



CHAPTER 5

User Group Management

This chapter contains information about setting up and managing user groups for authorization control in the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS. You use ACS to group network users for more efficient administration. Each user can belong to only one group in ACS. You can establish up to 500 groups for different levels of authorization.

ACS also supports external database group mapping; that is, if your external user database distinguishes user groups, you can map these groups into ACS. And if the external database does not support groups, you can map all users from that database to an ACS user group. For information about external database mapping, see [Group Mapping by External User Database, page 16-1](#).



Caution

ACS 4.0 introduced the concept of Network Access Profiles (NAPs) that affects how group authorization occurs. If you are not using NAPs, ACS functions similar to previous versions. If you do plan to use NAPs, you must understand how Remote Access Dial-in User Service (RADIUS) authorization can be split between group, user, and NAP (via RACs).

This chapter contains:

- [About User Group Setup Features and Functions, page 5-2](#)
- [Basic User Group Settings, page 5-3](#)
- [Configuration-Specific User Group Settings, page 5-12](#)
- [Group Setting Management, page 5-40](#)

Before you configure Group Setup, you should understand how this section functions. ACS dynamically builds the Group Setup section interface depending on the configuration of your network devices and the security protocols being used. That is, what you see under Group Setup is affected by settings in the Network Configuration and Interface Configuration sections. Also, you can replace any group settings for downloadable access-control lists (DACLS) and RADIUS authorization components (RACs) with the settings in the network authorization policies (NAPs). Not every setting that you add to a group may work if you perform attribute merging. For more information on attribute merging, see [Understanding RACs and NAPs, page 4-7](#).

About User Group Setup Features and Functions

The Group Setup section of the ACS web interface is the centralized location for operations regarding user group configuration and administration. For information about network device groups (NDGs), see [Configuring Network Device Groups, page 3-23](#).

This section contains:

- [Default Group, page 5-2](#)
- [Group TACACS+ Settings, page 5-2](#)
- [Group RADIUS Settings, page 5-3](#)

Default Group

If you have not configured group mapping for an external user database, ACS assigns users who are authenticated by the Unknown User Policy to the Default Group the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of ACS and kept your database information, ACS retains the group mappings that you configured before upgrading.

Group TACACS+ Settings

You can use ACS to create a full range of settings for Terminal Access Controller Access Control System (TACACS+) at the group level. If you have configured an authentication, authorization, and accounting (AAA) client to use TACACS+ as the security control protocol, you can configure standard service protocols, including Point-to-Point Protocol (PPP IP), Point-to-Point Protocol Link Control Protocol (PPP LCP), AppleTalk Remote Access Protocol (ARAP), Serial Line Internet Protocol (SLIP), and shell (exec), to apply for the authorization of each user who belongs to a particular group.

**Note**

You can also configure TACACS+ settings at the user level. User-level settings always override group-level settings.

You can also use ACS to enter and configure new TACACS+ services. For information about how to configure a new TACACS+ service to appear on the group setup page, see [Displaying TACACS+ Configuration Options, page 2-6](#).

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 1-14](#).

You can use the Shell Command Authorization Set feature to configure TACACS+ group settings. You use this feature to apply shell commands to a particular user group:

- Assign a shell command-authorization set, which you have already configured, for any network device.
- Assign a shell command-authorization set, which you have already configured, to particular NDGs.
- Permit or deny specific shell commands, which you define, on a per-group basis.

For more information about shell command-authorization sets, see [Command Authorization Sets, page 4-25](#).

Group RADIUS Settings

ACS contains a full range of settings for RADIUS at the group level. If a AAA client has been configured to use RADIUS as the security control protocol, you can configure standard services, including Internet Engineering Task Force (IETF), Microsoft, and Ascend, to apply to the authorization of each user who belongs to a particular group.

**Note**

You can also configure RADIUS settings at the user level. User-level settings always override group-level settings.

You can also use ACS to enter and configure new RADIUS services. For information about how to configure a new RADIUS service to appear on the group setup page, see [Displaying RADIUS Configuration Options, page 2-7](#).

If you decide to allow attribute merging in ACS, any RADIUS settings in all three (user, Shared Radius Authorization Component (SRAC), or group) will be overwritten by the user attributes first, then the shared RADIUS authorization component attributes, before allowing any group attributes settings.

Basic User Group Settings

This section presents the basic activities that you perform when configuring a new user group.

This section contains:

- [Group Disablement, page 5-3](#)
- [Enabling VoIP Support for a User Group, page 5-4](#)
- [Enabling VoIP Support for a User Group, page 5-4](#)
- [Setting Default Time-of-Day Access for a User Group, page 5-5](#)
- [Setting Callback Options for a User Group, page 5-5](#)
- [Setting Network Access Restrictions for a User Group, page 5-6](#)
- [Setting Max Sessions for a User Group, page 5-9](#)
- [Setting Usage Quotas for a User Group, page 5-10](#)

Group Disablement

You perform this procedure to disable a user group and, therefore, to prevent any member of the disabled group from authenticating.

**Note**

Group Disablement is the only setting in ACS where the setting at the group level may override the setting at the user level. If group disablement is set, all users within the disabled group are denied authentication, regardless of whether the user account is disabled. However, if a user account is disabled, it remains disabled; regardless of the status of the corresponding user group disablement setting. In other words, when group and user account disablement settings differ, ACS defaults to preventing network access.

To disable a group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, choose the group you want to disable, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** In the Group Disabled table, check the check box labeled **Members of this group will be denied access to the network**.
- Step 4** To disable the group immediately, click **Submit + Apply**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
The group is disabled, and all members of the group are disabled.
-

Enabling VoIP Support for a User Group



Note

If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Voice-over-IP (VoIP) Group Settings** check box.

Perform this procedure to enable support for the null password function of VoIP. This action enables users to authenticate (session or telephone call) on only the user ID (telephone number).

When you enable VoIP at the group level, all users in this group become VoIP users, and the user IDs are treated similarly to a telephone number. VoIP users must not enter passwords to authenticate.



Caution

Enabling VoIP disables password authentication and most advanced settings, including password aging and protocol attributes. If a password is submitted with a VoIP user ID, ACS fails the attempt.

To enable VoIP support for a group:




-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, choose the group that you want to configure for VoIP support, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** In the Voice-over-IP Support table, check the check box labeled **This is a Voice-over-IP (VoIP) group - and all users of this group are VoIP users**.
- Step 4** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 5** To continue and specify other group settings, perform other procedures in this chapter, as applicable.
-

Setting Default Time-of-Day Access for a User Group



Note If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Default Time-of-Day / Day-of-Week Specification** check box.

To define the times during which users in a particular group are permitted or denied access:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** In the Default Time-of-Day Access Settings table, check the **Set as default Access Times** check box.
-
-  **Note** You must check the **Set as default Access Times** check box to limit access based on time or day.
Times at which the system permits access are highlighted in green on the day-and-hour matrix.
-
-  **Note** The default sets accessibility during all hours.
-
- Step 4** In the day-and-hour matrix, click the times at which you do *not* want to permit access to members of this group.
-
-  **Tip** Clicking times of day on the graph clears those times; clicking again rechecks them.
At any time, you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.
-
- Step 5** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 6** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Setting Callback Options for a User Group

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

- **No callback allowed**—Disables callback for users in this group. This is the default setting.
- **Dialup client specifies callback number**—Allows the dialup client to specify the callback number. The dialup client must support RFC 1570, PPP LCP Extensions.

- **Use Windows Database callback settings (where possible)**—Uses the Microsoft Windows callback settings. 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 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 12-18](#).



Note The **Password Aging** feature does not operate correctly if you also use the callback feature. When you use callback, users cannot receive password aging messages at login.

To set callback options for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** Select a group from the Group list, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** In the Callback table, select one of the following three options:
- No callback allowed.
 - Dialup client specifies callback number.
 - Use Windows Database callback settings (where possible).
- Step 4** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 5** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Setting Network Access Restrictions for a User Group

You use the Network Access Restrictions table in Group Setup to apply network-access restrictions (NARs) in three distinct ways:

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



Note You can also use the CLI/DNIS-based access restrictions area to specify other values. For more information, see [About Network Access Restrictions, page 4-18](#).

Typically, you define (shared) NARs from within the Shared Components section so that these restrictions can apply to more than one group or user. For more information, see [Adding a Shared NAR, page 4-21](#). You must check the **Group-Level Shared Network Access Restriction** check box on the **Advanced Options** page of the Interface Configuration section for these options to appear in the ACS web interface.

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

**Note**

When an authentication request is forwarded by proxy to an ACS server, any NARs for RADIUS requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

To set NARs for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** To apply a previously configured shared NAR to this group:

**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 4-21](#).

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

**Tip**

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

- Step 4** To define and apply a NAR for this particular user group, that permits or denies access to this group based on IP address, or IP address and port:

**Tip**

You should define most NARs from within the Shared Components section so that the restrictions can apply to more than one group or user. For more information, see [Adding a Shared NAR, page 4-21](#).

- a. In the Per Group Defined Network Access Restrictions section of the Network Access Restrictions table, 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 **Permitted Calling/Point of Access Locations** or **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 the NDG or the name of the individual AAA client to which you want 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 filter on 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 the AAA client, port, and address information appears in the **NAR Access Control** list.

Step 5 To permit or deny access to this user group 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. From the AAA Client list, choose **All AAA Clients**, or the name of the NDG or the name of the particular AAA client to which to permit or deny access.
- d. Complete the following boxes:

**Note**

You must type 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 you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

- **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 or all numbers.

**Tip**

CLI is also the selection to use 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 4-18](#).

- **DNIS**—Type the DNIS number 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 or all numbers.

**Tip**

CLI is also the selection to use 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 4-18](#).

**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.

- e. Click **enter**.

The information, that specifies the AAA client, port, CLI, and DNIS appears in the list.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see [Saving Changes to User Group Settings, page 5-41](#).

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Max Sessions for a User Group

**Note**

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

Perform this procedure to define the maximum number of sessions that are available to a group, or to each user in a group, or both. The settings are:

- **Sessions available to group**—Sets the maximum number of simultaneous connections for the entire group.
- **Sessions available to users of this group**—Sets the maximum number of total simultaneous connections for each user in this group.


**Tip**

As an example, Sessions available to group is set to 10 and Sessions available to users of this group is set to 2. If each user is using the maximum 2 simultaneous sessions, no more than five users can log in.

A session is any type of connection that RADIUS or TACACS+ supports, such as PPP, NAS prompt, Telnet, ARAP, and IPX/SLIP.

The default setting for group Max Sessions is Unlimited for the group and the user within the group.

To configure Max Sessions settings for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** In the Max Sessions table, under Sessions available to group, select one of the following options:
- **Unlimited**—Allows this group an unlimited number of simultaneous sessions. (This action effectively disables Max Sessions.)
 - *n*—Type the maximum number of simultaneous sessions to allow this group.
- Step 4** In the lower portion of the Max Sessions table, under Sessions available to users of this group, select one of the following two options:
- **Unlimited**—Allows each individual in this group an unlimited number of simultaneous sessions. (This action effectively disables Max Sessions.)
 - *n*—Type the maximum number of simultaneous sessions to allow each user in this group.
-  **Note** Settings made in User Setup override group settings. For more information, see [Setting Max Sessions Options for a User, page 6-11](#).
-
- Step 5** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 6** Ensure the AAA client device has accounting enabled to allow Max Sessions checks to work. If accounting is not enabled, Max Sessions will not work.
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Setting Usage Quotas for a User Group



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

Perform this procedure to define usage quotas for members of a group. Session quotas affect each user of a group individually, not the group collectively. You can set quotas for a given period in two ways:

- Total duration of session
- The total number of sessions

If you make no selections in the Usage Quotas section for a group, no usage quotas are enforced on users who are assigned to that group; unless you configure usage quotas for the individual users.

**Note**

The Usage Quotas section on the Group Settings page does not show usage statistics. Usage statistics are available only on the settings page for an individual user. For more information, see [Options for Setting User Usage Quotas, page 6-12](#).


When a user exceeds his or her assigned quota, ACS denies that user access on attempting to start a session. If a quota is exceeded during a session, ACS allows the session to continue.

You can reset the usage quota counters for all users of a group from the Group Settings page. For more information about resetting usage quota counters for a whole group, see [Resetting Usage Quota Counters for a User Group, page 5-40](#).

**Tip**

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 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 Integrated Services Digital Network (ISDN), the quota is not updated until all sessions terminate. A second channel will, therefore, be accepted; even if the first channel has exhausted the quota for the user.

To set user usage quotas for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
- The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
- The name of the group appears at the top of the Group Settings page.
- Step 3** To define usage quotas based on duration of sessions:
- a. In the Usage Quotas table, check the **Limit each user of this group to x hours of online time per time unit** check box.
 - b. Type the number of hours to which you want to limit group members in the **to x hours** box. Use decimal values to indicate minutes. For example, a value of 10.5 would equal ten hours and 30 minutes.
- 

Note Up to five characters are allowed in the to x hours box.
- c. Select the period for which the quota is effective:
 - **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.
 - **Total**—An ongoing count of hours, with no end.
- Step 4** To define user session quotas based on number of sessions:
- a. In the Usage Quotas table, check the **Limit each user of this group to x sessions** check box.
 - b. Type the number of sessions to which you want to limit users in the **to x sessions** box.



Note Up to five characters are allowed in the to x sessions box.

- c. Select the period for which the session quota is effective:
- **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.
 - **Total**—An ongoing count of session, with no end.

Step 5 To save the group settings, that you have just made, click **Submit**.

For more information, see [Saving Changes to User Group Settings, page 5-41](#).

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuration-Specific User Group Settings

This section details procedures that you perform only as applicable to your particular network-security configuration. For instance, if you have no token server configured, you do not have to set token card settings for each group.

**Note**

When you configure a vendor-specific variety of RADIUS for use by network devices, the RADIUS (IETF) attributes are available because they are the base set of attributes, that all RADIUS vendors use per the RADIUS IETF specifications.

The web interface content corresponding to these procedures is dynamic and its appearance is based on:

- For a particular protocol (RADIUS or TACACS+) to be listed, at least one AAA client entry in the Network Configuration section of the web interface must use that protocol. For more information, see [Configuring AAA Clients, page 3-8](#).
- For specific protocol attributes to appear on a group profile page, you must enable the display of those attributes in the Interface Configuration section of the web interface. For more information, see [Displaying TACACS+ Configuration Options, page 2-6](#), or [Displaying RADIUS Configuration Options, page 2-7](#).

**Caution**

If you are using SRACs in 4.0, you should be aware of certain issues regarding attribute merging, and overwriting DACLS and 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. For more information on how to select RAC, the authorization rules that you use to set up your network profiles, see [Configuring an Authorization Rule, page 14-36](#).

This section contains:

- [Setting Enable Privilege Options for a User Group, page 5-13](#)
- [Setting Enable Privilege Options for a User Group, page 5-13](#)
- [Enabling Password Aging for the ACS Internal Database, page 5-15](#)

- [Enabling Password Aging for Users in Windows Databases](#), page 5-19
- [Setting IP Address Assignment Method for a User Group](#), page 5-21
- [Assigning a Downloadable IP ACL to a Group](#), page 5-22
- [Configuring TACACS+ Settings for a User Group](#), page 5-22
- [Configuring a Shell Command Authorization Set for a User Group](#), page 5-23
- [Configuring a PIX Command Authorization Set for a User Group](#), page 5-25
- [Configuring Device Management Command Authorization for a User Group](#), page 5-26
- [Configuring IETF RADIUS Settings for a User Group](#), page 5-27
- [Configuring Cisco IOS/PIX 6.0 RADIUS Settings for a User Group](#), page 5-28
- [Configuring Cisco Airespace RADIUS Settings for a User Group](#), page 5-29
- [Configuring Cisco Aironet RADIUS Settings for a User Group](#), page 5-30
- [Configuring Ascend RADIUS Settings for a User Group](#), page 5-31
- [Configuring VPN 3000/ASA/PIX v7.x+ RADIUS Settings for a User Group](#), page 5-32
- [Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group](#), page 5-33
- [Configuring Microsoft RADIUS Settings for a User Group](#), page 5-34
- [Configuring Nortel RADIUS Settings for a User Group](#), page 5-36
- [Configuring Juniper RADIUS Settings for a User Group](#), page 5-37
- [Configuring BBSM RADIUS Settings for a User Group](#), page 5-38
- [Configuring Custom RADIUS VSA Settings for a User Group](#), page 5-39

Setting Enable Privilege Options for a User Group



Note

If this section does not appear, choose **Interface Configuration > TACACS+ (Cisco)**. At the bottom of the page in the Advanced Configuration Options table, check the **Advanced TACACS+ features** check box.

Perform this procedure to configure group-level TACACS+ enabling parameters. The three possible TACACS+ enable options are:

- **No Enable Privilege**—(default) Disallows enable privileges for this user group.
- **Max Privilege for Any AAA Client**—Selects the maximum privilege level for this user group for any AAA client on which this group is authorized.
- **Define max Privilege on a per-network device group basis**—Defines maximum privilege levels for an NDG. To use this option, you create a list of device groups and corresponding maximum privilege levels. See your AAA client documentation for information about privilege levels.



Note

To define levels in this manner, you must have configured the option in Interface Configuration; if you have not done so already, choose **Interface Configuration > Advanced Settings**. Then, check the **Network Device Groups** check box.

If you are using NDGs, you use this option to configure the NDG for enable-level mapping; rather than having to do it for each user in the group.

To set enable privilege options for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** From the Jump To list at the top of the page, choose **Enable Options**.
- Step 4** Do one of the following:
- Disallow enable privileges for this user group, choose the **No Enable Privilege** option.
 - Set the maximum privilege level for this user group, for any ACS on which this group is authorized. Choose:
 - **Max Privilege for Any Access Server** option
 - Maximum privilege level from the list
 - Define the maximum NDG privilege level for this user group:
 - select the **Define max Privilege on a per-network device group basis** option
 - from the lists, choose the NDG and a corresponding privilege level
 - click **Add Association**
- Result:** The association of NDG and maximum privilege level appears in the table.
- Step 5** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 6** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Setting Token Card Settings for a User Group



Note

If this section does not appear, configure a token server. Then, choose **External User Databases> Database Configuration**. Then, add the applicable token card server.

Perform this procedure to allow a token to be cached. Users, therefore, can use a second B channel without having to enter a second one-time password (OTP).



Caution

This option is for use with token caching only for ISDN terminal adapters. You should fully understand token caching, and ISDN concepts and principles before implementing this option. Token caching allows you to connect to multiple B channels without having to provide a token for each channel connection. Token card settings are applied to all users in the selected group.

Options for token caching include the following:

- **Session**—You can select Session to cache the token for the entire session. This option allows the second B channel to dynamically go in and out of service.
- **Duration**—You can select Duration and specify a period of time to have the token cached (from the time of first authentication). If this time period expires, the user cannot start a second B channel.
- **Session and Duration**—You can select Session and Duration so that, if the session runs longer than the duration value, a new token is required to open a second B channel. Type a value high enough to allow the token to be cached for the entire session. If the session runs longer than the duration value, a new token is required to open a second B channel.

To set token card settings for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
 - Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
 - Step 3** From the Jump To list at the top of the page, choose **Token Cards**.
 - Step 4** In the Token Card Settings table, to cache the token for the entire session, choose **Session**.
 - Step 5** Also in the Token Card Settings table, to cache the token for a specified time period (measured from the time of first authentication):
 - a. Choose **Duration**.
 - b. Type the duration length in the box.
 - c. Choose the unit of measure: **Seconds**, **Minutes** or **Hours**.
 - Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
 - Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Attributes for OTP Token Caching

ACS uses the Token Card and Username attributes for OTP Token Caching. ACS caches the username and token password which bypasses the enable mode password.

Enabling Password Aging for the ACS Internal Database

You use the **Password Aging** feature of ACS to force users to change their passwords under one or more of the following conditions:

- After a specified number of days (age-by-date rules).
- After a specified number of logins (age-by-uses rules).
- The first time a new user logs in (password change rule).

Varieties of Password Aging Supported by ACS

ACS supports four distinct password-aging mechanisms:

- **Protected Extensible Authentication Protocol (PEAP) and Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling (EAP-FAST) Windows Password Aging**—Users must be in the Windows user database and be using a Microsoft client that supports EAP, such as Windows XP. For information on the requirements and configuration of this password-aging mechanism, see [Enabling Password Aging for Users in Windows Databases, page 5-19](#).
- **RADIUS-based Windows Password Aging**—Users must be in the Windows user database and be using a RADIUS client/supplicant that supports changing passwords by using Microsoft-Challenge Authentication Handshake Protocol (MS-CHAP). For information on the requirements and configuration of this password aging mechanism, see [Enabling Password Aging for Users in Windows Databases, page 5-19](#).
- **Password Aging for Device-hosted Sessions**—Users must be in the ACS internal database, the AAA client must be running TACACS+, and the connection must use Telnet. You can control the ability of users to change passwords during a device-hosted Telnet session. You can also control whether ACS propagates passwords changed by using this feature. For more information, see [Local Password Management, page 7-4](#).
- **Password Aging for Transit Sessions**—Users must be in the ACS internal database. Users must use a PPP dialup client. Further, the end-user client must have Cisco Authentication Agent (CAA) installed.



Tip The CAA software is available at <http://www.cisco.com>.

Also, to run password aging for transit sessions, the AAA client can be running RADIUS or TACACS+; moreover, the AAA client must be using Cisco IOS Release 11.2.7 or later and be configured to send a watchdog accounting packet (`aaa accounting new-info update`) with the IP address of the calling station. (Watchdog packets are interim packets sent periodically during a session. They provide an approximate session length in the event that no stop packet is received to mark the end of the session.)

You can control whether ACS propagates passwords changed by using this feature. For more information, see [Local Password Management, page 7-4](#).

ACS supports password aging by using the RADIUS protocol under MS CHAP versions 1 and 2. ACS does not support password aging over Telnet connections that use the RADIUS protocol.



Caution

If a user with a RADIUS connection tries to make a Telnet connection to the AAA client during or after the password aging warning or grace period, the Change Password option does not appear, and the user account is expired.

Password Aging Feature Settings

This section details only the Password Aging for Device-hosted Sessions and Password Aging for Transit Sessions mechanisms. For information on the Windows Password Aging mechanism, see [Enabling Password Aging for Users in Windows Databases, page 5-19](#). For information on configuring local password validation options, see [Local Password Management, page 7-4](#).



Note

The Password Aging feature does not operate correctly if you also use the Callback feature. When callback is used, users cannot receive password-aging messages at login.

The Password Aging feature in ACS has the following options:

- **Apply age-by-date rules**—Configures ACS to determine password aging by date. The age-by-date rules contain the following settings:
 - **Active period**—The number of days users will be allowed to log in before being prompted to change their passwords. For example, if you enter 20, users can use their passwords for 20 days without being prompted to change them. The default Active period is 20 days.
 - **Warning period**—The number of days, after which users will be notified to change their passwords. The existing password can be used; but the ACS presents a warning indicating that the password must be changed and displays the number of days left before the password expires. For example, if you enter 5 in this box and 20 in the Active period box, users will be notified to change their passwords on the 21st through 25th days.
 - **Grace period**—The number of days for the user grace period, which allows a user to log in once to change the password. The existing password can be used one last time after the number of days specified in the active and warning period fields has been exceeded. Then, a dialog box warns the user that the account will be disabled if the password is not changed, and prompts the user to change it. Continuing with the previous examples, if you allow a 5-day grace period, a user who did not log in during the active and warning periods would be permitted to change passwords up to and including the 30th day. However, even though the grace period is set for 5 days, a user is allowed only one attempt to change the password when the password is in the grace period. ACS displays the “last chance” warning only once. If the user does not change the password, this login is still permitted, but the password expires, and the next authentication is denied. An entry is logged in the Failed-Attempts log, and the user must contact an administrator to have the account reinstated.



Note

All passwords expire at midnight of the date that you enter, not the time of day at which they were set.

- **Apply age-by-uses rules**—Configures ACS to determine password aging by the number of logins. The age-by-uses rules contain the following settings:
 - **Issue warning after x logins**—The number of the login after which ACS begins prompting users to change their passwords. For example, if you enter 10, users are allowed to log in 10 times without a change-password prompt. On the 11th login, they are prompted to change their passwords.



Tip

To allow users to log in an unlimited number of times without changing their passwords, type **-1**.

- **Require change after x logins**—The number of logins after which to notify users that they must change their passwords. If this number is set to 12, users receive prompts requesting them to change their passwords on their 11th and 12th login attempts. On the 13th login attempt, they receive a prompt telling them that they must change their passwords. If users do not change their passwords now, their accounts expire and they cannot log in. This number must be greater than the **Issue warning after x login** number.



Tip

To allow users to log in an unlimited number of times without changing their passwords, type **-1**.

- **Apply password change rule**—Forces new users to change their passwords the first time they log in.

- **Generate greetings for successful logins**—Displays Greetings message whenever users log in successfully via the CAA client. The message contains the latest password information specific to this user account.

The password aging rules are not mutually exclusive; a rule is applied for each check box that is selected. For example, users can be forced to change their passwords every 20 days, and every 10 logins, and to receive warnings and grace periods accordingly.

If no options are selected, passwords never expire.


Unlike most other parameters, which have corresponding settings at the user level, password aging parameters are configured only on a group basis.

Users who fail authentication because they have not changed their passwords and have exceeded their grace periods are logged in the Failed Attempts log. The accounts expire and appear in the Accounts Disabled list.

Before You Begin

- Verify that your AAA client is running the TACACS+ or RADIUS protocol. (TACACS+ only supports password aging for device-hosted sessions.)
- Set up your AAA client to perform authentication *and* accounting using the same protocol, TACACS+ or RADIUS.
- Verify that you have configured your password validation options. For more information, see [Local Password Management, page 7-4](#).
- Set up your AAA client to use Cisco IOS Release 11.2.7 or later and to send a watchdog accounting packet (`aaa accounting new-info update`) with the IP address of the calling station.

To set **Password Aging** rules for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** From the Jump To list at the top of the page, choose **Password Aging**.
The Password Aging Rules table appears.
- Step 4** To set password aging by date, check the **Apply age-by-date rules** check box and type the number of days for the following options, as applicable:
- Active period
 - Warning period
 - Grace period
-  **Note** Up to five characters are allowed in each field.
-
- Step 5** To set password aging by use, check the **Apply age-by-uses rules** check box and type the number of logins for each of the following options, as applicable:
- Issue warning after *x* logins
 - Require change after *x* logins



Note Up to five characters are allowed in each field.

- Step 6** To force the user to change the password on the first login after an administrator has changed it, check the **Apply password change rule** check box.
- Step 7** To display a Greetings message, check the **Generate greetings for successful logins** check box.
- Step 8** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 9** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Enabling Password Aging for Users in Windows Databases

ACS supports three types of password aging for users in Windows databases. Both types of Windows password aging mechanisms are separate and distinct from the other ACS password aging mechanisms. For information on the requirements and settings for the password aging mechanisms that control users in the ACS internal database, see [Enabling Password Aging for the ACS Internal Database, page 5-15](#).

**Note**

You can run Windows Password Aging and ACS Password Aging for Transit Sessions mechanisms concurrently, provided that the users authenticate from the two different databases.

The types of password aging in Windows databases are:

- **RADIUS-based password aging**—RADIUS-based password aging depends on the RADIUS AAA protocol that you use to send and receive the password change messages. Requirements for implementing the RADIUS-based Windows password aging mechanism include the following:
 - Communication between ACS and the AAA client must be using RADIUS.
 - The AAA client must support MS CHAP password aging in addition to MS CHAP authentication.
 - Users must be in a Windows user database.
 - Users must be using the Windows RADIUS client and server that supports changing passwords by using MS-CHAP.
 - You must enable MS CHAP version 1 or MS CHAP version 2, or both, in the Windows configuration within the External User Databases section.

**Tip**

For information on enabling MS CHAP for password changes, see [Configuring a Windows External User Database, page 12-21](#). For information on enabling MS CHAP in System Configuration, see [Global Authentication Setup, page 9-21](#).

- **PEAP password aging**—PEAP password aging depends on the PEAP (EAP-GTC) or PEAP (EAP-MSCHAPv2) authentication protocol to send and receive the password change messages. Requirements for implementing the PEAP Windows password aging mechanism include:
 - The AAA client must support EAP.
 - Users must be in a Windows user database.

- Users must be using a Microsoft PEAP client, such as Windows XP.
- You must enable PEAP on the Global Authentication Configuration page within the System Configuration section.



Tip For information about enabling PEAP in System Configuration, see [Global Authentication Setup, page 9-21](#).

- You must enable PEAP password changes on the Windows Authentication Configuration page within the External User Databases section.



Tip For information about enabling PEAP password changes, see [Windows User Database, page 12-5](#).

- **EAP-FAST password aging**—If password aging occurs during phase zero of EAP-FAST, it depends on EAP-MSCHAPv2 to send and receive the password change messages. If password aging occurs during phase two of EAP-FAST, it depends on Extensible Authentication Protocol - Generic Token Card (EAP-GTC) to send and receive the password change messages. Requirements for implementing the EAP-FAST Windows password aging mechanism include:
 - The AAA client must support EAP.
 - Users must be in a Windows user database.
 - Users must be using a client that supports EAP-FAST.
 - You must enable EAP-FAST on the Global Authentication Configuration page within the System Configuration section.



Tip For information about enabling EAP-FAST in System Configuration, see [Global Authentication Setup, page 9-21](#).

- You must enable EAP-FAST password changes on the Windows Authentication Configuration page within the External User Databases section.



Tip For information about enabling EAP-FAST password changes, see [Windows User Database, page 12-5](#).

Users whose Windows accounts reside in remote domains (that is, not the domain within which ACS is running) can only use the Windows-based password aging if they supply their domain names.



The methods and functionality of Windows password aging differ according to the Microsoft Windows operating system that you are using, and whether you employ Active Directory (AD) or Security Accounts Manager (SAM). Setting password aging for users in the Windows user database is only one part of the larger task of setting security policies in Windows. For comprehensive information on Windows procedures, refer to your Windows system documentation.

Setting IP Address Assignment Method for a User Group

Perform this procedure to configure the way ACS assigns IP addresses to users in the group. The four possible methods are:

- **No IP address assignment**—No IP address is assigned to this group.
- **Assigned by dialup client**—Use the IP address that is configured on the dialup client network settings for TCP/IP.
- **Assigned from AAA Client pool**—The IP address is assigned by an IP address pool that is assigned on the AAA client.
- **Assigned from AAA server pool**—The IP address is assigned by an IP address pool that is assigned on the AAA server.

To set an IP address assignment method for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, choose a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** From the Jump To list at the top of the page, choose **IP Address Assignment**.
- Step 4** In the IP Assignment table, select one:
- **No IP address assignment.**
 - **Assigned by dialup client.**
 - **Assigned from AAA Client pool.** Then, type the AAA client IP pool name.
 - **Assigned from AAA pool.** Then, choose the AAA server IP pool name in the Available Pools list and click --> (right arrow button) to move the name into the Selected Pools list.
-  **Note** 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.
-  **Tip** To change the position of a pool in the list, choose the pool name and click **Up** or **Down** until the pool is in the order that you want.
- Step 5** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 6** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Assigning a Downloadable IP ACL to a Group

You use the Downloadable ACLs feature to assign an IP ACL at the group level.



Note

You must have established one or more IP ACLs before attempting to assign one. For instructions on how to add a downloadable IP ACL by using the Shared Profile Components section of the ACS web interface, see [Adding a Downloadable IP ACL, page 4-15](#).



Tip

The Downloadable ACLs table does not appear if you have not enabled it. To enable the Downloadable ACLs table, choose **Interface Configuration > Advanced Options**. Then, check the **Group-Level Downloadable ACLs** check box.

To assign a downloadable IP ACL to a group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
 - Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
 - Step 3** From the Jump To list at the top of the page, choose **Downloadable ACLs**.
 - Step 4** Under the Downloadable ACLs section, click the **Assign IP ACL** check box.
 - Step 5** Select an IP ACL from the list.
 - Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
 - Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Configuring TACACS+ Settings for a User Group

Perform this procedure to configure and enable the service or protocol parameters to apply to the authorization of each user who belongs to the group. For information on how to configure settings for the Shell Command Authorization Set, see [Configuring a Shell Command Authorization Set for a User Group, page 5-23](#).



Note

To display or hide additional services or protocols, choose **Interface Configuration > TACACS+ (Cisco IOS)**, and then choose or clear items in the group column, as applicable.

To configure TACACS+ settings for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
 - Step 2** From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

The system displays the TACACS+ Settings table section.

Step 4 To configure services and protocols in the TACACS+ Settings table to be authorized for the group:

- a. Select one or more service or protocol check boxes (for example, PPP IP or ARAP).
- b. Under each service or protocol that you selected in Step a, select attributes and then type in the corresponding values, as applicable, to further define authorization for that service or protocol.

To employ custom attributes for a particular service, you must check the **Custom attributes** check box under that service, and then specify the attribute or value in the box below the check box.

For more information about attributes, see [Appendix A, “TACACS+ Attribute-Value Pairs,”](#) or your AAA client documentation.



Tip

For ACLs and IP address pools, enter the name of the ACL or pool as defined on the AAA client. (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.)



Note

Leave the attribute value box blank to use the default (as defined on the AAA client).



Note

You can define and download an ACL. Click **Interface Configuration > TACACS+ (Cisco IOS)**, and then select **Display a window for each service selected in which you can enter customized TACACS+ attributes**. A box opens under each service or protocol in which you can define an ACL.

Step 5 To allow all services to be permitted unless specifically listed and disabled, check the **Default (Undefined) Services** check box under the Checking this option will PERMIT all UNKNOWN Services table.



Caution

The Default (Undefined) Services option is an advanced feature and should only be used by administrators who understand the security implications.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see [Saving Changes to User Group Settings, page 5-41](#).

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring a Shell Command Authorization Set for a User Group

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

- **None**—No authorization for shell commands.

- **Assign a Shell Command Authorization Set for any network device**—One shell command-authorization set is assigned, and it applies to all network devices.
- **Assign a Shell Command Authorization Set on a per Network Device Group Basis**—Associates particular shell command-authorization sets to be effective on particular NDGs.
- **Per Group Command Authorization**—Permits or denies specific Cisco IOS commands and arguments at the group level.



Note This feature requires that you have previously configured a shell command-authorization set. For detailed steps, see [Adding a Command Authorization Set, page 4-29](#).

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

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** From the Jump To list at the top of the page, choose **TACACS+**.
The system displays the TACACS+ Settings table section.
- Step 4** Use the vertical scroll bar to scroll to the Shell Command Authorization Set feature area.
- Step 5** To prevent the application of any shell command-authorization set, select (or accept the default of) the **None** option.
- Step 6** 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, choose the shell command-authorization set that you want applied to this group.
- Step 7** 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 a corresponding **Command Set**.



Tip You can select a **Command Set** that will be effective for all **Device Groups**, that are not otherwise assigned, by assigning that set to the *<default>* Device Group.

- Click **Add Association**.
The associated NDG and shell command-authorization set appear in the table.
- Step 8** To define the specific Cisco IOS commands and arguments to be permitted or denied at the group level:
- Select the **Per Group Command Authorization** option.
 - Under Unmatched Cisco IOS commands, select **Permit** or **Deny**.
If you select **Permit**, users can issue all commands not specifically listed. If you select **Deny**, users can issue only those commands listed.

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

**Caution**

Only an administrator who is skilled with Cisco IOS commands should use this powerful, advanced 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 4-28](#).

**Tip**

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

Configuring a PIX Command Authorization Set for a User Group

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

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

Before You Begin:

- Ensure that you configure a AAA client to use TACACS+ as the security control protocol.
- On the TACACS+ (Cisco) page of Interface Configuration section, ensure that you check the PIX Shell (**pixShell**) option in the Group column.
- Be certain that you have already configured one or more PIX command-authorization sets. For detailed steps, see [Adding a Command Authorization Set, page 4-29](#).

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

- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** From the Jump To list at the top of the page, choose **TACACS+**.
The system displays the TACACS+ Settings table section.
- Step 4** Scroll down to the PIX Command Authorization Set feature area within the TACACS+ Settings table.
- Step 5** To prevent the application of any PIX command-authorization set, select (or accept the default of) the **None** option.

Step 6 To assign a particular PIX command-authorization set that is to be effective on any configured network device:

- a. Select the **Assign a PIX Command Authorization Set for any network device** option.
- b. From the list directly below that option, choose the PIX command-authorization set that you want applied to this user group.

Step 7 To create associations that assign a particular PIX command-authorization set to be effective on a particular NDG, for each association:

- a. Select the **Assign a PIX Command Authorization Set on a per Network Device Group Basis** option.
- b. Select a **Device Group** and an associated **Command Set**.
- c. Click **Add Association**.

The associated NDG and PIX command-authorization sets appear in the table.



Note To remove or edit an existing PIX command-authorization set association, you can select the association from the list, and then click **Remove Association**.

Configuring Device Management Command Authorization for a User Group

Use this procedure to specify the device-management command-authorization set parameters for a group. Device-management command-authorization sets support the authorization of tasks in Cisco device-management applications that are configured to use ACS for authorization. The three options are:

- **None**—No authorization is performed for commands that are issued in the applicable Cisco 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 belonging to the NDG.



Note To use this feature, you must configure a command-authorization set for the applicable Cisco device-management application. For detailed steps, see [Adding a Command Authorization Set, page 4-29](#).

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

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

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

The system displays the TACACS+ Settings table section.

- Step 4** Use the vertical scroll bar to scroll to the *device-management application* feature area, where *device-management application* is the name of the applicable Cisco device-management application.
- Step 5** To prevent the application of any command-authorization set for the applicable device-management application, select the **None** option.
- Step 6** 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, choose the command-authorization set that you want applied to this group.
- Step 7** 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 a corresponding **device-management application**.
 - Click **Add Association**.
- The associated NDG and command-authorization sets appear in the table.
-

Configuring IETF RADIUS Settings for a User Group

These parameters appear only when the following are true. You have configured:

- A AAA client to use one of the RADIUS protocols in Network Configuration.
- Group-level RADIUS attributes on the RADIUS (IETF) page in the Interface Configuration section of the web interface.

RADIUS attributes are sent as a profile for each user from ACS to the requesting AAA client. To display or hide any of these attributes, see [Displaying RADIUS Configuration Options, page 2-7](#). For a list and explanation of RADIUS attributes, see [Appendix B, "RADIUS Attributes."](#) For more information about how your AAA client uses RADIUS, refer to your AAA client vendor documentation.

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

- Step 1** In the navigation bar, click **Group Setup**.
- The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
- The name of the group appears at the top of the Group Settings page.
- Step 3** From the Jump To list at the top of the page, choose **RADIUS (IETF)**.
- Step 4** For each IETF RADIUS attribute you must authorize the current group. Check the check box next to the attribute, and then define the authorization for the attribute in the field or fields next to it.
- Step 5** To save the group settings that you have just made and apply them immediately, click **Submit + Apply**.

**Tip**

To save your group settings and apply them later, click **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.

For more information, see [Saving Changes to User Group Settings, page 5-41](#).

- Step 6** To configure the vendor-specific attributes (VSAs) for any RADIUS network device vendor that ACS supports, see the appropriate section:
- [Configuring Cisco IOS/PIX 6.0 RADIUS Settings for a User Group, page 5-28](#)
 - [Configuring Cisco Airespace RADIUS Settings for a User Group, page 5-29](#)
 - [Configuring Cisco Aironet RADIUS Settings for a User Group, page 5-30](#)
 - [Configuring Ascend RADIUS Settings for a User Group, page 5-31](#)
 - [Configuring VPN 3000/ASA/PIX v7.x+ RADIUS Settings for a User Group, page 5-32](#)
 - [Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group, page 5-33](#)
 - [Configuring Microsoft RADIUS Settings for a User Group, page 5-34](#)
 - [Configuring Nortel RADIUS Settings for a User Group, page 5-36](#)
 - [Configuring Juniper RADIUS Settings for a User Group, page 5-37](#)
 - [Configuring BBSM RADIUS Settings for a User Group, page 5-38](#)
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco IOS/PIX 6.0 RADIUS Settings for a User Group

The Cisco IOS/PIX 6.x RADIUS parameters appear only when the following are true. You have configured:

- A AAA client to use RADIUS (Cisco IOS/PIX 6.x) in Network Configuration.
- Group-level RADIUS (Cisco IOS/PIX 6.x) attributes in Interface Configuration: RADIUS (Cisco IOS/PIX 6.x).

Cisco IOS/PIX 6.x RADIUS represents only the Cisco VSAs. You must configure the IETF RADIUS and Cisco IOS/PIX 6.x RADIUS attributes.

**Note**

To hide or display Cisco IOS/PIX 6.x RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have configured no AAA clients of this (vendor) type, the VSA settings do not appear in the group configuration interface.

To configure and enable Cisco IOS/PIX 6.x RADIUS attributes to apply as an authorization for each user in the current group:

- Step 1** Before you configure Cisco IOS/PIX 6.x RADIUS attributes, you must configure your IETF RADIUS attributes properly. For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).

Step 2 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, you use the current group for assigning authorizations to Network Admission Control (NAC) clients to which ACS assigns a system posture token of `Infected`, you could specify the following values for the `url-redirect`, `posture-token`, and `status-query-timeout` attributes:

```
url-redirect=http://10.1.1.1
posture-token=Infected
status-query-timeout=150
```

Step 3 If you want to use other Cisco IOS/PIX 6.x RADIUS attributes, check the corresponding check box and specify the required values in the adjacent text box.

Step 4 To save the group settings that you have just made, click **Submit**.

For more information, see [Saving Changes to User Group Settings, page 5-41](#).

Step 5 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Advanced Configuration Options

You use the Advanced Configuration Options section to enable the `cisco-av-pair` for authenticated port mapping.

When you enable the `cisco-av-pair` attribute, the following string is sent to the Cisco IOS/PIX device:

```
aaa:supplicant_name=username_attribute <content of User-Name attribute>
```



Note

The Enable Authenticated Port `cisco-av-pair` check box is ignored when the `cisco-av-pair` has the value `aaa:supplicant_name=` configured on the User level, Group level, or both.

The `cisco-av-pair` attribute for Layer 2 802.1X Authenticated Port Mapping is supported for the Catalyst 6000 devices that are running Cat OS.

Configuring Cisco Aireospace RADIUS Settings for a User Group

The Cisco Aireospace RADIUS parameters appear only when the following are true. You have configured:

- A AAA client to use **RADIUS (Cisco Aireospace)** in **Network Configuration**.
- Group-level **RADIUS (Cisco Aireospace)** attributes in **Interface Configuration > RADIUS (Cisco-Aireospace)**.

Cisco Aireospace RADIUS represents only the Cisco VSAs. Interface Configuration will display IETF RADIUS and Cisco IOS/PIX 6.x RADIUS attributes. You must configure the specific attributes manually.



Note

To hide or display Cisco Aireospace RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA that is applied as an authorization to a particular group 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 group configuration interface.

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

-
- Step 1** Confirm that you have configured your IETF RADIUS attributes properly. For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
ACS cannot allow for partial support of IETF; hence, adding a Cisco Airespace device (into the Network Config) will automatically enable IETF attributes just as adding a Cisco IOS device does.
- Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (Cisco Airespace)**.
- Step 5** In the Cisco Airespace RADIUS Attributes table, set the attributes to authorize for the group by checking the check box next to the attribute. Be certain to define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Configuring Cisco Aironet RADIUS Settings for a User Group

The single Cisco Aironet RADIUS Vendor Specific Attribute (VSA), Cisco-Aironet-Session-Timeout, is a virtual VSA. It is a specialized implementation of the IETF RADIUS `Session-Timeout` attribute (27) that ACS uses only when it responds to a RADIUS request from a AAA client by using RADIUS (Cisco Aironet). You can, therefore, provide different timeout values for users accessing your network through wireless and wired access devices. By specifying a timeout value specifically for WLAN connections, you avoid the conflicts 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).



Tip

In ACS 3.3, you only enable and configure the `Cisco-Aironet-Session-Timeout` when some or all members of a group connect through wired or wireless access devices. If members of a group always connect with a Cisco Aironet Access Point (AP) or always connect only with a wired access device, you do not need to use `Cisco-Aironet-Session-Timeout`; but you should instead configure RADIUS (IETF) attribute 27, `Session-Timeout`. In ACS 4.0 and later ACS versions, use a network-access profile to create a wireless-specific policy, which makes the Aironet timeout VSA obsolete. Existing configurations will not break because this VSA is supported for those configurations. RACs do not include support for this VSA.

Imagine a user group `Cisco-Aironet-Session-Timeout` set to 600 seconds (10 minutes) and that same user group IETF RADIUS `Session-Timeout` set to 3 hours. When a member of this group connects through a VPN concentrator, ACS uses three hours as the timeout value. However, if that same user connects via a Cisco Aironet AP, 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 access device or a Cisco Aironet AP.

The Cisco-Aironet-Session-Timeout VSA appears on the **Group Setup** page only when the following are true. You have configured:

- A AAA client to use **RADIUS (Cisco Aironet)** in **Network Configuration**.
- Group-level **RADIUS (Cisco Aironet)** attribute in **Interface Configuration > RADIUS (Cisco Aironet)**.

**Note**

To hide or display the Cisco Aironet RADIUS VSA, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA that is applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients configured to use RADIUS (Cisco Aironet), the VSA settings do not appear in the group configuration interface.

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

-
- Step 1** Confirm that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (Cisco Aironet)**.
- Step 5** In the Cisco Aironet RADIUS Attributes table, check the **[5842\001] Cisco-Aironet-Session-Timeout** check box.
- Step 6** 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 you configure 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 (27)` attribute, see [Appendix B, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 7** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 8** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Configuring Ascend RADIUS Settings for a User Group

The Ascend RADIUS parameters appear only when the following are true. You have configured:

- A AAA client to use RADIUS (Ascend) or RADIUS (Cisco IOS/PIX) in Network Configuration.
- Group-level RADIUS (Ascend) attributes in 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 for RADIUS is `Ascend-Remote-Addr`.

**Note**

To hide or display Ascend RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA that is applied as an authorization to a particular group 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 group configuration interface.

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

-
- Step 1** Confirm that you configured your IETF RADIUS attributes properly. For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (Ascend)**.
- Step 5** In the Ascend RADIUS Attributes table, determine the attributes to authorize for the group by checking the check box next to the attribute. Be certain to define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, "RADIUS Attributes,"](#) or your AAA client documentation.
- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Configuring VPN 3000/ASA/PIX v7.x+ RADIUS Settings for a User Group

To control Microsoft Point-to-Point Encryption (MPPE) settings for users accessing the network through Cisco VPN 3000 concentrators, for example, 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 VPN 3000/ASA/PIX v7.x+ RADIUS attribute configurations appear only if the following are true. You have configured:

- A AAA client to use RADIUS (Cisco VPN 3000/ASA/PIX v7.x+) in Network Configuration.
- Group-level RADIUS (Cisco VPN 3000/ASA/PIX v7.x+) attributes on the RADIUS (VPN 3000/ASA/PIX v7.x+) page of the Interface Configuration section.

Cisco VPN 3000/ASA/PIX v7.x+ RADIUS represents only the Cisco VPN 3000/ASA/PIX v7.x+ VSAs. You must configure the IETF RADIUS and VPN 3000/ASA/PIX v7.x+ RADIUS attributes.

**Note**

To hide or display VPN 3000/ASA/PIX v7.x+ RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group 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 group configuration interface.

To configure and enable VPN 3000/ASA/PIX v7.x+VPN 3000/ASA/PIX v7.x+ RADIUS attributes to apply as an authorization for each user in the current group:

-
- Step 1** Confirm that you properly configured your IETF RADIUS attributes.
For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (Cisco VPN 3000/ASA/PIX v7.x+)**.
- Step 5** In the Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes table, determine the attributes to authorize for the group by checking the check box next to the attribute. Further define the authorization for that attribute in the field next to it.
For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or the documentation for network devices that are using RADIUS.
- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group

The Cisco VPN 5000 Concentrator RADIUS attribute configurations appear only when the following are true. You have configured:

- A network device to use RADIUS (Cisco VPN 5000) in Network Configuration.
- Group-level RADIUS (Cisco VPN 5000) attributes on the RADIUS (Cisco VPN 5000) page of the Interface Configuration section.

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 [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group 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 group configuration interface.

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

-
- Step 1** Confirm that your IETF RADIUS attributes are configured properly.
For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (Cisco VPN 5000)**.
- Step 5** In the Cisco VPN 5000 Concentrator RADIUS Attributes table, choose the attributes that should be authorized for the group by checking the check box next to the attribute. Further define the authorization for each attribute in the field next to it.
For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or the documentation for network devices that use RADIUS.
- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Configuring Microsoft RADIUS Settings for a User Group

Microsoft RADIUS provides VSAs that support MPPE, which encrypts PPP links. These PPP connections can be via a dial-in line or over a VPN tunnel.

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, for example, 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 v7.x+) 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 when the following are true. You have configured:

- A network device in Network Configuration that uses a RADIUS protocol that supports the Microsoft RADIUS VSA.

- Group-level Microsoft RADIUS attributes on the RADIUS (Microsoft) page of the Interface Configuration section.

The following ACS RADIUS protocols support the Microsoft RADIUS VSA:

- Cisco IOS/PIX 6.0
- Cisco VPN 3000/ASA/PIX v7.x+
- 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 [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group 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 group configuration interface.

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

- Step 1** Confirm that your IETF RADIUS attributes are configured properly.
For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (Microsoft)**.
- Step 5** In the Microsoft RADIUS Attributes table, specify the attributes to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, "RADIUS Attributes,"](#) or the documentation for network devices by using RADIUS.

**Note**

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

- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Nortel RADIUS Settings for a User Group

The Nortel RADIUS attribute configurations appear only when the following are true. You have configured:

- A network device in Network Configuration that uses a RADIUS protocol that supports the Nortel RADIUS VSA.
- Group-level Nortel RADIUS attributes on the RADIUS (Nortel) page of the Interface Configuration section.

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



Note

To hide or display Nortel RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group 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 group configuration interface.

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

-
- Step 1** Confirm that your IETF RADIUS attributes are configured properly.
For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (Nortel)**.
- Step 5** In the Nortel RADIUS Attributes table, specify the attributes to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, "RADIUS Attributes,"](#) or the documentation for network devices that are using RADIUS.
-
- Note** ACS autogenerates the MS-CHAP-MPPE-Keys attribute value; there is no value to set in the web interface.
-
- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-


Configuring Juniper RADIUS Settings for a User Group

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

**Note**

To hide or display Juniper RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group 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 group configuration interface.

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

- Step 1** Confirm that you configured your IETF RADIUS attributes properly.
For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
 - Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
 - Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
 - Step 4** From the Jump To list at the top of the page, choose **RADIUS (Juniper)**.
 - Step 5** In the Juniper RADIUS Attributes table, specify the attributes to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or the documentation for network devices that are using RADIUS.
-  **Note** The MS-CHAP-MPPE-Keys attribute value is autogenerated by ACS; there is no value to set in the web interface.
- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
 - Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring 3COMUSR RADIUS Settings for a User Group

3COMUSR RADIUS represents only the 3COMUSR VSA. You must configure the IETF RADIUS and 3COMUSR RADIUS attributes.


The 3COMUSR VSA format differs from other VSAs in that 3COMUSR VSAs have a 32-bit extended Vendor-Type field and no length field.

**Note**

3Com/USR VSAs should be used for any device that uses these VSAs, not just the HiperARC cards.

To hide or display 3COMUSR RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group 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 group configuration interface.

To configure and enable 3COMUSR RADIUS attributes to apply as an authorization for each user in the current group:

-
- Step 1** Confirm that you configured your IETF RADIUS attributes properly.
For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (3COMUSR)**.
- Step 5** In the 3COMUSR RADIUS Attributes table, specify the attributes to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or the documentation for network devices that are using RADIUS.
-  **Note** The MS-CHAP-MPPE-Keys attribute value is autogenerated by ACS; there is no value to set in the web interface.
-
- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring BBSM RADIUS Settings for a User Group

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



- Note** To hide or display BBSM RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group 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 group configuration interface.

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

-
- Step 1** Confirm that you configured your IETF RADIUS attributes properly.
For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (BBSM)**.

Step 5 In the BBSM RADIUS Attributes table, specify the attribute to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or the documentation for network devices that are using RADIUS.



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

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see [Saving Changes to User Group Settings, page 5-41](#).

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Custom RADIUS VSA Settings for a User Group

User-defined, custom Radius VSA configurations appear only when all the following are true:

- You have defined and configured the custom RADIUS VSAs. (For information about creating user-defined RADIUS VSAs, see [Creating, Reading, Updating and Deleting Actions for AAA clients, page 8-22](#).)
- You have configured a network device in Network Configuration that uses a RADIUS protocol that supports the custom VSA.
- You have configured group-level custom RADIUS attributes on the RADIUS (*Name*) page of the Interface Configuration section.

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

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

Step 1 Confirm that you configured your IETF RADIUS attributes properly.

For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).

Step 2 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (custom name)**.

- Step 5** In the RADIUS (*custom name*) Attributes table, specify the attributes to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or the documentation for network devices that are using RADIUS.



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

- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Group Setting Management

This section describes how to use the **Group Setup** section to perform a variety of managerial tasks.

This section contains:

- [Listing Users in a User Group, page 5-40](#)
- [Resetting Usage Quota Counters for a User Group, page 5-40](#)
- [Renaming a User Group, page 5-41](#)
- [Saving Changes to User Group Settings, page 5-41](#)

Listing Users in a User Group

To list all users in a specified group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, choose the group.
- Step 3** Click **Users in Group**.
The User List page for the particular group that you selected opens in the display area.
- Step 4** To open a user account (to view, modify, or delete a user), click the name of the user in the User List.
The User Setup page for the particular user account selected appears.
-

Resetting Usage Quota Counters for a User Group

You can reset the usage quota counters for all members of a group, before or after a quota has been exceeded.

To reset usage quota counters for all members of a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, choose the group and click **Edit Settings**.
- Step 3** In the Usage Quotas section, check the **On submit reset all usage counters for all users of this group** check box.
- Step 4** Click **Submit** at the bottom of the browser page.
The usage quota counters for all users in the group are reset. The Group Setup Select page appears.
-

Renaming a User Group

To rename a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, choose the group.
- Step 3** Click **Rename Group**.
The Renaming Group: *Group Name* page appears.
- Step 4** Type the new name in the **Group** field. Group names cannot contain angle brackets (< >).
- Step 5** Click **Submit**.



Note The group remains in the same position in the list. The number value of the group is still associated with this group name. Some utilities, such as the database import utility, use the numeric value that is associated with the group.

The Select page opens with the new group name selected.

Saving Changes to User Group Settings

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

To save the configuration for the current group:

-
- Step 1** To save your changes and apply them immediately, click **Submit + Apply**. This action restarts ACS services and applies the changes.
You can click only the **Submit** button if you do not want to affect your network with a restart.
- Step 2** To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.
The group attributes are applied and services are restarted. The Edit page opens.



Note Restarting the service clears the Logged-in User Report and temporarily interrupts all ACS services. This action affects the Max Sessions counter.

Step 3 To verify that your changes were applied, choose the group and click **Edit Settings**. View the settings.
