



## Configuring Privileges

---

- [Viewing Privileges](#)
- [Creating a Privilege](#)
- [Editing a Privilege](#)

## Viewing Privileges

### Procedure

---

- Step 1** Choose **Configure > Privileges**.
- The system displays the Configure Privileges page.
- Step 2** 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 all privileges.
- Step 3** 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 4** To sort the privileges, click any header.
- Step 5** To delete a privilege, do the following:
- a. Select the privilege to delete.
  - b. Click **Delete**.



**Tip** You cannot delete the pfsread, pfsreadwrite, or the superuser privileges. However, privileges that are linked to a group can be deleted without prior warning and this will result in the group not having any privileges.

---

### Overview of Privileges

Cisco Unified SIP Proxy provides three predefined privileges that you can assign to groups. 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. 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 28 describes all available operations that you can add to privileges.

**Note**

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

- 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 28**      *List of Operations*

<b>Operation</b>	<b>Description</b>
cuspl.configuration	Configure cuspl read and write access.
cuspl.readonlyconfiguration	Configure cuspl readonly access.
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.  <b>Note</b> Also includes permission to reload the system.

**Table 28** *List of Operations (continued)*

<b>Operation</b>	<b>Description</b>
security.password	Configure settings for the system password 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>
security.pin	Configure settings for the system 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.
software.install	Install, upgrade, or inspect system software or add-ons such as languages and licenses. <b>Note</b> Also includes permission to reload the system.
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: <ul style="list-style-type: none"> <li>• First and Last Name</li> <li>• Nickname</li> <li>• Display Name</li> <li>• Language</li> </ul>
user.password	Create, set, or remove others passwords.
user.pin	Create, set, or remove others PINs.

**Related Topics**

Back to the [Configuring Privileges](#) menu page

## Creating a Privilege

**Procedure**

---

- Step 1** Choose **Configure > Privileges**.  
The system displays the Configure Privileges page.
- Step 2** Click **Add**.
- Step 3** Enter a name and description for the privilege.
- Step 4** Check the operations to add to the privilege. See [Table 28](#).
- Step 5** Click **Add**.
- 

**Related Topics**

Back to the [Configuring Privileges](#) menu page

## Editing a Privilege

**Restrictions**

- You cannot modify the pfsread, pfsreadwrite, or the superuser privilege.
- Some operations are mandatory and cannot be removed.

**Before You Begin**

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

**Procedure**

---

- Step 1** Choose **Configure > Privileges**.  
The system displays the Configure Privileges page.
- Step 2** Click the underlined name of the privilege to customize.
- Step 3** Select the operations to add to the privilege or deselect the operations to remove.
- Step 4** Click **Apply**.
- Step 5** Click **OK** to save your changes.
- 

**Related Topics**

Back to the [Configuring Privileges](#) menu page



