SonicWall® Global Management System Users

Administration Guide

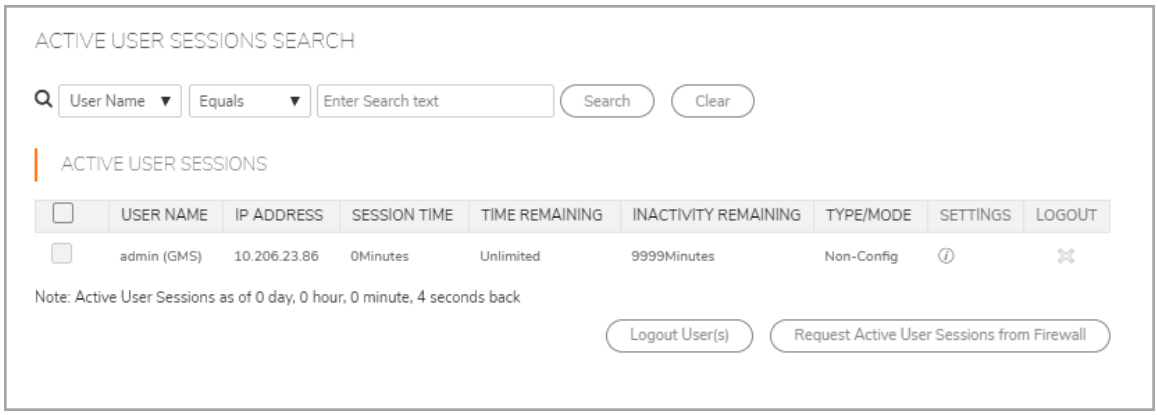
SONICWALL®

Contents

1

Configuring Users Status

The **Users > Status** page displays the **Active User Sessions** on the firewall. IPv4 and IPv6 IP addresses are accepted/displayed in the **Active User Sessions** table.



The **Active User Sessions** table lists the **User Name**, **IP Address**, **Session Time**, **Time Remaining**, **Inactivity Remaining**, **Type/Mode**, **Settings**, and **Logout**.

Topics:

- Logging Out a Single User
- Logging Out Multiple Users
- Searching for Active User Sessions

Logging Out a Single User

To log out a user:

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

2 Select the user you would like to logout and click **Logout User(s)** to log them out.

Logging Out Multiple Users

To log out multiple users:

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

2 Select the users you would like to logout and click **Logout User(s)** to log them out.

Searching for Active User Sessions

To search for active user sessions:

1. Navigate to the **Users > Status** page.
2. Specify search options in the **Active User Sessions Search** section.
3. Clicking **Search**. The **Active User Sessions** table displays only those users matching the search criteria. To restore the table, click **Clear**.

2

Configuring User Settings

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

For SonicWall appliances running SonicOS 5.0 and higher, 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 provides privileged access to multiple network resources with a single workstation login. SonicWall PRO and TZ series security appliances running SonicOS 5.0 and higher provide SSO functionality using the SonicWall Single Sign-On Agent (SSO Agent) to identify user activity based on workstation IP address when Active Directory is being used for authentication. The SonicWall SSO Agent must be installed on a computer in the same domain as Active Directory.

Topics:

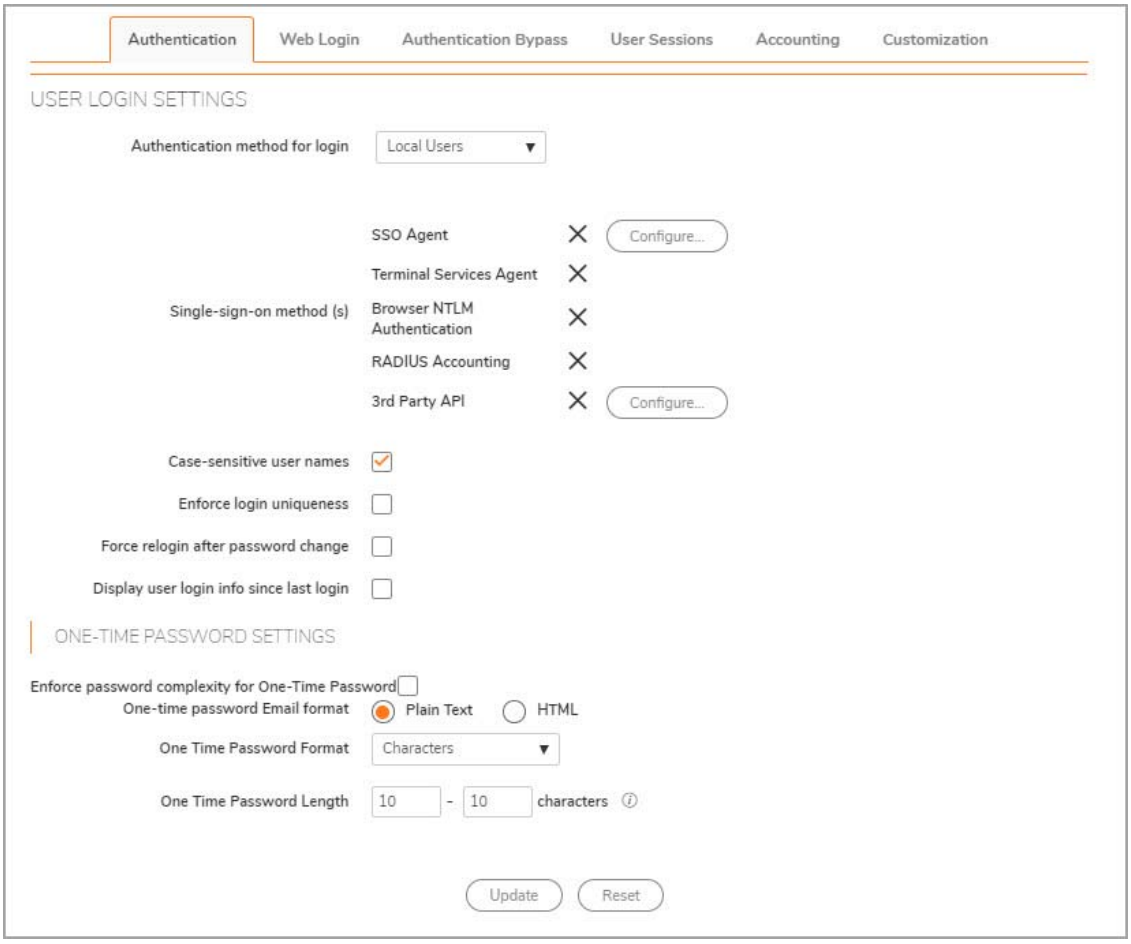
User Login Settings

Topics:

Setting the Authentication Method for Login

To set the authentication method for login:

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



2 Select one of the following authentication methods from **Authentication method for login**:

- **Local Users**—To configure users in the local database using the **Users > Local Users** and **Users > Local Groups** pages. For 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 the user to the SonicWall. If you select Use RADIUS for user authentication, users must log into the SonicWall using HTTPS in order to encrypt the password sent to the SonicWall. If a user attempts to log into the SonicWall 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. For information on configuring RADIUS, refer to Configuring RADIUS.
- **LDAP**—If you use a Lightweight Directory Access Protocol (LDAP) server or Microsoft Active Directory (AD) server to maintain all your user account data. 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 Terminal Access Controller Access-Control System Plus (TACAS+) protocol for authentication.
- **TACACS++Local Users**—If you use Terminal Access Controller Access-Control System Plus (TACAS+) protocol and the SonicWall local user database for authentication

3 Click **Update**.

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 **Users > Settings** page.

2 Enable or disable the methods, or click **Configure** to configure a single-sign-on method. These methods are available:

- **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 **Update**.

Requiring User Names be Treated as Case-sensitive

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

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

2 Select **Case-sensitive user names**. (This option is selected by default.)

3 Click **Update**.

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 the **Users > Settings** page.

2 Select **Enforce login uniqueness**. (This option is not selected by default.)

3 Click **Update**.

Forcing Users to Log In Immediately After Changing Their Passwords

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

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

2 Select **Force relogin after password change**. (This option is not selected by default.)

3 Click **Update**.

Displaying User Login Information Since the Last Login

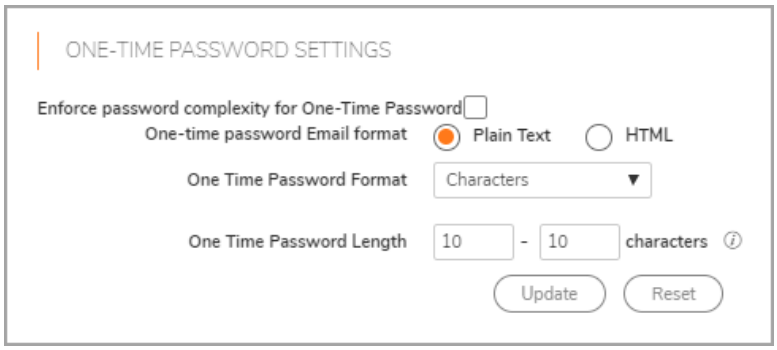
To display user login information since the last login:

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

2 Select **Display user login info since last login**. (This option is not selected by default.)

3 Click **Update**.

One-Time Password Settings



To configure the one-time password settings:

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

2 Choose an email format for **One-time password Email format**:

- **Plain Text**
- **HTML**

3 From **One-time password format**, select the password format:

- **Characters**
- **Characters + Numbers**
- **Numbers**

4 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.

5 Click **Update**.

Configuring the User Web Login Settings

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 the **Users > Settings > Web Login** page.

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 **Update**.

Setting How the Browser is Redirected

To set how the browser is redirected:

1 Navigate to the **Users > Settings | Web Login** page.

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 > Administrator** page. Otherwise, this option is dimmed. To enable redirection to a configured domain name, set the firewall's domain name on the **System > Administrator** 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 the **Its configured domain name** option.

  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.sonicall.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.sonicall.com`, the browser has no way to tell if that is correct, so it displays a certificate warning instead.

3 Click **Update**.

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 the **Users > Settings | Web Login** page.

2 In the **Limit redirecting users to** field, enter the number of times in the Limit redirecting users to times per minute per user field. The default value is **10** times.

3 To further limit redirects of the same page, select the **Don't redirect repeated gets of the same page** option. This option is selected by default.

4 Select **Redirect users from HTTPS to HTTP on completion of login** if the session does not need to be encrypted.

5 Click **Update**.

Using a CHAP challenge to Authenticate Users

If using RADIUS authentication (and if the RADIUS server supports it), a CHAP challenge can be used to authenticate users during web login. Such a login through HTTP is secure, so it is not necessary to enforce HTTPS for login.

Administrators who use this mechanism to log into the SonicWall appliance are restricted in the management operations they can perform. For some management operations, the appliance needs to know the user's password, which is not available with CHAP authentication by a remote authentication server. Consequently, if this option is enabled, users who are members of administrative user groups might have to log in manually through HTTPS when logging in for administration. This restriction does not apply to the built-in **admin** account.

TIP: When using LDAP, this mechanism can be used normally by:

1 Setting the **Authentication method for login** to **RADIUS**.

2 Selecting **LDAP** as the mechanism for setting user group memberships in the RADIUS configuration.

To use a CHAP challenge to authenticate users:

1 Navigate to the **Users > Settings | Web Login** page.

2 Select **Allow HTTP login with RADIUS CHAP mode** to enable type of login.

NOTE: This option is only available when the **Authentication method for login** is **RADIUS** or **RADIUS+Local Users**. This option is not selected by default.

3 Select the option **Authenticate user's other IP (v4/v6) addresses if possible**, if required.

4 Select the option **Use HTTP to initiate combined logins**, if required.

5 Click **Update**.

Redirecting Unauthenticated Users

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

1 Select **On redirecting unauthenticated users, redirect to an external login page URL**. 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 configure options related to the captive portal configured in a zone's guest settings, scroll to **Web Login Settings for Guest Captive Portal**.

4 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.

10 Click **Update**.

Authentication Bypass Settings

GMS Guest Services allows guest users to have access through your network directly to the Internet without access to your protected network. To do this, GMS 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 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.

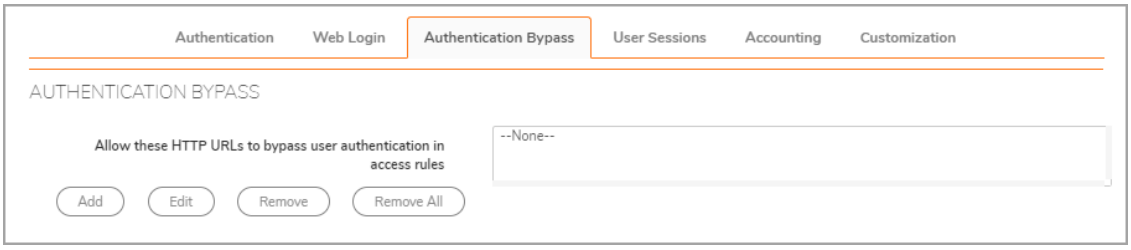
Topics:

- Adding URLs to Authentication Bypass

Adding URLs to Authentication Bypass

To add HTTP URLs user authentication bypass in Access Rules:

1 Navigate to **Users > Settings | Authentication Bypass**.



2 Click **Add**. The **Add URL** pop-up displays.

3 Enter the URL in the **URL** field.

4 Click **Update**. A change order pop-up confirmation displays.

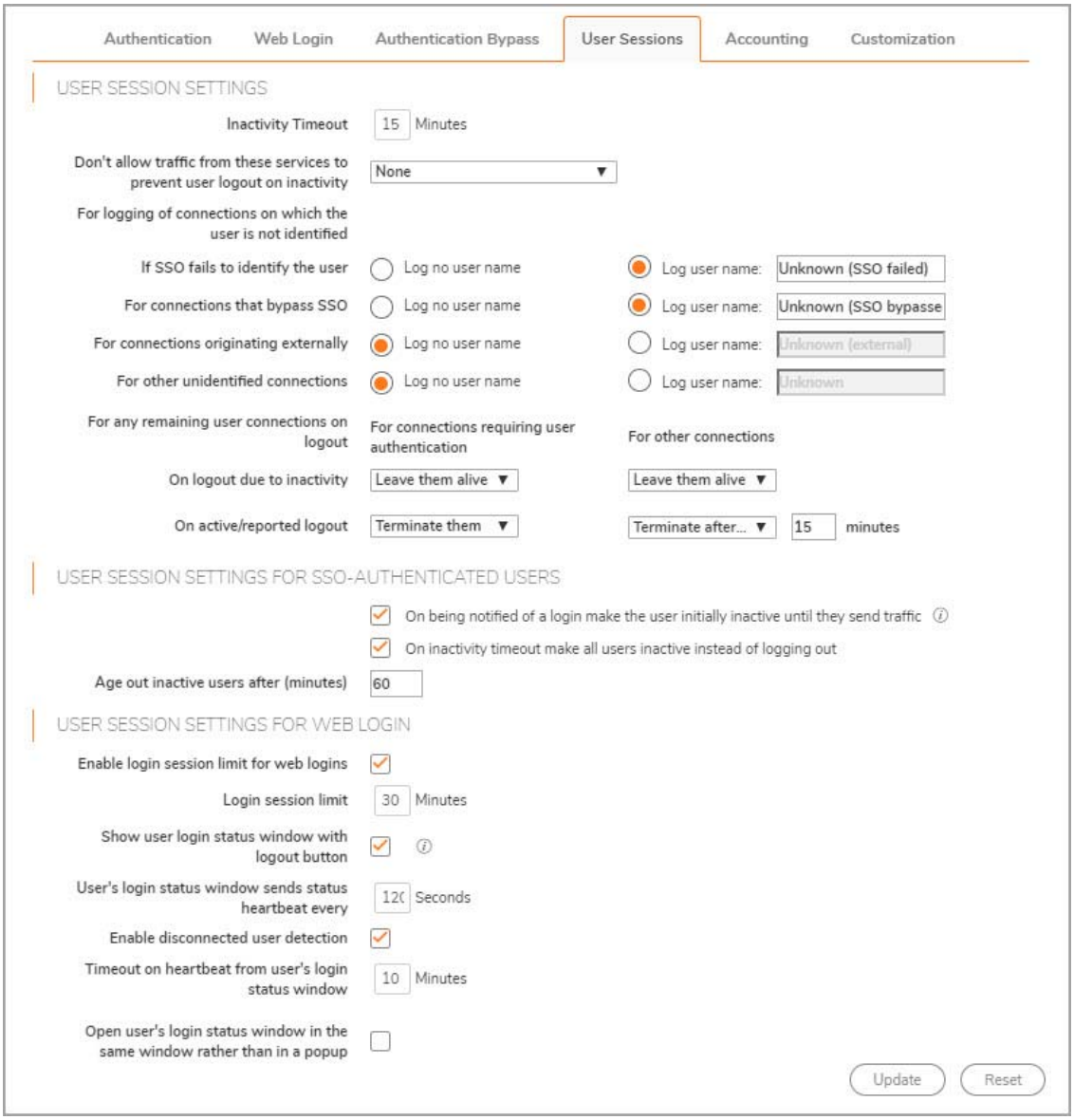
5 Click **Accept**.

User Session Settings

The settings that follow apply to all users when authenticated through the SonicWall.

To configure user session settings:

1 Navigate to **Users** > **Settings | User Sessions**.



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

1 Navigate to the **Users > Settings | User Sessions** page.

2 Specify the length of time for inactivity after which users are logged out of the firewall in the **Inactivity timeout (minutes)** field. 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 **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.

Type of logout	Action	
	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)

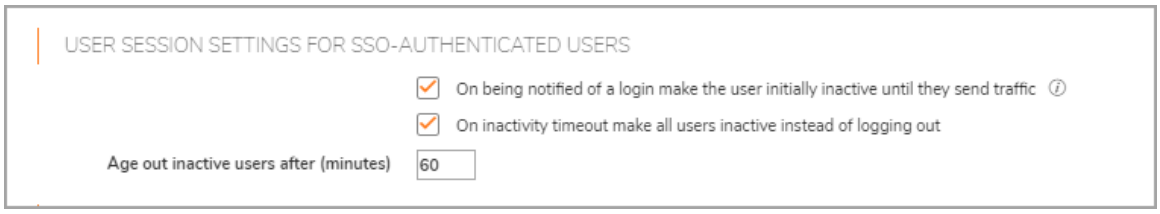
1. Applies for connections through access rules that allow only specific users.
2. Applies for other connections that do not have a specific user authentication requirement.

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 appliance as being logged out (the latter normally means that the user has logged out from the domain/user).

6 Click **Update**.

User Session Settings for SSO-Authenticated Users



To specify how inactive SSO-authenticated users are handled:

1 Navigate to the **Users > Settings | User Sessions** page.

To put a user identified to the SonicWall 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 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).

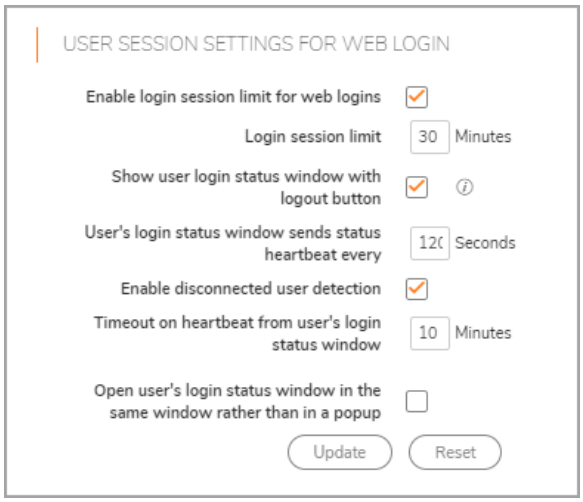
2 If an SSO-identified user who has been actively logged in is timed out because of inactivity, then users who cannot be re-identified are returned to an inactive state. To have users who would otherwise be logged out on inactivity to be returned to an inactive state, select **On inactivity timeout make 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.

3 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.

4 Click **Update**.

User Session Settings for Web Login



To configure user session settings for web login:

1 Navigate to the **Users > Settings | User Sessions** page.

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.

3 Select **Show user login status window with logout button** to display a status window with a **Log Out** button during the user's session. The user must click **Log Out** to log out of the 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.

> **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 the SonicWall. This heartbeat notifies the SonicWall 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 the SonicWall to 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 **Allow unauthenticated VPN users to access DNS** to allow that access.

8 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.

9 **LDAP read from server options** are available when the LDAP option is active. The options are:

- **Automatically update the schema configuration**
- **Export details of the schema**

10 Click **Update**.

Accounting

GMS 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:

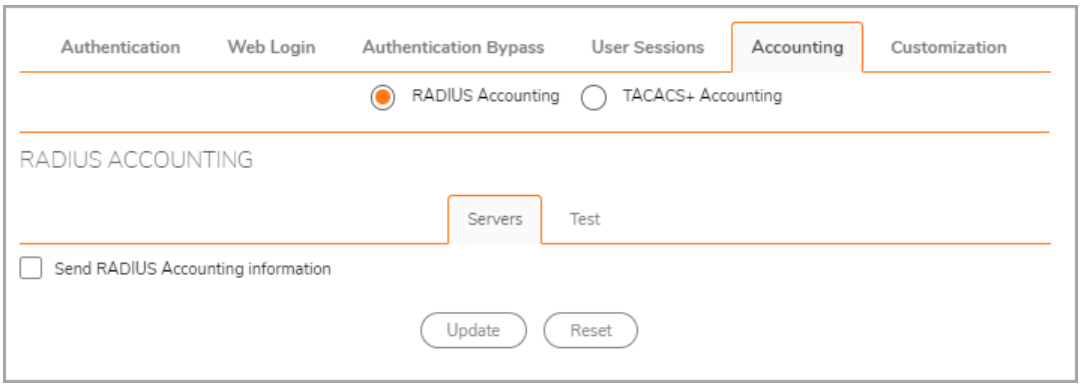
- Sending RADIUS Accounting Information to Servers
- Editing Servers
- Deleting Servers

Sending RADIUS Accounting Information to Servers

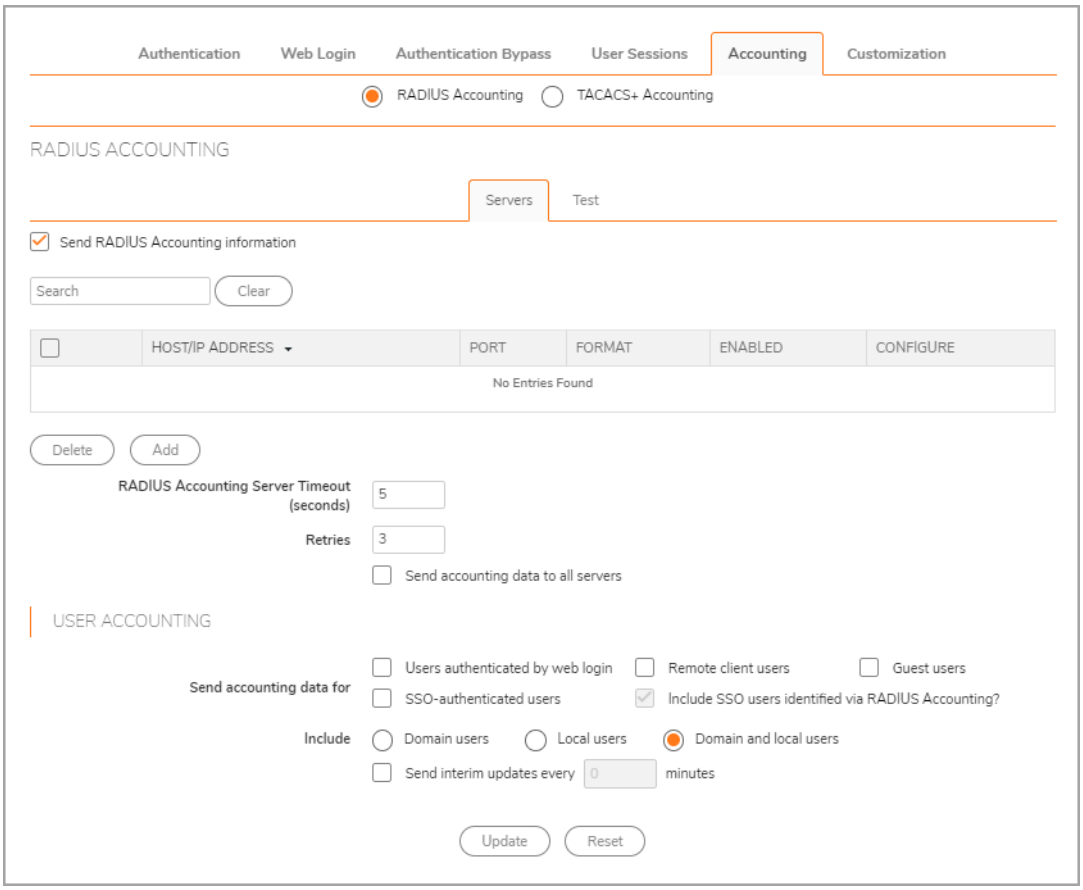
To send RADIUS accounting information to servers:

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

2 Scroll to the **RADIUS Accounting** section.

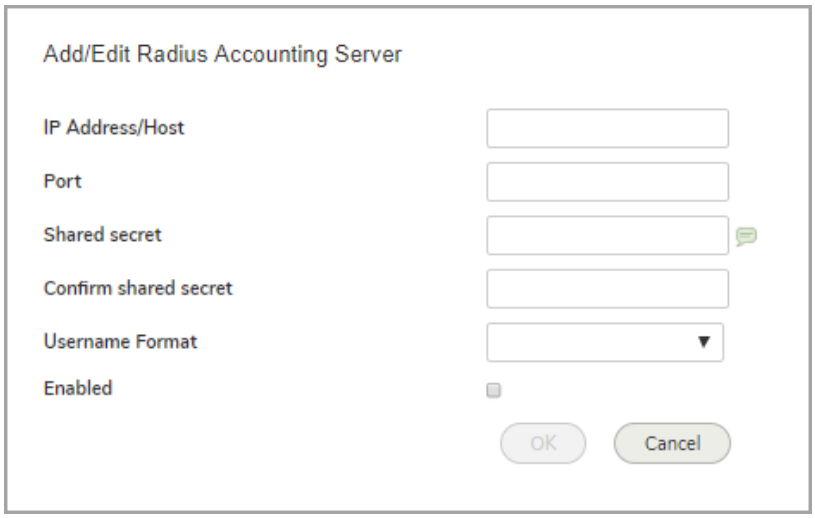


3 Select **Send RADIUS Accounting Information**. The section expands.



4 To add a RADIUS server:

a Click **Add**. The **Add/Edit Radius Accounting Server** dialog displays.



b Enter the host or IP address in the **IP Address/Host** field.

c Enter the port in the **Port** field.

d Enter the shared secret in the **Shared secret** and **Confirm shared secret** fields.

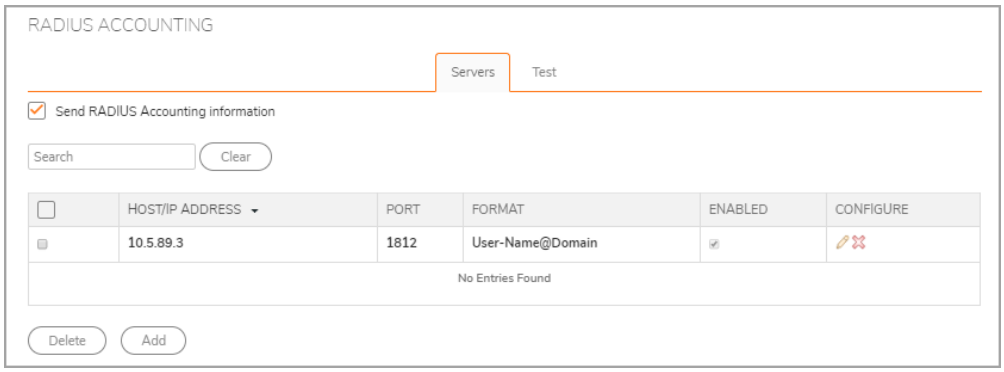
e Select the username format from **Username Format**:

- **User-Name**
- **User-Name@Domain**
- **Domain\User-Name**
- **User-Name.Domain**

f To enable the server, select **Enabled**. This option is not selected by default.

g Select the authentication partition from **Authentication partition**.

h Click **OK**. The **RADIUS Accounting** table is updated.



i For each server to add, repeat Step a through Step h.

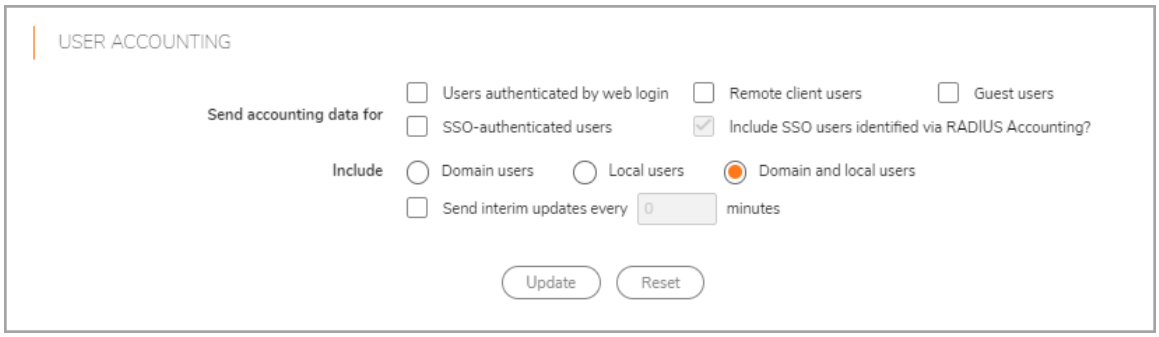
5 Enter a maximum time out, in seconds, in the **RADIUS Accounting Server Timeout (seconds)** field. The default is **5** seconds.

6 Enter the maximum number of retries in the **Retries** field. The default 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 **Update**.

User Accounting



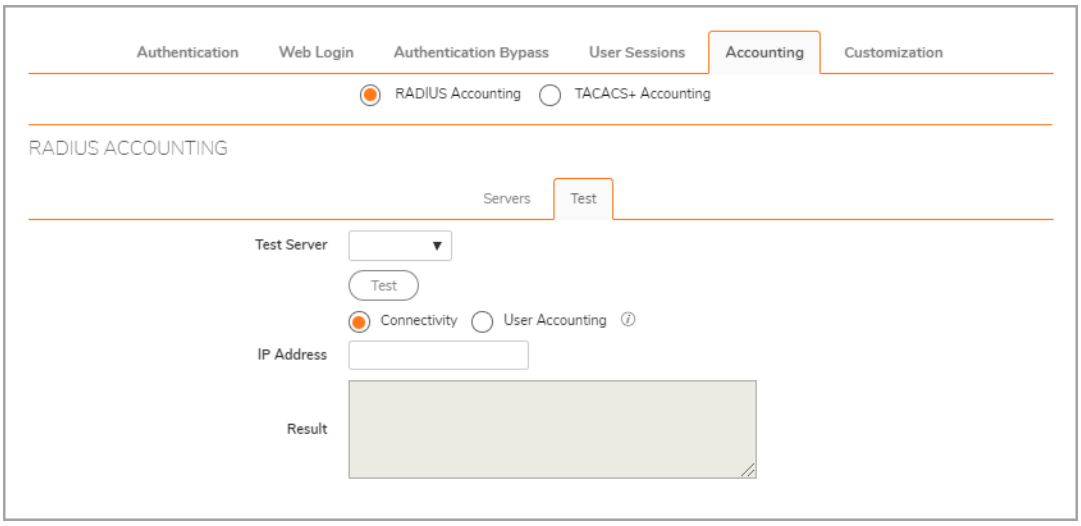
1 From **Send accounting data for**, select one or more types of users. **Include SSO users identified via RADIUS Accounting?** is not available by default. To make it selectable, first select the **SSO-authenticated users** field.

2 Choose whether to track domain and/or local users from **Include**. **Domain users** is selected by default.

3 To receive watchdog messages, select **Send Watchdog Messages**. This option is not selected by default.

4 After selecting this option, the **Every:....minutes** option appears. Indicate how often you would like to receive **Watchdog Messages**.

5 Click **Test**.



6 From **Select server to test**, select the IP address of the TACACS+ server.

7 Choose the type of test from **Test**. **Connectivity** is selected by default.

8 Click **Test**. The results of the test display in **Returned User Attributes**.

9 Click **Apply**.

10 Repeat these previous steps for each server.

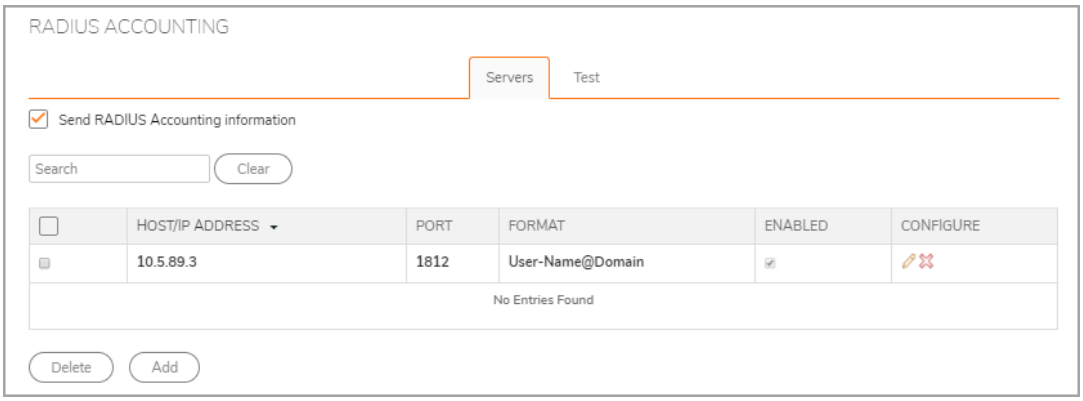
11 Click **OK**.

Editing Servers

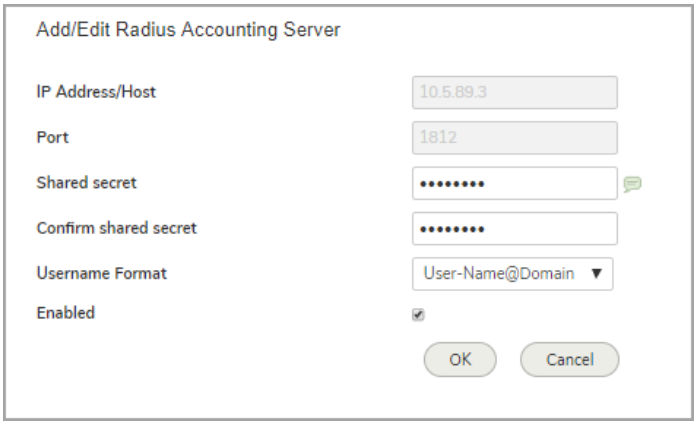
To edit a server:

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

2 Scroll to the **RADIUS Accounting** section.



3 Click the **Edit** icon for the server to edit. The **Add/Edit Radius Accounting Server** dialog for that server displays. The **IP Address/Host** and **Port** fields are dimmed and cannot be changed.



4 Make the changes.

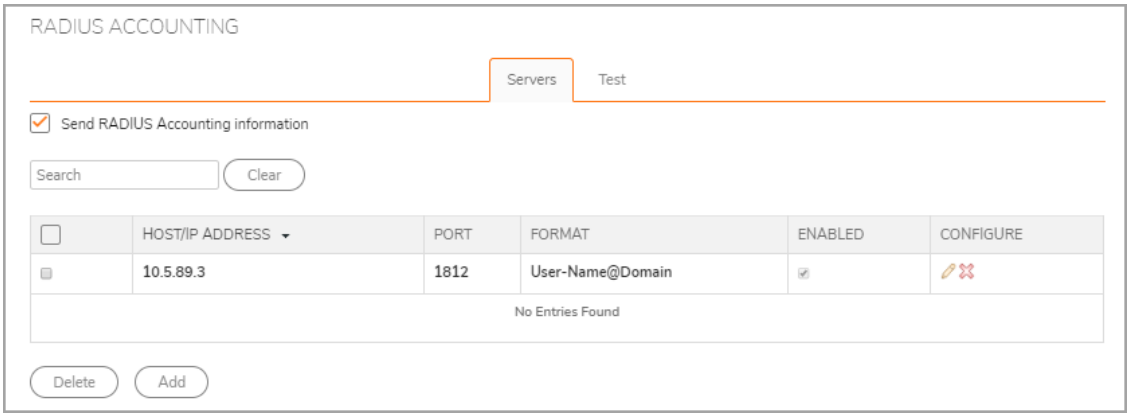
5 Click **OK**. The servers entry in the **RADIUS Accounting** table is updated.

Deleting Servers

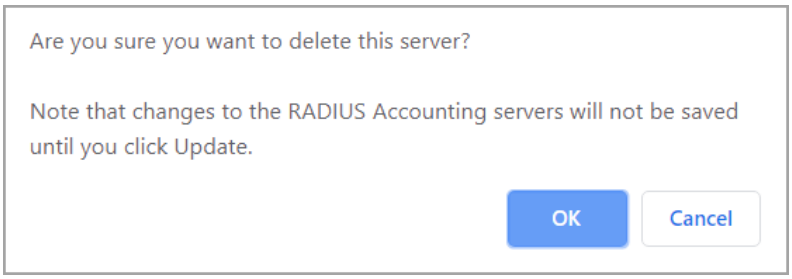
To delete a single server:

1 Navigate to the **Users > Settings | Accounting** page.

2 Scroll to the **RADIUS Accounting** section.



3 Click the **Delete** icon in the **Configure** column for the server to be deleted. A confirmation message displays.



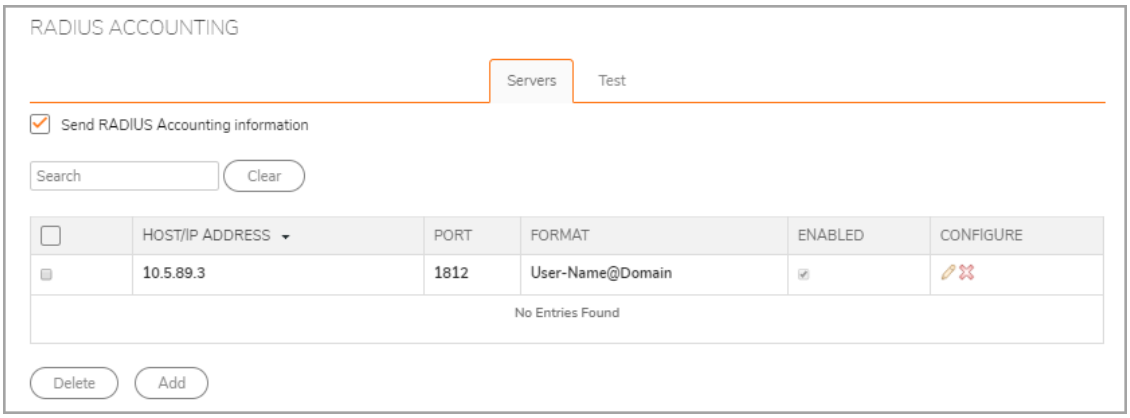
4 Click **OK**.

5 Click **Update**.

To delete one or more servers:

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

2 Scroll to the **RADIUS Accounting** section.



3 Select the servers in the **RADIUS Accounting** table to be deleted.

4 Click **Delete**. A confirmation message displays.

5 Click **OK**.

6 Click **Update**.

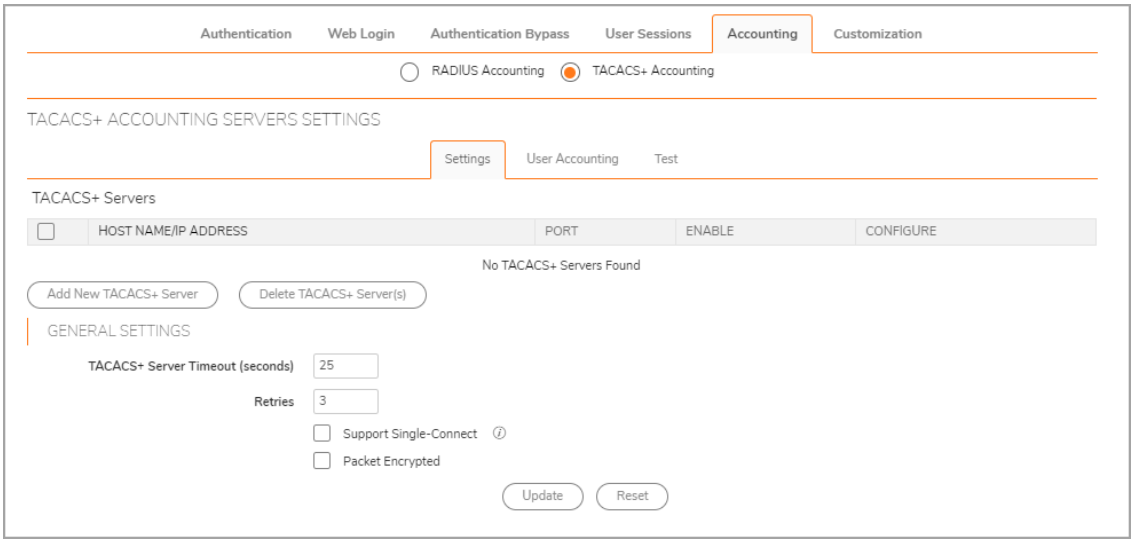
Configuring TACACS+ Accounting

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

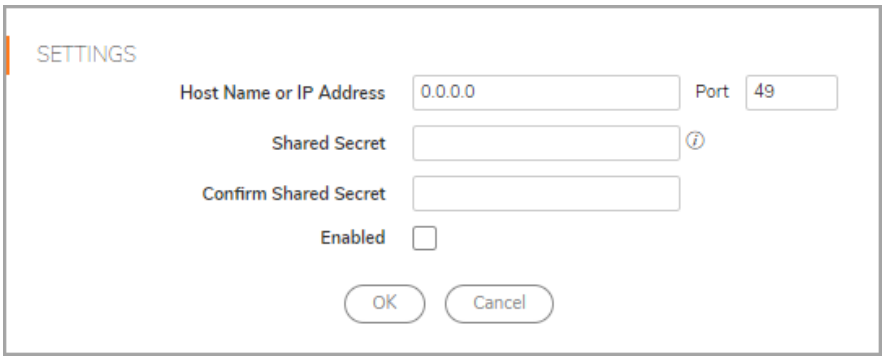
To configure TACACS+ accounting:

1 Navigate to **Users > Settings | Accounting**.

2 Click the **TACACS+ Accounting** option. The TACACS+ Accounting Configuration dialog displays.



3 To add a TACACS+ server, click **Add New TACACS+ Server**. The **Add TACACS+ Accounting Server** dialog displays.



4 Enter the host name or IP address of the TACACS+ server in the **Host Name or IP Address** field.

5 Enter the port number of the server in the **Port** field. The default is 49.

6 Enter the shared secret in the **Shared Secret** and **Confirm Shared Secret** fields.

7 Click **Enabled** when you are ready to put this TACACS+ server into use.

8 Click **OK**.

Customization

Topics:

- Pre-Login Policy Banner
- Acceptable Use Policy
- Customize Login Pages

Pre-Login Policy Banner

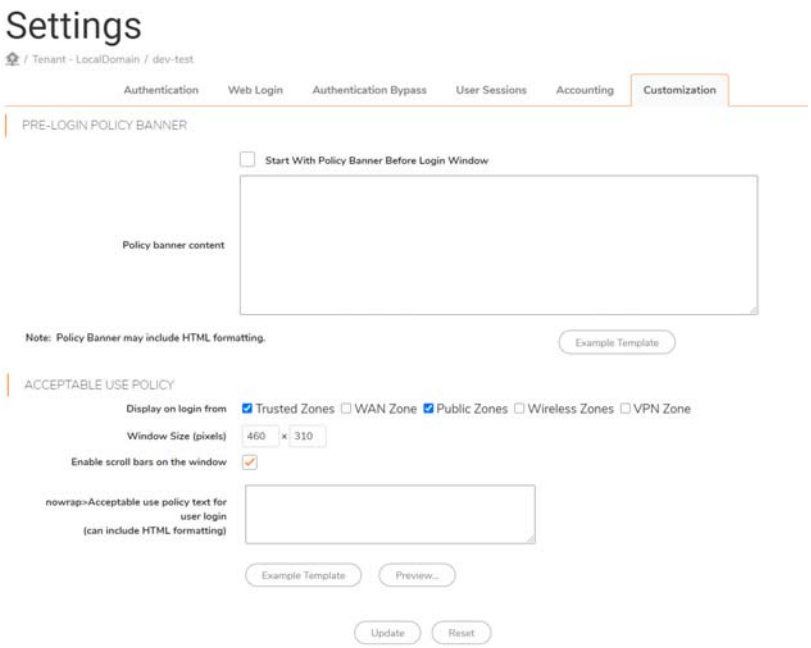
Create a policy statement that is presented to all users as a banner in the window before web login. The policy banner can include HTML formatting.

To display a banner containing a policy when the user logs in and that the user must accept to log in:

1 Navigate to **Users > Settings | Customization**.

2 Select **Start With Policy Banner Before Login Window**. This option is not selected by default.

   a To see a sample banner, click **Example Template**. The **Policy banner content** field is populated.



   b Make changes to the sample banner or enter new coding. The page that is displayed to the user includes **I Accept** and **Cancel** for user confirmation.

   c Click **Update**.

Topics:

- Example Template
- Preview Message

Example Template

Click **Example Template** to populate the content with the default Acceptable Use Policy (AUP) template, which you can modify:

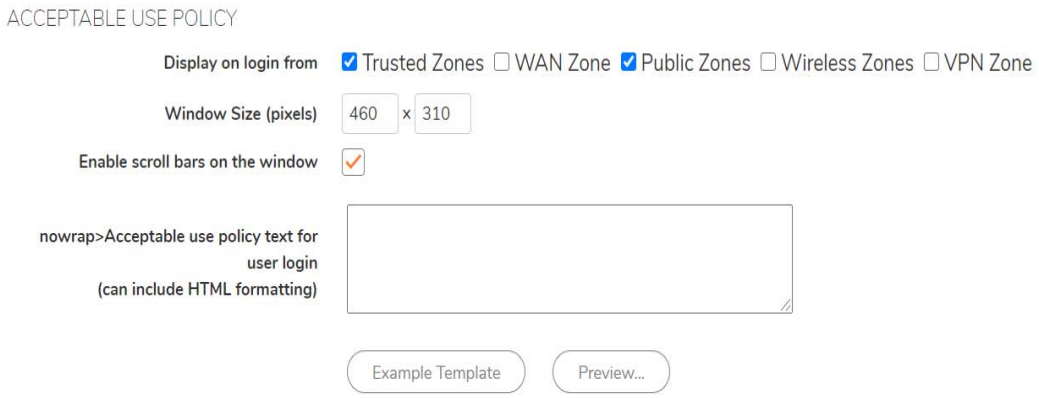
```
<font face=arial size=3>
<center><b><i>Welcome</center></b></i>
<font size=2>

<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 click "Cancel".
```

Preview Message

Click **Preview** to display your AUP message as it appears to the user.

Acceptable Use Policy

An acceptable use policy (AUP) is a policy that users must agree to follow to access a network or the Internet. It is common practice for many businesses and educational facilities to require that employees or students agree to an acceptable use policy before accessing the network or Internet through their Security Appliance.



The Post-Login Acceptable Use Policy section allows you to create the AUP message window for users. You can use HTML formatting in the body of your message. Clicking **Example Template** creates a preformatted HTML template for your AUP window; see Example Template.

To create a post-login AUP message window:

1. Navigate to **Users > Settings | Customization**.
2. Scroll to the **Acceptable Use Policy** section.
3. Specify these settings:

- **Display on login from** - Select the network interface(s) you want to display the Acceptable Use Policy page when users login. You can choose Trusted Zones (default), WAN Zone, Public Zones (default), Wireless Zones, and VPN Zone in any combination.
- **Window size (pixels)** - Allows you to specify the size of the AUP window, in pixels:
  - **Width**: Minimum size is 400 pixels, maximum size is 1280 pixels, and the default is 460 pixels.
  - **Height**: Minimum size is 200 pixels, maximum size is 1024 pixels, and the default is 310 pixels.
- **Enable scroll bars on window** - Turns on the scroll bars when your content exceeds the display size of the window. This option is selected by default.
- **Acceptable use policy text for user login** - Enter your Acceptable Use Policy text in this field. You can include HTML formatting. The page that is displayed to the user includes I Accept and Cancel for user confirmation.

4 Click **Update**.

Topics:

- Example Template
- Preview Meassage

Example Template

Click **Example Template** to populate the content with the default 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."
```

Preview Message

Click **Preview** to display your AUP message as it appears to the user.

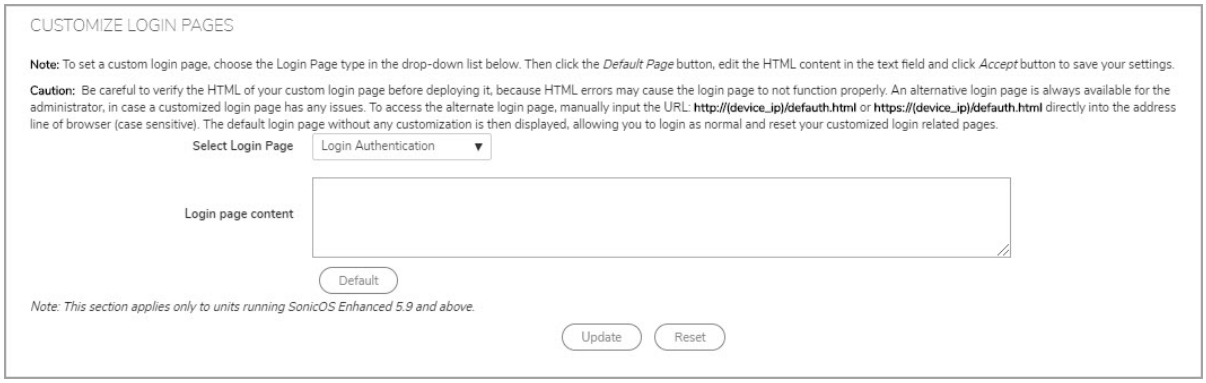
Customize Login Pages

The GMS provides the ability to customize the text of the login authentication pages that are presented to users. Administrators can translate the login-related pages with their own wording and apply the changes so that they take effect without rebooting.

Although the entire the GMS interface is available in different languages, sometimes the administrator does not want to change the entire UI language to a specific local language.

However, if the firewall requires authentication before users can access other networks, or enables external access services (for example, VPN, SSL-VPN), those login related pages usually should be localized to make them more usable for typical users.

The Customizable Login Page feature provides the following functionality:



The Customize Login Page feature provides the following functionality:

- Keeps the style of original login by default
- Customizes login related pages
- Uses the default login related pages as templates
- Saves customized pages into system preferences
- Allows a preview of changes before saving to preferences
- Presents customized login-related pages to typical users

The following login-related pages can be customized:

- Admin Preempt
- Login Authentication
- Logged Out
- Login Full
- Login Disallowed
- Login Lockout
- Login Status
- Guest Login Status
- Policy Access Barred
- Policy Access Down
- Policy Access Unavailable
- Policy Login Redirect
- Policy SSO Probe Failure
- User Password Update
- User Login Message

To customize one of these pages:

1 Navigate to **Users > Settings | Customization**.

2 Scroll to the **Customize Login Pages** section.

3 Select the page to be customized from the **Select Login Page** drop-down menu.

4 Select the page to be customized from **Select Login Page**:

Admin Preempt	**Login Lockout**	**Policy Access Unavailable**
Login Authentication (default)	**Login Status**	**Policy Login Redirect**
Logged Out	**Guest Login Status**	**Policy SSO Probe Failure**
Login Full	**Policy Access Barred**	**User Password Update**
Login Disallowed	**Policy Access Down**	**User Login Message**

5 Click **Default** to load the default content for the page into the **Login page content** field.

6 Edit the content of the page.

NOTE: The `var strXXX =` lines in the template pages are customized JavaScript Strings. You can change them into your preferring wording. Modifications should follow the JavaScript syntax. You can also edit the wording in the HTML section.

CAUTION: Be careful to verify the HTML of your custom login page before deploying it, because HTML errors might cause the login page to not function properly. An alternative login page is always available for the administrator, in case a customized login page has any issues. To access the alternate login page, manually input the URL `https://(device_ip)/defauth.html` directly into the address line of browser (case sensitive). The default login page without any customization is then displayed, allowing you to login as normal and reset your customized login related pages.

TIP: Leave the **Login Page Contents** field blank and apply the change to revert to the default page.

7 Click **Update**.

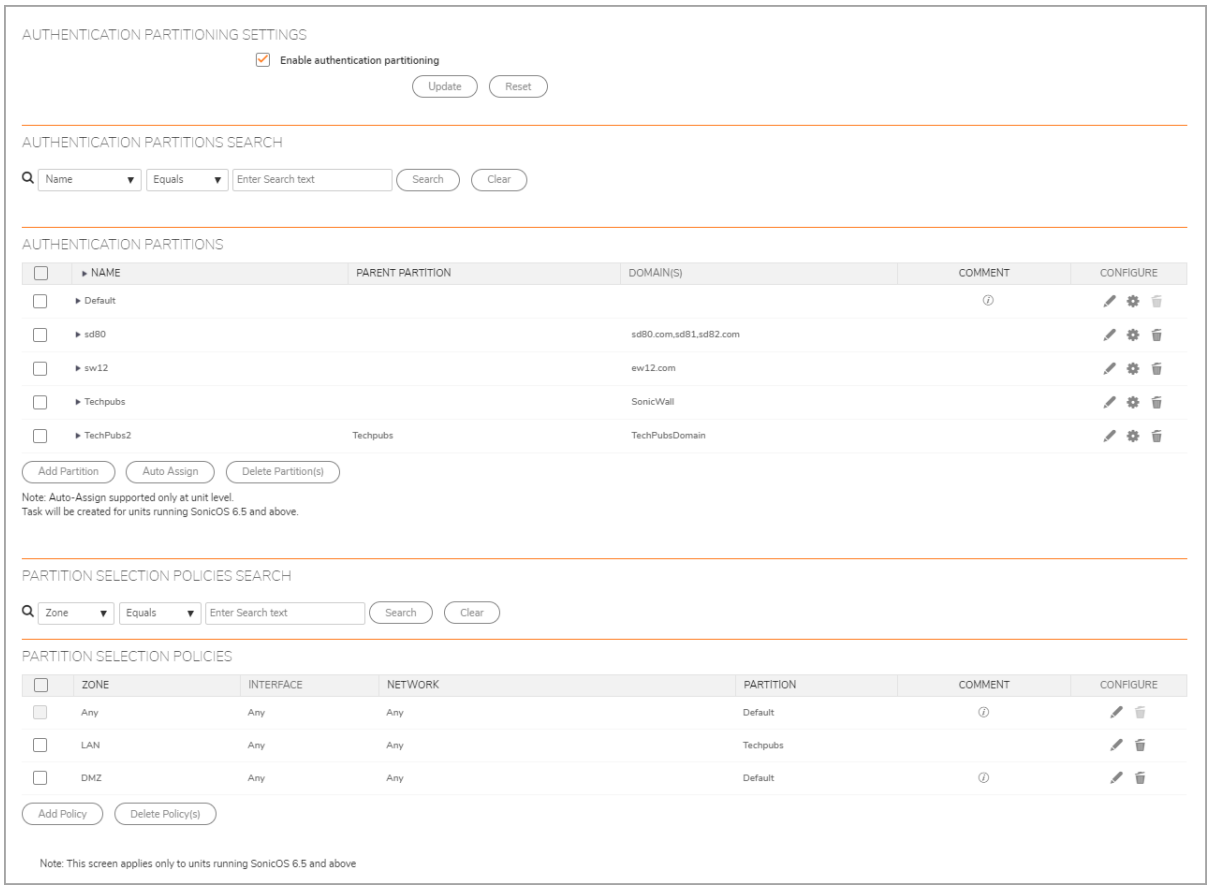
3

Configuring and Managing Partitions

Topics:

NOTE: Users > Partitions displays only if partitioning has been configured on the SonicWall appliance.

Users > Partitions Page

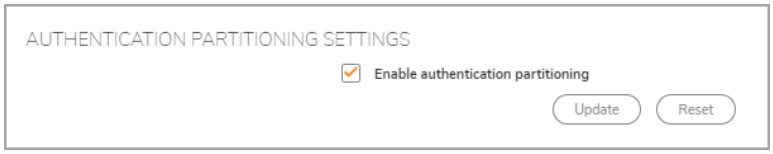


The **Users > Partitions** page includes two Search features and three sections:

- Authentication Partitioning Settings
- Authentication Partitions
- Partition Selection Policies

Authentication Partitioning Settings

This section enables/disables authentication partitioning. When authentication partitioning is disabled, the other sections do not display.



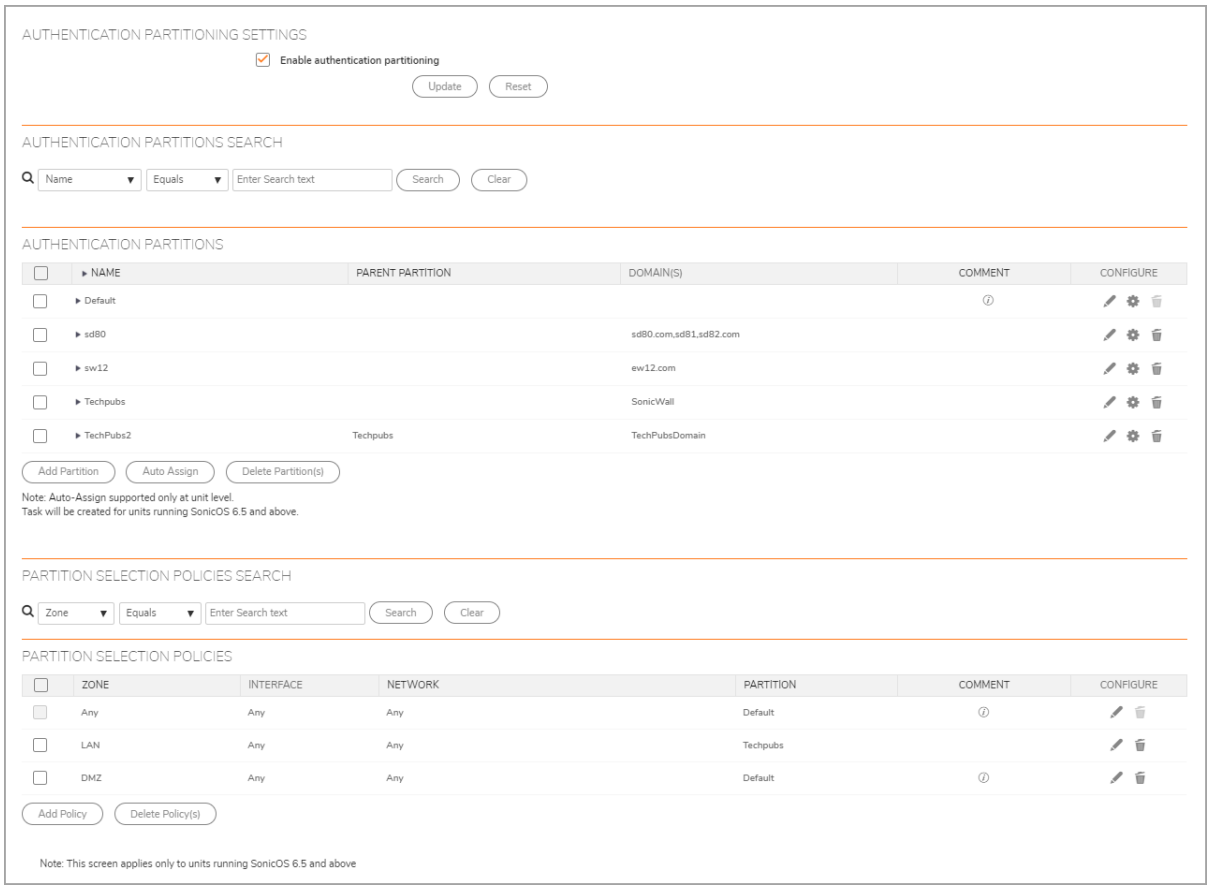
When authentication partitioning is enabled, the two **Search** features and two additional sections; **Authentication Partitions** and **Authentication Selection Policies**, also display.

Authentication Partitions

NOTE: This section displays only when authentication partitioning is enabled.

This section displays a table of authentication partitions and allows you to create, edit, delete, and manage the partitions. The partitions you configure here control which authentication servers are used for which users.

You can expand a partition's tree to show the servers, agents, and clients assigned to it.



Selection checkbox	Allows you to select one or more partitions and/or subpartitions in the table. Selecting the checkbox in the table heading selects all entries except the **Default** partition.
Name	Specifies the name of the authentication partition. Subpartitions are indicated by a **Link** ↳ icon in front of the name.
Parent Partition	Specifies the parent authentication partition for subpartitions. This column is blank for parent partitions.
Domain(s)	Specifies the domain(s) to which the partition or subpartition belongs. This column is blank for the **Default** partition.
Comment	Displays the comment included when the partition was added. The comment for the **Default** partition is **Auto-created default partition**.
Configure	Displays the **Edit**, **Selection**, and **Delete** icons for the partition. **NOTE:** The **Delete** icons are dimmed for the **Default** partition.
Add Partition	Displays the **Add an authentication partition** pop-up dialog for adding an authentication partition or subpartition.

Auto Assign	Assigns any unassigned LDAP servers, RADIUS servers, SSO agents, TSAs, and RADIUS accounting clients to the relevant partitions automatically, based on their IP addresses or host names.
Delete Partition(s)	Deletes the selected authentication partition(s) or subpartition(s). **NOTE:** You cannot delete the **Default** partition.

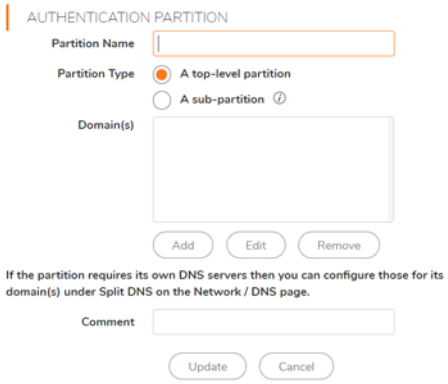
There is always one authentication partition in this table, the auto-created **Default** partition. You cannot delete this partition. You can, however, edit it and select servers, agents, and clients for it as well as subpartitions. If you disable authentication partitioning, all LDAP servers, SSO agents, TSAs, and RADIUS accounting clients are reassigned to the **Default** partition; when you re-enable authentication partitioning, you must reassign them. RADIUS servers are not affected and remain with their assigned partitions.

Adding Partitions and Subpartitions

To add a partition:

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

2 In the **Authentication Partitions** section, click **Add Partition**. The **Add Authentication Partition** pop-up dialog displays.



3 Enter a friendly, meaningful name in the **Partition Name** field. The name can be from 1 to 32 alphanumeric characters.

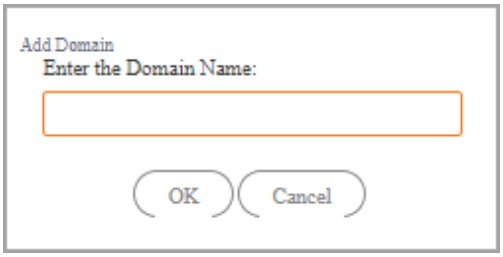
4 For **Partition type**, choose whether the authentication partition is:

- **A top-level partition**; go to Step 6.
- **A sub-partition**; the **Parent partition** drop-down menu displays.

5 Select a parent partition from the drop-down menu. The default partition is **Default**.

> **TIP:** If your installation does not have multiple partitions, then create subpartitions as subpartitions of the **Default** partition.

6 Under the **Domain(s)** list, click **Add**. The **Add Domain** pop-up dialog displays.



7 Enter a **Domain Name**.

8 Click **OK**.

9 Repeat Step 6 through Step 8 for each domain you want to add.

10 Optionally, enter a comment in the **Comment** field.

11 Click **Save**. The partitions and/or subpartitions are added to the **Authentication Partitions** table. Subpartitions are positioned immediately after their parent partitions, with a **Link** icon indicating they are subpartitions.

Deleting Partitions and Subpartitions

NOTE: In this section, partition refers to both partitions and subpartitions.

You can delete a single partition, multiple partitions, or all partitions. If you delete a single partition, the servers, agents, and clients are reassigned to the **Default** partition.

NOTE: You cannot delete the **Default** partition.

Topics:

- Deleting a Single Partition
- Deleting Multiple Partitions
- Deleting All Partitions (Except Default)

Deleting a Single Partition

To delete a single partition:

1 Navigate to **Users > Partitions**.

2 Under the **Authentication Partitions** table, click the **Delete** icon in the **Configure** column for the partition to be deleted. A verification message displays.

3 Click **OK**.

Deleting Multiple Partitions

To delete multiple partitions:

1 Navigate to **Users > Partitions**.

2 In the **Authentication Partitions** table, click the checkbox(es) of the authentication partition(s) you want to delete. You can select multiple partitions.

3 Click **Delete Partition(s)**. A verification message displays.

4 Click **OK**.

Deleting All Partitions (Except Default)

To delete all partitions (except Default):

1 Navigate to **Users > Partitions**.

2 In the **Authentication Partitions** table, click the checkbox at the top of the table's left column. All partitions should be selected.

3 Deselect the **Default** partition.

4 Click **Delete Partition(s)**. A verification message displays.

5 Click **OK**. All servers/agents/clients are reassigned to the **Default** partition.

Expanding Trees

Expanding an authentication partition's tree shows the servers, clients, and agents assigned to the partition:

You can expand the tree of:

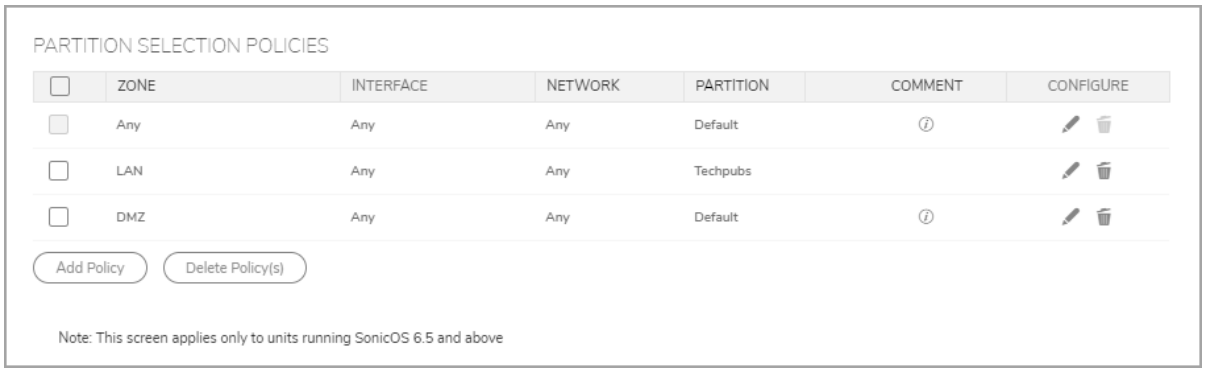
- All table entries by clicking the triangle next to the checkbox in the heading.
- One or more table entries by clicking the **Expand** icon of each.

Partition Selection Policies

NOTE: This section displays only when authentication partitioning is enabled.

This section displays a table of policies affecting the selection of authentication partitions and allows you to create, delete, and edit the policies you create. These policies select the partitions in the **Authentication Partitions** table based on the physical locations of the users being authenticated. When authenticating users whose domain names are not available for matching against those in the selected partitions, the users' partitions are selected base on their physical locations set by these policies. These selection policies are also used for auto-assigning authentication devices to partitions based on the physical locations of those devices.

The Default selection policy for the Default partition cannot be deleted.



Selection checkbox	Allows you to select one or more entries in the table. Selecting the checkbox in the table heading selects all entries except that of the **Default** selection policy.
Zone	Displays the zone assigned to the partition selection policy.
Interface	Displays the interface assigned to the authentication partition selection policy.
Network	Displays the network assigned to the authentication partition selection policy.
Partition	Displays the authentication partition to which the selection policy applies.
Comment	Displays any comment you entered when creating or editing the selection policy. The selection policy for the **Default** partition has the comment **Auto-created default policy**.
Configure	Displays the **Edit** and **Delete** icons, which are dimmed for the default policy.
Add Policy	Displays the **Add Authentication Partition Policy** pop-up dialog for adding a selection policy for an authentication partition or subpartition.
Delete Policy(s)	Deletes the selected policy or policies. **NOTE:** You cannot delete the policy for the **Default** partition. **Delete** is dimmed unless at least one policy has been selected.

There is always one selection policy in this table, the auto-created default policy for the **Default** partition. You cannot select this policy, delete it, change its priority, or edit it, except for choosing the partition to which it applies.

Assigning Servers, Agents, and Clients

After you have added the authentication partitions, you can assign servers, agents, and/or clients to the partitions. You can also assign them to the authentication partitions at any time by following the same procedures.

You can have unassigned servers, agents, and clients auto-assigned to the partition.

Topics:

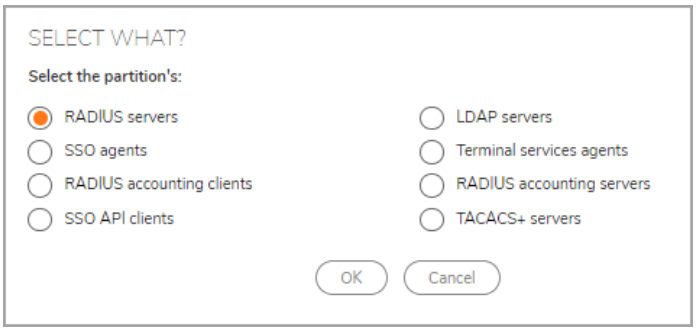
- Assigning Manually
- Auto Assigning

Assigning Manually

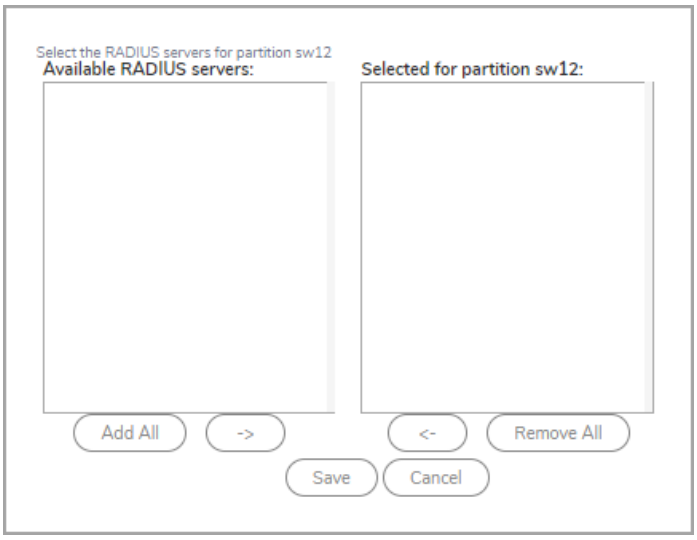
To assign servers, agents, and clients:

1 Navigate to **Users > Partitions**.

2 In the **Authentication Partition** table, click the partition's **Selection** icon in the **Configure** column. The **Select what?** popup dialog displays.



3 Select the type of server, agent, or client to assign. The appropriate **Select the *server/agent/client* for partition *partitionName*** pop-up menu displays with a list of available servers, agents, or clients.



4 Do one of the following:

- Select a server/agent/client from the **Available** list and click the **Right-arrow**.
- Select multiple items from the **Available** list by pressing the **Ctrl** key while selecting each item and then click the **Right-arrow**.
- Select all items by clicking **Add All**.

5 Click **Save**.

Auto Assigning

There is an **Auto Assign** button for assigning any unassigned servers, agents, and clients, based on their IP addresses or host names, to the relevant partitions automatically.

To auto assign servers, agents, and clients:

1 Navigate to **Users > Partitions**.

2 In the **Authentication Partitions** table, click the checkbox(es) of the authentication partition(s) to which you want to assign unassigned servers, agents, and/or clients. You can select more than one partition. **Auto assign** becomes active.

3 Click **Auto Assign**. The auto-assign message appears.

4 Click **OK**.

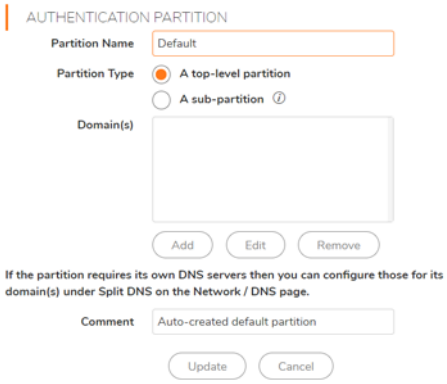
Editing Partitions

You can edit all partitions including the **Default** partition.

To edit a partition:

1 Navigate to **Users > Partitions**.

2 In the **Authentication Partitions** table, click the **Edit** icon in the **Configuration** column of the authentication partition you want to modify. The **Edit authentication partition** pop-up displays.

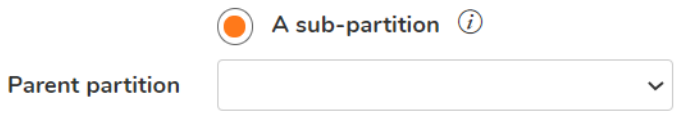


3 You can change the partition's name in the **Partition Name** field. The name can be from 1 to 32 alphanumeric characters.

4 You can change a partition from a top-level partition to a subpartition or from a subpartition to a top-level partition by changing the **Partition Type**; choose whether the authentication partition is now to be:

> **NOTE:** A top-level partition that has subpartitions cannot be changed to a subpartition unless you first delete the subpartitions, reallocate them to a different top-level partition, or make them top-level partitions.

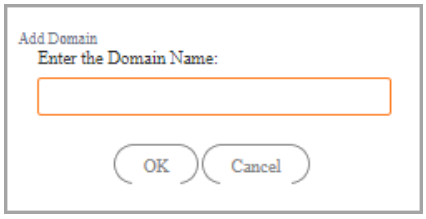
- **A top-level partition**, go to Step 6.
- **A sub-partition**; the **Parent partition** drop-down menu displays.



5 Select a parent partition from the **Parent partition** drop-down menu. The default partition is **Default**.

6 You can also do the following:

- Edit a domain, go to Step 10.
- Delete a domain, go to Step 15.
- Add a domain, under the **Domain(s)** list, click **Add**. The **Add domain** popup dialog displays.



7 Enter a domain name, which can be from 1 to 32 alphanumeric characters.

8 Click **OK**.

9 Go to Step 17.

10 Select a domain to edit by clicking on it.

11 Click **Edit**. The **Edit domain** dialog displays.

12 Change the domain name.

13 Click **OK**.

14 Go to Step 17

15 Select a domain to delete.

16 Click **Remove**.

17 Repeat Step 6 for each domain you want to add, edit, or delete.

18 Optionally, enter a comment in the **Comment** field.

19 Click **Save**.

4

Configuring Multi-RADIUS

To configure Multi-RADIUS server settings:

1 Navigate to **Users > Multi-RADIUS**.

2 Click **Add**.

3 Configure the following options in **Settings | RADIUS Servers**.

- **Host Name or IP Address** — Enter the FQDN or the IP address of the RADIUS 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.
- **Port** —In the Port field, enter the port for the RADIUS server to use for communication with GMS. The default is 1812.
- **Authentication Partition** — Select an associated **Authentication Partition** from the drop-down menu.
- **Shared Secret/Confirm Shared Secret** — Enter the RADIUS server administrative password or shared secret in the **Shared Secret** and **Confirm Shared Secret** fields. The case-sensitive, alphanumeric Shared Secret can range from 1 to 31 characters in length.

4 Click **Advanced**.

5 Optionally, select **Send Through VPN tunnel**. This option is not selected by default.

6 Select the format for the user name from **User Name Format**:

- **Simple-Name** (default)
- **Name@Domain**
- **Domain\Name**
- **Name.Domain**

7 If the RADIUS server requires user names be sent with the domain component included, then select the format for that here.

> **NOTE:** If the server accepts either the simple name without any domain component or a qualified name with the domain, then you can leave the selection as the default simple name unless you specifically want to force including the domain in the name sent to the server.

> **NOTE:** In a Windows domain, if users are to be allowed to log in with a qualified user-name format that differs from what is set here (for example, to allow a login to the firewall with domain\name when name@domain is selected or vice versa), then LDAP must be enabled for looking up the domain name mappings; otherwise, the user must enter a correctly-formatted name acceptable by the RADIUS server.

8 Click **Update**.

9 Click **OK**. The server is added to the **RADIUS Accounting Servers** table.

Multi-RADIUS General Settings

1 On the **General Settings** view, define the **RADIUS Server Timeout (seconds)**. The allowable range is 1-60 seconds with a default value of **5**.

2 Define the number of times the SonicWall attempts to contact the RADIUS server in the **Retries** field. If the RADIUS server does not respond within the specified number of retries, the connection is dropped. This field can range between 0 and 10, however 3 RADIUS server retries is recommended.

3 To periodically check the status of RADIUS servers, select **Periodically check RADIUS servers that are down**. This option is selected by default.

   If the primary RADIUS server fails to respond to a request, then its status is changed to down (showing red on the **RADIUS servers** table of the **RADIUS Configuration** dialog and further authentication requests are sent to the secondary server until the primary comes back up. If this setting is checked, then while a a server is down, dummy authentication requests are periodically sent to check it. When the server responds to one, its status is restore to up. Your RADIUS server may log an occasional authentication request failure with user name, status check.

   Disabling this option generally does not adversely affect user authentication. However, if it is disabled when the primary server goes down temporarily, then the firewall does not know when it becomes up, and so continues to show the server as down and sends authentication requests to the secondary server. This continues until secondary fails to respond to a request or the primary's status is checked manually, which can be done via the RADIUS test under **Test** on the **Configure RADIUS** dialog.

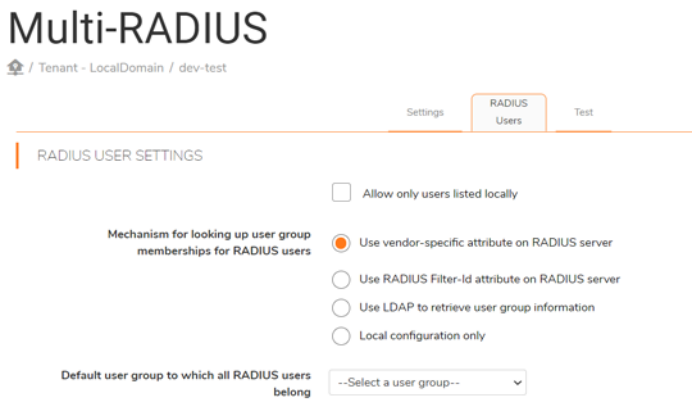
   NOTE: If the secondary server goes down while the primary server is down, then the firewall reverts to sending requests to the primary server, so the firewall detects when/if the primary server is responsive regardless of this setting.

4 Optionally, to enforce MS-CHAPv2 RADIUS authentication, select **Force PAP to MSCHAPv2**. This option is not selected by default.

5 Click **Update**.

Configuring Multi-RADIUS User Settings

On the RADIUS Users page of the RADIUS Configuration dialog, you can specify what types of local or LDAP information to use in combination with RADIUS authentication. You can also define the default user group for RADIUS users.



To configure the RADIUS user settings:

1 Navigate to **Users > Multi-RADIUS | RADIUS Users**.

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

3 Select the **Mechanism for looking up user group memberships for RADIUS users** option:

> **NOTE:** If the **Use vendor-specific attribute on Radius server** or **Use RADIUS Filter-ID attribute on RADIUS server** options are selected, the RADIUS server must be properly configured to return these attributes to the SonicWall appliance when a user is authenticated. The RADIUS server should return zero (0) or more instances of the selected attribute, each giving the name of a user group to which the user belongs.

- **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. The preferred vendor-specific RADIUS attribute is SonicWall-User-Group.
- **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.
- **Use LDAP to retrieve user group information** (default) – To obtain the user group from the LDAP server. You can click **Configure** to set up LDAP if you have not already configured it or if you need to make a change.
- **Local configuration only** – If you do not plan to retrieve user group information from RADIUS or LDAP.

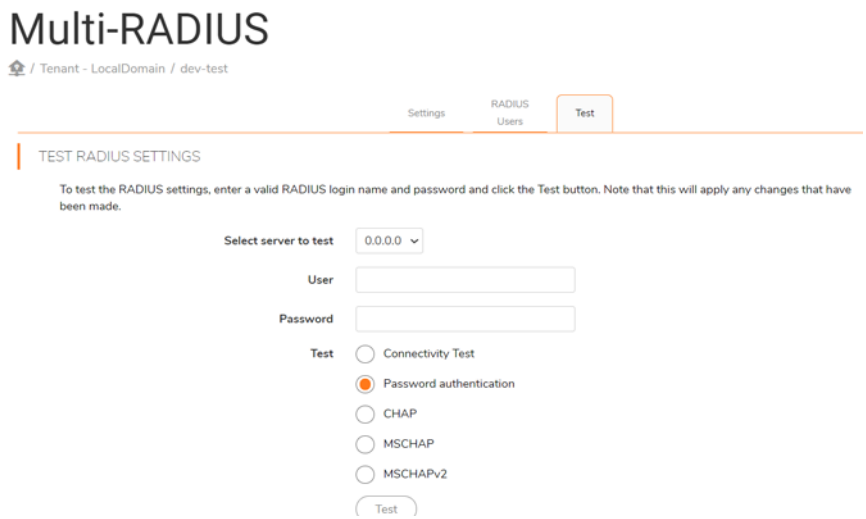
4 If you have previously configured User Groups in GMS, select the group from the **Default user group to which all RADIUS users belong** drop-down menu.

5 Click **Update** if you have finished configuring the RADIUS server.

6 If you have previously configured User Groups on the SonicWall, select the group from the **Default user group to which all RADIUS users belong** menu.

Configuring Multi-RADIUS Client Test

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 applies any changes you have made.



To test your Multi-RADIUS settings:

1. Navigate to **Users > Multi-RADIUS | Test**.
2. Select the **Server to test**.
3. In the **User** field, type a valid RADIUS login name.
4. In the **Password** field, type the password.
5. For **Test**, select one of the following:
   - **Connectivity** – Select this to test RADIUS connectivity.
   - **Password authentication** – Select this to use the password for authentication.
   - **CHAP** – elect this to use the Challenge Handshake Authentication Protocol. After initial verification, CHAP periodically verifies the identity of the client by using a three-way handshake.
   - **MSCHAP** – Select this to use the Microsoft implementation of CHAP. MSCHAP works for all Windows versions before Windows Vista.
   - **MSCHAPv2** – Select this to use the Microsoft version 2 implementation of CHAP. MSCHAPv2 works for Windows 2000 and later versions of Windows.
6. Click **TEST**. If the validation is successful, the Status messages changes to **Success**. If the validation fails, the Status message changes to **Failure**.
7. To complete the RADIUS configuration, click **Update**.

After GMS has been configured, a VPN Security Association requiring RADIUS authentication prompts incoming VPN clients to enter a **User Name** and **Password** into the dialog.

5

Configuring RADIUS

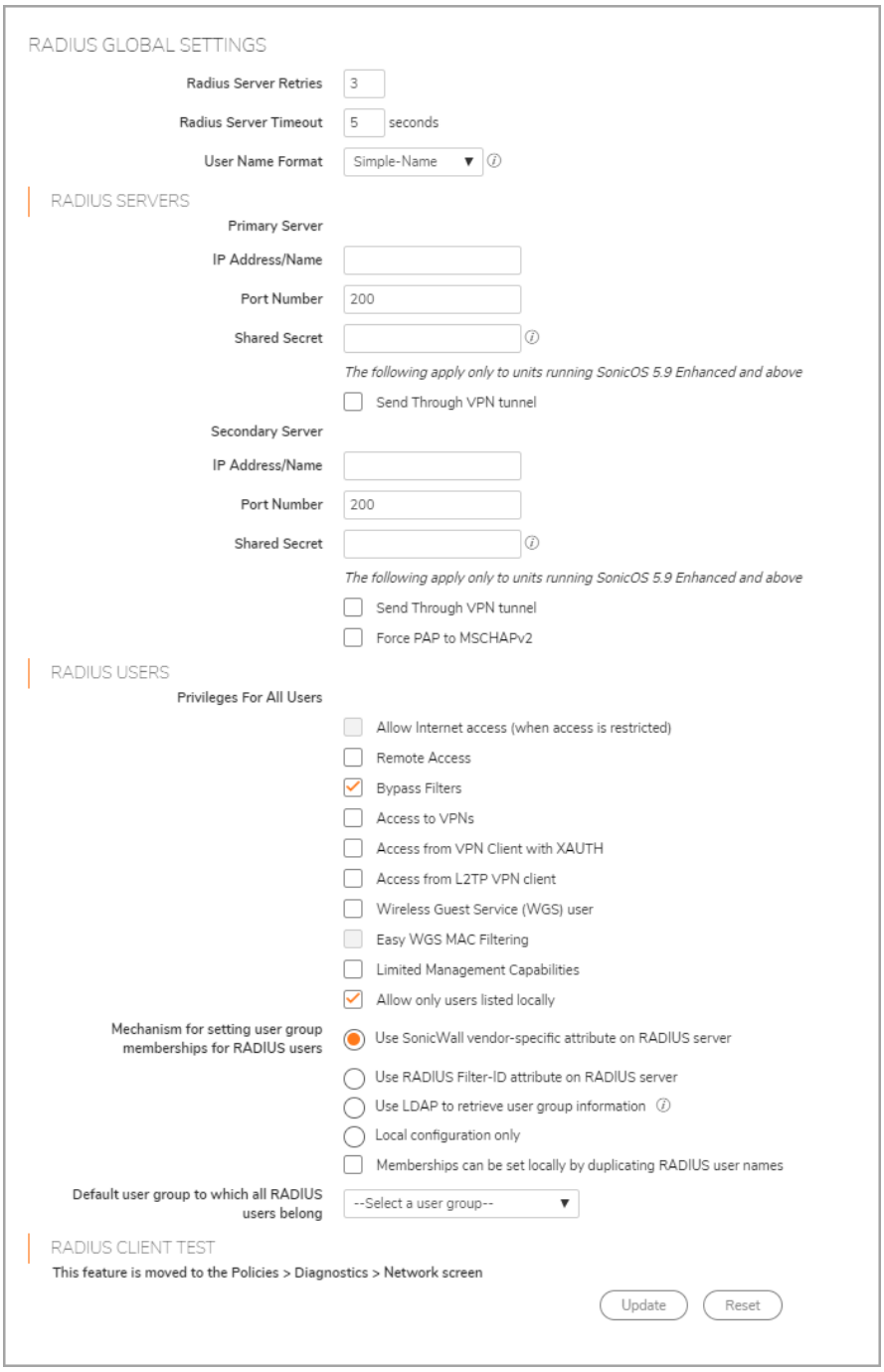
If you selected **Use RADIUS for user authentication** or **Use RADIUS but also allow locally configured users**, you must now configure RADIUS information.

Topics:

Configuring RADIUS

To configure RADIUS Global Settings:

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



2 Define the number of times the SonicWall attempts to contact the RADIUS server in the **Radius Server Retries** field. If the RADIUS server does not respond within the specified number of retries, the connection is dropped. This field can range between 0 and 10, however, at least three (3) Radius Server Retries is recommended.

3 Define the **Radius Server Timeout (seconds)**. The allowable range is 1-60 seconds with a default value of five (**5**).

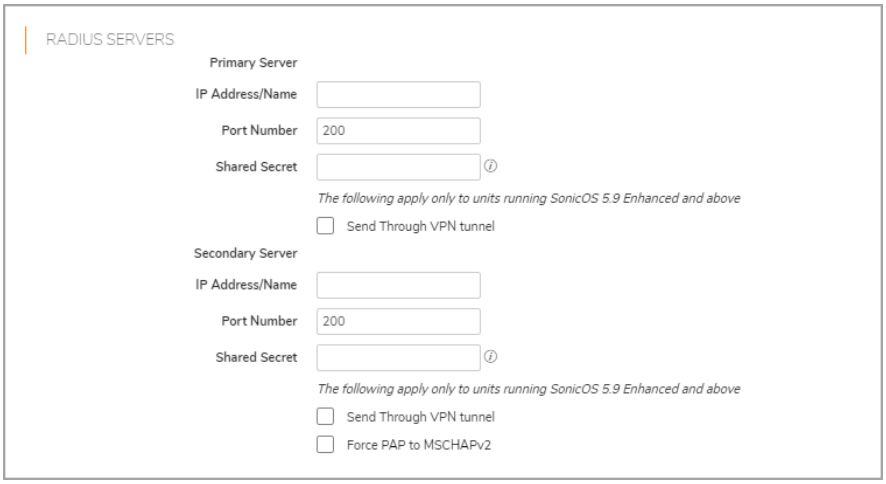
4 Define the **User Name Format** by selecting one of the preferred format styles offered in the drop-down menu.

RADIUS Servers

To configure RADIUS servers:

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

2 Scroll to the **Radius Servers** section.



3 Specify these settings for the primary RADIUS server in the **Primary Server** section:

- Type the IP address of the RADIUS server in the **IP Address/Name** field.
- Type the **Port Number** for the RADIUS server.
- Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.

4 Optionally, select **Send Through VPN tunnel**. This option is not selected by default.

5 If there is a secondary RADIUS server, type the appropriate information in the **Secondary Server** section.

6 Optionally, select **Send Through VPN tunnel**. This option is not selected by default.

7 Optionally, to enforce MS-CHAPv2 RADIUS authentication, select **Force PAP to MSCHAPv2**. This option is not selected by default.

RADIUS Users

To configure RADIUS users:

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

2 Scroll to the **RADIUS Users** section.

3 Select from the list of privileges you would like to provide for ALL users.

> **NOTE:** The **Bypass Filters** and **Limited Management Capabilities** privileges are returned based on membership to user groups named *Content Filtering Bypass* and *Limited Administrators* – these are not configurable.

4 To only allow users that are configured locally, but to still use RADIUS to authenticate them, select **Allow only users listed locally**. This option is selected by default.

5 Select the mechanism used for setting user group memberships for RADIUS users from the following list:

- **Use SonicWall vendor-specific attribute on RADIUS server**: select to tell the RADIUS server to send vendor-specific attributes back to the SonicWall appliance.
- **Use RADIUS Filter-ID attribute on RADIUS server**: select to tell the RADIUS server to send Filter-ID user attributes back to the SonicWall appliance. Filter-ID attributes include the names of user groups that a user belongs to.
- **Use LDAP to retrieve user group information**: To obtain the user group from the LDAP server. To configure LDAP settings, go to **Users > LDAP**.
- **Local configuration only** – If you do not plan to retrieve user group information from RADIUS or LDAP.

6 For a shortcut for managing RADIUS user groups, check **Memberships can be set locally by duplicating RADIUS user names**. When you create users with the same name locally on the security appliance and manage their group memberships, the memberships in the RADIUS database automatically changes to mirror your local changes.

7 If you have previously configured User Groups on the SonicWall, select the group from the **Default user group to which all RADIUS user belong** drop-down menu.

8 You can create a new group by choosing **Create a new user group...** from the list. The Add Group window displays.

9 Click **Update**.

RADIUS Client Test

To test your RADIUS Client user name and password:

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

2 Scroll to the **Diagnostic Data Request** section and click **Client Test**.

3 Ensure that **Radius** is selected as the **Test Type**.

4 Enter a valid user name to test in the **User** field, and a valid user password in the **Password** field.

5 Click **Update**.

If the validation is successful, the **Status** messages changes to **Success**. If the validation fails, the **Status** message changes to **Failure**. After the SonicWall has been configured, a VPN Security Association requiring RADIUS authentication prompts incoming VPN clients to type a User Name and Password into a dialogue box.

6

Configuring LDAP

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

Active Directory support in GMS is not a single-sign on mechanism by itself, but rather the ability for GMS to act as an LDAP client against an Active Directory's LDAP interface using Microsoft's implementation of an LDAP schema. GMS provides extremely flexible schema interoperability, with support for the Microsoft AD schema, the LDAP core schema, the RFC2798 inetOrgPerson schema, and even user-defined schemas. Connectivity to LDAP servers is also flexible, with support from the following protocols:

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

Topics:

LDAP Terms

- **Attribute**—A data item stored in an object in an LDAP directory. 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 throughout LDAP.
- **dc**—The domain component attribute is commonly found at the root of a distinguished name, and is commonly a required attribute.
- **dn**—A distinguished name, that is, a globally unique name for a user or other object. It is made up of a number of components, usually starting with a common name (`cn`) component and ending with a domain specified as two or more domain components (`dc`). For example, `cn=john,cn=users,dc=domain,dc=com`.
- **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 fashions, 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 define the type of entries that an LDAP directory might contain. A sample object class, as used by AD, would be user or group.
- **ou**—The organizational unit attribute is a required component of most LDAP schema implementations.
- **Schema**—The schema is the set of rules or the structure that defines the types of data that can be stored in a directory, and how that data can be stored. Data is stored in the form of entries.
- **TLS**—Transport Layer Security is the IETF standardized version of SSL (Secure Sockets Layer). TLS 1.0 is the successor to SSL 3.0.

Microsoft Active Directory's Classes can be browsed at <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/classes_all.asp>

LDAP / AD Configuration is executed on the **User > Settings** page.

Selecting either **LDAP** or **LDAP+Local Users** and clicking **Update** enables LDAP support, the former using an LDAP directory server exclusively, and the latter using a combination of the LDAP server and the local user database. Upon applying these settings, an informational alert is presented. Because SonicWall is receiving sensitive username and password information from authenticating clients, HTTPS logins are automatically enabled to secure the credential exchanges.

Prerequisites for an Active Directory Configuration

Before beginning your Active Directory configuration, you should prepare your LDAP server and your SonicWall for LDAP over TLS support. This involves installing a server certificate and your LDAP server, and a CA (Certificate Authority) certificate for the issuing CA on your SonicWall. Assuming this has not already been done, the steps for completing these tasks in an Active Directory environment follow:

Configuring the CA on an Active Directory server:

1. Navigate to Window's **Start > Settings > Control Panel > Add/Remove Programs**.
2. Select **Add/Remove Windows Components**.

   NOTE: Skip step numbers 3 through 7 if Certificate Services are already installed.

3. Select **Certificate Services**.
4. Select **Enterprise Root CA** when prompted.
5. Enter the requested information. For detailed information on CA setup, see: https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx.
6. Launch the **Domain Security Policy** application:

   `Start > Run > dompol.msc.`

7. Open **Security Settings > Public Key Policies**.
8. Right click on **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 AD server:

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

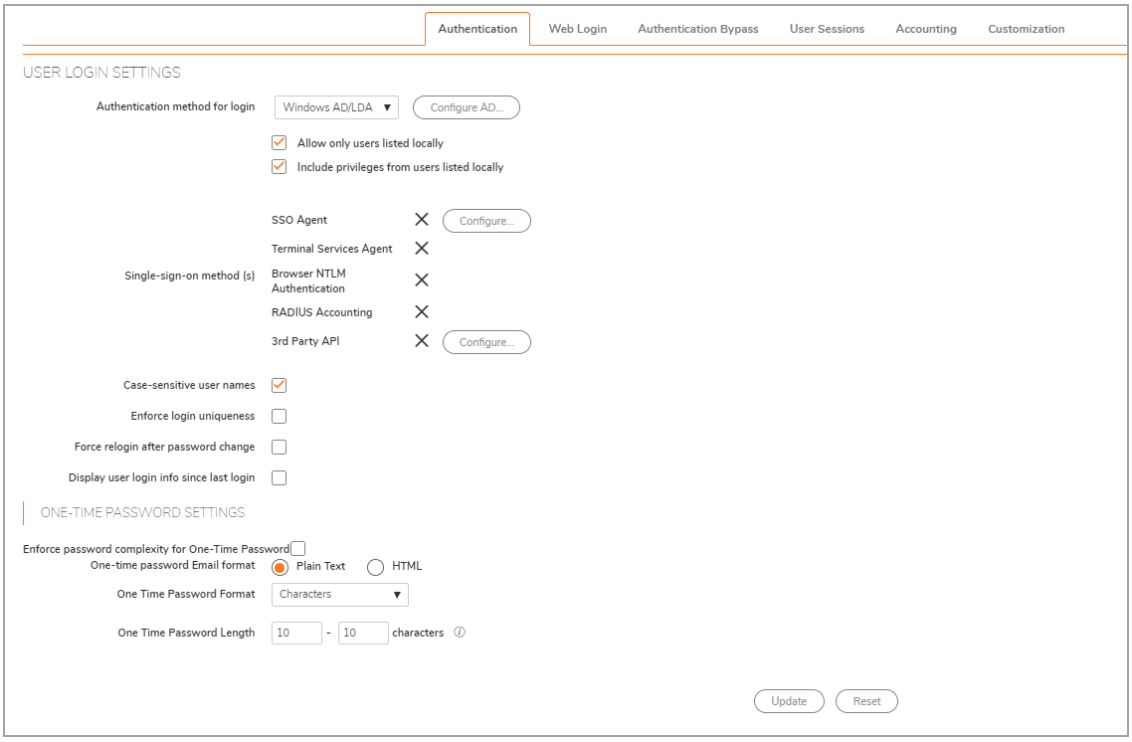
Configuring LDAP

Topics:

Configuring LDAP Authentication

To configure LDAP authentication:

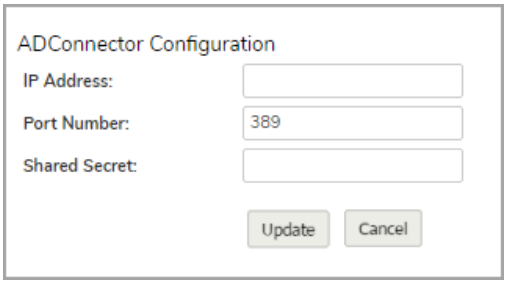
1 Navigate to the **Users > Settings** page.



2 From **Authentication method for login**, select either **Windows AD/LDAP** or **LDAP + Local Users**.

3 Click **Configure AD Connector**.

If you are connected to your firewall through HTTP rather than HTTPS, a message displays warning you of the sensitive nature of the information stored in directory services and offering to change your connection to HTTPS. If you have HTTPS management enabled for the interface to which you are connected (recommended), click **Yes**. The **ADConnector Configuration** dialog displays.



4 After you have established a connection with the LDAP server, navigate to **Users > LDAP** and configure the following options:

- **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 fails.
- **Port Number**—The default LDAP over TLS port number is TCP 636. The default LDAP (unencrypted) port number is TCP **389**, but you can select from the **Standard port choices**

drop-down menu for more options. If you are using a custom listening port on your LDAP server, specify it here.

- **Server timeout (seconds)**—The amount of time, in seconds, that GMS waits for a response from the LDAP server before timing out. The range is 1 to 99999, with a default of **10** seconds.
- **Overall operation timeout (minutes)**—The amount of time, in minutes, to spend on any automatic operation. Five (**5**) minutes is the default time. Some operations, such as directory configuration or importing user groups, can take several minutes, especially when multiple LDAP servers are in use.
- Choose one of these options:
  - **Anonymous Login**—Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (MS AD generally does not), then you could select this option.
  - **Give login name/location in tree**—Select this option to build the distinguished name (dn) that is used to bind to the LDAP server from the `Login user name` and `User tree for login to server` fields according to the following rules:
    - The first name component begins `cn=`.
    - The 'location in tree' components all use `ou=` (apart from certain Active Directory built-ins that begin with `cn=`).
    - The domain components all use `dc=`.
    - If the User tree for the login to server field is given as a `dn`, you can also select this option if the bind `dn` conforms to the first bullet above, but not to the second and/or the third bullet.
  - **Give bind distinguished name**—Select this option if the bind `dn` does not conform to the first bullet above (if the first name component does not begin with `cn=`). This option can always be selected if the `dn` is known. You must provide the bind `dn` explicitly if the bind `dn` does not conform to the first bullet above.
- **Login user name**—Specify a user name that has rights to log in to the LDAP directory. The login name is automatically presented to the LDAP server in full '`dn`' notation. This can be any account with LDAP read privileges (essentially any user account) – Administrative privileges are not required.

  NOTE: This is the user's name, not their login ID (for example, `John Smith` rather than `jsmith`).

- **Login password**—The password for the user account specified above.
- **Protocol version**—Select either LDAPv3 or LDAPv2. Most modern implementations of LDAP, including AD, employ LDAPv3.
- **Use TLS (SSL)**—Use Transport Layer Security (SSL) to log in to the LDAP server. 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 Active Directory, support TLS. Deselecting this default setting provides an alert that must be accepted to proceed.
- **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 when required by your LDAP server.
- **Require valid certificate from server**—Validates the certificate presented by the server during the TLS exchange, matching the name specified above to the name on the certificate. Deselecting this default option presents an alert, but exchanges between GMS and the LDAP server still use TLS – only without issuance validation.

- **Local certificate for TLS**—Optional, to be used only if the LDAP server requires a client certificate for connections. Useful for LDAP server implementations that require passwords to ensure the identity of the LDAP client (AD does not require passwords). This setting is not required for AD.

  If your network uses multiple LDAP/AD servers with referrals, then select one of them 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 GMS to the other servers for users in domains other than its own. For GMS to access 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 the primary server. This might entail creating a special user in the directory for the GMS login.

  NOTE: Only read access to the directory is required.

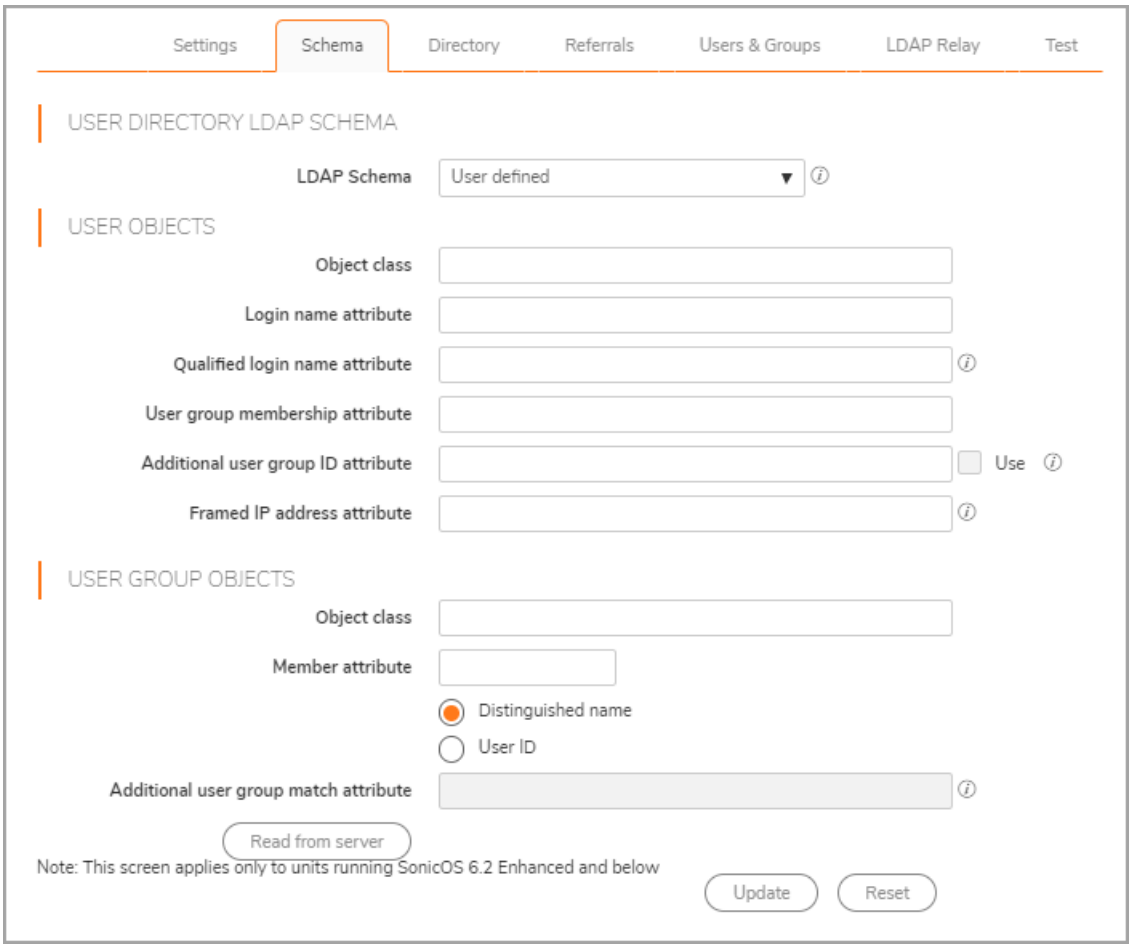
- **Force PAP to MSCHAPv2** – Optional, select this option to enforce MS-CHAPv2 LDAP authentication. If a RADIUS server is also configured, it provides authentication if the LDAP authentication fails. This option is not selected by default.

5 Click **Update**.

Configuring the Schema

To configure the LDAP server schema:

1 Navigate to the **Users > LDAP | Schema** page.



- **LDAP Schema**—Select one of the following from the **LDAP Schema**:

  NOTE: Selecting any of the predefined schemas automatically populates the fields used by that schema with their correct values. These values cannot be changed and their fields are dimmed.

  - **Microsoft Active Directory**
  - **RFC2798 inetOrgPerson**
  - **RFC2307 Network Information Service**
  - **Samba SMB**
  - **Novell eDirectory**
  - **User defined**—Allows you to specify your own values; use this only if you have a specific or proprietary LDAP schema configuration. (default)
- **Object class**—This defines which attribute represents the individual user account to which the next two fields apply.
- **Login name attribute**—This defines which attribute is used for login authentication:
  - **sAMAccountName** for Microsoft Active Directory
  - **inetOrgPerson** for RFC2798 inetOrgPerson
  - **posixAccount** for RFC2307 Network Information Service
  - **sambaSAMAccount** for Samba SMB
  - **inetOrgPerson** for Novell eDirectory
- **Qualified login name attribute**—Optionally, select an attribute of a user object that sets an alternative login name for the user in `name@domain` format. This might be needed with multiple domains in particular, where the simple login name might not be unique across domains.

  NOTE: For **Microsoft Active Directory**, this is normally set to **userPrinicpalName** for log in using `name@domain`, but could be set to **mail** to enable log in by email address. For **RFC2798 inetOrgPerson**, it is set to **mail**.

- **User group membership attribute**—this attribute contains the information in the user object of which groups it belongs to. This is **memberOf** in Microsoft Active Directory. The other pre-defined schemas store group membership information in the group object rather than the user object, and therefore do not use this field.
- **Framed IP address attribute**—this attribute can be used to retrieve a static IP address that is assigned to a user in the directory. Currently it is only used for a user connecting through L2TP with the SonicWall's L2TP server In future, this might also be supported for Global VPN Client. In Active Directory the static IP address is configured in the **Dial-in** view of a user's properties.
- **User Group Objects**—This section is auto-configured unless you select **User Defined** for the **LDAP Schema**.
  - **Object class**—Specify the name associated with the group of attributes.
  - **Member attribute**—Specify the attribute associated with a member.
    - Select whether this attribute is a **Distinguished name** or **User ID**.
  - **Additional user group match attribute**—The `Additional user group ID` user attribute and `Additional user group match` user group attribute allow for a schema that could set additional memberships for a user on top of those that are found through `member/memberOf` attributes, such as Active Directory's primary group attribute.

If the `Additional user group ID` user attribute is set and its use is enabled (**Use** is selected), then when a user object is found with one or more instances of this attribute, a search for additional user groups matching those are made in the LDAP directory. If a group is found with the `Additional user group match` attribute set to that value then the user is also made a member of that group.

NOTE: This additional LDAP sear is comparatively inefficient and so to maximize performance and minimize load on the LDAP server it is only recommended to use this if it is absolutely needed.

TIP: With Active Directory, you can set these to **primaryGroupID** and **primaryGroupToken** to include membership of their primary user group (typically `Domain Users`) for users.

- **Read from server**—Click to read the user group object information from the LDAP server.

NOTE: You must enter the primary domain on the **Directory** page first.

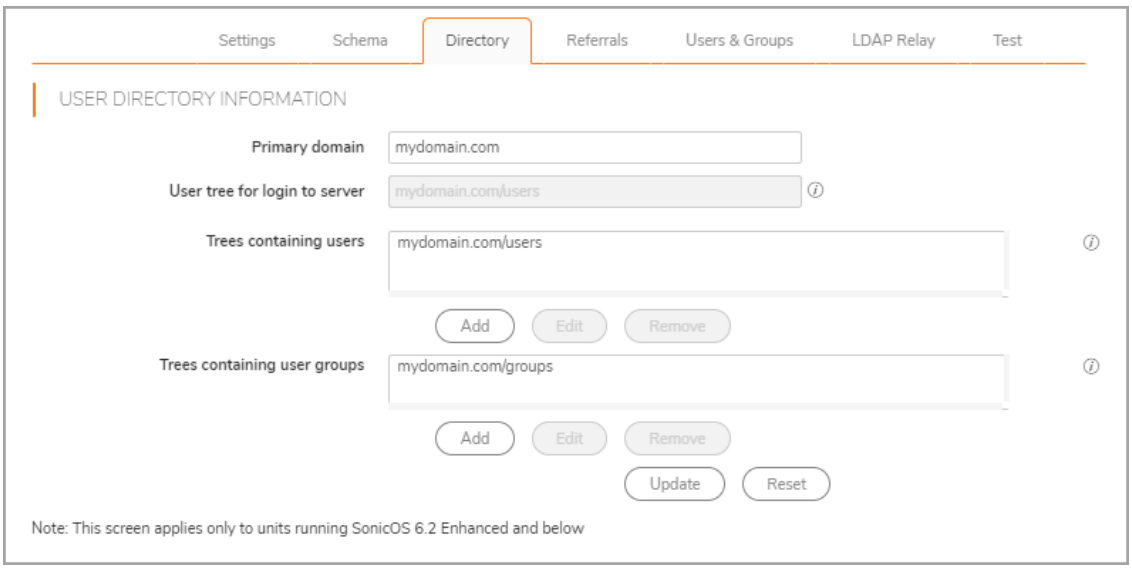
- Select whether you want to **Automatically update the schema configuration** or **Export details of the schema**.

2 Click **Update**.

Configuring the Directory

To configure the Directory:

1 Navigate to the **Users > LDAP | Directory** page.



- **Primary Domain**—specify the user domain used by your LDAP implementation. For AD, this is the Active Directory domain name; for example, `yourADdomain.com`. Changes to this field, optionally, automatically update the tree information in the rest of the page. This is set to **mydomain.com** by default for all schemas except Novell eDirectory, for which it is set to **o=mydomain**.
- **User tree for login to server**—The tree in which the user specified in **Settings** resides. For example, in AD the administrator account's default tree is the same as the user tree.
- **Trees containing users**—The trees where users commonly reside in the LDAP directory. One default value is provided that can be edited, and up to a total of 64 DN values can be added by

clicking **Add**. GMS searches the directory using them all until a match is found or when the list is exhausted. If you have created other user containers within your LDAP or AD directory, you should specify them here.

- **Trees containing user groups**—Same as the previous, only with regard to user group containers, and a maximum of 32 DN values can be added by clicking **Add**. These are only applicable when there is no user group membership attribute in the schema's user object, and are not used with AD.

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

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

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

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

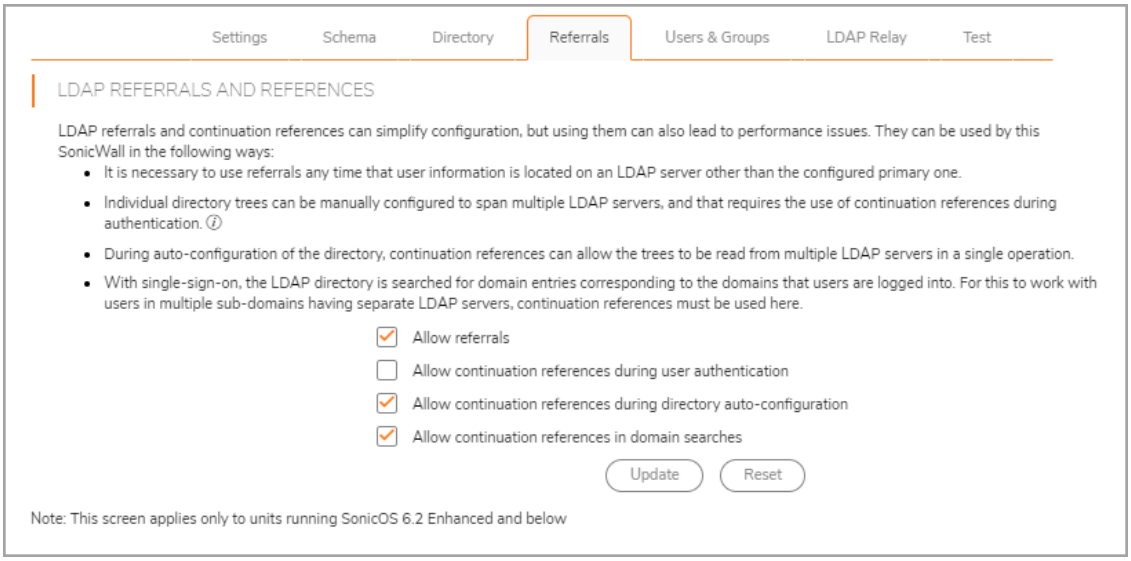
2 Click **Update**.

NOTE: The auto-configuration process might also locate trees that are not needed for user login. You can manually remove these entries, which might be worthwhile.

Configuring Referrals

To configure LDAP server referrals:

1 Navigate to the **Users > LDAP | Referrals** page.



2 Configure these fields:

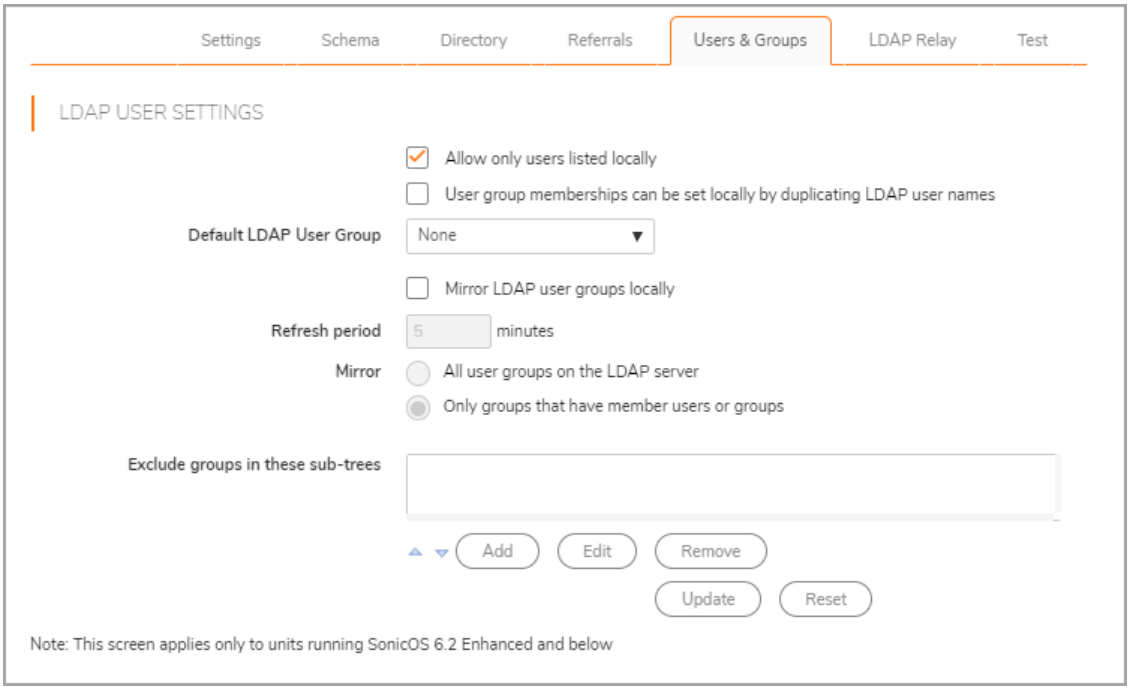
- **Allow referrals**—Select this option any time that user information is located on an LDAP server other than the configured primary one.
- **Allow continuation references during user authentication**—Select this option any time that individual directory trees have been manually configured to span multiple LDAP servers.
- **Allow continuation references during directory auto-configuration**—Select this option to allow the trees to be read from multiple LDAP servers in a single operation.
- **Allow continuation references in domain searches**—Select this option when using single-sign-on with users in multiple sub-domains having separate LDAP servers.

3 Click **Update**.

Configuring LDAP Users & Groups

To configure the LDAP users and groups settings:

1 Navigate to the **Users > LDAP | Users & Groups** page.



2 Configure these fields:

- **Allow only users listed locally** – Requires that LDAP users also be present in the GMS local user database for logins to be allowed.
- **User group membership can be set locally by duplicating LDAP user names** – Allows for group membership (and privileges) to be determined by the intersection of local user and LDAP user configurations.
- **Default LDAP User Group** – A default group on GMS to which LDAP users belong in addition to group memberships configured on the LDAP server.

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

  GMS can retrieve group memberships more efficiently in the case of Active Directory by taking advantage of its unique trait of returning a `memberOf` attribute for a user.

  The list of users read from the LDAP server can be quite long, and you might not want to import all of them. **Remove** is provided, along with several methods of selecting unwanted users. You can use these options to reduce the list to a manageable size and then select the users to import.

  Having users in GMS with the same name as existing LDAP users allows SonicWall user privileges to be granted upon successful LDAP authentication.
- **Mirror** – Select the type of user groups that are mirrored by choosing:
  - **All user groups on the LDAP server**

- **Only groups that have member users or groups**

- **Exclude groups in these sub-trees** – Enter groups to be excluded in this field using **Add**. You can reorder, edit, and remove groups using the buttons underneath the field.

3 Click **Update**.

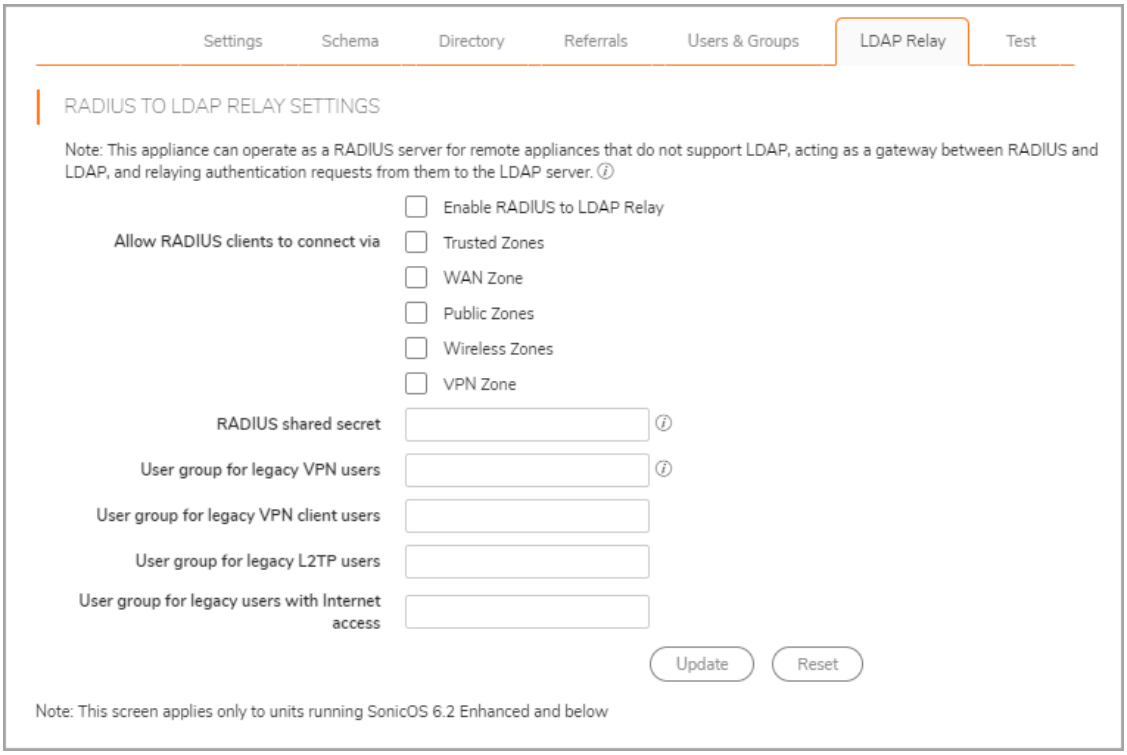
Configuring LDAP Relay

The RADIUS to LDAP Relay feature is designed for use in a topology where there is a central site with an LDAP/AD server and a central SonicWall, with remote satellite sites connected into it through low-end SonicWall security appliances that might not support LDAP. In that case, the central SonicWall can operate as a RADIUS server for the remote SonicWalls, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

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 through LDAP. This avoids what can be very complex configuration of an external RADIUS server such as IAS for those SonicWalls.

To configure the LDAP server relay settings:

1 Navigate to the **Users > LDAP | LDAP Relay** page.



2 Configure these LDAP Relay options:

- **Enable RADIUS to LDAP Relay** – Enables this feature.
- **Allow RADIUS clients to connect via** - Check the relevant checkboxes and policy rules are added to allow incoming Radius requests accordingly.
- **RADIUS shared secret** - This is a shared secret common to all remote SonicWalls.

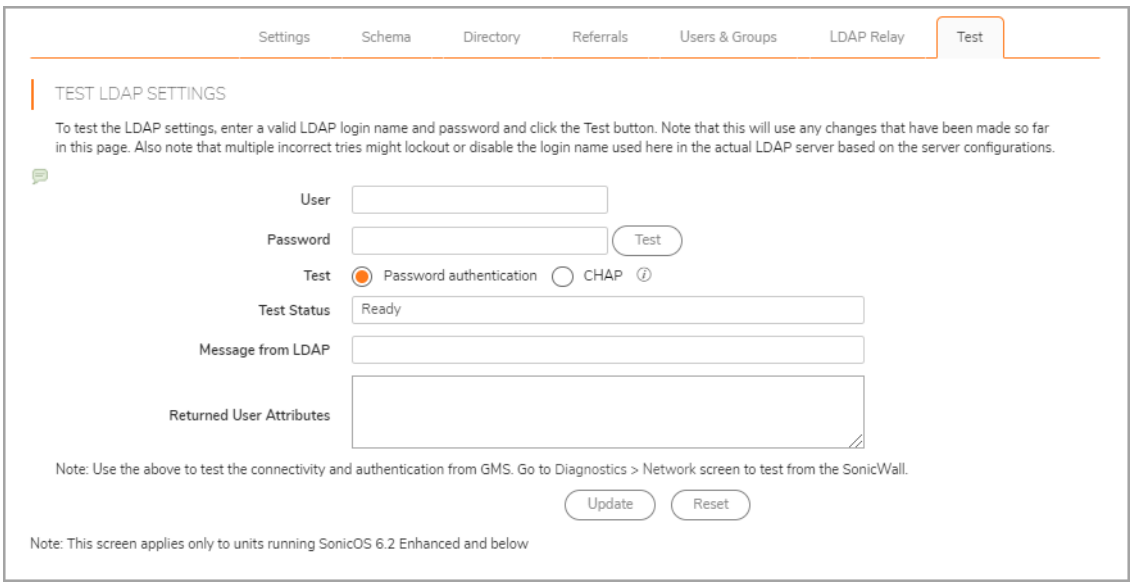
- **User group for legacy VPN users** – Defines the user group that corresponds to the legacy **Access to VPNs** privileges. When a user in this user group is authenticated, the remote SonicWall is notified to give the user the relevant privileges.
- **User group for legacy VPN client users** – Defines 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.
- **User group for legacy L2TP users** – Defines 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.
- **User group for legacy users with Internet access** – Defines 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.

Configuring Test Settings

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

To configure the LDAP server test settings:

1 Navigate to the **Users > LDAP | Test** page to test the configured LDAP settings.



2 Enter a valid LDAP login name in the **User** field.

3 Enter the password for the LDAP login name in the **Password** field.

4 Choose the type of test:

- **Password authentication**
- **CHAP**

5 Click **Test**. The results are displayed in the **Test Status** and **Returned User Attributes** sections.

More Information on LDAP Schemas

- **Microsoft Active Directory**: Schema information is available at https://msdn.microsoft.com/library?url=/library/en-us/ldap/ldap/ldap_reference.asp
- **RFC2798 InetOrgPerson**: Schema definition and development information is available at <http://rfc.net/rfc2798.html>
- **RFC2307 Network Information Service**: Schema definition and development information is available at <http://rfc.net/rfc2307.html>
- **Samba SMB**: Development information is available at <http://us5.samba.org/samba/>
- **Novell eDirectory**: LDAP integration information is available at <http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/h0000007.html>
- **User-defined schemas**: See the documentation for your LDAP installation.

7

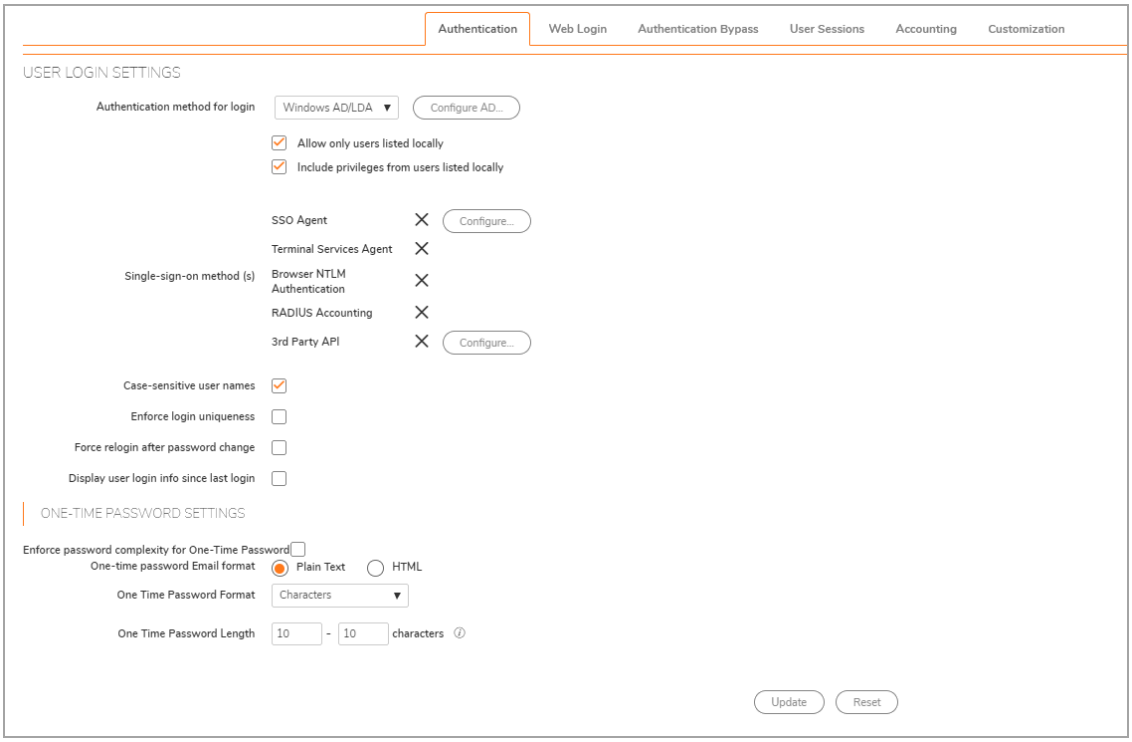
Configuring Multi-LDAP

Topics:

Managing Multi-LDAP Integration

To manage a multi-LDAP integration:

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

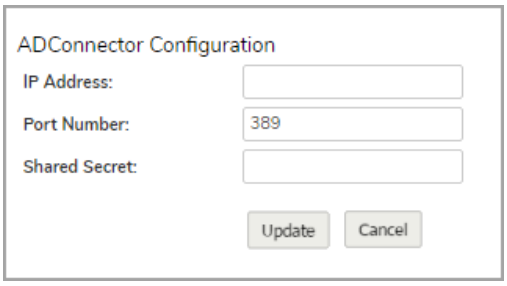


2 From **Authentication method for login**, select either **Windows AD/LDAP** or **LDAP + Local Users**.

3 Click **Configure AD Connector**.

If you are connected to your firewall through HTTP rather than HTTPS, a message displays warning you of the sensitive nature of the information stored in directory services and offering to change your

connection to HTTPS. If you have HTTPS management enabled for the interface to which you are connected (recommended), click **Yes**. The **ADConnector Configuration** dialog displays.



4 After you have established a connection with the LDAP server, you can begin to add multiple LDAP servers by navigating to **Users > Multi-LDAP | Settings** and click **Add**. Additional options appear.

5 Configure the following:

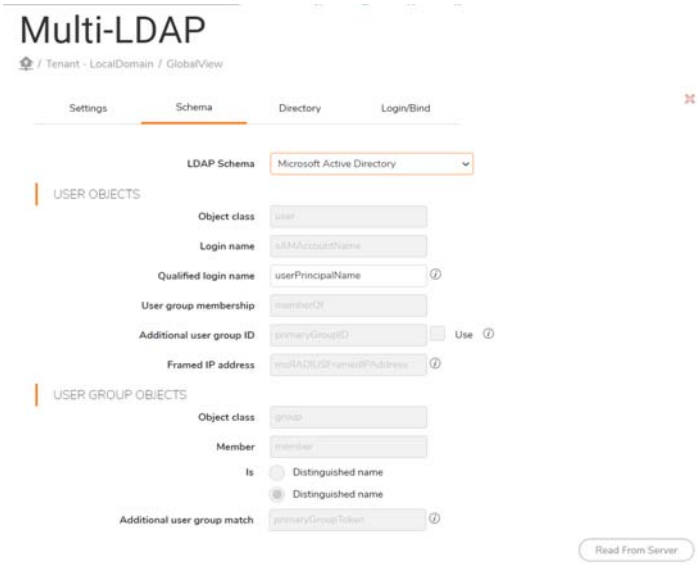
- **Role**—Select a role for the server you are adding. You can choose a primary LDAP server role, secondary server, or backup/replica server.
- **Name or IP Address**—Enter the FQDN or the IP address of the LDAP server against which you wish to authenticate. If using a name, be certain it can be resolved 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 fails.
- **Port Number**—The default LDAP over TLS port number is TCP 636. The default LDAP (unencrypted) port number is TCP **389**, but you can select from the **Standard port choices** drop-down menu for more options. If you are using a custom listening port on your LDAP server, specify it here.
- **Server timeout (seconds)**—The amount of time, in seconds, that GMS waits for a response from the LDAP server before timing out. The range is 1 to 99999, with a default of **10** seconds.
- **Overall operation timeout (minutes)**—The amount of time, in minutes, to spend on any automatic operation. Five (**5**) minutes is the default time. Some operations, such as directory configuration or importing user groups, can take several minutes, especially when multiple LDAP servers are in use.
- **Use TLS (SSL)**—Use Transport Layer Security (SSL) to log in to the LDAP server. 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 Active Directory, support TLS. Deselecting this default setting provides an alert that must be accepted to proceed.
- **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 when required by your LDAP server.

6 Click **Update**.

Configuring the Schema

To configure the LDAP server schema:

1 Navigate to the **Users > Multi-LDAP | Schema** page.



- **LDAP Schema**—Select one of the following from the **LDAP Schema**:

  > **NOTE:** Selecting any of the predefined schemas automatically populates the fields used by that schema with their correct values. These values cannot be changed and their fields are dimmed.

  - **Microsoft Active Directory** (default)
  - **RFC2798 inetOrgPerson**
  - **RFC2307 Network Information Service**
  - **Samba SMB**
  - **Novell eDirectory**
  - **User defined**—Allows you to specify your own values; use this only if you have a specific or proprietary LDAP schema configuration.
- **Object class**—This defines which attribute represents the individual user account to which the next two fields apply.
- **Attributes Login name** —This defines which attribute is used for login authentication:
  - **sAMAccountName** for Microsoft Active Directory
  - **inetOrgPerson** for RFC2798 inetOrgPerson
  - **posixAccount** for RFC2307 Network Information Service
  - **sambaSAMAccount** for Samba SMB
  - **inetOrgPerson** for Novell eDirectory
- **Qualified login name** —Optionally, select an attribute of a user object that sets an alternative login name for the user in `name@domain` format. This might be needed with multiple domains in particular, where the simple login name might not be unique across domains.

  > **NOTE:** For **Microsoft Active Directory**, this is normally set to **userPrinicpalName** for log in using `name@domain`, but could be set to **mail** to enable log in by email address. For **RFC2798 inetOrgPerson**, it is set to **mail**.

- **User group membership** —this attribute contains the information in the user object of which groups it belongs to. This is **memberOf** in Microsoft Active Directory. The other pre-defined

schemas store group membership information in the group object rather than the user object, and therefore do not use this field.

- **Framed IP address**—this attribute can be used to retrieve a static IP address that is assigned to a user in the directory. Currently it is only used for a user connecting through L2TP with the SonicWall's L2TP server In future, this might also be supported for Global VPN Client. In Active Directory the static IP address is configured in the **Dial-in** view of a user's properties.
- **User Group Objects**—This section is auto-configured unless you select **User Defined** for the **LDAP Schema**.
  - **Object class**—Specify the name associated with the group of attributes.
  - **Attributes Member**—Specify the attribute associated with a member.
    - Select whether this attribute is a **Distinguished name** or **User ID**.
  - **Additional user group match**—The `Additional user group ID` user attribute and `Additional user group match` user group attribute allow for a schema that could set additional memberships for a user on top of those that are found through `member/memberOf` attributes, such as Active Directory's primary group attribute.

    If the `Additional user group ID` user attribute is set and its use is enabled (**Use** is selected), then when a user object is found with one or more instances of this attribute, a search for additional user groups matching those are made in the LDAP directory. If a group is found with the `Additional user group match` attribute set to that value then the user is also made a member of that group.

NOTE: This additional LDAP sear is comparatively inefficient and so to maximize performance and minimize load on the LDAP server it is only recommended to use this if it is absolutely needed.

TIP: With Active Directory, you can set these to **primaryGroupID** and **primaryGroupToken** to include membership of their primary user group (typically `Domain Users`) for users.

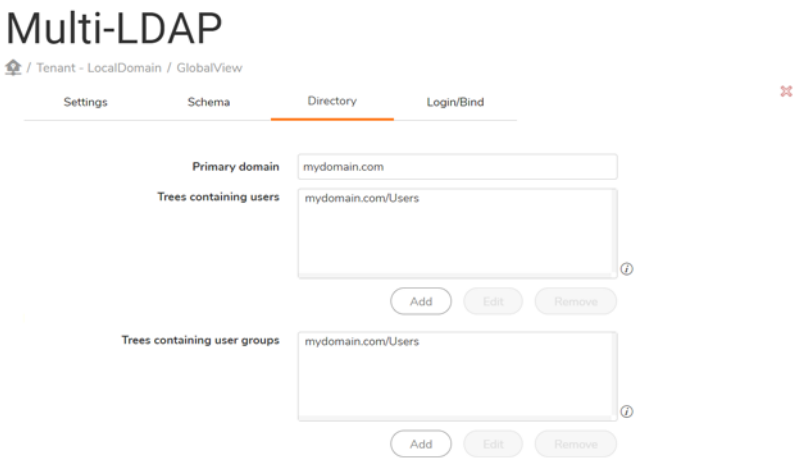
- **Read from server**—Click to read the user group object information from the LDAP server.

NOTE: You must enter the primary domain on the **Directory** page first.

Configuring the Directory

To configure the Directory:

1 Navigate to the **Users > Multi-LDAP | Directory** page.



- **Primary Domain**—specify the user domain used by your LDAP implementation. For AD, this is the Active Directory domain name; for example, `yourADdomain.com`. Changes to this field, optionally, automatically update the tree information in the rest of the page. This is set to **mydomain.com** by default for all schemas except Novell eDirectory, for which it is set to **o=mydomain**.
- **Trees containing users**—The trees where users commonly reside in the LDAP directory. One default value is provided that can be edited, and up to a total of 64 DN values can be added by clicking **Add**. GMS searches the directory using them all until a match is found or when the list is exhausted. If you have created other user containers within your LDAP or AD directory, you should specify them here.
- **Trees containing user groups**—Same as the previous, only with regard to user group containers, and a maximum of 32 DN values can be added by clicking **Add**. These are only applicable when there is no user group membership attribute in the schema's user object, and are not used with AD.

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

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

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

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

Configuring Login/Bind

1 Navigate to **Users > Multi-LDAP | Login/Bind**.

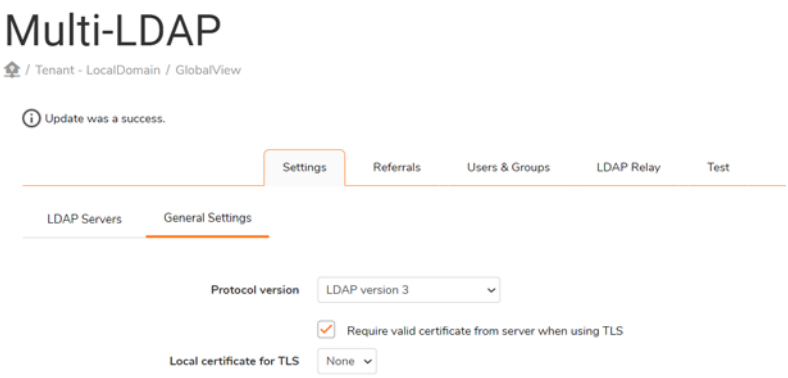
Choose one of the following radio buttons:

- **Anonymous Login** – Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (Active Directory generally does not), then you might select this option.
- **Give login name/location in tree** – Select this option to build the distinguished name (dn) that is used to bind to the LDAP server from the Login user name and User tree for login to server fields according to the following rules:
  - The first name component begins cn=
  - The 'location in tree' components all use ou= (apart from certain Active Directory built-ins that begin with cn=)
  - The domain components all use dc=
  - If the User tree for login to server field is given as a dn, you can also select this option if the bind dn conforms to the first bullet above, but not to the second and/or the third bullet.
- **Give bind distinguished name** – Select this option if the bind dn does not conform to the first bullet above (if the first name component does not begin with cn=). This option can always be selected if the dn is known. You must provide the bind dn explicitly if the bind dn does not conform to the first bullet above.

- **Login user name** – Provide the user account to use to log in to (bind) to the LDAP server.
- **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 to login (bind) to the LDAP server.
- **Password** – The password for the user account specified above.
- **When referred to other servers** – Choose between **Bind with this account** or **Bind with an equivalent account on that server (same password)**.

Configuring the General Settings

1 Navigate to **Users > Multi-LDAP | Settings | General Settings**.



2 Configure the following:

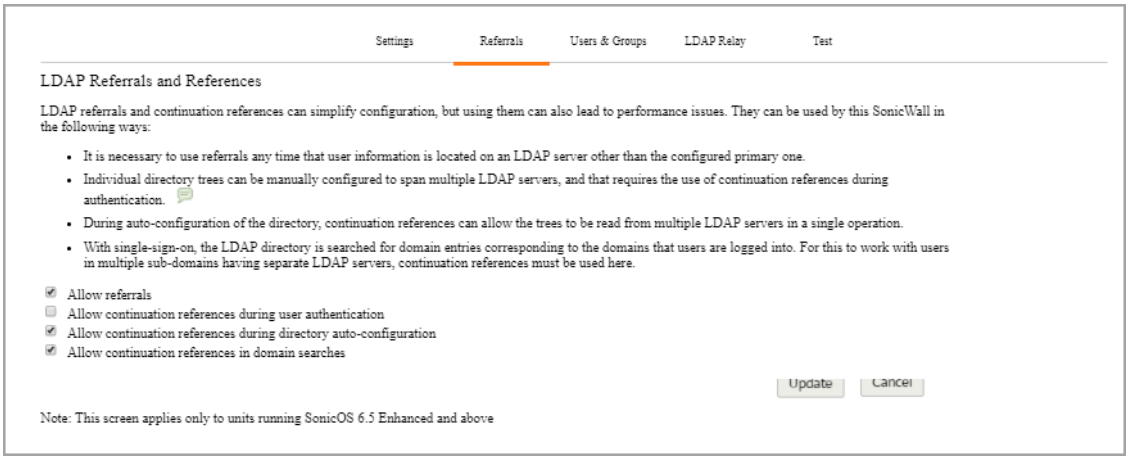
- **Protocol version** – Select either LDAPv3 or LDAPv2 from the drop-down menu. Most modern implementations of LDAP, including Active Directory, employ LDAPv3.
- **Require valid certificate from server** – Validates the certificate presented by the server during the TLS exchange, matching the name specified above to the name on the certificate. Deselecting this default option presents an alert, but exchanges between GMS and the LDAP server still use TLS – only without issuance validation.
- **Local certificate for TLS** – Optional, to be used only if the LDAP server requires a client certificate for connections. Useful for LDAP server implementations that require passwords to ensure the identity of the LDAP client (Active Directory does not require passwords). This setting is not required for Active Directory.

  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 GMS to the other servers for users in domains other than its own. For GMS 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 the login to the primary server. This might entail creating a special user in the directory for the GMS login. Note that only read access to the directory is required.

Configuring Referrals

To configure LDAP server referrals:

1 Navigate to the **Users > Multi-LDAP | Referrals** page.



2 Configure these fields:

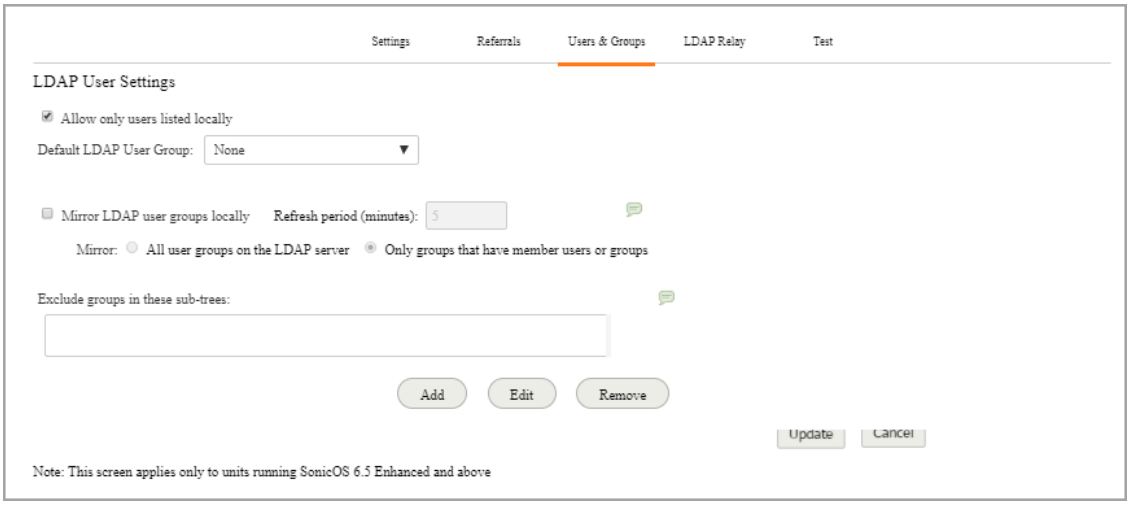
- **Allow referrals**—Select this option any time that user information is located on an LDAP server other than the configured primary one.
- **Allow continuation references during user authentication**—Select this option any time that individual directory trees have been manually configured to span multiple LDAP servers.
- **Allow continuation references during directory auto-configuration**—Select this option to allow the trees to be read from multiple LDAP servers in a single operation.
- **Allow continuation references in domain searches**—Select this option when using single-sign-on with users in multiple sub-domains having separate LDAP servers.

3 Click **Update**.

Configuring Multi-LDAP Users & Groups

To configure the LDAP users and groups settings:

1 Navigate to the **Users > Multi-LDAP | Users & Groups** page.



2 Configure these fields:

- **Allow only users listed locally** – Requires that LDAP users also be present in the GMS local user database for logins to be allowed.
- **Default LDAP User Group** – A default group on GMS to which LDAP users belong in addition to group memberships configured on the LDAP server.

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

  GMS can retrieve group memberships more efficiently in the case of Active Directory by taking advantage of its unique trait of returning a `memberOf` attribute for a user.

  The list of users read from the LDAP server can be quite long, and you might not want to import all of them. **Remove** is provided, along with several methods of selecting unwanted users. You can use these options to reduce the list to a manageable size and then select the users to import.

  Having users in GMS with the same name as existing LDAP users allows SonicWall user privileges to be granted upon successful LDAP authentication.

- **Mirror LDAP user groups locally** – When this option is enabled, GMS periodically auto-imports user groups and user group nestings (memberships where groups are members of other groups) from the LDAP server(s) to create local user groups that mirror those in the LDAP directory.

  These mirror user groups are listed separately on the Users/Local Groups page and have names that include the domain in which they are located. They can be selected in access rules, CFS policies, and so on, just like other local user groups, although there are a few restrictions with them such as they cannot have other user groups added as members locally on the SonicWall (although they can be made members of other local user groups and local users can be made members of them). Users who are members of a user group on the LDAP server are automatically given any access privileges set through its local mirror group.

The groups are imported from the directory trees and configured from the trees containing user group lists in the **Directory** view, and filters can be set below to exclude importing groups from the given sub-trees under those.

The maximum number of user groups that can be imported is limited per product and an event log is generated when not all of the groups found on the LDAP server can be imported because of exceeding that.

> **TIP:** To avoid hitting this limit, select to import only groups that have members or set filters to avoid importing unnecessary groups. To see an XML list of all the user groups that you might want to mirror, enter the following in the browser's address bar: `https://ip-address/ldapMirror.xml`.

- **Mirror** – Select the type of user groups that are mirrored by choosing:
  - **All user groups on the LDAP server**
  - **Only groups that have member users or groups**
- **Exclude groups in these sub-trees** – Enter groups to be excluded in this field using **Add**. You can reorder, edit, and remove groups using the buttons underneath the field.

3 Click **Update**.

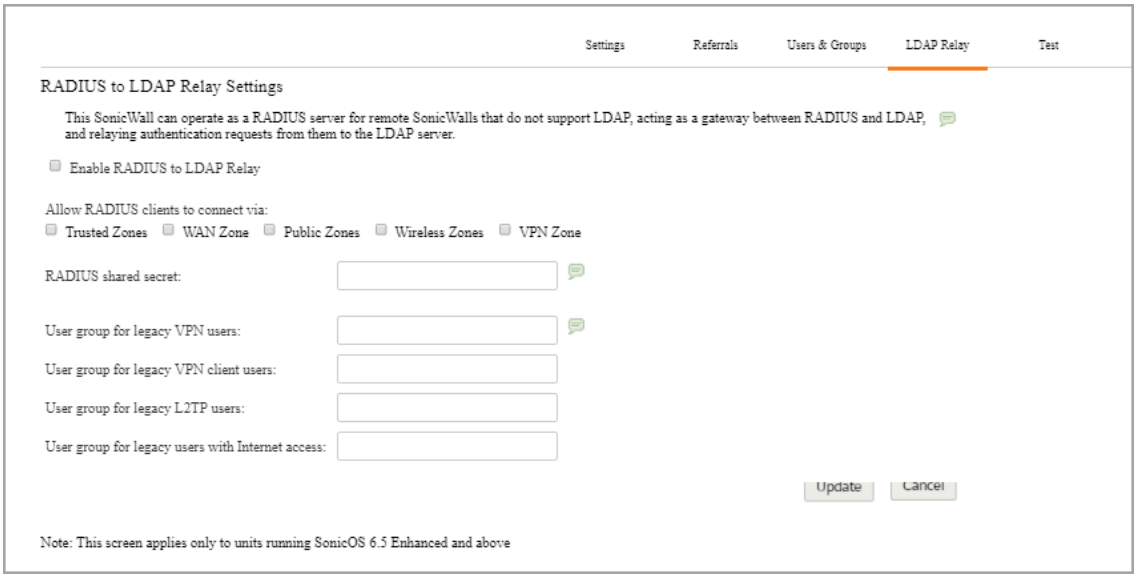
Configuring LDAP Relay

The RADIUS to LDAP Relay feature is designed for use in a topology where there is a central site with an LDAP/AD server and a central SonicWall, with remote satellite sites connected into it through low-end SonicWall security appliances that might not support LDAP. In that case, the central SonicWall can operate as a RADIUS server for the remote SonicWalls, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

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 through LDAP. This avoids what can be very complex configuration of an external RADIUS server such as IAS for those SonicWalls.

To configure the LDAP server relay settings:

1 Navigate to the **Users > Multi-LDAP | LDAP Relay** page.



2 Configure these LDAP Relay options:

- **Enable RADIUS to LDAP Relay** – Enables this feature.
- **Allow RADIUS clients to connect via** - Check the relevant checkboxes and policy rules are added to allow incoming Radius requests accordingly.
- **RADIUS shared secret** - This is a shared secret common to all remote SonicWalls.
- **User group for legacy VPN users** – Defines 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.
- **User group for legacy VPN client users** – Defines 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.
- **User group for legacy L2TP users** – Defines 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.
- **User group for legacy users with Internet access** – Defines 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.

Configuring Test Settings

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

To configure the LDAP server test settings:

1 Navigate to the **Users > Multi-LDAP | Test** page to test the configured LDAP settings.

2 Choose the test method:

- **Via Firewall**
- **Via GMB**

3 Choose the type of test:

- **Connectivity/bind test**
- **User authentication test**
- **LDAP search**

4 Click **Test**. The results are displayed in the **Test Status** and **Returned User Attributes** sections.

8

Configuring TACACS+

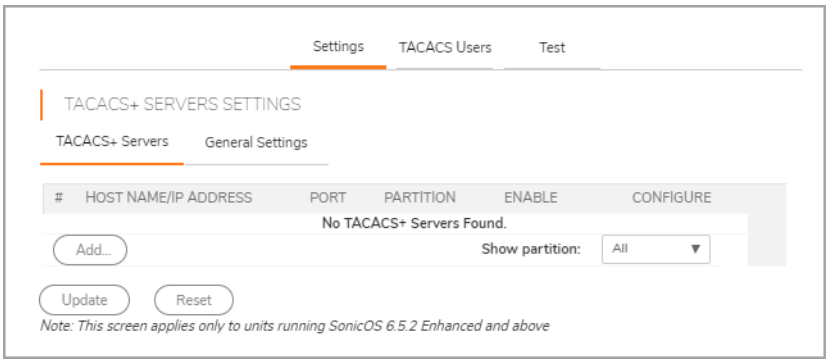
If you selected **Use TACACS+ for user authentication** or **Use TACACS+ but also allow locally configured users**, you must now configure TACACS+ information.

Topics:

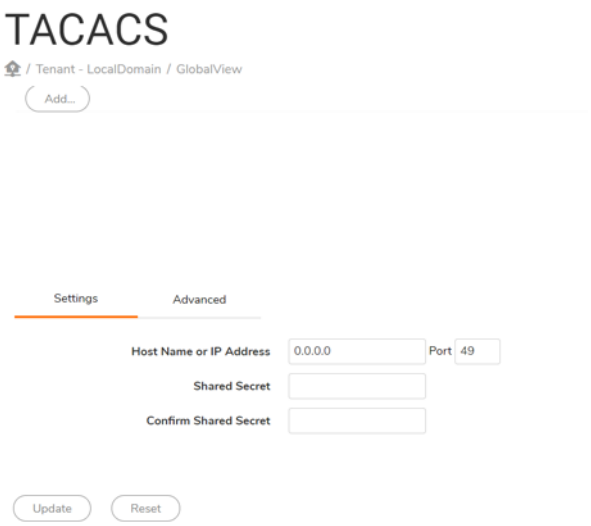
Configuring TACACS+ Servers

To configure TACACS+ servers:

1 Navigate to the **Users > TACACS+ | Settings** page.



2 Under the **TACACS+ Servers** view, click **Add**.



3 Enter the **Host Name or IP Address** of the TACACS+ server and port number.

4 Enter a **Port**. The default port is **49**.

5 Enter and confirm the **Shared Secret**.

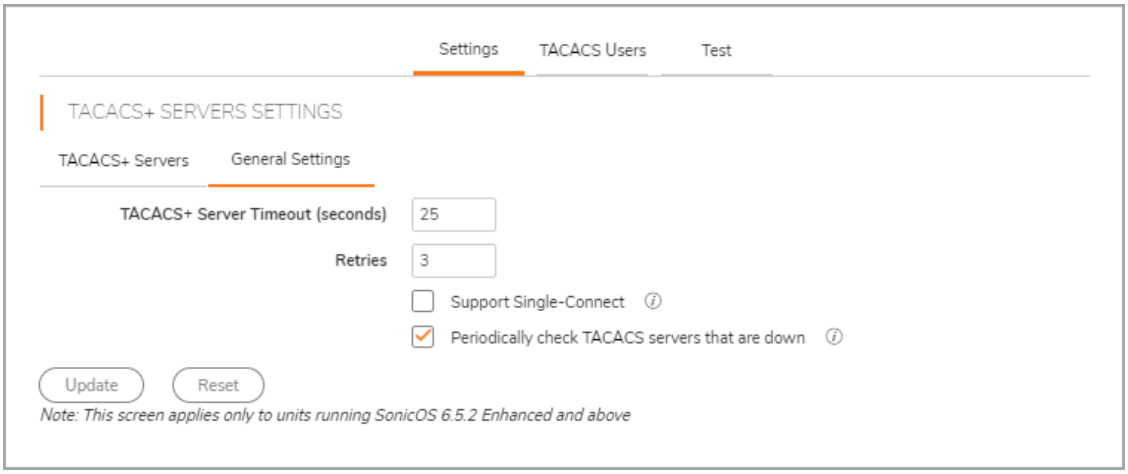
6 If you want to send the traffic through a VPN tunnel, click **Advanced** and then check **Send Through VPN tunnel**.

7 Click **Update**.

Configuring TACACS+ General Settings

To configure TACACS+ general settings:

1 Navigate to the **Users > TACACS+ | Settings | General Settings** page.



2 Specify the **TACACS+ Server Timeout** in seconds. The default is **25** seconds.

3 Define the number of times the SonicWall attempts to contact the TACACS+ server in the **Retries** field. If the TACACS+ server does not respond within the specified number of retries, the connection is dropped. This field can range between 0 and 10, **3** tries is the default value.

4 If you want to enable Single-Connect, check **Support Single-Connect**. Using Single-Connect, you can support multiple TACACS+ sessions using a single TCP connection.

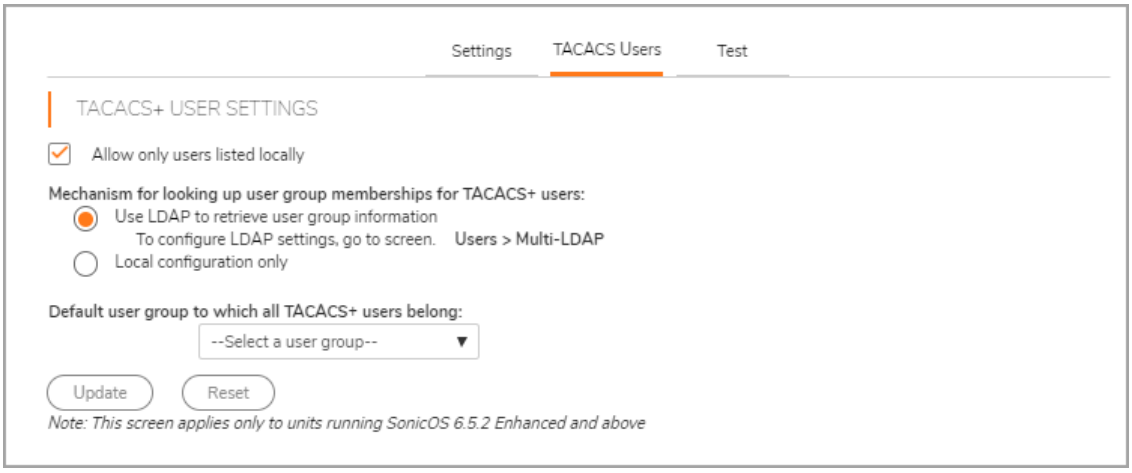
5 If you want GMS to check for malfunctioning servers - unresolved DNS and so on, check the **Periodically check TACACS servers that are down** option.

6 Click **Update**.

TACACS+ Users

To configure TACACS+ users:

1 Navigate to the **Users > TACACS+ | TACACS Users** page.



2 To allow only those users who are configured locally, but to still use TACACS+ to authenticate them, select **Allow only users listed locally**.

3 Select the mechanism used for setting user group memberships for TACACS+ users from the following list:

- **Use LDAP to retrieve user group information**: select to tell the RADIUS server to send vendor-specific attributes back to the SonicWall appliance.
- **Local configuration only**: select when you want TACACS+ users to use local settings only.

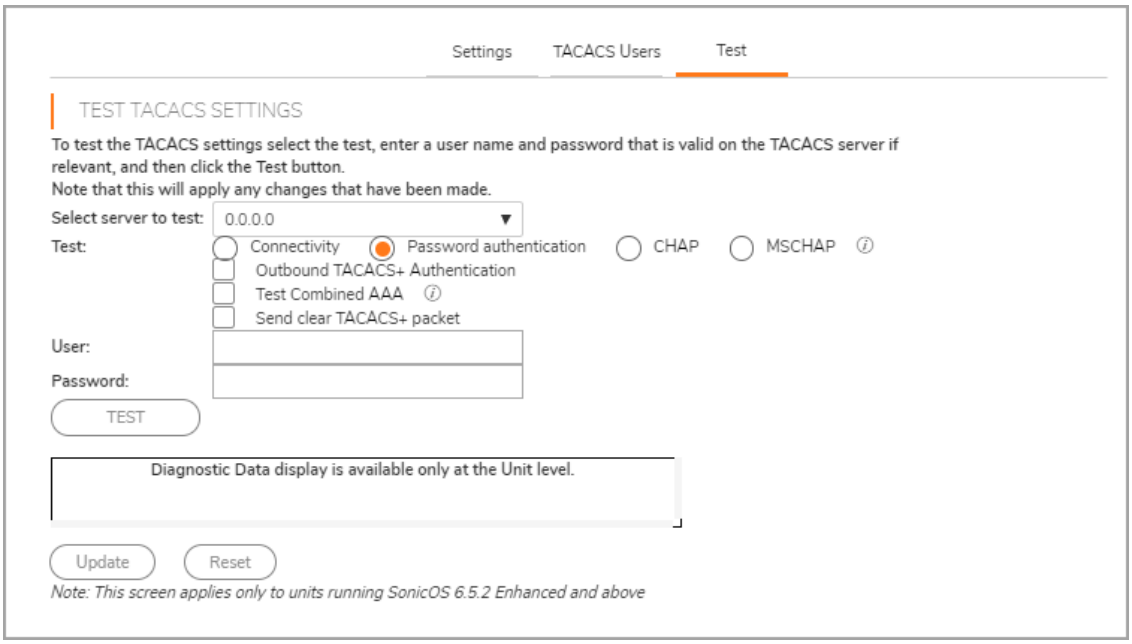
4 From the drop-down menu select the user group for all TACACS+ users.

5 Click **Update**.

TACACS+ Test

To test your TACACS+ Settings:

1 Navigate to the **Users > TACACS+ | Test** page.



2 Select the server to test from the drop-down list.

3 Check one of the radio buttons based on what you want to check. You can check **Connectivity**, **Password Authentication**, **CHAP**, or **MS-CHAP**.

4 Select one of the check-boxes for the type of testing you would like to complete:

- **Outbound TACACS+ Authentication**
- **Test Combined AAA**
- **Send clear TACACS+ packet**

5 Enter a **User Name** and **Password**.

6 Click **Test**.

If the validation is successful, the **Status** message changes to **Success**. If the validation fails, the **Status** message changes to **Failure**.

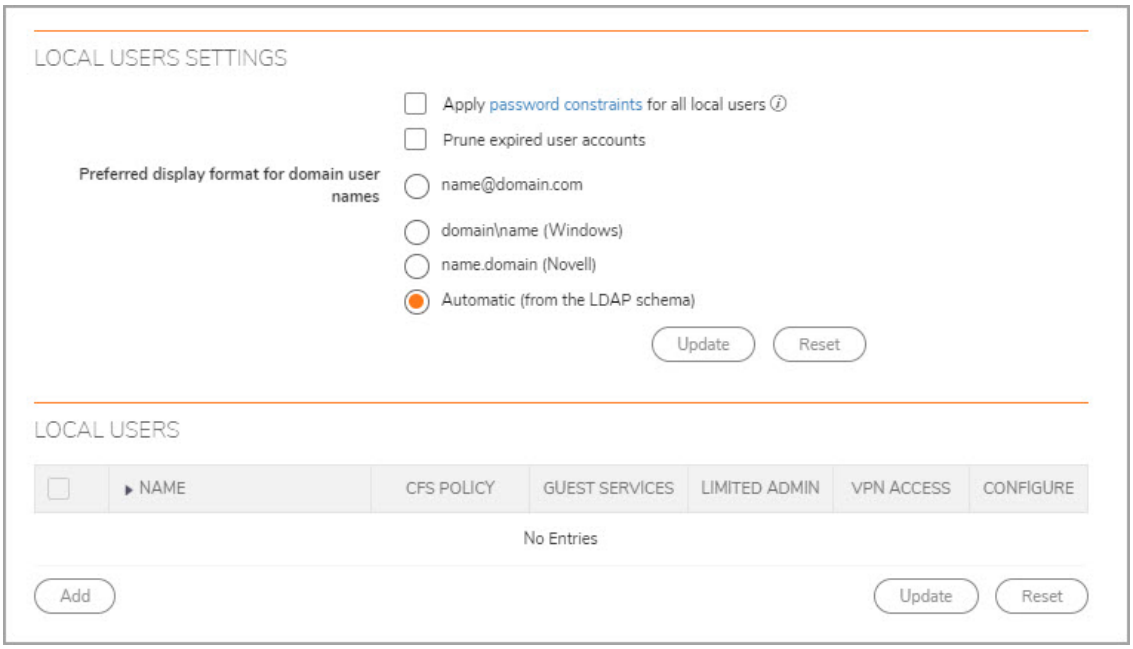
9

Configuring Local Users

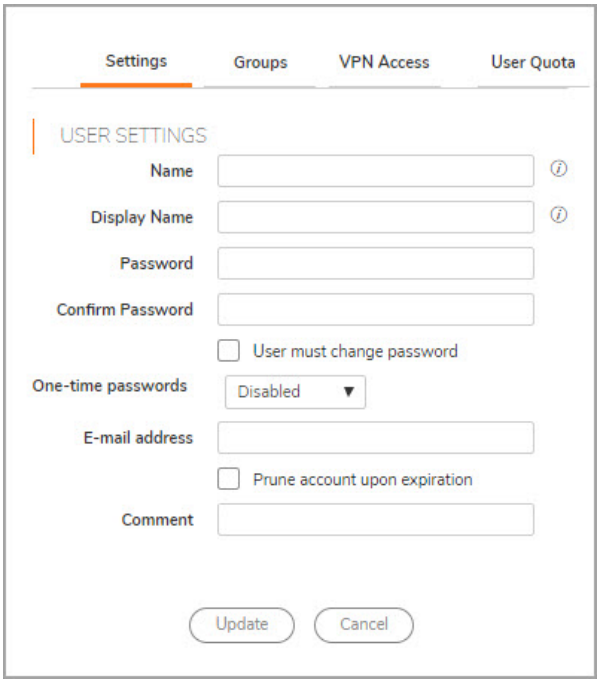
GMS uses a Group/User hierarchy for organizing users. This section describes how to configure new users and groups.

To add or edit a user:

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



2 To add a local group, click **Add**. To edit the settings of an existing user, click its **Configure** icon.



3 Configure the following options:

- **Name**—name of the user.
- **Display Name**—the user's name as you would like it displayed
- **Password/Confirm**—password of the user.

4 Optionally, select **User must change password** to force users to change their passwords the first time they login. This option is not selected by default.

5 From **One-time password method**, 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. Go to Step 12.
- **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 smart-phone.

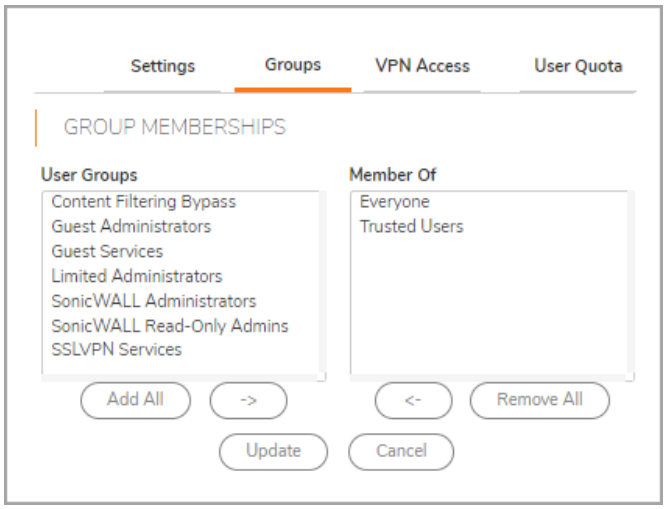
  The **unbind totp key** displays.

6 Enter the user's email address so they can receive one-time passwords.

7 Optionally, enter a comment in the **Comment** field.

8 Click the **Groups** view.

Groups



1 Select one or more **User Groups** to which this user is a member and click the right arrow (**>**). Repeat this step for each group to add. You can also choose **Add All**.

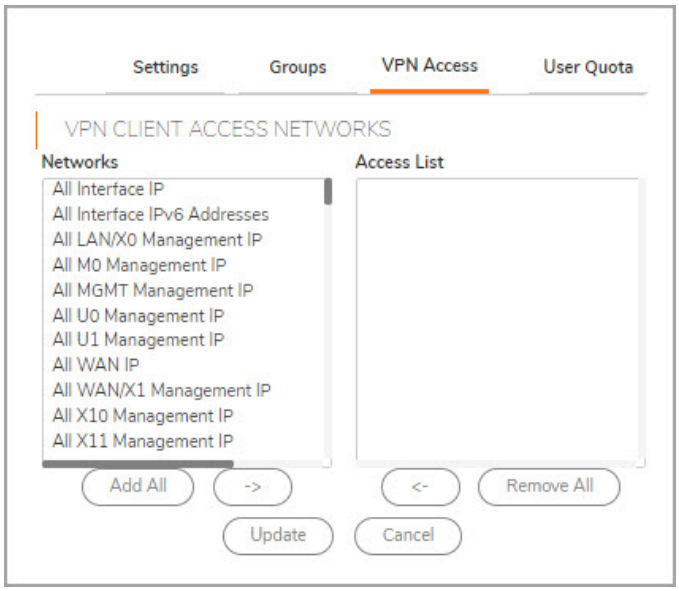
> **NOTE:** To remove a user from a group:
>
> 1 Select the group from the **Member of** list.
>
> 2 Either:
>
> - Click the **Left Arrow <-**.
> - Click **Remove All**.

> **NOTE:** You cannot delete **Everyone** and **Trusted Users** from **Member Of**.

3 To configure which network resources VPN users (either GVC, NetExtender, or Virtual Office bookmarks) can access, click **VPN Access**.

4 Click the **VPN Access** view.

VPN Access



1 Select one or more networks from **Networks**.

2 Click the **Right Arrow** (**->**). Repeat this step for each network to add.

> **NOTE: VPN Access** affects the ability of remote clients using GVC, NetExtender, and Virtual Office bookmarks to access network resources. To allow these users to access a network resource, the network address objects or groups must be added to the **Access List**.

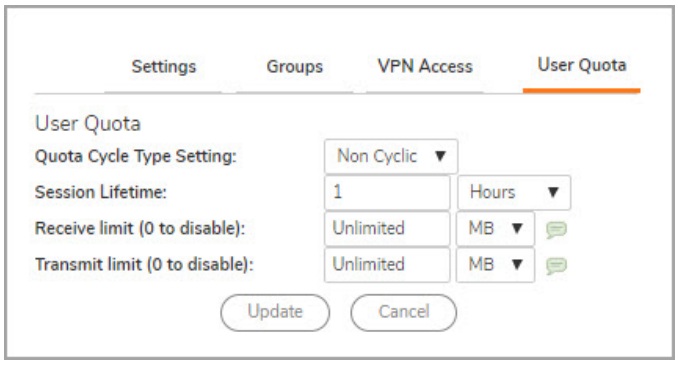
3 To remove the user's access from a network:

- Select the network(s) from the **Access List**, and then click **Left Arrow (<-)**.
- Click **Remove All**.

4 When you are finished, click **OK**. The settings are saved. Repeat this procedure for each user to add or modify.

5 Click **User Quota**.

User Quota



1 Configure the options.

2 Click **Update** to complete the User configuration.

10

Configuring Local Groups

By default, GMS includes the following groups:

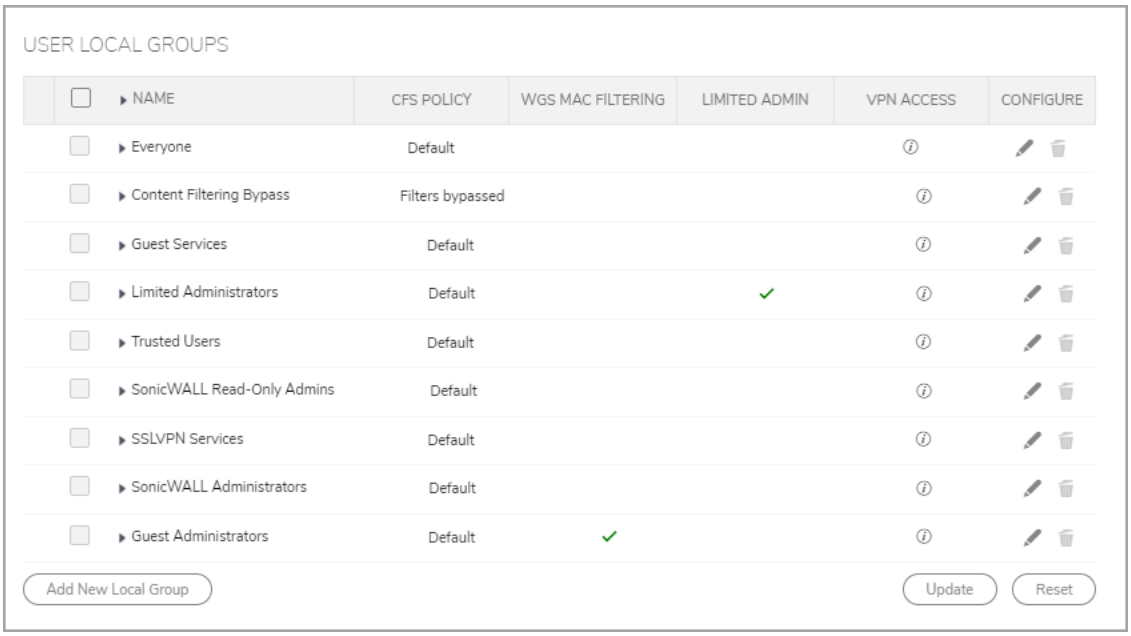
- Everyone
- Guest Services
- Limited Administrators
- Trusted Users
- SonicWall Read-Only Admins
- SSLVPN Services
- SonicWall Administrators
- Guest Administrators

The permissions of these groups are automatically applied to its members unless you manually modify a user's settings.

To add or edit a group:

1 Navigate to the **Users > Local Groups** page.

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 **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.

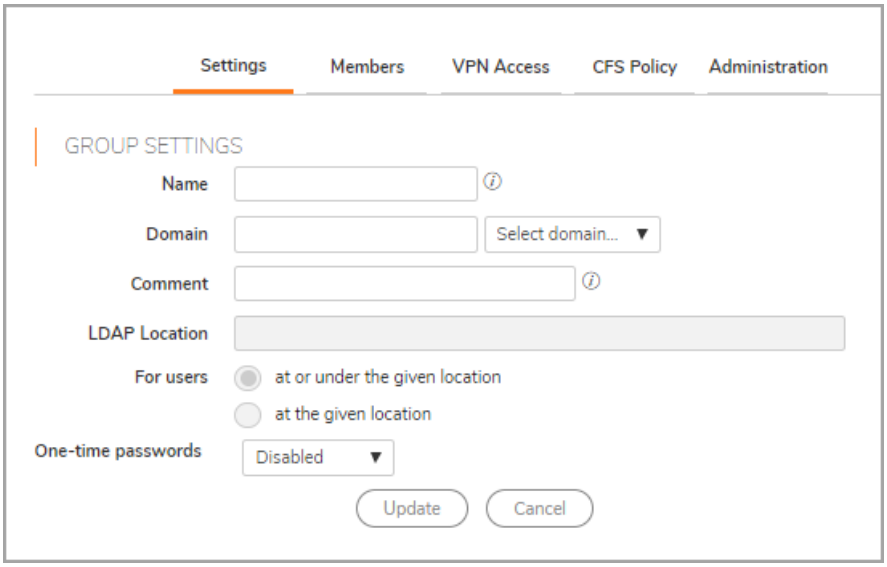
  For remote users, a **Comment** icon displays `Not applicable with remote authentication`.

- **Limited 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`.

- **Comment** – Lists any comment provided for the local group.
- **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.
- **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.

2 To add a local group, click **Add New Local Group**. To edit the settings of an existing group, click **Configure**.



3 Enter a name for the new local group in the **Name** field.

> **NOTE:** The name of a predefined user or group cannot be edited and the field is dimmed.

4 Enter the domain name in the **Domain** field. You can select the Domain from the drop-down menu. If you enter a domain name that is not listed, you must enter the full domain name or a message is displayed.

5 Optionally, enter a comment about the local group in the **Comment** field.

6 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:

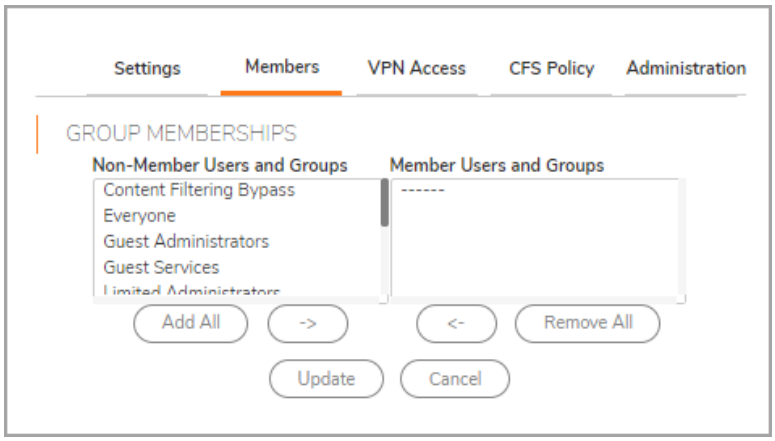
- **at or under the given location** (default)
- **at the given location**

7 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.

8 Click **Update**.

9 Click the **Members** view.

Members



1 Select the members or groups that belong to this group and click the right arrow (**->**).

Click **Add All** to add all users and groups.

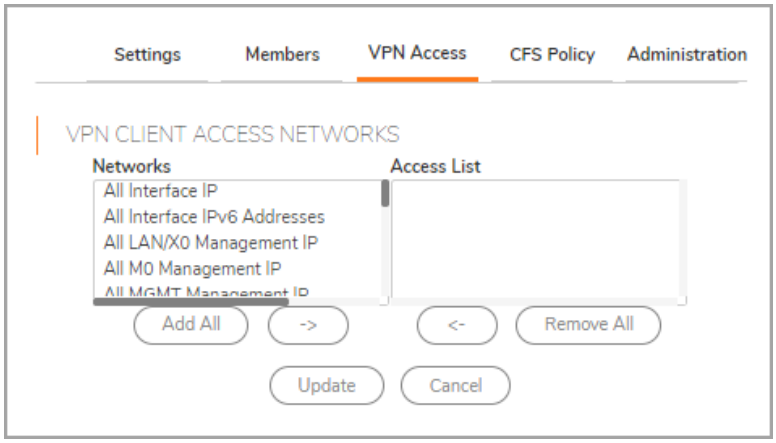
> **NOTE:** You can add any group as a member of another group except **Everybody** and **All LDAP Users**. Be aware of the membership of the groups you add as members of another group.

To remove users and/or groups, from the **Member Users and Groups** list, select the user(s) and/or group(s) and click the **Left Arrow <-**. To remove all users and groups, click **Remove All**.

2 Click **Update**.

3 Click the **VPN Access** view.

VPN Access



1 From the **Networks** list, select the network resource(s) to which this group has VPN Access by default.

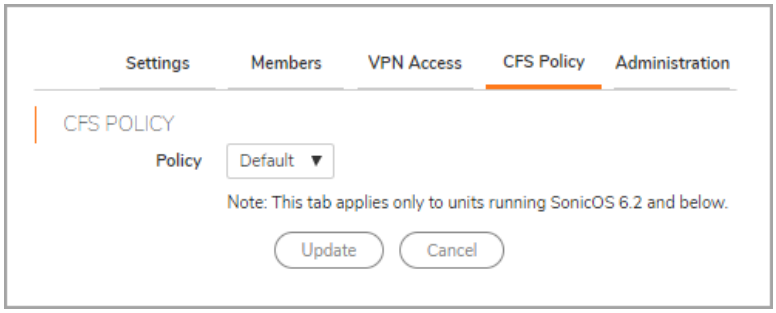
> **NOTE:** Group VPN access settings affect remote clients and SSL VPN Virtual Office bookmarks.

2 Click the **Right Arrow ->** to add the resource(s) to **Access List**.

To remove resource(s), from the **Member Users and Groups** list, select the resource(s) and click the **Left Arrow <-**. To remove resources, click **Remove All**.

3 Click the **CFS Policy** view.

CFS Policy

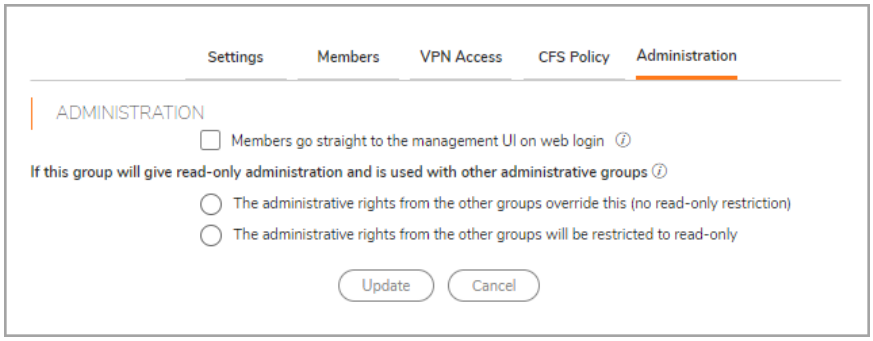


1 Select a CFS policy to apply to the group in the **Policy** drop-down menu.

2 When you are finished, click **Update**. The settings are saved.

3 Click the **Administration** view.

Administration



1 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.

2 The **If this read-only admin group 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.

3 Click **Update** to complete the configuration.

Editing Local Groups

To edit a local group:

1 Navigate to **Users > Local Groups**.

2 Click the **Edit** icon in the Configuration column for the group that you want to edit. The **Edit Group** dialog displays, which is the same as the **Add Group** dialog.

3 Follow the steps in Configuring Local Groups.

11

Configuring Guest Services

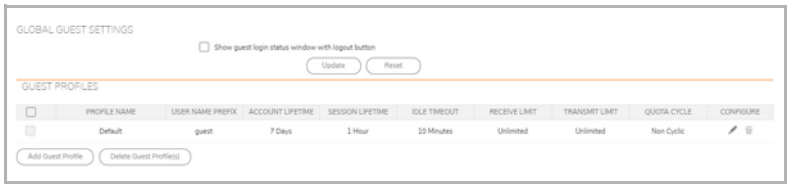
Guest Services determine the limits and configuration of the guest accounts. Guest accounts are temporary accounts set up for users to log into your network.

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

Configuring Guest Services

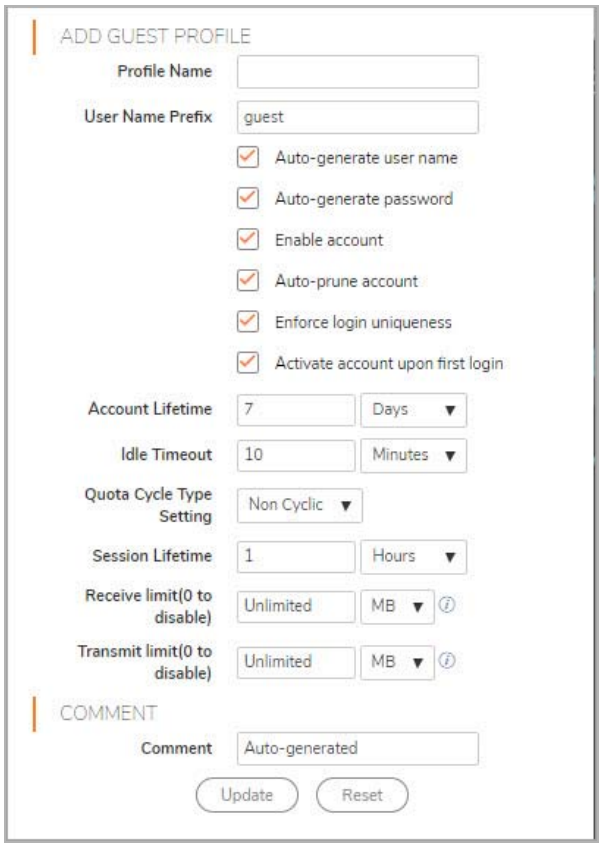
To configure Guest Services:

1 Navigate to the **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 **Update** 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 Configuring Guest Services.

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**.

12

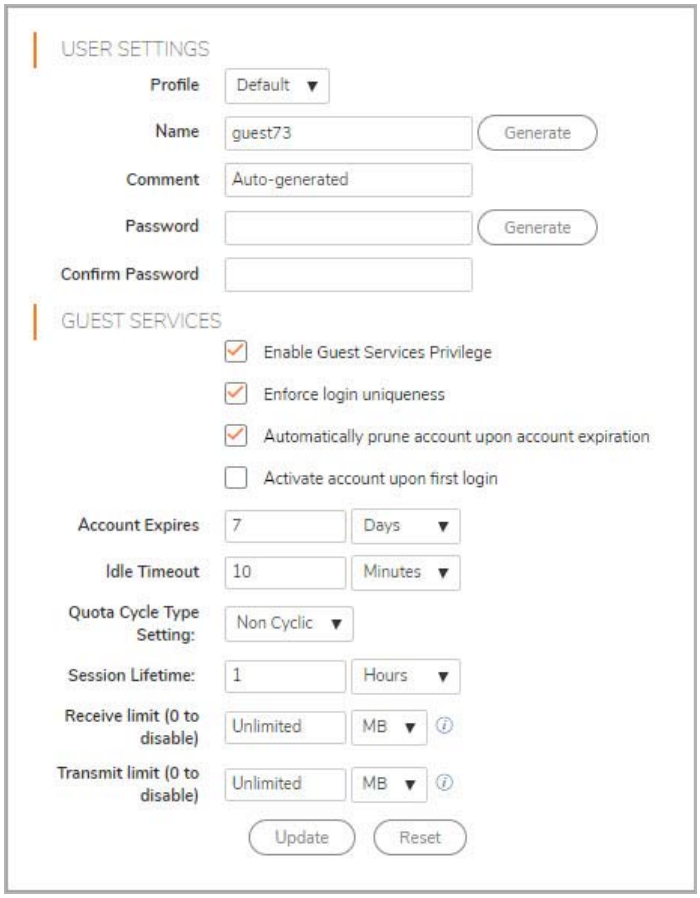
Configuring Guest Accounts

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.

To add a new guest account:

1 Navigate to the **Users > Guest Accounts** page.

2 Under the list of guest accounts, click **Add Guest Account**.



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.
- **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.
- To begin the timing for the account expiration, select **Activate account upon first login**.
- **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 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**.

4 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**

5 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**.

6 **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.

7 **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.

8 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).

9 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).

10 Click **Update** to generate the 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 Configuring Guest Accounts.

Deleting Guest Accounts

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**.

To delete one or more guest accounts:

1 Navigate to **Users > Local Users** or **Local 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**.

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**.

13

SonicWall Support

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

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.SonicWall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.SonicWall.com/support/contact-support.

About This Document

Legend

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

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

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

Global Management System Users Setup Users Administration Guide
Updated - January 2021
Software Version - 9.3
232-005129-00 RevB