



User Management

This chapter contains information about setting up and managing user accounts in Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

This chapter contains the following topics:

- [About User Setup Features and Functions, page 7-1](#)
- [About User Databases, page 7-2](#)
- [Basic User Setup Options, page 7-2](#)
- [Advanced User Authentication Settings, page 7-15](#)
- [User Management, page 7-36](#)



Caution

Settings at the user level override settings that you configured at the group level.

Before you configure User Setup, you should understand how this section functions. ACS dynamically builds the User Setup section interface depending on the configuration of your Authentication, Authorization, and Accounting (AAA) client and the security protocols that you use. That is, what you see under User Setup is affected by settings in the Network Configuration and Interface Configuration sections.

About User Setup Features and Functions

The User Setup section of the ACS web interface is the centralized location for all operations regarding user account configuration and administration.

From within the User Setup section, you can:

- View a list of all users in the ACS internal database.
- Find a user.
- Add a user.
- Assign the user to a group, including Voice-over-IP (VoIP) groups.
- Edit user account information.
- Establish or change user authentication type.
- Configure callback information for the user.
- Set network-access restrictions (NARs) for the user.

- Configure Advanced Settings.
- Set the maximum number of concurrent sessions (Max Sessions) for the user.
- Disable or reenable the user account.
- Delete the user.

About User Databases

ACS authenticates users against one of several possible databases, including its ACS internal database. Regardless of which database that you configure ACS to use when authenticating a user, all users have accounts within the ACS internal database, and authorization of users is always performed against the user records in the ACS internal database. The following list details the basic user databases that are used and provides links to greater details on each:

- **ACS internal database**—Authenticates a user from the local ACS internal database. For more information, see [ACS Internal Database, page 13-1](#).



Tip

The following authentication types appear in the web interface only when the corresponding external user database has been configured in the Database Configuration area of the External User Databases section.

- **Windows Database**—Authenticates a user with an existing account in the Windows user database in the local domain or in domains that you configure in the Windows user database. For more information, see [Windows User Database, page 13-5](#).
- **Generic LDAP**—Authenticates a user from a Generic Lightweight Directory Access Protocol (LDAP) external user database (including Network. Directory Services (NDS) users). For more information, see [Generic LDAP, page 13-22](#).
- **ODBC Database**—Authenticates a user from an Open Database Connectivity-compliant database server. For more information, see [ODBC Database, page 13-34](#).
- **LEAP Proxy RADIUS Server Database**—Authenticates a user from a Lightweight and Efficient Application Protocol (LEAP) Proxy Remote Access Dial-In User Service (RADIUS) server. For more information, see [LEAP Proxy RADIUS Server Database, page 13-46](#).
- **Token Server**—Authenticates a user from a token server database. ACS supports the use of a variety of token servers for the increased security that one-time passwords provide. For more information, see [Token Server User Databases, page 13-48](#).

Basic User Setup Options

This section presents the basic tasks that you perform when configuring a new user. At its most basic level, configuring a new user requires only three steps:

-
- Step 1** Specify a name.
 - Step 2** Specify an external user database or a password.
 - Step 3** Submit the information.
-

The steps for editing user account settings are nearly identical to those used when adding a user account; but, to edit, you navigate directly to the field or fields to change. You cannot edit the name that is associated with a user account. To change a username, you must delete the user account and establish another.

What other procedures that you perform when setting up new user accounts is a function of the complexity of your network and of the granularity of control that you want.

This section contains the following topics:

- [Adding a Basic User Account, page 7-3](#)
- [Setting Supplementary User Information, page 7-4](#)
- [Setting a Separate CHAP/MS-CHAP/ARAP Password, page 7-5](#)
- [Assigning a User to a Group, page 7-5](#)
- [Setting the User Callback Option, page 7-6](#)
- [Assigning a User to a Client IP Address, page 7-7](#)
- [Setting Network Access Restrictions for a User, page 7-8](#)
- [Setting Max Sessions Options for a User, page 7-11](#)
- [Options for Setting User Usage Quotas, page 7-12](#)
- [Setting Options for User Account Disablement, page 7-13](#)
- [Assigning a Downloadable IP ACL to a User, page 7-14](#)

Adding a Basic User Account

This procedure details the minimum steps necessary to add a new user account to the ACS internal database.

To add a user account:

Step 1 In the navigation bar, click **User Setup**.

The User Setup Select page opens.

Step 2 Type a name in the **User** box.



Note The username can contain up to 64 characters. Names cannot contain the pound sign (#), the question mark (?), the quote ("), the asterisk (*), the right angle bracket (>), or the left angle bracket (<). Leading and trailing spaces are not allowed.

Step 3 Click **Add/Edit**.

The User Setup Edit page opens. The username that you are adding appears at the top of the page.

Step 4 Ensure that you uncheck the **Account Disabled** check box.



Note Alternatively, you can check the **Account Disabled** check box to create a user account that is disabled, and enable the account at another time.

Step 5 Under Password Authentication in the User Setup table, select the applicable authentication type from the list.



Tip The authentication types that appear reflect the databases that you have configured in the Database Configuration area of the External User Databases section.

Step 6 Enter a single ACS Password Authentication Protocol (PAP) password by typing it in the first set of **Password** and **Confirm Password** boxes.



Note Up to 32 characters are allowed each for the **Password** box and the **Confirm Password** box.



Tip The ACS PAP password is also used for CHAP/MS-CHAP/ARAP if you do not check the **Separate CHAP/MS-CHAP/ARAP** check box.



Tip You can configure the AAA client to ask for a PAP password first and then a Challenge Authentication Handshake Protocol (CHAP) or Microsoft-Challenge Authentication Handshake Protocol (MS-CHAP) password; so that, when users dial in by using a PAP password, they will authenticate. For example, the following line in the AAA client configuration file causes the AAA client to enable CHAP after PAP: **ppp authentication pap chap**

Step 7 Do one:

- Finish configuring the user account options and establish the user account, click **Submit**.
- Continue to specify the user account options, perform other procedures in this chapter, as applicable.



Tip For lengthy account configurations, you can click **Submit** before continuing. This action will prevent loss of information that you already entered if an unforeseen problem occurs.

Setting Supplementary User Information

Supplementary User Information can contain up to five fields that you configure. The default configuration includes two fields: Real Name and Description.

For information about how to display and configure these optional fields, see [User Data Configuration Options, page 3-4](#).

To enter optional information into the Supplementary User Information table:

Step 1 Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Complete each box that appears in the Supplementary User Info table.



Note Up to 128 characters are allowed each for the **Real Name** and the **Description** boxes.

- Step 3** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 4** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting a Separate CHAP/MS-CHAP/ARAP Password

Setting a separate CHAP/MS-CHAP/ARAP password adds more security to ACS authentication. However, you must have an AAA client configured to support the separate password.

To allow the user to authenticate by using a CHAP, MS-CHAP, or AppleTalk Remote Access Protocol (ARAP) password, instead of the PAP password in the ACS internal database:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Select the **Separate CHAP/MS-CHAP/ARAP** check box in the User Setup table.
- Step 3** Enter the CHAP/MS-CHAP/ARAP password to use by typing it in each of the second set of **Password** or **Confirm** boxes under the **Separate (CHAP/MS-CHAP/ARAP)** check box.



Note Up to 32 characters are allowed each for the **Password** box and the **Confirm Password** box.



Note These **Password** and **Confirm Password** boxes are only required for authentication by the ACS database. Additionally, if you assign a user to a VoIP (null password) group, and the optional password is also included in the user profile, the password is not used until the user is remapped to a non-VoIP group.

- Step 4** Do one:
- If you are finished configuring the user account options, click **Submit** to record the options.
 - To continue to specify the user account options, perform other procedures in this chapter, as applicable.
-


Assigning a User to a Group

A user can only belong to one group in ACS. The user inherits the attributes and operations that are assigned to his or her group. However, in the case of conflicting settings, the settings at the user level override the settings that you configure at the group level.

By default, users are assigned to the Default Group. Users who authenticate via the Unknown User method and who are not mapped to an existing ACS group are also assigned to the Default Group.

Alternatively, you can choose not to map a user to a particular group; but instead, to have the group mapped by an external authenticator. For external user databases from which ACS can derive group information, you can associate the group memberships—defined for the users in the external user database—to specific ACS groups. For more information, see [Chapter 17, “About User Group Mapping and Specification.”](#)


To assign a user to a group:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** From the Group to which user is assigned list in the User Setup table, select the group to which to assign the user.
-  **Tip** Alternatively, you can scroll up in the list to select the **Mapped By External Authenticator** option.
-
- Step 3** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 4** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting the User Callback Option

Callback is a command string that is passed to the access server. You can use a callback string to initiate a modem to call the user back on a specific number for added security or reversal of line charges.

To set the user callback option:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Under Callback in the User Setup table, select the applicable option. Choices include:
- **Use group setting**—Click if you want this user to use the setting for the group.
 - **No callback allowed**—Click to disable callback for this user.
 - **Callback using this number**—Click and type the complete number, including area code if necessary, on which to always call back this user.
-  **Note** The maximum length for the callback number is 199 characters.
-
- **Dialup client specifies callback number**—Click to enable the Windows dialup client to specify the callback number.
 - **Use Windows Database callback settings**—Click to use the settings specified for Windows callback. If a Windows account for a user resides in a remote domain, the domain in which ACS resides must have a two-way trust with that domain for the Microsoft Windows callback settings to operate for that user.



Note The dial-in user must have configured Windows software that supports callback.



Note If you enable the Windows Database callback settings, the Windows Callback feature must also be enabled in the Windows Database Configuration Settings. See [Windows User Database Configuration Options, page 13-18](#).

- Step 3** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 4** If you are finished configuring the user account options, click **Submit** to record the options.

Assigning a User to a Client IP Address

To assign a user to a client IP address:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Under **Client IP Address Assignment** in the User Setup table, select the applicable option. Choices include:



Note The IP address assignment in User Setup overrides the IP address assignment in Group Setup.

- **Use group settings**—Click this option to use the IP address group assignment.
- **No IP address assignment**—Click this option to override the group setting if you do not want an IP address returned by the client.
- **Assigned by dialup client**—Click this option to use the IP address dialup client assignment.
- **Assign static IP address**—Click this option and type the IP address in the box (up to 15 characters), if a specific IP address should be used for this user.



Note If the IP address is being assigned from a pool of IP addresses or by the dialup client, leave the **Assign static IP address** box blank.

- **Assigned by AAA client pool**—Click this option and type the AAA client IP pool name in the box, if this user is to have the IP address assigned by an IP address pool that is configured on the AAA client.
- **Assigned from AAA pool**—Click this option and type the applicable pool name in the box, if this user is to have the IP address that is assigned by an IP address pool configured on the AAA server. Select the AAA server IP pool name from the **Available Pools** list, and then click --> (right arrow button) to move the name into the **Selected Pools** list. If the **Selected Pools** list contains more than one pool, the users in this group are assigned to the first available pool in the order listed. To move the position of a pool in the list, select the pool name, and click **Up** or **Down** until the pool is in the position that you want.

- Step 3** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 4** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Network Access Restrictions for a User

You use the Network Access Restrictions table in the Advanced Settings area of User Setup to set NARs in three ways:

- Apply existing shared NARs by name.
- Define IP-based access restrictions to permit or deny user access to a specified AAA client or to specified ports on an AAA client when an IP connection has been established.
- Define calling line ID/Dialed Number Identification Service (CLI/DNIS)-based access restrictions to permit or deny user access based on the CLI/DNIS that is used.



Note You can also use the CLI/DNIS-based access restrictions area to specify other values. For more information, see [Network Access Restrictions, page 5-17](#).

Typically, you define (shared) NARs from within the Shared Components section so that you can apply these restrictions to more than one group or user. For more information, see [Adding a Shared NAR, page 5-20](#). You must have selected the **User-Level Network Access Restrictions** check box on the Advanced Options page of the Interface Configuration section for this set of options to appear in the web interface.

However, you can also use ACS to define and apply a NAR for a single user from within the User Setup section. You must have enabled the **User-Level Network Access Restrictions** setting on the Advanced Options page of the Interface Configuration section for single user IP-based filter options and single user CLI/DNIS-based filter options to appear in the web interface.



Note

When an authentication request is forwarded by proxy to an ACS, any NARs for Terminal Access Controller Access Control System (TACACS+) requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

When you create access restrictions on a per-user basis, ACS does not enforce limits to the number of access restrictions nor does it enforce a limit to the length of each access restriction; however, there are strict limits:

- The combination of fields for each line item cannot exceed 1024 characters in length.
- The shared NAR cannot have more than 16 KB of characters. The number of line items supported depends on the length of each line item. For example, if you create a CLI/DNIS-based NAR where the AAA client names are 10 characters, the port numbers are 5 characters, the CLI entries are 15 characters, and the DNIS entries are 20 characters, you can add 450 line items before reaching the 16 KB limit.

To set NARs for a user:

Step 1 Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 To apply a previously configured shared NAR to this user:



Note To apply a shared NAR, you must have configured it under Network Access Restrictions in the Shared Profile Components section. For more information, see [Adding a Shared NAR, page 5-20](#).

- a. Check the **Only Allow network access when** check box.
- b. To specify whether one or all shared NARs must apply for the user to be permitted access, select one, as applicable:
 - All selected NARS result in permit.
 - Any one selected NAR results in permit.
- c. Select a shared NAR name in the NARs list, and then click --> (right arrow button) to move the name into the Selected NARs list.



Tip To view the server details of the shared NARs you have selected to apply, you can click **View IP NAR** or **View CLID/DNIS NAR**, as applicable.

Step 3 To define and apply a NAR, for this particular user, that permits or denies this user access based on IP address, or IP address and port:



Tip You should define most NARs from within the Shared Components section so that you can apply them to more than one group or user. For more information, see [Adding a Shared NAR, page 5-20](#).

- a. In the Network Access Restrictions table, under Per User Defined Network Access Restrictions, check the **Define IP-based access restrictions** check box.
- b. To specify whether the subsequent listing specifies permitted or denied IP addresses, from the Table Defines list, select one:
 - **Permitted Calling/Point of Access Locations**
 - **Denied Calling/Point of Access Locations**
- c. Select or enter the information in the following boxes:
 - **AAA Client**—Select **All AAA Clients**, or the name of a network device group (NDG), or the name of the individual AAA client, to which to permit or deny access.
 - **Port**—Type the number of the port to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports on the selected AAA client.
 - **Address**—Type the IP address or addresses to use when performing access restrictions. You can use the asterisk (*) as a wildcard.



Note The total number of characters in the AAA Client list, and the Port and Src IP Address boxes must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

d. Click **Enter**.

The specified AAA client, port, and address information appears in the table above the AAA Client list.

Step 4 To permit or deny this user access based on calling location or values other than an established IP address:

- a. Check the **Define CLI/DNIS based access restrictions** check box.
- b. To specify whether the subsequent listing specifies permitted or denied values, from the Table Defines list, select one:
 - **Permitted Calling/Point of Access Locations**
 - **Denied Calling/Point of Access Locations**
- c. Complete the following boxes:



Note You must make an entry in each box. You can use the asterisk (*) as a wildcard for all or part of a value. The format that you use must match the format of the string that you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

- **AAA Client**—Select **All AAA Clients**, or the name of the NDG, or the name of the individual AAA client, to which to permit or deny access.
- **PORT**—Type the number of the port to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports.
- **CLI**—Type the CLI number to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access based on part of the number.



Tip Use the CLI entry if you want to restrict access based on other values such as a Cisco Aironet client MAC address. For more information, see [About Network Access Restrictions, page 5-18](#).

- **DNIS**—Type the DNIS number to which to permit or deny access. Use this entry to restrict access based on the number into which the user will be dialing. You can use the asterisk (*) as a wildcard to permit or deny access based on part of the number.



Tip Use the DNIS selection if you want to restrict access based on other values such as a Cisco Aironet AP MAC address. For more information, see [About Network Access Restrictions, page 5-18](#).



Note The total number of characters in the AAA Client list and the **Port**, **CLI**, and **DNIS** boxes must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

d. Click **enter**.

The information, specifying the AAA client, port, CLI, and DNIS, appears in the table above the AAA Client list.

- Step 5** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 6** If you are finished configuring the user account options, click **Submit** to record the options.

Setting Max Sessions Options for a User

You use the Max Sessions feature to set the maximum number of simultaneous connections permitted for this user. For ACS purposes, a session is considered any type of user connection RADIUS or TACACS+ supports, for example Point-to-Point Protocol (PPP), or Telnet, or ARAP. Note, however, that accounting must be enabled on the AAA client for ACS to be aware of a session. All session counts are based on user and group names only. ACS does not support any differentiation by type of session—all sessions are counted as the same. To illustrate, a user with a Max Session count of 1 who is dialed in to an AAA client with a PPP session will be refused a connection if that user then tries to Telnet to a location whose access is controlled by the same ACS.



Note

Each ACS holds its own Max Sessions counts. There is no mechanism for ACS to share Max Sessions counts across multiple ACSs. Therefore, if two ACSs are set up as a mirror pair with the workload distributed between them, they will have completely independent views of the Max Sessions totals.



Tip

If the Max Sessions table does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Max Sessions** check box.

To set max sessions options for a user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** In the Max Sessions table, under Sessions available to user, select one:
- **Unlimited**—Select to allow this user an unlimited number of simultaneous sessions. (This effectively disables Max Sessions.)
 - **n**—Select and then type the maximum number of simultaneous sessions to allow this user.
 - **Use group setting**—Select to use the Max Sessions value for the group.



Note

The default setting is Use group setting.



Note

User Max Sessions settings override the group Max Sessions settings. For example, if the group Sales has a Max Sessions value of only 10, but a user in the group Sales, John, has a User Max Sessions value of Unlimited, John is still allowed an unlimited number of sessions.

- Step 3** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 4** If you are finished configuring the user account options, click **Submit** to record the options.
-

Options for Setting User Usage Quotas

You can define usage quotas for individual users. You can limit users by the:

- Duration of sessions for the period selected.
- Number of sessions for the period selected.

For ACS purposes, a session is considered any type of user connection the RADIUS or TACACS+ supports, for example PPP, or Telnet, or ARAP. Note, however, that accounting must be enabled on the AAA client for ACS to be aware of a session. If you make no selections in the Session Quotas section for an individual user, ACS applies the session quotas of the group to which the user is assigned.



Note

If the User Usage Quotas feature does not appear, choose **Interface Configuration > Advanced Options**. Then check the **Usage Quotas** check box.



Tip

The Current Usage table under the User Usage Quotas table on the User Setup Edit page displays usage statistics for the current user. The Current Usage table lists online time and sessions used by the user, with columns for daily, weekly, monthly, and total usage. The Current Usage table appears only on user accounts that you have established; that is, it does not appear during initial user setup.

For a user who has exceeded his quota, ACS denies him access on his next attempt to start a session. If a quota is exceeded during a session, ACS allows the session to continue. If a user account has been disabled because the user has exceeded usage quotas, the User Setup Edit page displays a message stating that the account has been disabled for this reason.

You can reset the session quota counters on the User Setup page for a user. For more information about resetting usage quota counters, see [Resetting User Session Quota Counters, page 7-39](#).

To support time-based quotas, we recommend enabling accounting update packets on all AAA clients. If update packets are not enabled, the quota is updated only when the user logs off. If the AAA client through which the user is accessing your network fails, the quota is not updated. In the case of multiple sessions, such as with ISDN, the quota is not updated until all sessions terminate, which means that a second channel will be accepted; even if the first channel has exhausted the quota that is allocated to the user.

To set usage quota options for a user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** In the Usage Quotas table, select **Use these settings**.
- Step 3** To define a usage quota based on duration of sessions for a user:
- a. Check the **Limit user to x hours of online time** check box.

- b. Type the number of hours to which you want to limit the user in the **Limit user to x hours of online time** box. Use decimal values to indicate minutes. For example, a value of 10.5 would equal 10 hours and 30 minutes.



Note This field can contain up to 10 characters.

- c. Select the period for which you want to enforce the time usage quota:
- **per Day**—From 12:01 a.m. until midnight.
 - **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
 - **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
 - **Absolute**—A continuous, open-ended count of hours.

Step 4 To define usage quotas based on the number of sessions for a user:

- a. Check the **Limit user to x sessions** check box.
- b. Type the number of sessions to which you want to limit the user in the **Limit user to x sessions** box.



Note Up to 10 characters are allowed for this field.

- c. Select the period for which you want to enforce the session usage quota:
- **per Day**—From 12:01 a.m. until midnight.
 - **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
 - **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
 - **Absolute**—A continuous, open-ended count of hours.

Step 5 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 6 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Options for User Account Disablement

The Account Disable feature defines the circumstances under which a user account is disabled.



Note


Do not confuse this feature with account expiration due to password aging. Password aging is defined for groups only, not for individual users. This feature is distinct from the **Account Disabled** check box. For instructions on how to disable a user account, see [Disabling a User Account, page 7-38](#).




Note


If the user is authenticated with a Windows user database, this expiration information is in addition to the information in the Windows user account. Changes here do not alter settings configured in Windows.

To set options for user account disablement:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Do one:
- a. Select the **Never** option to keep the user account always enabled.
-  **Note** This is the default setting.
-
- b. Select the **Disable account if** option to disable the account under specific circumstances. Then, specify one or both of the circumstances under the following boxes:
 - **Date exceeds**—Check the **Date exceeds** check box. Then select the month and type the date (two characters) and year (four characters) on which to disable the account.

 **Note** The default is 30 days after the user is added.

 - **Failed attempts exceed**—Check the **Failed attempts exceed** check box and then type the number of consecutive unsuccessful login attempts to allow before disabling the account.

 **Note** The default is 5.

- Step 3** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 4** If you are finished configuring the user account options, click **Submit** to record the options.
-

Assigning a Downloadable IP ACL to a User

You can use the Downloadable ACLs feature to assign an IP Access Control List (ACL) at the user level. You must configure one or more IP ACLs before you assign one. For instructions on how to configure a downloadable IP ACL by using the Shared Profile Components section of the ACS web interface, see [Adding a Downloadable IP ACL, page 5-15](#).



Note The Downloadable ACLs table does not appear if it has not been enabled. To enable the Downloadable ACLs table, click **Interface Configuration > Advanced Options**, and then check the **User-Level Downloadable ACLs** check box.

To assign a downloadable IP ACL to a user account:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username being added and edited is at the top of the page.
- Step 2** Under the Downloadable ACLs section, click the **Assign IP ACL:** check box.

- Step 3** Select an IP ACL from the list.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Advanced User Authentication Settings

This section presents the activities that you perform to configure user-level TACACS+ and RADIUS enable parameters.

This section contains the following topics:

- [TACACS+ Settings \(User\), page 7-16](#)
 - [Configuring TACACS+ Settings for a User, page 7-16](#)
 - [Configuring a Shell Command Authorization Set for a User, page 7-17](#)
 - [Configuring a PIX Command Authorization Set for a User, page 7-19](#)
 - [Configuring Device-Management Command Authorization for a User, page 7-20](#)
 - [Configuring the Unknown Service Setting for a User, page 7-21](#)
- [Advanced TACACS+ Settings for a User, page 7-22](#)
 - [Setting Enable Privilege Options for a User, page 7-22](#)
 - [Setting TACACS+ Enable Password Options for a User, page 7-23](#)
 - [Setting TACACS+ Outbound Password for a User, page 7-24](#)
- [RADIUS Attributes, page 7-24](#)
 - [Setting IETF RADIUS Parameters for a User, page 7-25](#)
 - [Setting Cisco IOS/PIX 6.0 RADIUS Parameters for a User, page 7-26](#)
 - [Setting Cisco Airespace RADIUS Parameters for a User, page 7-27](#)
 - [Setting Cisco Aironet RADIUS Parameters for a User, page 7-28](#)
 - [Setting Ascend RADIUS Parameters for a User, page 7-29](#)
 - [Setting Cisco VPN 3000/ASA/PIX 7.x+ RADIUS Parameters for a User, page 7-30](#)
 - [Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User, page 7-31](#)
 - [Setting Microsoft RADIUS Parameters for a User, page 7-32](#)
 - [Setting Nortel RADIUS Parameters for a User, page 7-33](#)
 - [Setting Juniper RADIUS Parameters for a User, page 7-34](#)
 - [Setting BBSM RADIUS Parameters for a User, page 7-35](#)
 - [Setting Custom RADIUS Attributes for a User, page 7-35](#)

TACACS+ Settings (User)

You can use TACACS+ Settings section to enable and configure the service and protocol parameters to apply for the authorization of a user.

This section contains the following topics:

- [Configuring TACACS+ Settings for a User, page 7-16](#)
- [Configuring a Shell Command Authorization Set for a User, page 7-17](#)
- [Configuring a PIX Command Authorization Set for a User, page 7-19](#)
- [Configuring Device-Management Command Authorization for a User, page 7-20](#)
- [Configuring the Unknown Service Setting for a User, page 7-21](#)

Configuring TACACS+ Settings for a User

You can use this procedure to configure TACACS+ settings at the user level for the following services and protocols:

- PPP IP
- PPP IPX
- PPP Multilink
- PPP Apple Talk
- PPP VPDN
- PPP LCP
- ARAP
- Shell (exec)
- Project Information Exchange (PIX) PIX Shell (pixShell)
- Serial Line Internet Protocol (SLIP)

You can also enable any *new* TACACS+ services that you configure. Because having all service/protocol settings appear within the User Setup section would be cumbersome, you choose what settings to hide or display at the user level when you configure the interface. For more information about setting up new or existing TACACS+ services in the ACS web interface, see [Protocol Configuration Options for TACACS+, page 3-7](#).


If you have configured ACS to interact with a Cisco device-management application, new TACACS+ services may appear automatically, as needed, to support the device-management application. For more information about ACS interaction with device-management applications, see [Support for Cisco Device-Management Applications, page 1-13](#).

For more information about attributes, see [Appendix B, “TACACS+ AV Pairs,”](#) or your AAA client documentation. For information on assigning an IP ACL, see [Assigning a Downloadable IP ACL to a User, page 7-14](#).

Before You Begin

- For the TACACS+ service/protocol configuration to appear, you must configure an AAA client to use TACACS+ as the security control protocol.
- In **Interface Configuration > Advanced Options**, ensure that the **Per-user TACACS+/RADIUS Attributes** check box is selected.

To configure TACACS+ settings for a user:

-
- Step 1** Click **Interface Configuration > TACACS+ (Cisco IOS)**. In the TACACS+ Services table, under the heading User, ensure that the check box is selected for each service/protocol that you want to configure.
- Step 2** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 3** Scroll down to the TACACS+ Settings table and select the bold service name check box to enable that protocol; for example **PPP IP**.
- Step 4** To enable specific parameters within the selected service, Check the check box next to a specific parameter and then do one of the following, as applicable:
- Check the **Enabled** check box.
 - Enter a value in the corresponding attribute box.
- To specify ACLs and IP address pools, enter the name of the ACL or pool as defined on the AAA client. Leave the box blank if the default (as defined on the AAA client) should be used. For more information about attributes, see [Appendix B, “TACACS+ AV Pairs,”](#) or your AAA client documentation. For information on assigning a IP ACL, see [Assigning a Downloadable IP ACL to a User, page 7-14](#).
-  **Tip** An ACL is a list of Cisco IOS commands that you use to restrict access to or from other devices and users on the network.
-
- Step 5** To employ custom attributes for a particular service, check the **Custom attributes** check box under that service, and then enter the attribute and value in the box below the check box.
- Step 6** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 7** If you are finished configuring the user account options, click **Submit** to record the options.
-

Configuring a Shell Command Authorization Set for a User

Use this procedure to specify the shell command-authorization set parameters for a user. You can choose:

- **None**—No authorization for shell commands.
- **Group**—The group-level shell command-authorization set applies for this user.
- **Assign a Shell Command Authorization Set for any network device**—One shell command-authorization set is assigned, and it applies all network devices.
- **Assign a Shell Command Authorization Set on a per Network Device Group Basis**—Particular shell command-authorization sets will be effective on particular NDGs. When you select this option, you create the table that lists what NDG associates with what shell command-authorization set.
- **Per User Command Authorization**—Permits or denies specific Cisco IOS commands and arguments at the user level.

Before You Begin

- Ensure that you configure an AAA client to use TACACS+ as the security control protocol.
- In **Interface Configuration > Advanced Options**, ensure that the **Per-user TACACS+/RADIUS Attributes** check box is selected.
- In the TACACS+ (Cisco) section of Interface Configuration, ensure that the Shell (exec) option is selected in the User column.
- Ensure that you have already configured one or more shell command-authorization sets. For detailed steps, see [Adding a Command Authorization Set, page 5-28](#).

To specify shell command-authorization set parameters for a user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Scroll down to the TACACS+ Settings table and to the Shell Command Authorization Set feature area within it.
- Step 3** To prevent the application of any shell command-authorization set, click (or accept the default of) the **None** option.
- Step 4** To assign the shell command-authorization set at the group level, select the **As Group** option.
- Step 5** To assign a particular shell command-authorization set to be effective on any configured network device:
- Select the **Assign a Shell Command Authorization Set for any network device** option.
 - Then, from the list directly below that option, select the shell command-authorization set that you want to apply to this user.
- Step 6** To create associations that assign a particular shell command-authorization set to be effective on a particular NDG, for each association:
- Select the **Assign a Shell Command Authorization Set on a per Network Device Group Basis** option.
 - Select a **Device Group** and an associated **Command Set**.
 - Click **Add Association**.



Tip You can also select which command set applies to network device groups that are not listed simply by associating that command set with the NDG *<default>* listing.

The NDG or NDGs and associated shell command-authorization set or sets are paired in the table.

- Step 7** To define the specific Cisco IOS commands and arguments to permit or deny for this user:

**Caution**

This step configures a powerful, advanced feature. Only an administrator who is skilled with Cisco IOS commands should use this feature. Correct syntax is the responsibility of the administrator. For information on how ACS uses pattern matching in command arguments, see [About Pattern Matching, page 5-27](#).

- Select the **Per User Command Authorization** option.
- Under Unmatched Cisco IOS commands, select **Permit** or **Deny**.

If you select **Permit**, the user can issue all commands that are not specifically listed. If you select **Deny**, the user can issue only those commands that are listed.

- c. To list particular commands to permit or deny, check the **Command** check box and then type the name of the command, define its arguments using standard permit or deny syntax, and select whether unlisted arguments are to be permitted or denied.



Tip To enter several commands, you must click **Submit** after entering a command. A new command entry box appears below the box that you just completed.

- Step 8** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 9** If you are finished configuring the user account options, click **Submit** to record the options.

Configuring a PIX Command Authorization Set for a User

Use this procedure to specify the PIX command-authorization set parameters for a user. The four options are:

- **None**—No authorization for PIX commands.
- **Group**—The group-level PIX command-authorization set applies for this user.
- **Assign a PIX Command Authorization Set for any network device**—One PIX command-authorization set is assigned, and it applies to all network devices.
- **Assign a PIX Command Authorization Set on a per Network Device Group Basis**—Particular PIX command-authorization sets will be effective on particular NDGs.

Before You Begin

- Ensure that you configure an AAA client to use TACACS+ as the security control protocol.
- In **Interface Configuration > Advanced Options**, ensure that the **Per-user TACACS+/RADIUS Attributes** check box is selected.
- In **Interface Configuration > TACACS+ (Cisco)**, ensure that the **PIX Shell (pixShell)** option is selected in the User column.
- Ensure that you have configured one or more PIX command-authorization sets. For detailed steps, see [Adding a Command Authorization Set, page 5-28](#).

To specify PIX command-authorization set parameters for a user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Scroll down to the TACACS+ Settings table and to the PIX Command Authorization Set feature area within it.
- Step 3** To prevent the application of any PIX command-authorization set, select (or accept the default of) the **None** option.
- Step 4** To assign the PIX command-authorization set at the group level, select the **As Group** option.

- Step 5** To assign a particular PIX command-authorization set to be effective on any configured network device:
- Select the **Assign a PIX Command Authorization Set for any network device** option.
 - From the list directly below that option, select the PIX command-authorization set that you want to apply to this user.
- Step 6** To create associations that assign a particular PIX command-authorization set to be effective on a particular NDG, for each association:
- Select the **Assign a PIX Command Authorization Set on a per Network Device Group Basis** option.
 - Select a **Device Group** and an associated **Command Set**.
 - Click **Add Association**.
- The associated NDG and PIX command-authorization sets appear in the table.
- Step 7** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 8** If you are finished configuring the user account options, click **Submit** to record the options.
-

Configuring Device-Management Command Authorization for a User

Use this procedure to specify the device-management command-authorization set parameters for a user. Device-management command-authorization sets support the authorization of tasks in Cisco device-management applications that are configured to use ACS for authorization. You can choose:

- **None**—No authorization is performed for commands that are issued in the applicable Cisco device-management application.
- **Group**—For this user, the group-level command-authorization set applies for the applicable device-management application.
- **Assign a <device-management application> for any network device**—For the applicable device-management application, one command-authorization set is assigned, and it applies to management tasks on all network devices.
- **Assign a <device-management application> on a per Network Device Group Basis**—For the applicable device-management application, you use this option to apply command-authorization sets to specific NDGs, so that it affects all management tasks on the network devices that belong to the NDG.

Before You Begin

- Ensure that an AAA client is configured to use TACACS+ as the security control protocol.
- In **Interface Configuration > Advanced Options**, ensure that the **Per-user TACACS+/RADIUS Attributes** check box is selected.
- In **Interface Configuration > TACACS+ (Cisco)**, ensure that the new TACACS+ service corresponding to the applicable device-management application is selected under **New Services** in the User column.
- If you want to apply command-authorization sets, be certain that you have configured one or more device-management command-authorization sets. For detailed steps, see [Adding a Command Authorization Set, page 5-28](#).

To specify device-management application command authorization for a user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Scroll down to the TACACS+ Settings table and to the applicable device-management command-authorization feature area within it.
- Step 3** To prevent the application of any command authorization for actions that are performed in the applicable device-management application, select (or accept the default of) the **None** option.
- Step 4** To assign command authorization for the applicable device-management application at the group level, select the **As Group** option.
- Step 5** To assign a particular command-authorization set that affects device-management application actions on any network device:
- Select the **Assign a <device-management application>** for any network device option.
 - Then, from the list directly below that option, select the command-authorization set that you want to apply to this user.
- Step 6** To create associations that assign a particular command-authorization set that affects device-management application actions on a particular NDG, for each association:
- Select the **Assign a <device-management application>** on a per Network Device Group Basis option.
 - Select a **Device Group** and an associated *<device-management application>*.
 - Click **Add Association**.
The associated NDG and command-authorization sets appear in the table.
- Step 7** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 8** If you are finished configuring the user account options, click **Submit** to record the options.
-

Configuring the Unknown Service Setting for a User

If you want TACACS+ AAA clients to permit unknown services, you can check the Default (Undefined) Services check box. Checking this option will PERMIT all UNKNOWN Services.

To configure the Unknown Service setting for a user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Scroll down to the table under the heading PERMIT all UNKNOWN Services.
- Step 3** To allow TACACS+ AAA clients to permit unknown services for this user, select the **Default (Undefined) Services** check box.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Advanced TACACS+ Settings for a User

The information in this section applies when you have configured an AAA client with TACACS+.



Tip

If the Advanced TACACS+ Settings (User) table does not appear, choose **Interface Configuration > TACACS+ (Cisco IOS)**. Then, choose **Advanced TACACS+ Features**.

This section contains the following topics:

- [Setting Enable Privilege Options for a User, page 7-22](#)
- [Setting TACACS+ Enable Password Options for a User, page 7-23](#)
- [Setting TACACS+ Outbound Password for a User, page 7-24](#)

Setting Enable Privilege Options for a User

You use a TACACS+ Enable Control with Exec session to control administrator access. Typically, you use it for router-management control. Select and specify the user privilege level:

- **Use Group Level Setting**—Sets the privileges for this user identical to the privileges configured at the group level.
- **No Enable Privilege**—Disallows enable privileges for this user.



Note

No Enable Privilege is the default setting.

- **Max Privilege for any AAA Client**—You can select from a list the maximum privilege level that will apply to this user on any AAA client on which this user is authorized.
- **Define Max Privilege on a per-Network Device Group Basis**—You can associate maximum privilege levels for this user in one or more NDGs.



Note

For information about privilege levels, refer to your AAA client documentation.



Tip

You must configure NDGs from within Interface Configuration before you can assign user privilege levels to them.

To select and specify the privilege level for a user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Under TACACS+ Enable Control in the Advanced TACACS+ Settings table, select one of the four privilege options:
- **Use Group Level Setting**
 - **No Enable Privilege**



Note **No Enable Privilege** is the default setting; when setting up a new user account, this privilege should already be selected.

- **Max Privilege for Any Access Server**
- **Define Max Privilege on a per-Network Device Group Basis**

Step 3 If you selected **Max Privilege for Any Access Server** in Step 2, select the appropriate privilege level from the corresponding list.

Step 4 If you selected **Define Max Privilege on a per-Network Device Group Basis** in Step 2, perform the following steps to define the privilege levels on each NDG, as applicable:

- a. From the Device Group list, select a device group.



Note You must have already configured a device group for it to be listed.

- b. From the Privilege list, select a privilege level to associate with the selected device group.
- c. Click **Add Association**.
An entry appears in the table, which associates the device group with a particular privilege level.
- d. Repeat Step a through Step c for each device group that you want to associate to this user.



Tip To delete an entry, select the entry and then click **Remove Associate**.

Step 5 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 6 If you are finished configuring the user account options, click **Submit** to record the options.

Setting TACACS+ Enable Password Options for a User

When setting the TACACS+ Enable Password Options for a user, you can use:

- **ACS PAP password.**
- **External database password.**
- **A separate password.**

To set the options for the TACACS+ Enable password:

Step 1 Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Select a password option:

- To use the information that is configured in the Password Authentication section, select **Use Cisco Secure PAP password**.



Note For information about basic password setup, see [Adding a Basic User Account, page 7-3](#).

- To use an external database password, select **Use external database password**, and then choose the database that authenticates the enable password for this user.



Note The list of databases displays only the databases that you have configured. For more information, see [About External User Databases, page 13-3](#).

- To use a separate password, click **Use separate password**, and then type and retype to confirm a control password for this user. This password is used in addition to the regular authentication.

Step 3 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 4 If you are finished configuring the user account options, click **Submit** to record the options.

Setting TACACS+ Outbound Password for a User

The TACACS+ outbound password enables an AAA client to authenticate itself to another AAA client via outbound authentication. The outbound authentication can be PAP, CHAP, MS-CHAP, or ARAP, and results in the ACS password being given out. By default, the user ASCII/PAP or CHAP/MS-CHAP/ARAP password is used. To avoid compromising inbound passwords, you can configure a separate SENDAUTH password.



Caution

Use an outbound password only if you are familiar with the use of a TACACS+ SendAuth/OutBound password.

To set a TACACS+ outbound password for a user:

Step 1 Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Type and retype to confirm a TACACS+ outbound password for this user.

Step 3 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 4 If you are finished configuring the user account options, click **Submit** to record the options.

RADIUS Attributes

You can configure user attributes for RADIUS authentication generally, at the Internet Engineering Task Force (IETF) level, or for vendor-specific attributes (VSAs) on a vendor-by-vendor basis. For general attributes, see [Setting IETF RADIUS Parameters for a User, page 7-25](#). ACS ships with many popular VSAs already loaded and available to configure and apply. For information about creating additional, custom RADIUS VSAs, see [Custom RADIUS Vendors and VSAs, page 9-19](#).

**Caution**

If you are using Shared Radius Authorization Components (SRACs), you should be aware of issues regarding attribute merging and overwriting RADIUS attributes on a user or group level. You should not assign RADIUS attributes to an individual user (only as a last resort). Use group or SRACs to assign RADIUS attributes in the user's group or profile levels.

This section contains the following topics:

- [Setting IETF RADIUS Parameters for a User, page 7-25](#)
- [Setting Cisco IOS/PIX 6.0 RADIUS Parameters for a User, page 7-26](#)
- [Setting Cisco Aironet RADIUS Parameters for a User, page 7-28](#)
- [Setting Ascend RADIUS Parameters for a User, page 7-29](#)
- [Setting Cisco VPN 3000/ASA/PIX 7.x+ RADIUS Parameters for a User, page 7-30](#)
- [Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User, page 7-31](#)
- [Setting Microsoft RADIUS Parameters for a User, page 7-32](#)
- [Setting Nortel RADIUS Parameters for a User, page 7-33](#)
- [Setting Juniper RADIUS Parameters for a User, page 7-34](#)
- [Setting BBSM RADIUS Parameters for a User, page 7-35](#)
- [Setting Custom RADIUS Attributes for a User, page 7-35](#)

Setting IETF RADIUS Parameters for a User

RADIUS attributes are sent as a profile for the user from ACS to the requesting AAA client.

These parameters appear only if:

- AAA clients (one or more) are configured to use one of the RADIUS protocols in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level IETF RADIUS attributes are enabled under **Interface Configuration > RADIUS (IETF)**.

**Note**

To display or hide any of these attributes in the web interface, see [Protocol Configuration Options for RADIUS, page 3-9](#).

**Note**

For a list and explanation of RADIUS attributes, see [Appendix C, "RADIUS Attributes,"](#) or the documentation for your particular network device that is using RADIUS.

To configure IETF RADIUS attribute settings to apply as an authorization for the current user:

Step 1

Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

- Step 2** In the IETF RADIUS table, for each attribute that you need to authorize for the current user, check the check box next to the attribute and then further define the authorization for the attribute in the box or boxes next to it, as applicable.
- Step 3** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 4** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Cisco IOS/PIX 6.0 RADIUS Parameters for a User

The Cisco IOS RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco IOS/PIX 6.0)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Cisco IOS/PIX 6.0)** attributes are enabled under **Interface Configuration > RADIUS (Cisco IOS/PIX 6.0)**.



Note

To hide or display the Cisco IOS RADIUS VSA, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

Cisco IOS RADIUS represents only the Cisco IOS VSAs. You must configure the IETF RADIUS and Cisco IOS RADIUS attributes.

To configure and enable Cisco IOS RADIUS attributes to apply as an authorization for the current user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Cisco IOS RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 7-25](#).
- Step 3** If you want to use the [009\001] `cisco-av-pair` attribute to specify authorizations, check the check box next to the attribute and then type the attribute-value pairs in the text box. Separate each attribute-value pair by pressing **enter**.
For example, if the current user profile corresponds to a Network Admission Control (NAC) client to which ACS always assigns a `status-query-timeout` attribute value that must be different than a value that any applicable group profile contains, you could specify the value as:
`status-query-timeout=1200`
- Step 4** If you want to use other Cisco IOS/PIX 6.0 RADIUS attributes, select the corresponding check box and specify the required values in the adjacent text box.

- Step 5** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 6** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Cisco Airespace RADIUS Parameters for a User

The Cisco Airespace RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco Airespace)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Cisco Airespace)** attributes that you want to apply are enabled under **Interface Configuration > RADIUS (Cisco Airespace)**.

Cisco Airespace RADIUS represents only the Cisco Airespace proprietary attributes. You must configure IETF RADIUS and Cisco Airespace RADIUS attributes that you want to use.



Note

To hide or display Cisco Airespace RADIUS attributes, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Cisco Airespace RADIUS attributes to apply as an authorization for the current user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
- The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Cisco Airespace RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 7-25](#).
- Step 3** In the Cisco Airespace RADIUS Attributes table, to specify the attributes that should be authorized for the user:
- a. Check the check box next to the particular attribute.
 - b. Further define the authorization for that attribute in the box next to it.
 - c. Continue to select and define attributes, as applicable.
- For more information about attributes, see [Appendix C, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 4** Do one:
- If you are finished configuring the user account options, click **Submit** to record the options.
 - To continue to specify the user account options, perform other procedures in this chapter, as applicable.
-

Setting Cisco Aironet RADIUS Parameters for a User

The single Cisco Aironet RADIUS VSA, Cisco-Aironet-Session-Timeout, is a virtual VSA. This VSA acts as a specialized implementation (that is, a remapping) of the IETF RADIUS Session-Timeout attribute (27) to respond to a request from a Cisco Aironet Access Point. Use the Cisco-Aironet-Session-Timeout attribute to provide a different timeout value when a user must be able to connect via wireless and wired devices. This capability to provide a second timeout value specifically for WLAN connections avoids the difficulties that would arise if you had to use a standard timeout value (typically measured in hours) for a WLAN connection (that is typically measured in minutes). You do not need to use Cisco-Aironet-Session-Timeout if the particular user will always connect only with a Cisco Aironet Access Point. Rather, use this setting when a user may connect via wired or wireless clients.

For example, imagine a user's **Cisco-Aironet-Session-Timeout** set to 600 seconds (10 minutes) and that same user's IETF RADIUS Session-Timeout set to 3 hours. When the user connects via a VPN, ACS uses 3 hours as the timeout value. However, if that same user connects via a Cisco Aironet Access Point, ACS responds to an authentication request from the Aironet AP by sending 600 seconds in the IETF RADIUS **Session-Timeout** attribute. Thus, with the **Cisco-Aironet-Session-Timeout** attribute configured, different session-timeout values can be sent depending on whether the end-user client is a wired device or a Cisco Aironet Access Point.

The Cisco Aironet RADIUS parameters appear on the User Setup page only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco Aironet)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Cisco Aironet)** attribute is enabled under RADIUS (Cisco Aironet) in the **Interface Configuration > RADIUS (Cisco Aironet)**.



Note

To hide or display the Cisco Aironet RADIUS VSA, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable the Cisco Aironet RADIUS attribute to apply as an authorization for the current user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Cisco Aironet RADIUS attributes, ensure that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 7-25](#).
- Step 3** In the Cisco Aironet RADIUS Attributes table, select the **[5842\001] Cisco-Aironet-Session-Timeout** check box.
- Step 4** In the **[5842\001] Cisco-Aironet-Session-Timeout** box, type the session-timeout value (in seconds) that ACS is to send in the IETF RADIUS Session-Timeout (27) attribute when the AAA client is configured in Network Configuration to use the RADIUS (Cisco Aironet) authentication option. The recommended value is 600 seconds.

For more information about the IETF RADIUS Session-Timeout attribute, see [Appendix C, “RADIUS Attributes,”](#) or your AAA client documentation.

- Step 5** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 6** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Ascend RADIUS Parameters for a User

The Ascend RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Ascend)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Ascend)** attributes that you want to apply are enabled under in the **Interface Configuration > RADIUS (Ascend)**.

Ascend RADIUS represents only the Ascend proprietary attributes. You must configure the IETF RADIUS and Ascend RADIUS attributes. Proprietary attributes override IETF attributes.

The default attribute setting that appears for RADIUS is `Ascend-Remote-Addr`.



Note

To hide or display Ascend RADIUS attributes, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#). A VSA that is applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Ascend RADIUS attributes to apply as an authorization for the current user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Ascend RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 7-25](#).
- Step 3** In the Ascend RADIUS Attributes table, to specify the attributes that should be authorized for the user:
- Check the check box next to the particular attribute.
 - Further define the authorization for that attribute in the box next to it.
 - Continue to select and define attributes, as applicable.
For more information about attributes, see [Appendix C, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Cisco VPN 3000/ASA/PIX 7.x+ RADIUS Parameters for a User

To control Microsoft Point-to-Point Encryption (MPPE) settings for users who access the network through a Cisco VPN 3000-series concentrator, an Adaptive Security Appliance (ASA), or PIX Security Appliance version 7.x+, use the **CVPN3000-PPTP-Encryption** (VSA 20) and **CVPN3000-L2TP-Encryption** (VSA 21) attributes. Settings for **CVPN3000-PPTP-Encryption** (VSA 20) and **CVPN3000-L2TP-Encryption** (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) attributes; regardless of whether RADIUS (Microsoft) attributes are enabled in the ACS web interface or how those attributes might be configured.

The Cisco VPN 3000/ASA/PIX 7.x+ RADIUS attribute configurations appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** attributes that you want to apply are enabled under **Interface Configuration > RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**.

Cisco VPN 3000/ASA/PIX 7.x+ RADIUS represents only the Cisco VPN 3000/ASA/PIX 7.x+ VSA. You must configure the IETF RADIUS and Cisco VPN 3000/ASA/PIX 7.x+ RADIUS attributes.



Note

To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Cisco VPN 3000/ASA/PIX 7.x+ RADIUS attributes to apply as an authorization for the current user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Cisco VPN 3000/ASA/PIX 7.x+ RADIUS attributes, ensure that your IETF RADIUS attributes are configured properly.
For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 7-25](#).
- Step 3** In the Cisco VPN 3000/ASA/PIX 7.x+ Attribute table, to specify the attributes that should be authorized for the user:
- Check the check box next to the particular attribute.
 - Further define the authorization for that attribute in the box next to it.
 - Continue to select and define attributes, as applicable.
- For more information about attributes, see [Appendix C, “RADIUS Attributes,”](#) or your AAA client documentation.

- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User

The Cisco VPN 5000 Concentrator RADIUS attribute configurations appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco VPN 5000)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level RADIUS (Cisco VPN 5000) attributes that you want to apply are enabled under **Interface Configuration > RADIUS (Cisco VPN 5000)**.

Cisco VPN 5000 Concentrator RADIUS represents only the Cisco VPN 5000 Concentrator VSA. You must configure the IETF RADIUS and Cisco VPN 5000 Concentrator RADIUS attributes.



Note

To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Cisco VPN 5000 Concentrator RADIUS attributes to apply as an authorization for the current user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Cisco VPN 5000 Concentrator RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 7-25](#).
- Step 3** In the Cisco VPN 5000 Concentrator Attribute table, to specify the attributes that should be authorized for the user:
- a. Check the check box next to the particular attribute.
 - b. Further define the authorization for that attribute in the box next to it.
 - c. Continue to select and define attributes, as applicable.
For more information about attributes, see [Appendix C, "RADIUS Attributes,"](#) or your AAA client documentation.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Microsoft RADIUS Parameters for a User

Microsoft RADIUS provides VSAs supporting Microsoft Point-to-Point Encryption (MPPE), which is an encryption technology developed by Microsoft to encrypt point-to-point (PPP) links. These PPP connections can be via a dial-in line, or over a Virtual Private Network (VPN) tunnel.

To control Microsoft MPPE settings for users who access the network through a Cisco VPN 3000-series concentrator, use the **CVPN3000-PPTP-Encryption** (VSA 20) and **CVPN3000-L2TP-Encryption** (VSA 21) attributes. Settings for **CVPN3000-PPTP-Encryption** (VSA 20) and **CVPN3000-L2TP-Encryption** (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the **RADIUS (Cisco VPN 3000)** attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the ACS web interface or how those attributes might be configured.

The Microsoft RADIUS attribute configurations appear only if the following are true:

- AAA clients (one or more) are configured in **Network Configuration** that use a RADIUS protocol that supports the Microsoft RADIUS VSA.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Microsoft)** attributes that you want to apply are enabled under **Interface Configuration > RADIUS (Microsoft)**.

The following ACS RADIUS protocols support the Microsoft RADIUS VSA:

- Cisco IOS/PIX 6.0
- Cisco VPN 3000/ASA/PIX 7.x+
- Cisco VPN 5000
- Ascend
- Cisco Airespace

Microsoft RADIUS represents only the Microsoft VSA. You must configure the IETF RADIUS and Microsoft RADIUS attributes.



Note

To hide or display Microsoft RADIUS attributes, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Microsoft RADIUS attributes to apply as an authorization for the current user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
- The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Cisco IOS RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 7-25](#).
- Step 3** In the Microsoft RADIUS Attributes table, to specify the attributes that should be authorized for the user:
- Check the check box next to the particular attribute.
 - Further define the authorization for that attribute in the box next to it.

- c. Continue to select and define attributes, as applicable.

For more information about attributes, see [Appendix C, “RADIUS Attributes,”](#) or your AAA client documentation.



Note The **MS-CHAP-MPPE-Keys** attribute value is autogenerated by ACS; there is no value to set in the web interface.

Step 4 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 5 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Nortel RADIUS Parameters for a User

The Nortel RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Nortel)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Nortel)** attributes that you want to apply are enabled under in the **Interface Configuration > RADIUS (Nortel)**.

Nortel RADIUS represents only the Nortel proprietary attributes. You must configure the Internet Engineering Task Force (IETF) RADIUS and Nortel RADIUS attributes. Proprietary attributes override IETF attributes.



Note To hide or display Nortel RADIUS attributes, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#). A VSA that is applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Nortel RADIUS attributes to apply as an authorization for the current user:

Step 1 Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Before configuring Nortel RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 7-25](#).

Step 3 In the Nortel RADIUS Attributes table, to specify the attributes that should be authorized for the user:

- a. Check the check box next to the particular attribute.
- b. Further define the authorization for that attribute in the box next to it.
- c. Continue to select and define attributes, as applicable.

For more information about attributes, see [Appendix C, “RADIUS Attributes,”](#) or your AAA client documentation.

- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Juniper RADIUS Parameters for a User

The Juniper RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Juniper)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Juniper)** attributes that you want to apply are enabled under **Interface Configuration > RADIUS (Juniper)**.

Juniper RADIUS represents only the Juniper proprietary attributes. You must configure the IETF RADIUS and Juniper RADIUS attributes. Proprietary attributes override IETF attributes.



Note

To hide or display Juniper RADIUS attributes, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Juniper RADIUS attributes to apply as an authorization for the current user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
- The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Juniper RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 7-25](#).
- Step 3** In the Juniper RADIUS Attributes table, to specify the attributes to authorize for the user:
- Check the check box next to the particular attribute.
 - Further define the authorization for that attribute in the box next to it.
 - Continue to select and define attributes, as applicable.
- For more information about attributes, see [Appendix C, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting BBSM RADIUS Parameters for a User

The Building Broadband Services Manager (BBSM) RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (BBSM)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (BBSM)** attributes that you want to apply are enabled under **Interface Configuration > RADIUS (BBSM)**.

BBSM RADIUS represents only the BBSM proprietary attributes. You must configure the IETF RADIUS and BBSM RADIUS attributes. Proprietary attributes override IETF attributes.

**Note**

To hide or display BBSM RADIUS attributes, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable BBSM RADIUS attributes to apply as an authorization for the current user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring BBSM RADIUS attributes, ensure that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 7-25](#).
- Step 3** In the BBSM RADIUS Attributes table, to specify the attributes that should be authorized for the user:
- a. Check the check box next to the particular attribute.
 - b. Further define the authorization for that attribute in the box next to it.
 - c. Continue to select and define attributes, as applicable.
For more information about attributes, see [Appendix C, "RADIUS Attributes,"](#) or your AAA client documentation.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Custom RADIUS Attributes for a User

Custom RADIUS parameters appear only if all the following are true:

- You have defined and configured the custom RADIUS VSAs. (For information about creating user-defined RADIUS VSAs, see [Custom RADIUS Vendors and VSAs, page 9-19](#).)
- AAA clients (one or more) are configured in **Network Configuration** that use a RADIUS protocol that supports the custom VSA.

- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level RADIUS (*custom name*) attributes that you want to apply are enabled under RADIUS (*custom name*) in the **Interface Configuration** section.

You must configure the IETF RADIUS and the custom RADIUS attributes. Proprietary attributes override IETF attributes.

To configure and enable custom RADIUS attributes to apply as an authorization for the current user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 7-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring custom RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 7-25](#).
- Step 3** In the RADIUS *custom name* Attributes table, to specify the attributes that should be authorized for the user:
- Check the check box next to the particular attribute.
 - Further define the authorization for that attribute in the box next to it, as required.
 - Continue to select and define attributes, as applicable.
For more information about attributes, see [Appendix C, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

User Management

This section describes how to use the User Setup section to perform a variety of user account-management tasks.

This section contains the following topics:

- [Listing All Users, page 7-37](#)
- [Finding a User, page 7-37](#)
- [Disabling a User Account, page 7-38](#)
- [Deleting a User Account, page 7-38](#)
- [Resetting User Session Quota Counters, page 7-39](#)
- [Resetting a User Account after Login Failure, page 7-39](#)
- [Removing Dynamic Users, page 7-40](#)
- [Saving User Settings, page 7-41](#)

Listing All Users

The User List displays all user accounts (enabled and disabled). The list includes, for each user, the username, status, and the group to which the user belongs.

Username appear in the order in which they were entered into the database. This list cannot be sorted.

To view a list of all user accounts:

-
- Step 1** In the navigation bar, click **User Setup**.
The User Setup Select page opens.
- Step 2** Click **List All Users**.
In the display area on the right, the User List appears.
- Step 3** To view or edit the information for an individual user, click the username in the right window.
The user account information appears.
-

Finding a User

To find a user:

-
- Step 1** In the navigation bar, click **User Setup**.
The User Setup Select page opens.
- Step 2** Type the name in the **User** box, and then click **Find**.



Tip You can use an asterisk (*) as a wildcard in this box.



Tip To display a list of usernames that begin with a particular letter or number, click the letter or number in the alphanumeric list. A list of users, whose names begin with that letter or number, opens in the display area on the right.

The username, status (enabled or disabled), and group to which the user belongs appear in the display area on the right.

- Step 3** To view or edit the information for the user, click the username in the display area on the right.
The user account information appears.
-

Disabling a User Account

To manually disable a user account in the ACS internal database:



Note

To configure the conditions by which a user account will automatically be disabled, see [Setting Options for User Account Disablement, page 7-13](#).



Note

Do not confuse this procedure with account expiration due to password aging. Password aging is defined for groups only, not for individual users.

To disable a user account:

-
- Step 1** In the navigation bar, click **User Setup**.
The User Setup Select page opens.
- Step 2** In the **User** box, type the name of the user whose account is to be disabled.
- Step 3** Click **Add/Edit**.
The User Setup Edit page opens. The username being edited is at the top of the page.
- Step 4** Select the **Account Disabled** check box.
- Step 5** Click **Submit** at the bottom of the page.
The specified user account is disabled.
-

Deleting a User Account

You can delete user accounts one at a time by using the web interface.



Note

If you are authenticating using the Unknown User policy and you want deny a user access by deleting the user account, you must also delete the user account from the external user database. This action prevents the username from being automatically added to the ACS internal database the next time the user attempts to log in.



Tip

For deleting batches of user accounts, use the Relational Database Management System (RDBMS) Synchronization feature with action code 101 (see [RDBMS Synchronization, page 9-17](#), for more information.).

To delete a user account:

-
- Step 1** Click **User Setup**.
The User Setup Select page of the web interface opens.
- Step 2** In the **User** box, type the complete username to be deleted.



Note Alternatively, you can click **List All Users** and then select the user from the list that appears.

Step 3 Click **Add/Edit**.

Step 4 At the bottom of the User Setup page, click **Delete**.



Note The Delete button appears only when you are editing user information, not when you are adding a username.

A popup window appears and prompts you to confirm the user deletion.

Step 5 Click **OK**.

The user account is removed from the ACS internal database.

Resetting User Session Quota Counters

You can reset the session quota counters for a user before or after the user exceeds a quota.

To reset user usage quota counters:

Step 1 Click **User Setup**.

The Select page of the web interface opens.

Step 2 In the **User** box, type the complete username of the user whose session quota counters that you are going to reset.



Note Alternatively, you can click **List All Users** and then select the user from the list that appears.

Step 3 Click **Add/Edit**.

Step 4 In the Session Quotas section, select the **Reset All Counters on submit** check box.

Step 5 Click **Submit** at the bottom of the browser page.

The session quota counters are reset for this user. The User Setup Select page appears.

Resetting a User Account after Login Failure

Perform this procedure when an account is disabled because the failed attempts count has been exceeded during an unsuccessful user attempt to log in.

To reset a user account after login failure:

Step 1 Click **User Setup**.

The User Setup Select page of the web interface opens.

Step 2 In the **User** box, type the complete username of the account to be reset.



Note Alternatively, you can click **List All Users** and then select the user from the list that appears.

Step 3 Click **Add/Edit**.

Step 4 In the **Account Disable** table, select the **Reset current failed attempts count on submit** check box, and then click **Submit**.

The **Failed attempts since last successful login**: counter resets to zero (0) and the system reenables the account.



Note This counter shows the number of unsuccessful login attempts since the last time this user logged in successfully.



Note If the user authenticates with a Windows user database, this expiration information is in addition to the information in the Windows user account. Changes here do not alter settings that you configured in Windows.

Removing Dynamic Users

External sources can manage dynamic users, their identities and other related properties. Dynamic users are created in the ACS internal database after they are successfully authenticated against the external sources.

Users that are dynamically mapped will keep on being dynamically mapped even when their group mapping settings are modified to a group which is set to **Disable caching of dynamically mapped users**.

You can remove dynamic users in user groups that are cached.



Note All CSAuth activities will be suspended while dynamic users are being removed from the database.

To remove dynamic users:

Step 1 In the navigation bar, click **User Setup**.

The **User Setup Select** page appears.

Step 2 Click **Remove Dynamic Users**.

A message appears in the right pane, indicating the number of dynamic users removed or whether any errors occurred.



Note Dynamically mapped users *are not* saved when you perform replication, upgrade or overinstall ACS. Dynamically mapped users *are* saved when you back up or restore ACS.

Saving User Settings

After you have completed configuration for a user you must save your work.

To save the configuration for the current user:

-
- Step 1** To save the user account configuration, click **Submit**.
 - Step 2** To verify that your changes were applied, type the username in the **User** box and click **Add/Edit**, and then review the settings.
-

