



CHAPTER 3

Network Configuration

This chapter details concepts and procedures for configuring the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS. You use the configuration process to establish a distributed system, and set up interaction with authentication, authorization, and accounting (AAA) clients and servers. You can also configure remote agents for the ACS SE.

This chapter contains:

- [About Network Configuration, page 3-1](#)
- [About ACS in Distributed Systems, page 3-2](#)
- [Proxy in Distributed Systems, page 3-3](#)
- [Network Device Searches, page 3-6](#)
- [Configuring AAA Clients, page 3-8](#)
- [Configuring AAA Servers, page 3-15](#)
- [Configuring Remote Agents \(ACS SE Only\), page 3-19](#)
- [Configuring Network Device Groups, page 3-23](#)
- [Configuring Proxy Distribution Tables, page 3-28](#)

About Network Configuration

The appearance of the page that you see when you click Network Configuration differs according to the network-configuration selections that you made in the Interface Configuration section.

The tables that might appear in this section are:

- **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 [Displaying Advanced Options, page 2-6](#).

- **AAA Servers**—This table lists each AAA server that is configured on the network together with its IP address and associated type. After installation, this table automatically lists the machine on which ACS is installed. In ACS SE, the name of the machine is listed as *self*.

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 [Displaying Advanced Options, page 2-6](#).

- **Remote Agents** (ACS SE)—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 3-19](#).



Note The Remote Agents 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 [Displaying Advanced Options, page 2-6](#).

- **Network Device Groups**—This table lists the name of each NDG that has been configured, and the number of AAA clients and AAA servers that are 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 AAA clients or AAA servers, 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 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 [Displaying Advanced Options, page 2-6](#).

- **Proxy Distribution Table**—You can use the Proxy Distribution Table to configure proxy capabilities including domain stripping. For more information, see [Configuring Proxy Distribution Tables, page 3-28](#).

This table appears only when you have configured the interface to enable Distributed Systems Settings. For more information about this interface configuration, see [Displaying Advanced Options, page 2-6](#).

About ACS in Distributed Systems

These topics describe how ACS can be used in a distributed system.

- [AAA Servers in Distributed Systems, page 3-2](#)
- [Default Distributed System Settings, page 3-3](#)

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. Multiple AAA servers can be configured to communicate with one another as primary, backup, client, or peer systems. You can, therefore, use powerful features such as:

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

You can configure AAA servers 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 can 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. You can, therefore, centrally control dial-up access, and secure network devices from unauthorized access.

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

Completing the AAA functionality, ACS serves as a central repository for accounting information. Each user session that ACS grants can be fully accounted for, and its accounting information can be stored in the server. You can use this accounting information for billing, capacity planning, and security audits.

**Note**

If the fields mentioned in this section do not appear in the ACS web interface, you can enable them by choosing **Interface Configuration > Advanced Options**. Then, check the **Distributed System Settings** check box.

Default Distributed System Settings

You use the AAA Servers table and the Proxy Distribution Table to establish distributed system settings. The parameters that are configured within these tables create the foundation so that you can configure multiple ACSs to work with one another. Each table contains an ACS entry for itself. In the AAA Servers table, the only AAA server that is initially listed is itself (in ACS SE, the server name is listed as *self*); the Proxy Distribution Table lists an initial entry of (*Default*), which displays how the local ACS is configured to handle each authentication request locally.

You can configure additional AAA servers in the AAA Servers table. These devices can, therefore, become visible in the web interface so that they can be configured for other distributed features such as proxy, ACS internal database replication, remote logging, and RDBMS synchronization. For information about configuring additional AAA servers, see [Adding AAA Servers, page 3-17](#).

Proxy in Distributed Systems

Proxy is a powerful feature that enables you to use ACS for authentication in a network that uses more than one AAA server. This section contains:

- [The Proxy Feature, page 3-3](#)
- [Fallback on Failed Connection, page 3-4](#)
- [Remote Use of Accounting Packets, page 3-5](#)
- [Other Features Enabled by System Distribution, page 3-6](#)

The Proxy Feature

Using proxy, ACS automatically forwards an authentication request from AAA clients to AAA servers. After the request has been successfully authenticated, the authorization privileges that you configured for the user on the remote AAA server are passed back to the original 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 configure proxy, you choose **Interface Configuration > Advanced Options**. Then, check the **Distributed System Settings** check box.

An Example

This section presents a scenario of proxy that is 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*. The New York ACS does not recognize her username, but the Proxy Distribution Table contains an entry, *@la.corporate.com*, to forward the authentication request to the Los Angeles ACS. Because the username and password information for Mary reside on that AAA server, when she authenticates correctly, the AAA client in the New York office applies the authorization parameters that are assigned to her.

Proxy Distribution Table

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 ACSs throughout your network. For information about configuring the Proxy Distribution Table, see [Configuring Proxy Distribution Tables, page 3-28](#).

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



Note

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



Note

When an ACS proxies to a second ACS, the second ACS responds to the first by using only IETF attributes, no VSAs, when it recognizes the first ACS as the AAA server. Alternatively, you can configure the second ACS to see an ACS as a AAA client; in this case, the second 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.

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

Fallback on Failed Connection

You can configure the order in which ACS checks remote AAA servers if a failure of the network connection to the primary AAA server occurs. 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 checking

continues, in order, down the list, until the AAA servers 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 ACS cannot connect to any server in the list, authentication fails.

Character String

ACS forwards authentication requests by using a configurable set of characters with a delimiter, such as periods (`.`), slashes (`/`), or hyphens (`-`). When configuring the ACS character string, 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 the asterisk (`*`) represents any delimiter. An example of a prefix character string is `domain.*username`, where the asterisk (`*`) would be used to detect the slash(`/`).

Stripping

Stripping allows ACS to remove, or strip, the matched character string from the username. When you enable stripping, ACS examines each authentication request for matching information. When ACS finds a match by character string in the Proxy Distribution Table, as described in the example under [Proxy in Distributed Systems, page 3-3](#), ACS strips off the character string if you have configured it to do so. For example, in the following proxy example, 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, ACS might find a match on the `@corporate.com` character string, and strip the `@corporate.com`, leaving a username of `mary`, which might be the username format that the destination AAA server requires to identify the correct entry in its database.



Note

Realm stripping does not work with Extensible Authentication Protocol (EAP)-based authentication protocols, such as Protected Extensible Authentication Protocol (PEAP) or Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST). For example, if you are using Protected Extensible Authentication Protocol Microsoft Challenge Authentication Handshake Protocol (PEAP MSCHAP), authentication will fail if a realm is stripped by proxy.

Remote Use of Accounting Packets

When proxy is employed, 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 ACS offers several benefits.

- When 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. 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 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 an ACS and the Max Sessions feature is implemented, you can track the number of sessions that are allowed for each user or group.
- You can also choose to have Voice-over-IP (VoIP) accounting information logged remotely, appended to the RADIUS Accounting log, entered in a separate VoIP Accounting log, or both.

Other Features Enabled by System Distribution

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

- **Replication**—For more information, see [ACS Internal Database Replication, page 8-1](#).
- **RDBMS synchronization**—For more information, see [RDBMS Synchronization, page 8-17](#).
- **Remote and centralized logging**—For more information, see [Remote Logging for ACS for Windows, page 10-10](#), and [Remote Logging for ACS SE with ACS Remote Agents, page 10-10](#).

Network Device Searches

You can search for any network device that is configured in the Network Configuration section of the ACS web interface.

This section contains:

- [Network Device Search Criteria, page 3-6](#)
- [Searching for Network Devices, page 3-7](#)

Network Device Search Criteria

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

- **Name**—The name assigned to the network device in ACS. You can use an asterisk (*) as a wildcard character. 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 ACS. For each octet in the address, you have three options:
 - **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.*.

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.*.*.

- **Type**—The device type, as specified by the AAA protocol that it is configured to use, or the kind of AAA server it is. You can also search for Solution Engine remote agents. If you do not want to limit the search based on device type, choose **Any** from the Type list.
- **Device Group**—The NDG to which the device is assigned. 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:

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 that was previously conducted for this session, if any.



Tip When you leave the Search for Network Devices page, ACS retains your search criteria and results for the duration of the current administrative session. Until you log out of 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 3-6](#).



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

Step 4 Click **Search**.

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

The table listing that matches 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 want, in 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 in the table of matching network devices.

ACS displays the applicable setup page. For information about the AAA Client Setup page, see [AAA Client Configuration Options, page 3-8](#). For information about the AAA Server Setup page, see [AAA Server Configuration Options, page 3-15](#).

- 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 by using different criteria, repeat Step 3 and Step 4.
-

Configuring AAA Clients

This guide uses the term “AAA client” comprehensively to signify the device through which or to which service access is attempted. This is the RADIUS or TACACS+ client device, and may comprise Network Access Servers (NASs), PIX Firewalls, routers, or any other RADIUS or TACACS+ hardware or software client.

This section contains:

- [AAA Client Configuration Options, page 3-8](#)
- [Adding AAA Clients, page 3-12](#)
- [Editing AAA Clients, page 3-13](#)
- [Deleting AAA Clients, page 3-14](#)

AAA Client Configuration Options

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

The Add AAA Client and AAA Client Setup pages include:

- **AAA Client Hostname**—The name that you assign to the AAA client configuration. Each AAA client configuration can represent multiple network devices; thus, the AAA client hostname configured in 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 AAA client hostnames is 32 characters.



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

- **AAA Client IP Address**—At a minimum, a single IP address of the 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. 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 the AAA client configuration in ACS to represent multiple network devices, you can specify multiple IP addresses. Separate each IP address by pressing **Enter**.

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

- **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.*.

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.*.*.

- **Shared Secret**—The shared secret key of the AAA client. Maximum length for the AAA client key is 64 characters.

For correct operation, the key must be identical on the AAA client and ACS. Keys are case sensitive. If the shared secret does not match, ACS discards all packets from the network device.

- **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 ACS to use NDGs. To enable NDGs, choose **Interface Configuration > Advanced Options**. Then, check the **Network Device Groups** check box.

- **RADIUS Key Wrap**—The shared secret keys for RADIUS Key Wrap in PEAP, EAP-FAST and EAP-TLS authentications. Each key must be unique, and must also be distinct from the RADIUS shared key. These shared keys are configurable for each AAA Client, as well as for each NDG. The NDG key configuration overrides the AAA Client configuration.
 - **Key Encryption Key (KEK)**—This is used for encryption of the Pairwise Master Key (PMK). In ASCII mode, enter a key length of exactly 16 characters; in hexadecimal mode, enter a key length of 32 characters.
 - **Message Authentication Code Key (MACK)**—This is used for the keyed hashed message authentication code (HMAC) calculation over the RADIUS message. In ASCII mode, enter a key length of exactly 20 characters; in hexadecimal mode, enter a key length of 40 characters.



Note If you leave a key field empty when key wrap is enabled, the key will contain only zeros.

- **Key Input Format**—Select whether to enter the keys as ASCII or hexadecimal strings (the default is ASCII).



Note You must enable the Key Wrap feature in the NAP Authentication Settings page to implement these shared keys in PEAP, EAP-FAST and EAP-TLS authentication.

- **Authenticate Using**—The AAA protocol to use 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 [Creating, Reading, Updating and Deleting Actions for AAA clients, page 8-22](#). The Authenticate Using list always contains:

- **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 Airespace)**—RADIUS using Cisco Airespace VSAs. Select this option if the network device is a Cisco Airespace WLAN device supporting authentication via RADIUS.
- **RADIUS (Cisco Aironet)**—RADIUS using Cisco Aironet VSAs. Select this option if the network device is a Cisco Aironet Access Point used by users who authenticate with the Lightweight and Efficient Application Protocol (LEAP) or the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) protocol, 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, ACS first attempts authentication by using LEAP; if this fails, ACS fails over to EAP-TLS. If LEAP is not enabled on the Global Authentication Setup page, ACS immediately attempts EAP-TLS authentication. If neither LEAP nor EAP-TLS is enabled on the Global Authentication Setup, any authentication attempt received from a Cisco Aironet RADIUS client fails. For more information about enabling LEAP or EAP-TLS, see [Global Authentication Setup, page 9-21](#).

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

Users accessing the network through a Cisco Aironet network device can only be authenticated against the:

- ACS internal database
- Windows user database
- ODBC user database
- MCIS database

**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). ACS cannot support PEAP authentication by using the RADIUS (Cisco Aironet) protocol.

- **RADIUS (Cisco BBSM)**—RADIUS using Cisco Broadband Services Manager (BBSM) Vendor Specific Attributes (VSAs). Select this option if the network device is a Cisco BBSM network device supporting authentication via RADIUS.
- **RADIUS (Cisco IOS/PIX 6.0)**—RADIUS using Cisco IOS/PIX 6.0 VSAs. This option enables you to pack commands sent to a Cisco IOS or Project Information Exchange (PIX)S 6.0 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 and PIX equipment.
- **RADIUS (Cisco VPN 3000/ASA/PIX7.x+)**—RADIUS using Cisco VPN 3000 concentrator, ASA device, and PIX 7.x device VSAs. Select this option if the network device is a Cisco VPN 3000 series concentrator, an ASA, or PIX 7.x+ device supporting authentication via RADIUS.
- **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 who authenticate 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 that supports authentication via RADIUS.
- **RADIUS (Juniper)**—RADIUS using Juniper RADIUS VSAs. Select this option if the network device is a Juniper network device that supports authentication via RADIUS.
- **RADIUS (Nortel)**—RADIUS using Nortel RADIUS VSAs. Select this option if the network device is a Nortel network device that supports 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. The iPass RADIUS is identical to IETF RADIUS.
- **RADIUS (3COMUSR)**—RADIUS using 3COMUSR RADIUS VSAs. Select this option if the network device is a 3COMUSR network device that supports authentication via 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 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 unchecked.

If this feature is selected and the connection fails, a stop record is sent to the TACACS+ accounting log for each user connected through the AAA client.



Note If TCP connections between 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 that are sent periodically during a session. They provide you with an approximate session length if the AAA client fails and, therefore, no stop packet is received to mark the end of the session. By default, this check box is unchecked.
- **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 unchecked.
- **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 ACS IP pools server and the AAA client does not provide a unique port for each user, ACS assumes that a reused port number indicates that the previous user session has ended and ACS may reassign the IP address that was previously assigned to the session with the non-unique port number. By default, this check box is unchecked.



Note If this option is enabled, 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 the AAA client with this feature enabled.

- **Match Framed-IP-Address with user IP address for accounting packets from this AAA Client**—Select this option when the AAA client uses Cisco SSL WebVPN. This action ensures that ACS assigns different IP addresses to two different users when they log in via a Cisco SSL WebVPN client. By default, this check box is unchecked.

Adding AAA Clients

You can use this procedure to add AAA client configurations.

Before You Begin

For ACS to provide AAA services to AAA clients, you must ensure that gateway devices between AAA clients and ACS allow communication over the ports needed to support the applicable AAA protocol (RADIUS or TACACS+). For information about ports that AAA protocols use, see [AAA Protocols—TACACS+ and RADIUS, page 1-3](#).

To add AAA clients:

-
- 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 you want to assign the AAA client. Then, click **Add Entry** below the AAA Clients table.
 - To add AAA clients when you have not enabled NDGs, click **Add Entry** below the AAA Clients table.
- The Add AAA Client page appears.
- Step 3** Enter the AAA client settings, as needed. For information about the configuration options available for the AAA client, see [AAA Client Configuration Options, page 3-8](#).
- Step 4** To save your changes and apply them immediately, click **Submit + Apply**.



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



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

Editing AAA Clients

You can use the following procedure to edit the settings for AAA client configurations.

**Note**

You cannot directly edit the names of AAA clients; rather, you must delete the AAA client entry and then reestablish the entry with the corrected name. For steps about deleting AAA client configurations, see [Deleting AAA Clients, page 3-14](#). For steps about creating AAA client configurations, see [Adding AAA Clients, page 3-12](#).

Before You Begin

For ACS to provide AAA services to AAA clients, you must ensure that gateway devices between AAA clients and ACS permit communication over the ports that support the applicable AAA protocol (RADIUS or TACACS+). For information about ports that AAA protocols use, see [AAA Protocols—TACACS+ and RADIUS, page 1-3](#).

To edit AAA clients:

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 AAA clients 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 the AAA client, see [AAA Client Configuration Options, page 3-8](#).

**Note**

You cannot directly edit the name of the AAA client; rather, you must delete the AAA client entry and then re-establish the entry with the corrected name. For steps about deleting the AAA client entry, see [Deleting AAA Clients, page 3-14](#). For steps about creating the AAA client entry, see [Adding AAA Clients, page 3-12](#).

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

**Tip**

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

**Note**

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

Configuring a Default AAA Client

You can configure a default AAA Client to accommodate any unrecognized AAA Clients (NAS):

-
- Step 1** Follow the steps for [Adding AAA Clients, page 3-12](#).
 - Step 2** Leave the AAA Client Hostname and AAA Client IP address blank.
 - Step 3** Complete the rest of the fields and continue with the rest of the procedure for adding AAA Clients.



Note

Only TACACS+ can have a default AAA Client configured. The default name for the client is **Others** and the default IP address is 0.0.0.0.

Deleting AAA Clients

To delete AAA clients:

-
- 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 AAA clients 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 + Apply**.



Note

Restarting ACS services clears the Logged-in User report and temporarily interrupts all ACS services. As an alternative to restarting when you delete AAA clients, you can click **Delete**. However, when you do, the change does not take effect until you restart the system, which you can do by choosing **System Configuration > Service Control**. Then, choose **Restart**.

A confirmation dialog box appears.

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

ACS restarts AAA services and the AAA client is deleted.

If you have a configured RADIUS/TACACS source-interface command on the AAA client, ensure that you configure the client on ACS by using the IP address of the interface that is specified.

Configuring AAA Servers

This section presents procedures for configuring AAA servers in the ACS web interface. For additional information about AAA servers, see [AAA Servers in Distributed Systems, page 3-2](#).

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

**Tip**

If the AAA Servers table does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Distributed System Settings** check box.

This section contains:

- [AAA Server Configuration Options, page 3-15](#)
- [Adding AAA Servers, page 3-17](#)
- [Editing AAA Servers, page 3-17](#)
- [Deleting AAA Servers, page 3-18](#)

AAA Server Configuration Options

AAA server configurations enable ACS to interact with the AAA server that the configuration represents. AAA servers that do not have a corresponding configuration in ACS, or whose configuration in ACS is incorrect, do not receive AAA services from ACS, such as proxied authentication requests, database replication communication, remote logging, and RDBMS synchronization. Also, several distributed systems features require that the other ACSs included in the distributed system be represented in the AAA Servers table. For more information about distributed systems features, see [About ACS in Distributed Systems, page 3-2](#).

After installation, the AAA Servers table automatically lists the machine on which ACS is installed. This machine is also defined as the default proxy server in the Proxy Distribution table, and appears by default in the RDBMS table.

**Note**

In ACS SE, the name of the machine in the AAA servers table is listed as *self*; in the Proxy Distribution and RDBMS tables the appliance hostname is listed.

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

- **AAA Server Name**—The name that you assign to the AAA server configuration. The AAA server hostname that is configured in 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 AAA server names is 32 characters.

**Note**

After you submit the AAA server name, you cannot change it. If you want to use a different name for the AAA server, delete the AAA server configuration and create the AAA server configuration by 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 AAA server keys is 64 characters. For correct operation, the key must be identical on the remote AAA server and ACS. Keys are case sensitive. Because shared secrets are not synchronized, you could easily to make mistakes when entering them on remote AAA servers and ACS. If the shared secret does not match, 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 ACS to use NDGs. To enable NDGs, choose **Interface Configuration > Advanced Options**. Then, check 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 ACS. Watchdog packets are interim packets that are sent periodically during a session. They provide you with an approximate session length if the AAA client fails and, therefore, no stop packet is received to mark the end of the session.
- **AAA Server Type**—One of types:
 - **RADIUS**—Select this option if the remote AAA server is configured by using any type of RADIUS protocol.
 - **TACACS+**—Select this option if the remote AAA server is configured by using the TACACS+ protocol.
 - **ACS**—Select this option if the remote AAA server is another ACS. This action enables you to configure features that are only available with other ACSs, such as ACS internal database replication and remote logging.
- **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 ACS. The list includes:
 - **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 the AAA server that is configured for Outbound, the authentication request is not sent.
 - **Inbound/Outbound**—The remote AAA server forwards and accepts authentication requests, allowing the selected server to handle authentication requests in any manner that is defined in the distribution tables.
- **AAA Server RADIUS Authentication Port**—Specify the port on which the AAA server accepts authentication requests. The standard port is 1812, and another commonly used port is 1645. If you select **TACACS+** in the AAA Server Type field, this RADIUS Authentication Port field is dimmed.
- **AAA Server RADIUS Accounting Port**—Specify the port on which the AAA server accepts accounting information. The standard port is 1813, and another commonly used port is 1646. If you select **TACACS+** in the AAA Server Type field, this RADIUS Accounting Port field is dimmed.

Adding AAA Servers

Before You Begin

For descriptions of the options that are available while adding a remote AAA server configuration, see [AAA Server Configuration Options, page 3-15](#).

For ACS to provide AAA services to a remote AAA server, you must ensure that gateway devices between the remote AAA server and ACS permit communication over the ports that support the applicable AAA protocol (RADIUS or TACACS+). For information about ports that AAA protocols use, see [AAA Protocols—TACACS+ and RADIUS, page 1-3](#).

To add and configure AAA servers:

-
- 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 AAA servers when you have not enabled NDGs, below the AAA Servers table, click **Add Entry**.
- The Add AAA Server page appears.
- Step 3** Enter the AAA server settings, as needed. For information about the configuration options available for the AAA server, see [AAA Server Configuration Options, page 3-15](#).
- Step 4** To save your changes and apply them immediately, click **Submit + Apply**.



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



Note Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter and resets it to (0).

Editing AAA Servers

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



Note You cannot edit the names of AAA servers. To rename AAA servers, 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 3-15](#).

For ACS to provide AAA services to a remote AAA server, you must ensure that gateway devices between the remote AAA server and ACS permit communication over the ports that support the applicable AAA protocol (RADIUS or TACACS+). For information about ports that AAA protocols use, see [AAA Protocols—TACACS+ and RADIUS, page 1-3](#).

To edit AAA servers:

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 change AAA server settings, as needed. For information about the configuration options available for the AAA server, see [AAA Server Configuration Options, page 3-15](#).

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



Tip

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



Note

Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter and resets it to (0).

Deleting AAA Servers

To delete AAA servers:

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 + Apply**.

**Note**

Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. As an alternative to restarting when you delete AAA servers, 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 choosing **System Configuration > Service Control**. Then, choose **Restart**.

A confirmation dialog box appears.

Step 4 Click **OK**.

ACS performs a restart and the AAA server is deleted.

Configuring Remote Agents (ACS SE Only)

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

This section contains:

- [About Remote Agents, page 3-19](#)
- [Remote Agent Configuration Options, page 3-19](#)
- [Adding a Remote Agent, page 3-21](#)
- [Editing a Remote Agent Configuration, page 3-22](#)
- [Deleting a Remote Agent Configuration, page 3-23](#)

About Remote Agents

An ACS SE can use remote agents for remote logging and authentication of users with a Windows external user database. Before you can configure remote logging and authentication by 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 the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

Remote Agent Configuration Options

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

**Note**

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

- **Remote Agent Name**—The name that you assign to the remote agent configuration. You configure remote agent logging and Windows authentication by using remote agent names. We recommend that you adopt a descriptive, consistent naming convention for remote agents. For example, you could assign the same name as the hostname of the server that runs the remote agent. The 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 by 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-decimal format. For example, 10.77.234.3.
- **Remote Agent Port**—The TCP port on which the remote agent listens for communication from ACS. The maximum length for the TCP port number is 6 characters. The Remote Agent Port must be a numeric value in the range of 0 to 65535.



Note If the port number that you provide does not match the port the remote agent that you configured for listening, ACS cannot communicate with the remote agent. For information about configuring the remote agent port, see the *Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2*.

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

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 ACS can contact the remote agent, the uptime for the remote agent appears. If ACS cannot contact the remote agent, the message `Not responding` appears.
- **Configuration Provider**—The ACS from which the remote agent receives its configuration.



Tip Click on the ACS name to access the web interface for the ACS that provides configuration data to a remote agent. A new browser window displays the web interface for the ACS that provides configuration data to the remote agent.

- **Service Table**—ACS displays a table of remote agent services below the Configuration Provider. 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 ACS into which you are logged is currently using the corresponding service.

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 3-19](#).

For ACS to communicate with a remote agent, you must ensure that gateway devices between a remote agent and ACS permit communication over the TCP ports used by remote agents. For information about ports used by remote agents, see the *Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2*.

To add and configure a remote agent:

-
- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration section opens.
- Step 2** Perform one of the following steps, based on your use of NDGs:
- If you are using NDGs, click the name of the NDG to which you want to assign the remote agent. Then, in the NDG Remote Agents table, click **Add Entry**.
 - If you are not using NDGs, click **Add Entry** in the Remote Agents table.
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 on which the remote agent listens for communication from ACS (up to 6 digits). The default TCP port is 2004.



Note If this port number does not match the port on which the remote agent is configured to listen, ACS cannot communicate with the remote agent. For information about configuring the port number on which the remote agent listens, see the *Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2*.

- 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 > Advanced Options**, and then click **Network Device Groups**.

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



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



Note Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. The Max Sessions counter is reset to 0.

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 by 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 3-19](#).



Note

For ACS to communicate with a remote agent, you must ensure that gateway devices between a remote agent and ACS permit communication over the TCP ports used by remote agents. For information about ports used by remote agents, see the *Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2*.

To edit a remote agent configuration:

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

The Network Configuration section opens.

Step 2 Perform one of the following steps, based on your use of NDGs:

- a. If you are using NDGs, click the name of the NDG to which the remote agent belongs. 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 that you want to edit.

The Remote Agent Setup for the *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 (displayed if enabled in Advanced Options in the interface configuration)



Note

If the ACS into which you are currently logged does not provide configuration data for the remote agent, none of the options can be edited. You can access the web interface for the ACS that does provide configuration data to the remote agent by clicking the ACS name listed as the Configuration Provider.

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



Tip

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

**Note**

Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. The Max Sessions counter is reset to 0.

Deleting a Remote Agent Configuration

**Note**

You cannot delete a remote agent that you have configured to use for remote logging or Windows authentication.

To delete a remote agent configuration:

- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration section opens.
- Step 2** Perform one of the following steps, based on your use of NDGs:
- If you are using NDGs, click the name of the NDG to which the remote agent belongs. Then, in the NDG Remote Agents table, click the name of the remote agent configuration you want to delete.
 - 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 the *agent* page appears.
- Step 3** To delete the remote agent and have the deletion take effect immediately, click **Delete + Apply**.

**Note**

Restarting services clears the Logged-in User report and temporarily interrupts all 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 > Service Control > Restart**.

A confirmation dialog box appears.

- Step 4** Click **OK**.
ACS restarts its services and the remote agent configuration is deleted.

Configuring Network Device Groups

Network Device Grouping is an advanced feature that you use 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 action creates two levels of network devices within 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 web interface, you must check the Network Device Groups option 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 uncheck the Network Device Groups option. Therefore, if you choose to configure NDGs, ensure that you leave the Network Device Groups option selected on the Advanced Option page.

This section contains:

- [Adding a Network Device Group, page 3-24](#)
- [Assigning an Unassigned AAA Client or AAA Server to an NDG, page 3-25](#)
- [Reassigning AAA Clients or AAA Servers to an NDG, page 3-26](#)
- [Editing a Network Device Group, page 3-26](#)
- [Deleting a Network Device Group, page 3-27](#)

Adding a Network Device Group

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

- [Setting TACACS+ Enable Password Options for a User, page 6-23](#)
- [Setting Enable Privilege Options for a User Group, page 5-13](#)

To add an NDG:

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, choose **Interface Configuration > Advanced Options**. Then, choose **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 In the **Shared Secret** box, enter a key for the Network Device Group. The maximum length is 64 characters.

Each device that is assigned to the Network Device Group will use the shared key that you enter here. The key that was assigned to the device when it was added to the system is ignored. If the key entry is null, the AAA client key is used. See [AAA Client Configuration Options, page 3-8](#). This feature simplifies key management for devices.

Step 5 In the **RADIUS Key Wrap** section, enter the shared secret keys for RADIUS Key Wrap in PEAP, EAP-FAST, and EAP-TLS authentications.

Each key must be unique, and must also be distinct from the RADIUS shared key. These shared keys are configurable for each AAA Client, as well as for each NDG. The NDG key configuration overrides the AAA Client configuration. If the key entry is null, the AAA client key is used. See [AAA Client Configuration Options, page 3-8](#).

- **Key Encryption Key (KEK)**—This is used for encryption of the Pairwise Master Key (PMK). In ASCII mode, enter a key length of exactly 16 characters; in hexadecimal mode, enter a key length of 32 characters.
- **Message Authentication Code Key (MACK)**—This is used for the keyed hashed message authentication code (HMAC) calculation over the RADIUS message. In ASCII mode, enter a key length of exactly 20 characters; in hexadecimal mode, enter a key length of 40 characters.



Note If you leave a key field empty when key wrap is enabled, the key will contain only zeros.

- **Key Input Format**—Select whether to enter the keys as ASCII or hexadecimal strings (the default is ASCII).



Note You must enable the Key Wrap feature in the NAP Authentication Settings page to implement these shared keys in PEAP, EAP-FAST, and EAP-TLS authentication.



Note Click **Submit**.

The Network Device Groups table displays the new NDG.

Step 6 To populate the newly established NDG with AAA clients or AAA servers, perform one or more of the following procedures, as applicable:

- [Adding AAA Clients, page 3-12](#)
 - [Adding AAA Servers, page 3-17](#)
 - [Assigning an Unassigned AAA Client or AAA Server to an NDG, page 3-25](#)
 - [Reassigning AAA Clients or AAA Servers to an NDG, page 3-26](#)
-

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:

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, choose **Interface Configuration > Advanced Options**. Then, check the **Network Device Groups** check box.

- Step 3** Click the name of the network device that 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 AAA Clients or AAA Servers to an NDG

To reassign AAA clients or AAA servers to a new NDG:

-
- 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 the AAA Clients table or AAA Servers table, as applicable, click the name of the client or server that 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.
-

Editing a Network Device Group

You can rename an NDG, change the shared secret, and the key wrap configuration.



Caution

When renaming an NDG, ensure that there are no NARs or other shared profile components (SPCs) that invoke the original NDG name. 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 nonexistent (or renamed) NDG, the attempt will fail and the user will be rejected.

To edit an NDG:

-
- 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 edit.



Tip If the Network Device Groups table does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Network Device Groups** check box.

Step 3 At the bottom of the page, click **Edit Properties**.

Step 4 Change the network device group properties as required. For more information about these properties, see [Adding a Network Device Group, page 3-24](#).

Step 5 Click **Submit**.

The NDG properties are 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 might 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 AAA Clients or AAA Servers to an NDG, page 3-26](#); or, in cases where you have a large number of devices to reassign, use the RDBMS Synchronization feature.



Caution

When deleting an NDG, ensure that there are no NARs or other SPCs that invoke the original NDG. 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 nonexistent (or renamed) NDG, the attempt will fail and the user will be rejected.

To delete an NDG:

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, choose **Interface Configuration > Advanced Options**. Then check 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.

Configuring Proxy Distribution Tables

This section describes the Proxy Distribution Table.

This section contains:

- [About the Proxy Distribution Table, page 3-28](#)
- [Adding a New Proxy Distribution Table Entry, page 3-28](#)
- [Sorting the Character String Match Order of Distribution Entries, page 3-29](#)
- [Editing a Proxy Distribution Table Entry, page 3-30](#)
- [Deleting a Proxy Distribution Table Entry, page 3-30](#)

About the Proxy Distribution Table

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



Tip

To enable Distributed Systems Settings in the ACS, choose **Interface Configuration > Advanced Options**. Then, check 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 3-3](#).

The entries that you define and place in the Proxy Distribution Table are treated one at a time for each authentication request that ACS receives from the AAA client. The authentication request is defined in the Proxy Distribution Table according to the forwarding destination. If a match to an entry in the Proxy Distribution Table that contains proxy information is found, 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 that are received by the local 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 ACS. You might sometimes find it 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:

-
- 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, choose **Interface Configuration > Advanced Options**. 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 (<>) cannot be used.

Step 4 From the Position list, select **Prefix** if the character string that 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** to strip the character string from the username that you entered, or select **No** to leave it.

Step 6 In the AAA Servers column, select the AAA server that you want to use for proxy. Click the --> (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 that you want.



Tip If the AAA server that you want to use is not listed, choose **Network Configuration > AAA Servers**. Then, choose **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 ACS.
- **Remote**—Send accounting packets to the remote ACS.
- **Local/Remote**—Keep accounting packets on the local ACS and send them to the remote ACS.



Tip This information is especially important if you are using the Max Sessions feature to control the number of connections that 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. See [Remote Use of Accounting Packets, page 3-5](#) for an example.

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

Sorting the Character String Match Order of Distribution Entries

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

To determine the order by which ACS searches entries in the Proxy Distribution Table:

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 configure 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 that you want.

Step 4 When you finish sorting, click **Submit** or **Submit + Apply**.

Editing a Proxy Distribution Table Entry

To edit a Proxy Distribution Table entry:

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 that 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 3-28](#).

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

Deleting a Proxy Distribution Table Entry

To delete a Proxy Distribution Table entry:

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 that 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.
