Single Sign-On

Document Scope
This document describes how to plan, design, implement, and maintain the Single Sign-On feature in the SonicWALL SonicOS 5.1 Enhanced.

This document contains the following sections:

• “Single Sign-On Overview” section on page 2
  – “Benefits” section on page 3
  – “Supported Standards” section on page 3
  – “How Does Single Sign-On Work?” section on page 4

• “Configuring Single Sign-On Task List” section on page 7
  – “Installing the SonicWALL SSO Agent” section on page 8
  – “Configuring the SonicWALL SSO Agent” section on page 12
  – “Configuring Your SonicWALL Security Appliance” section on page 19

• “Glossary” section on page 33
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 2
- “Benefits” section on page 3
- “How Does Single Sign-On Work?” section on page 4
- “Supported Standards” section on page 3

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 workstation login. SonicWALL security appliances provide SSO functionality using the SonicWALL Single Sign-On Agent (SSO Agent) to identify user activity based on workstation IP address. 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 identifies users by IP address using a SonicWALL ADConnector-compatible protocol and automatically determines when a user has logged out to prevent unauthorized access. Based on data from SonicWALL SSO Agent, the SonicWALL security appliance queries LDAP or the local database to determine group membership. Memberships are matched against policy, and based on user privileges, access is granted or denied. The configured inactivity and session limit timers apply with SSO, though users who are logged out are automatically and transparently logged back in when they send further traffic.

Users logged into a workstation directly but not logged into the domain will not be authenticated. For users that are not logged into the domain, 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 Denied
Benefits

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, 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 specific 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 workstation on the LAN.
• Login mechanism works with any protocol, not just HTTP.

Supported Standards

The SonicWALL SSO feature supports LDAP and local database protocols.

To use SonicWALL SSO, it is required that the SonicWALL SSO Agent be installed on the workstations within your Windows domain that can reach clients directly using a static IP or through a VPN path. The following requirements must be met in order to run the SSO Agent:

• Port 2258 must be open; the firewall uses UDP port 2258 by default to communicate with SonicWALL SSO Agent
• Windows 32 or XP, with latest service pack
• .NET Framework 2.0
• Net API or WMI
How Does Single Sign-On Work?

SonicWALL SSO requires minimal administrator configuration and is transparent to the user. There are six steps involved in SonicWALL SSO authentication, as illustrated in Figure 3.

**Figure 3  SonicWALL Single Sign-On Process**

1. **User attempts to send traffic through SonicWALL appliance.**
2. **SonicWALL appliance sends user’s IP address to the SSO workstation for “User Name Request.” Blocked packets are saved.**
3. **SSO workstation replies with the username of the user who is logged into the workstation.**
4. **LDAP or Local Database is used to find group membership.**
5. **Based on group membership and policy match, access is granted and the SonicWALL appliance allows the user traffic out. If applicable, saved packets are reinstated and sent.**

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, similar to RADIUS and LDAP.

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.

The SonicWALL security appliance polls the authorization agent running the SSO Agent at a configurable 
rate to determine when a user has logged out. Configurable user session limits, inactivity timers, and user 
name request polls are other methods to determine user logout status. Upon user logout, the authentication 
agent running the SSO Agent sends a User Logged Out response to the SonicWALL security appliance, 
confirming the user has been logged out and terminating the SSO session.
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 8. 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. 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

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

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`.

---

**Configuring Single Sign-On Task List**

Configuring SSO is a process that includes installing and configuring the SonicWALL SSO Agent and configuring a SonicWALL security appliance to use the SSO Agent.

This section contains the following subsections:

- “Installing the SonicWALL SSO Agent” section on page 8
- “Configuring the SonicWALL SSO Agent” section on page 12
  - “Adding a SonicWALL Security Appliance” section on page 16
  - “Editing Appliances in SonicWALL SSO Agent” section on page 18
  - “Deleting Appliances in SonicWALL SSO Agent” section on page 18
  - “Modifying Services in SonicWALL SSO Agent” section on page 18
- “Configuring Your SonicWALL Security Appliance” section on page 19
  - “Advanced LDAP Configuration” section on page 24
- “Configuring Firewall Access Rules” section on page 32
  - “Viewing User Status” section on page 32
  - “Configuring User Settings” section on page 32
Installing the SonicWALL SSO Agent

The SonicWALL SSO Agent is an application that must be installed on a workstation or server in the Windows domain that is accessible using VPN or IP. The SonicWALL SSO Agent must have access to your SonicWALL security appliance. To install the SonicWALL SSO Agent, perform the following steps:

**Step 1** Locate the SonicWALL Directory Connector executable file and double click it. It may take several seconds for the InstallShield to prepare for the installation.

**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  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, the installation icon is displayed by default next to the SonicWALL SSO Agent feature. Click Next.

Step 7  Click Install to install SSO Agent.
Step 8  To configure a common service account that the 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 9  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.

The SonicWALL SSO Agent installs. The status bar displays.

Step 10  When installation is complete, optionally check the Launch SonicWALL Directory Connector box to launch the SonicWALL Directory Connector, and click Finish.
If you checked the **Launch SonicWALL Directory Connector** box, the SonicWALL Directory Connector will display.
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 2003, Windows XP, 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.

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.

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**.

![Directory Connector Configurator](image)

**Note** NetAPI will provide faster, though possibly slightly less accurate, performance. WMI will provide slower, though possibly more accurate, performance. WMI is pre-installed on Windows Server 2003, Windows XP, 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.

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`.

![Directory Connector Configurator](image)

**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 to generate a shared key. When you are finished, click OK.

Your appliance will display in the left-hand navigation panel under the SonicWALL Appliances tree.
Configuring Single Sign-On Task List

**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 Your SonicWALL Security Appliance

Your SonicWALL security appliance must be configured to use SonicWALL SSO Agent as the SSO method.

To configure your SonicWALL security appliance, perform the following steps:

**Step 1**  
Login to your SonicWALL security appliance.

**Step 2**  
Navigate to Users > Settings.

**Step 3**  
In the Single-sign-on method drop-down menu, select SonicWALL SSO Agent.
Step 4  Click **Configure**. The Authentication Agent Settings page displays.

![Authentication Agent Settings](image)

**Step 5** In the **Name or IP Address** field, enter the name or IP Address of the workstation on which SonicWALL SSO Agent is installed.

**Step 6** In **Port Number**, enter the port number of the workstation on which SonicWALL SSO Agent is installed. The default port is 2258.

**Step 7** 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 8** In the **Timeout (seconds)** field, enter a number of seconds before the authentication attempt times out.

**Step 9** In the **Retries** field, enter the number of authentication attempts.
Step 10 Click the Users tab. The User Settings page displays.

Step 11 Check the box next to **Allow only users listed locally** to allow only users listed locally to be authenticated.

Step 12 Check the box next to **Simple user names in local database** to use simple user names. This setting ignores the domain component of a user name. 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 13 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 access to the Trusted Users user group. They are identified in logs as `computer-name/user-name`. When performing local 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 14 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 configuration information for this page, refer to “**Advanced LDAP Configuration**” section on page 24.

Step 15 To use local configuration, select the **Local configuration** radio button.

Step 16 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.

Step 17 In the **Hold time after (minutes)** field, enter a time, in minutes, that the security appliance will wait before trying again to identify traffic after an initial failure to do so. This feature rate-limits requests to the agent.
**Step 18**  Click on the **Content Filter** tab if you are using the SonicWALL Content Filtering Service (CFS) and there is a proxy server in your network.

**Note**  The **Content Filter** tab is only displayed if Premium CFS is enabled on the SonicWALL security appliance.

---

**Step 19**  To bypass SSO for content filtering traffic and apply the default content filtering policy to the traffic, select the appropriate address object or address group from the pulldown menu. This setting should be used where traffic that would be subject to content filtering 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 20**  Click the **Test** tab. The Test Authentication Agent Settings page displays.

**Step 21**  Select the **Check agent connectivity** radio button then click the **Test** button. This will test communication with the authentication agent. If the SonicWALL security appliance can connect to the agent, you will see the message **Agent is ready**.

**Step 22**  Select the **Check user** radio button, enter the IP address of a workstation in the **Workstation IP address** field, then click **Test**. This will test if the agent is properly configured to identify the user logged into a workstation.

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

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

**Step 23**  When you are finished, click **OK**.
Advanced LDAP Configuration

If you selected Use LDAP to retrieve user group information in step 14 of “Configuring Your SonicWALL Security Appliance” section on page 19, you must configure your LDAP settings. To configure LDAP settings, perform the following steps:

**Step 1**  The Settings tab displays. In the Name or IP address field, enter the name or IP address of your LDAP server.

Step 2  In the Port Number field, enter the port number of your LDAP server. The default port is 636.

Step 3  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 4  Check the Anonymous login box 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.

Step 5  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 6  Select the LDAP version from the Protocol version drop-down menu, either LDAP version 2 I (LDAPv2) or LDAP version 3 (LDAPv3). Most implementations of LDAP, including AD, employ LDAPv3.
Step 7 Check the **Use TLS (SSL)** box 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 8 Check the **Send LDAP ‘Start TLS’ request** 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 9 Check the **Require valid certificate from server** 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 10 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 11 Click **Apply**.

Step 12 Click the **Schema** tab.
Step 13 From the LDAP Schema pull-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 14 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 15 The Login name attribute field defines which attribute is used for login authentication. This will not be modifiable unless you select User defined.

Step 16 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 17 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 18 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 19 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 20 The Member attribute field defines which attribute is used for login authentication.
Step 21  Select the Directory tab.

Step 22  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 23  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 24  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 25  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.
Configuring Single Sign-On Task List

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 26
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 27 Select the LDAP Users tab.

Step 28 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 29 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 30 From the Default LDAP User Group pull-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 31 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 32  Select the LDAP Relay tab.

Step 33  Check the Enable RADIUS to LDAP Relay box 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 34  Under Allow RADIUS clients to connect via, check 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 35  In the RADIUS shared secret field, enter a shared secret common to all remote SonicWALL security appliances.
Step 36  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 37  Select the Test tab.

![Test LDAP Settings](image)

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

Step 39  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 40  Click Test.
Configuring Single Sign-On Task List

Configuring Firewall Access Rules

Firewall access rules provide the administrator with the ability to control user access. Rules set under **Firewall > Access Rules** are checked against the user group memberships returned from a SSO LDAP query, and are applied automatically. 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. The subsequent sections provide high-level overviews on configuring access rules by zones and configuring bandwidth management using access rules.

Note

More specific policy rules should be 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 to the LAN from the Internet.

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*.

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 logout a user, click the trash can 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 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.
Glossary

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

Single Sign-On Agent (SSO Agent) - The authentication method 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.