



# Configuring Authentication, Authorization, and Accounting

This chapter contains procedures for:

- [Configuring the Accounting Server, page 2](#)
- [Configuring the Authentication Server, page 4](#)
- [Configuring the AAA Policy, page 5](#)
- [Configuring Privileges, page 8](#)
- [Configuring Accounting Event Logging, page 18](#)
- [Configuring Console Authentication, page 21](#)

## Overview

Release 7.0 provides a set of new features for Authentication, Authorization, and Accounting (AAA). These features expand on the authentication and authorization functionality available in previous releases, such as determining which user could access restricted services by assigning predefined privileges to groups.

In release 7.0, you can create new privileges and customize existing privileges and then assign these privileges to groups as you did in previous releases.

In addition, release 7.0 also includes these new AAA features:

- The ability to log AAA accounting information that enables you to easily audit configuration changes, maintain security, accurately allocate resources, and determine who should be billed for the use of resources.
- The ability to use a remote RADIUS server for authentication.
- The ability to configure failover capabilities to for the accounting and authentication servers.

To configure the AAA features, use the following procedures:

- [Configuring the Accounting Server, page 2](#)
- [Configuring the Authentication Server, page 4](#)
- [Configuring the AAA Policy, page 5](#)
- [Configuring Privileges, page 8](#)
- [Configuring Accounting Event Logging, page 18](#)

**REVIEW DRAFT - CISCO CONFIDENTIAL**

- [Configuring Console Authentication, page 21](#)

## Configuring the Accounting Server

You can configure up to two AAA accounting servers. Automatic failover functionality is provided if you have two accounting servers configured. In this case, 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.

For an accounting server, you can configure the following information used to log into the server:

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

**Note**

---

Only RADIUS servers are supported.

---

## Specifying AAA Accounting Settings

### SUMMARY STEPS

1. **config t**
2. **aaa accounting server remote**
3. **address *address* [port *port*] secret *secret***
4. **address *address* [port *port*] credentials hidden *cred***
5. **retries *number***
6. **timeout *seconds***
7. **end**
8. **show aaa accounting service**

**REVIEW DRAFT - CISCO CONFIDENTIAL****DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>config t</b>  <b>Example:</b> se-10-0-0-0# config t	Enters configuration mode.
<b>Step 2</b>	<b>aaa accounting server remote</b>  <b>Example:</b> se-10-0-0-0(config)# aaa accounting server remote	Enters aaa-authentication submode to enable you to configure the AAA authentication server.
<b>Step 3</b>	<b>address address [port port] secret secret</b>  <b>Example:</b> se-10-0-0-0(config)# address 10.2.2.10 prt 1808 secret ezsecret	Defines the access parameters for the AAA accounting server.
<b>Step 4</b>	<b>address address [port port] credentials hidden cred</b>  <b>Example:</b> se-10-0-0-0(config)# address 10.2.2.10 port 1808 credentials hidden "EugxIjn3MbL3WgUZUdUb90nfGW TYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3x lk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmP"	Defines the access parameters for the AAA accounting server.
<b>Step 5</b>	<b>retries number</b>  <b>Example:</b> se-10-0-0-0(config)# retries 6	Specifies the maximum number of times an AAA accounting request is retried before the accounting request fails.
<b>Step 6</b>	<b>timeout seconds</b>  <b>Example:</b> se-10-0-0-0(config)# timeout 24	Specifies the amount of time to wait before an AAA accounting request is considered to be unanswered.
<b>Step 7</b>	<b>end</b>  <b>Example:</b> se-10-0-0-0(config)# end	Exits to privileged EXEC mode.
<b>Step 8</b>	<b>show aaa accounting service</b>  <b>Example:</b> se-10-0-0-0# show aaa accounting service	(Optional) Displays the settings for the AAA accounting server.

**Examples**

The following is sample output from the **show aaa accounting service** command:

```
se-10-0-0-0# show aaa accounting service
AAA Accounting Service Configuration
Accounting: Enabled
```

## REVIEW DRAFT - CISCO CONFIDENTIAL

```
Address: 192.168.1.101 Port: 1813 Credentials:
EugxIjn3MbL3WgUZUdUb90nfGWTYHfmpSd8ZZNgd+Y9J3x1k2B35j0nfGW
TYHfmpSd8ZZNgd+Y9J3x1k2B35j0nfGWTYHfmp
Address: 192.168.1.100 Port: 1813 Credentials:
EugxIjn3MbL3WgUZUdUb90nfGWTYHfmpSd8ZZNgd+Y9J3x1k2B35j0nfGW
TYHfmpSd8ZZNgd+Y9J3x1k2B35j0nfGWTYHfmp
Timeout: 5 (sec)
Retries: 3
```

# Configuring the 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

This section covers only the first procedure. The second procedure is covered in the [“Configuring the AAA Policy” section on page 5](#).

For an AAA authentication server, you can configure the following information used to log into the server:

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

**Note**

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

## Specifying AAA Authentication Settings

### SUMMARY STEPS

1. **config t**
2. **aaa authentication server remote**
3. **address address [port port] secret secret**
4. **address address [port port] credentials hidden cred**
5. **retries number**
6. **timeout seconds**
7. **end**

**REVIEW DRAFT - CISCO CONFIDENTIAL****DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>config t</b>  <b>Example:</b> se-10-0-0-0# config t	Enters configuration mode.
<b>Step 2</b>	<b>aaa authentication server remote</b>  <b>Example:</b> se-10-0-0-0(config)# aaa authentication server remote	Enters aaa-authentication submode to enable you to configure the AAA authentication server.
<b>Step 3</b>	<b>address address [port port] secret secret</b>  <b>Example:</b> se-10-0-0-0(config)# address 10.2.2.10 port 1808 secret ezsecret	Defines the access parameters for the AAA authentication server.
<b>Step 4</b>	<b>address address [port port] credentials hidden cred</b>  <b>Example:</b> se-10-0-0-0(config)# address 10.2.2.10 port 1808 credentials hidden "EugxIjn3MbL3WgUZUdUb90nfGW TYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmP"	Defines the access parameters for the AAA authentication server.
<b>Step 5</b>	<b>retries number</b>  <b>Example:</b> se-10-0-0-0(config)# retries 6	Specifies maximum number of times an AAA authentication request is retried before the authentication request fails.
<b>Step 6</b>	<b>timeout seconds</b>  <b>Example:</b> se-10-0-0-0(config)# timeout 24	Specifies the amount of time to wait before an AAA authentication request is considered unanswered.
<b>Step 7</b>	<b>end</b>  <b>Example:</b> se-10-0-0-0(config)# end	Exits to privileged EXEC mode.

## Configuring the AAA Policy

The AAA policy specifies the failover functionality that you can optionally configure for the authentication server. You can choose from two types of failover functionality:

- Authentication failover
- Unreachable failover

You can also use a combination of both failover methods.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

## 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:

- Only the local database
- Only the remote server
- 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, users of the TUI, VVE, AvT, and IMAP interfaces must be configured locally in order to gain access. 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. Any security features such as password expiration, must be configured separately for Cisco Unity Express and the RADIUS server. Also, Cisco Unity Express users are not prompted when security events, such as password expiration or account lockout, occur on the RADIUS server, and vis versa.
- 

## Unreachable Failover

The unreachable failover 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, messages are sent to users to notify them when a RADIUS server:

- Cannot be reached
- Fails to authenticate the user

## Example

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 is a sequence of events that 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.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

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.

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

### SUMMARY STEPS

1. `config t`
2. `aaa policy system`
3. `authentication-order {remote [local] | local [remote]}`
4. `authorization merge-attributes`
5. `end`
6. `show aaa policy`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>config t</code>  <b>Example:</b> <code>se-10-0-0-0# config t</code>	Enters configuration mode.
Step 2	<code>aaa policy system</code>  <b>Example:</b> <code>se-10-0-0-0(config)# aaa policy system</code>	Enters aaa-authentication submode to enable you to specify the policy that controls the behavior of authentication and authorization.
Step 3	<code>authentication-order {remote [local]   local [remote]}</code>  <b>Example:</b> <code>se-10-0-0-0(config)# authentication-order remote local</code>	Specifies the order in which to query the authentication servers and local authentication database.
Step 4	<code>authorization merge-attributes</code>  <b>Example:</b> <code>se-10-0-0-0(config)# authorization merge-attributes</code>	Specifies whether the user attributes that are retrieved from a remote RADIUS AAA server are merged with attributes for the same username found in the local user database.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

	Command or Action	Purpose
Step 5	<b>end</b>  <b>Example:</b> se-10-0-0-0(config)# end	Exits to privileged EXEC mode.
Step 6	<b>show aaa accounting policy</b>  <b>Example:</b> se-10-0-0-0# show aaa policy	(Optional) Displays the AAA policy settings.

**Examples**

The following is sample output from the **show aaa policy** command:

```
se-10-0-0-0# show aaa policy
authentication-order local
merge-attributes enable
preferred-server remote
```

## Configuring Privileges

Cisco Unity Express software provides several predefined privileges that you can assign to groups. Starting with 7.0, you can also create your own privileges and modify the predefined privileges.

When you assign a privilege to a group, any member of the group is granted the privilege rights. An administrator group is created automatically by the software initialization process from the imported subscribers designated as administrators.

When you create or modify privileges, you add or delete the operations allowed by that privilege. Operations define the CLI commands and GUI functions that are allowed. In addition to adding operations to a privilege, you can also configure a privilege to have another privilege nested inside of it. A privilege configured with a nested privilege includes all operations configured for the nested privilege.

As part of the planning process, you should decide:

- How many categories of user privileges you want to create for your company.
- Which functions each privilege will allow your users to perform.

After you decide which privileges you want your users to have:

1. Review the predefined privileges to determine whether any of them are similar to the permissions that you want to give to each of your categories of users.
2. Configure a separate privilege for each category by specifying which operations each category of users will be allowed to perform, optionally including predefined privileges (see [“Creating and Customizing Privileges” on page 15](#)).
3. Create a group for each category of user privilege and assign the appropriate privilege to each group of users (see [“Adding and Modifying a Group” on page 7](#)).
4. Add your users to the appropriate group.

**Tip**

For an example of the commands used for these steps, see the [“Configuration Example” section on page 13](#).



**REVIEW DRAFT - CISCO CONFIDENTIAL****Note**

You cannot modify the superuser privilege.

Table 9-1 describes the predefined privileges provided with the Cisco Unity Express software and the operations associated with them. Table 9-2 describes all available operations that you can add to privileges.

**Note**

Two new permissions were added in 7.0: manage-users and manage-passwords.

To display a list of privileges, use the **show privileges** command in Cisco Unity Express EXEC mode. To display detailed information about a specific privilege, use the **show privilege detail** command.

**Note**

Users do not need privileges to access their own data. The user's data is primarily associated with the voice mail application and includes the user's:

- Language (configured for the user's voice mailbox)
- Password
- PIN
- Membership to groups owned by the user
- Ownership of groups owned by the user
- Notification profile
- Cascade settings
- Personal voice mail zero out number
- Voice mail greeting type
- Voice mail play tutorial flag
- Public distribution lists owned by the user
- Private distribution lists

**Table 9-1 Privileges**

Privilege	Description	Operations
Superuser	Grants unrestricted system access.	all
Manageprompts	Allows subscriber access to the AvT prompt management but not to any other administrative functions.	prompt.modify, system.debug
Broadcast	Allows subscribers to send broadcast messages across the network.	broadcast.local, broadcast.remote, system.debug
Local-broadcast	Allows subscribers to send broadcast messages only to subscribers on the local network.	broadcast.local, system.debug
ManagePublicList	Allows subscribers to create and modify public distribution lists.	voicemail.lists. public, system.debug

**REVIEW DRAFT - CISCO CONFIDENTIAL****Table 9-1 Privileges (continued)**

Privilege	Description	Operations
ViewPrivateList	Allows subscribers to view another subscriber's private distribution lists. The subscriber cannot modify or delete the private lists.	voicemail.lists.private.view
vm-imap	Allows subscribers to access the IMAP feature.	voicemail.imap.user
ViewHistorical Reports	Allows subscribers to view historical reports.	report.historical
ViewRealTime Reports	Allows subscribers to view real-time reports	report.realtime
manage-users	Allows subscribers to create, modify, and delete users	user.configuration, user.pin, user.password, user.mailbox, user.notification, user.remote, group.configuration, system.debug
manage-passwords	Allows subscribers to create, modify, and delete user passwords and PINs	user.pin, user.password, system.debug

**Table 9-2 Operations**

Operation	Description
broadcast.local	Create and send broadcast messages to local locations. Delete or reschedule broadcast messages.
broadcast.remote	Create and send broadcast messages to remote and local locations.
call.control	Configure settings for Cisco Unified CME (SIP) and Cisco Unified Communications Manager (JTAPI).
group.configuration	Create, modify, and delete groups.
network.location	Create, modify, and delete network locations, network location caching, and NDR/DDR configuration.
prompt.modify	Create, modify, and delete system prompts for AA scripts. Also includes upload/download of prompts on the CLI.
report.historical.manage	Configure and generate historical reports. Collect data from Cisco Unity Express using the <b>copy</b> command.
report.historical.view	View historical reports
report.realtime	Run and view real-time reports.
report.voicemail	Run and view voice mail reports.
restriction.tables	Create, modify, and delete restriction tables.

**REVIEW DRAFT - CISCO CONFIDENTIAL****Table 9-2 Operations (continued)**

Operation	Description
script.modify	Create, modify, and delete system AA scripts. Also include upload and download of scripts on the CLI and Editor Express.
security.aaa	Configure and view AAA service settings.
security.access	Configure system level security regarding encryption of data, including defining crypto keys.  <b>Note</b> Also includes permission to reload the system.
security.configuration	Configure settings for the system password/PIN and policy, such as: <ul style="list-style-type: none"> <li>• Expiry</li> <li>• Lockout (temporary and permanent)</li> <li>• History</li> <li>• Length</li> </ul>
services.configuration	Configure system services: DNS, NTP/clock, SMTP, SNMP, Fax Gateway, Cisco UMG, hostname, domain, interfaces (counters) and system default language.  <b>Note</b> Also includes permission to reload the system.
services.manage	System level services commands not related to configuration like clearing DNS cache and ping
site.configuration	Create, modify, or delete sites for use with Cisco UMG.
software.install	Install, upgrade, or inspect system software or addons such as languages and licenses.  <b>Note</b> Also includes permission to reload the system.
spokenname.modify	Create, modify, and delete spoken names for remote locations, remote users, and public distribution lists. Copy spoken names.
system.application	Configure system applications, such as voice mail, auto-attendant, PromptManagement, and so on.
system.backup	Configure backup.
system.calendar	Create, modify, and delete system schedules and holidays.
system.debug	Collect and configure trace and debug data. Includes copying data like core and log files.
system.documents	Manage tiff, general, and template documents.

**REVIEW DRAFT - CISCO CONFIDENTIAL****Table 9-2 Operations (continued)**

Operation	Description
system.numbers	Create, modify, and delete call-in numbers for voice mail, AA, AvT, and IVR. This includes SIP, JTAPI, and HTTP triggers.
system.sessions	Terminate others voice mail sessions (VVE, SIP, or JTAPI). Unlock locked mailboxes.
system.view	View system settings and configuration.
user.configuration	Create, modify, and delete users and groups, including the configuration of: <ul style="list-style-type: none"> <li>• First and Last Name</li> <li>• Nickname</li> <li>• Display Name</li> <li>• Language</li> </ul>
user.mailbox	Create, modify, and delete a user or group voice mailbox.
user.notification	Set or change others notification/cascade profiles.
user.password	Create, set, or remove others passwords.
user.pin	Create, set, or remove others pins.
user.remote	Create, modify, and delete remote users.
voicemail.configuration	Configure system-level voice-mail features: <ul style="list-style-type: none"> <li>• Mailboxes</li> <li>• Fax</li> <li>• Notification/cascade</li> <li>• Non-subscriber options</li> <li>• Broadcast</li> <li>• TUI config</li> <li>• Live-record</li> <li>• Live-reply</li> <li>• IMAP</li> <li>• VVE</li> </ul>
voicemail.imap.user	Manage personal voice mail via IMAP client.
voicemail.mwi	Reset/Refresh phone message waiting indicators. Configure SIP MWI delivery.
voicemail.lists.private	Create, modify, and delete others private voice mail lists.
voicemail.lists.public	Create, modify, and delete public voice mail distribution lists.
voicemail.lists.private.view	(GUI Only) View others private voice mail lists.

**REVIEW DRAFT - CISCO CONFIDENTIAL****Table 9-2 Operations (continued)**

Operation	Description
webapp.modify	Deploy web applications on Cisco Unity Express.
webapp.control	Start, stop, or restart web applications.

## Configuration Example

In this example, a company wants a security structure with two levels of security administration. The two levels allow the following actions to be taken by the administrator:

- The first level enables the security administrator to reset the passwords and PINs for users that have locked themselves out of the system, whether they forgot their password or their account is locked because of too many failed login attempts. This level will be called PASSWORD RESET.
- The second level enables the security administrator to act as a system guardian by:
  - Ensuring that the proper security policies are implemented for issues such as password aging, account lockout, encryption, authentication, authorization, and accounting
  - Ensuring that voicemail messages and other data remain safe from attackers without overburdening end users with security related details and tasks
  - Monitoring the system to ensure that only legitimate users have access
  - Troubleshooting any problems that legitimate users have with accessing the system
  - Resetting passwords and PINs for users that have locked themselves out of the system, whether they forgot their password or their account is locked because of too many failed login attempts

This level will be called SYSTEM GUARDIAN

When you use the general planning and configuration steps as described in the “[Configuring Privileges](#)” section on page 8, to set up the security administration levels for this example, these are the results:

- You have already decided:
  - How many levels or categories of user privileges you want to create for your company
  - Which functions each privilege will allow your users to perform

There will be two levels, called PASSWORD RESET and SYSTEM GUARDIAN, as described above.

- After reviewing the predefined privileges to determine whether any of them are similar to the permissions that you want to give each of your security levels, you find that:
  - The predefined privilege called *manage-passwords* can be used for the security level named PASSWORD RESET because it has all of the permissions needed to help users that have locked themselves out of the system.
  - The *manage-passwords* privilege also has a subset of the permissions needed the security level named SYSTEM GUARDIAN and is the predefined privilege closest to your requirements. However, to act as system guardian, the following additional operations will have to included: *security.access*, *security.aaa*, *security.password*, *security.pin*, *system.debug*, and *system.view*. See [Table 9-2 on page 10](#) for more information.
- Use the following commands to configure a privilege for the SYSTEM GUARDIAN security level by including the predefined privilege *manage-password* and adding the operations listed in the previous bullet:

```
se-10-0-0-0(config)# privilege guardian-privilege create
```

**REVIEW DRAFT - CISCO CONFIDENTIAL**

```

se-10-0-0-0(config)# privilege guardian-privilege member manage-passwords
se-10-0-0-0(config)# privilege guardian-privilege operation security.access
se-10-0-0-0(config)# privilege guardian-privilege operation security.aaa
se-10-0-0-0(config)# privilege guardian-privilege operation security.password
se-10-0-0-0(config)# privilege guardian-privilege operation security.pin
se-10-0-0-0(config)# privilege guardian-privilege operation system.debug
se-10-0-0-0(config)# privilege guardian-privilege operation system.view

```

**Note**

You do not have to configure a privilege for the PASSWORD RESET security level because you can use the predefined privilege *manage-passwords*.

- Use the following commands to create a new group called *password-reset* and assign the privilege called *manage-passwords* to it:

```

se-10-0-0-0(config)# groupname password-reset create
se-10-0-0-0(config)# groupname password-reset privilege manage-passwords

```

- Use the following commands to create a new group called *system-guardian* and assign the privilege called *guardian-privilege*:

```

se-10-0-0-0(config)# groupname system-guardian create
se-10-0-0-0(config)# groupname system-guardian privilege guardian-privilege

```

- Assign the appropriate users to the new groups, associating them with their roles. For example, if you want Bob and Ned to have the privileges of the PASSWORD RESET security administration level and Ann to have the privileges of the SYSTEM GUARDIAN security administration level, use the following commands:

```

se-10-0-0-0(config)# groupname password-reset member bob
se-10-0-0-0(config)# groupname password-reset member ned
se-10-0-0-0(config)# groupname system-guardian member ann

```

- The configuration of this example is now complete. You can verify your configuration using the following commands.

The following is sample output from the **show group detail groupname password-reset expanded** command:

```

se-10-0-0-0# show group detail groupname password-reset expanded
Groupname:          password-reset
Full Name:          password-reset
Description:
Email:
Epage:

Group Members:      <none>
User Members:       bob ned
Group Owners:       <none>
User Owners:        <none>
Privileges:         manage-passwords

```

The following is sample output from the **show group detail groupname system-guardian expanded** command:

```

se-10-0-0-0# show group detail groupname system-guardian expanded
Groupname:          system-guardian
Full Name:          system-guardian
Description:
Email:
Epage:

Group Members:      <none>

```

**REVIEW DRAFT - CISCO CONFIDENTIAL**

```

User Members:      ann
Group Owners:      <none>
User Owners:       <none>
Privileges:        guardian-privilege

```

The following is sample output from the **show privilege detail manage-passwords expanded** command:

```

se-10-0-0-0# show privilege detail manage-passwords expanded
Privilege:         manage-passwords
Description:       Privilege to reset user passwords

Privilege Members: <none>
Operations:        system.debug user.password user.pin

```

The following is sample output from the **show privilege detail guardian-privilege expanded** command:

```

se-10-0-0-0# show privilege detail guardian-privilege expanded
Privilege:         guardian-privilege
Description:

Privilege Members: manage-passwords
Operations:        security.aaa security.access security.password security.pin
                  system.debug system.view
manage-passwords: system.debug user.password user.pin

```

## Creating and Customizing Privileges

### SUMMARY STEP

1. **config t**
2. **privilege *privilege-name* create**
3. **privilege *privilege-name* description *string***
4. **privilege *privilege-name* operation *operation-name***
5. **privilege *privilege-name* member *privilege-name2***
6. **end**
7. **show operations**
8. **show operation detail *operation-name***
9. **show privileges**
10. **show privilege detail *privilege-name***

**REVIEW DRAFT - CISCO CONFIDENTIAL****DETAILED STEPS**

	Command or Action	Purpose
Step 1	<b>config t</b>  <b>Example:</b> se-10-0-0-0# config t	Enters configuration mode.
Step 2	<b>privilege privilege-name create</b>  <b>Example:</b> se-10-0-0-0(config)# privilege security-privilege create	Creates a new privilege. <ul style="list-style-type: none"> <li><i>privilege-name</i>—Label used to identify and configure a new or existing privilege.</li> </ul>
Step 3	<b>privilege privilege-name [description string]</b>  <b>Example:</b> se-10-0-0-0(config)# privilege security-privilege description administer of system security	(Optional) Assigns a description to the privilege. <ul style="list-style-type: none"> <li><i>string</i>—Description to add to the privilege.</li> </ul>
Step 4	<b>privilege privilege-name operation operation-name</b>  <b>Example:</b> se-10-0-0-0(config)# privilege security-privilege operation security.configuration	(Optional) Assigns an operation to the privilege: <ul style="list-style-type: none"> <li><i>operation-name</i>—Operation to associate with the privilege.</li> </ul>
Step 5	<b>privilege privilege-name member privilege-name2</b>  <b>Example:</b> se-10-0-0-0(config)# privilege security-privilege include manage-users	(Optional) Includes or nests another privilege into this privilege: <ul style="list-style-type: none"> <li><i>privilege-name2</i>—Privilege to include or nest into this privilege.</li> </ul>
Step 6	<b>end</b>  <b>Example:</b> se-10-0-0-0(config)# end	Exits to privileged EXEC mode.
Step 7	<b>show operations</b>  <b>Example:</b> se-10-0-0-0# show operations	(Optional) Displays information about all operations.
Step 8	<b>show operation detail operation-name</b>  <b>Example:</b> se-10-0-0-0# show operation detail security.configuration	(Optional) Displays information about the specified operation: <ul style="list-style-type: none"> <li><i>operation-name</i>—Label used to identify and configure a new or existing operation.</li> </ul>



**REVIEW DRAFT - CISCO CONFIDENTIAL**

	Command or Action	Purpose
Step 9	<b>show privileges</b>  <b>Example:</b> se-10-0-0-0# show privilege	(Optional) Displays information about all privileges.
Step 10	<b>show privilege detail <i>privilege-name</i></b>  <b>Example:</b> se-10-0-0-0# show privilege detail sales_vp	(Optional) Displays information about the specified privilege: <ul style="list-style-type: none"> <li><i>privilege-name</i>—Label used to identify and configure a new or existing privilege.</li> </ul>

**Examples**

The following is sample output from the **show operations** command:

```
se-10-0-0-0# show operations
show operations
broadcast.local
broadcast.remote
call.control
database.enterprise
group.configuration
network.location
prompt.modify
report.historical.manage
report.historical.view
report.realtime
report.voicemail
restriction.tables
script.modify
security.aaa
security.access
security.password
security.pin
services.configuration
services.exec
services.manage
site.configuration
software.install
spokenname.modify
system.application
system.backup
system.calendar
system.configuration
system.debug
system.documents
system.numbers
system.sessions
system.view
user.configuration
user.mailbox
user.notification
user.password
user.pin
user.remote
user.supervisor
voicemail.configuration
voicemail.imap.user
voicemail.lists.private.view
voicemail.lists.public
```

**REVIEW DRAFT - CISCO CONFIDENTIAL**

```
voicemail.mwi
webapp.control
webapp.modify

46 total operation(s)
```

The following is sample output from the **show operation detail** command:

```
se-10-0-0-0# show operation detail user.password
Operation:      user.password
Description:    Set and reset passwords for other users
CLI:
               config-user-password
               exec-configure-terminal
               exec-copy-running-config-startup-config
               exec-show-user-auth
               exec-user-password
               exec-write

6 total command(s)
```

The following is sample output from the **show privileges** command:

```
se-10-0-0-0# show privileges
ManagePrompt
ManagePublicList
ViewHistoricalReports
ViewPrivateList
ViewRealTimeReports
broadcast
local-broadcast
manage-password
manage-users
superuser
vm-imap

11 total privilege(s)
```

The following is sample output from the **show privilege detail** command:

```
se-10-0-0-0# show privilege detail ManagePrompt
Privilege:      ManagePrompt
Description:    Privilege to create, modify, or delete system prompts
Privilege Members:  user1, user2
Operations:     prompt.modify system.debug
```

## Configuring 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:

**REVIEW DRAFT - CISCO CONFIDENTIAL**

- 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:

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

The detailed content of the log entries is explained in the [“Examples” section on page 21](#).

**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 Accounting Event Logging

### SUMMARY STEPS

1. **config t**
2. **aaa accounting enable**
3. **aaa accounting event**
4. **login**
5. **logout**
6. **login-fail**
7. **config-commands**
8. **exec-commands**
9. **system-startup**
10. **system-shutdown**
11. **end**
12. **show aaa accounting event**

**REVIEW DRAFT - CISCO CONFIDENTIAL****DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>config t</b>  <b>Example:</b> se-10-0-0-0# config t	Enters configuration mode.
<b>Step 2</b>	<b>aaa accounting enable</b>  <b>Example:</b> se-10-0-0-0(config)# aaa accounting enable	Enables the recording of AAA account events.
<b>Step 3</b>	<b>aaa accounting event</b>  <b>Example:</b> se-10-0-0-0(config)# aaa accounting event	Enters aaa-accounting submode to enable you to configure event filtering for accounting packets.
<b>Step 4</b>	<b>login</b>  <b>Example:</b> se-10-0-0-0(config)# login	Enables the logging of logins.
<b>Step 5</b>	<b>logout</b>  <b>Example:</b> se-10-0-0-0(config)# logout	Enables the logging of logouts
<b>Step 6</b>	<b>login-fail</b>  <b>Example:</b> se-10-0-0-0(config)# login-fail	Enables the logging of failed logins.
<b>Step 7</b>	<b>config-commands</b>  <b>Example:</b> se-10-0-0-0(config)# config-commands	Enables the logging of configuration mode commands.
<b>Step 8</b>	<b>exec-commands</b>  <b>Example:</b> se-10-0-0-0(config)# exec-commands	Enables the logging of configuration mode commands.
<b>Step 9</b>	<b>system-startup</b>  <b>Example:</b> se-10-0-0-0(config)# system-startup	Enables the logging of system startups.
<b>Step 10</b>	<b>system-shutdown</b>  <b>Example:</b> se-10-0-0-0(config)# system-shutdown	Enables the logging of system shutdowns.

**REVIEW DRAFT - CISCO CONFIDENTIAL**

	Command or Action	Purpose
Step 11	<b>end</b>  <b>Example:</b> se-10-0-0-0(config)# end	Exits to privileged EXEC mode.
Step 12	<b>show aaa accounting event</b> se-10-0-0-0# show aaa accounting	(Optional) Displays the AAA accounting events that are designated to be logged.

**Examples**

The following is sample output from the **show aaa accounting event** command:

```
se-10-0-0-0# show aaa accounting event
Event      State      Description
login      Enabled    Log accounting events for successful login
logout     Enabled    Log accounting events for user logout
login-fail  Enabled    Log accounting events for failed login attempts
config-commands Enabled    Log accounting events for any changes to configuration
exec-commands Enabled    Log accounting events for execution of commands
system-startup Enabled    Log accounting events for system startup
system-shutdown Enabled    Log accounting events for system shutdown
imap       Enabled    Log accounting events for all imap events
```

## Configuring Console Authentication

By default, console authentication is disabled, allowing any user logging into the system through the console to have superuser privileges and to log in without providing a username or password.

Therefore, to protect your console from unauthorized access, you must enter the **login** command in config-line mode, as described below.

**Note**

To see whether authentication is enabled for the console, you must view the running configuration.

## Specifying Whether the Console Connection is Subject to Authentication

**SUMMARY STEPS**

1. **config t**
2. **line console**
3. **login**
4. **end**

**REVIEW DRAFT - CISCO CONFIDENTIAL****DETAILED STEPS**

	Command or Action	Purpose
Step 1	<b>config t</b>  <b>Example:</b> se-10-0-0-0# config t	Enters configuration mode.
Step 2	<b>line console</b>  <b>Example:</b> se-10-0-0-0(config)# line console	Enters config-line mode to enable you to specify whether the console connection is subject to authentication.
Step 3	<b>login</b>  <b>Example:</b> se-10-0-0-0(config-line)# line console	Requires that any user logging in through the console connection is subject to authentication. The <b>no</b> or <b>default</b> form of this command disables authentication for the console.
Step 4	<b>end</b>  <b>Example:</b> se-10-0-0-0(config)# end	Exits to privileged EXEC mode.