



Using the Web Interface

Ease of use is the overriding design principle of the web interface in the Cisco Secure Access Control Server Release 4.0 Solution Engine, henceforth referred to as ACS. ACS presents intricate concepts of network security from the perspective of an administrator. You can use the Interface Configuration section of ACS to configure the ACS web interface. You can tailor the interface to simplify screens by hiding the features that you do not use and adding fields for your specific configuration.



Note

We recommend that you return to this section to review and confirm your initial settings. While it is logical to begin your ACS configuration efforts with configuring the interface, sometimes a section of the web interface that you initially believed should be hidden from view may later require configuration from within this section.



Tip

If a section of the ACS web interface appears to be missing or broken, return to the Interface Configuration section and confirm that the particular section has been activated.

This chapter contains the following topics:

- [Administrative Sessions, page 3-1](#)
- [Interface Design Concepts, page 3-4](#)
- [User Data Configuration Options, page 3-4](#)
- [Advanced Options, page 3-5](#)
- [Protocol Configuration Options for TACACS+, page 3-7](#)
- [Protocol Configuration Options for RADIUS, page 3-9](#)

Administrative Sessions

We recommend that administrative sessions take place without the use of an HTTP proxy server, without a firewall between the browser and ACS, and without a NAT gateway between the browser and ACS. Because these limitations are not always practical, this section discusses how various network environmental issues affect administrative sessions.

This section contains the following topics:

- [Administrative Sessions and HTTP Proxy, page 3-2](#)
- [Administrative Sessions Through Firewalls, page 3-2](#)
- [Administrative Sessions Through a NAT Gateway, page 3-2](#)

Administrative Sessions and HTTP Proxy

ACS does not support HTTP proxy for administrative sessions. If the browser used for an administrative session is configured to use a proxy server, ACS sees the administrative session originating from the IP address of the proxy server rather than from the actual address of the computer. Administrative session tracking assumes each browser resides on a computer with a unique IP.

Also, IP filtering of proxied administrative sessions has to be based on the IP address of the proxy server rather than the IP address of the computer. This conflicts with administrative session communication that does use the actual IP address of the computer. For more information about IP filtering of administrative sessions, see [Access Policy, page 12-8](#).

For these reasons, we do not recommend performing administrative sessions using a web browser that is configured to use a proxy server. Administrative sessions using a proxy-enabled web browser is not tested. If your web browser is configured to use a proxy server, disable HTTP proxying when attempting ACS administrative sessions.

Administrative Sessions Through Firewalls

In the case of firewalls that do not perform network address translation (NAT), administrative sessions conducted across the firewall can require additional configuration of ACS and the firewall. This is because ACS assigns a random HTTP port at the beginning of an administrative session.

To allow administrative sessions from browsers outside a firewall that protects ACS, the firewall must permit HTTP traffic across the range of ports that ACS is configured to use. You can control the HTTP port range using the HTTP port allocation feature. For more information about the HTTP port allocation feature, see [HTTP Port Allocation for Administrative Sessions, page 1-18](#).

While administering ACS through a firewall that is not performing NAT is possible, we do not recommend that you administer ACS through a firewall. For more information, see [HTTP Port Allocation for Administrative Sessions, page 1-18](#).

Administrative Sessions Through a NAT Gateway

We do not recommend conducting administrative sessions across a network device performing NAT. If the administrator runs a browser on a computer behind a NAT gateway, ACS receives the HTTP requests from the public IP address of the NAT device, which conflicts with the computer private IP address, included in the content of the HTTP requests. ACS does not permit this.

If ACS is behind a NAT gateway and the URL used to access the web interface specifies ACS by its hostname, administrative sessions operate correctly, provided that DNS is functioning correctly on your network or that computers used to access the web interface have a hosts file entry for ACS.

If the URL used to access the web interface specifies ACS by its IP address, you could configure the gateway to forward all connections to port 2002 to ACS, using the same port. Additionally, all the ports allowed using the HTTP port allocation feature would have to be similarly mapped. We have not tested such a configuration and do not recommend implementing it.

Accessing the Web Interface

Remote administrative sessions always require that you log in using a valid administrator name and password, as configured in the Administration Control section. If the Allow automatic local login check box is cleared on the Sessions Policy Setup page in the Administration Control section, ACS requires a valid administrator name and password for administrative sessions accessed from a browser on the computer running ACS.

Before You Begin

Determine whether a supported web browser is installed on the computer you want to use to access the web interface. If not, install a supported web browser or use a computer that already has a supported web browser installed. For a list of supported browsers, see the *Release Notes for Cisco Secure ACS Solution Engine 4.0*. The latest revision to the Release Notes is posted on Cisco.com (<http://www.cisco.com>).

Because the web interface uses Java in a few places, the computer running the browser used to access the web interface must have a Java Virtual Machine available for the use of the browser.

To access the web interface:

-
- Step 1** Open a web browser. For a list of supported web browsers, see the Release Notes for the version of ACS you are accessing. The most recent revision to the Release Notes is posted on Cisco.com (<http://www.cisco.com>).
- Step 2** In the Address or Location bar in the web browser, type the applicable URL. For a list of possible URLs, see [Uniform Resource Locator for the Web Interface, page 1-20](#).
- Step 3** If the ACS login page appears:
- In the Username box, type a valid ACS administrator name.
 - In the Password box, type the password for the administrator name you specified.
 - Click **Login**.

The initial page appears, listing build and copyright information.

Logging Off the Web Interface

When you are finished using the web interface, we recommend that you log off. While ACS can timeout unused administrative sessions, logging off prevents unauthorized access by someone using the browser after you or by unauthorized persons using the HTTP port left open to support the administrative session.

To log off the ACS web interface, click the **X** in the upper-right corner of the screen.



Note

The Logoff button appears in the upper-right corner of the browser window, except on the initial page, where it appears in the upper-left corner of the configuration area.

Interface Design Concepts

Before you begin to configure the ACS web interface for your particular configuration, you should understand a few basic precepts of the system operation. The information in the following sections is necessary for effective interface configuration.

Introduction of Network Access Profiles

Network-access profiles (NAPs) play a role with RADIUS provisioning and DACL assignment. You no longer only need to rely on user and group settings. With NAPs you can set up authorization rules that allow you to set user groups, RACs, and DACLs as part of a profile.

User-to-Group Relationship

A user can belong to only one group at a time. As long as there are no conflicting attributes, users inherit group settings.

**Note**

If a user profile has an attribute configured differently from the same attribute in the group profile, the user setting always overrides the group setting.

If a user has a unique configuration requirement, you can make that user a part of a group and set unique requirements on the User Setup page; or you can assign that user to his or her own group.

User and group can be mapped to network-access profiles by using authorization rules. For more details on authorization rules, see [Configuring Authorization Policies, page 15-43](#).

Per-User or Per-Group Features

You can configure most features at both the group and user levels, with the following exceptions:

- **User level only**—Static IP address, password, and expiration.
- **Group level only**—Password aging and time-of-day/day-of-week restrictions.

User Data Configuration Options

The Configure User Defined Fields page enables you to add (or edit) up to five fields for recording information on each user. The fields you define in this section subsequently appear in the Supplementary User Information section at the top of the User Setup page. For example, you could add the user's company name, telephone number, department, billing code, and so on. You can also include these fields in the accounting logs. For more information about the accounting logs, see [About ACS Logs and Reports, page 11-4](#). For information on the data fields that compose the user data options, see [User-Defined Attributes, page E-24](#).

Configuring New User Data Fields

To configure new user data fields:

Step 1 Click **Interface Configuration**, and then click **User Data Configuration**.

The Configure User Defined Fields page appears. Check boxes in the Display column indicate which fields are configured to appear in the Supplementary User Information section at the top of the User Setup page.

Step 2 Check a check box in the Display column.

Step 3 In the corresponding **Field Title** box, type a title for the new field.

Step 4 To configure another field, repeat Step 2 and Step 3.

Step 5 When you have finished configuring new user data fields, click **Submit**.



Tip You can change the title of a field by editing the text in the **Field Title** box and then clicking **Submit**.

Advanced Options

You use the Advanced Options page to determine which advanced features ACS displays. You can simplify the pages that appear in other areas of the ACS web interface by hiding advanced features that you do not use.



Caution

Disabling an advanced feature in the Interface Configuration section does not affect anything except the display of that feature in the web interface. Settings made while an advanced feature was visible remain in effect when that advanced feature is no longer visible. Further, the interface displays any advanced feature that has nondefault settings, even if you have configured that advanced feature to be hidden. If you later disable the feature or delete its settings, ACS hides the advanced feature. The only exception is the Network Device Groups feature. Regardless of whether Network Device Groups are in use, they are hidden when you clear the appropriate check box on the Advanced Options page.

The advanced option features include:

- **Per-User TACACS+/RADIUS Attributes**—When selected, this feature enables TACACS+/RADIUS attributes to be set at a per-user level, in addition to being set at the group level. After this option is enabled, you must edit the TACACS+ (Cisco IOS) or any RADIUS page in the Interface Configuration section to specify which attributes you want to appear in user accounts. After you do this, user accounts display the selected attributes and enable them to be configured. Attributes configured at the user level override those defined at the group level.
- **User-Level Shared Network Access Restrictions**—When selected, this feature enables the Shared Profile Component network-access restrictions (NARs) options on the User Setup page. You use these options to apply previously configured, named, IP-based and CLID/DNIS-based NARs at the user level. For information on defining a NAR, or NAR set, within Shared Profile Components, see [Adding a Shared NAR, page 5-20](#).

- **User-Level Network Access Restrictions**—When selected, this feature enables the two sets of options for defining user-level, IP-based and CLI/DNIS-based NARs, on the User Setup page.
- **User-Level Downloadable ACLs**—When selected, this feature enables the Downloadable ACLs (access-control lists) section on the User Setup page.
- **Default Time-of-Day/Day-of-Week Specification**—When selected, this feature enables the default time-of-day/day-of-week access settings grid on the Group Setup page.
- **Group-Level Shared Network Access Restrictions**—When selected, this feature enables the Shared Profile Component NAR options on the Group Setup page. You use these options to apply previously configured, named, IP-based and CLID/DNIS-based NARs at the group level. For information on defining a NAR, or NAR set, within Shared Profile Components, see [Adding a Shared NAR, page 5-20](#).
- **Group-Level Network Access Restrictions**—When selected, this feature enables the two sets of options for defining group-level, IP-based and CLI/DNIS-based NARs on the Group Setup page.
- **Group-Level Downloadable ACLs**—When selected, this feature enables the Downloadable ACLs section on the Group Setup page.
- **Group-Level Password Aging**—When selected, this feature enables the Password Aging section on the Group Setup page. The Password Aging feature enables you to force users to change their passwords.
- **Network Access Filtering**—When selected, this feature enables the Network Access Filtering (NAF) section on the Shared Profiles Components pages. The Network Access Filtering option lets you set up groups of authentication, authorization, and accounting (AAA) client configurations (which may represent multiple network devices), network device groups (NDGs), or IP addresses of specific AAA client devices. You can use NAFs with downloadable IP ACLs and network-access restrictions to control access easily by device, which is important when creating your NAPs.
- **Max Sessions**—When selected, this feature enables the Max Sessions section on the User Setup and Group Setup pages. The Max Sessions option sets the maximum number of simultaneous connections for a group or a user.
- **Usage Quotas**—When selected, this feature enables the Usage Quotas sections on the User Setup and Group Setup pages. The Usage Quotas option sets one or more quotas for usage by a group or a user.
- **Distributed System Settings**—When selected, this feature displays the AAA server and proxy tables on the Network Interface page. If the tables have information other than the defaults in them, they always appear.
- **Remote Logging**—When selected, this feature enables the Remote Logging feature on the Logging page of the System Configuration section.
- **ACS Database Replication**—When selected, this feature enables the ACS database replication information on the System Configuration page.
- **RDBMS Synchronization**—When selected, this feature enables the Relational Database Management System (RDBMS) Synchronization option on the System Configuration page. If RDBMS Synchronization is configured, this option always appears.
- **IP Pools**—When selected, this feature enables the IP Pools Address Recovery and IP Pools Server options on the System Configuration page.
- **Network Device Groups**—When selected, this option enables network device groups (NDGs). When NDGs are enabled, the Network Configuration section and parts of the User Setup and Group Setup pages change to enable you to manage groups of network devices (AAA clients or AAA servers). This feature is useful if you have many devices to administer.

- **Voice-over-IP (VoIP) Group Settings**—When selected, this feature enables the VoIP option on the Group Setup page.
- **Voice-over-IP (VoIP) Accounting Configuration**—When selected, this feature enables the VoIP Accounting Configuration option on the System Configuration page. You use this option to determine the logging format of RADIUS VoIP accounting packets.

Setting Advanced Options for the ACS User Interface

To set advanced options for the ACS web interface:

Step 1 Click **Interface Configuration**, and then click **Advanced Options**.

The Advanced Options table appears.

Step 2 Select each option that you want enabled in the ACS web interface.



Caution

Disabling an advanced feature in the Interface Configuration section does not affect anything except the display of that feature in the web interface. Settings made while an advanced feature was visible remain in effect when that advanced feature is no longer visible. Furthermore, the interface displays any advanced feature that has nondefault settings, even if you have configured that advanced feature to be hidden. If you later disable the feature or delete its settings, ACS hides the advanced feature. The only exception is the Network Device Groups feature. Regardless of whether Network Device Groups are in use, they are hidden when you clear the appropriate check box on the Advanced Options page.

Step 3 When you have finished making selections, click **Submit**.

ACS alters the contents of various sections of the web interface according to your selections.

Protocol Configuration Options for TACACS+

The TACACS+ (Cisco) page details the configuration of the ACS web interface for TACACS+ settings. You use the interface settings to display or hide TACACS+ administrative and accounting options. You can simplify the web interface by hiding the features that you do not use.

The TACACS+ (Cisco) page comprises three distinct areas:



Tip

The default interface setting presents a single column of check boxes, at the group level only, for selecting TACACS+ Services Settings and New Service Settings. To view two columns of check boxes that you check to configure settings at the Group level or the User level, you must have enabled the Per-user TACACS+/RADIUS Attributes option on the Advanced Options page of Interface Configuration section.

- **TACACS+ Services Settings**—This area contains a list of the most commonly used services and protocols for TACACS+. You select each TACACS+ service that you want to appear as a configurable option on the User Setup page or Group Setup page.
- **New Services**—In this area you can enter any services or protocols that are particular to your network configuration.



Note If you have configured ACS to interact with device-management applications for other Cisco products, such as Management Center for Firewalls, ACS might display new TACACS+ services as dictated by these device-management applications. To ensure the proper functioning of ACS, of device-management applications with which ACS interacts, and of the Cisco network devices managed by those applications, do not change or delete automatically generated TACACS+ service types.

- **Advanced Configuration Options**—In this area you can add more detailed information for even more tailored configurations.

The four items that you can choose to hide or display are:

- **Advanced TACACS+ Features**—This option displays or hides the Advanced TACACS+ Options section on the User Setup page. These options include Privilege Level Authentication and Outbound Password Configuration for SENDPASS and SENDAUTH clients, such as routers.
- **Display a Time-of-Day access grid for every TACACS+ service where you can override the default Time-of-Day settings**—If this option is checked, a grid appears on the User Setup page that you use to override the TACACS+ scheduling attributes on the Group Setup page.

You can control the use of each TACACS+ service by the time of day and day of week. For example, you can restrict Exec (Telnet) access to business hours but permit PPP-IP access at any time.

The default setting is to control time-of-day access for all services as part of authentication. However, you can override the default and display a time-of-day access grid for every service. This setting keeps user and group setup easy to manage, while making this feature available for the most sophisticated environments. This feature applies only to TACACS+ because TACACS+ can separate the authentication and authorization processes. RADIUS time-of-day access applies to all services. If TACACS+ and RADIUS are used simultaneously, the default time-of-day access applies to both. The default provides a common method by which to control access regardless of the access-control protocol.

- **Display a window for each service selected in which you can enter customized TACACS+ attributes**—If you check this option, an area appears on the User Setup and Group Setup pages in which you enter custom TACACS+ attributes.

ACS can also display a custom command field for each service. You use this text field to make specialized configurations to be downloaded for a particular service for users in a particular group.

You can use this feature to send many TACACS+ commands to the access device for the service, provided that the device supports the command, and that the command syntax is correct. This feature is disabled by default, but you can enable it the same way you enable attributes and time-of-day access.

- **Display enable Default (Undefined) Service Configuration**—If this check box is checked, an area appears on the User Setup and Group Setup pages in which you permit unknown TACACS+ services, such as Cisco Discovery Protocol (CDP).



Note Only advanced system administrators should use this option.



Note Customized settings at the user level take precedence over settings at the group level.

Setting Options for TACACS+

**Note**

The ACS web interface displays any protocol option that is enabled or has nondefault values, even if you have configured that protocol option to be hidden. If you later disable the option or delete its value and the protocol option is configured to be hidden, ACS hides the protocol option. This behavior prevents ACS from hiding active settings.

You use this procedure to display or hide TACACS+ administrative and accounting options. It is unlikely that you will use every service and protocol available for TACACS+. Displaying each would make setting up a user or group cumbersome. To simplify setup, you can use the TACACS+ (Cisco IOS) Edit page to customize the services and protocols that appear.

To configure the user interface for TACACS+ options:

Step 1 Click **Interface Configuration**, and then click **TACACS+ (Cisco IOS)**.

The TACACS+ (Cisco) page appears.

Step 2 In the **TACACS+ Services** table, check the check box for each TACACS+ service that you want to be visible on the applicable setup page.

Step 3 To add new services and protocols:

- a. In the New Services section of the TACACS+ Services table, type in any Service and Protocol to be added.

**Note**

If you have configured ACS to interact with device-management applications for other Cisco products, such as a Management Center for Firewalls, ACS may display new TACACS+ services as dictated by these device-management applications. To ensure the proper functioning of ACS, of device-management applications with which ACS interacts, and of the Cisco network devices managed by those applications, do not change or delete automatically generated TACACS+ service types.

- b. Check the appropriate check box to select those that should be visible for configuration under User Setup, or Group Setup, or both.

Step 4 In the Advanced Configurations Options section, check the check boxes of the display options that you want to enable.

Step 5 When you have finished setting TACACS+ interface display options, click **Submit**.

The selections made in this procedure determine what TACACS+ options ACS displays in other sections of the web interface.

Protocol Configuration Options for RADIUS

It is unlikely that you would want to install every attribute available for every protocol. Displaying each would make setting up a user or group cumbersome. To simplify setup, use the options in this section to customize the attributes that are visible. For a list of supported RADIUS AV pairs and accounting AV pairs, see [Appendix C, “RADIUS Attributes.”](#)

Depending on which AAA client or clients you have configured, the Interface Configuration page displays different choices of RADIUS protocol configuration settings. The Interface Configuration page displays RADIUS Internet Engineering Task Force (IETF) settings whenever any RADIUS AAA client is configured. The Interface Configuration page also displays additional settings for each vendor-specific RADIUS type. The settings that appear for various types of AAA client depend on what settings that type of device can employ. These combinations are detailed in [Table 3-1](#).

Table 3-1 RADIUS Listings in Interface

Configure this Type of AAA Client	The Interface Configuration Page Lists the Types of Settings Shown										
	RADIUS (IETF)	RADIUS (Cisco Airespace)	RADIUS (Cisco Aironet)	RADIUS (BBSM)	RADIUS (Cisco IOS/PIX 6.0)	RADIUS (Microsoft)	RADIUS (Ascend)	RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)	RADIUS (Cisco VPN 5000)	RADIUS (Juniper)	RADIUS (Nortel)
RADIUS (IETF)/ RADIUS (iPass)	Yes	No	No	No	No	No	No	No	No	No	No
RADIUS (Cisco Airespace)	Yes	Yes	No	No	No	No	No	No	No	No	No
RADIUS (Cisco Aironet)	Yes	No	Yes	No	Yes	No	No	No	No	No	No
RADIUS (BBSM)	Yes	No	No	Yes	No	No	No	No	No	No	No
RADIUS (Cisco IOS/ PIX 6.0)	Yes	No	No	No	Yes	Yes	Yes	No	No	No	No
RADIUS (Ascend)	Yes	No	No	No	No	Yes	Yes	No	No	No	No
RADIUS (Cisco VPN3000/ASA/ PIX 7.x+)	Yes	No	No	No	Yes	Yes	No	Yes	No	No	No
RADIUS (Cisco VPN 5000)	Yes	No	No	No	No	No	No	No	Yes	No	No
RADIUS (Juniper)	Yes	No	No	No	No	No	No	No	No	Yes	No
RADIUS (Nortel)	Yes	No	No	No	No	No	No	No	No	No	Yes



Tip

You must configure your network devices before you can select, on the Interface Configuration page, a type of setting for further configuration.

From the Interface Configuration page, when you select a type of RADIUS setting to configure, the web interface displays the corresponding list of available RADIUS attributes and associated check boxes. If you have selected the Per-user TACACS+/RADIUS Attributes check box in Interface Configuration: Advanced Options, a User check box appears alongside the Group check box for each attribute. Otherwise, only the Group check box for each attribute appears. By checking check boxes in a list of attributes, you determine whether the corresponding (IETF) RADIUS attribute or vendor-specific attribute (VSA) is configurable from the User Setup and Group Setup sections.

Details regarding the types of RADIUS settings pages:

- **(IETF) RADIUS Settings**—This page lists attributes available for (IETF) RADIUS.

These standard (IETF) RADIUS attributes are available for any network device configuration when using RADIUS. If you want to use IETF attribute number 26 (for VSAs), select Interface Configuration and then RADIUS for the vendors whose network devices you use. Attributes for (IETF) RADIUS and the VSA for each RADIUS network device vendor supported by ACS appear in User Setup or Group Setup.



Note The RADIUS (IETF) attributes are shared with RADIUS VSAs. You must configure the first RADIUS attributes from RADIUS (IETF) for the RADIUS vendor.

The Tags to Display Per Attribute option (located under Advanced Configuration Options) enables you to specify how many values to display for tagged attributes on the User Setup and Group Setup pages. Examples of tagged attributes include [064]Tunnel-Type and [069]Tunnel-Password.

For detailed steps, see [Setting Protocol Configuration Options for IETF RADIUS Attributes, page 3-12](#).

- **RADIUS (Cisco IOS/PIX 6.0) Settings**—You use this section to enable the specific attributes for RADIUS (Cisco IOS/PIX 6.0). Selecting the first attribute listed under RADIUS (Cisco IOS/PIX 6.0), 026/009/001, displays an entry field under User Setup and/or Group Setup in which any TACACS+ commands can be entered to fully leverage TACACS+ in a RADIUS environment. For detailed steps, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#).
- **RADIUS (Cisco Aironet) Settings**—This section is now obsolete. You can now use the session-timeout in a dedicated WLAN RADIUS Authorization Component (RAC).



Tip

We recommend that you do not use the RADIUS Cisco Aironet settings to enable a specific attribute for RADIUS (Cisco Aironet) unless it is an existing configuration.

When ACS responds to an authentication request from a Cisco Aironet Access Point and the Cisco-Aironet-Session-Timeout attribute is configured in the RAC, ACS sends to the wireless device this value in the IETF Session-Timeout attribute. This setting enables you to provide different session-timeout values for wireless and wired end-user clients. For steps on adding a WLAN RAC session-timeout, see [Adding RADIUS Authorization Components, page 5-9](#).

- **RADIUS (Cisco Airespace) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Cisco Airespace). This page appears if you have configured a RADIUS (Cisco Airespace) device. For detailed procedures, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#).

- **RADIUS (Ascend) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Ascend). This page appears if you have configured a RADIUS (Ascend) or a RADIUS (Cisco IOS/PIX 6.0) device. For detailed procedures, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#).
- **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Cisco VPN 3000/ASA/PIX 7.x+). For detailed procedures, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#).
- **RADIUS (Cisco VPN 5000) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Cisco VPN 5000). For detailed procedures, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#).
- **RADIUS (Microsoft) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Microsoft). This page appears if you configure a RADIUS (Ascend), or a RADIUS (VPN 3000/ASA/PIX 7.x+), or a RADIUS (Cisco IOS/PIX 6.0) device. For detailed procedures, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#).
- **RADIUS (Nortel) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Nortel). For detailed procedures, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#).
- **RADIUS (Juniper) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Juniper). For detailed procedures, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#).
- **RADIUS (BBSM) Settings**—From this section you enable the RADIUS VSAs for RADIUS Building Broadband Service Manager (BBSM). For detailed procedures, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-13](#).

While ACS ships with these prepackaged VSAs, you can also define and configure custom attributes for any VSA set that is not already contained in ACS. If you have configured a custom VSA and a corresponding AAA client, from the Interface Configuration section you can select the custom VSA and then set the options for how particular attributes appear as configurable options on the User Setup or Group Setup page. For information about creating user-defined RADIUS VSAs, see [Custom RADIUS Vendors and VSAs, page 9-19](#).

Setting Protocol Configuration Options for IETF RADIUS Attributes

This procedure enables you to hide or display any of the standard IETF RADIUS attributes for configuration from other portions of the ACS web interface.



Note

If the Per-user TACACS+/RADIUS Attributes check box in Interface Configuration: Advanced Options is selected, a User check box appears alongside the Group check box for each attribute.



Note

Your RADIUS network devices must support each checked RADIUS attribute.

To set protocol configuration options for IETF RADIUS attributes:

- Step 1** Click **Interface Configuration**, and then click **RADIUS (IETF)**.
The RADIUS (IETF) page appears.

- Step 2** For each IETF RADIUS attribute that you want to appear as a configurable option on the User Setup or Group Setup page, check the corresponding check box.



Note Your RADIUS network devices must support each checked RADIUS attribute.

- Step 3** To specify how many values to display for tagged attributes on the User Setup and Group Setup pages, select the **Tags to Display Per Attribute** option, and then select a value from the corresponding list. Examples of tagged attributes are [064] Tunnel-Type and [069] Tunnel-Password.

- Step 4** When you have finished selecting the attributes, click **Submit**.

Each IETF RADIUS attribute that you checked appears as a configurable option on the User Setup or Group Setup page, as applicable.

Setting Protocol Configuration Options for Non-IETF RADIUS Attributes

You use this procedure to hide or display various RADIUS VSAs for configuration from the User Setup and Group Setup portions of the ACS web interface.

To set protocol configuration options for a set of RADIUS VSAs:

-
- Step 1** Click **Interface Configuration**.

- Step 2** Click one of the RADIUS VSA set types, for example, RADIUS (Ascend).

- Step 3** The page listing the selected set of available RADIUS VSAs appears.



Note If the Per-user TACACS+/RADIUS Attributes check box in Interface Configuration: Advanced Options is checked, a User check box appears beside the Group check box for each attribute.

- Step 4** For each RADIUS VSA that you want to appear as a configurable option on the User Setup or Group Setup page, check the corresponding check box.



Note Each checked attribute must be supported by your RADIUS network devices.

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

According to your selections, the RADIUS VSAs appear on the User Setup or Group Setup pages, or both, as a configurable option.
