Configuring Authentication, Authorization, and Accounting

This chapter contains procedures for:

- Configuring the AAA Authentication Server
- Specifying the Policy that Controls the Behavior of Authentication and Authorization
- Configuring the AAA Accounting Server

Configuring the AAA Authentication Server

The two procedures for configuring AAA authentication consist of:

- Configuring connection parameters for the AAA authentication server
- Configuring whether the authentication servers or local authentication database will be queried first

Note To help protect the cryptographic information of the RADIUS server, you must view the running configuration to see this information.

- About the Authentication Order
- About Authentication Failover
- About Unreachable Failover
- Example of Authentication Sequence
- Configuring Connection Parameters for the AAA Authentication Server

About the Authentication Order

The AAA policy specifies the failover functionality that you can optionally configure for the authentication server. You can use these two types of failover functionality separately or in combination:

- Authentication failover
- Unreachable failover

About Authentication Failover

The authentication failover feature enables you to optionally use a remote RADIUS server for user login authentication, in addition to the local database. The procedure in this section configures the order in which authentication is resolved. You can configure authentication to use:

- The local database only
- The remote server only
- The local database first, then the remote server
- The remote server first, then the local database

When using both local and remote authentication, you can also configure whether you want the user attributes that are retrieved from a remote RADIUS AAA server to be merged with the attributes found in the local user database for the same username.

Note The authentication failover feature has the following limitations:

- Authentication with a RADIUS server is available only when accessing the GUI or CLI interface and requires only a user ID and password. Authentication for the TUI, VVE, AvT, and IMAP interfaces can use only the local database. Therefore, to gain access, users of the TUI, VVE, AvT, and IMAP interfaces must be configured locally. The auto-attendant interface does not require authentication because it is user independent.
- Login information is not synchronized between the local system and the remote server. Therefore:
  - Any security features such, as password expiration, must be configured separately for Cisco Unity Express and the RADIUS server.
  - Cisco Unity Express users are not prompted when security events, such as password expiration or account lockout, occur on the RADIUS server.
  - RADIUS server users are not prompted when security events, such as password expiration or account lockout, occur on Cisco Unity Express.

About Unreachable Failover

The Unreachable Failover feature is used only with RADIUS servers. This feature enables you to configure up to two addresses that can be used to access RADIUS servers.

As Cisco Unity Express attempts to authenticate a user with the RADIUS servers, the system sends messages to users to notify them when a RADIUS server either cannot be reached or fails to authenticate the user.

Example of Authentication Sequence

In this example, authentication is performed by the remote server first, then by the local database. Also, two addresses are configured for the remote RADIUS server.

This sequence of events could occur during authentication for this example:

1. Cisco Unity Express tries to contact the first remote RADIUS server.

2. If the first RADIUS server does not respond or does not accept the authentication credentials of the user, Cisco Unity Express tries to contact the second remote RADIUS server.
3. If the second RADIUS server does not respond or does not accept the authentication credentials of the user, the user receives the appropriate error message and Cisco Unity Express tries to contact the local database.
4. If the local database does not accept the authentication credentials of the user, the user receives an error message.

Configuring Connection Parameters for the AAA Authentication Server

Procedure

Step 1 Choose **Configure > AAA > Authentication**.

The system displays the AAA Authentication Server Configuration window.

Step 2 Enter the following information in the appropriate fields for the primary server, and optionally, for the secondary server:

- Server IP address or DNS name
- Port number used
- Cryptographic shared secret and security credentials
- Number of login retries
- Length of login timeout

Step 3 Click **Apply**.

Step 4 Click **OK** to save your changes.

Specifying the Policy that Controls the Behavior of Authentication and Authorization

Use this procedure to configure the information used to log into the authentication server.

Procedure

Step 1 Choose **Configure > AAA > Authorization**.

The system displays the Configure AAA Authorization Server Configuration window.

Step 2 Select or deselect whether you want to merge the attributes of the remote AAA server with the attributes in the local database.

Step 3 Click **Apply**.

Step 4 Click **OK** to save your changes.

Configuring the AAA Accounting Server

This section covers the following topics:

Overview

You can configure up to two AAA accounting servers. Automatic failover functionality is provided if you have two accounting servers configured. If the first server is unreachable, the accounting information is sent to the second server. If both accounting servers are unreachable, accounting records are cached until a server becomes available. If a server cannot be reached before the cache is full, the oldest accounting packets are dropped to make room for the new packets.

Because the configuration of the AAA accounting server is completely independent of the AAA authentication server, you can configure the AAA accounting server to be on the same or different machine from the AAA authentication server.

If you use a syslog server, it is not affected by the AAA configuration and continues to use the existing user interfaces. When the RADIUS server sends AAA accounting information to a syslog server, it is normalized into a single string before being recorded. If no syslog server is defined, the AAA accounting logs are recorded by the syslog server running locally on Cisco Unity Express.

Note Only RADIUS servers are supported.

AAA Accounting Event Logging

AAA accounting logs contain information that enables you to easily:

- Audit configuration changes.
- Maintain security.
- Accurately allocate resources.
- Determine who should be billed for the use of resources.

You can configure AAA accounting to log the following types of events:

- Logins—All forms of system access except IMAP, including access to the CLI, GUI, TUI, and VVE, when a login is required.
- Logouts—All forms of system access except IMAP, including access to the CLI, GUI, TUI, and VVE, when a login is required before logout.
- Failed logins—Failed login attempts for all forms of system access except IMAP, including access to the CLI, GUI, TUI, and VVE, when a login is required.
- Configuration mode commands—Any changes made to the Cisco Unity Express configuration using any interface except IMAP (CLI, GUI, TUI, and VVE).

- EXEC mode commands—Any commands entered in Cisco Unity Express EXEC mode using any interface except IMAP (CLI, GUI, TUI, and VVE).
- System startups—System startups, which include information about the system's software version, installed licenses, installed packages, installed languages, and so on.
- System shutdowns—System shutdowns, which include information about the system's software version, installed licenses, installed packages, installed languages, and so on.
- IMAP—Access to the IMAP system.

In addition to information specific to the type of action performed, the accounting logs also indicate the following:

- User that authored the action
- Time when the action was executed
- Time when the accounting record was sent to the server

Note Account logging is not performed during the system power-up playback of the startup configuration. When the system boots up, the startup-config commands are not recorded.

Configuring the AAA Accounting Server

Use this procedure to configure the information used to log into the accounting server.

Procedure

Step 1 Choose **Configure > AAA > Accounting**.

The AAA Accounting Server Configuration window appears.

Step 2 Click **Accounting Enabled**.

Step 3 Enter the following information in the appropriate field for the primary server, and optionally, for the secondary server:

- Server IP address or DNS name
- Port number used
- Cryptographic shared secret and security credentials
- Number of login retries
- Length of login timeout

Step 4 Click **Apply**.

Step 5 Click **OK** to save your changes.

Configuring Accounting Event Logging

Use this procedure to configure which event types to log for AAA accounting.

Procedure

Step 1 Choose **Configure > AAA > Accounting**.

The system displays the Accounting Server Configuration window.

Step 2 Select the log events that you want to include in the log and deselect those you do not want to include.

Step 3 Click **Apply** to save your changes.