



Interface Configuration

Ease of use is the overriding design principle of the HTML interface in the Cisco Secure ACS for Windows Server. Cisco Secure ACS presents intricate concepts of network security from the perspective of an administrator. The Interface Configuration section of Cisco Secure ACS enables you to configure the Cisco Secure ACS HTML interface—you can tailor the interface to simplify the screens you will use by hiding the features that you do not use and by 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 Cisco Secure ACS configuration efforts with configuring the interface, sometimes a section of the HTML interface that you initially believed should be hidden from view may later require configuration from within this section.



Tip

If a section of the Cisco Secure ACS HTML 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:

- [Interface Design Concepts, page 3-2](#)
- [User Data Configuration Options, page 3-3](#)
- [Advanced Options, page 3-4](#)

- [Protocol Configuration Options for TACACS+, page 3-7](#)
- [Protocol Configuration Options for RADIUS, page 3-11](#)

Interface Design Concepts

Before you begin to configure the Cisco Secure ACS HTML 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.

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.

Per-User or Per-Group Features

You can configure most features at both 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 Cisco Secure ACS Logs and Reports, page 11-6](#). For information on the data fields that compose the user data options, see [User-Defined Attributes, page F-34](#).

Defining New User Data Fields

To configure new user data fields, follow these steps:

-
- 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** Select 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. For the change to take effect, you must restart the Cisco Secure ACS services by clicking Restart at the bottom of the Service Control page in the System Configuration section and then stopping and restarting the CSAdmin service by using the Services section of the Administrative Tools folder in Windows Control Panel.

Restarting Cisco Secure ACS-related Windows services should be done during off hours because it briefly interrupts authentication, authorization, and accounting.

Advanced Options

The Advanced Options page enables you to determine which advanced features Cisco Secure ACS displays. You can simplify the pages displayed in other areas of the Cisco Secure ACS HTML 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 HTML interface. Settings made while an advanced feature was displayed remain in effect when that advanced feature is no longer displayed. Further, the interface displays any advanced feature that has non-default settings, even if you have configured that advanced feature to be hidden. If you later disable the feature or delete its settings, Cisco Secure 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 deselected on the Advanced Options page.

The advanced option features include the following:

- **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.
- **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. These options allow you 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 Network Access Restriction, page 5-19](#).

- **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. These options allow you 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 Network Access Restriction, page 5-19](#).
- **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.
- **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.
- **Cisco Secure ACS Database Replication**—When selected, this feature enables the Cisco Secure ACS database replication information on the System Configuration page.

- **RDBMS Synchronization**—When selected, this feature enables the RDBMS (Relational Database Management System) 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. This option is used to determine the logging format of RADIUS VoIP accounting packets.
- **ODBC Logging**—When selected, this feature enables the ODBC logging sections on the Logging page of the System Configuration section.

Setting Advanced Options for the Cisco Secure ACS User Interface

To set advanced options for the Cisco Secure ACS HTML interface, follow these steps:

-
- Step 1** Click **Interface Configuration**, and then click **Advanced Options**.
The Advanced Options table appears.
- Step 2** Select each option that you want displayed (enabled) in the Cisco Secure ACS HTML interface.

**Caution**

Disabling an advanced feature in the Interface Configuration section does not affect anything except the display of that feature in the HTML interface. Settings made while an advanced feature was displayed remain in effect when that

advanced feature is no longer displayed. Further, the interface displays any advanced feature that has non-default settings, even if you have configured that advanced feature to be hidden. If you later disable the feature or delete its settings, Cisco Secure 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 deselected on the Advanced Options page.

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

Cisco Secure ACS alters the contents of various sections of the HTML interface according to the selections you have made.

Protocol Configuration Options for TACACS+

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

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



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 enable you 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**—In this area is 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 either the User Setup page or Group Setup page.
- **New Services**—In this area you can enter any services or protocols particular to your network configuration.

**Note**

If you have configured Cisco Secure ACS to interact with device management applications for other Cisco products, such as Management Center for Firewalls, Cisco Secure ACS may display new TACACS+ services as dictated by these device management applications. To ensure the proper functioning of Cisco Secure ACS, of device management applications with which Cisco Secure 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 you can choose to hide or display are as follows:

- **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 selected, a grid appears on the User Setup page that enables you 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 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. This provides a common method 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 this option is selected, an area appears on the User Setup and Group Setup pages that enables you to enter custom TACACS+ attributes.

Cisco Secure ACS can also display a custom command field for each service. This text field enables you 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 selected, an area appears on the User Setup and Group Setup pages that enables you to permit unknown TACACS+ services, such as Cisco Discovery Protocol (CDP).

**Note**

This option should be used by advanced system administrators only.

**Note**

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

Setting Options for TACACS+

This procedure enables you 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, follow these steps:

**Note**

The Cisco Secure ACS HTML interface displays any protocol option that is enabled or has non-default 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, Cisco Secure ACS hides the protocol option. This behavior prevents Cisco Secure ACS from hiding active settings.

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

The TACACS+ (Cisco) page appears.

Step 2 In the TACACS+ Services table, select the check box for each TACACS+ service you want displayed on the applicable setup page.

Step 3 To add new services and protocols, follow these steps:

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

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

Step 4 In the Advanced Configurations Options section, select the check boxes of the display options 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 Cisco Secure ACS displays in other sections of the HTML 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, this section allows you to customize the attributes that are displayed. 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 types of RADIUS protocol configuration settings choices. The Interface Configuration page displays RADIUS 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 on page 3-12](#).

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 Aironet)	RADIUS (BBSM)	RADIUS (Cisco IOS/PIX)	RADIUS (Micro-soft)	RADIUS (Ascend)	RADIUS (Cisco VPN 3000)	RADIUS (Cisco VPN 5000)	RADIUS (Juniper)	RADIUS (Nortel)
RADIUS (IETF)	Yes	No	No	No	No	No	No	No	No	No
RADIUS (Cisco Aironet)	Yes	Yes	No	Yes	No	No	No	No	No	No
RADIUS (BBSM)	Yes	No	Yes	No	No	No	No	No	No	No
RADIUS (Cisco IOS/PIX)	Yes	No	No	Yes	Yes	Yes	No	No	No	No

Table 3-1 RADIUS Listings in Interface (continued)

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

**Tip**

You must have your network devices configured 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 HTML 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

selecting 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 follow:

- **(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 Cisco Secure 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 3-16](#).

- **RADIUS (Cisco IOS/PIX) Settings**—This section allows you to enable the specific attributes for RADIUS (Cisco IOS/PIX). Selecting the first attribute listed under RADIUS (Cisco IOS/PIX), 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 3-17](#).
- **RADIUS (Cisco Aironet) Settings**—This section allows you to enable the specific attribute for RADIUS (Cisco Aironet). The single Cisco Aironet RADIUS VSA, Cisco-Aironet-Session-Timeout, is a specialized implementation of the IETF RADIUS Session-Timeout attribute (27). When Cisco Secure ACS responds to an authentication request from a Cisco Aironet Access Point and the Cisco-Aironet-Session-Timeout attribute is configured, Cisco Secure ACS sends to the wireless device this value in the IETF

Session-Timeout attribute. This enables you to provide different session timeout values for wireless and wired end-user clients. For detailed steps, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17](#).

- **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) device. For detailed procedures, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17](#).
- **RADIUS (Cisco VPN 3000) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Cisco VPN 3000). For detailed procedures, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17](#).
- **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 3-17](#).
- **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), or a RADIUS (Cisco IOS/PIX) device. For detailed procedures, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17](#).
- **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 3-17](#).
- **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 3-17](#).
- **RADIUS (BBSM) Settings**—From this section you enable the RADIUS VSAs for RADIUS “Building Broadband Service Manger” (BBSM). For detailed procedures, see [Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17](#).

While Cisco Secure ACS ships with these listed VSAs prepackaged, it also enables you to define and configure custom attributes for any VSA set not already contained in Cisco Secure 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 9-28](#).

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 Cisco Secure ACS HTML 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

Each selected IETF RADIUS attribute must be supported by all your network devices using RADIUS.

To set protocol configuration options for IETF RADIUS attributes, follow these steps:

- 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, select the corresponding check box.



Note

Each attribute selected must be supported by your RADIUS network devices.

- 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** at the bottom of the page.

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

Setting Protocol Configuration Options for Non-IETF RADIUS Attributes

This procedure enables you to hide or display various RADIUS VSAs for configuration from the User Setup and Group Setup portions of the Cisco Secure ACS HTML interface.

To set protocol configuration options for a set of RADIUS VSAs, follow these steps:

Step 1 Click **Interface Configuration**.

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

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 selected, a User check box appears alongside the Group check box for each attribute.

Step 3 For each RADIUS VSA that you want to appear as a configurable option on the User Setup or Group Setup page, select the corresponding check box.



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

Step 4 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.
