



Configuring Privileges

- [Viewing Privileges](#)
- [Overview of Privileges](#)
- [Creating a New Privilege](#)
- [Deleting a Privilege](#)
- [Customizing an Existing Privilege](#)

Viewing Privileges

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 > Privileges .

The system displays the Configure Privileges page. |
| Step 3 | To see a different number of privileges on each page, on the top right, choose another number from the drop-down box and click Go . You can choose to see 10, 25, 50, 100, or 500 privileges. |
| Step 4 | To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press Enter . |
| Step 5 | To sort the privileges, click any header. |
-

Overview of Privileges

Cisco Unified SRSV provides one predefined privilege, called superuser, that you can assign to groups. This privilege grants unrestricted system access and includes all operations. You can also create your own privileges and modify the predefined privileges.

When you assign a [privilege](#) to a group, each member of the group is granted the privilege rights. The software initialization process automatically creates an administrator group from the imported subscribers designated as administrators.

When you create or modify privileges, you add or delete the operations allowed by that privilege. An [operation](#) defines the CLI commands and GUI functions that are allowed. Most operations include only one CLI command and GUI function. 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.

[Table 7](#) describes all available operations that you can add to privileges.

To display a list of privileges, use the **show privileges** command in 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. A user's data is primarily associated with the voicemail application and includes the user's:

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

Table 7 **List of Operations**

Operation	Description
group.configuration	Create, modify, and delete groups.
security.aaa	Configure and modify AAA service settings.
security.access	Configure system level security regarding encryption of data, including defining crypto keys.
security.password	Configure settings for the system password and policy, such as: • Expiry • Lockout (temporary and permanent) • History • Length

Table 7 *List of Operations (continued)*

Operation	Description
security.pin	Configure settings for the system PIN and policy, such as: • Expiry • Lockout (temporary and permanent) • History • Length
services.configuration	Configure system services: DNS, NTP, SMTP, SNMP, fax gateway, Cisco UMG, hostname, domain, interfaces (counters), and system default language. Note Also includes permission to reload the system.
services.manage	System level services commands not related to configuration like clearing DNS cache and ping.
software.install	Install, upgrade, or inspect system software or add-ons such as languages and licenses. Note Also includes permission to reload the system.
srsx	Configure the SRSV-UMG application.
system.backup	Configure backup.
system.configuration	Configure system settings such as the clock, hostname, domain name, default language, and interfaces (counters).
system.debug	Collect and configure trace and debug data. Includes copying data like core and log files.
system.view	View system settings and configuration.
user.configuration	Create, modify, and delete users and groups, including the configuration of: • First and Last Name • Nickname • Display Name • Language
user.password	Create, set, or remove others passwords.
user.pin	Create, set, or remove others PINs.

Creating a New Privilege

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 > Privileges**.
The system displays the Configure Privileges page.
- Step 3** Click **Add**.
The system displays the Add page.
- Step 4** Enter a name and description for the privilege.
- Step 5** Check the operations that you want to add to the privilege.
- Step 6** Click **Add**.
-

Deleting a Privilege

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 > Privileges**.
The system displays the Configure Privileges page.
- Step 3** Select the privilege that you want to delete.
- Step 4** Click **Delete**.
-

Customizing an Existing Privilege

Restrictions

- You cannot modify the [superuser](#) privilege.
- Some operations are mandatory and cannot be removed.

Before You Begin

- Create a privilege. See [Creating a New Privilege](#).

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 > Privileges**.
The system displays the Configure Privileges page.
- Step 3** Click the name of the privilege that you want to customize.
- Step 4** Select the operations that you want to add to the privilege or deselect the operations that you want to remove.
- Step 5** Click **Apply**.
- Step 6** Click **OK** to save your changes.
-

