SONICWALL®

SonicOS 8

Users

Administration Guide

Contents

1

About SonicOS

This guide is a part of the SonicOS collection of administrative guides that describe how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators with the management interface, API (Application Program Interface), and Command Line Interface (CLI) for firewall configuration. You can configure and manage your firewall by setting objects to secure and protect the network services, manage traffic, and provide the desired level of network service. This guide focuses on guidance to manage locally and remotely authenticated users.

Topics:

Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and outside threats to your network. SonicOS functions in conjunction with SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices such as access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration, and diagnostics.

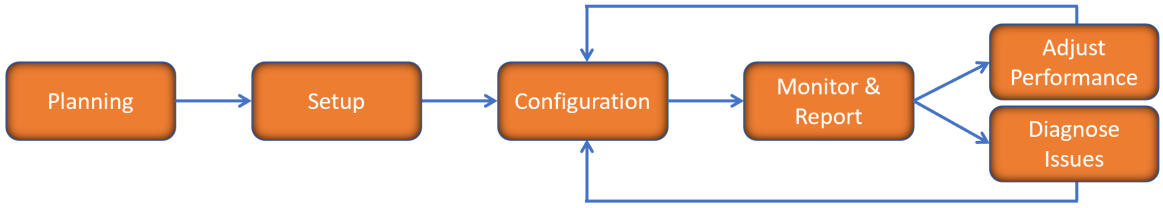
This following table identifies which of these modes can be used on various SonicWall firewalls:

Firewall Type	Comments
TZ Series	The entry level TZ Series, also known as desktop firewalls, delivers revamped features such as 5G readiness, better connectivity options, improved threat protection, SSL and decryption performance that addresses HTPPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support. It provides advanced networking and security features, like the multi-engine Capture Advanced Threat Protection (ATP) cloud-based sandbox service with patent-pending Real-Time Deep Memory Inspection (RTDMI™).

In addition to the management interface, SonicOS also has a full-featured API and a command-line interface (CLI) to manage the firewalls.

SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.

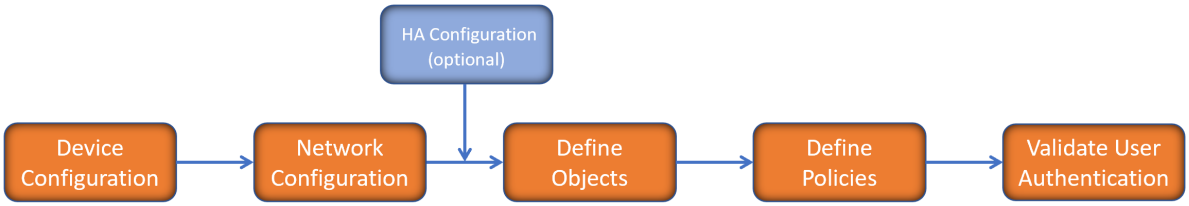


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing product information and solutions. After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The Getting Started Guides for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used use only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the specific Administration Guide for a SonicOS feature for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

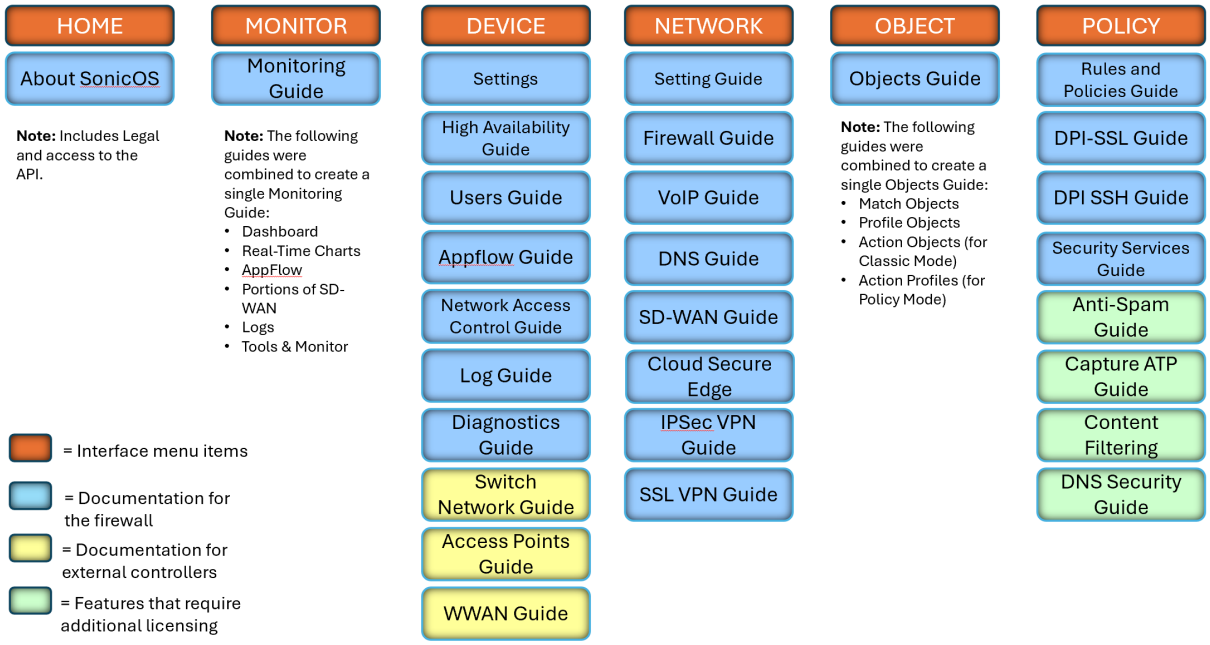


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the SonicOS 8 Monitor Guide and the SonicOS 8 Objects Guide which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicOS management interface.



The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the Technical Documentation portal.

Guide Conventions

These text conventions are used in this guide:

ⓘ | **NOTE:** A NOTE icon indicates supporting information.

ⓘ | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

ⓘ | **TIP:** A TIP icon indicates helpful information.

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

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

Convention	Description
Bold text	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Function | Menu group > Menu item	Indicates a multiple step menu choice on the user interface. For example, **NETWORK | System > Interfaces** means to select the **NETWORK** functions at the top of the window, then click on **System** in the left navigation menu to open the menu group (if needed) and select **Interfaces** to display the page.
`Code`	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<Variable>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment **serialnumber=***<your serial number>*, replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004.
Italics	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

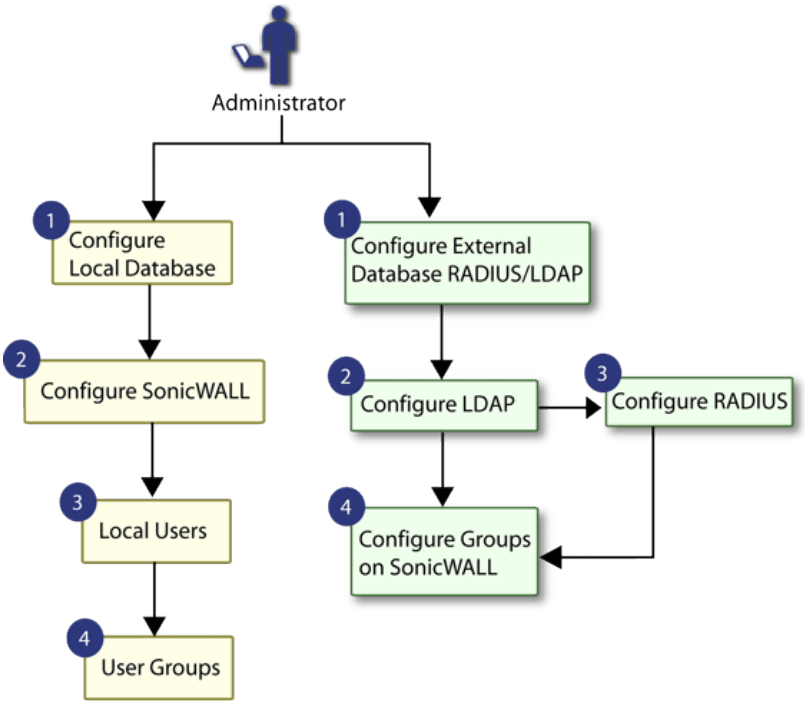
2

About User Management

The SonicWall network security appliance (firewall) provides a mechanism for managing locally and remotely authenticated users. User-level authentication gives users access to the LAN from remote locations on the Internet and allows you to enforce or bypass content filtering policies for LAN users attempting to access the Internet. You can also permit only authenticated users to access VPN tunnels and send data across the encrypted connection.

The firewall authenticates all users when they attempt to access network resources in a different zone (such as WAN, VPN, or WLAN), which causes the network traffic to pass through the firewall. The firewall does not authenticate users who log into a computer on the LAN but performs only local tasks. User-level authentication can be performed using a local user database, LDAP, RADIUS, or a combination of a local database with either LDAP or RADIUS. Authentication using LDAP or RADIUS servers can be more efficient for networks with many users.

SonicOS offers Single Sign-On (SSO) capabilities, which can be used with LDAP.



Topics:

Using Local Users and Groups for Authentication

This section explains the use of local user databases for firewall authentication, highlighting their benefits over LDAP and RADIUS for smaller user groups. It details how these databases store user and group information for access control and content filtering, emphasizing the role of user groups in applying Content Filtering Service (CFS) policies. The integration of local and remote authentication methods is also noted to simplify group management within network security.

Topics:

About User Databases

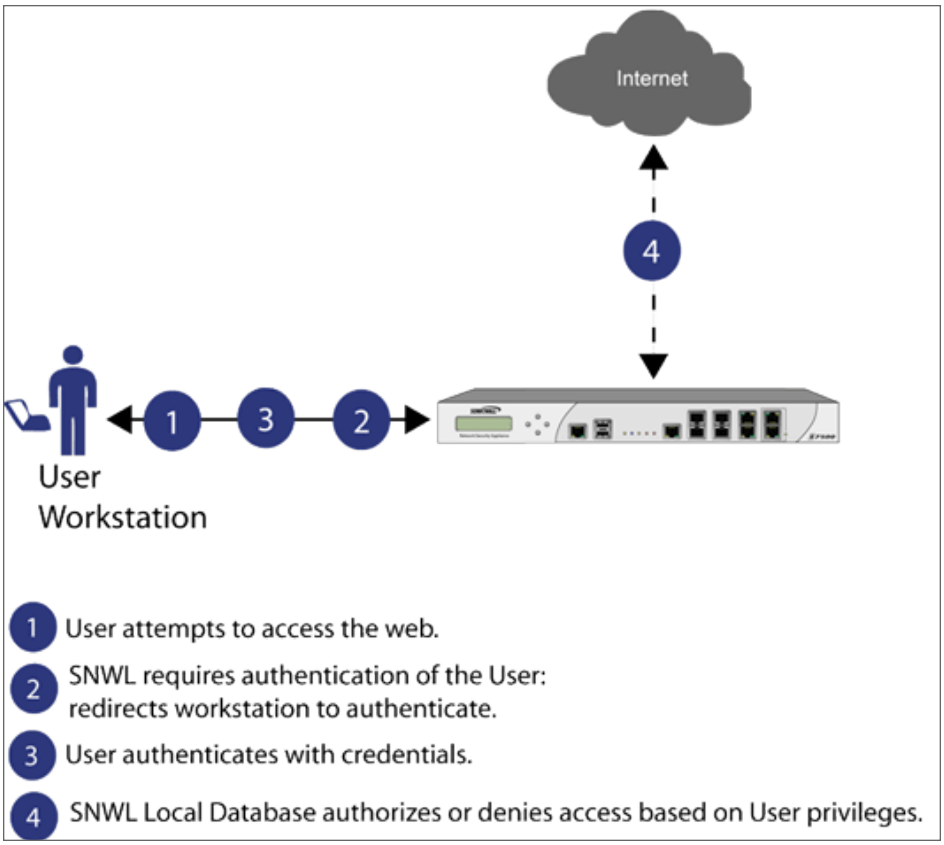
The firewall provides a local database for storing user and group information. You can configure the firewall to use this local database to authenticate users and control their access to the network. The local database is a good choice over LDAP or RADIUS when the number of users accessing the network is relatively small. Creating entries for dozens of users and groups takes time; however, once the entries are in place, they are not difficult to maintain.

The number of users supported by the local database on the firewall varies by platform, as shown in the "Maximum Number of Supported Users by Platform." The overall maximum user limit is equal to the maximum number of SSO users. The maximum number of native users is also equal to the maximum number of SSO users. Additionally, the maximum number of web users represents the combined maximum user logins from the web, GVC, SSL-VPN, and L2TP clients.

About User Groups

To apply Content Filtering Service (CFS) policies to users, the users must be members of local groups, and the CFS policies are then applied to these groups. To use CFS, you cannot utilize LDAP or RADIUS without

combining that method with local authentication. When using this combined authentication method to implement CFS policies, the local group names must exactly match the LDAP or RADIUS group names. By using the LDAP + Local Users authentication method, you can import the groups from the LDAP server into the local database on the firewall. This greatly simplifies the creation of matching groups to which CFS policies can then be applied. See Using Local Users and Groups for Authentication.



The SonicOS Management Interface provides a way to create local user and group accounts. You can add users and edit the configuration for any user, including settings for:

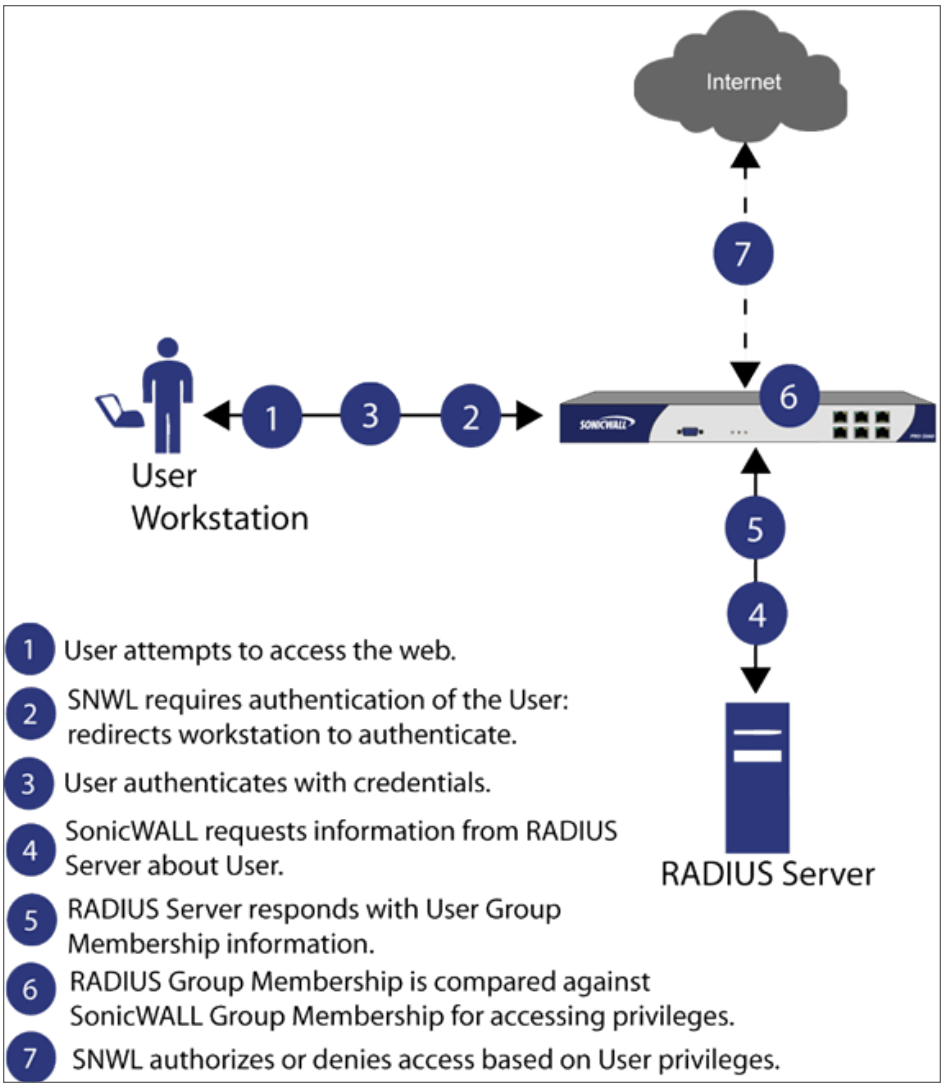
Group membership	Users can belong to one or more local groups. By default, all users belong to the groups **Everyone** and **Trusted Users**. You can remove these group memberships for a user and can add memberships in other groups.
VPN access	You can configure the networks that are accessible to a VPN client initiated by a user. When setting up VPN access, you can select from a list of networks designated by their Address Group or Address Object names. **NOTE:** The VPN access configuration for users and groups affects the ability of remote clients using GVC, NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the corresponding network address objects or groups must be added to the “allow” list on the VPN Access tab.

You can also add or edit local groups. Below are the configurable settings for these groups:

Group settings	For administrator groups, you can configure SonicOS to allow login to the Management Interface without displaying the login status popup window.
Group members	Groups can consist of members who are either local users or other local groups.
VPN access	VPN access for groups is configured in the same way as VPN access for users. You can configure the networks that are accessible to a VPN client initiated by a member of this group. When configuring VPN access settings, you can select from a list of networks, which are designated by their Address Group or Address Object names.
CFS policy	You can apply a content filtering (CFS) policy to group members. The CFS policy setting is only available if the firewall is currently licensed for the Premium Content Filtering Service.

Using RADIUS for Authentication

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting for SonicWall security appliances and SonicWave appliances, allowing them to authenticate users attempting to access the network. The RADIUS server contains a database with user information and checks a user's credentials using authentication schemes such as Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP), or MS-CHAPv2. See Using RADIUS for authentication. For SonicWave appliances providing RADIUS authentication, see SonicOS 8 SSL VPN Administration Guide.



While RADIUS is very different from LDAP, primarily providing secure authentication, it can also supply numerous attributes for each entry. These attributes include several that can be used to convey user group memberships. RADIUS can store information for thousands of users and is a good choice for user authentication purposes when many users need access to the network.

Using LDAP/Active Directory/eDirectory Authentication

Lightweight Directory Access Protocol (LDAP) defines a directory service structure for storing and managing information about elements in your network, such as user accounts, user groups, hosts, and servers. Several different standards exist that use LDAP to manage user accounts, groups, and permissions. Some are

proprietary systems, like Microsoft Active Directory (AD), which can be managed using LDAP, or Novell eDirectory, which provides an LDAP API for managing user repository information. Others are open standards, like SAMBA, which implements LDAP standards.

In addition to RADIUS and the local user database, SonicOS supports LDAP for user authentication. It is compatible with various schemas, including Microsoft Active Directory, Novell eDirectory, and a fully configurable user-defined option that allows SonicOS to interact with any schema.

Microsoft Active Directory also works with SonicWall Single Sign-On and the SonicWall SSO Agent. For more information, see What is Single Sign-On?

Topics:

LDAP Terms

- **Active Directory (AD)**:The Microsoft directory service is commonly used with Windows-based networking. Microsoft Active Directory is compatible with LDAP.
- **Attribute**: A data item stored in an object in an LDAP directory. An object can have required attributes or allowed attributes. For example, the "dc" attribute is a required attribute of the "dcObject" (domain component) object.
- **cn**: The common name attribute is a required component of many object classes within LDAP.
- **dc**: The domain component attribute is commonly found at the root of a distinguished name and is often a required attribute.
- **dn**: A distinguished name is a globally unique identifier for a user or other object. It is composed of several components, usually starting with a common name (cn) component and ending with a domain specified by two or more domain components (dc). For example cn=john,cn=users,dc=domain,dc=com.
- **eDirectory**:The Novell directory service is used for Novell NetWare-based networking. Novell eDirectory features an LDAP gateway that can be utilized for management.
- **Entry**: The data that is stored in the LDAP directory. Entries are stored in `attribute/value` (or `name/value`) pairs, where the attributes are defined by object classes. A sample entry would be `cn=john` where `cn` (common name) is the attribute, and `john` is the value.
- **Object**: In LDAP terminology, the entries in a directory are referred to as objects. For the purposes of the GMS implementation of the LDAP client, the critical objects are User and Group objects. Different implementations of LDAP can refer to these object classes in different ways. For example, Active Directory refers to the user object as "user" and the group object as "group," while RFC2798 refers to the user object as "inetOrgPerson" and the group object as "groupOfNames."
- **Object class**: Object classes specify the types of entries that an LDAP directory can contain. Examples of object classes used by Active Directory include user and group.
- **ou**: The organizational unit attribute is a required component of most LDAP schema implementations.

- **Schema**: The schema is the set of rules or structure that defines the types of data that can be stored in a directory and how that data can be organized. Data is stored in the form of entries.
- **TLS**: Transport Layer Security (TLS) is the IETF-standardized version of SSL (Secure Sockets Layer). TLS 1.0 is the successor to SSL 3.0, and TLS 1.1 and 1.2 are later versions.

LDAP Directory Services Supported in SonicOS

To integrate with the most common directory services used in company networks, SonicOS supports integration with the following LDAP schemas:

- Microsoft Active Directory
- RFC2798 InetOrgPerson
- RFC2307 Network Information Service
- Samba SMB
- Novell eDirectory
- User-defined schemas

SonicOS provides support for directory servers running the following protocols:

- LDAPv2 (RFC3494)
- LDAPv3 (RFC2251-2256, RFC3377)
- LDAPv3 over TLS (RFC2830)
- LDAPv3 with STARTTLS (RFC2830)
- LDAP Referrals (RFC2251)

Integrating LDAP into the SonicOS Network Security Appliance

Integrating your network security appliance with an LDAP directory service requires configuring your LDAP server for certificate management, installing the correct certificate on your firewall, and configuring the firewall to use the information from the LDAP Server. For an introduction to LDAP, see Using LDAP/Active Directory/eDirectory Authentication.

Topics:

- Preparing Your LDAP Server for Integration
- Configuring the CA on the Active Directory Server
- Exporting the CA Certificate from the Active Directory Server
- Importing the CA Certificate into SonicOS

Preparing Your LDAP Server for Integration

Before beginning your LDAP configuration, you should prepare your LDAP server and your SonicWall network security appliance for LDAP over TLS support.This requires:

- Installing a server certificate on your LDAP server.
- Installing a CA (Certificate Authority) certificate for the issuing CA on your firewall.

The following procedures describe how to perform these tasks in an Active Directory environment.

Topics:

Configuring the CA on the Active Directory Server

To configure the CA on the Active Directory server:

ⓘ | **TIP:** Skip the first five steps if Certificate Services are already installed.

1. Navigate to **Start > Settings > Control Panel > Add/Remove Programs**.
2. Select **Add/Remove Windows Components**.
3. Select **Certificate Services**.
4. When prompted, **Select Enterprise Root CA**.
5. Enter the requested information.

   ⓘ | **NOTE:** For information about certificates on Windows systems, see http://support.microsoft.com/kb/931125.
6. Launch the **Domain Security Policy** application by
   a. Navigate to **Start > Run**.
   b. Run the command: `dompol.msc`.
7. Open **Security Settings > Public Key Policies**.
8. Right click **Automatic Certificate Request Settings**.
9. Select **New > Automatic Certificate Request**.
10. Step through the wizard, and select **Domain Controller** from the list.

Exporting the CA Certificate from the Active Directory Server

To export the CA certificate from the AD server:

1. Launch the **Certification Authority** application:
2. a. Navigate to **Start > Run**.
   b. Run the command: `certsrv.msc`.
3. Right click on the CA you created, and select **properties**.
4. On the **General** tab, click **View Certificate**.
5. On the **Details** tab, select **Copy to File**.
6. Step through the wizard, and select the **Base-64 Encoded X.509 (.cer)** format.
7. Specify a path and filename to which to save the certificate.

Importing the CA Certificate into SonicOS

To import the CA certificate in to SonicOS:

1. Navigate to **Device > Certificates**.
2. Click **Import**.
3. Select **Import a CA certificate** option.
4. Click Add File and browse to and select the certificate file you just exported.
5. Click **Import**.

Using RADIUS

SonicOS supports Remote Authentication Dial In User Service (RADIUS). RADIUS is a protocol for carrying information related to authentication, authorization, and configuration between a Network Access Server (NAS) that seeks to authenticate its links and a shared Authentication Server.

The main characteristics of RADIUS are:

- RADIUS is an AAA protocol for applications such as Network Access or IP Mobility.
- Uses PAP, CHAP or EAP protocols to authenticate users.
- Look in text file, LDAP Servers, Database for authentication.
- After authentication services parameters passed back to NAS.

Using TACACS+

SonicOS supports Terminal Access Controller Access-Control System latest generation (TACACS+) for user authentication. The main characteristics of TACACS+ are:

- Provides separate authentication, authorization and accounting (AAA) services.
- Uses TCP for its transport.
- Entire TACACS+ body might be protected by the encryption.

Using Single Sign-On

Topics:

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 domain login to a workstation or through Windows Terminal Services or a Citrix server.

SonicWall SonicWall network security appliances provide Single Sign-On (SSO) functionality using the Single Sign-On Agent (SSO Agent) and the SonicWall Terminal Services Agent (TSA) to identify user activity. The SSO Agent identifies users based on their workstation IP address, while the TSA identifies users through a combination of server IP address, username, and domain..

SonicWall SSO is also available for Mac and Linux users when used with Samba. Additionally, browser NTLM authentication allows SonicWall SSO to authenticate users who send HTTP traffic without involving the SSO Agent or Samba.

SonicWall SSO is configured in the **Device > Users > Settings** page of the SonicWall 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.

Based on data from SonicWall SSO Agent or TSA, the 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 Control to control what they are allowed to access. User names learned UNIX SSO are reported in logs of traffic and events from the users, and in AppFlow Monitoring.

The configured inactivity timer applies with SSO, but the session limit does not. However, 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, are not authenticated unless they send HTTP traffic and browser NTLM authentication is enabled. (However, they can optionally be authenticated for limited access.) For users who are not authenticated by SonicWall SSO, a message will display indicating that a manual login to the Security Appliance is required for further authentication.

Users who are identified but lack the necessary group memberships required by the configured policy rules will be redirected to the **Access Barred** page.

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 Single Sign-On (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 Directory Connector-compatible protocol.

SonicWall SSO works for any service on the firewall that uses user-level authentication, including the Content Filtering Service (CFS), access rules, group membership and inheritance, and security services such as IPS, GAV, and Anti-Spyware inclusion/exclusion lists.

SonicWall SSO Agent can be installed on any Windows server on the LAN, and the TSA can be installed on any terminal server.

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 into the appliance using a Web browser.
Transparency to users	Users are not required to re-enter username and password for authentication.
Secure communication	Shared key encryption for data transmission protection.
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 model of the SonicWall Security Appliance and ranges from 8 to 512.
Login mechanism	Works with any protocol, not just HTTP.
Browser NTLM authentication	SonicWall SSO can authenticate users sending HTTP traffic without using the SSO Agent.
MacOS and Linux support	With Samba 3.5 and higher, SonicWall SSO is supported for Mac and Linux users.
Per-zone enforcement	SonicWall SSO can be triggered for traffic from any zone even when not automatically initiated by firewall access rules or security services policies, providing user identification in event logging or AppFlow Monitoring.

Platforms and Supported Standards

The SSO Agent is compatible with all versions of SonicOS that support SonicWall SSO. SonicWall TSA also is supported.

The SSO feature supports LDAP and local database protocols. SonicWall SSO supports SonicWall Directory Connector. For all features of SonicWall SSO to work properly, SonicOS should be used with Directory Connector 3.1.7 or higher.

To use SonicWall SSO with Windows Terminal Services or Citrix, SonicOS 6.0 or higher is required, and SonicWall TSA must be installed on the server.

To use SonicWall SSO with browser NTLM authentication, SonicOS 6.0 or higher is required. The SSO Agent is not required for browser NTLM authentication.

Except when using only browser NTLM authentication, using SonicWall SSO requires that the 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 TSA be installed on any terminal servers in the domain.

The following requirements must be met 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
- .NET Framework 2.0
- Net API or WMI

NOTE: Mac and Linux PCs do not support the Windows networking requests that are used by the SSO Agent, and hence require Samba 3.5 or newer to work with SonicWall SSO. Without Samba, Mac and Linux users can still get access, but you need to log in to do so. You can be redirected to the login prompt if policy rules are set to require authentication. For more information, see Accommodating Mac and Linux Users.

To run the TSA, the following requirements must be met:

- 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 Terminal Services or Citrix installed on the Windows Terminal Server system(s)

How Does Single Sign-On Work?

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

SSO is triggered in these situations:

- If firewall access rules requiring user authentication apply to traffic that is not incoming from the WAN zone
- When no user groups are specified in access rules, but any of the following conditions exist, SSO is triggered for all traffic on the zone and not just for traffic subject to these conditions:
    - CFS is enabled on the zone and multiple CFS policies are set
    - IPS is enabled on the zone and there are IPS policies that require authentication
    - Anti-Spyware is enabled on the zone and there are Anti-Spyware policies that require authentication
    - Application Control policies that require authentication apply to the source zone
    - Per-zone enforcement of SSO is set for the zone

The SSO user table is also used for user and group identification needed by security services, including Content Filtering, Intrusion Prevention, Anti-Spyware, and Application Control.

Topics:

- SonicWall SSO Authentication Using the SSO Agent
- SonicWall SSO Authentication Using the Terminal Services Agent
- SonicWall SSO Authentication Using Browser NTLM Authentication

SonicWall SSO Authentication Using the SSO Agent

For users on individual Windows workstations, the SSO Agent (on the SSO workstation) handles the authentication requests from the firewall. There are six steps involved in SonicWall SSO authentication using the SSO Agent.

The SSO authentication process is initiated when user traffic passes through a firewall. For example, when a user accesses the Internet. The sent packets are temporarily blocked and saved while the firewall sends a “User Name” request and workstation IP address to the authorization agent running the SSO Agent (the SSO workstation).

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

SonicWall SSO Authentication Using the Terminal Services Agent

For users logged in from a Terminal Services or Citrix server, the 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 firewall.
- 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 SonicOS when the user logs out, so no polling occurs.

After a user has been identified, the 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 is 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 firewall local user database to match).
- 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 is 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` is 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 is 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 is made from the top of the directory tree.

When 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 is deleted and another search for the domain object is made.

User logout is handled slightly differently by SonicWall SSO using the SSO Agent as compared to SSO with TSA. The network 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 firewall, confirming that the user has been logged out and terminating the SSO session. Rather than being polled by the network security appliance, the TSA itself monitors the Terminal Services/Citrix server for logout events and notifies the network security 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).

SonicWall SSO Authentication Using Browser NTLM Authentication

For users who are browsing using Mozilla-based browsers (including Internet Explorer, Firefox, Chrome, and Safari) the firewall supports identifying them through NTLM (NT LAN Manager) authentication. NTLM is part of a browser authentication suite known as “Integrated Windows Security” and is supported by all Mozilla-based browsers. NTLM allows a direct authentication request from the appliance to the browser without involving the SSO agent. NTLM is often used when a domain controller is not available, such as when the user is remotely authenticating over the Web.

NTLM Authentication is currently available for HTTP; it is not available for use with HTTPS traffic.

Browser NTLM authentication can be tried before or after the SSO agent attempts to acquire the user information. For example, if the SSO agent is tried first and fails to identify the user, then, if the traffic is HTTP, NTLM is tried.

To use this method with Linux or Mac clients as well as Windows clients, you can also enable SSO to probe the client for either **NetAPI** or **WMI**, depending on which is configured for the SSO Agent. This causes the firewall 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 fail SSO immediately. For a:

- Windows PC, the probe generally works (unless blocked by a personal firewall) and the SSO agent is used.
- Linux/Mac PC (assuming it is not set up to run Samba server), the probe fails, the SSO agent is bypassed, and NTLM authentication is used when HTTP traffic is sent.

NTLM cannot identify the user until they browse with HTTP, so any traffic sent before that is treated as unidentified. The default CFS policy is applied, and any rule requiring authenticated users does not allow the traffic to pass.

If NTLM is configured to be used before the SSO agent, then if HTTP traffic is received first, the user is authenticated with NTLM. If non-HTTP traffic is received first, the SSO agent is used for authentication.

How Does SSO Agent Work?

The SSO Agent can be installed on any workstation or server with a Windows domain that can communicate with clients and the firewall directly using the IP address or using a path, such as VPN. It is recommended, however, that the SSO Agent be installed on separate, standalone workstations or servers. For installation instructions for the SSO Agent, see Installing the SonicWall SSO Agent.

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: When using NetAPI or WMI, one SSO Agent can support up to approximately 2500 users, depending on the performance level of the hardware that it is running on, how it is configured on the firewall, and other network-dependent factors. Depending on similar factors, when configured to read from domain controller security logs, one SSO Agent can support a much larger number of users identified through that mechanism, potentially up to 50,000+ users

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

NOTE: The shared key is generated in the SSO Agent and the key entered in the firewall during SSO configuration must match the SSO Agent-generated key exactly.

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

Topics:

Logging

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

The network security appliance also logs SSO Agent-specific events in its event log:

The Notes field of log messages specific to the SSO Agent contain the text `<domain/user-name>`, authentication by SSO Agent. For more information about log messages, see *SonicOS 7 Users*.

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

How Does Terminal Services Agent Work?

The 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 firewall directly using the IP address or using a path, such as VPN.

For installation instructions for the TSA, refer to Installing the SonicWall Terminal Services Agent.

Topics:

Multiple TSA Support

To accommodate large installations with thousands of users, firewalls 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 Multiple TSA Support per Model table.

MULTIPLE TSA SUPPORT PER MODEL

SonicWall Model	TS Agents Supported
NSA 6600	256
NSA 5600	128
NSA 4600	64
NSA 3600	16
NSA 2600	8
TZ 600	4
TZ 500	4
TZ 400	4
TZ 300	4

For all SonicWall network security appliances, a maximum of 32 IP addresses is supported per terminal server, where the server might have multiple NICs (network interface controllers). There is no limit on users per terminal server.

Encryption of TSA Messages and Use of Session IDs

The TSA uses a shared key for encryption of messages between the TSA and the firewall 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 firewall 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, after being learned, it does 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 network security appliance has the **Allow limited access for non-domain users** setting for optionally giving limited access to non-domain users (those logged into their local machine and not into the domain), and this works for terminal services users as it does for other SSO users.

If your network includes non-Windows devices or Windows computers with personal firewalls running, select **Probe user for** and choose the radio button for either **NetAPI** or **WMI** depending on which is configured for the SSO Agent. This causes the firewall 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 fail SSO immediately. Such devices do not respond to, or could block, the Windows networking messages used by the SSO Agent to identify a user.

How Does Browser NTLM Authentication Work?

Topics:

NTLM Authentication of Domain Users

For domain users, the NTLM response is authenticated through the MSCHAP mechanism in RADIUS. RADIUS must be enabled on the appliance. For more information about NTLM authentication, refer to NTLM.

NTLM Authentication of Non-Domain Users

With NTLM, non-domain users could be users who are logged into their PC rather than into the domain, or could be users who were prompted to enter a user name and password and entered something other than their domain credentials. In both cases, NTLM allows for distinguishing these from domain users.

If the user name matches a local user account on the firewall, then the NTLM response is validated locally against the password of that account. If successful, the user is logged in and given privileges based on that account. User group memberships are set from the local account, not from LDAP, and (as the password has been validated locally) include membership of the Trusted Users group.

If the user name does not match a local user account, the user is not logged in. The **Allow limited access for non-domain users** option does not apply for users authenticated through NTLM.

Credentials for NTLM Authentication in the Browser

For NTLM authentication, the browser either uses the domain credentials (if the user is logged into the domain), thus providing full single-sign-on functionality, or prompts the user to enter a name and password for the website being accessed (the firewall in this case). Different factors affect the browser's ability to use the domain credentials when the user is logged into the domain. These factors depend on the type of browser being used:

Internet Explorer (9.0 or above)	Uses the user's domain credentials and authenticates transparently if the website that it is logging into the firewall (the SonicWall Security Appliance) is in the local intranet, according to the Security tab in its Internet Options. This requires adding the firewall to the list of websites in the Local Intranet zone in the Internet Options. This can be done through the domain's group policy in the Site to Zone Assignment List under Computer Configuration, Administrative Templates, Windows Components, Internet Explorer, Internet Control Panel, Security Page.
Google Chrome	Behaves the same as Internet Explorer, including requiring that the firewall be added to the list of websites in the Local Intranet zone in the Internet Options.
Firefox	Uses the user's domain credentials and authenticates transparently if the website that it is logging into the firewall is listed in the `network.automatic-ntlm-auth.trusted-uris` entry in its configuration (accessed by entering `about:config` in the Firefox address bar)
Safari	Although Safari does support NTLM, it does not currently support fully transparent log on using the user's domain credentials. **NOTE:** Safari does not operate on Windows platforms.
Browsers on Non-PC Platforms	Non-PC platforms, such as Linux and Mac, can access resources in a Windows domain through Samba, but do not have the concept of "logging the PC into the domain" as Windows PCs do. Hence, browsers on these platforms do not have access to the user's domain credentials and cannot use them for NTLM.

When a user is not logged into the domain or the browser cannot use their domain credentials, it prompts for a name and password to be entered, or uses cached credentials if the user has previously opted to have it save them.

In all cases, should authentication fail when using the user's domain credentials (which could be because the user does not have the privileges necessary to get access), then the browser prompts the user to enter a name and password. This allows the user to enter credentials different from the domain credentials to get access.

NOTE: When NTLM is enabled for Single Sign-On enforcement, an HTTP/HTTPS access rule with Trusted Users as Users Allowed must be added to the LAN to WAN rules in the **MANAGE | Policies > Rules > Access Rules** page (for more information, see *SonicOS 7 Rules and Policies*). This rule triggers an NTLM authentication request to the user. Without the access rule, other configurations, such as restrictive Content Filter policies, might block the user from Internet access and prevent the authentication request.

How Does RADIUS Accounting for Single-Sign-On Work?

RADIUS Accounting is specified by RFC 2866 as a mechanism for a network access server (NAS) to send user login session accounting messages to an accounting server. These messages are sent at user login and logoff. Optionally, they can also be sent periodically during the user's session.

When a customer uses an external or third-party network access appliance to perform user authentication (typically for remote or wireless access) and the appliance supports RADIUS accounting, a SonicWall network security appliance can act as the RADIUS Accounting Server, and can use RADIUS Accounting messages sent from the customer's network access server for single sign-on (SSO) in the network.

NOTE: A SonicWallSMA 1000 Series appliance running SMA 12 or higher can be configured as an external RADIUS Accounting client, with the SonicWall network security appliance as the RADIUS Accounting server.

When a remote user connects through a SonicWall Secure Mobile Access or third-party appliance, the SMA or third-party appliance sends an accounting message to the SonicWall network security appliance (configured as a RADIUS accounting server). The SonicWall network security appliance adds the user to its internal database of logged in users based on the information in the accounting message.

When the user logs out, the SonicWall SMA or third-party appliance sends another accounting message to the SonicWall network security appliance, which then logs the user out.

NOTE: When a network access server (NAS) sends RADIUS accounting messages, it does not require the user to be authenticated by RADIUS. The NAS can send RADIUS accounting messages even when the third-party appliance is using LDAP, its local database, or any other mechanism to authenticate users.

RADIUS accounting messages are not encrypted. RADIUS accounting is inherently secure against spoofing because it uses a request authenticator and a shared secret. RADIUS accounting requires that a list of the network access servers (NASs), that can send RADIUS Accounting messages, be configured on the appliance. This configuration supplies the IP address and shared secret for each NAS.

Topics:

RADIUS Accounting Messages

RADIUS accounting uses two types of accounting messages:

- **Accounting-Request**
- **Accounting-Response**

An **Accounting-Request** can send one of three request types specified by the **Status-Type** attribute:

This request	Is sent
Start	When a user logs in.
Stop	When a user logs out.
Interim-Update	Periodically during a user login session.

Accounting messages follow the RADIUS standard specified by RFC 2866. Each message contains a list of attributes and an authenticator that is validated by a shared secret.

These SSO-relevant attributes are set in **Accounting-Requests**:

Status-Type	Type of accounting request (**Start**, **Stop**, or **Interim-Update**)
User-Name	User's login name. The format is not specified by the RFC and can be a simple login name or a string with various values such as login name, domain, or distinguished name (DN).
Framed-IP-Address	User's IP address. If NAT is used, this must be the user's internal IP address.
Calling-Station-ID	String representation of the user's IP address, used by some appliances such as SMA.
Proxy-State	Pass-though state used for forwarding requests to another RADIUS accounting server.

SonicWall Compatibility with Third-Party Network Appliances

For SonicWall network security appliances to be compatible with third-party network appliances for SSO through RADIUS Accounting, the third-party appliance must be able to:

- Support RADIUS Accounting.
- Send both **Start** and **Stop** messages. Sending **Interim-Update** messages is not required.
- Send the user's IP address in either the **Framed-IP-Address** or **Calling-Station-Id** attribute in both **Start** and **Stop** messages.

NOTE: In the case of a remote access server using NAT to translate a user's external public IP address, the attribute must provide the internal IP address that is used on the internal network, and it must be a unique IP address for the user. If both attributes are being used, the **Framed-IP-Address** attribute must use the internal IP address, and the **Calling-Station-Id** attribute should use the external IP address.

The user's login name should be sent in the **User-Name** attribute of **Start** messages and **Interim-Update** messages. The user's login name can also be sent in the **User-Name** attribute of **Stop** messages, but is not required. The **User-Name** attribute must contain the user's account name and might include the domain also, or it must contain the user's distinguished name (DN).

Proxy Forwarding

A SonicWall network security appliance acting as a RADIUS accounting server can proxy-forward requests to up to four other RADIUS accounting servers for each network access server (NAS). Each RADIUS accounting server is separately configurable for each NAS.

To avoid the need to re-enter the configuration details for each NAS, SonicOS allows you to select the forwarding for each NAS from a list of configured servers.

The proxy forwarding configuration for each NAS client includes timeouts and retries. How to forward requests to two or more servers can be configured by selecting these options:

- **try the next server on a timeout**
- **forward each request to all the servers**

Non-Domain Users

Users reported to a RADIUS accounting server are determined to be local (non-domain) users in these cases:

- The user name was sent without a domain, and it is not configured to look up domains for the server through LDAP.
- The user name was sent without a domain, and it is configured to look up domains for the server through LDAP, but the user name was not found.
- The user name was sent with a domain, but the domain was not found in the LDAP database.
- The user name was sent with a domain, but the user name was not found in the LDAP database.

A non-domain user authenticated by RADIUS accounting is subject to the same constraints as one authenticated by the other SSO mechanisms, and the following restrictions apply:

- The user is logged in only if **Allow limited access for non-domain users** is set.
- The user is not made a member of the Trusted Users group.

IPv6 Considerations

In RADIUS accounting, these attributes are used to contain the user's IPv6 address:

- Framed-Interface-Id / Framed-IPv6-Prefix
- Framed-IPv6-Address

Currently, all these IPv6 attributes are ignored.

Some devices pass the IPv6 address as text in the **Calling-Station-ID** attribute.

The **Calling-Station-ID** is also ignored if it does not contain a valid IPv4 address.

RADIUS accounting messages that contain an IPv6 address attribute and no IPv4 address attribute are forwarded to the proxy server. If no proxy server is configured, IPv6 attributes discarded.

RADIUS Accounting Server Port

RADIUS accounting normally uses UDP port:

1813	IANA-specified port. The SonicWall network security appliance listens on port 1813 by default.
1646	An older, unofficial, standard port.

Other port numbers can be configured for the RADIUS accounting port, but the SonicWall Security Appliance can listen on only one port. So, if you are using multiple network access servers (NASs), they must all be configured to communicate on the same port number.

Installing the Single Sign-On Agent and/or Terminal Services Agent

Configuring SSO is a process that includes installing and configuring the SonicWall SSO Agent and/or the SonicWall Terminal Services Agent (TSA), and configuring a network security appliance running SonicOS to use the SSO Agent or TSA. For an introduction to SonicWall SSO, refer to Using Single Sign-On.

Topics:

- Installing the SonicWall SSO Agent
- Installing the SonicWall Terminal Services Agent

Installing the SonicWall SSO Agent

The SonicWall SSO Agent is part of the SonicWall Directory Connector. The SonicWall SSO Agent must be installed on at least one, and up to eight, workstations or servers in the Windows domain that have access to the Active Directory server using VPN or IP. It is recommended that these workstations or servers be separate, standalone workstations or servers. The SonicWall SSO Agent must have access to your firewall.

To install the SonicWall SSO Agent, see the procedure in Directory Services Connector .

Installing the SonicWall Terminal Services Agent

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

SonicWall TSA is available for download without charge from MySonicWall.

For instructions on installing the SonicWall TSA, see Directory Services Connector.

Topics:

- Accessing the SonicWall Terminal Services Agent
- Creating a SonicWall TSA Troubleshooting Report

Accessing 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 troubleshooting report (TSR), or to see the status and version information.

For more information, refer to the Directory Services Connector.

Creating a SonicWall TSA Troubleshooting Report

You can create a troubleshooting 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.

To create a TSR for the SonicWall TSA:

1. Double-click the SonicWall TSA desktop icon. The **SonicWall Terminal Services Agent** window displays.
2. Click the **Reports** tab.
3. To generate the TSR and:
    - automatically email it to SonicWall Technical Support, click **Send**.
    - examine it in your default text editor, click **View**.
    - save it as a text file, click **Save As**.
4. When finished, click **Close**.

Single Sign-On Advanced Features

The maximum requests to send at a time setting is available when configuring SSO agents. For more information about configuring SSO agents, see SSO Agents.

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 and Viewing SSO Mouseover Statistics). 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.

Topics:

Viewing SSO Mouseover Statistics

The **SSO Authentication Configuration** dialog provides mouseover statistics about each agent and for all SSO agents.

On the **SSO Agents** page:

- a green LED-style icon next to an agent indicates the agent is up and running.
- a red LED-style icon indicates the agent is down.

To view the statistics for:

- A particular agent, hover your mouse over the **Statistics** icon for the SSO agent.
- All SSO agents, hover your mouse over the **Statistics** icon under the table.

  ⓘ | **TIP:** This also works for individual TSAs on **Terminal Services**.

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

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

Using the Single Sign-On Statistics in the TSR

The Tech Support Report (TSR) includes a rich set of SSO performance and error statistics. These can be used to gauge how well SSO is performing in your installation.

To view the Tech Support Report:

1. Navigate to the **Device > Diagnostics > Tech Support Report** page.
2. Click **Download Tech Support Report**.
3. Search for the title, **SSO operation statistics**.
4. Download and open the report.

Here are the counters to look at in particular:

- 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 increases the load on the agent, and if the agent cannot handle the additional load, then problems result, in which case it might be necessary to consider moving the agent to a more powerful PC or adding additional agents.
- 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.
- 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 do 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.
- 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 through 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.
- 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.
- 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 traffic from** setting on the **Enforcement** tab of the **SSO configuration** dialog.
- 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 are Mac/Linux PCs, see Accommodating Mac and Linux Users.

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

Examining the Agent

If the statistics in the TSR report 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. For more information, refer to Using the Single Sign-On Statistics in the TSR.

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 in the **Users** section of the **SSO Authentication** dialog by increasing the poll time. This reduces the load on the agent, at the cost of detecting logouts less quickly.

  NOTE: 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 Access Rules

Access rules provide you with the ability to control user access. Rules set from the **Policies > Rules > Access Rules** page 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 Security Appliance. The **Rules > Access Rules** page provides a sortable access rule management interface.

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, the firewall'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.

CAUTION: 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 access rules, refer to SonicOS 8 Rules and Policies Administration Guide for Classic Mode.

Topics:

- Automatically Generated Rules for SonicWall SSO
- Accommodating Mac and Linux Users
- Allowing ICMP Pings from a Terminal Server

Automatically Generated Rules for SonicWall SSO

When a SonicWall SSO agent or TSA is configured in the SonicOS Management Interface, an 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 through DNS (where an agent is given by DNS name).

If SonicWall SSO agents or TSAs are configured in different zones, the 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.

NOTE: Do not enable Guest Services in the same zone where SonicWall SSO is being used. Enabling Guest Services disables SSO in that zone, causing users who have authenticated through SSO to lose access. Create a separate zone for Guest Services.

Accommodating Mac and Linux Users

Mac and Linux systems do not support the Windows networking requests that are used by the SonicWall SSO agent, but can use Samba 3.5 or newer to work with SonicWall SSO.

Topics:

- Using SSO on Mac and Linux With Samba
- Using SSO on Mac and Linux Without Samba

Using SSO on Mac and Linux With Samba

ⓘ | **NOTE:** SonicWall SSO is supported by Samba 3.5 or newer.

For Windows users, SonicWall SSO is used by a network security appliance to automatically authenticate users in a Windows domain. It allows the users to get access through the network security appliance with correct filtering and policy compliance without the need to identify themselves through any additional login process after their Windows domain login.

Samba is a software package used by Linux/UNIX or Mac machines to give their users access to resources in a Windows domain (through Samba's `smbclient` utility) and/or to give Windows domain users access to resources on the Linux or Mac machine (through a Samba server).

A user working on a Linux PC or Mac with Samba in a Windows domain can be identified by SonicWall SSO, but it requires proper configuration of the Linux/Mac machine, the SSO Agent, and possibly some reconfiguration of the appliance. For example, the following configuration is necessary:

- To use SonicWall SSO with Linux/Mac users, the SonicWall SSO Agent must be configured to use **NetAPI** rather than **WMI** to get the user login information from the user's machine.
- For Samba to receive and respond to the requests from the SonicWall SSO Agent, it must be set up as a member of the domain and the Samba server must be running and properly configured to use domain authentication.

ⓘ | **NOTE:** If multiple users log into a Linux PC, access to traffic from that PC is granted based on the most recent login.

Using SSO on Mac and Linux Without Samba

Without Samba, Mac and Linux users can still get access, but you need to log in to the firewall to do so. 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 is 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 are redirected to the login page after the SSO failure, but the failure might 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** option is available when configuring access rules on the **Policies > Rules > Access Rules** page (for more information about configuring access rules, refer to SonicOS 8 Rules and Policies Administration Guide for Classic Mode). This option is visible

only when SonicWall SSO is enabled. If this option is selected, SSO is not attempted for traffic that matches the rule, and unauthenticated HTTP connections that match it are directed straight to the login page. Typically, the **Source** drop-down menu would be set to an address object containing the IP addresses of Mac and Linux systems.

In the case of Content Filtering Service (CFS), a rule with this option 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 could 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 through a socket, so they are not seen by the TSA, and hence the network security appliance receives 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.

Managing SonicOS with HTTP Login from a Terminal Server

The SonicWall network security appliance normally grants access through policies based on authentication credentials supplied through an 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 network security appliance based on credentials supplied through an 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 fails 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 network security appliance as an entirely separate login session.
- Only one user at a time can manage the network security 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 sees 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 and Managing SSO User Sessions

Topics:

Logging Out SSO Users

The **Current Status > User Sessions > Active Users** page displays user sessions on the network security appliance. For information about viewing the user's settings and how to log out users, refer to SonicOS 8 Users Administration Guide

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

Configuring Additional SSO User Settings

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

The options to limit user sessions under **User Session** apply to users logged in using SSO. SSO users are logged out according to session limit settings, but are 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 are not reflected during that session.

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

Viewing SSO and LDAP Messages with Packet Monitor

The **Packet Monitor** feature available on **Tools > Packet Monitor** provides options to enable capture of decrypted messages to and from the SSO agent, and decrypted LDAP over TLS (LDAPS) messages. For further information, refer to SonicOS 8 Diagnostic Administration Guide for Classic Mode

Capturing SSO Messages

For further information about using the Packet Monitor, refer to SonicOS 8 Diagnostic Administration Guide for Classic Mode.

To capture decrypted messages to or from the SSO authentication agent:

1. Navigate to **Tools > Packet Monitor**.
2. In the **Hex Dump** section, click **Configure**. The **Packet Monitor Configuration** dialog displays.
3. Click **Advanced Monitor Filter**.
4. Select **Monitor intermediate Packets**.
5. Select **Monitor intermediate decrypted Single Sign On agent messages**.
6. Click **OK**.

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

This enables decrypted SSO packets to be fed to the Packet Monitor, but any monitor filters are still applied to them.

Captured SSO messages are displayed fully decoded on the **Tools > Packet Monitor** page.

Capturing LDAP Over TLS Messages

To capture decrypted LDAP over TLS (LDAPS) packets:

1. Navigate to **Tools > Packet Monitor**.
2. In the **Hex Dump** section, click **Configure**. The **Packet Monitor Configuration** dialog displays.
3. Click **Advanced Monitor Filter**.
4. Select **Monitor intermediate Packets**.
5. Select **Monitor intermediate decrypted LDAP over TLS packets**.
6. Click **OK**.

The packets are marked with **(ldp)** in the **ingress/egress interface** field. They have dummy Ethernet, TCP, and IP headers, so some values in these fields might not be correct. The LDAP server port is set to 389 so that an external capture analysis program (such as Wireshark) knows to decode these packets as LDAP. Passwords in

captured LDAP bind requests are 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 enables decrypted LDAPS packets to be fed to the packet monitor, but any monitor filters are still applied to them.

NOTE: LDAPS capture only works for connections from the firewall's LDAP client, and does not display LDAP over TLS connections from an external LDAP client that pass through the firewall.

Multiple Administrator Support

To configure multiple administrator profiles, refer to Configuring Local Users and Groups.

When using RADIUS or LDAP authentication, if you want to ensure that some or all administrative users are always able to manage the appliance, even when the RADIUS or LDAP server becomes unreachable, then you can use the **RADIUS + Local Users or LDAP + Local Users** option and configure the accounts for those particular users locally.

For users authenticated by RADIUS or LDAP, create user groups named SonicWall Administrators and/or SonicWall Read-Only Admins on the RADIUS or LDAP server (or its back-end) and assign the relevant users to those groups.

For RADIUS, you probably need a special configuration of the RADIUS server to return the user group information.

Topics:

- Preempting Administrators
- Logging in with Administrator Rights

Preempting Administrators

When an administrator attempts to log in while another administrator is logged in, a message is displayed that provides you with these options:

Config	Preempts the current administrator. The current administrator is dropped to non-config mode and you are given full administrator access.
Non-config	You are logged into the network security appliance in non-config mode. The current administrator's session is not disturbed.
do not begin management	Returns to the login screen.

Logging in with Administrator Rights

A user other than **admin** (that is, not the **admin** user) can log in with administrator rights.

To log in with Administrator rights:

1. Log in with your administrator credentials. The **User Login Status** message displays.
2. To go to the SonicWall web management interface, click **Manage**. You are prompted to enter your password again. This is a safeguard to protect against unauthorized access when administrators are away from their computers and do not log out of their sessions.
3. To change your password, click **CHANGE PASSWORD**. The dialog for changing your password displays.

Disabling the User Login Status Popup

You can disable the **User Login Status** popup, if you prefer to allow certain users to log in solely for the purpose of managing the network security appliance, rather than for privileged access through the network security appliance.

To disable the popup:

1. Select the **Members go straight to the management UI on web login** option when adding or editing the local group.
2. If you want some user accounts to be administrative only, while other users need to log in for privileged access through the appliance, but also with the ability to administer it (that is, some go straight to the management interface on login, while others get the **User Login Status** popup dialog with a **Manage** button), this can be achieved by:
    a. Creating a local group with the **Members go straight to the management UI on web login** option selected.
    b. Adding the group to the relevant administrative group, but do not select this option in the administrative group.
    c. Adding those user accounts that are to be administrative-only to the new user group. The **User Login Status** popup is disabled for these users.
    d. Adding the user accounts that are to have privileged and administrative access directly to the top-level administrative group.

Configuring Multiple Administrator Support

Topics:

Configuring Additional Administrator User Profiles

Configuring additional administrators is the same as configuring additional local users and then adding them to the proper local group:

This group	Gives the user
Limited Administrators	Limited administrator configuration privileges.
SonicWall Administrators	Full administrator configuration privileges.
SonicWall Read-Only Admins	Viewing privileges only for the entire Management Interface.

For how to configure local users and local groups, refer to Configuring Local Users and Groups.

Configuring Administrators Locally when Using LDAP or RADIUS

When using RADIUS or LDAP authentication, if you want to ensure that some or all administrative users are always able to manage the network security appliance, even if the RADIUS or LDAP server becomes unreachable, then you can use the **RADIUS + Local Users** or **LDAP + Local Users** option and configure the accounts for those particular users locally.

For users authenticated by RADIUS or LDAP, create user groups named **SonicWall Administrators** and/or **SonicWall Read-Only Admins** on the RADIUS or LDAP server (or its back-end) and assign the relevant users to those groups.

NOTE: For RADIUS, you probably need a special configuration of the RADIUS server to return the user group information.

For how to configure administrators when using LDAP or RADIUS, refer to Configuring Local Users and Groups.

Verifying Multiple Administrators Support Configuration

User accounts with administrator and read-only administrators can be viewed on the **Users > Local Users & Groups > Local Groups** page.

You can determine which configuration mode you are in by looking at **Mode** in the top right corner of the web management interface:

Mode: Configuration	When changes are made, the status bar reads: **Status: The configuration has been updated.**
Mode: Non-Config	When changes are attempted, the status bar reads: **Error: Not allowed in current mode**

Viewing Multiple Administrator Related Log Messages

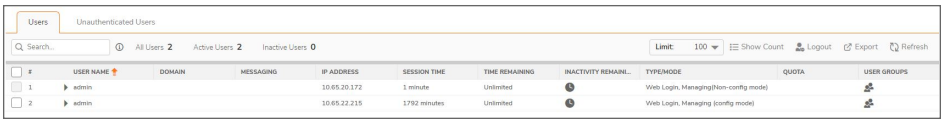
Log messages are generated for these events:

- A GUI or CLI user begins configuration mode (including when an administrator logs in).
- A GUI or CLI user ends configuration mode (including when an administrator logs out).
- A GUI user begins management in non-config mode (including when an administrator logs in and when a user in configuration mode is preempted and dropped back to read-only mode).
- A GUI user begins management in read-only mode.
- A GUI user terminates either of the above management sessions (including when an administrator logs out).

3

Configuring Users Status

The **Device > Users > Status** page displays **All Users**, **Active User Sessions**, and **Inactive Users** on the firewall. The table displays IPv4 and IPv6 IP addresses.



The **Active User Sessions** lists:

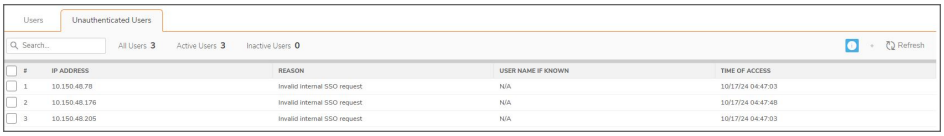
- **User Name**
- **Domain**
- **Messaging**
- **IP Address**
- **Session Time**
- **Time Remaining**
- **Inactivity Remaining**
- **Type/Mode**
- **Quota**
- **User Groups**

Topics:

Displaying Unauthenticated Users

To display unauthenticated users:

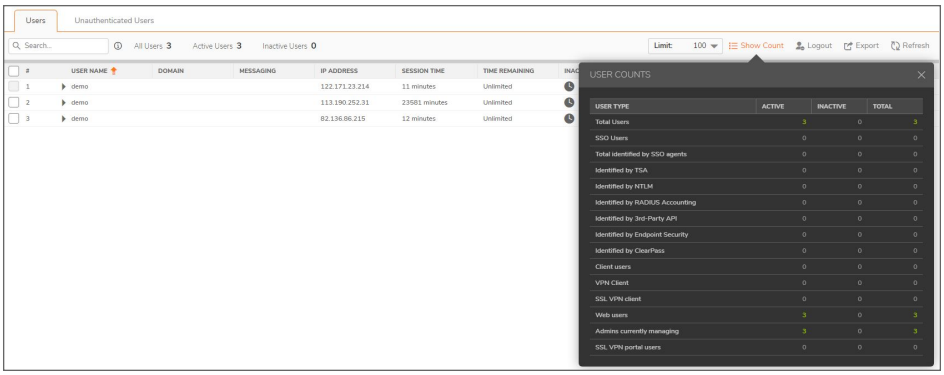
- Navigate to the **Device > Users > Status > Unauthenticated Users** page. Unauthenticated users are displayed.



Displaying the User Count

To display the current user count:

1. Navigate to the **Device > Users** page.



2. Click the **Show Count** icon on the far right of the toolbar above the list. The **User Counts** window displays:
    - **User Type**
    - **Active**
    - **Inactive**
    - **Total**
3. Click the X on the top right of **User Counts** window to close it.

Refreshing the Users List

To refresh the Users list:

1. Navigate to the **Device > Users > Status**.
2. Click the **Refresh** icon on the far right of the toolbar above the list.

Logging Out Users

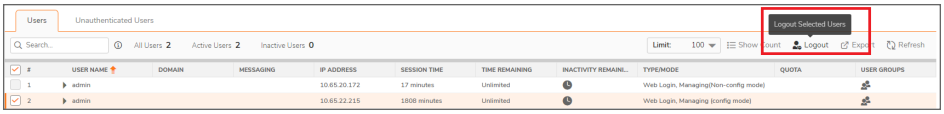
Topics:

- Logging Out a Single User
- Logging Out Multiple Users

Logging Out a Single User

To log out a user:

1. Navigate to the **Device > Users > Status**.
2. Select the user you would like to logout from the list.
3. Click **Logout Selected Users**.

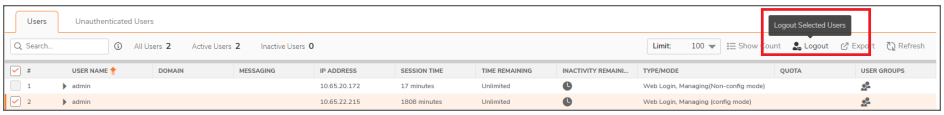


Logging Out Multiple Users

To log out multiple users:

1. Navigate to the **Device > Users > Status**.
2. Select the checkbox at the top left of the list, just below the **Search** icon, to select all of the users currently displayed.

3. Click **Logout Selected Users**.



4

Configuring User Settings

In addition to the regular authentication methods, SonicOS allows you to use Lightweight Directory Access Protocol (LDAP) to authenticate users. LDAP is compatible with Microsoft's Active Directory.

For SonicWall appliances, you can select the SonicWall Single Sign-On Agent to provide Single Sign-On functionality. Single Sign-On (SSO) is a transparent user authentication mechanism that allows privileged access to multiple network resources with a single workstation login. SW network security appliances provide SSO functionality using the SonicWall Single Sign-On Agent (SSO Agent) to identify user activity based on the workstation's IP address when Active Directory is used for authentication. The SonicWall SSO Agent must be installed on a computer that is in the same domain as Active Directory.

Topics:

User Login Settings

Topics:

Setting the Authentication Method for Login

To set the authentication method for login:

1. Navigate to the **Device > Users > Settings > Authentication** page.
2. Select one of the following authentication methods from **User authentication method**:

Local Users	To configure users in the local database, use the Users > Local Users and Users > Local Groups pages. For more information on configuring local users and groups, refer to Configuring Local Users and Configuring Local Groups.
RADIUS	If you have more than 1,000 users or want to add an extra layer of security for authenticating users to the SonicWall, you can select "Use RADIUS" for user authentication. This requires users to log into the SonicWall using HTTPS to encrypt the password sent to the device. If a user attempts to log in using HTTP, the browser is automatically redirected to HTTPS. For information on configuring RADIUS, refer to Configuring RADIUS.
RADIUS + Local Users	If you want to use both RADIUS and the SonicWall local user database for authentication, refer to Configuring RADIUS.
LDAP	If you use a Lightweight Directory Access Protocol (LDAP) server or a Microsoft Active Directory (AD) server to maintain all your user account data, it is essential to ensure proper configuration and security measures are in place. For information about configuring LDAP, refer to Configuring LDAP.
LDAP + Local Users	If you want to use both LDAP and the SonicWall local user database for authentication. For information about configuring LDAP, refer to Configuring LDAP.
TACACS+	If you use the Terminal Access Controller Access-Control System Plus (TACACS+) protocol for authentication.
TACACS+ + Local Users	If you use the Terminal Access Controller Access-Control System Plus (TACACS+) protocol along with the SonicWall local user database for authentication.

3. Click **Accept**.

Configuring RADIUS

- Configuring RADIUS Settings
- Configuring RADIUS Users Settings
- Testing RADIUS Settings

Configuring RADIUS Settings

1. Navigate to **Device >Users > Settings > Authentication**.
2. Next to **Configure RADIUS**, click **Configure**.
   The **RADIUS Configuration** page is displayed.
3. Under the **Settings** > **Radius Server** tab, do the following:
   a. Click **Add**. The **Settings** page displays.
   b. In the **Host Name or IP Address** field, enter the host name or IP address .
   c. In the **Port** field, enter the port number.
   d. In the **Shared Secret** and **Confirm Shared Secret** fields, enter the shared secret.
4. On the **Advanced** tab, do the following:
   a. Select **Send Through VPN tunnel** to send the requests across the VPN tunnel but it also binds these requests to X0 interface even if we have specified local network for site to site VPN.
   b. From the **User Name Format** list, select the username format:
      - **Simple-Name**
      - **Name@Domain**
      - **Domain\Name**
      - **Name.Domain**
   c. Click **Save**. The RADIUS Accounting table is updated.
5. Click on **General Settings**, do the following:
   a. In the **RADIUS Accounting Server Timeout (seconds)** field, enter a maximum time out, in seconds. The default value is **5** seconds.
   b. In the **Retries** field, enter the maximum number of retries. The default value is **3** retries.
   c. Enable **Periodically check RADIUS servers that are down** to request then its status changes to down and then further authentication requests is sent to the secondary server until the primary comes back up again.
   d. Enable **Force MSCHAPv2** mode to allow password updating.
6. Click **Save**.
7. For each RADIUS server you want to add, repeat these steps.
8. Click **Save**.

Configuring RADIUS Users Settings

1. Navigate to **Device >Users > Settings > Authentication**.
2. Next to **Configure RADIUS**, click **Configure**.
   The **RADIUS Configuration** page is displayed.
3. On the **RADIUS Users** tab, do the following:

a. Select **Allow only users listed locally** if only the users listed in the SonicOS database are authenticated using RADIUS.

b. Select the mechanism used for setting user group memberships for RADIUS users from the following choices:

- Select **Use vendor-specific attribute on RADIUS server** to apply a configured vendor-specific attribute from the RADIUS server. The attribute must provide the user group to which the user belongs.
- Select **Use RADIUS Filter-Id attribute on RADIUS server** to apply a configured Filter-Id attribute from the RADIUS server. The attribute must provide the user group to which the user belongs.
- Select **Use LDAP to retrieve user group information** to obtain the user group from the LDAP server. You can click the **Configure** button to set up LDAP if you have not already configured it or if you need to make a change.
- If you do not plan to retrieve user group information from RADIUS or LDAP, select **Local configuration only**.
- Select the group from the **Default user group to which all RADIUS users** belong drop-down menu. See Configuring Local Groups.

4. Click **Save**.

Testing RADIUS Settings

You can test your RADIUS Client user name, password and other settings by typing in a valid user name and password and selecting one of the authentication choices for Test. Performing the test will apply any changes that you have made.

1. Navigate to **Device >Users > Settings > Authentication**.
2. Next to **Configure RADIUS**, click **Configure**.
   The **RADIUS Configuration** page is displayed.
3. On the **Test** tab, do the following:
   a. Select the server in the **Select server to test** drop-down menu.
   b. For **Test**, select one of the following:
      - **Connectivity**
      - **Password authentication**
      - **CHAP**
      - **MSCHAP**
      - **MSCHAPv2**
   c. In the **User** field, type a valid RADIUS login name.
   d. In the **Password** field, type the password.

4. Click **Test**.
   The **Test Status** is update and any user attributes returned will be displayed in **Returned User Attributes**.

Configuring LDAP

In addition to RADIUS and the local user database, SonicOS supports LDAP and Microsoft Active Directory (AD) directory services for user authentication.

- Configuring LDAP Setting
- Configuring Referrals
- LDAP User Settings
- Enabling LDAP Relay
- Testing LDAP Settings

Configuring LDAP Setting

1. Navigate to **Device > Users > Settings > Authentication**.
2. Next to **Configure LDAP**, click **Configure**.
   The **LDAP Configuration** page is displayed.
3. Under the **Settings** > **LDAP servers** tab, click **Add Server**.
   The **Settings** page displays.
4. Under **Settings**, do the following:
   a. Select the one of the LDAP server roles in **Role**.
      - **Primary LDAP server**
      - **Secondary LDAP server**
      - **Backup/replica server**
   b. In **Name or IP Address** enter the FQDN or the IP address of the LDAP server against which you wish to authenticate.
      If using a name, be certain it can be resolved by your DNS server. Also, if using TLS with the 'Require valid certificate from server' option, the name provided here must match the name to which the server certificate was issued (such as the CN) or the TLS exchange will fail.
   c. In **Port Number**, select one of the following:
      - **Default LDAP over TLS port number (636)**
      - **Default LDAP port (389)**
      - **Windows Global Catalog port (3268)**
      - **Global Catalog over TLS port (3269)**

d. In **Server timeout**, enter the amount of time, in seconds, that the SonicWALL waits for a response from the LDAP server before timing out.

   Allowable ranges are 1 to 99999 (in case you are running your LDAP server on a VIC-20 located on the moon), with a default of 10 seconds.

e. In **Overall operation timeout (minutes)**, enter the maximum time to spend on any auto-operation.

f. Select the **Use TLS** (SSL), to log in to the LDAP server. This is selected by default.

   It is strongly recommended that TLS be used to protected the username and password information that is sent across the network. Most modern implementations of LDAP server, including AD, support TLS.

g. Select the **Send LDAP 'Start TLS' Request**.

   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.

h. Click **Save**.

5. Under **Login/Bind** do the following:

   a. Select the **Anonymous Login** option for some LDAP servers allow for the tree to be accessed anonymously.
   If your server supports this (MS AS generally does not), then you could select this option.

   b. If you select **Give login name/location in tree** provide the following:

      - In **Login user name** specify a user name that has rights to log in to the LDAP directory.
      - Select the **User tree for login to server** when **Give login name/location in tree** is selected this specifies the tree in the directory that holds the user object for the user account configured there for login (bind) to the LDAP server.
      - The password for the user account in **Password**.

   c. If you select **Give bind distinguished name** provide the following:

      - In **Bind distinguished name** specify a user name.
      - The password for the user account in **Password**.

   d. In **When referred to other servers** select one of the following:

      - **Bind with this account**
      - **Bind with an equivalent account on that server (same password)**

   e. Click **Save**.

6. Under **Schema**, do the following:

   a. In **LDAP Schema**, select the predefined schemas will automatically populate the fields used by that schema with their correct values.

- **Microsoft Active Directory**
- **RFC2798 InetOrgPerson**
- **RFC2307 Network Information Service**
- **Samba SMB**
- **Novell eDirectory**
- **User defined**
  Selecting **User defined** allows you to specify your own value use this only if you have a specific or proprietary LDAP schema configuration.

b. In **Object class**, select which attribute represents the individual user account.

c. In **Attributes**, enter the following:

- Enter **Login name**
- Enter **Qualified login name** to specify an attribute of a user object that sets an alternative login name for the user in name@domain format
- In **User group membership** enter the information in the user object of which groups it belongs.
- In **Additional user group ID** enter the user group id and select **Use**.
  If the **Additional user group ID** user attribute is set and its use is enabled (the **Use** is enabled) then when a user object is found with one or more instances of this attribute, a search for additional user groups matching those will be made in the LDAP directory. If a group is found with the **Additional user group match** attribute set to that value then the user will also be made a member of that group.
- In **Framed IP address** enter the IP address to retrieve a static IP address that is assigned to a user in the directory.

d. Click **Save**.

7. Under **Directory**, do the following:

a. In **Primary Domain**, specify the user domain used by your LDAP implementation.

b. Click **Auto-configure** 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.

c. In **Trees containing users** add the users. The trees where users commonly reside in the LDAP directory. One default value is provided which can be edited, an up to a total of 64 DN values might be provided, and the SonicWALL search the directory using them all 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.

d. In **Trees containing user groups** add the groups. A maximum of 32 DN values might 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.

e. Click **Save**.

8. Click **Apply**.

9. In **General Settings** do the following:
    a. In the **Protocol version** from the drop-down menu select either **LDAP version 3** or **LDAP version 2**.
    b. Select **Require valid certificate from server when using TLS** to validate the certificate presented by the server during the TLS exchange, matching the name specified above to the name on the certificate.
    c. In the **Local certificate for TLS** to be used only if the LDAP server requires a client certificate for connections.
    d. In the **Allowed cipher suites for TLS** The allowed cipher suites for TLS specify the cryptographic algorithms that can be used in Transport Layer Security (TLS) connections.
    e. Click **Apply**.

Configuring Referrals

If your network uses multiple LDAP/AD servers with referrals, then select one as the primary server (probably the one that holds the bulk of the users) and use the above settings for that server. It then refers the SonicWall on to the other servers for users in domains other than its own. For the SonicWall to be able to log in to those other servers, each server must have a user configured with the same credentials (user name, password and location in the directory) as per the login to primary server. This might entail creating a special user in the directory for the SonicWall login. Note that only read access to the directory is required.

1. Navigate to **Device > Users > Settings > Authentication**.
2. Next to **Configure LDAP**, click **Configure**.
   The **LDAP Configuration** page is displayed.
3. Click **Referrals** tab.
4. Select the following:
    - **Allow referrals**
    - **Allow continuation references during user authentication**
    - **Allow continuation references during directory auto-configuration**
    - **Allow continuation references in domain searches**
5. Click **Apply**.

LDAP User Settings

1. Navigate to **Device > Users > Settings > Authentication**.
2. Next to **Configure LDAP**, click **Configure**.
   The **LDAP Configuration** page is displayed.
3. Under the **Users & Groups** tab, do the following:

a. Select **Allow only users listed locally** allows the LDAP users also be present in theSonicWall local user database for logins.

b. In the **Default LDAP User Group** drop-down select a default group on the SonicWall to which LDAP users will belong in addition to group memberships configured on the LDAP server.

c. Click **Import Users** and select one of the following:

- **Select the LDAP server to import from**
- **Import from all LDAP servers**

d. When importing users you can choose whether or not to include the domains in the imported user objects. Select one of the following:

- **Include the domains**
- **No domains (imported user objects will match the named users in any domain)**

e. Click **OK**.

f. Click **Import User Groups** and select one of the following:

- **Import User Groups from the LDAP directory**
- **Auto-create groups for setting memberships by LDAP location (OU)**

g. When importing you can select where to import from. Select one of the following:

- **Select the LDAP server to import from**
- **Import from all LDAP servers**

h. When importing users you can choose whether or not to include the domains in the imported user objects. Select one of the following:

- **Include the domains**
- **No domains (imported user objects will match the named users in any domain)**

i. Click **OK**.

j. Select **Mirror LDAP user groups locally** to mirror the LDAP user groups locally.

k. In **Mirror** select one of the following:

- **All user groups on the LDAP server**
- **Only groups that have member users or groups**

l. Enter the **Refresh period (minutes)** in minutes to refresh the mirroring and click **Refresh**.

m. In **Exclude groups in these sub-trees**, add the user groups to be exclude in the sub-tress.

4. Click **Apply**.

Enabling LDAP Relay

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.

ⓘ | **NOTE:**

- The RADIUS client on the remote SonicWall should be configured to use port 1812 and the shared secret below (See step 7)
- On remoteSonicWall running SonicOS enhanced firmware, select **Use SonicWall vendor-specific attribute on RADIUS server** on the **RADIUS Users** tab.

1. Navigate to **Device > Users > Settings > Accounting**.
2. Next to **Configure LDAP**, click **Configure**.
   The **LDAP Configuration** page is displayed.
3. Under the **LDAP Relay** tab do the following:
   a. Select **Enable RADIUS to LDAP Relay**
   b. In **Allow RADIUS clients to connect via** select one of the policy rules to allow incoming RADIUS requests accordingly.
      - **Trusted Zones**
      - **WAN Zone**
      - **Public Zones**
      - **Wireless Zones**
      - **VPN Zone**
   c. In the **RADIUS shared secret** enter a shared secret common to all remote SonicWall.
      Additionally, for remote SonicWalls running non-enhanced firmware, with this feature the central SonicWall can return legacy user privilege information to them based on user group memberships learned via LDAP. This avoids what can be very complex configuration of an external RADIUS server such as IAS for those SonicWalls.
   d. In **User groups for legacy VPN users**, enter the user group that corresponds to the legacy **Access to VPNs** privileges. When a user in this user group is authenticated, the remote SonicWall is notified to give the user the relevant privileges.
   e. In **User groups for legacy VPN client users**, enter the user group that corresponds to the legacy **Access from VPN client with XAUTH** privileges. When a user in this user group is authenticated, the remote SonicWall is notified to give the user the relevant privileges
   f. In **User groups for legacy L2TP users**, enter the user group that corresponds to the legacy **Access from L2TP VPN client** privileges. When a user in this user group is authenticated, the remote SonicWall is notified to give the user the relevant privileges.
   g. In **User groups for legacy users with Internet access**, enter the user group that corresponds to the legacy **Allow Internet access (when access is restricted)** privileges. When a user in this user group is authenticated, the remote SonicWall is notified to give the user the relevant privileges.
4. Click **Apply**.

Testing LDAP Settings

You can test your LDAP client user name, password and other settings by typing in a valid user name and password and selecting one of the authentication choices for Test. To test the LDAP settings select the test, enter a user name and password that is valid on the LDAP server if relevant, and then click the Test button. Note that this will apply any changes that have been made.

1. Navigate to **Device >Users > Settings > Accounting**.
2. Next to **Configure LDAP**, click **Configure**.
   The **LDAP Configuration** page is displayed.
3. On the **Test** tab, do the following:
   a. Select the server in the **Select server to test** drop-down menu.
   b. For **Test**, select one of the following:
      - **Connectivity / bind test**
      - **User authentication test**
      - **LDAP search**
   c. If you selected **User authentication test**, then:
      1. In the **User** field, type a valid login name.
      2. In the **Password** field, type the password and select **Password authentication** or **CHAP** to test whether LDAP can work as the back-end for authenticating a front-end that does CHAP or MSCHAP authentication with the SonicWall.
      3. Click **Test**.
   d. If you selected **LDAP search**, then:
      1. Select an LDAP in **Search for** a user or user group using the **Login Name**, **Qualified Login Name**, or **Common Name**, and specify what the name should be equal to.
         Or
         Select **Advanced Search Options** and **More Options** to search from base or scope.
      2. Select from **Search base** to search from:
         - **Top of the domain tree**
         - **Root of the directory**
         - **Other**: to search from Search base DN
      3. Select from **Search scope** to search from:
         - **Search the sub-tree**
         - **Search the base entry only**
         - **Search one level below the base**

4. Click **Test**.
   The **Test Status** is update and any user attributes returned will be displayed in **Returned User Attributes**.

Configuring TACACS+

- Configuring TACACS+ Settings
- Configuring TACACS+ User Settings
- Testing TACACS+ Settings

Configuring TACACS+ Settings

1. Navigate to **Device > Users > Settings > Authentication**.
2. Next to **Configure TACACS+**, click **Configure**.
   The **TACACS Configuration** page is displayed.
3. Under the **Settings** tab, do the following:
   a. Click **Add Server**. The **Settings** page displays.
   b. In the **Host Name or IP Address** field, enter the host name or IP address .
   c. In the **Port** field, enter the port number.
   d. In the **Shared Secret** and **Confirm Shared Secret** fields, enter the shared secret.
   e. Click **Save**.
4. Under the **Advanced** tab, select **Send Through VPN tunnel** to send the requests across the VPN tunnel but it also binds these requests to X0 interface even if we have specified local network for site to site VPN.
5. Click **Save**.
6. Click on **General Settings**, do the following:
   a. In the **TACACS Server Timeout (seconds)** field, enter a maximum time out, in seconds.The default value is **5** seconds.
   b. In the **Retries** field, enter the maximum number of retries. The default value is **3** retries.
   c. Enable **Support Single-Connect** to connect Multiple TACACS+ sessions simultaneously and/or consecutively on a single TCP connection if both the daemon and client support this.
   d. Enable **Periodically check TACACS servers that are down** to periodically check TACACS servers that are down.
7. Click **Save**.

Configuring TACACS+ User Settings

1. Navigate to **Device >Users > Settings > Accounting**.
2. Next to **Configure TACACS+**, click **Configure**.
   The **TACACS Configuration** page is displayed.
3. In the **TACACS Users** tab do the following:
   a. Select **Allow only users listed locally** if only the users listed in the SonicOS database are authenticated using RADIUS.
   b. Select the mechanism used for setting user group memberships for TACAS+ users.
      - Select **Use LDAP to retrieve user group information** to obtain the user group from the LDAP server. You can click the **Configure** button to set up LDAP if you have not already configured it or if you need to make a change.
      - If you do not plan to retrieve user group information from RADIUS or LDAP, select **Local configuration only**.
   c. Select the group from the **Default user group to which all TACACS+ users** belong drop-down menu. See Configuring Local Groups.
4. Click **Save**.

Testing TACACS+ Settings

1. Navigate to **Device >Users > Settings > Authentication**.
2. Next to **Configure TACACS+**, click **Configure**.
   The **TACACS Configuration** page is displayed.
3. On the **Test** tab, do the following:
   a. Select the server in the **Select server to test** drop-down menu.
   b. For **Test**, select one of the following:
      - **Connectivity**
      - **Password authentication**
      - **CHAP**
      - **MSCHAP**
   c. In the **User** field, type a valid login name.
   d. In the **Password** field, type the password.
   e. Select one of the following for the type of testing you would like to complete:
      - **Outbound TACACS+ Authentication**
      - **Test Combined AAA**
      - **Send clear TACACS+ packet**

4. Click **Test**.
   The **Test Status** is update and any user attributes returned will be displayed in **Returned User Attributes**.

Requiring User Names be Treated as Case-Sensitive

To require that user names are treated as case-sensitive:

1. Navigate to the **Device > Users > Settings > Authentication** page.
2. Under **User Authentication settings** select **Case-sensitive user names**. (This option is selected by default.)
3. Click **Accept**.

Preventing Users From Logging in from More than One Location

To prevent users from logging in from more than one location at a time:

1. Navigate to **Device > Users > Settings > Authentication**.
2. Select **Enforce login uniqueness**. This option is not selected by default.
3. Click **Accept**.

Forcing Users to Log In Immediately After Changing Their Passwords

To force the user to login immediately after changing the password:

1. Navigate to **Device > Users > Settings > Authentication**.
2. Select **Force relogin after password change**. This option is not selected by default.
3. Click **Accept**.

Displaying User Login Information Since the Last Login

To display user login information since the last login:

1. Navigate to the **Device > Users > Settings > Authentication** page.
2. Select **Display user login info since last login**. This option is not selected by default.
3. Click **Accept**.

Setting the Single-Sign-On Methods

The **Single-sign-on method(s)** displays the status of the available method(s). You can enable/disable methods, or click **Configure** to configure a single-sign-on method. The following methods are available:

To set the single-sign-on methods:

1. Navigate to the **Device > Users > Settings > Authentication** page.
2. Enable or disable the methods, or click **Configure** to configure a single-sign-on method. These methods are available:

Configure SSO	Configure SSO to use the SSO Agent or TSA.
SSO Agent	Configure the **SSO Agent** if you are using Active Directory for authentication and the SonicWall SSO Agent is installed on a computer in the same domain.
Terminal Services Agent	Configure the SSO Agent if you are using Terminal Services and the SonicWall Terminal Services Agent (TSA) is installed on a terminal server in the same domain.
Browser NTLM Authentication	Configure **Browser NTLM Authentication** if you want to authenticate Web users without using the SonicWall SSO Agent or TSA. Users are identified as soon as they send HTTP traffic. NTLM requires RADIUS to be configured (in addition to LDAP, if using LDAP), for access to MSCHAP authentication.
RADIUS Accounting	Configure **RADIUS Accounting** if you want a network access server (NAS) to send user login session accounting messages to an accounting server.
3rd Party API	Configure the XML-/JSON-based REST API for third-party devices or scripts to pass user login/logout notifications to the firewall.

3. Click **Accept**.

Configuring SSO

To configure a single-sign-on methods click Next to **Configure SSO**, click **Configure**.The following methods are displayed:

- SSO Agents
- Users
- Enforcement
- Terminal Services
- NTLM
- RADIUS Accounting
- 3rd Party API
- Capture Client
- Test

SSO Agents

To set the single-sign-on methods:

1. Navigate to the **Device > Users > Settings > Authentication** page.
2. Next to **Configure SSO**, click **Configure**.
   The **SSO Configuration** page is displayed.
3. Under the **SSO Agents** tab, to add a agent click **Add Agent**.
4. In the **Settings** tab, enter the following:
   a. Enter **Host Name or IP Address**.
   b. Enter **Port**.
   c. Enter **Shared Key**
   d. Re-enter the shared key in the **Confirm Shared Key** field.
   e. Enter **Timeout (seconds)**, default is 5 seconds.
   f. Enter **Retries**, default is 3 seconds.
5. In the **Advanced** tab, enter **Maximum requests to send at a time**.
6. Click **Save**.
7. Under the **General Settings** tab, select the following:
   a. Enable **Enable SSO agent authentication** to use the SSO Agent for user authentication. This setting is enabled by default.

b. Enable **Try next agent on getting no name from NetAPI/WMI** to force a retry of the authentication via a different SSO agent if there is no response or error from the first agent. This only affects agents using NetAPI/WMI. This setting is disabled by default.

c. Enable **Don't block user traffic while waiting for SSO** to use the default policy while the user is being identified. This prevents browsing delays. This setting is disabled by default.

d. On enabling **Don't block user traffic while waiting for SSO**, the **Including for** is enabled and allows traffic affected by access rules that require user authentication, while waiting for user identification. Select anyone of the following:

- **All access rules**
- **Selected access rules**

e. Select anyone of the following in **When agent synchronize their user databases**

- **Sync those with the same user identification mechanisms**:To synchronize only those databases using the same identification mechanism; this is the default.
- **Sync all agents**: To synchronize together no matter what identification mechanisms they use, thus giving a single, homogenous user database duplicated on every agent.

8. Click **Add Service User Names** to add a windows service user names.

a. Enter the name in **Enter New Service Users Name**.

b. Click **Save**.

The list of Windows service user names in the User names used by Windows services is listed in the windows services table.

9. Click **Save**.

Users

1. Navigate to the **Device > Users > Settings > Authentication** page.
2. Next to **Configure SSO**, click **Configure**.
The **SSO Configuration** page is displayed.
3. Under **Users** tab, select the following:

a. Enable **Allow only users listed locally** to allow only users listed locally to be authenticated.

b. Enable **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.

c. If your network includes non-Windows devices or Windows computers with personal firewalls running select **Enable Probe Users**. In the **Probe user for** select one of the following, depending on which is configured for the SSO Agent:

- **NetAPI over NetBIOS**
- **NetAPI over TCP**
- **WMI**

d. Set the **Probe timeout (seconds)** for the firewall to probe for a response on the NetAPI/WMI port before requesting that the SSO Agent identify a user. The default is 5 seconds.

e. Enable the **Probe test mode** to test that SSO probes are functioning correctly during SSO without interfering with user authentications. Probes are sent after initiating user authentication through the SSO agent. This setting is disabled by default.

f. For the **Mechanism for setting user group memberships**, select either:

- **Use LDAP to retrieve user group information**: to use LDAP to retrieve user information.
- **Local configuration**: to use locally configured user group settings.

g. In the **Polling rate (minutes)** field, enter a polling interval, in minutes. The default is 5 minutes.

h. Enable the **Poll the same agent that authenticated the user** if the network topology requires that particular agents be used depending on the location of users, rather than polling any agent to determine if the user is still logged in. This setting is disabled by default.

i. In the **Hold time after (minutes)** field, enter a time, in minutes, that the security appliance waits before trying again to identify traffic after an initial failure to do so. This feature rate limits requests to the agent to avoid possibly flooding it with requests if further traffic continues to be received from sources that repeatedly fail SSO. The default is 1 minute.

j. In the **after finding no user** field, enter the number of minutes that the appliance should wait before trying again if it gets errors from the SSO agent or when the agent reports that no user is logged in. The default is 1 minute.

k. Enable the **Ramp up** and select the **rate**.

l. In **When different SSO sources report different name variants for a user's domain** select any one of the following to give consistent naming for a domain in logging:

- **Use the domain name as received**: is selected as default.
- **Always use a consistent domain name**

4. Click **Save**.

Enforcement

The settings in the **Enforcement** tab are if you want to either trigger SSO on traffic from a particular zone, or bypass SSO for traffic from non-user devices such as internal proxy web servers or IP phones.

1. Navigate to the **Device > Users > Settings > Authentication** page.
2. Next to **Configure SSO**, click **Configure**.
   The **SSO Configuration** page is displayed.
3. Under **Enforcement** tab, select the following:
   a. Under **Per-Zone SSO Enforcement**, select for any zones on which you want to trigger SSO to identify users when traffic is sent.
      - **DMZ**
      - **LAN**

- **MGMT**
- **VPN**

b. Click **Save**.

These per-zone SSO enforcement settings are useful for identifying and tracking users in event logging and AppFlow Monitor visualizations, even when SSO is not otherwise triggered by content filtering, IPS, or Application Control policies, or by firewall access rules requiring user authentication.

4. To bypass SSO for traffic from certain services or locations and apply the default content filtering policy to the traffic, select the appropriate service or location from the list in the **SSO Bypass** table or add a new service or location to the table. The table displays the built-in services that bypass SSO; these services cannot be delete.
   a. Click the **Add Bypass** button.
      The **Add an SSO bypass rule** dialog displays.
   b. For **Bypass SSO** for, select either the **Services** or **Addresses**.
   c. Select a service or address from the drop-down menu.
   d. Select the **Bypass type**:
      - **Full bypass (don't trigger SSO)**
      - **Trigger SSO but bypass holding packets while waiting for it**
   e. Click **Save**.
5. Enable **SSO bypass user name for logging**. This is enabled by default.
   a. To select a SSO bypass user name for logging, select the **Log user name <bypass name> for SSO bypasses** and specify a name for the SSO bypassed user.
   b. Optionally, select **Create a dummy user**. If this setting is enabled, on receiving SSO bypass traffic, a dummy user entry is created with the given user name for the originating IP address.
   c. Optionally, specify an inactivity timeout, in minutes, in the **Inactivity timeout (mins)** field. The default is 15 minutes.
6. Click **Save**.

Terminal Services

The **Terminal Services** tab to specify the following Terminal Services Agent Settings options.

1. Navigate to the **Device > Users > Settings > Authentication** page.
2. Next to **Configure SSO**, click **Configure**.
   The **SSO Configuration** page is displayed.
3. Under the **Terminal Services** tab, select the following:

a. Click the **Add Agent** button.

b. 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.

c. At **Port**, enter the port number that the SonicWALL TSA is using to communicate with the appliance. The default port is 2259. Note that agents at different IP addresses can have the same port number.

d. In the **Shared Key** field, enter the shared key that you created or generated in the SonicWALL TSA.

e. Re-enter the shared key in the **Confirm Shared Key** field.

4. Under the **General Settings** tab, select the following:

a. Select the **Enable Terminal Services agent authentication** to use the TSA for user authentication. This setting is enabled by default.

b. The **Allow traffic from services on the terminal server to bypass user authentication in access rules** is selected by default. This allows service traffic, such as Windows updates or anti-virus updates not associated with any user login session, to pass without authentication. That traffic normally would be blocked if the applicable firewall rules are set to require user authentication.

5. Click **Save**.

NTLM

NTLM browser authentication allows the SonicWall to automatically authenticate the user of a browser directly with no SSO agent involvement.

NTLM authentication is supported by Mozilla-based browsers and can be used as a supplement to identifying users via an SSO agent or, with some limitations, on its own without the agent. The firewall interacts directly with the browser to authenticate the user. Users logged in with domain credentials are authenticated transparently; in other cases the user may need to enter credentials to login to the appliance, but should only need to do so once as the credentials are saved.

1. Navigate to the **Device > Users > Settings > Authentication** page.
2. Next to **Configure SSO**, click **Configure**.
   The **SSO Configuration** page is displayed.
3. Under the **NTLM** tab, select the following:

a. Select **Use NTLM to authenticate HTTP/HTTPS traffic** to use NTML authentication.

b. Select the **Use the domain from the LDAP configuration** to use the same domain that is used in the LDAP configuration.

c. In **Authentication domain**, enter the full DNS name of the firewall's domain in the form "www.somedomain.com"

d. In **Redirect the browser to this appliance via**, select one of the following options to determine how a user's browser is initially redirected to the firewall's own Web server:

- **The interface IP address**: Select this to redirect the browser to the IP address of the appliance Web server interface.
- **Its domain name from a reverse DNS lookup of the interface IP address**: Enables the Show Reverse DNS Cache button at the bottom of the window; when clicked, a popup displays the appliance Web server's Interface, IP Address, DNS Name, and TTL in seconds. Click the button to verify the domain name (DNS name) being used for redirecting the user's browser.
- **Its configured domain name**: Use the firewall's domain name as configured on the **Device** > **Settings** > **Administration** page.
- **The name from the administration certificate**: Use the imported certificate that is selected for HTTPS Web Management on the **Device** > **Settings** > **Administration** page.

e. Enter a number of retries in the **Maximum retries to allow on authentication failure**.

f. If you are using older legacy servers that require legacy LAN Manager components to be included in NTLM messages, select the **Forward legacy LanMan in NTLM**.

g. To detect when users log out, select the polling method to be used by the appliance for Windows, Linux, and Macintosh users in the **On the poll timer, for users authenticated user via NTLM** options. Select the one of the following methods for users on each type of computer:

- **Re-authenticate via NTLM**: This method is transparent to the user if the browser is configured to store the domain credentials, or the user instructed the browser to save the credentials.
- **Don't re-authenticate**: If you select this option, logout will not be detected other than via the inactivity timeout.

4. Click **Save**.

RADIUS Accounting

Single Sign-On by RADIUS accounting allows the appliance to act as a RADIUS accounting server for external third-party appliances, and to log users in or out based on the accounting messages from those devices. For third-party appliances that use RADIUS accounting for other purposes, SonicOS can also forward the RADIUS accounting messages to another RADIUS accounting server.

1. Navigate to the **Device > Users > Settings > Authentication** page.
2. Next to **Configure SSO**, click **Configure**.
   The **SSO Configuration** page is displayed.
3. In the **RADIUS Accounting** tab, under **Accounting Clients** select the following:
   a. Click **Add Client**.
   b. Under the **Settings** tab, do the following:
      1. In the **Client host name or IP address** field, enter the name or the IP address for the RADIUS client host.

2. In the **Shared Key** field and the **Confirm Shared Key** field, enter your shared secret for the client.
3. Click **Save**.

c. Under the **Radius** tab, do the following:

1. From the **User-Name attribute format** drop-down menu, select the format for the user name login. You can select from some common formats:
    - **User-name**
    - **Domain\User-name**
    - **Domain/User-name**
    - **User-name@Domain**
    - **SonicWALL Aventail**
    - Or, you can select a non-standard format, **Others**.
2. If you selected **User-name** go to Select a Log user out if no accounting interim updates are received option.
3. If you select **Others**, more settings appear so you can configure the components to be found in the attribute:
    1. In **Format** enter a limited scanf-style string, with either a %s or %[…] directive for each component.
    2. Click **Add Component**.
    3. Select the **This is the last component**.
    4. Select the type of component from the **Component** to add drop-down menu:
        - **User-name**
        - **Domain**
        - **DN**
    5. Enter text to separate entries in the **Any text that precedes it** and **Any text that follows it** fields.
    6. Click **Add**.
    7. To delete the last component you added, click **Remove last**.
4. Select a **Log user out if no accounting interim updates are received** option.
    - **Disabled**: to not have messages sent.
    - **Enabled**: to manually specify the Timeout interval. Set the timeout value greater than the period at which the RADIUS Accounting client sends the Interim-Update messages, and for dropped/missed Interim-Update messages, set the Timeout value at least 2 to 3 times greater than the period.
    - **Auto (default)**: to have the appliance detect automatically whether Interim-Update

message are being sent periodically and, if they are, to use them as specified under Enabled and setting automatically the timeout accordingly.

5. Click **Save**.

d. Under the **Forwarding** tab, do the following:

1. You can enter up to four RADIUS accounting servers in these fields:
   - **Name or IP address**
   - **Port (default 1813)**
   - **Shared Secret** for the RADIUS accounting servers to which you want the client to forward message
   - **Confirm Shared Secret**
2. When you enter this information for a server, the **Select** from drop down menu displays.
   - **No forwarding**
   - **IP address of the accounting server**
3. In the **Timeout (seconds)** field, enter the timeout period in seconds. The default for Timeout (seconds) is 10 seconds,
4. In the **Retries** field enter and the number of retries. The default for retries is 3.

e. Select how the RADIUS accounting messages are forwarded from this client, either:
   - **Try next on timeout**
   - **Forward to all**

4. In the **General Settings** tab, do the following:

a. Enable SSO or RADIUS accounting by selecting the **Enable SSO or RADIUS accounting**. This setting is enabled by default.

b. Specify the port in the **Port number** field. The default port is 1813.

c. In **Mechanism for looking up user group memberships for RADIUS Accounting users** select one of the following:
   - **Use the mechanism selected on the SSO Users tab**
   - **Use Filter-Id attribute from RADIUS Accounting requests**

5. Click **Save**.

6. In the **Advanced Settings** tab, do the following:

a. Select **Expect Start/Stop messages due to wireless roaming** to notify the SonicWall of users connecting/disconnecting.

b. In the **Maximum switch-over time(seconds)** enter in seconds. The default is 30 seconds.

c. In **Wireless Roaming Transitions** select one of the following:
   - **Expect logical transitions**
   - **Ignore transition message sequence/source(s)**

d. Select to ignore any radius accounting messages in **For users at these IP addresses** and **For users not at these IP addresses**.

e. Click **Add User Names**.

f. Select **Begin** with or **End** with in **Ignore any user names that**.

7. Click **Save**.

3rd Party API

The SSO API is an XML/JSON based REST API for 3rd-Party devices or scripts to pass user login/logout notifications to the SonicWall.

1. Navigate to the **Device > Users > Settings > Authentication** page.
2. Next to **Configure SSO**, click **Configure**.
   The **SSO Configuration** page is displayed.
3. Click the **3rd Party API** tab.
4. In the **API Clients** tab, click **Add Client**.
   a. Under the **Settings** tab, select the following:
      1. In the **Client host name or IP address** field, enter the name or IP address of the terminal server on which SonicWALL TSA is installed.
      2. In **Authenticate the client via** select one of the following:
         - **Shared secret**
         - **Certificate**
         - **Both**
      3. In the **Shared Key** field, enter the shared key that you created or generated in the SonicWALL TSA.
      4. Re-enter the shared key in the **Confirm Shared Key** field.
   b. Click **Save**.
   c. Under the **Advanced** tab, select the following:
      1. To select the level of security to use for verification of the shared secret, in **Shared secret verification security level**, select one of the following :
         - **High with** and select the checkboxes **SHA256** and **SHA512**
         - **Medium (SHA256 but no replay prevention)**
         - **Low (no shared secret verification)**
      2. Select the **Enable CSRF/replay prevention** check box to prevent the Cross-Site Request Forgery.
      3. Enable the **Restrict origins if client uses CORS** check box to prevent if a client uses Cross-Origin Resource Sharing (CORS) then as an additional security precaution this can be set to restrict the origins of the XML/JSON data that it sends.

4. Enter the URL of a domain in **Allow origins**.
5. To allow to keep connections on the SSO API open across multiple requests enable the **Allow persistent connections**.

d. Click **Save**.

5. In the **General Settings**, do the following:
   a. Select the **Enable SSO 3rd-Party API** option. This option is disabled by default.
   b. Select the **Use the HTTPS Management port** option. This option is enabled by default.
   c. Enter the **HTTPS port number** field. The default is 444.
6. Click **Save**.

Capture Client

The **Capture Client** allows the users of endpoints to automatically authenticate the user of a browser directly with no SSO agent involvement.

You can access the Endpoint Security Configurations from the **Policy** > **Endpoint Security** > **Settings** page.

1. Navigate to the **Device > Users > Settings > Authentication** page.
2. Next to **Configure SSO**, click **Configure**.
   The **SSO Configuration** page is displayed.
3. Click the **Capture Client** tab.
4. Select the **Enable SSO via Endpoint Security** option.
5. Click **Save**.

Test

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

You can 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.

1. Navigate to the **Device > Users > Settings > Authentication** page.
2. Next to **Configure SSO**, click **Configure**.
   The **SSO Configuration** page is displayed.
3. Under the **Test** tab, select the following:
   a. Select the SSO agent or TSA to test from the **Select agent to test** drop-down menu.
   b. In **Test** select one of the following:
      - **Check agent connectivity**:This tests communication with the authentication agent. If the firewall can connect to the SSO agent, the message Agent is ready displays.
      - **Check user**: enter the IP address of a workstation in the **Workstation IP address** field and select one of the following:

- **From other mechanisms**
- **Via NetAPI/WMI**
- **Allow Both**

c. Click **Test**.

This tests if the SSO agent is properly configured to identify the user logged into a workstation.

One-Time Password Settings

To configure the one-time password settings:

1. Navigate to **Device > Users > Settings > Authentication**.
2. Select **Enforce password complexity for One-Time Password** to meet complexity requirements of the one-time password.
3. For the **One-time password Email format**, choose an email format for :
   - **Plain Text**
   - **HTML**
4. For the **One-time Password Format**, select the password format:
   - **Characters**
   - **Characters + Numbers**
   - **Numbers**
5. In the **One-time Password Length** beginning and ending fields, enter the minimum and maximum length of the password. The length must be between 4-14 characters. The default for both fields is 10 characters.
6. Click **Accept**.

Configuring the User Web Login Settings

Topics:

Setting the Timeout for the Authentication Page

While the login authentication page is displayed, it uses system resources. By setting a limit on how long a login can take before the login page is closed, you free up those resources.

To set the timeout for the Authentication Page:

1. Navigate to **Device > Users > Settings > Web Login**.
2. In the **Show user authentication page for (minutes)** field, enter the number of minutes that users have to log in with their username and password before the login page times out. If it times out, a message displays informing them what they must do before attempting to log in again. The default time is **1** minute.
3. Click **Accept**.

Setting How the Browser is Redirected

To set how the browser is redirected:

1. Navigate to **Device > Users > Settings > Web Login**.
2. From **Redirect the browser to this appliance via**, choose one of the following options to determine how a user's browser is initially redirected to the SonicWall appliance's Web server:
    - **The interface IP address** – Select this to redirect the browser to the IP address of the appliance Web server interface. This option is selected by default.
    - **Its domain name from a reverse DNS lookup of the interface IP address** – When clicked, displays the appliance Web server's Interface, IP Address, DNS Name, and TTL (in seconds). This option is not selected by default.
    - **Its configured domain name** – Select to enable redirecting to a domain name configured on the **System > Administration** page.

      ⓘ **NOTE:** This option is available only if a domain name has been specified on the **System > Administration** page. Otherwise, this option is dimmed. To enable redirection to a configured domain name, set the firewall's domain name on the **System > Administration** page. Redirection is allowed when an imported certificate has been selected for HTTPS web management of that page.
    - **The name from the administration certificate** – Select to enable redirecting to a configured domain name with a properly signed certificate. Redirecting to the name from this administration certificate is allowed when an imported certificate has been selected for HTTPS web management on that page.

      ⓘ **NOTE:** This option is available only if a certificate has been imported for HTTPS management in the **Web Management Settings** section of the **System > Administration** page. Otherwise, this option is dimmed.

      ⓘ **TIP:** If you are using imported administration certificates, use this option. If you are not going to use an administration certificate, select **Its configured domain name**.

To do HTTPS management without the browser displaying invalid-certificate warnings, you need to import a certificate properly signed by a certification authority (administration certificate) rather than use the internally generated self-signed one. This certificate must be generated for the appliance and its host domain name. A properly signed certificate is the best way to obtain an appliance's domain name.

If you use an administration certificate, then to avoid certificate warnings, the browser needs to redirect to that domain name rather than to the IP address. For example, if you browse the internet and are redirected to log in at `https://gateway.SonicWall.com/auth.html`, the administration certificate on the appliance says that the appliance really is `gateway.sonicwall.com`, so the browser displays the login page. If you are redirected to `https://10.0.02/auth.html`, however, even though the certificate says it is `gateway.sonicwall.com`, the browser has no way to tell if that is correct, so it displays a certificate warning instead.

3. Click **Accept**.

Managing Redirections to the Login Page

Limiting redirections prevents possibly overloading the SonicWall appliances' web server by limiting redirections to the login page should HTTP/HTTPS connections that would otherwise get redirected there be repeatedly opened at a high rate from some unauthorized users.

To manage redirections to the login page:

1. Navigate to **Device > Users > Settings > Web Login**.
2. In the **Redirect users to the login page** field, select any of the following:
   - **Via an informatory intermediate page**: redirect to informatory page first, and then go to the login page.
   - **Directly**: If you experience high core CPU load, select **Directly**.
3. Click **Accept**.

Redirecting Unauthenticated Users

You can can redirect HTTP/HTTPS traffic from unauthenticated users to a specified URL instead of the SonicWall's own login page.

To redirect HTTP/HTTPS traffic from unauthenticated users:

1. Select **On redirecting unauthenticated users, redirect to an external login page**. This option allows users to be authenticated by an external authentication system. This option is not selected by default.

   TIP: To allow only unauthenticated users to be redirected, you need to create one or more access rules for this situation.

   NOTE: The external system can subsequently use the SSO third-party API or RADIUS Accounting to pass the user's name and credentials to the firewall so they are identified for such activities as access control and logging.

2. When you select this option, the **URL** field displays. Enter the URL for redirection in the field.
3. To authenticate multiple IP address see Authenticating user's multiple IP addresses
4. Select **Allow an SSO login notification to log out and replace a web user session** regarding how to handle user sessions in relation to SSO logins. When a user logs in via SSO, it can trigger a logout of any existing web sessions and then establish a new session with the SSO credentials.
    - Always- Select to trigger a logout of any existing web session and then establish a new session with the SSO credentials.
    - When Not Managing: Select this option if the SSO behavior should only apply when the user is not actively managing sessions or accounts.
    - Never- Select when the SSO login should not log out or replace any existing session under any circumstances.
5. To configure options related to the captive portal configured in a zone's guest settings, scroll to **Web Login Settings for Guest Captive Portal**.
6. For captive portal guest authentication, to allow the authentication page to show in a portal host page as a frame, select **Allow authentication page in frame**. This option is not selected by default.
7. Click **Accept**.

Authenticating user's multiple IP addresses

You can authenticate user's multiple IP addresses (IPv4/IPv6) simentaniously via web login. When a user has logs in using IPv4, enabling **Authenticate user's other IP(v4/v6) addresses if possible** there is no need to perform an additional login when navigating to an IPv6 site.

To authenticate multiple IP address:

1. Navigate to **Device > Users > Settings > Web Login**.
2. Select **Authenticate user's other IP(v4/v6) addresses if possible**. This option is not selected by default.
3. Only on selecting **Authenticate user's other IP(v4/v6) addresses if possible** you can select **Use HTTP to initiate combined logins** to enforce HTTP for the combined login requests instead of the protocol used by the accessed login page.
4. Click **Accept**.

Adding URLs to Authentication Bypass

SonicOS Guest Services allows guest users to have access through your network directly to the Internet without access to your protected network. To do this, SonicOS uses the IP address of the user's computer.

Using the IP address as the identifier is useful when guest user traffic passes through a network router, as this changes the source MAC address to that of the router. However, the user's IP address passes through unchanged.

If only the MAC address is used for identification, two clients behind the same router have the same MAC address upon reaching the network security appliance. When one client gets authenticated, the traffic from the other client is also treated as authenticated and bypasses the guest service authentication.

By using the client IP address for identification, all guest clients behind the routed device are required to authenticate independently.

To add HTTP URLs user authentication bypass in Access Rules:

1. Navigate to **Device > Users > Settings > Authentication Bypass**.
2. Click **Add**. The **Add URL** page displays.
3. In the **Add URL** field, enter the URL.
4. Click **Add**. A change order pop-up confirmation displays.
5. Click **OK**.
6. Click **Accept**.

User Session Settings

These settings apply to all users when authenticated through your SonicWall network security appliance.

To configure settings that apply to all users who are authenticated through the firewall:

1. Navigate to **Device > Users > Settings > User Sessions**.
2. In the **Inactivity timeout (minutes)** field, specify the length of time for inactivity after which users are logged out of the firewall. The default is **15** minutes.
3. From **Don't allow traffic from these services to prevent user logout on inactivity**, select the service or service group option to be prevented from logging out inactive users. This option saves system overhead and possible delays re-identifying aged-out authenticated users by making them inactive instead of logging them out. Inactive users do not use up system resources and can be displayed on the **Users > Status** page. The default is **None**.
4. For the following **For logging of connections on which the user is not identified** options, choose the type of logging, **Log no user name** or **Log user name**, to be done, and, optionally, the log user name:
    - **If SSO fails to identify the user: Log user name Unknown SSO failed** (default)
    - **For connections that bypass SSO: Log user name SSO Bypass** (default)

      ⓘ **NOTE:** This option also can be set in the **SSO Bypass** section of the **Enforcement of the SSO Authentication Configuration** dialog.
    - **For connections originating externally**: **Log no user name** (default). If **Log user name** is selected, the default user name is **Unknown (external)**.
    - **For other unidentified connects**: **Log no user name** (default). If **Log user name** is selected, the default user name is **Unknown**.

5. Specify how to handle a user's connections that remain after the user logs out from the SonicWall appliance with the Actions for remaining user connections on logout options.

	Action	
Type of logout	**For connections requiring user authentication 1**	**For other connections 2**
On logout due to inactivity	• Leave them alive (default) • Terminate them • Terminate after… minutes	• Leave them alive (default) • Terminate them • Terminate after… minutes
On active/reported logout	• Leave them alive • Terminate them (default) • Terminate after… minutes	• Leave them alive • Terminate them • Terminate after… 15 minutes (default)

1. Applies for connections through access rules that allow only specific users.
2. Applies for other connections that do not have a specific user authentication requirement.

You can set different actions for:

- Inactivity logout, where the user might or might not still be logged into the domain/computer.
- Users actively logging themselves out or being reported to the SonicWall network security appliance as being logged out (the latter normally means that the user has logged out from the domain/user).

6. Click **Accept**.

Topics:

- User Session Settings for SSO-Authenticated Users
- User Session Settings for Web Login

User Session Settings for SSO-Authenticated Users

To specify how inactive SSO-authenticated users are handled:

1. Navigate to **Device > Users > Settings > User Sessions**.
2. To put a user identified to the SonicWall network security appliance through an SSO mechanism, but no traffic has yet been received from the user, into an inactive state so they do not use resources, select **On being notified of a login make the user initially inactive until they send traffic**. The users remain in an inactive state until traffic is received. This option is selected by default.

   Some SSO mechanisms do not give any way for the SonicWall network security appliance to actively re-identify a user, and if users identified by such a mechanism do not send traffic, they remain in the inactive state until the appliance eventually receives a logout notification for the user. For other users who can be

re-identified, if they stay inactive and do not send traffic, they are aged-out and removed after a period (see the paragraphs that follow).

3. If an SSO-identified user who has been actively logged in is timed out because of inactivity, then users who cannot be re-identified are returned to an inactive state. To have users who would otherwise be logged out on inactivity to be returned to an inactive state, select **On inactivity timeout make all user inactive instead of logged out**. Doing this avoids overhead and possible delays re-identifying the users when they become active again. This setting is selected by default.
4. For inactive users who are subject to getting aged out, you can set the time, in minutes, after which they are aged-out and removed if they stay inactive and do not send traffic by selecting **Age out inactive users after (minutes)** and specifying the timeout in the field. This setting is selected by default, and the minimum timeout value is 10 minutes, the maximum is 10000 minutes, and the default is **60** minutes.

   ⓘ **NOTE:** As the reason for keeping inactive user separate from active users is to minimize the resources used to manage them, the age-out timer runs once every 10 minutes. It might, therefore, take up to 10 minutes longer to remove inactive users from active status.
5. Click **Accept**.

User Session Settings for Web Login

To configure user session settings for web login:

1. Navigate to **Device > Users > Settings > User Sessions**.
2. **Enable login session limit for web logins**: Limit the time a user is logged into the firewall through web login before the login page times out by selecting this option and typing the amount of time, in minutes, in the **Login session limit … Minutes** field. This setting is selected by default The default value is **30** minutes.

   If the session times out, a message displays that reads you must log out before attempting to log in again.

   Select **Show user login status window** to display a status window during the user's session. This option is not selected by default.

   ⓘ **NOTE:** The window must be kept open throughout the user's session as closing it logs the user out.

   ⓘ **IMPORTANT:** If this option is not enabled, the status window is not displayed and users might not be able to log out. In this case, a login session limit must be set to ensure that they do eventually get logged out.

   The **User Login Status window refreshes every (minutes)** displays the number of minutes the user has left in the login session. The user can set the remaining time to a smaller number of minutes by entering the number and clicking **Update**.

   When this option is enabled, a mechanism that monitors heartbeats sent from that window also can be enabled to detect and log out users who disconnect without logging out.
3. **IMPORTANT:** If this option is not enabled, users might be unable to log out. Set a login session limit to ensure users are logged out eventually.
4. In the **User's login status window sends status heartbeat every … Seconds** field, specify how often a heartbeat is sent back to your SonicWall network security appliance. This heartbeat notifies your

SonicWall network security appliance of your connection status and continues to be sent as long at the status window is open. The default is **120** seconds.

5. Select **Enable disconnected user detection** to have your SonicWall network security appliance detect when the user's connection is no longer valid and then end the session. This option is already selected by default.
6. In the **Timeout on heartbeat from user's login status window … Minutes** field, specify the time needed without a reply from the heartbeat before ending the user session. The minimum delay before ending the user session is 1 minute, the maximum is 65535 minutes, and the default is **10** minutes.
7. Select **Open user's login status window in the same window rather than in a popup** if you do not want the login status window to open as a separate pop-up window. This option is not selected by default.
8. Click **Accept**.

Accounting

SonicOS supports both RADIUS accounting and TACACS+ accounting. If both a RADIUS server and a TACACS+ server are configured, a user's accounting messages are sent to both servers.

Topics:

- Configuring RADIUS Accounting
- Configuring TACACS+ Accounting

Configuring RADIUS Accounting

Topics:

- Sending RADIUS Accounting Information to Servers
- Configuring User Accounting
- Testing RADIUS Accounting
- Editing RADIUS Servers
- Deleting RADIUS Servers

Sending RADIUS Accounting Information to Servers

To send RADIUS accounting information to servers:

1. Navigate to **Device > Users > Settings > Accounting**.
2. Next to **RADIUS Accounting**, click **Configure**.

3. To add a RADIUS server:
    a. Click **Add Server**. The **Settings** page displays.
    b. In the **Host Name or IP Address** field, enter the host name or IP address .
    c. In the **Port** field, enter the port number.
    d. In the **Shared Secret** and **Confirm Shared Secret** fields, enter the shared secret.
    e. On the **Advanced** tab, from the **User Name Format** list, select the username format:
        - **Simple-Name**
        - **Name@Domain**
        - **Domain\Name**
        - **Name.Domain**
    f. Click **Save**. The RADIUS Accounting table is updated.

    For each RADIUS server you want to add, repeat these steps.
4. Click on **General Settings**.
5. In the **RADIUS Accounting Server Timeout (seconds)** field, enter a maximum time out, in seconds, . The default value is **5** seconds.
6. In the **Retries** field, enter the maximum number of retries. The default value is **3** retries.
7. To send accounting data to all servers listed in the RADIUS Accounting table, select **Send accounting data to all servers**.
8. Click **Accept**.

Configuring User Accounting

To configure user accounting for RADIUS:

1. Select one or more types of users.
    - **Users authenticated by web login**
    - **Remote client users**
    - **Guest users**
2. Select the **SSO-authenticated users** field to enable **Include SSO users identified via RADIUS Accounting?**.
3. From the **Include** list, select which users should be included:
    - **Domain users**
    - **Local users**
    - **Domain and local users**
4. Select **Send interim updates** to send interim updates.

Testing RADIUS Accounting

To test RADIUS accounting:

1. Navigate to **Device > Users > Settings > Accounting**.
2. Next to **RADIUS Accounting**, click **Configure**.
3. Click the **Test** tab.
4. From the **Select server to test** list, select which RADIUS server you want to test.
5. From the **Test** list, select the functionality you want to test:
   - **Connectivity**
   - **User Accounting**: enter the **User** and **IP Address**
6. Click **Test**.

   The **Test Status** is update and any user attributes returned will be displayed in **Returned User Attributes**.

Editing RADIUS Servers

To edit a RADIUS server:

1. Navigate to **Device > Users > Settings > Accounting**.
2. Next to **RADIUS Accounting**, click **Configure**.
3. Select the Radius server and click the **Edit** icon for the RADIUS server you want to edit. The **Shared Secret** and **Confirm Shared Secret** fields are dimmed and cannot be changed.
4. Make any changes you need.
5. Click **Save**.

Deleting RADIUS Servers

To delete a single server:

1. Navigate to **Device > Users > Settings > Accounting**.
2. Next to **RADIUS Accounting**, click **Configure**.
3. Hover over the far right on the row for the server you want to delete until the icons appear. Click the **Delete** icon. A confirmation message displays.
4. Click **Confirm**.
5. Click **Update**.

To delete one or more servers:

1. Navigate to **Device > Users > Settings > Accounting**.
2. Next to **RADIUS Accounting**, click **Configure**.
3. Select the servers in the RADIUS Accounting table you want to delete.
4. Click **Delete**. A confirmation message displays.
5. Click **Confirm**.

6. Click **Update**.

Configuring TACACS+ Accounting

SonicOS supports TACACS+ accounting Start, Watchdog and Stop messages, but not the TACACS+ accounting proxy, that is, SonicOS does not forward the accounting request to the accounting server.

To configure TACACS+ accounting:

1. Navigate to **Device > Users > Settings**.
2. Click **Accounting**.
3. Nex to **TACACS+ Accounting**, click **Configure**.
4. In the **Settings** tab click **Add Server**.
    a. Enter the **Host Name or IP Address** of the TACACS+ server.
    b. Enter the port number of the server in the **Port** field. The default is 49.
    c. Enter the shared secret in the **Shared Secret** and **Confirm Shared Secret** fields.
    d. Click **Save**.
5. Click on **General Settings**.
    a. In the **TACACS+ Server Timeout (seconds)** field, enter a maximum time out, in seconds, . The default value is **5** seconds.
    b. In the **Retries** field, enter the maximum number of retries. The default value is **3** retries.
6. To support single connect, select **Support Single Connect**. This option is not selected by default.
7. To allow encrypted packets, select **Packet Encrypted**. This option is selected by default.
8. Click **Save**.

Configuring User Accounting

To configure user accounting for TACACS:

1. Navigate to **Device > Users > Settings**.
2. Click **Accounting**.
3. Nex to **TACACS+ Accounting**, click **Configure**.
4. Navigate to **User Accounting** tab.
5. Select one or more types of users.
    - **Users authenticated by web login**
    - **Remote client users**
    - **Guest users**

6. Select the **SSO-authenticated users** field to enable **Include SSO users identified via RADIUS Accounting?**.
7. From the **Include** list, select which users should be included:
    - **Domain users**
    - **Local users**
    - **Domain and local users**
8. Select **Send Watchdog Messages**. This option is not selected by default. After selecting this option, enter for **Every** minutes indicating how often you would like to receive watchdog messages.
9. Click **Save**.

Testing TACACS Accounting

To test TACACS accounting:

1. Navigate to **Device > Users > Settings > Accounting**.
2. Next to **TACACS+Accounting**, click **Configure**.
3. Click the **Test** tab.
4. From the **Select server to test** list, select which server you want to test.
5. Next to **Test Connectivity**, click **Test**.
   The **Test Status** is update and any user attributes returned will be displayed in **Returned User Attributes**.

Editing TACACS+ Servers

To edit a TACACS+ server:

1. Navigate to **Device > Users > Settings > Accounting**.
2. Next to **TACACS Accounting**, click **Configure**.
3. Select the server and click the **Edit** icon for the server you want to edit.
4. Make any changes you need.
5. Click **Save**.

Deleting TACACS Servers

To delete a single server:

1. Navigate to **Device > Users > Settings > Accounting**.
2. Next to **TACACS Accounting**, click **Configure**.
3. Hover over the far right on the row for the server you want to delete until the icons appear. Click the **Delete** icon. A confirmation message displays.
4. Click **Confirm**.
5. Click **Update**.

To delete one or more servers:

1. Navigate to **Device > Users > Settings > Accounting**.
2. Next to **TACACS Accounting**, click **Configure**.
3. Select the servers in the TACACS Accounting table you want to delete.
4. Click **Delete**. A confirmation message displays.
5. Click **Confirm**.
6. Click **Update**.

Post-Login Acceptable Use Policy Example Template

Click **Example Template** to populate the content with the default acceptable use policy (AUP) template, which you can modify:

```
<font face=arial size=3>
<center><b><i>Welcome to the SonicWall</center></b></i>
<font size=2>
<table width="100%" border="1">
<tr><td>
<font size=2>
<br><br><br>
<center>Enter your usage policy terms here.
<br><br><br>
</td></tr>
</table>
Click "I Accept" only if you wish to accept these terms and continue, or otherwise
select "Cancel".
```

Post-Login Acceptable Use Policy Preview Message

Click **Preview** to display your acceptable use policy (AUP) message as it appears to the user.

5

Configuring Local Users and Groups

Topics:

About Authentication and Passwords

Topics:

Using Two-Factor Authentication

Many user login authentication require one-time passwords (OTP). SonicOS provides authentication through:

- One-Time Password (OTP) sent to the user by email
- Time-Based One-Time Password (TOTP) authentication using an authenticator application

  To use this feature:

  - Users must download a TOTP client app (such as Google Authenticator, DUO, or Microsoft Authenticator) on their mobile device.
  - You must select **TOTP** from the **One-time password method** list on the **User Settings** page.

Enforcing First Login Password Change

SonicOS allows you to force users to change their password before their first login when you create or edit a local user. You can specify the login password change for users or for groups.

Configuring Local Users

Local users are users stored and managed on the SonicWall network security appliance's local database. In **Device > Users > Local Users & Groups**, you can view and manage all local users, add new local users, and edit existing local users. You can also import users from your LDAP server.

Check box	Used to select individual local users.
Expand/Collapse icons	By default, only the local user's username is listed. Clicking the Expand icon displays the groups to which the local user belongs.
Name	Lists the username of the local user; when expanded lists the name(s) of the groups to which the local user belongs.
Guest Services	Indicates with a green checkmark icon whether guest services is active for the local user.
Admin	Displays the type of administration capabilities available to the local user.
VPN Access	Displays a **Comment** icon for each local user and each group to which the local user is a member. Mousing over the icon displays the status of the local group's VPN access and that of each member of the group.
Comments	Displays a **Comment** icon for each local user and each group to which the local user is a member. Hovering over on the icon displays the comment entered when the local user or group was configured or edited.
UUID	Displays a alphanumeric label for the connected device.
Quota	For each local user, displays a **Statistics** icon. Mousing over the icon displays any usage quota for the local user.
Configure	Hovering over the each local user, displays the **Edit** and **Delete** icons. If an icon is dimmed or otherwise disabled, that function is not available for that local user or local group.

For information about authentication and two-factor passwords, refer to About Authentication and Passwords.

Topics:

- Quota Control for all Users
- Viewing Local Users
- Adding Local Users
- Editing Local Users

Quota Control for all Users

The quota control for users feature provides quota control based on the user's account. The quota can be specified as a session lifetime, or a transmit and/or receive traffic limit. With a cyclic quota, a user can not access

the Internet upon meeting the account quota until the next cycle (day, week, or month) begins. If the quota cycle is **Non Cyclic**, the user is unable to access the Internet upon meeting the quota.

Viewing Local Users

You can view all the groups to which a user belongs on **Device > Users > Local Users & Groups**. Click on the **Expand** icon next to a user to view the group memberships for that user.

The columns to the right of the user's name list the privileges that the user has. In the expanded view, it displays which group the user gets each privilege from.

To:

- View the network resources to which the user has VPN access, hover the mouse pointer over the **Comment** icon in the user's **VPN Access** column.
- View the quota for the user, hover the mouse over the **Statistics** icon in the **Quota** column
- Remove the user from a group, in the expanded view, click the **Remove** icon in the user's **Configure** column.

  ⓘ | **NOTE:** If the user cannot be deleted from a group, the icon is dimmed.
- Edit the user, click the **Edit** icon in the user's **Configure** column. Refer to Editing Local Users for more information.
- Delete the user or group in that row, click the **Delete** icon in the user's **Configure** column.

  ⓘ | **NOTE:** If the local user cannot be deleted from a group, the icon is dimmed.

The bottom of the **Device > Users > Local Users & Groups** page displays the total number of local users:

Adding Local Users

You can add local users to the internal database on the network security appliance from the **Device > Users > Local Users & Groups** page.

ⓘ | **NOTE:** To create a user for an SSL VPN client, refer to SonicOS 8 SSL VPN Administration Guide.

Topics:

- Configuring Local Users Settings
- Configuring Local Users Groups
- Configuring Local Users VPN Access
- Configuring Local Users User Quota

Configuring Local Users Settings

You can add local users to the internal database on the network security appliance from the **Device > Users > Local Users & Groups** page.

NOTE: To create a user for an SSL VPN client, refer to SonicOS 8 SSL VPN Administration Guide.

To add local users to the database:

1. Navigate to **Device > Users > Local Users & Groups**.
2. Click the **Add User**.
3. The **User Settings** select **Settings** tab.
4. Select **This represents a domain user** if:
   - If **This represents a domain user** is enabled then any group memberships, access rights, etc. that are set using this user object will apply for users who log in using the named domain account (authenticated via RADIUS or LDAP) or who are identified as that domain user by SSO. When it is checked you can then choose to have it apply for the named user account in a specific domain, or for a user with the given name in any domain.
   - If This represents a domain user is not checked, then it is a local account and anything that is set using it will apply only for users who log in using it, authenticated locally (a password must be set here for this case).
5. In the **Name** field, enter the name associated with the user.
6. In the **Password** and **Confirm Password** fields, enter the password assigned to the user.
7. Optional: select **User must change password** to force users to change their passwords the first time they login. This option is not selected by default.
8. From the **One-time password method** list, select the method to require SSL VPN users to submit a system-generated password for two-factor authentication:

   TIP: When a Local User does not have a one-time password enabled, while a group it belongs to does, ensure the user's email address is configured, otherwise this user cannot login.

   TIP: To avoid another password change request for this user, this option applies only to the first login.

   - **Disabled** (default) – If **User must change password** is selected, a dialog to change it displays at the first login attempt.
   - **OTP via Mail** – Users receive a temporary password by email after they enter their user name and first password. After receiving the password-containing email, they can enter the second password to complete the login process.
   - **TOTP** – Users receive a temporary password by email after they input their user name and first password, but to use this feature, users must download a TOTP client app (such as Google Authentication, DUO, or Microsoft Authentication) on their mobile device.

     The **unbind totp key** displays.
9. In the **E-mail Address** field, enter the user's email address so they can receive one-time passwords.
10. In **Account Lifetime**, select **Never expires** to make the account permanently. Or select **Minutes**, **Hours**, or **Days** to specify a lifetime after which the user account will either be deleted or disabled.
11. Optional: In the **Comment** field, enter any comments.
12. Click **Save**.

Configuring Local Users Groups

To a user to groups:

1. Navigate to the **Device > Users > Local Users** page.
2. Click **Add User**.
3. In **User Settings** click on the **Groups** tab.
4. From the **Available User Groups** list, select the groups(s) in which this user should be included.
5. Click the **Add** (right arrow) icon to add the user to the **Selected User Groups** list.

   To remove resource(s), from the **Selected User User Groups** list, select the group(s) and click the **Remove** (left arrow) icon. To remove the user from all of the groups, click the **Remove All** (double left arrow) icon.

Configuring Local Users VPN Access

To configure VPN access for local users:

1. Navigate to the **Device > Users > Local Users** page.
2. Click **Add User**.
3. In **User Settings** click on the **VPN Access** tab.
4. From the **Available Networks** list, select the network resource(s) to which this user has VPN Access by default.

   ⓘ | **NOTE:** Group VPN access settings affect remote clients and SSL VPN Virtual Office bookmarks.
5. Click the **Add** (right arrow) icon to add the resource(s) to the **Selected Networks** list.

   To remove resource(s), from the **Selected Networks** list, select the resource(s) and click the **Remove** (left arrow) icon. To remove resources, click the **Remove All** (double left arrow) icon.

Configuring Local Users User Quota

To configure the quota for the user:

1. Navigate to **Device >Users > Local Users & Groups**.
2. Click **Add User**.
3. In **User Settings** click on the **User Quota** tab.
4. From the **Quota cycle type setting** list, select:
   - **Non Cyclic** (default)
   - **Per Day**

- **Per Week**
- **Per Month**

5. From the **Session Lifetime** list, specify the duration for how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account.
6. From the Session Lifetime list, and select the type of duration:
    - Minutes
    - Hours
    - Days
7. In the **Minutes/Hours/Days** field, specify the duration. You can enter a value from 1 to 9999.
8. In the **Receive Limit** field, enter the amount (in MB) the amount of data the user can receive. The range is from 0 (no data can be received) to 999999999 MB to Unlimited (default).
9. In the **Transmit Limit** field, enter the amount (in MB) of data the user can send. The range is from 0 (no data can be sent) to 999999999 MB to Unlimited (default).
10. Click **Save**.

Topics:

- Quota Control for all Users

Editing Local Users

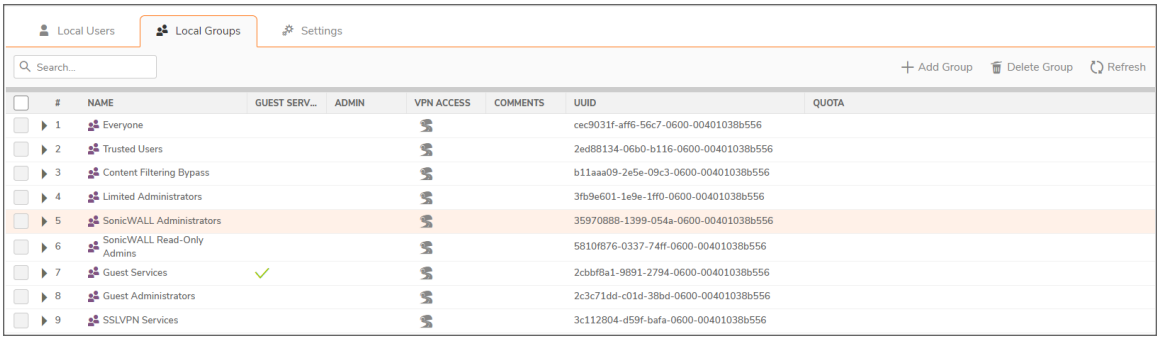
You can edit local users from the **Device > Users > Local Users & Groups** page.

To edit a local user:

1. In the **Local Users** table, hover over the user and click the **Edit** icon. The **User Settings** page displays.
2. Configure the **Settings**, **Groups**, **VPN Access**, and **User Quota** options exactly as when adding a new user. Refer to Adding Local Users for more information.
3. In the **Local Users** table, hover over the user and click the **Edit Bookmark Settings** to configure the user bookmarks.

Configuring Local Groups

Local groups are displayed in the **Local Groups** table. Certain local groups are default groups that can be modified, but not deleted.



Checkbox	Used to select individual local groups. Default local groups cannot be changed, and, therefore, their checkboxes are dimmed.
Expand/Collapse icons	By default, only the local group's name is listed. Clicking the: • **Expand** icon expands the listing to show all members of the group. If the local group does not have any members, the words, No Members, appears under that group's listing. • **Collapse** icon hides the local group's membership.
Name	Lists both the default and configured local groups by name. If the **Enable Multiple Administrator Role** option has been enabled on the **System > Administration** page, the **Device > Users > Local Groups** page lists these default role-based administrator groups: • System Administrators • Cryptographic Administrators • Audit Administrators
Bypass content filters	Indicates with a green checkmark icon whether content filtering is bypassed for the local group. Mousing over the icon displays a tooltip. For remote users, a **Comment** icon displays `Not applicable with remote authentication`.
Guest Services	Indicates with a green checkmark icon whether guest services is active for the local group. Mousing over the icon displays a tooltip. For remote users, a **Comment** icon displays `Not applicable with remote authentication`.
Admin	Displays the type of administration capabilities available to the local group. Mousing over the icon displays a tooltip regarding the listed capability. For remote users, a **Comment** icon displays `Not applicable with remote authentication`.
VPN Access	Displays a **Comment** icon for each group and each member of the group. Mousing over the icon displays the status of the local group's VPN access and that of each member of the group.
Comments	Lists any comment provided for the local group.

UUID	Lists the UUID for the connected device.
Quota	Displays the usage quota assigned to that group.
Configure	Displays the **Edit** and **Delete** icons for each local group and group member, and for group members, a **Remove** icon. If an icon is dimmed, that function is not available for that local group or group member.

Topics:

- Adding Local Groups
- Editing Local Groups

Adding Local Groups

Topics:

- Configuring Local Groups Settings
- Configuring Local Group Settings Members
- Configuring Local Group Settings VPN Access
- Configuring Local Group Settings Administration

Configuring Local Groups Settings

To add or edit a group:

1. Navigate to the **Device > Users > Local Groups** page.
2. Click **Add Group**.
3. In the **Membership Settings** select any one of the following:
    - **This can match a domain user group**
    - **Members are set locally only**
    - **Memberships are set by the user's location in the LDAP directory**
4. In the **Name** field, enter a name for the new local group.
   ⓘ | **NOTE:** The name of a predefined user or group cannot be edited and the field is dimmed.
5. In the **Domain Name** field, enter the domain name.
6. In the **Domain** field, select **Any** or **Select Domain**.
   ⓘ | **NOTE:** If you enter a domain name that is not listed, you must enter the full domain name or an error message is displayed.
7. Optionally, in the **Comment** field enter a comment about the local group .
8. Optionally, select Memberships are set by user's location in the LDAP directory checkbox. If this setting is enabled, when users log in or are identified through SSO, if their user object on the LDAP server is at the

location specified in LDAP Location (or under it if appropriate), they are given membership to this user group for the session. This setting is disabled by default.

ⓘ **TIP:** Local users and other groups also can be made members of the group on the Members view.

If you enable this setting, the **LDAP Location** field becomes active.

a. In the **LDAP Location** field, enter the location in the LDAP directory tree. The location can be given as a path (for example, domain.com/users) or as an LDAP distinguished name.

ⓘ **NOTE:** If LDAP user group mirroring is enabled, then for mirror user groups this field is read-only and displays the location in the LDAP directory of the mirrored group.

b. Select precisely where the location is from one of the **For Users** options:

- **at or under the given location** (default)
- **at the given location**

9. Optionally, to require one-time passwords for the group, select **One-time passwords**. If you enable this setting, users must have their email addresses set.
10. Click **Update**.

Configuring Local Group Settings Members

To configure members for local groups:

1. Navigate to the **Device > Users > Local Groups** page.
2. Click **Add Group**.
3. Click the **Members** tab.
4. In the **Available User Groups** list, select the members or groups that belong to this group and click the **Add** (right arrow) icon.

   Click the **Add All** icon (double right arrow) to add all users and groups.

   ⓘ **NOTE:** You can add any group as a member of another group except **Everybody** and **All LDAP Users**. Be aware of the membership of the groups you add as members of another group.

   To remove users and/or groups from the **Selected User Groups** list, select the user(s) and/or group(s) and click the **Remove** (left arrow) icon. To remove all users and groups, click the **Remove All** (double left arrow) icon.
5. Click **Save**.

Configuring Local Group Settings VPN Access

To configure VPN access for local groups:

1. Navigate to the **Device > Users > Local Groups** page.
2. Click **Add Group**.
3. In **Add Group Settings > VPN Access**, from the **Available Networks** list, select the network resource (s) to which this group has VPN Access by default.

ⓘ | **NOTE:** Group VPN access settings affect remote clients and SSL VPN Virtual Office bookmarks.

4. Click the **Add** (right arrow) icon to add the resource(s) to the **Selected Networks** list.
   To remove resource(s), from the **Selected Networks** list, select the resource(s) and click the **Remove** (left arrow) icon. To remove resources, click the **Remove All** (double left arrow) icon.

Configuring Local Group Settings Administration

To configure administration for local groups:

1. Navigate to the **Device > Users > Local Groups** page.
2. Click **Add Group**.
3. Click on the **Administration** tab.
4. If the new group is to be made an administrative group by giving it membership in another administrative group, select **Members go straight to the management UI on web login**. This option is not selected by default.
5. Enable **Number of concurrent sessions** and enter the maximum number of users who can log in simultaneously without needing to log out and back in.
6. The **If this group will give read-only administration and is used with other administrative groups** options control what happens when users start with membership in a user group that gives read-only administration (that is, the SonicWall Read-Only Admins group or one with membership in it) and then are added to other administrative user groups. To give users the:
   - Admin rights set by their other administrative groups with no read-only restriction, choose **The administrative rights from the other groups override this (no read-only restriction)**. This setting allows the read-only admin group to be the default for a set of users, but then overrides the default for selected users by making them members of other administrative groups so they can do configuration. This option is selected by default. In the Local Users table, the Admin column for the user displays the other group's designation, such as Ltd or "Full."
   - To give member users the administration level set by their other groups, but restrict them to read-only access, select **The administrative rights from the other groups will be restricted to read-only**. In the Local Users table, the Admin column for the user displays the dual designation, such as Rd-Only Ltd.

   ⓘ | **TIP:** To do a mix of both, select the first option for SonicWall Read-Only Admins, and then create another group that is a member of this group, but that has the second option selected (but not vice versa).

   ⓘ | **NOTE:** If a user is a member of a read-only admin group and has membership in no other administrative groups, then that member gets full-level access (as per SonicWall Administrators) restricted to read-only.
7. Click **Save**.

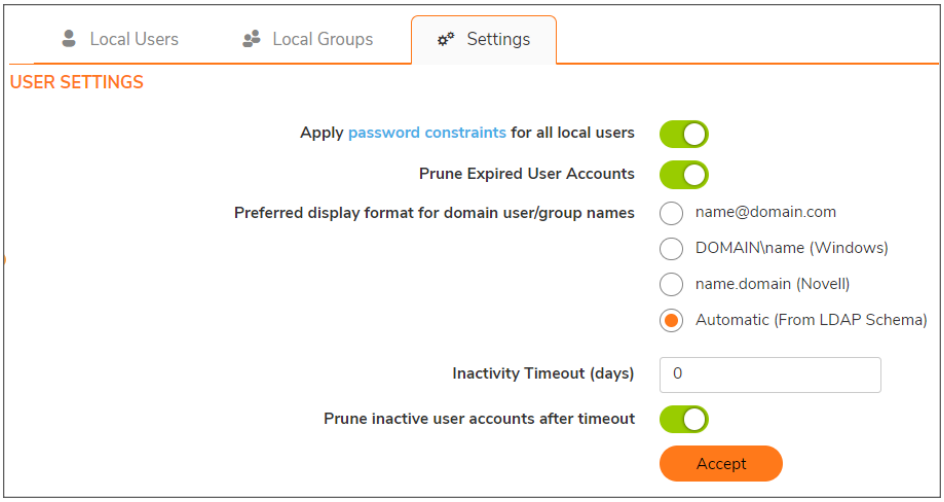
Editing Local Groups

To edit a local group:

1. Navigate to **Device > Users > Local Groups**.
2. Click the **Edit User Group** icon in the **Configuration** column for the group that you want to edit. The **Local Group Settings** dialog displays.
3. Follow the steps in Adding Local Groups.

Configuring Settings

In **Device > Users > Local Users and Groups**, you can configure user settings.



1. Select **Apply password constraints for all local users** to apply the password constraints that are specified on the **Users > Local Users** page to all local users.
2. Select **Prune Expired User Accounts** to delete a user account that is configured with a limited lifetime after the lifetime expires.
3. In **Preferred display format for domain user/group names** select any one of the following formats to specify an alternative login name of the user:
    - **name@domain.com**
    - **DOMAIN\name (Windows)**
    - **name.domain (Novell)**
    - **Automatic (From LDAP Schema)**

4. In **Inactivity Timeout (days)** enter the time in days to terminate if a user session is idle for certain amount of time.
5. Select **Prune inactive user accounts after timeout** to delete an inactive user account that is configured with a limited lifetime after the lifetime expires.
6. Click **Accept**.

6

Configuring Guest Services

Guest Services determine the limits and configuration of the guest accounts. Guest accounts are temporary accounts set up for users to log into your network.

You can create guest accounts manually as needed or generate them in batches. Guest accounts are typically limited to a predetermined lifespan. After their lifespan, by default, the accounts are removed.

Topics:

Adding Guest Profiles

To add a Guest Profile:

1. Navigate to the **Device > Users > Guest Services** page.
2. Check **Show guest login status window with logout** to display a user login window on the user's workstation whenever the user is logged in. Users must keep this window open during their login session. The window displays the time remaining in their current session. Users can log out by clicking **Logout** in the login status window.
3. Click **Add Guest Profile** below the **Guest Profiles** list to create a guest profile. The **Add Guest Profile** window displays.
4. In the **Add Guest Profile** window, configure these options:
    - **Profile Name:** Enter the name of the profile.
    - **User Name Prefix:** Enter the first part of every user account name generated from this profile.
    - **Auto-generate user name:** Check this to allow guest accounts generated from this profile to have an automatically generated user name. The user name is usually the prefix plus a two- or three-digit number.

- **Auto-generate password:** Check this to allow guest accounts generated from this profile to have an automatically generated password. The generated password is an eight-character unique alphabetic string.
- **Enable Account:** Check this for all guest accounts generated from this profile to be enabled upon creation.
- **Auto-Prune Account:** Check this to have the account removed from the database after its lifetime expires.
- **Enforce login uniqueness:** Check this to allow only a single instance of an account to be used at any one time. By default, this feature is enabled when creating a new guest account. If you want to allow multiple users to login with a single account, disable this enforcement by clearing **Enforce login uniqueness**.
- **Activate account upon first login:** To delay the Account Expiration timer until a user logs into the account for the first time, select **Activate Account Upon First Login**. This option is not selected by default.
- **Account Lifetime:** This setting defines how long an account remains on the security appliance before the account expires. You can specify from 1 to 9999 in the Account Lifetime field and select the type of duration from the drop-down menu:

  - Minutes
  - Hours
  - Days

  The default is 7 Days.

  If **Auto-Prune** is enabled, the account is deleted when it expires. If **Auto-Prune** is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation.
- **Idle Timeout:** Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** has not expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.

  You can specify from 1 to 9999 in the Account Lifetime field and select the type of duration from the drop-down menu:

  - Minutes
  - Hours
  - Days

  The default is **10 Minutes**.
- To specify the quota cycle type, select from the **Quota Cycle Type Setting** drop-down menu:

  - Non Cyclic (default)
  - Per Day
  - Per Week
  - Per Month

- **Session Lifetime:** Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. Alternatively, activation can occur at the time the account is created by clearing **Activate account upon first login**. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**.

  You can specify from 1 to 9999 in the **Session Lifetime** field and select the type of duration from the drop-down menu:

  - Minutes
  - Hours
  - Days

  The default is 1 Hours.
- To limit the amount of data the user can receive, enter the amount, in MB, in **Receive limit (0 to disable)** field. The range is from 0 (no data can be received) to 999999999 MB to **Unlimited** (default).
- To limit the amount of data the user can send, enter the amount, in MB, in **Transmit limit (0 to disable)** field. The range is from 0 (no data can be received) to 999999999 MB to **Unlimited** (default).
- **Comment:** Any text can be entered as a comment in the **Comment** field.

5. Click **Add** to add the profile.

Editing Guest Profiles

To edit guest profiles:

1. Click the **Edit** icon in the **Configure** column for the profile.
2. Follow the steps in Adding Guest Profiles.

Deleting Guest Profiles

You can delete all guest profiles, except the **Default** profile.

To delete guest profiles:

1. Select either:
   - The checkbox(es) of the guest profile(s) to be deleted.
   - The top left checkbox in the **Guest Profiles** table. All checkboxes (except for the **Default** profile) become selected.

   Delete **Guest Profile(s)** becomes active.
2. Click **Delete Guest Profile(s)**. A confirmation message displays.
3. Click **Update**.

7

Configuring Guest Accounts

Lists the guest services accounts configured on the SonicWall Security Appliance. You can enable or disable individual accounts, groups of accounts, or all accounts, as well as set the Auto-Prune feature for accounts, set an Account or Session Expiration date or time, and you can add, edit, delete, and print accounts.

Topics:

Adding Guest Accounts

To add a new guest account:

1. Navigate to the **Device > Users > Guest Accounts** page.
2. Under the list of guest accounts, click **Add Guest Account > Settings**.
3. Configure these parameters for the guest account:
    - **Profile:** Select the Guest Profile from which to generate this account.
    - **Name:** Enter a name for the account or click **Generate**. The generated name is the prefix in the profile and a random two or three digit number.
    - **Comment:** Enter a descriptive comment.
    - **Password:** Enter the user account password or click **Generate**. The generated password is a random string of eight alphabetic characters.
    - **Confirm Password:** If you did not generate the password, re-enter it.
4. Go to **Add Guest > Guest Services**.
    - **Enable Guest Services Privilege:** Check this for the account to be enabled upon creation.
    - **Enforce login uniqueness:** Check this to allow only one instance of this account to log into the security appliance at one time. Leave it unchecked to allow multiple users to use this account immediately.

- **Automatically prune account upon account expiration:** Check this option to have the account removed from the database after its lifetime expires.
- Select **Activate account upon first login** to begin the timing for the account expiration.
- **Account Expires:** This setting defines how long an account remains on the security appliance before the account expires. You can specify from 1 to 9999 in the **Account Expires** field and select the type of duration from the drop-down menu:
  - **Minutes**
  - **Hours**
  - **Days**

  The default is **7 Days**.
- If **Automatically prune account upon account expiration** is:
  - **Enabled**, the account is deleted when it expires.
  - **Disabled**, the account remains in the **Guest Accounts** table with an **Expired** status to allow easy reactivation.
- To define the maximum period of time when no traffic is passed on an activated guest services session, enter the timeout duration in **Idle Timeout**. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** has not expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.

  ⓘ | **NOTE:** This setting overrides the idle timeout setting in the profile.

  You can specify from 1 to 9999 in the Account Lifetime field and select the type of duration from the drop-down menu:
  - Minutes
  - Hours
  - Days

  The default is **10 Minutes**.

5. To specify the quota cycle type, select from the **Quota Cycle Type Setting** drop-down menu:
   - **Non Cyclic** (default)
   - **Per Day**
   - **Per Week**
   - **Per Month**
6. To define how long a guest login session remains active after it has been activated, specify the duration in **Session Lifetime**. By default, activation occurs the first time a guest user logs into an account. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**.

   ⓘ | **NOTE:** This setting overrides the session lifetime setting in the profile.

   You can specify from 1 to 9999 in the Session Lifetime field and select the type of duration from the drop-down menu:
   - **Minutes**
   - **Hours**
   - **Days**

   The default is **1 Hours**.

7. **Receive limit (0 to disabled):** Enter the number of megabytes the user is allowed to receive. The minimum number is 0, which disables the limit; the maximum is **Unlimited**, the default.
8. **Transmit limit (0 to disabled):** Enter the number of megabytes the user is allowed to transmit. The minimum number is 0, which disables the limit; the maximum is **Unlimited**, the default.
9. To limit the amount of data the user can receive, enter the amount, in MB, in **Receive limit (0 to disable)** field. The range is from 0 (no data can be received) to 999999999 MB to **Unlimited** (default).
10. To limit the amount of data the user can send, enter the amount, in MB, in **Transmit limit (0 to disable)** field. The range is from 0 (no data can be received) to 999999999 MB to **Unlimited** (default).
11. Click **Save** to generate the guest account.

Editing Guest Accounts

To edit guest accounts:

1. Click the **Edit** icon in the **Configure** column for the profile.
2. Follow the steps in Adding Guest Accounts.

Deleting Guest Accounts

You can delete all guest profiles, except the **Default** profile.

Topics:

- Deleting a Guest Account
- Deleting Multiple Guest Accounts
- Deleting All Guest Accounts

Deleting a Guest Account

You can delete all guest profiles, except the **Default** profile.

To delete a guest account:

1. Click the **Delete** icon for the guest account. A confirmation message displays.
2. Click **OK**.

Deleting Multiple Guest Accounts

You can delete all guest profiles, except the **Default** profile.

To delete one or more guest accounts:

1. Navigate to **Device > Users > Local Users & Groups**.
2. Select the checkbox(es) of the guest profile(s) to be deleted.
3. Click the **Delete** icons in the **Configuration** column. A confirmation message displays.
4. Click **OK**.

Deleting All Guest Accounts

You can delete all guest profiles, except the **Default** profile.

To delete all guest accounts:

1. Select the checkbox in header of the **Guest Accounts** table. All checkboxes (except for the **Default** profile) become selected. **Delete Guest Accounts** becomes available.
2. Click **Delete Guest Accounts**. A confirmation message displays:
3. Click **OK**.

8

Managing Guest Status

The **Guest Status** page displays the current status of all of the guest accounts currently logged in.

Topics:

Logging Out Guests

To log out one or more guests:

1. Navigate to **Device > Users > Guest Status**.
2. Select the Guests you want to log out from the list.
3. Click the **Logout** icon on the far right.

Logging Out All Guests

To log out all guests:

1. Navigate to **Device > Users > Guest Status**.
2. Click the **Logout All** icon on the far right.

9

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

SonicOS Users Administration Guide
Updated - November 2024
Software Version - 8
232-006196-00 Rev A

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035