# Configuring Authentication, Authorization, and Accounting


- 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


- 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. 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** 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 the Cisco Unified SRSV system and the RADIUS server.
- Cisco Unified SRSV 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 the Cisco Unified SRSV system.

# 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 the Cisco Unified SRSV system 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. The Cisco Unified SRSV system 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, the Cisco Unified SRSV system 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 the Cisco Unified SRSV system 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** Log in to the Cisco UMG GUI. See the Logging In to the Cisco UMG Graphical User Interface (GUI) module.

**Step 2** Choose **Configure > AAA > Authentication**.

The system displays the Configure AAA Authentication page.

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

- Authentication order
- Number of login retries
- Length of login timeout
- Hostname
- Port
- Password

**Step 4** Click **Apply**.

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

# Specifying the Policy that Controls the Behavior of Authentication and Authorization

**Procedure**

**Step 1** Log in to the Cisco UMG GUI. See the Logging In to the Cisco UMG Graphical User Interface (GUI) module.

**Step 2** Choose **Configure > AAA > Authorization**.

The system displays the Configure AAA Authorization page.

**Step 3** Select or deselect whether you want to merge the attributes of the remote AAA server with the attributes in the local database.

**Step 4** Click **Apply**.

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

# Configuring the AAA Accounting Server

- Overview of AAA Accounting
- About Event Logging for AAA Accounting
- Configuring the AAA Accounting Server and Event Logging

# Overview of AAA Accounting

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 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.

# About Event Logging for AAA Accounting

AAA accounting logs contain information that enable 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:

| Log Name | Description |
|---|---|
| login | All forms of system access when a login is required. |
| logout | All forms of system access when a login is required before logout. |
| login-fail | Failed login attempts for all forms of system access when a login is required. |
| config-commands | Any changes made to the system configuration using any interface. |
| exec-commands | Any commands entered in EXEC mode using any interface. |
| system-startup | System startups, which include information about the system's software version, installed licenses, installed packages, installed languages, and so on. |
| system-shutdown | System shutdowns, which include information about the system's software version, installed licenses, installed packages, installed languages, and so on. |

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

- 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 and Event Logging

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

**Procedure**

**Step 1** Log in to the Cisco UMG GUI. See the Logging In to the Cisco UMG Graphical User Interface (GUI) module.

**Step 2** Choose **Configure > AAA > Accounting**.

The system displays the Configure AAA Accounting page.

**Step 3** Enter the following information in the appropriate fields:

- If accounting is enabled
- Number of login retries
- Length of login timeout, in seconds
- Server IP address or DNS name
- Port number used
- Password

**Step 4** Select the log events that you want to include in the log and deselect those you do not want to include.

**Step 5** Click **Apply**.

**Step 6** Click **OK** to save your changes.