler URL format.

Ordering is not critical, but since they are searched in the given order it is most efficient to place the most commonly used trees first in each list. If referrals between multiple LDAP servers are to be used, then the trees are best ordered with those on the primary server first, and the rest in the same order that they will be referred.

**Note**

When working with AD, to locate the location of a user in the directory for the 'User tree for login to server' field, the directory can be searched manually from the Active Directory Users and Settings control panel applet on the server, or a directory search utility such as queryad.vbs in the Windows NT/2000/XP Resource Kit can be run from any PC in the domain.

Step 28 The **Auto-configure** button causes the SonicWALL security appliance to auto-configure the 'Trees containing users' and 'Trees containing user groups' fields by scanning through the directory/directories looking for all trees that contain user objects. The 'User tree for login to server' must first be set.

Select whether to append new located trees to the current configuration, or to start from scratch removing all currently configured trees first, and then click **OK**. Note that it will quite likely locate trees that are not needed for user login and manually removing such entries is recommended.

If using multiple LDAP/AD servers with referrals, this process can be repeated for each, replacing the 'Domain to search' accordingly and selecting 'Append to existing trees' on each subsequent run.

Step 29 Select the **Referrals** tab.



Step 30 If multiple LDAP servers are in use in your network, LDAP referrals may be necessary. Select one or more of the following check boxes:

- **Allow referrals** – Select when user information is located on an LDAP server other than the primary one.
- **Allow continuation references during user authentication** – Select when individual directory trees span multiple LDAP servers.
- **Allow continuation references during directory auto-configuration** – Select to read directory trees from multiple LDAP servers in the same operation.

- **Allow continuation references in domain searches** – Select to search for sub-domains in multiple LDAP servers.

Step 31 Select the **LDAP Users** tab.

- Step 32** Check the **Allow only users listed locally** box to require that LDAP users also be present in the SonicWALL security appliance local user database for logins to be allowed.
- Step 33** Check the **User group membership can be set locally by duplicating LDAP user names** box to allow for group membership (and privileges) to be determined by the intersection of local user and LDAP user configurations.
- Step 34** From the **Default LDAP User Group** drop-down menu, select a default group on the SonicWALL security appliance to which LDAP users will belong in addition to group memberships configured on the LDAP server.



Tip

Group memberships (and privileges) can also be assigned simply with LDAP. By creating user groups on the LDAP/AD server with the same name as SonicWALL security appliance built-in groups (such as **Guest Services**, **Content Filtering Bypass**, **Limited Administrators**) and assigning users to these groups in the directory, or creating user groups on the SonicWALL security appliance with the same name as existing LDAP/AD user groups, SonicWALL group memberships will be granted upon successful LDAP authentication.

The SonicWALL security appliance can retrieve group memberships more efficiently in the case of Active Directory by taking advantage of its unique trait of returning a 'memberOf' attribute for a user.

- Step 35** Click the **Import user groups** button to import user groups from the LDAP server. The names of user groups on the LDAP server need to be duplicated on the SonicWALL if they are to be used in policy rules, CFS policies, etc.

Step 36 Select the **LDAP Relay** tab.

SONICWALL Network Security Appliance

Settings Schema Directory Referrals LDAP Users **LDAP Relay** Test

RADIUS to LDAP Relay Settings

This SonicWALL can operate as a RADIUS server for remote SonicWALLs that do not support LDAP, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

☐ Enable RADIUS to LDAP Relay

Allow RADIUS clients to connect via:

☐ Trusted Zones ☒ WAN Zone ☐ Public Zones ☐ Wireless Zones ☒ VPN Zone

RADIUS shared secret:

User group for legacy VPN users:

User group for legacy VPN client users:

User group for legacy L2TP users:

User group for legacy users with Internet access:

Ready

OK Cancel Apply Help

Step 37 Select the **Enable RADIUS to LDAP Relay** checkbox to enable RADIUS to LDAP relay. The RADIUS to LDAP Relay feature is designed for use in a topology where there is a central site with an LDAP/AD server and a central SonicWALL security appliance with remote satellite sites connected into it using SonicWALL security appliances that may not support LDAP. In that case the central SonicWALL security appliance can operate as a RADIUS server for the remote SonicWALL security appliances, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

Additionally, for remote SonicWALL security appliances running non-enhanced firmware, with this feature the central SonicWALL security appliance can return legacy user privilege information to them based on user group memberships learned using LDAP. This avoids what can be very complex configuration of an external RADIUS server such as IAS for those SonicWALL security appliances.

Step 38 Under **Allow RADIUS clients to connect via**, select the relevant checkboxes and policy rules will be added to allow incoming Radius requests accordingly. The options are:

- **Trusted Zones**
- **WAN Zone**
- **Public Zones**
- **Wireless Zones**
- **VPN Zone**

Step 39 In the **RADIUS shared secret** field, enter a shared secret common to all remote SonicWALL security appliances.

Step 40 In the **User groups for legacy users** fields, define the user groups that correspond to the legacy 'VPN users,' 'VPN client users,' 'L2TP users' and 'users with Internet access' privileges. When a user in one of the given user groups is authenticated, the remote SonicWALL security appliances will be informed that the user is to be given the relevant privilege.

**Note**

The 'Bypass filters' and 'Limited management capabilities' privileges are returned based on membership to user groups named 'Content Filtering Bypass' and 'Limited Administrators' – these are not configurable.

Step 41 Select the **Test** tab.

SONICWALL Network Security Appliance

Settings Schema Directory Referrals LDAP Users LDAP Relay **Test**

Test LDAP Settings

To test the LDAP settings, enter a valid LDAP login name and password and click the Test button. Note that this will apply any changes that have been made.

User:

Password:

Test: ☒ Password authentication ☐ CHAP

Test Status:
Ready

Message from LDAP:

Returned User Attributes:

Ready

OK Cancel Apply Help

The 'Test' page allows for the configured LDAP settings to be tested by attempting authentication with specified user and password credentials. Any user group memberships and/or framed IP address configured on the LDAP/AD server for the user will be displayed.

Step 42 In the **Username** and **Password** fields, enter a valid LDAP login name for the LDAP server you configured.

Step 43 Select **Password authentication** or **CHAP** (Challenge Handshake Authentication Protocol).

**Note**

CHAP only works with a server that supports retrieving user passwords using LDAP and in some cases requires that the LDAP server to be configured to store passwords reversibly. CHAP cannot be used with Active Directory.

Step 44 Click **Test**. Status and information returned from the LDAP server are displayed in the **Test Status**, **Message from LDAP**, and **Returned User Attributes** fields.

Tuning Single Sign-On Advanced Settings

This section provides detailed information to help you tune the advanced SSO settings on your SonicWALL appliance. See the following sections:

- [“Overview” on page 52](#)
- [“About the Advanced Settings” on page 52](#)
- [“Using the Single Sign-On Statistics in the TSR” on page 53](#)
- [“Examining the Agent” on page 54](#)
- [“Remedies” on page 54](#)

Overview

When a user first tries to send traffic through a SonicWALL that is using SSO, the appliance sends a “who is this” request to SonicWALL SSO Agent. The agent queries the user’s PC via Windows networking, and returns the user name to the SonicWALL appliance. If the user name matches any criteria set in the policies, then the user is considered as “logged on” by the SonicWALL. When users are logged into the SonicWALL using SSO, the SSO feature also provides detection of logouts. To detect logouts, the appliance repeatedly polls the agent to check if each user is still logged in. This polling, along with the initial identification requests, could potentially result in a large loading on the SonicWALL SSO Agent application and the PC on which it is running, especially when very large numbers of users are connecting.

The SonicWALL SSO feature utilizes a rate-limiting mechanism to prevent the appliance from swamping the agent with these user requests. Both automatic calculations and a configurable setting on the appliance govern how this rate-limiting operates. The SonicWALL SSO feature automatically calculates the maximum number of user requests contained in each message to the agent that can be processed in the poll period, based on recent polling response times. Also, the timeout on a multi-user request is automatically set to be long enough to reduce the likelihood of an occasional long timeout during polling. The configurable setting controls the number of requests to send to the agent at a time, and can be tuned to optimize SSO performance and prevent potential problems. This section provides a guide to choosing suitable settings.

The potential for problems resulting from overloading the agent can be reduced by running the agent on a dedicated high-performance PC, and possibly also by using multiple agents on separate PCs, in which case the load will be shared between them. The latter option also provides redundancy in case one of the agent PCs fails. The agent should run on a Windows Server PC (some older workstations could be used but changes in later Windows 2000/XP/Vista workstation releases and in service packs for the older versions added a TCP connection rate limiting feature that interferes with operation of the SSO agent).

About the Advanced Settings

The **Maximum requests to send at a time** setting is available on the **Advanced** tab of the SSO agent configuration.

This setting controls the maximum number of requests that can be sent from the appliance to the agent at the same time. The agent processes multiple requests concurrently, spawning a separate thread in the PC to handle each. Sending too many requests at a time can overload the PC on which the agent is running. If the number of requests to send exceeds the maximum, then some are placed on an internal “ring buffer” queue (see [“Using the Single Sign-On Statistics in the TSR” on page 53](#) and [“Viewing SSO Statistics and Tooltips” on page 57](#)). Requests waiting on the ring buffer for too long could lead to slow response times in SSO authentication.

This setting works in conjunction with the automatically calculated number of user requests per message to the agent when polling to check the status of logged in users. The number of user requests per message is calculated based on recent polling response times. SonicOS adjusts this number as high as possible to minimize the number of messages that need to be sent, which reduces the load on the agent and helps reduce

network traffic between the appliance and the agent. However, the number is kept low enough to allow the agent to process all of the user requests in the message within the poll period. This avoids potential problems such as timeouts and failures to quickly detect logged out users.

Using the Single Sign-On Statistics in the TSR

A rich set of SSO performance and error statistics is included in the trouble shooting report (TSR). These can be used to gauge how well SSO is performing in your installation. Download the TSR on the **System > Diagnostics** page and search for the title “SSO operation statistics”. The following are the counters to look at in particular:

1. Under **SSO ring buffer statistics**, look at **Ring buffer overflows** and **Maximum time spent on ring**. If the latter approaches or exceeds the polling rate, or if any ring buffer overflows are shown, then requests are not being sent to the agent quickly enough. Also, if the **Current requests waiting on ring** is constantly increasing, that would indicate the same. This means that the **Maximum requests to send at a time** value should be increased to send requests faster. However, that will increase the load on the agent, and if the agent cannot handle the additional load, then problems will result, in which case it may be necessary to consider moving the agent to a more powerful PC or adding additional agents.
2. Under **SSO operation statistics**, look at **Failed user id attempts with time outs** and **Failed user id attempts with other errors**. These should be zero or close to it – significant failures shown here indicate a problem with the agent, possibly because it cannot keep up with the number of user authentications being attempted.
3. Also under **SSO operation statistics**, look at the **Total users polled in periodic polling**, **User polling failures with time outs**, and **User polling failures with other errors**. Seeing some timeouts and errors here is acceptable and probably to be expected, and occasional polling failures will not cause problems. However, the error rate should be low (an error rate of about 0.1% or less should be acceptable). Again, a high failure rate here would indicate a problem with the agent, as above.
4. Under **SSO agent statistics**, look at the **Avg user ID request time** and **Avg poll per-user resp time**. These should be in the region of a few seconds or less – something longer indicates possible problems on the network. Note, however, that errors caused by attempting to authenticate traffic from non-Windows PCs via SSO (which can take a significantly long time) can skew the **Avg user ID request time** value, so if this is high but **Avg poll per-user resp time** looks correct, that would indicate the agent is probably experiencing large numbers of errors, likely due to attempting to authenticate non-Windows devices – see below, #6.
5. If using multiple agents, then also under **SSO agent statistics** look at the error and timeout rates reported for the different agents, and also their response times. Significant differences between agents could indicate a problem specific to one agent that could be addressed by upgrading or changing settings for that agent in particular.
6. Traffic from devices other than PCs can trigger SSO identification attempts and that can cause errors and/or timeouts to get reported in these statistics. This can be avoided by configuring an address object group with the IP addresses of such devices, and doing one or both of the following:
 - If using Content Filtering, select that address object with the **Bypass the Single Sign On process for content filtering of traffic from** setting on the Security Services tab of the SSO configuration.
 - If access rules are set to allow only authenticated users, set separate rules for that address object with **Users Allowed** set to **All**.

To identify the IP addresses concerned, look in the TSR and search for “IP addresses held from SSO attempts”. This lists SSO failures in the preceding period set by the **Hold time after failure** setting.



Note

If any of the listed IP addresses are for Mac/Linux PCs, see the [“Accommodating Mac and Linux Users”](#) section on page 55.

To limit the rate of errors due to this you can also extend the **Hold time after failure** setting on the Users tab.

For information about viewing SSO statistics on the SSO configuration page, see [“Viewing SSO Statistics and Tooltips” on page 57](#).

Examining the Agent

If the above statistics indicate a possible problem with the agent, a good next step would be to run Windows Task Manager on the PC on which the agent is running and look at the CPU usage on the **Performance** tab, plus the CPU usage by the “CIAService.exe” process on the **Processes** tab. If the latter is using a large percentage of the CPU time and the CPU usage is spiking close to 100%, this is an indication that the agent is getting overloaded. To try to reduce the loading you can decrease the **Maximum requests to send at a time** setting; see [“Using the Single Sign-On Statistics in the TSR” above, #1](#).

Remedies

If the settings cannot be balanced to avoid overloading the agent’s PC while still being able to send requests to the agent fast enough, then one of the following actions should be taken:

- Consider reducing the polling rate configured on the **Users** tab by increasing the poll time. This will reduce the load on the agent, at the cost of detecting logouts less quickly. Note that in an environment with shared PCs, it is probably best to keep the poll interval as short as possible to avoid problems that could result from not detecting logouts when different users use the same PC, such as the initial traffic from the second user of a PC possibly being logged as sent by the previous user.
- Move the agent to a higher-performance, dedicated PC.
- Configure an additional agent or agents.

Configuring Firewall Access Rules

Enabling SonicWALL SSO affects policies on the **Firewall > Access Rules** page of the SonicOS Enhanced management interface. Rules set under **Firewall > Access Rules** are checked against the user group memberships returned from a SSO LDAP query, and are applied automatically.

See the following sections for more information:

- [“Automatically Generated Rules for SonicWALL SSO” on page 54](#)
- [“Accommodating Mac and Linux Users” on page 55](#)
- [“Allowing ICMP Pings from a Terminal Server” on page 56](#)
- [“About Firewall Access Rules” on page 56](#)

Automatically Generated Rules for SonicWALL SSO

When a SonicWALL SSO agent or TSA is configured in the SonicOS Enhanced management interface, a Firewall access rule and corresponding NAT policy are created to allow the replies from the agent into the LAN. These rules use either a **SonicWALL SSO Agents** or **SonicWALL Terminal Services Agents** address group object, which has a member address object for each configured agent. The member address objects are automatically added to and deleted from the group object as agents are added or deleted. The member address objects are also updated automatically as an agent’s IP address changes, including when an IP address is resolved via DNS (where an agent is given by DNS name).

If SonicWALL SSO agents or TSAs are configured in different zones, the Firewall access rule and NAT policy are added to each applicable zone. The same **SonicWALL SSO Agents** or **SonicWALL Terminal Services Agents** address group is used in each zone.

Accommodating Mac and Linux Users

Mac and Linux systems do not support the Windows networking requests that are used by the SonicWALL SSO agent, and hence do not work with Single Sign-On. This can cause the following problems:

- Traffic from Mac or Linux systems might keep triggering SSO identification attempts unless the user logs in. This could potentially be a performance overhead to the SSO system if there are a large number of such systems, although the effect would be somewhat mitigated by the “hold after failure” timeout.
- If per-user Content Filtering (CFS) policies are used without policy rules with user level authentication, the default CFS policy will be applied to users of Mac and Linux systems unless they manually log in first.
- If policy rules are set requiring user level authentication, Web browser connections from users of Mac and Linux systems will be redirected to the login page after the SSO failure, but the failure may initiate a timeout that would cause a delay for the user.

To avoid these problems, the **Don't invoke Single Sign On to Authenticate Users** checkbox is available when configuring Firewall access rules by clicking **Add** on the Firewall > Access Rules page (with **View Style** set to **All Rules**). This checkbox is visible only when SonicWALL SSO is enabled and when the **Users Allowed** field on the Add Rule page is not set to **All**. If this checkbox is selected, SSO will not be attempted for traffic that matches the rule, and unauthenticated HTTP connections that match it will be directed straight to the login page. Typically, the **Source** field would be set to an address object containing the IP addresses of Mac and Linux systems.

In the case of CFS, a rule with this checkbox enabled can be added “in front of” CFS so that HTTP sessions from Mac and Linux systems are automatically redirected to log in, avoiding the need for these users to log in manually.

**Note**

Do not select the **Don't invoke Single Sign On to Authenticate Users** option for use with devices that are allowed to bypass the user authentication process entirely. Any devices that may be affected by an access rule when this option is enabled must be capable of logging in manually. A separate access rule should be added for such devices, with **Users Allowed** set to **All**.

Allowing ICMP Pings from a Terminal Server

In Windows, outgoing ICMP pings from users on the Terminal Server are not sent via a socket and so are not seen by the TSA, and hence the appliance will receive no notifications for them. Therefore, if firewall rules are using user level authentication and pings are to be allowed through, you must create separate access rules to allow them from "All".

About Firewall Access Rules

Firewall access rules provide the administrator with the ability to control user access. Access rules are network management tools that allow you to define inbound and outbound access policy, configure user authentication, and enable remote management of the SonicWALL security appliance. The SonicOS **Firewall > Access Rules** page provides a sortable access rule management interface.

**Note**

More specific policy rules are given higher priority than general policy rules. The general specificity hierarchy is source, destination, service. User identification elements, for example, user name and corresponding group permissions, are not included in defining the specificity of a policy rule.

By default, SonicWALL security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic from the Internet to the LAN.

Additional network access rules can be defined to extend or override the default access rules. For example, access rules can be created that block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

**Note**

The ability to define network access rules is a powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.

For detailed information about the **Firewall > Access Rules** page, refer to the *SonicOS Enhanced Administrator's Guide*.


Managing SonicOS with HTTP Login from a Terminal Server

The SonicWALL UTM appliance normally grants access through policies based on authentication credentials supplied via HTTP login for one user at an IP address. For users on a terminal server, this method of authenticating one user per IP address is not possible. However, HTTP login is still allowed from a terminal server only for the purpose of administration of the appliance, subject to the following limitations and requirements:

- Internet access from the terminal server is controlled from the TSA, and HTTP login does not override that – a user on a terminal server is not granted any access through the appliance based on credentials supplied via HTTP login.
- HTTP login from a terminal server is allowed only for the built-in **admin** account and other user accounts with administrator privileges. An attempt to log in with a non-administrative account will fail with the error “Not allowed from this location.”
- On successful HTTP login, an administrative user is taken straight to the management interface. The small “User Login Status” page is not displayed.
- The administrative user account used for HTTP login from the terminal server does not need to be the same user account that was used for login to the terminal server. It is shown on the appliance as an entirely separate login session.
- Only one user at a time can manage the appliance from a given terminal server. If two users attempt to do so simultaneously, the most recently logged in user takes precedence, and the other user will see the error “This is not the browser most recently used to log in.”
- On a failure to identify a user due to communication problems with the TSA, an HTTP browser session is not redirected to the Web login page (as happens on a failure in the SSO case). Instead, it goes to a new page with the message “The destination that you were trying to reach is temporarily unavailable due to network problems.”

Viewing SSO Statistics and Tooltips

The SSO Configuration page provides mouseover statistics about each agent, and mouseover tooltips for many fields. On the Settings tab, a green LED-style icon next to an agent indicates that the agent is up and running. A red LED icon indicates that the agent is down.

To view the statistics for a particular agent, hover your mouse pointer over the statistics icon  to the right of the SSO agent. This also works for individual TSAs on the Terminal Services tab.



The screenshot shows the 'Settings' tab of the SonicWALL Security Appliance. Under 'Authentication Agent Settings', there is a table with columns: #, Status, Host Name/IP Address, Port, Timeout, Retries, Max Rqpts, and Enable. The first agent (ID 1) is shown with a green status icon and IP address 192.168.168.3. A mouseover tooltip titled 'SSO Agent 1 Statistics' is displayed, showing the following data:

Field	Value
Agent:	192.168.168.3:2258
IP address:	192.168.168.3
Status:	up
User requests, replies:	11, 11
Multi-user requests, replies:	882, 876
Users per multi-user request (min, max):	1, 1
SSO ping requests, replies:	1, 1
Error, invalid, timed-out, late replies:	9, 0, 6, 0
Max outstanding requests:	2
SSO ping response time (avg, max):	17 mS, 17 mS
User ID request time (avg, max, current):	203 mS, 2.95 secs, 203 mS
Poll request time (avg, max, current):	33 mS, 6.02 secs, 200 mS
Per-user poll resp time (avg, max, current):	33 mS, 6.02 secs, 200 mS

At the bottom of the tooltip, there is a link that says 'Click to reset'.

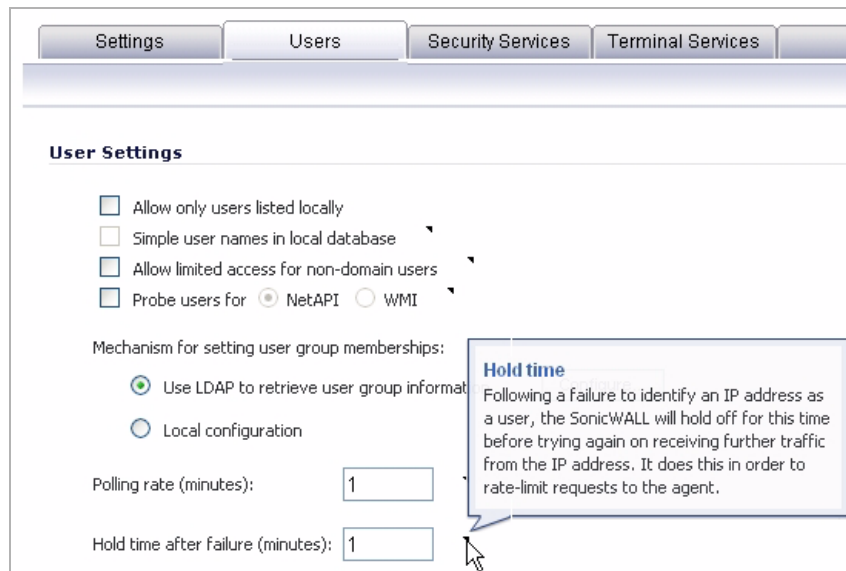
To view the statistics for all SSO agent activity on the appliance, hover your mouse pointer over the statistics icon at the bottom of the table, in the same row as the **Add** button. Use this same method on the Terminal Services tab to view all TSA activity.



To close the statistics display, click **close**.

To clear all the displayed values, click **Click to reset**.

To view the tooltips available for many fields in the SSO configuration screens, hover your mouse pointer over the triangular icon to the right of the field. The tooltip will display until you move your mouse pointer away.



Viewing User Status

The **Users > Status** page displays **Active User Sessions** on the SonicWALL security appliance. The table lists **User Name**, **IP Address**, **Session Time**, **Time Remaining**, **Inactivity Remaining**, **Settings**, and **Logout**. For users authenticated using SonicWALL SSO Agent, the message **Auth. by SSO Agent** will display.

To log a user out, click the Logout icon next to the user's entry.



Note

Changes in a user's settings, configured under **Users > Settings**, will not be reflected during that user's current session; you must manually log the user out for changes to take effect. The user will be transparently logged in again, with the changes reflected.

Configuring Additional User Settings

The **Users > Settings** page provides the administrator with configuration options for user session settings, global user settings, and acceptable use policy settings, in addition to SSO and other user login settings.

The **Enable login session limit** and corresponding **Login session limit (minutes)** settings under User Session Settings apply to users logged in using SSO. SSO users will be logged out according to session limit settings, but will be automatically and transparently logged back in when they send further traffic.



Note

Do not set the login session limit interval too low. This could potentially cause performance problems, especially for deployments with many users.

Changes applied in the **Users > Settings** page during an active SSO session will not be reflected during that session.



Tip

You must log the user out for changes to take effect. The user will immediately and automatically be logged in again, with the changes made.

For information about the **Users > Settings** page, refer to the *SonicOS Enhanced Administrator's Guide*.

Viewing SSO and LDAP Messages with Packet Monitor

In SonicOS Enhanced 5.6 and above, the Packet Monitor feature available on **System > Packet Monitor** provides two checkboxes to enable capture of decrypted messages to and from the SSO agent, and decrypted LDAP over TLS (LDAPS) messages.

In SonicOS Enhanced 5.5, this functionality was introduced in the Packet Capture feature available on **System > Packet Capture**.

Capturing SSO Messages

To capture decrypted messages to or from the SSO authentication agent, perform the following steps:

- Step 1** Click the **Configuration** button in the **System > Packet Monitor** page
- Step 2** Click the **Advanced Monitor Filter** tab

Step 3 Select the **Monitor intermediate Packets** checkbox.

Step 4 Select the **Monitor intermediate decrypted Single Sign On agent messages** checkbox.

Step 5 Click **OK**.

The packets will be marked with **(sso)** in the ingress/egress interface field. They will have dummy Ethernet, TCP, and IP headers, so some values in these fields may not be correct.

This will enable decrypted SSO packets to be fed to the packet monitor, but any monitor filters will still be applied to them.

Captured SSO messages are displayed fully decoded on the **System > Packet Monitor** screen.

Captured Packets Items 1 to 4 (of 4)

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
1	03/02/2009 16:50:47.672	--	X0*(sso)	192.168.168.40	192.168.168.3	IP	UDP	2259,2259	GENERATED	106[106]
2	03/02/2009 16:50:47.672	--	X0*(s)	192.168.168.40	192.168.168.3	IP	UDP	2259,2259	GENERATED	106[106]
3	03/02/2009 16:50:47.688	X0*()	--	192.168.168.3	192.168.168.40	IP	UDP	3047,2259	CONSUMED	114[114]
4	03/02/2009 16:50:47.704	X0*(sso)	--	192.168.168.3	192.168.168.40	IP	UDP	3047,2259	CONSUMED	114[114]

Packet Detail

```

Mag len = 64
Req Id = 0x01000007
Signature = 0x00000000
Protocol: 0005 0008: 00 00 00 02 00 00 00 02
Serial #: 0004 000D: 30 30 31 37 43 35 31 41 32 44 34 38 00
User Name: 0002 0008: 53 44 38 30 2F 69 61 6E 'SD80/lan'
User IP: 0001 0004: C0 A8 A8 09 '192.168.168.9'
  
```

Hex Dump

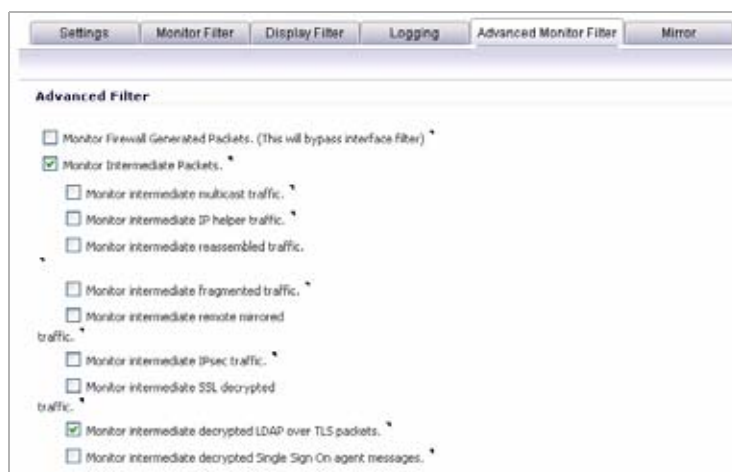
```

00000000 00000000 00000000 08004510 00640000 40008011 *......E..d...@...*
0000c0a8 a803c0a8 a8280be7 08d30050 00000000 00000000 *......P.....*
00000202 00400100 00070000 00000005 00080000 00020000 *......@.....*
00020004 000d3030 31374335 31413244 34380000 02000853 *......0017C51A2D48.....5*
4438302f 69616e00 010004c0 a8a80900 0000      *D80/lan.....*
  
```

Capturing LDAP Over TLS Messages

To capture decrypted LDAP over TLS (LDAPS) packets, perform the following steps:

- Step 1** Click the **Configuration** button in the **System > Packet Monitor** page
- Step 2** Click the **Advanced Monitor Filter** tab
- Step 3** Select the **Monitor intermediate Packets** checkbox.
- Step 4** Select the **Monitor intermediate decrypted LDAP over TLS packets** checkbox.



- Step 5** Click **OK**.

The packets will be marked with **(ldp)** in the ingress/egress interface field. They will have dummy Ethernet, TCP, and IP headers, so some values in these fields may not be correct. The LDAP server port will be set to 389 so that an external capture analysis program (such as Wireshark) will know to decode these packets as LDAP. Passwords in captured LDAP bind requests will be obfuscated. The LDAP messages are not decoded in the Packet Monitor display, but the capture can be exported and displayed in WireShark to view them decoded.

This will enable decrypted LDAPS packets to be fed to the packet monitor, but any monitor filters will still be applied to them.



Note

LDAPS capture only works for connections from the SonicWALL appliance's LDAP client, and will not display LDAP over TLS connections from an external LDAP client that pass through the appliance.

Glossary

ADConnector (ADC) - A SonicWALL authentication agent for Microsoft Active Directory users.

Directory Connector (DSC) - A SonicWALL application suite that includes SSO Agent, ADConnector, and NDConnector.

NDConnector (NDC) - A SonicWALL authentication agent for Novell eDirectory users.

Single Sign-On Agent (SSO Agent) - The authentication application used by SonicWALL security appliances to return the identity of a user at an IP address using ADConnector-compatible protocol.

Single Sign-on - A method of automatic authentication that recognizes a user upon network login.

Terminal Services Agent (TSA) - The authentication application used by SonicWALL security appliances to return the identity of a user on a Terminal Services system.

Solution Document Version History

Version Number	Date	Notes
1	7/31/2006	This document was created for SonicOS Enhanced 4.0
2	3/1/2007	Document finalized for SonicOS Enhanced 4.0
3	7/25/2007	Document updated for SonicOS Enhanced 5.0
4	1/5/2009	Document updated for SonicOS Enhanced 5.1
5	5/20/2009	Document updated for SonicOS Enhanced 5.5 by sweigand
6	7/27/2009	Additional updates for SonicOS Enhanced 5.5 by sweigand
7	1/5/2010	Updated for SonicOS Enhanced 5.6 by sweigand: Added TSA for Terminal Services/Citrix support; changed Packet Capture to Packet Monitor; added NDConnector sections