User Management

This chapter describes how to manage users, user groups, and configure user authentication settings. It includes the following sections:

To access the Users pages, click **Users** in the left hand navigation pane.

Viewing Active User Sessions

Use the Active User Sessions page to view information for all active user sessions that are currently logged into the security appliance. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data. Click the **Logout** icon to terminate a web login user session or a VPN user session.

Users > Active User Sessions

Field	Description
User Name	Name of the logged user.
IP Address	Host IP address from which the user accessed the security appliance.
Login Method	How the user logs into the security appliance, such as WEB, SSL VPN, IPsec Remote Access, or Captive Portal.
Session Time	Time that the user has logged into the security appliance.

Configuring Users and User Groups

This section describes how to maintain the users and user groups in local database. Refer to the following topics:

- **Default User and User Group, page 389**
- **Available Services for User Groups, page 389**
- **Preempt Administrators, page 390**
- **Configuring Local Users, page 390**
- **Configuring Local User Groups, page 391**

Default User and User Group

The security appliance maintains user and user group information in the local database. The local database supports up to 100 users and 50 user groups. A user group can include up to 100 users. Any user must be a member of a user group.

The default administrator account ("cisco") has full privilege to set the configuration and read the system status. The default administrator account cannot be deleted. For security purposes, you must change the default administrator password at the first login. See Changing the Default Administrator Password, page 32.

The default user group ("admin") has the administrative web login access ability and enables the SSL VPN, IPsec Remote Access, and Captive Portal services. The default user group cannot be deleted, but its service policy can be modified.

Available Services for User Groups

A user can only belong to one user group. The users in the same user group share the same service policy. A user group has only one service policy. The services available for a user group include:

- **Web Login:** Allows the members of the user group to log into the Configuration Utility through the web browser to view the configuration only or to set the configuration.
- **SSL VPN:** Allows the members of the user group at remote sites to establish the SSL VPN tunnels based on the selected SSL VPN group

policy to access your network resources. The Cisco AnyConnect Secure Mobility Client software must be installed on user's PC.

- **IPsec Remote Access:** Allows the members of the user group at remote sites to establish the VPN tunnels to securely access your network resources.
- **Captive Portal:** Allows the wireless users who have authenticated successfully to be directed to a specified web page (portal) before they can access the Internet. This service only applies to ISA550W and ISA570W.

NOTE The security appliance can perform the authentications in parallel when multiple services need to authenticate at the same time.

Preempt Administrators

When an administrator attempts to log in while another administrator is logged in, a warning message appears saying "Another administrative user is logged into the application. Do you want to take control of the session? (The other user will be logged out.)" Click **Yes** to preempt the current administrator, or click **No** to return to the login screen.

Configuring Local Users

Use the Users and Groups page to view, add, edit, or delete local users. The local database supports up to 100 users.

STEP 1 Click **Users > Users and Groups**.

The Users and Groups window opens. All existing local users are listed in the Local Users table.

STEP 2 In the **Local Users** area, click **Add** to add a user.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The Local User - Add/Edit window opens.

STEP 3 Enter the following information:

- **User:** Enter the username for the user.
- **New Password:** Enter the password for the user. Passwords are case sensitive.

  NOTE: A password requires a minimum of 8 characters, including at least three of these character classes: uppercase letters, lowercase letters, digits, and special characters. Do not repeat any password more than three times in a row. Do not set the password as the username or “cisco.” Do not capitalize or spell these words backwards.
- **New Password Confirm:** Enter the password again for confirmation.
- **Group:** Choose the user group to which the user belongs.

  NOTE: For a SSL VPN user, make sure that the selected user group enables the SSL VPN service. For an IPsec VPN user, make sure that the selected user group enables the IPsec Remote Access service.

STEP 4 Click **OK** to save your settings.

Configuring Local User Groups

A user group is used to create a logical grouping of users that share the same service policy. Use the Users and Groups page to view, add, edit, or delete local user groups. The local database supports up to 50 user groups.

STEP 1 Click **Users > Users and Groups**.

The Users and Groups window opens. All existing user groups are listed in the Groups table.

STEP 2 In the **Groups** area, click **Add** to add a user group.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The Group - Add/Edit window opens.

STEP 3 In the **Group Settings** tab, enter the following information:

- **Name:** Enter the name for the user group.
- **Services:** Specify the service policy for the user group. You can enable multiple services for a user group.
  - **Web Login:** Choose one of the following web login policies for the user group.

    Disable: All members of the user group cannot log into the Configuration Utility through the web browser.

    Read Only: All members of the user group can only read the system status after they login. They cannot edit any configuration.

    Administrator: All members of the user group have full privilege to set the configuration and read the system status.

    NOTE: You cannot disable the web login service or change its service level for the default user group (“admin”).
  - **SSL VPN:** Choose a SSL VPN group policy to enable the SSL VPN service for the user group, or choose **Disable** to disable it. If you enable SSL VPN, all members of the user group can establish the SSL VPN tunnels based on the selected SSL VPN group policy to securely access your network resources. For more information about the SSL VPN group policy, see Configuring SSL VPN Group Policies, page 379.
  - **IPsec Remote Access:** Click **Enable** to enable the IPsec Remote Access service for the user group, or click **Disable** to disable it. If you enable IPsec Remote Access, all members of the user group can establish the VPN tunnels to securely access your network resources.
  - **Captive Portal:** Click **Enable** to enable the Captive Portal service for the user group, or click **Disable** to disable it. If you enable Captive Portal, the members of the user group will be directed to a specified web page (portal) before they can access the Internet. To configure Captive Portal, see Configuring Captive Portal, page 221,.

STEP 4 In the **Membership** tab, specify the members of the user group.

- To add a member, select an existing user from the **User** list and click the right arrow. The members of the user group appear in the **Membership** list.
- To delete a member from the user group, select the user from the **Membership** list and click the left arrow.

STEP 5 Click **OK** to save your settings.

Configuring User Authentication Settings

User authentication is a means of identifying the user and verifying that the user is allowed to access some restricted services. For example, a user can be identified as a SSL VPN user in order to access your network resources over SSL VPN tunnels.

The security appliance authenticates all users when they attempt to access your network resources in different zones. Users on the VLANs perform only local tasks, and are not required to be authenticated by the security appliance.

The security appliance supports a local database that is stored on the security appliance and a variety of AAA server types, such as RADIUS, Lightweight Directory Access Protocol (LDAP), and Active Directory (AD). You can use the local database, an AAA server, or both to perform user authentication. The local database supports up to 100 users, so you need to use the AAA server for authentication if the number of users accessing the network is more than 100 users.

NOTE The user group service policy can only be configured locally. All user groups on an AAA server need to be duplicated locally.

Refer to the following topics:

- **Using Local Database for User Authentication, page 394**
- **Using RADIUS Server for User Authentication, page 394**
- **Using Local Database and RADIUS Server for User Authentication, page 397**
- **Using LDAP for User Authentication, page 398**
- **Using Local Database and LDAP for Authentication, page 400**

Using Local Database for User Authentication

Use the local database to authenticate users when the number of users accessing the network is less than 100 users.

The local database verifies the user's credentials. Only the valid local users are allowed to access the network. For information on configuring local users in the local database, see **Configuring Local Users, page 390**.

STEP 1 Click **Users > User Authentication.**

STEP 2 Choose **Local Database** as the authentication method.

STEP 3 Click **Save** to apply your settings.

Using RADIUS Server for User Authentication

The security appliance can use RADIUS servers for user authentication for network access. The RADIUS server uses the Framed-Filter-ID attribute to store user and user group information, and checks the user's credentials by using the Password Authentication Protocol (PAP) authentication scheme.

When a user authenticates, the security appliance verifies the user's credentials through the RADIUS server. The RADIUS server returns the authentication results to the security appliance. For a valid RADIUS user, the security appliance checks its user group service policy from the local database and permits access. For an invalid RADIUS user, the security appliance blocks access.

STEP 1 Click **Users > User Authentication.**

STEP 2 Choose **RADIUS** as the authentication method.

STEP 3 Click **Configure** to configure the RADIUS settings.

STEP 4 In the **Settings** tab, choose the RADIUS group for authentication and configure the global timeout and retry settings.

- **Global RADIUS Settings:** Specify the global timeout and retry settings for the selected RADIUS servers:
  - **RADIUS Server Timeout:** Enter the number of seconds that the connection can exist before re-authentication is required. The range is 1-60 seconds. The default value is 3 seconds.

  - **Retries:** Enter the number of times that the security appliance will try to contact the RADIUS server. The range is 0-10 attempts. The default value is 2.

  The security appliance first sends a request message to the primary RADIUS server. If there is no response from the primary RADIUS server, the security appliance waits the number of seconds that you set in the **RADIUS Server Timeout** field, and then sends another request message. This continues for the number of times that you set in the **Retries** field (or until there is a valid response). If there is no valid response from the primary RADIUS server after the specified number of retries, the security appliance uses the secondary RADIUS server for the next authentication attempt. If the secondary server also fails to respond after the specified number of retries, the connection is dropped.

- **RADIUS Servers:** Choose the RADIUS group index from the drop-down list. The RADIUS server settings of the selected group are displayed. You can edit these settings here but the settings you specify will replace the default settings of the selected group. To maintain the RADIUS server settings, go to the Users > RADIUS Servers page. See **Configuring RADIUS Servers, page 401**.

STEP 5 In the **RADIUS Users** tab, enter the following information:

- **Allow Only Users Listed Locally:** Click **On** to allow only the RADIUS users who also are present in the local database to login, or click **Off** to disable it.

- **Mechanism for Setting User Group Memberships for RADIUS Users:** Select one of the following mechanisms to configure the user group memberships for RADIUS users:

  - **Use RADIUS Filter-ID:** Find the user group information by using the Framed-Filter-ID attribute from the RADIUS server.

    For example, the RADIUS server has three user groups (Group1, Group2, and Group3) and the local database has two user groups (Group1 and Group2). The following table displays the user group membership settings.

Local Database Settings	**RADIUS Server Settings**		
	User1 in Group1	User1 in Group2	User1 in Group3

User1 in Group1	Group1	Group2	Default Group
User1 in Group2	Group1	Group2	Default Group
User1 does not exist	Group1	Group2	Default Group

In the above table, if the User1 in the RADIUS server belongs to the Group1 but the User1 in the local database belongs to the Group2, then the User1 will belong to the Group1 after the user passes the RADIUS authentication. If the User1 in the RADIUS server belongs to the Group3 but the local database has not the Group3, then the User1 will be set to the specified default group.

- **Local Configuration Only:** Find the user group information from the local database only.

For example, the RADIUS server has three user groups (Group1, Group2, and Group3) and the local database has two user groups (Group1 and Group2). The following table displays the user group membership settings.

Local Database Settings	**RADIUS Server Settings**		
	User1 in Group1	User1 in Group2	User1 in Group3
User1 in Group1	Group1	Group1	Group1
User1 in Group2	Group2	Group2	Group2
User1 does not exist	Default Group	Default Group	Default Group

In the above table, if the User1 in the RADIUS server belongs to the Group1 but the User1 in the local database belongs to the Group2, then the User1 will belong to the Group2 after the user passes the RADIUS authentication. If the User1 does not exist in the local database, it will be set to the specified default group.

- **Default User Group to Which All RADIUS Users Belong:** Choose a local user group as the default group to which the RADIUS users belong. If the group does not exist in the local database when getting user group information from the RADIUS server, the RADIUS user will be automatically set to the specified local user group.

STEP 6 In the **Test** tab, enter the user's credentials in the **User** and **Password** fields, and then click the **Test** button to verify whether the RADIUS user is valid.

STEP 7 Click **OK** to save your settings.

STEP 8 Click **Save** to apply your settings.

Using Local Database and RADIUS Server for User Authentication

You can use both the local database and RADIUS server to authenticate users who try to access the network.

When a user authenticates, the security appliance first verifies the user's credentials through the RADIUS server. The RADIUS server returns the authentication results to the security appliance. For a valid RADIUS user, the security appliance checks its user group service policy from the local database and permits access. For an invalid RADIUS user, then the security appliance uses the local database to verify it again. For a valid local user, the security appliance checks its user group service policy from the local database and permits access. For an invalid local user, the security appliance blocks access.

STEP 1 Click **Users > User Authentication**.

STEP 2 Choose **RADIUS + Local Database** as the authentication method.

STEP 3 Click **Configure** to configure the RADIUS settings for user authentication. For complete details, see **Using RADIUS Server for User Authentication, page 394**.

STEP 4 Click **Save** to apply your settings.

Using LDAP for User Authentication

The security appliance can use the LDAP directory for user authentication, with support of three schemes including Microsoft Active Directory, RFC2798 InterOrgPerson, and RFC2307 Network Information Service.

STEP 1 Click **Users > User Authentication**.

STEP 2 Choose **LDAP** as the authentication method.

STEP 3 Click **Configure** to configure the LDAP settings.

STEP 4 In the **Settings** tab, enter the following information:

- **IP Address:** Enter the IP address of the LDAP server.
- **Port Number:** Enter the listening IP port number used on the LDAP server. Typically, non-secure connections use 389 and secure connections use 636. The default is 389.
- **Server Timeout:** Enter the amount of time in seconds that the security appliance will wait for a response from the LDAP server before timing out. The default value is 5 seconds.

  The security appliance will retry to log in to the LDAP server if there is no response from the LDAP server after the timeout. For example, if the server timeout is set as 5 seconds and there is no response from the LDAP server after 5 seconds, the security appliance will then retry to log in to the LDAP server 5 seconds later.
- **Login Method:** Choose one of the following login methods:
  - **Anonymous Login:** Choose this option if the LDAP server allows for the user tree to be accessed anonymously.
  - **Give Login Name or Location in Tree:** Choose this option if the distinguished name that is used to bind to the LDAP server is built from the **Primary Domain** and **User Tree for Login to Server** fields in the **Directory** tab.
  - **Give Bind Distinguished Name:** Choose this option if the destination name is known. You must provide the destination name explicitly to be used to bind to the LDAP server.
- **Login User Name:** If you choose **Give Login Name or Location in Tree** or **Give Bind Distinguished Name** as the login method, enter the user distinguished name of the account that can log into the LDAP server.

- **Login Password:** If you choose **Give Login Name or Location in Tree** or **Give Bind Distinguished Name** as the login method, enter the password of the account that can log into the LDAP server.
- **Protocol Version:** Choose the LDAP version from the drop-down list. The security appliance supports LDAP Version 2 and LDAP Version 3. Most LDAP directories, including Active Directory, use LDAP Version 3.

STEP 5 In the **Schema** tab, enter the following information:

- **LDAP Schema:** Choose one of the following schemes:
  - Microsoft Active Directory
  - RFC2798 InetOrgPerson
  - RFC2307 Network Information Service
- **User Objects:** The following fields display their correct values used by the selected scheme. The fields that are grayed out cannot be edited, but you can specify the editable fields if you have a specific LDAP scheme configuration.
  - **Object Class:** The object class of the individual user account.
  - **Login Name Attribute:** The attribute that is used for login authentication.
  - **Qualified Login Name Attribute:** The attribute of a user object that sets an alternative login name for the user in name@domain format.
  - **User Group Membership Attribute:** The membership attribute that contains information about the group to which the user object belongs. This option is only available for Microsoft Active Directory.
  - **Framed IP Address Attribute:** The attribute to retrieve a static IP address that is assigned to a user in the directory.
- **User Group Objects:** The following fields display their correct values used by the selected scheme.
  - **Object Class:** The name associated with the group of attributes.
  - **Member Attribute:** The attribute associated with a member.

STEP 6 In the **Directory** tab, enter the user direction information in the following fields:

- **Primary Domain:** Enter the user domain used by your LDAP implementation. All domain components use “dc=”. The domain is formatted as “dc=ExampleCorporation, dc=com”.

- **User Tree for Login to Server:** If you choose **Give Login Name or Location in Tree** as the login method in the **Settings** tab, specify the user tree that is used to log into the LDAP server.
- **Trees Containing Users:** Specify the user trees in the LDAP directory. To add an entry, click **Add**. To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click **Remove**. To modify the priority of an entry in the tree, click the up arrow or the down arrow.
- **Trees Containing User Groups:** Specify the user trees in the LDAP directory. These are only applicable when there is no user group membership attribute in the scheme's user object, and are not used with AD. To add an entry, click **Add**. To edit an entry, click **Edit**. To delete an entry, click **Remove**. To modify the priority of an entry in the tree, click the up arrow or the down arrow.

  NOTE: All the above trees are given in the format of distinguished names (“cn=Users, dc=ExampleCorporation, dc=com”).

STEP 7 In the **LDAP Users** tab, enter the following information:

- **Allow Only Users Listed Locally:** Click **On** to allow only the LDAP users who also are present in the local database to login, or click **Off** to disable it.
- **Default LDAP User Group:** Choose a local user group as the default group to which the LDAP users belong. If the group does not exist in the local database when getting user group information from the LDAP server, the LDAP user will be automatically set to the specified local user group.

STEP 8 In the **Test** tab, enter the user’s credentials in the **User** and **Password** fields and then click **Test** to verify whether the LDAP user is valid.

STEP 9 Click **OK** to save your settings.

STEP 10 Click **Save** to apply your settings.

Using Local Database and LDAP for Authentication

You can use both the local database and LDAP to authenticate users who try to access to the network.

STEP 1 Click **Users > User Authentication**.

STEP 2 Choose **LDAP + Local Database** as the authentication method.

STEP 3 Click **Configure** to configure the LDAP settings for user authentication. For complete details, see **Using LDAP for User Authentication, page 398**.

STEP 4 Click **Save** to apply your settings.

Configuring RADIUS Servers

Use the RADIUS Servers page to configure the RADIUS servers that are used to authenticate users who try to access the network resources. A RADIUS group includes a primary RADIUS server and a backup RADIUS server. The security appliance predefines three RADIUS groups.

STEP 1 Click **Users > RADIUS Servers**.

The RADIUS Servers window opens. All predefined RADIUS groups are listed in the table.

STEP 2 To edit the settings for a predefined RADIUS group, click the **Edit** (pencil) icon.

The RADIUS Group - Edit window opens.

STEP 3 Enter the following information:

- **Primary RADIUS Server IP:** Enter the IP address of the primary RADIUS server.
- **Primary RADIUS Server Port:** Enter the port number on the primary RADIUS server that is used to send the RADIUS traffic. The default is 1812.
- **Primary RADIUS Server Pre-shared Key:** Enter the pre-shared key that is configured on the primary RADIUS server.
- **Secondary RADIUS Server IP:** Enter the IP address of the secondary RADIUS server.
- **Secondary RADIUS Server Port:** Enter the port number on the secondary RADIUS server that is used to send the RADIUS traffic. The default is 1812.
- **Secondary RADIUS Server Pre-shared Key:** Enter the pre-shared key that is configured on the secondary RADIUS server.

STEP 4 Click **OK** to save your settings.

STEP 5 Repeat the above steps to edit the settings for other RADIUS groups if needed.

STEP 6 Click **Save** to apply your settings.