



Network Configuration

This chapter details concepts and procedures for configuring Cisco Secure ACS Solution Engine to interact with AAA clients, AAA servers, and remote agents, and for establishing a distributed system.

This chapter contains the following topics:

- [About Network Configuration, page 4-2](#)
- [About Distributed Systems, page 4-3](#)
- [Proxy in Distributed Systems, page 4-4](#)
- [Network Device Searches, page 4-8](#)
- [AAA Client Configuration, page 4-11](#)
- [AAA Server Configuration, page 4-22](#)
- [Remote Agent Configuration, page 4-29](#)
- [Network Device Group Configuration, page 4-36](#)
- [Proxy Distribution Table Configuration, page 4-41](#)

About Network Configuration

The appearance of the page you see when you click Network Configuration differs according to the network configuration selections you made in the Interface Configuration section. The five tables that may appear in this section are as follows:

- **AAA Clients**—This table lists each AAA client that is configured on the network, together with its IP address and associated protocol.

If you are using network device groups (NDGs), this table does not appear on the initial page, but is accessed through the Network Device Group table. For more information about this interface configuration, see [Advanced Options, page 3-4](#).
- **AAA Servers**—This table lists each AAA server that is configured on the network together with its IP address and associated type.

If you are using NDGs, this table does not appear on the initial page, but is accessed through the Network Device Groups table. For more information about this interface configuration, see [Advanced Options, page 3-4](#).
- **Remote Agents**—This table lists each remote agent that is configured together with its IP address and available services. For more information about remote agents, see [About Remote Agents, page 4-29](#).

This table does not appear unless you have enabled the Distributed System Settings feature in Interface Configuration.

If you are using NDGs, this table does not appear on the initial page, but is accessed through the Network Device Groups table. For more information about this interface configuration, see [Advanced Options, page 3-4](#).
- **Network Device Groups**—This table lists the name of each NDG that has been configured, and the number of AAA clients and AAA servers assigned to each NDG. If you are using NDGs, the AAA Clients table and AAA Servers table do not appear on the opening page. To configure a AAA client or AAA server, you must click the name of the NDG to which the device is assigned. If the newly configured device is not assigned to an NDG, it automatically belongs to the (Not Assigned) group.

This table appears only when you have configured the interface to use NDGs. For more information about this interface configuration, see [Advanced Options, page 3-4](#).

- **Proxy Distribution Table**—You can use the Proxy Distribution Table to configure proxy capabilities including “domain” stripping. For more information, see [Proxy Distribution Table Configuration, page 4-41](#).

This table appears only when you have configured the interface to enable Distributed Systems Settings. For more information about this interface configuration, see [Advanced Options, page 3-4](#).

About Distributed Systems

Cisco Secure ACS can be used in a distributed system; that is, multiple Cisco Secure ACSes and authentication, authorization, and accounting (AAA) servers can be configured to communicate with one another as primary, backup, client, or peer systems. This enables you to use powerful features such as the following:

- Proxy
- Fallback on failed connection
- CiscoSecure database replication
- Remote and centralized logging

AAA Servers in Distributed Systems

“AAA server” is the generic term for an access control server (ACS), and the two terms are often used interchangeably. AAA servers are used to determine who can access the network and what services are authorized for each user. The AAA server stores a profile containing authentication and authorization information for each user. Authentication information validates user identity, and authorization information determines what network services a user is permitted to use. A single AAA server can provide concurrent AAA services to many dial-up access servers, routers, and firewalls. Each network device can be configured to communicate with a AAA server. This makes it possible to centrally control dial-up access, and to secure network devices from unauthorized access.

These types of access control have unique authentication and authorization requirements. With Cisco Secure ACS, system administrators can use a variety of authentication methods that are used with different degrees of authorization privileges.

Completing the AAA functionality, Cisco Secure ACS serves as a central repository for accounting information. Each user session granted by Cisco Secure ACS can be fully accounted for, and its accounting information can be stored in the server. This accounting information can be used for billing, capacity planning, and security audits.

**Note**

If the fields mentioned in this section do not appear in the Cisco Secure ACS HTML interface, enable them by clicking Interface Configuration, clicking Advanced Options, and then selecting the Distributed System Settings check box.

Default Distributed System Settings

You use both the AAA Servers table and the Proxy Distribution Table to establish distributed system settings. The parameters configured within these tables create the foundation to enable multiple Cisco Secure ACSes to be configured to work with one another. Each table contains a Cisco Secure ACS entry for itself. In the AAA Servers table, the only AAA server initially listed is itself; the Proxy Distribution Table lists an initial entry of (Default), which displays how the local Cisco Secure ACS is configured to handle each authentication request locally.

You can configure additional AAA servers in the AAA Servers table. This enables these devices to become available in the HTML interface so that they can be configured for other distributed features such as proxy, CiscoSecure user database replication, remote logging, and RDBMS synchronization. For information about configuring additional AAA servers, see [Adding a AAA Server, page 4-25](#).

Proxy in Distributed Systems

Proxy is a powerful feature that enables you to use Cisco Secure ACS for authentication in a network that uses more than one AAA server. Using proxy, Cisco Secure ACS automatically forwards an authentication request from a AAA client to another AAA server. After the request has been successfully authenticated, the authorization privileges that have been configured for the user on the remote AAA server are passed back to the original Cisco Secure ACS, where the AAA client applies the user profile information for that session.

Proxy provides a useful service to users, such as business travelers, who dial in to a network device other than the one they normally use and would otherwise be authenticated by a “foreign” AAA server. To use proxy, you must first click **Interface Configuration**, click **Advanced Options**, and then select the **Distributed System Settings** check box.

Whether, and where, an authentication request is to be forwarded is defined in the Proxy Distribution Table on the Network Configuration page. You can use multiple Cisco Secure ACSes throughout your network. For information about configuring the Proxy Distribution Table, see [Proxy Distribution Table Configuration, page 4-41](#).

Cisco Secure ACS employs character strings defined by the administrator to determine whether an authentication request should be processed locally or forwarded, and to where. When an end user dials in to the network device and Cisco Secure ACS finds a match for the character string defined in the Proxy Distribution Table, Cisco Secure ACS forwards the authentication request to the associated remote AAA server.

**Note**

When a Cisco Secure ACS receives a TACACS+ authentication request forwarded by proxy, any Network Access Restrictions for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

**Note**

When a Cisco Secure ACS proxies to a second Cisco Secure ACS, the second Cisco Secure ACS responds to the first using only IETF attributes, no VSAs, when it recognizes the first Cisco Secure ACS as a AAA server. Alternatively, you can configure an Cisco Secure ACS to be seen as a AAA client by the second Cisco Secure ACS; in this case, the second Cisco Secure ACS responses include the RADIUS VSAs for whatever RADIUS vendor is specified in the AAA client definition table entry—in the same manner as any other AAA client.

For example, a Cisco Secure ACS receives an authentication request for mary.smith@corporate.com, where “@corporate.com” is a character string defined in the server distribution table as being associated with another specific AAA server. The Cisco Secure ACS receiving the authentication request for mary.smith@corporate.com then forwards the request to the AAA server with which that character string is associated. The entry in the Proxy Distribution Table defines the association.

Administrators with geographically dispersed networks can configure and manage the user profiles of employees within their immediate location or building. This enables the administrator to manage the policies of just their users and allows all authentication requests from other users within the company to be forwarded to their respective AAA server for authentication. Not every user profile needs to reside on every AAA server. This saves administration time and server space, and facilitates end users receiving the same privileges regardless of which access device they connect through.

Fallback on Failed Connection

You can configure the order in which Cisco Secure ACS checks remote AAA servers when a failure of the network connection to the primary AAA server has occurred. If an authentication request cannot be sent to the first listed server, because of a network failure for example, the next listed server is checked. This continues, in order, down the list until a AAA server handles the authentication request. (Failed connections are detected by failure of the nominated server to respond within a specified time period. That is, the request is timed out.) If Cisco Secure ACS cannot connect to any server in the list, authentication fails.

Character String

Cisco Secure ACS forwards authentication requests using a configurable set of characters with a delimiter, such as dots (.), slashes (/), or hyphens (-). When configuring the Cisco Secure ACS character string to match, you must specify whether the character string is the prefix or suffix. For example, you can use “domain.us” as a suffix character string in `username*domain.us`, where * represents any delimiter. An example of a prefix character string is `domain.*username`, where the * would be used to detect the “/” character.

Stripping

Stripping allows Cisco Secure ACS to remove, or strip, the matched character string from the username. When you enable stripping, Cisco Secure ACS examines each authentication request for matching information. When Cisco Secure ACS finds a match by character string in the Proxy Distribution Table, as described in the example under [Proxy in Distributed Systems, page 4-4](#), Cisco Secure ACS strips off the character string if you have configured it to do so.

For example, in the proxy example that follows, the character string that accompanies the username establishes the ability to forward the request to another AAA server. If the user must enter the user ID of `mary@corporate.com` to be forwarded correctly to the AAA server for authentication, Cisco Secure ACS might find a match on the “@corporate.com” character string, and strip the “@corporate.com”, leaving a username of “mary”, which may be the username format that the destination AAA server requires to identify the correct entry in its database.

Proxy in an Enterprise

This section presents a scenario of proxy used in an enterprise system. Mary is an employee with an office in the corporate headquarters in Los Angeles. Her username is `mary@la.corporate.com`. When Mary needs access to the network, she accesses the network locally and authenticates her username and password. Because Mary works in the Los Angeles office, her user profile, which defines her authentication and authorization privileges, resides on the local Los Angeles AAA server. However, Mary occasionally travels to a division within the corporation in New York, where she still needs to access the corporate network to get her e-mail and other files. When Mary is in New York, she dials in to the New York office and logs in as `mary@la.corporate.com`. Her username is not recognized by the New York Cisco Secure ACS, but the Proxy Distribution Table contains an entry, “@la.corporate.com”, to forward the authentication request to the Los Angeles Cisco Secure ACS. Because the username and password information for Mary reside on that AAA server, when she authenticates correctly, the authorization parameters assigned to her are applied by the AAA client in the New York office.

Remote Use of Accounting Packets

When proxy is employed, Cisco Secure ACS can dispatch AAA accounting packets in one of three ways:

- Log them locally.
- Forward them to the destination AAA server.
- Log them locally and forward copies to the destination AAA server.

Sending accounting packets to the remote Cisco Secure ACS offers several benefits. When Cisco Secure ACS is configured to send accounting packets to the remote AAA server, the remote AAA server logs an entry in the accounting report for that session on the destination server. Cisco Secure ACS also caches the user connection information and adds an entry in the List Logged on Users report. You can then view the information for users that are currently connected. Because the accounting information is being sent to the remote AAA server, even if the connection fails, you can view the Failed Attempts report to troubleshoot the failed connection.

Sending the accounting information to the remote AAA server also enables you to use the Max Sessions feature. The Max Sessions feature uses the Start and Stop records in the accounting packet. If the remote AAA server is a Cisco Secure ACS and the Max Sessions feature is implemented, you can track the number of sessions allowed for each user or group.

You can also choose to have Voice-over-IP (VoIP) accounting information logged remotely, either appended to the RADIUS Accounting log, in a separate VoIP Accounting log, or both.

Other Features Enabled by System Distribution

Beyond basic proxy and fallback features, configuring a Cisco Secure ACS to interact with distributed systems enables several other features that are beyond the scope of this chapter. These features include the following:

- **Replication**—For more information, see [CiscoSecure Database Replication, page 9-1](#).
- **RDBMS synchronization**—For more information, see [RDBMS Synchronization, page 9-25](#).
- **Remote and centralized logging**—For more information, see [Remote Logging, page 11-17](#).

Network Device Searches

You can search for any network device configured in the Network Configuration section of the Cisco Secure ACS HTML interface.

This section contains the following topics:

- [Network Device Search Criteria, page 4-9](#)
- [Searching for Network Devices, page 4-10](#)

Network Device Search Criteria

You can specify search criteria for network device searches. Cisco Secure ACS provides the following search criteria:

- **Name**—The name assigned to the network device in Cisco Secure ACS. You can use asterisks (*) as wildcard characters. For example, if you wanted to find all devices with names starting with the letter M, you would enter “M*” or “m*”. Name-based searches are case-insensitive. If you do not want to search based on device name, you can leave the Name box blank or you can put only an asterisk in the Name box.
- **IP Address**—The IP address specified for the network device in Cisco Secure ACS. For each octet in the address, you have three options, as follows:
 - **Number**—You can specify a number, such as 10.3.157.98.
 - **Numeric Range**—You can specify the low and high numbers of the range in the octet, separated by a hyphen, such as 10.3.157.10-50.
 - **Wildcard**—You can use an asterisk (*) to match all numbers in that octet, such as 10.3.157.*.

Cisco Secure ACS allows multiple octets in the IP Address box to be either a number, a numeric range, or an asterisk, such as 172.16-31.*.*.

- **Type**—The device type, as specified by the AAA protocol it is configured to use or the kind of AAA server it is. You can also specify that you want to search for remote agents. If you do not want to limit the search based on device type, select “Any” from the Type list.
- **Device Group**—The NDG the device is assigned to. This search criterion only appears if you have enabled Network Device Groups on the Advanced Options page in the Interface Configuration Section. If you do not want to limit the search based on NDG membership, select “Any” from the Device Group list.

Searching for Network Devices

To search for a network device, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Click **Search**.

The Search for Network Devices page appears. In the configuration area, the controls for setting search criteria appear above the search results for the most recent search previously conducted for this session, if any.



Tip When you leave the Search for Network Devices page, Cisco Secure ACS retains your search criteria and results for the duration of the current administrative session. Until you log out of Cisco Secure ACS, you can return to the Search for Network Devices page to view your most recent search criteria and results.

Step 3 Set the criteria for a device search. For information about search criteria, see [Network Device Search Criteria, page 4-9](#).



Tip To reset the search criteria to default settings, click **Clear**.

Step 4 Click **Search**.

A table lists each network device configured in Cisco Secure ACS that matches the search criteria you specified. If Cisco Secure ACS did not find a matching network device, the message “No Search Results” appears.

The table listing matching network devices includes the device name, IP address, and type. If you have enabled Network Device Groups on the Advanced Options page in the Interface Configuration Section, the table also includes the NDG of each matching network device.

**Tip**

You can sort the table rows by whichever column you like, in either ascending or descending order. Click a column title once to sort the rows by the entries in that column in ascending order. Click the column a second time to sort the rows by the entries in that column in descending order.

Step 5 If you want to view the configuration settings for a network device found by the search, click the network device name in the Name column of the table of matching network devices.

Cisco Secure ACS displays the applicable setup page. For information about the AAA Client Setup page, see [AAA Client Configuration Options, page 4-12](#). For information about the AAA Server Setup page, see [AAA Server Configuration Options, page 4-23](#).

Step 6 If you want to download a file containing the search results in a comma-separated value format, click **Download** and use your browser to save the file to a location and filename of your choice.

Step 7 If you want to search again using different criteria, repeat Step 3 and Step 4.

AAA Client Configuration

In this guide we use the term “AAA client” comprehensively to signify the device through which or to which service access is being attempted. This is the RADIUS or TACACS+ client device, and may comprise network access servers (NASes), PIX Firewalls, routers, or any other RADIUS or TACACS+ hardware/software client.

This section contains the following topics:

- [AAA Client Configuration Options, page 4-12](#)
- [Adding a AAA Client, page 4-17](#)
- [Editing a AAA Client, page 4-20](#)
- [Deleting a AAA Client, page 4-21](#)

AAA Client Configuration Options

A AAA client configuration enables Cisco Secure ACS to interact with the network devices the configuration represents. A network device that does not have a corresponding configuration in Cisco Secure ACS, or whose configuration in Cisco Secure ACS is incorrect, does not receive AAA services from Cisco Secure ACS.

The Add AAA Client and AAA Client Setup pages include the following options:

- **AAA Client Hostname**—The name you assign to the AAA client configuration. Each AAA client configuration can represent multiple network devices; thus, the AAA client hostname configured in Cisco Secure ACS is not required to match the hostname configured on a network device. We recommend that you adopt a descriptive, consistent naming convention for AAA client hostnames. Maximum length for a AAA client hostname is 32 characters.

**Note**

After you submit the AAA client hostname, you cannot change it. If you want to use a different name for a AAA client, delete the AAA client configuration and create a AAA client configuration using the new name.

- **AAA Client IP Address**—At a minimum, a single IP address of a AAA client or the keyword “dynamic”.

If you only use the keyword “dynamic”, with no IP addresses, the AAA client configuration can only be used for command authorization for Cisco multi-device management applications, such as Management Center for Firewalls. Cisco Secure ACS only provides AAA services to devices based on IP address, so it ignores such requests from a device whose AAA client configuration only has the keyword “dynamic” in the Client IP Address box.

If you want a AAA client configuration in Cisco Secure ACS to represent multiple network devices, you can specify multiple IP addresses. Separate each IP address by pressing Enter.

In each IP address you specify, you have three options for each octet in the address, as follows:

- **Number**—You can specify a number, for example, 10.3.157.98.
- **Numeric Range**—You can specify the low and high numbers of the range in the octet, separated by a hyphen, for example, 10.3.157.10-50.
- **Wildcard**—You can use an asterisk (*) to match all numbers in that octet, for example, 10.3.157.*.

Cisco Secure ACS allows any octet or octets in the IP Address box to be a number, a numeric range, or an asterisk, for example 172.16-31.*.*.

- **Key**—The shared secret of the AAA client. Maximum length for a AAA client key is 32 characters.

For correct operation, the key must be identical on the AAA client and Cisco Secure ACS. Keys are case sensitive. Because shared secrets are not synchronized, it is easy to make mistakes when entering them on network devices and Cisco Secure ACS. If the shared secret does not match, Cisco Secure ACS discards all packets from the network device.



Note If the AAA client represents multiple network devices, the key must be identical on all network devices represented by the AAA client.

- **Network Device Group**—The name of the NDG to which this AAA client should belong. To make the AAA client independent of NDGs, use the Not Assigned selection.



Note This option does not appear if you have not configured Cisco Secure ACS to use NDGs. To enable NDGs, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

- **Authenticate Using**—The AAA protocol to be used for communications with the AAA client. The Authenticate Using list includes Cisco IOS TACACS+ and several vendor-specific implementations of RADIUS. If you have configured user-defined RADIUS vendors and VSAs, those vendor-specific RADIUS implementations appear on the list also. For information about creating user-defined RADIUS VSAs, see [Custom RADIUS Vendors and VSAs, page 9-28](#).

The Authenticate Using list always contains the following selections:

- **TACACS+ (Cisco IOS)**—The Cisco IOS TACACS+ protocol, which is the standard choice when using Cisco Systems access servers, routers, and firewalls. If the AAA client is a Cisco device-management application, such as Management Center for Firewalls, you must use this option.
- **RADIUS (Cisco Aironet)**—RADIUS using Cisco Aironet VSAs. Select this option if the network device is a Cisco Aironet Access Point used by users authenticating with LEAP or EAP-TLS, provided that these protocols are enabled on the Global Authentication Setup page in the System Configuration section.

When an authentication request from a RADIUS (Cisco Aironet) AAA client arrives, Cisco Secure ACS first attempts authentication by using LEAP; if this fails, Cisco Secure ACS fails over to EAP-TLS. If LEAP is not enabled on the Global Authentication Setup page, Cisco Secure ACS immediately attempts EAP-TLS authentication. If neither LEAP nor EAP-TLS are enabled on the Global Authentication Setup, any authentication attempt received from a Cisco Aironet RADIUS client fail. For more information about enabling LEAP or EAP-TLS, see [Global Authentication Setup, page 10-26](#).

Using this option enables Cisco Secure ACS to send the wireless network device a different session timeout value for user sessions than Cisco Secure ACS sends to wired end-user clients.



Note If all authentication requests from a particular Cisco Aironet Access Point are PEAP or EAP-TLS requests, use RADIUS (IETF) instead of RADIUS (Cisco Aironet). Cisco Secure ACS cannot support PEAP authentication using the RADIUS (Cisco Aironet) protocol.

- **RADIUS (Cisco BBMS)**—RADIUS using Cisco BBMS VSAs. Select this option if the network device is a Cisco BBMS network device supporting authentication via RADIUS.

- **RADIUS (Cisco IOS/PIX)**—RADIUS using Cisco IOS/PIX VSAs. This option enables you to pack commands sent to a Cisco IOS AAA client. The commands are defined in the Group Setup section. Select this option for RADIUS environments in which key TACACS+ functions are required to support Cisco IOS equipment.
- **RADIUS (Cisco VPN 3000)**—RADIUS using Cisco VPN 3000 VSAs. Select this option if the network device is a Cisco VPN 3000 series Concentrator.
- **RADIUS (Cisco VPN 5000)**—RADIUS using Cisco VPN 5000 VSAs. Select this option if the network device is a Cisco VPN 5000 series Concentrator.
- **RADIUS (IETF)**—IETF-standard RADIUS, using no VSAs. Select this option if the AAA client represents RADIUS-enabled devices from more than one manufacturer and you want to use standard IETF RADIUS attributes. If the AAA client represents a Cisco Aironet Access Point used only by users authenticating with PEAP or EAP-TLS, this is also the protocol to select.
- **RADIUS (Ascend)**—RADIUS using Ascend RADIUS VSAs. Select this option if the network device is an Ascend network device supporting authentication via RADIUS.
- **RADIUS (Juniper)**—RADIUS using Juniper RADIUS VSAs. Select this option if the network device is a Juniper network device supporting authentication via RADIUS.
- **RADIUS (Nortel)**—RADIUS using Nortel RADIUS VSAs. Select this option if the network device is a Nortel network device supporting authentication via RADIUS.
- **RADIUS (iPass)**—RADIUS for AAA clients using iPass RADIUS. Select this option if the network device is an iPass network device supporting authentication via RADIUS. iPass RADIUS is identical to IETF RADIUS.
- **Single Connect TACACS+ AAA Client (Record stop in accounting on failure)**—If you select TACACS+ (Cisco IOS) from the Authenticate Using list, you can use this option to specify that Cisco Secure ACS use a single TCP connection for all TACACS+ communication with the AAA client, rather than a new one for every TACACS+ request. In single connection mode, multiple requests from a network device are multiplexed over a single TCP session. By default, this check box is not selected.



Note If TCP connections between Cisco Secure ACS and the AAA client are unreliable, do not use this feature.

- **Log Update/Watchdog Packets from this AAA Client**—Enables logging of update, or watchdog, packets. Watchdog packets are interim packets sent periodically during a session. They provide you with an approximate session length if a AAA client fails and, therefore, no stop packet is received to mark the end of the session. By default, this check box is not selected.
- **Log RADIUS Tunneling Packets from this AAA Client**—Enables logging of RADIUS tunneling accounting packets. Packets are recorded in the RADIUS Accounting reports of Reports and Activity. By default, this check box is not selected.
- **Replace RADIUS Port info with Username from this AAA Client**—Enables use of username rather than port number for session state tracking. This option is useful when the AAA client cannot provide unique port values, such as a gateway GPRS support node (GGSN). For example, if you use the Cisco Secure ACS IP pools server and the AAA client does not provide unique port for each user, Cisco Secure ACS assumes that a reused port number indicates that the previous user session has ended and Cisco Secure ACS may reassign the IP address previously assigned to the session with the non-unique port number. By default, this check box is not selected.



Note If this option is enabled, Cisco Secure ACS cannot determine the number of user sessions for each user. Each session uses the same session identifier, the username; therefore, the Max Sessions feature is ineffective for users accessing the network through a AAA client with this feature enabled.

Adding a AAA Client

You can use this procedure to add a AAA client configuration.

Before You Begin

For descriptions of the options available while adding a AAA client configuration, see [AAA Client Configuration Options, page 4-12](#).

For Cisco Secure ACS to provide AAA services to a AAA client, you must ensure that gateway devices between AAA clients and Cisco Secure ACS allow communication over the ports needed to support the applicable AAA protocol (RADIUS or TACACS+). For information about ports used by AAA protocols, see [AAA Protocols—TACACS+ and RADIUS, page 1-6](#).

To add a AAA client, follow these steps:

-
- Step 1** In the navigation bar, click **Network Configuration**.
- The Network Configuration page opens.
- Step 2** Do one of the following:
- If you are using NDGs, click the name of the NDG to which the AAA client is to be assigned. Then, click **Add Entry** below the AAA Clients table.
 - To add a AAA client when you have not enabled NDGs, click **Add Entry** below the AAA Clients table.
- The Add AAA Client page appears.
- Step 3** In the AAA Client Hostname box, type the name assigned to this AAA client (up to 32 characters).
- Step 4** In the AAA Client IP Address box, do one of the following:
- Type the AAA client IP address or addresses. For information about using wildcards, octet ranges, or multiple IP address, see [AAA Client Configuration Options, page 4-12](#).
 - If the AAA client configuration will only be used for command authorization of Cisco multi-device management applications, type **dynamic**.



Note If you only provide the keyword “dynamic”, the AAA client configuration cannot be used by Cisco Secure ACS to provide AAA services to a network device and is used solely for command authorization of Cisco multi-device management applications, such as Management Center for Firewalls.

Step 5 In the Key box, type the shared secret that the AAA client and Cisco Secure ACS use to encrypt the data (up to 32 characters).



Note For correct operation, the identical key must be configured on the AAA client and Cisco Secure ACS. Keys are case sensitive.

Step 6 If you are using NDGs, from the Network Device Group list, select the name of the NDG to which this AAA client should belong, or select **Not Assigned** to set this AAA client to be independent of NDGs.



Note If you want to enable NDGs, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

Step 7 From the Authenticate Using list, select the network security protocol used by the AAA client.



Tip If you are uncertain which protocol to select on the Authenticate Using list, see [AAA Client Configuration Options, page 4-12](#).

Step 8 If you want to enable a single connection from a AAA client, rather than a new one for every TACACS+ request, select the **Single Connect TACACS+ AAA Client (Record stop in accounting on failure)** check box.



Note If TCP connections between Cisco Secure ACS and the AAA client are unreliable, do not use this feature.

- Step 9** If you want to enable logging of watchdog packets, select the **Log Update/Watchdog Packets from this AAA Client** check box.
- Step 10** If you want to enable logging of RADIUS tunneling accounting packets, select the **Log RADIUS tunneling Packets from this AAA Client** check box.
- Step 11** If you want to track session state by username rather than port number, select the **Replace RADIUS Port info with Username from this AAA** check box.



Note If this option is enabled, Cisco Secure ACS cannot determine the number of user sessions for each user. Each session uses the same session identifier, the username; therefore, the Max Sessions feature is ineffective for users accessing the network through a AAA client with this feature enabled.

- Step 12** If you want to save your changes and apply them immediately, click **Submit + Restart**.



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



Tip If you want to save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.

Editing a AAA Client

You can use this procedure to edit the settings for a AAA client configuration.

**Note**

You cannot directly edit the name of a AAA client; rather, you must delete the AAA client entry and then re-establish the entry with the corrected name. For steps about deleting a AAA client configuration, see [Deleting a AAA Client, page 4-21](#). For steps about creating a AAA client configuration, see [Adding a AAA Client, page 4-17](#).

Before You Begin

For descriptions of the options available while editing a AAA client configuration, see [AAA Client Configuration Options, page 4-12](#).

For Cisco Secure ACS to provide AAA services to a AAA client, you must ensure that gateway devices between AAA clients and Cisco Secure ACS permit communication over the ports needed to support the applicable AAA protocol (RADIUS or TACACS+). For information about ports used by AAA protocols, see [AAA Protocols—TACACS+ and RADIUS, page 1-6](#).

To edit a AAA client, follow these steps:

-
- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration page opens.
- Step 2** Do one of the following:
- If you are using NDGs, click the name of the NDG to which the AAA client is assigned. Then, click the name of the AAA client.
 - To edit a AAA client when you have not enabled NDGs, click the name of the AAA client in the AAA Client Hostname column of the AAA Clients table.
- The AAA Client Setup For *Name* page appears.
- Step 3** Modify the AAA client settings, as needed. For information about the configuration options available for a AAA client, see [AAA Client Configuration Options, page 4-12](#).



Note You cannot directly edit the name of a AAA client; rather, you must delete the AAA client entry and then re-establish the entry with the corrected name. For steps about deleting a AAA client entry, see [Deleting a AAA Client, page 4-21](#). For steps about creating a AAA client entry, see [Adding a AAA Client, page 4-17](#).

Step 4 To save your changes and apply them immediately, click **Submit + Restart**.



Tip To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.



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

Deleting a AAA Client

To delete a AAA client, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA client is assigned. Then, click the AAA client hostname in the AAA Clients table.
- To delete a AAA client when you have not enabled NDGs, click the AAA client hostname in the AAA Clients table.

The AAA Client Setup for the *Name* page appears.

Step 3 To delete the AAA client and have the deletion take effect immediately, click **Delete + Restart**.



Note Restarting Cisco Secure ACS services clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. As an alternative to restarting when you delete a AAA client, you can click **Delete**. However, when you do this, the change does not take effect until you restart the system, which you can do by clicking **System Configuration**, clicking **Service Control**, and then clicking **Restart**.

A confirmation dialog box appears.

Step 4 Click **OK**.

Cisco Secure ACS restarts AAA services and the AAA client is deleted.

AAA Server Configuration

This section presents procedures for configuring AAA servers in the Cisco Secure ACS HTML interface. For additional information about AAA servers, see [AAA Servers in Distributed Systems, page 4-3](#).

To configure distributed system features for a given Cisco Secure ACS, you must first define the other AAA server(s). For example, all Cisco Secure ACSes involved in replication, remote logging, authentication proxying, and RDBMS synchronization must have AAA server configurations for each other; otherwise, incoming communication from an unknown Cisco Secure ACS is ignored and the distributed system feature will fail.



Tip

If the AAA Servers table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Distributed System Settings** check box.

This section contains the following topics:

- [AAA Server Configuration Options, page 4-23](#)
- [Adding a AAA Server, page 4-25](#)

- [Editing a AAA Server, page 4-27](#)
- [Deleting a AAA Server, page 4-28](#)

AAA Server Configuration Options

A AAA server configuration enables Cisco Secure ACS to interact with the AAA server that the configuration represents. A AAA server that does not have a corresponding configuration in Cisco Secure ACS, or whose configuration in Cisco Secure ACS is incorrect, does not receive AAA services from Cisco Secure ACS, such as proxied authentication requests, database replication communication, remote logging, and RDBMS synchronization. Also, several distributed systems features require that the other Cisco Secure ACSes included in the distributed system be represented in the AAA Servers table. For more information about distributed systems features, see [About Distributed Systems, page 4-3](#).

The Add AAA Server and AAA Server Setup pages include the following options:

- **AAA Server Name**—The name you assign to the AAA server configuration. The AAA server hostname that is configured in Cisco Secure ACS does not have to match the hostname configured on a network device. We recommend that you adopt a descriptive, consistent naming convention for AAA server names. Maximum length for a AAA server name is 32 characters.



Note

After you submit the AAA server name, you cannot change it. If you want to use a different name for a AAA server, delete the AAA server configuration and create a AAA server configuration using the new name.

- **AAA Server IP Address**—The IP address of the AAA server, in dotted, four octet format. For example, 10.77.234.3.
- **Key**—The shared secret of the AAA server. Maximum length for a AAA server key is 32 characters.

For correct operation, the key must be identical on the remote AAA server and Cisco Secure ACS. Keys are case sensitive. Because shared secrets are not synchronized, it is easy to make mistakes when entering them upon remote AAA servers and Cisco Secure ACS. If the shared secret does not match, Cisco Secure ACS discards all packets from the remote AAA server.

- **Network Device Group**—The name of the NDG to which this AAA server should belong. To make the AAA server independent of NDGs, use the Not Assigned selection.



Note This option does not appear if you have not configured Cisco Secure ACS to use NDGs. To enable NDGs, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

- **Log Update/Watchdog Packets from this remote AAA Server**—Enables logging of update, or watchdog, packets from AAA clients that are forwarded by the remote AAA server to this Cisco Secure ACS. Watchdog packets are interim packets sent periodically during a session. They provide you with an approximate session length if a AAA client fails and, therefore, no stop packet is received to mark the end of the session.
- **AAA Server Type**—One of the following three types:
 - **RADIUS**—Select this option if the remote AAA server is configured using any type of RADIUS protocol.
 - **TACACS+**—Select this option if the remote AAA server is configured using the TACACS+ protocol.
 - **Cisco Secure ACS**—Select this option if the remote AAA server is another Cisco Secure ACS. This enables you to configure features that are only available with other Cisco Secure ACSes, such as CiscoSecure user database replication and remote logging.



Note The remote Cisco Secure ACS must be using version 2.1 or later.

- **Traffic Type**—The Traffic Type list defines the direction in which traffic to and from the remote AAA server is permitted to flow from this Cisco Secure ACS. The list includes the following options:
 - **Inbound**—The remote AAA server accepts requests that have been forwarded to it and does not forward the requests to another AAA server. Select this option if you do not want to permit any authentication requests to be forwarded from the remote AAA server.

- **Outbound**—The remote AAA server sends out authentication requests but does not receive them. If a Proxy Distribution Table entry is configured to proxy authentication requests to a AAA server that is configured for Outbound, the authentication request is not sent.
- **Inbound/Outbound**—The remote AAA server forwards and accepts authentication requests. This allows the selected server to handle authentication requests in any manner defined in the distribution tables.

Adding a AAA Server

Before You Begin

For descriptions of the options available while adding a remote AAA server configuration, see [AAA Server Configuration Options, page 4-23](#).

For Cisco Secure ACS to provide AAA services to a remote AAA server, you must ensure that gateway devices between the remote AAA server and Cisco Secure ACS permit communication over the ports that support the applicable AAA protocol (RADIUS or TACACS+). For information about ports used by AAA protocols, see [AAA Protocols—TACACS+ and RADIUS, page 1-6](#).

To add and configure a AAA server, follow these steps:

-
- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration page opens.
- Step 2** Do one of the following:
- If you are using NDGs, click the name of the NDG to which the AAA server is to be assigned. Then, click **Add Entry** below the [name] AAA Servers table.
 - To add a AAA server when you have not enabled NDGs, below the AAA Servers table, click **Add Entry**.
- The Add AAA Server page appears.
- Step 3** In the AAA Server Name box, type a name for the remote AAA server (up to 32 characters).
- Step 4** In the AAA Server IP Address box, type the IP address assigned to the remote AAA server.

- Step 5** In the Key box, type the shared secret that the remote AAA server and the Cisco Secure ACS use to encrypt the data (up to 32 characters).



Note The key is case sensitive. If the shared secret does not match, Cisco Secure ACS discards all packets from the remote AAA server.

- Step 6** From the Network Device Group list, select the NDG to which this AAA server belongs.



Note To enable NDGs, click **Interface Configuration**, click **Advanced Options**, and then click **Network Device Groups**.

- Step 7** To enable watchdog packets, select the **Log Update/Watchdog Packets from this remote AAA Server** check box.

- Step 8** From the AAA Server Type list, select the AAA server type applicable to the remote AAA server. If the remote AAA server is another Cisco Secure ACS, identify it as such by selecting **CiscoSecure ACS**.

- Step 9** From the Traffic Type list, select the type of traffic you want to permit between the remote AAA server and Cisco Secure ACS.

- Step 10** To save your changes and apply them immediately, click **Submit + Restart**.



Tip To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.



Note Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter and resets it to zero.

Editing a AAA Server

Use this procedure to edit the settings for a AAA server that you have previously configured.

**Note**

You cannot edit the name of a AAA server. To rename a AAA server, you must delete the existing AAA server entry and then add a new server entry with the new name.

Before You Begin

For descriptions of the options available while editing a remote AAA server entry, see [AAA Server Configuration Options, page 4-23](#).

For Cisco Secure ACS to provide AAA services to a remote AAA server, you must ensure that gateway devices between the remote AAA server and Cisco Secure ACS permit communication over the ports that support the applicable AAA protocol (RADIUS or TACACS+). For information about ports used by AAA protocols, see [AAA Protocols—TACACS+ and RADIUS, page 1-6](#).

To edit a AAA server, follow these steps:

-
- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration page opens.
- Step 2** Do one of the following:
- If you are using NDGs, click the name of the NDG to which the AAA server is assigned. Then, in the AAA Servers table, click the name of the AAA server to be edited.
 - If you have not enabled NDGs, in the AAA Servers table, click the name of the AAA server to be edited.
- The AAA Server Setup for *X* page appears.
- Step 3** Enter or select new settings for one or more of the following fields:
- AAA Server IP Address
 - Key
 - Log Update/Watchdog Packets from this remote AAA Server
 - AAA Server Type

- Traffic Type

Step 4 To save your changes and apply them immediately, click **Submit + Restart**.

**Tip**

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

**Note**

Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter and resets it to zero.

Deleting a AAA Server

To delete a AAA server, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA server is assigned. Then, click the AAA server name in the AAA Servers table.
- If you have not enabled NDGs, click the AAA server name in the AAA Servers table.

The AAA Server Setup for *X* page appears.

Step 3 To delete the AAA server and have the deletion take effect immediately, click **Delete + Restart**.



Note Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. As an alternative to restarting when you delete a AAA server, in the preceding step you can click **Delete**. However, when you do this, the change does not take effect until you restart the system, which you can do by clicking **System Configuration**, clicking **Service Control**, and then clicking **Restart**.

A confirmation dialog box appears.

Step 4 Click **OK**.

Cisco Secure ACS performs a restart and the AAA server is deleted.

Remote Agent Configuration

This section presents information about remote agents and procedures for configuring remote agents in the Cisco Secure ACS HTML interface.

This section contains the following topics:

- [About Remote Agents, page 4-29](#)
- [Remote Agent Configuration Options, page 4-30](#)
- [Adding a Remote Agent, page 4-32](#)
- [Editing a Remote Agent Configuration, page 4-34](#)
- [Deleting a Remote Agent Configuration, page 4-35](#)

About Remote Agents

Remote agents are small programs that run on computers on your network. A Cisco Secure ACS Solution Engine can use them for remote logging and authentication of users with a Windows external user database. Before you can configure remote logging and before you can configure authentication using a Windows external user database, you must add at least one remote agent configuration to the Remote Agents table in the Network Configuration section.

For more information about remote agents, including how to install and configure them, see *Installation and Configuration Guide for Cisco Secure ACS Remote Agents*.

Remote Agent Configuration Options

A remote agent configuration enables Cisco Secure ACS to interact with the remote agent that the configuration represents. A remote agent that does not have a corresponding configuration in Cisco Secure ACS, or whose configuration in Cisco Secure ACS is incorrect, cannot communicate with Cisco Secure ACS to receive its configuration, logging data, or Windows authentication requests.

The Add Remote Agent and Remote Agent Setup pages include the following options:

- **Remote Agent Name**—The name you assign to the remote agent configuration. Remote agent logging and Windows authentication are configured by referring to remote agents by their name. We recommend that you adopt a descriptive, consistent naming convention for remote agent names. For example, you could assign to remote agent configurations the same name as the hostname of the server that runs the remote agent. Maximum length for a remote agent name is 32 characters.



Note After you submit the remote agent name, you cannot change it. If you want to use a different name for a remote agent, delete the remote agent configuration, create a new remote agent configuration using the new name, and change remote logging and Windows authentication configurations that use the remote agent.

- **Remote Agent IP Address**—The IP address of the remote agent, in dotted, four-octet format. For example, 10.77.234.3.
- **Remote Agent Port**—The TCP port that the remote agent listens to for communication from Cisco Secure ACS. Maximum length for the TCP port number is 6 characters.

If the port number provided here does not match the port the remote agent is configured to listen to, Cisco Secure ACS cannot communicate with the remote agent. For information about configuring the port number that the remote agent listens to, see *Installation and Configuration Guide for Cisco Secure ACS Remote Agents*.

- **Network Device Group**—The name of the NDG to which this remote agent should belong. To make the remote agent independent of NDGs, use the Not Assigned selection.



Note This option does not appear if you have not configured Cisco Secure ACS to use NDGs. To enable NDGs, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

In addition to the options in the preceding list, the Remote Agent Setup page includes the following options:

- **Running Status**—Information about the status of the remote agent. If Cisco Secure ACS can contact the remote agent, the uptime for the remote agent is displayed. If Cisco Secure ACS cannot contact the remote agent, the message “Not responding” is displayed.
- **Configuration Provider**—The Cisco Secure ACS that the remote agent receives its configuration from.



Tip

You can access the HTML interface for the Cisco Secure ACS that provides a remote agent its configuration by clicking on the Cisco Secure ACS name. A new browser window displays the HTML interface for the Cisco Secure ACS providing configuration data to the remote agent.

- **Service Table**—Below the Configuration Provider, Cisco Secure ACS displays a table of information about the remote agent. The table includes the following columns:
 - **Service**—A list of services that a remote agent can provide: remote logging and Windows authentication.

- **Available**—Whether the remote agent can currently provide the corresponding service.
- **Used by this ACS**—Whether the corresponding service is currently used by the Cisco Secure ACS you are logged into.

Adding a Remote Agent

Before You Begin

For descriptions of the options available while adding a remote agent configuration, see [Remote Agent Configuration Options, page 4-30](#).

For Cisco Secure ACS to communicate with a remote agent, you must ensure that gateway devices between a remote agent and Cisco Secure ACS permit communication over the TCP ports used by remote agents. For information about ports used by remote agents, see *Installation and Configuration Guide for Cisco Secure ACS Remote Agents*.

To add and configure a remote agent, follow these steps:

-
- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration section opens.
- Step 2** Do one of the following:
- If you are using NDGs, click the name of the NDG that you want to assign the remote agent to. Then, in the *NDG Remote Agents* table, click **Add Entry**.
 - If you are not using NDGs, in the Remote Agents table, click **Add Entry**.
The Add Remote Agent page appears.
- Step 3** In the Remote Agent Name box, type a name for the remote agent (up to 32 characters).
- Step 4** In the Remote Agent IP Address box, type the IP address of the computer that runs the remote agent.
- Step 5** In the Port box, type the number of the TCP port the remote agent listens to for communication from Cisco Secure ACS (up to 6 digits). The default TCP port is 2003.



Note If the port number provided here does not match the port the remote agent is configured to listen to, Cisco Secure ACS cannot communicate with the remote agent. For information about configuring the port number that the remote agent listens to, see *Installation and Configuration Guide for Cisco Secure ACS Remote Agents*.

Step 6 From the Network Device Group list, select the NDG to which this remote agent belongs.



Note The Network Device Group list appears only if NDGs are enabled. To enable NDGs, click **Interface Configuration**, click **Advanced Options**, and then click **Network Device Groups**.

Step 7 To save your changes and apply them immediately, click **Submit + Restart**.



Tip To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.



Note Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter and resets it to zero.

Editing a Remote Agent Configuration

Use this procedure to edit the settings for a remote agent that you have previously configured.

**Note**

You cannot edit the name of a remote agent. If you want to use a different name for a remote agent, delete the remote agent configuration, create a remote agent configuration using the new name, and change remote logging and Windows authentication configurations that use the remote agent.

Before You Begin

For descriptions of the options available while editing a remote agent configuration, see [Remote Agent Configuration Options, page 4-30](#).

For Cisco Secure ACS to communicate with a remote agent, you must ensure that gateway devices between a remote agent and Cisco Secure ACS permit communication over the TCP ports used by remote agents. For information about ports used by remote agents, see *Installation and Configuration Guide for Cisco Secure ACS Remote Agents*.

To edit a remote agent configuration, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration section opens.

Step 2 Do one of the following:

- a. If you are using NDGs, click the name of the NDG that the remote agent belongs to. Then, in the *NDG Remote Agents* table, click the name of the remote agent configuration you want to edit.
- b. If you are not using NDGs, in the Remote Agents table, click the name of the remote agent you want to edit.

The Remote Agent Setup for *agent* page appears.

Step 3 Enter or select new settings for one or more of the following options:

- Remote Agent IP Address
- Port
- Network Device Group



Note If the Cisco Secure ACS you are currently logged into does not provide configuration data for the remote agent, none of the options are editable. You can access the HTML interface for the Cisco Secure ACS that does provide configuration data to the remote agent by clicking the Cisco Secure ACS name listed as the Configuration Provider.

Step 4 To save your changes and apply them immediately, click **Submit + Restart**.



Tip To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.



Note Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter and resets it to zero.

Deleting a Remote Agent Configuration



Note You cannot delete a remote agent that Cisco Secure ACS is configured to use for remote logging or Windows authentication.

To delete a remote agent configuration, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration section opens.

Step 2 Do one of the following:

- a. If you are using NDGs, click the name of the NDG that the remote agent belongs to. Then, in the *NDG Remote Agents* table, click the name of the remote agent configuration that you want to delete.

- b. If you are not using NDGs, in the Remote Agents table, click the name of the remote agent configuration that you want to delete.

The Remote Agent Setup for *agent* page appears.

- Step 3** To delete the remote agent and have the deletion take effect immediately, click **Delete + Restart**.



Note Restarting services clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. As an alternative to restarting when you delete a remote agent, in the preceding step you can click **Delete**. However, when you do this, the change does not take effect until you restart services, which you can do by clicking **System Configuration**, clicking **Service Control**, and then clicking **Restart**.

A confirmation dialog box appears.

- Step 4** Click **OK**.

Cisco Secure ACS restarts its services and the remote agent configuration is deleted.

Network Device Group Configuration

Network Device Grouping is an advanced feature that enables you to view and administer a collection of network devices as a single logical group. To simplify administration, you can assign each group a name that can be used to refer to all devices within that group. This creates two levels of network devices within Cisco Secure ACS—single discrete devices such as an individual router or network access server, and an NDG; that is, a collection of routers or AAA servers.



Caution

To see the Network Device Groups table in the HTML interface, you must have the Network Device Groups option selected on the Advanced Options page of the Interface Configuration section. Unlike in other areas of Interface Configuration, it is possible to remove from sight an active NDG if you deselect the Network

Device Groups option. Therefore, if you choose to configure NDGs, make sure you leave the Network Device Groups option selected on the Advanced Option page.

This section contains the following topics:

- [Adding a Network Device Group, page 4-37](#)
- [Assigning an Unassigned AAA Client or AAA Server to an NDG, page 4-38](#)
- [Reassigning a AAA Client or AAA Server to an NDG, page 4-39](#)
- [Renaming a Network Device Group, page 4-39](#)
- [Deleting a Network Device Group, page 4-40](#)

Adding a Network Device Group

You can assign users or groups of users to NDGs. For more information, see one of the following sections:

- [Setting TACACS+ Enable Password Options for a User, page 7-35](#)
- [Setting Enable Privilege Options for a User Group, page 6-19](#)

To add an NDG, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Under the Network Device Groups table, click **Add Entry**.



Tip If the Network Device Groups table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select **Network Device Groups**.

Step 3 In the Network Device Group Name box, type the name of the new NDG.



Tip The maximum name length is 24 characters. Quotation marks (“”) and commas (,) are not allowed. Spaces are allowed.

Step 4 Click **Submit**.

The Network Device Groups table displays the new NDG.

Step 5 To populate the newly established NDG with AAA clients or AAA servers, perform one or more of the following procedures, as applicable:

- [Adding a AAA Client, page 4-17](#)
 - [Adding a AAA Server, page 4-25](#)
 - [Assigning an Unassigned AAA Client or AAA Server to an NDG, page 4-38](#)
 - [Reassigning a AAA Client or AAA Server to an NDG, page 4-39](#)
-

Assigning an Unassigned AAA Client or AAA Server to an NDG

You use this procedure to assign an unassigned AAA client or AAA server to an NDG. Before you begin this procedure, you should have already configured the client or server and it should appear in the Not Assigned AAA Clients or Not Assigned AAA Servers table.

To assign a network device to an NDG, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 In the Network Device Groups table, click **Not Assigned**.



Tip If the Network Device Groups table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

Step 3 Click the name of the network device you want to assign to an NDG.

- Step 4** From the Network Device Groups list, select the NDG to which you want to assign the AAA client or AAA server.
- Step 5** Click **Submit**.
The client or server is assigned to an NDG.
-

Reassigning a AAA Client or AAA Server to an NDG

To reassign a AAA client or AAA server to a new NDG, follow these steps:

- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration page opens.
- Step 2** In the Network Device Groups table, click the name of the current group of the network device.
- Step 3** In either the AAA Clients table or AAA Servers table, as applicable, click the name of the client or server you want to assign to a new NDG.
- Step 4** From the Network Device Group list, select the NDG to which you want to reassign the network device.
- Step 5** Click **Submit**.
The network device is assigned to the NDG you selected.
-


Renaming a Network Device Group



Caution

When renaming an NDG, ensure that there are no NARs or other shared profile components (SPCs) that invoke the original NDG name. Cisco Secure ACS performs no automatic checking to determine whether the original NDG is still invoked. If a user's authentication request incorporates an SPC that invokes a non-existent (or renamed) NDG, the attempt will fail and the user will be rejected.

To rename an NDG, follow these steps:

-
- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration page opens.
- Step 2** In the Network Device Groups table, click the NDG that you want to rename.
-  **Tip** If the Network Device Groups table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.
-
- Step 3** At the bottom of the page, click **Rename**.
The Rename Network Device Group page appears.
- Step 4** In the Network Device Group Name box, type the new name (up to 24 characters).
- Step 5** Click **Submit**.
The name of the NDG is changed.
-

Deleting a Network Device Group

When you delete an NDG, all AAA clients and AAA servers that belong to the deleted group appear in the Not Assigned AAA Clients or Not Assigned AAA Servers table.



Tip

It may be useful to empty an NDG of AAA clients and AAA servers before you delete it. You can do this manually by performing the procedure [Reassigning a AAA Client or AAA Server to an NDG, page 4-39](#), or, in cases where there are a large number of devices to reassign, you can use the RDBMS Synchronization feature.

**Caution**

When deleting an NDG, ensure that there are no NARs or other SPCs that invoke the original NDG. Cisco Secure ACS performs no automatic checking to determine whether the original NDG is still invoked. If a user authentication request incorporates an SPC that invokes a non-existent (or renamed) NDG, the attempt will fail and the user will be rejected.

To delete an NDG, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 In the Network Device Groups table, click the NDG that you want to delete.

**Tip**

If the Network Device Groups table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

Step 3 At the bottom of the page, click **Delete Group**.

A confirmation dialog box appears.

Step 4 Click **OK**.

The NDG is deleted and its name is removed from the Network Device Groups table. Any AAA clients and AAA servers that were in the NDG are now in the Not Assigned AAA Clients or Not Assigned AAA Servers table.

Proxy Distribution Table Configuration

This section describes the Proxy Distribution Table and provides procedures for working with the Proxy Distribution Table.

This section contains the following topics:

- [About the Proxy Distribution Table, page 4-42](#)
- [Adding a New Proxy Distribution Table Entry, page 4-43](#)

- [Sorting the Character String Match Order of Distribution Entries](#), page 4-44
- [Editing a Proxy Distribution Table Entry](#), page 4-45
- [Deleting a Proxy Distribution Table Entry](#), page 4-46

About the Proxy Distribution Table

If you have Distributed Systems Settings enabled, when you click Network Configuration, you will see the Proxy Distribution Table.



Tip

To enable Distributed Systems Settings in the Cisco Secure ACS, click **Interface Configuration**, click **Advanced Options**, and then select the **Distributed System Settings** check box.

The Proxy Distribution Table includes entries that show the character strings on which to proxy, the AAA servers to proxy to, whether to strip the character string, and where to send the accounting information (Local/Remote, Remote, or Local). For more information about the proxy feature, see [Proxy in Distributed Systems](#), page 4-4.

The entries you define and place in the Proxy Distribution Table can be considered turnstiles for each authentication request that Cisco Secure ACS receives from the AAA client. The authentication request is defined in the Proxy Distribution Table according to where it is to be forwarded. If a match to an entry in the Proxy Distribution Table that contains proxy information is found, Cisco Secure ACS forwards the request to the appropriate AAA server.

The Character String column in the Proxy Distribution Table always contains an entry of “(Default)”. The “(Default)” entry matches authentication requests received by the local Cisco Secure ACS that do not match any other defined character strings. While you cannot change the character string definition for the “(Default)” entry, you can change the distribution of authentication requests matching the “(Default)” entry. At installation, the AAA server associated with the “(Default)” entry is the local Cisco Secure ACS. It can sometimes be easier to define strings that match authentication requests to be processed locally rather than defining strings that match authentication requests to be processed remotely. In such a case, associating the “(Default)” entry with a remote AAA server permits you to configure your Proxy Distribution Table with the more easily written entries.

Adding a New Proxy Distribution Table Entry

To create a Proxy Distribution Table entry, follow these steps:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Under the Proxy Distribution Table, click **Add Entry**.



Note If the Proxy Distribution Table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Distributed System Settings** check box.

Step 3 In the Character String box, type the string of characters, including the delimiter to forward on when users dial in to be authenticated. For example, .uk.



Note Angle brackets (< and >) cannot be used.

Step 4 From the Position list, select **Prefix** if the character string you typed appears at the beginning of the username or **Suffix** if the character string appears at the end of the username.

Step 5 From the Strip list, select **Yes** if the character string you entered is to be stripped off the username, or select **No** if it is to be left intact.

Step 6 In the AAA Servers column, select the AAA server you want to use for proxy. Click --> (right arrow button) to move it to the Forward To column.



Tip You can also select additional AAA servers to use for backup proxy if the prior servers fail. To set the order of AAA servers, in the Forward To column, click the name of the applicable server and click **Up** or **Down** to move it into the position you want.



Tip If the AAA server you want to use is not listed, click **Network Configuration**, click **AAA Servers**, click **Add Entry** and complete the applicable information.

- Step 7** From the Send Accounting Information list, select one of the following areas to which to report accounting information:
- **Local**—Keep accounting packets on the local Cisco Secure ACS.
 - **Remote**—Send accounting packets to the remote Cisco Secure ACS.
 - **Local/Remote**—Keep accounting packets on the local Cisco Secure ACS and send them to the remote Cisco Secure ACS.



Tip This information is especially important if you are using the Max Sessions feature to control the number of connections a user is allowed. Max Sessions depends on accounting start and stop records, and where the accounting information is sent determines where the Max Sessions counter is tracked. The Failed Attempts log and the Logged in Users report are also affected by where the accounting records are sent.

- Step 8** When you finish, click **Submit** or **Submit + Restart**.
-

Sorting the Character String Match Order of Distribution Entries

You can use this procedure to set the priority by which Cisco Secure ACS searches character string entries in the Proxy Distribution Table when users dial in.

To determine the order by which Cisco Secure ACS searches entries in the Proxy Distribution Table, follow these steps:

-
- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration page opens.
- Step 2** Below the Proxy Distribution Table, click **Sort Entries**.

**Tip**

Before you sort the entries, you must have configured at least two unique Proxy Distribution Table entries in addition to the (Default) table entry.

- Step 3** Select the character string entry to reorder, and then click **Up** or **Down** to move its position to reflect the search order you want.
- Step 4** When you finish sorting, click **Submit** or **Submit + Restart**.
-

Editing a Proxy Distribution Table Entry

To edit a Proxy Distribution Table entry, follow these steps:

-
- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration page opens.
- Step 2** In the Character String column of the Proxy Distribution Table, click the distribution entry you want to edit.
The Edit Proxy Distribution Entry page appears.
- Step 3** Edit the entry as necessary.

**Tip**

For information about the parameters that make up a distribution entry, see [Adding a New Proxy Distribution Table Entry, page 4-43](#).

- Step 4** When you finish editing the entry, click **Submit** or **Submit + Restart**.
-

Deleting a Proxy Distribution Table Entry

To delete a Proxy Distribution Table entry, follow these steps:

- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration page opens.
- Step 2** In the Character String column of the Proxy Distribution Table, click the distribution entry you want to delete.
The Edit Proxy Distribution Entry page appears.
- Step 3** Click **Delete**.
A confirmation dialog box appears.
- Step 4** Click **OK**.
The distribution entry is deleted from the Proxy Distribution Table.
-