Manage User Access

User Access Overview

Manage user access to Cisco Unified Communications Manager by configuring the following items:

- Access Control Groups
- Roles
- User Rank

Access Control Group Overview

An access control group is a list of users and the roles that are assigned to those users. When you assign an end user, application user, or administrator user to an access control group, the user gains the access permissions of the roles that are associated to the group. You can manage system access by assigning users with similar access needs to an access control group with only the roles and permissions that they need.

There are two types of access control groups:

- Standard Access Control Groups—These are predefined default groups with role assignments that meet common deployment needs. You cannot edit the role assignments in a standard group. However, you can add and delete users, in addition to editing the User Rank requirement. For a list of standard access control groups, and their associated roles, see Standard Roles and Access Control Groups, on page 15.
- Custom Access Control Groups—Create your own access control groups when none of the standard groups contain the role permissions that meet your needs.

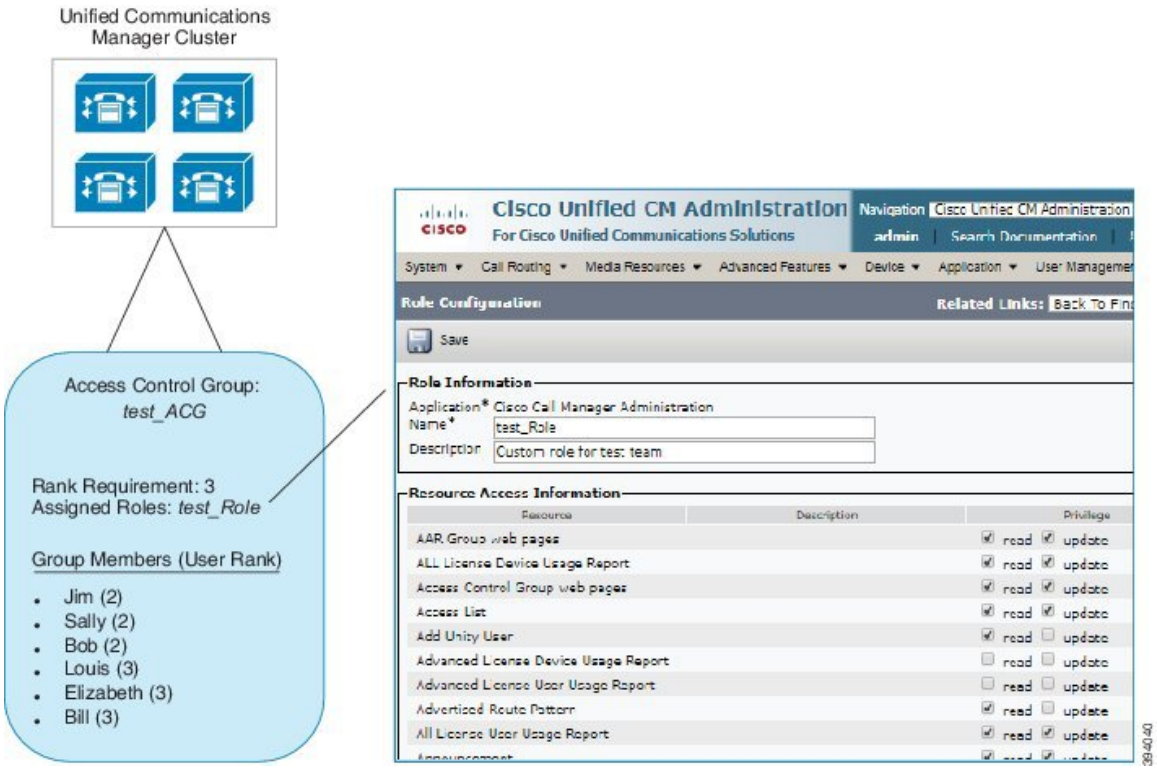
The User Rank framework provides a set of controls over the access control groups to which a user can be assigned. To be assigned to an access control group, a user must meet the minimum rank requirement for that group. For example, end users whom have a User Rank of 4 can be assigned only to access control groups

with minimum rank requirements between 4 and 10. They cannot be assigned to groups with a minimum rank of 1.

Example - Role Permissions with Access Control Groups

The following example illustrates a cluster where the members of a testing team are assigned to access control group **test_ACG**. The screen capture on the right displays the access settings of test_Role, which is the role that is associated to the access control group. Also note that the access control group has a minimum rank requirement of 3. All of the group members must have a rank between 1-3 to be able to join the group.

Figure 1: Role Permissions with Access Control Groups



Roles Overview

Users obtain system access privileges via the roles that are associated to the access control group of which the user is a member. Each role contains a set of permissions that is attached to a specific resource or application, such as Cisco Unified CM Administration or CDR Analysis and Reporting. For an application such as Cisco Unified CM Administration, the role may contain permissions that let you view or edit specific GUI pages in the application. There are three levels of permissions that you can assign to a resource or application:

- Read—Allows a user to view settings for a resource.
- Update—Allows a user to edit settings for a resource.
- No Access—If a user has neither Read or Update access, the user has no access to view or edit settings for a given resource.

Role Types

When provisioning users, you must decide what roles you want to apply and then assign users to an access control group that contains the role. There are two main types of roles in Cisco Unified Communications Manager:

- Standard roles—These are preinstalled default roles that are designed to meet the needs of common deployments. You cannot edit permissions for standard roles.
- Custom roles—Create custom roles when no standard roles have the privileges you need. In addition, if you need a more granular level of access control, you can apply advanced settings to control an administrator's ability to edit key user settings. See the below section for details.

Advanced Role Settings

For custom roles, you can add a detailed level of control to selected fields on the **Application User Configuration** and **End User Configuration** windows.

The **Advanced Role Configuration** window lets you configure access to Cisco Unified CM Administration while restricting access for tasks such as:

- Adding users
- Editing passwords
- Editing user ranks
- Editing access control groups

The following table details more controls that you can apply with this configuration:

Table 1: Advanced Resource Access Information

Advanced Resource	Access Control
Permission Information	Controls the ability to add or edit access control groups: • **View**—User can view access control groups, but cannot add, edit, or delete access control groups. • **Update**—User can add, edit, or delete access control groups. **Note** When both the values are not selected, the **Permission Information** section is not available. **Note** If you choose **View**, the **User can update Permissions Information for own user** field is set to **No** and is disabled. If you want to be able to edit this field, you must set the **Permission Information** field to **Update**.

Advanced Resource	Access Control
User can update Permissions Information for own user	Controls a user's ability to edit their own access permissions: • **Yes**—User can update their own Permission Information. • **No**—User cannot update their own Permission Information. However, the user can view or modify the permission information of same or lower ranked users. **Note** The **User can update Permissions Information for own user** field is set to **No** and is disabled if the **Permission Information Update** check box is not selected.
User Rank	Controls the ability to change the user rank: • **View**—User can view the user rank, but cannot change the user rank. • **Update**—User can change the user rank. **Note** When both the values are not selected, the **User Rank** section is not available. **Note** If you choose **View**, the **User can update User Rank for own user** field is set to **No** and is disabled. If you want to be able to edit this field, you must set the **User Rank** field to **Update**.
User can update User Rank for own user	Controls a user's ability to edit their own user rank: • **Yes**—User can update their own User Rank. • **No**—User cannot update their own User Rank. However, the user can view or modify the rank of same or lower ranked users. **Note** The **User can update User Rank for own user** field is set to **No** and is disabled, if the **User Rank Update** check box is not selected.
Add New Users	Controls the ability to add a new user: • **Yes**—User can add a new user. • **No**—The **Add New** button is not available.
Password	Controls the ability to change the password: • **Yes**—User can change the user passwords under **Application User Information** section. • **No**—The **Password** and **Confirm Password** under **Application User Information** section is not available.

User Rank Overview

The User Rank hierarchy provides a set of controls over which access control groups an administrator can assign to an end user or application user.

When provisioning end users or application users, administrators can assign a user rank for the user. Administrators can also assign a user rank requirement for each access control group. When adding users to access conttrol groups, administrators can assign users only to the groups where the user's User Rank meets the group's rank requirement. For example, an administrator can assign a user whom has a User Rank of 3 to access control groups that have a User Rank requirement between 3 and 10. However, an administrator cannot assign that user to an access control group that has a User Rank requirement of 1 or 2.

Administrators can create their own user rank hierarchy within the **User Rank Configuration** window and can use that hierarchy when provisioning users and access control groups. Note that if you don't configure a user rank hierarchy, or if you simply don't specify the User Rank setting when provisioning users or access conrol groups, all users and access control groups are assigned the default User Rank of 1 (the highest rank possible).

User Access Prerequisites

Make sure to review your user needs so that you know what level of access your users require. You will want to assign roles that have the access privileges your users require, but which do not provide access to systems that they should not be able to access.

Before you create new roles and acess control groups, review the list of standard roles and access control groups to verify whether an existing access control group has the roles and access permissions that you need. For details, see Standard Roles and Access Control Groups, on page 15.

User Access Configuration Task Flow

Complete the following tasks to configure user access.

Before you begin

If you want to use default roles and access control groups then you can skip tasks for creating customized roles and access control groups. You can assign your users to the existing default access control groups.

Procedure

	Command or Action	Purpose
Step 1	Configure User Rank Hierarchy, on page 6	Set up the user rank hierarchy. Note that if you skip this task, all users and access control groups get assigned the default user rank of 1 (the highest rank).
Step 2	Create a Custom Role, on page 6	Create custom roles if the default roles don't have the access permissions you need.
Step 3	Configure Advanced Role for Administrators, on page 7	Optional. Advanced permissions in a custom role let you control an administrator’s ability to edit key user settings.
Step 4	Create Access Control Group, on page 8	Create custom access control groups if the default groups don't have the role assignments you need.

	Command or Action	Purpose
Step 5	Assign Users to Access Control Group, on page 8	Add or delete users from a standard or custom access control group.
Step 6	Configure Overlapping Privilege Policy for Access Control Groups, on page 9	Optional. This setting is used if users are assigned to multiple access control groups with conflicting permissions.

Configure User Rank Hierarchy

Use this procedure to create a custom user rank hierarchy.

Note If you don't configure a user rank hierarchy, all users and access control groups get assigned a user rank of 1 (the highest possible rank) by default.

Procedure

Step 1 From Cisco Unified CM Administration, choose**User Management** > **User Settings** > **User Rank**.

Step 2 Click **Add New**.

Step 3 From the **User Rank** drop-down menu, select a rank setting between 1–10. The highest rank is 1.

Step 4 Enter a **Rank Name** and **Description**.

Step 5 Click **Save**.

Step 6 Repeat this procedure to add additional user ranks.
You can assign the user rank to users and access control groups to control which groups a user can be assigned to.

Create a Custom Role

Use this procedure to create a new role with customized privileges. You may want to do this if there are no standard roles with the exact privileges that you need. There are two ways to create a role:

- Use the **Add New** button to create and configure the new role from scatch.
- Use the **Copy** button if an existing role has access privileges that are close to what you need. You can copy the privileges of the existing role to a new role that is editable.

Procedure

Step 1 In Cisco Unified CM Administration, click **User Management** > **User Settings** > **Role**.

Step 2 Do either of the following:

- To create a new role, click **Add New**. Choose the **Application** with which this role associates, and click **Next**.
- To copy settings from an existing role, click **Find** and open the existing role. Click **Copy** and enter a name for the new role. Click **OK**.

Step 3 Enter a **Name** and **Description** for the role.

Step 4 For each resource, check the boxes that apply:

- Check the **Read** check box if you want users to be able to view settings for the resource.
- Check the **Update** check box if you want users to be able to edit setttings for the resource.
- Leave both check boxes unchecked to provide no access to the resource.

Step 5 Click **Grant access to all** or **Deny access to all** button to grant or remove privileges to all resources that display on a page for this role.

Note If the list of resources displays on more than one page, this button applies only to the resources that display on the current page. You must display other pages and use the button on those pages to change the access to the resources that are listed on those pages.

Step 6 Click **Save**.

Configure Advanced Role for Administrators

Advanced Role Configuration lets you edit permissions for a custom role at a more granular level. You can control an administrator's ability to edit the following key settings in the **End User Configuration** and **Application User Configuration** windows:

- Editing User Ranks
- Editing Access Control Group assignments
- Adding new users
- Editing user passwords

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Role**.

Step 2 Click **Find** and select a custom role.

Step 3 From **Related Links**, select **Advanced Role Configuration** and click **Go**.

Step 4 From the **Resource Web Page**, select **Application User Web Pages** or **User Web Pages**.

Step 5 Edit the settings. Refer to the online help for help with the fields and their settings.

Step 6 Click **Save**.

Create Access Control Group

Use this procedure if you need to create a new access control group. You may want to do this if no standard group has the roles and access privileges you need. There are two ways to create a customized group:

- Use the **Add New** button to create and configure the new access control group from scatch.
- Use the **Copy** button if an existing group has role assignments that are close to what you need. You can copy the settings from the existing group to a new and editable group.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Groups.**

Step 2 Do either of the following:

- To create a new group from scratch, click **Add New**.
- To copy settings from an existing group, click **Find** and open the existing access control group. Click **Copy** and enter a name for the new group. Click **OK**.

Step 3 Enter a **Name** for the access control group.

Step 4 From the **Available for Users with User Rank as** drop-down, select the minimum User Rank a user must meet to be assigned to this group. The default user rank is 1.

Step 5 Click **Save**.

Step 6 Assign roles to the access control group. The roles you select will be assigned to group members:

a) From **Related Links**, select **Assign Role to Access Control Group**, and click **Go**.
b) Click **Find** to search for existing roles.
c) Check the roles that you want to add and click **Add Selected**.
d) Click **Save**.

What to do next

Assign Users to Access Control Group, on page 8

Assign Users to Access Control Group

Add or delete users from a standard or custom access control group. .

Note You can add only those users whose user rank is the same or higher than the minimum user rank for the access control group.

Note If you are syncing new users from a company LDAP Directory, and your rank hierarchy and access control groups are created with the appropriate permissions, you can assign the group to synced users as a part of the LDAP sync. For details on how to set up an LDAP directory sync, see the *System Configuration Guide for Cisco Unified Communications Manager.*

Procedure

Step 1 Choose **User Management** > **User Settings** > **Access Control Group**.

The **Find and List Access Control Group** window appears.

Step 2 Click **Find** and select the access control group for which you want to update the list of users.

Step 3 From the **Available for Users with User Rank as** drop-down, select the rank requirement that users must meet to be assigned to this group.

Step 4 In the **User** section, click **Find** to display the list of users.

Step 5 If you want to add end users or application users to the access control group, do the following:

a) Click **Add End Users to Access Control Group** or **Add App Users to Access Control Group**.
b) Select the users whom you want to add.
c) Click **Add Selected**.

Step 6 If you want to delete users from the access control group:

a) Select the users whom you want to delete.
b) Click **Delete Selected**.

Step 7 Click **Save**.

Configure Overlapping Privilege Policy for Access Control Groups

Configure how Cisco Unified Communications Manager handles overlapping user privileges that can result from access control group assignments. This is to cover situations where an end user is assigned to multiple access control groups, each with conflicting roles and privilege settings.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Under **User Management Parameters**, configure one of the following values for the **Effective Access Privileges For Overlapping User Groups and Roles** as follows:

- **Maximum**—The effective privilege represents the maximum of the privileges of all the overlapping access control groups. This is the default option.
- **Minimum**—The effective privilege represents the minimum of the privileges of all the overlapping access control groups.

Step 3 Click **Save**.

View User Privilege Report

Perform the following procedure to view the User Privilege report for either an existing end user or an existing application user. The User Privilege report displays the access control groups, roles, and access privileges that are assigned to an end user or application user.

Procedure

Step 1 In Cisco Unified CM Administration, perform either of the following steps:

- For end users, choose **User Management** > **End User**.
- For application users, choose **User Management** > **Application User**.

Step 2 Click **Find** and select the user for whom you want to view access privileges

Step 3 From the **Related Links** drop-down list, choose the **User Privilege Report** and click **Go**.
The User Privilege window appears.

Create Custom Help Desk Role Task Flow

Some companies want their help desk personnel to have privileges to be able to perform certain administrative tasks. Follow the steps in this task flow to configure a role and access control group for help desk team members that allows them to perform tasks such as adding a phone and adding an end user.

Procedure

	Command or Action	Purpose
Step 1	Create Custom Help Desk Role, on page 11	Create a custom role for help desk team members and assign the role privileges for items such as adding new phones and adding new users.
Step 2	Create Custom Help Desk Access Control Group, on page 11	Create a new access control group for the Help Desk role.
Step 3	Assign Help Desk Role to Access Control Group, on page 11	Assign the Help Desk role to the Help Desk access control group. Any users assigned to this access control group will be assigned the privileges of the Help Desk role.
Step 4	Assign Help Desk Members to Access Control Group, on page 12	Assign help desk team members with the privileges of the custom help desk role.

Create Custom Help Desk Role

Perform this procedure to create a custom help desk role that you can assign to help desk members in your organization.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **User Management** > **User Settings** > **Role**.

Step 2 Click **Add New**.

Step 3 From the Application drop-down list, choose the application that you want to assign to this role. For example, **Cisco CallManager Administration**.

Step 4 Click **Next**.

Step 5 Enter the **Name** of the new role. For example, **`Help Desk`**.

Step 6 Under **Read and Update Privileges** select the privileges that you want to assign for help desk users. For example, if you want help desk members to be able to add users and phones, check the **Read** and **Update** check boxes for User web pages and Phone web pages.

Step 7 Click **Save**.

What to do next

Create Custom Help Desk Access Control Group, on page 11

Create Custom Help Desk Access Control Group

Before you begin

Create Custom Help Desk Role, on page 11

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Group**.

Step 2 Click **Add New**.

Step 3 Enter a name for the access control group. For example, **`Help_Desk`**.

Step 4 Click **Save**.

What to do next

Assign Help Desk Role to Access Control Group, on page 11

Assign Help Desk Role to Access Control Group

Perform the following steps to configure the Help Desk access control group with the privileges from the Help Desk role.

Before you begin

Create Custom Help Desk Access Control Group, on page 11

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Group**.

Step 2 Click **Find** and select the access control group that you created for Help Desk.
The **Access Control Group Configuration** window displays.

Step 3 In the **Related Links** drop-down list box, choose the **Assign Role to Access Control Group** option and click **Go**.
The **Find and List Roles** popup displays.

Step 4 Click the **Assign Role to Group** button.

Step 5 Click **Find** and select the Help Desk role.

Step 6 Click **Add Selected**.

Step 7 Click **Save**.

What to do next

Assign Help Desk Members to Access Control Group, on page 12

Assign Help Desk Members to Access Control Group

Before you begin

Assign Help Desk Role to Access Control Group, on page 11

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Group.**

Step 2 Click **Find** and select the custom Help Desk access control group that you created.

Step 3 Perform either of the following steps:

- If your help desk team members are configured as end users, click **Add End Users to Group**.
- If your help desk team members are configured as application users, click **Add App Users to Group**.

Step 4 Click **Find** and select your help desk users.

Step 5 Click **Add Selected**.

Step 6 Click **Save**.
Cisco Unified Communications Manager assigns your help desk team members with the privileges of the custom help desk role that you created.

Delete Access Control Group

Use the following procedure to delete an access control group entirely.

Before you begin

When you delete an access control group, Cisco Unified Communications Manager removes all access control group data from the database. Ensure you are aware which roles are using the access control group.

Procedure

Step 1 Choose **User Management** > **User Settings** > **Access Control Group**.

The **Find and List Access Control Groups** window appears.

Step 2 Find the access control group that you want to delete.

Step 3 Click the name of the access control group that you want to delete.

The access control group that you chose appears. The list shows the users in this access control group in alphabetical order.

Step 4 If you want to delete the access control group entirely, click **Delete**.

A dialog box appears to warn you that you cannot undo the deletion of access control groups.

Step 5 To delete the access control group, click **OK** or to cancel the action, click **Cancel**. If you click **OK**, Cisco Unified Communications Manager removes the access control group from the database.

Revoke Existing OAuth Refresh Tokens

Use an AXL API to revoke existing OAuth refresh tokens. For example, if an employee leaves your company, you can use this API to revoke that employee's current refresh token so that they cannot obtain new access tokens and will no longer be able to log in to the company account. The API is a REST-based API that is protected by AXL credentials. You can use any command-line tool to invoke the API. The following command provides an example of a cURL command that can be used to revoke a refresh token:

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

where:

- `admin:password` is the login ID and password for the Cisco Unified Communications Manager administrator account.
- `UCMaddress` is the FQDN or IP address of the Cisco Unified Communications Manger publisher node.
- `end_user` is the user ID for the user for whom you want to revoke refresh tokens.

Disable Inactive User Accounts

Use the following procedure to disable the inactive user accounts using Cisco Database Layer Monitor service.

Cisco Database Layer Monitor changes the user account status to inactive during scheduled maintenance tasks if you have not logged in to Cisco Unified Communications Manager within a specified number of days. Disabled users are audited automatically in the subsequent audit logs.

Before you begin

Enter the **Maintenance Time** for the selected server in the Cisco Database Layer Monitor service (**System** > **Service Parameters**).

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list box, choose a server.

Step 3 From the **Service** drop-down list box, choose the **Cisco Database Layer Monitor** parameter.

Step 4 Click **Advanced**.

Step 5 In the **Disable User Accounts unused for (days)** field, enter the number of days. For example, 90. The system uses the entered value as a threshold to declare the account status as inactive. To turn-off auto disable, enter the value as 0.

Note This is a required field. The default and minimum value is 0 and the unit is days.

Step 6 Click **Save**.
The user gets disabled if remained inactive within the configured number of days (for example, 90 days). An entry is made in the audit log and it displays the message as: "<userID> user is marked inactive".

Set up a Remote Account

Configure a remote account in the Unified Communications Manager so that Cisco support can temporarily gain access to your system for troubleshooting purposes.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Services** > **Remote Support**.

Step 2 In the **Account Name** field, enter a name for the remote account.

Step 3 In the **Account Duration** field, enter the account duration in days.

Step 4 Click **Save**.
The system generates an encrypted pass phrase.

Step 5 Contact Cisco support to provide them with the remote support account name and pass phrase.

Standard Roles and Access Control Groups

The following table summarizes the standard roles and access control groups that come preconfigured on Cisco Unified Communications Manager. The privileges for a standard role are configured by default. In addition, the access control groups that are associated with a standard role are also configured by default.

For both standard roles and the associated access control group, you cannot edit any of the privileges, or the role assignments.

Table 2: Standard Roles, Privileges, and Access Control Groups

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard AXL API Access	Allows access to the AXL database API	Standard CCM Super Users
Standard AXL API Users	Grants login rights to execute AXL APIs.	
Standard AXL Read Only API Access	Allows you to execute AXL read only APIs (list APIs, get APIs, executeSQLQuery API) by default.	
Standard Admin Rep Tool Admin	Allows you to view and configure Cisco Unified Communications Manager CDR Analysis and Reporting (CAR).	Standard CAR Admin Users, Standard CCM Super Users
Standard Audit Log Administration	Allows you to perform the following tasks for the audit logging feature : • View and configure audit logging in the Audit Log Configuration window in Cisco Unified Serviceability • View and configure trace in Cisco Unified Serviceability and collect traces for the audit log feature in the Real-Time Monitoring Tool • View and start/stop the Cisco Audit Event service in Cisco Unified Serviceability • View and update the associated alert in the RTMT	Standard Audit Users

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM Admin Users	Grants log-in rights to Cisco Unified Communications Manager Administration.	Standard CCM Admin Users, Standard CCM Gateway Administration, Standard CCM Phone Administration, Standard CCM Read Only, Standard CCM Server Monitoring, Standard CCM Super Users, Standard CCM Server Maintenance, Standard Packet Sniffer Users
Standard CCM End Users	Grant an end user log-in rights to the Cisco Unified Communications Self Care Portal	Standard CCM End Users

Standard CCM Feature Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration:
	• View, delete, and insert the following items by using the Bulk Administration Tool:
	  • Client matter codes and forced authorization codes
	  • Call pickup groups
	• View and configure the following items in Cisco Unified Communications Manager Administration:
	  • Client matter codes and forced authorization codes
	  • Call park
	  • Call pickup
	  • Meet-Me numbers/patterns
	  • Message Waiting
	  • Cisco Unified IP Phone Services
	  • Voice mail pilots, voice mail port wizard, voice mail ports, and voice mail profiles
		Standard CCM Server Maintenance

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM Gateway Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure gateway templates in the Bulk Administration Tool • View and configure gatekeepers, gateways, and trunks	Standard CCM Gateway Administration

Standard CCM Phone Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration:
	• View and export phones in the Bulk Administration Tool
	• View and insert user device profiles in the Bulk Administration Tool
	• View and configure the following items in Cisco Unified Communications Manager Administration:
	  • BLF speed dials
	  • CTI route points
	  • Default device profiles or default profiles
	  • Directory numbers and line appearances
	  • Firmware load information
	  • Phone button templates or softkey templates
	  • Phones
	  • Reorder phone button information for a particular phone by clicking the Modify Button Items button in the Phone Configuration window
		Standard CCM Phone Administration

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM Route Plan Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure application dial rules • View and configure calling search spaces and partitions • View and configure dial rules, including dial rule patterns • View and configure hunt lists, hunt pilots, and line groups • View and configure route filters, route groups, route hunt list, route lists, route patterns, and route plan report • View and configure time period and time schedule • View and configure translation patterns	

Standard CCM Service Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration:
	• View and configure the following items:
	  • Annunciators, conference bridges, and transcoders
	  • audio sources and MOH servers
	  • Media resource groups and media resource group lists
	  • Media termination point
	  • Cisco Unified Communications Manager Assistant wizard
	• View and configure the Delete Managers, Delete Managers/Assistants, and Insert Managers/Assistants windows in the Bulk Administration Tool
		Standard CCM Server Maintenance

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)

Standard CCM System Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration:
	• View and configure the following items:
	  • Automate Alternate Routing (AAR) groups
	  • Cisco Unified Communications Managers (Cisco Unified CMs) and Cisco Unified Communications Manager groups
	  • Date and time groups
	  • Device defaults
	  • Device pools
	  • Enterprise parameters
	  • Enterprise phone configuration
	  • Locations
	  • Network Time Protocol (NTP) servers
	  • Plug-ins
	  • Security profiles for phones that run Skinny Call Control Protocol (SCCP) or Session Initiation Protocol (SIP); security profiles for SIP trunks
	  • Survivable Remote Site Telephony (SRST) references
	  • Servers
	• View and configure the Job Scheduler windows in the Bulk Administration Tool
		Standard CCM Server Maintenance

Standard CCM User Privilege Management	Allows you to view and configure application users in Cisco Unified Communications Manager Administration.	
Standard CCMADMIN Administration	Allows you access to all aspects of the CCMAdmin system	
Standard CCMADMIN Administration	Allows you to view and configure all items in Cisco Unified Communications Manager Administration and the Bulk Administration Tool.	Standard CCM Super Users

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCMADMIN Administration	Allows you to view and configure information in the Dialed Number Analyzer.	
Standard CCMADMIN Read Only	Allows read access to all CCMAdmin resources	
Standard CCMADMIN Read Only	Allows you to view configurations in Cisco Unified Communications Manager Administration and the Bulk Administration Tool.	Standard CCM Gateway Administration, Standard CCM Phone Administration, Standard CCM Read Only, Standard CCM Server Maintenance, Standard CCM Server Monitoring
Standard CCMADMIN Read Only	Allows you to analyze routing configurations in the Dialed Number Analyzer.	
Standard CCMUSER Administration	Allows access to the Cisco Unified Communications Self Care Portal.	Standard CCM End Users
Standard CTI Allow Call Monitoring	Allows CTI applications/devices to monitor calls	Standard CTI Allow Call Monitoring
Standard CTI Allow Call Park Monitoring	Allows CTI applications/devices to use call park. **Important** The maximum number of opened lines and park lines must not exceed 65,000. If the total exceeds 65,000, remove the Standard CTI Allow Call Park Monitoring role from the application user or reduce the number of park lines that are configured.	Standard CTI Allow Call Park Monitoring
Standard CTI Allow Call Recording	Allows CTI applications/devices to record calls	Standard CTI Allow Call Recording
Standard CTI Allow Calling Number Modification	Allows CTI applications to transform calling party numbers during a call	Standard CTI Allow Calling Number Modification
Standard CTI Allow Control of All Devices	Allows control of all CTI-controllable devices	Standard CTI Allow Control of All Devices
Standard CTI Allow Control of Phones Supporting Connected Xfer and conf	Allows control of all CTI devices that supported connected transfer and conferencing	Standard CTI Allow Control of Phones supporting Connected Xfer and conf

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CTI Allow Control of Phones Supporting Rollover Mode	Allows control of all CTI devices that supported Rollover mode	Standard CTI Allow Control of Phones supporting Rollover Mode
Standard CTI Allow Reception of SRTP Key Material	Allows CTI applications to access and distribute SRTP key material	Standard CTI Allow Reception of SRTP Key Material
Standard CTI Enabled	Enables CTI application control	Standard CTI Enabled
Standard CTI Secure Connection	Enables a secure CTI connection to Cisco Unified Communications Manager	Standard CTI Secure Connection
Standard CUReporting	Allows application users to generate reports from various sources	
Standard CUReporting	Allows you to view, download, generate, and upload reports in Cisco Unified Reporting	Standard CCM Administration Users, Standard CCM Super Users
Standard EM Authentication Proxy Rights	Manages Cisco Extension Mobility (EM) authentication rights for applications; required for all application users that interact with Cisco Extension Mobility (for example, Cisco Unified Communications Manager Assistant and Cisco Web Dialer)	Standard CCM Super Users, Standard EM Authentication Proxy Rights
Standard Packet Sniffing	Allows you to access Cisco Unified Communications Manager Administration to enable packet sniffing (capturing).	Standard Packet Sniffer Users
Standard RealtimeAndTraceCollection	Allows an you to access Cisco Unified Serviceability and the Real-Time Monitoring Tool view and use the following items: • Simple Object Access Protocol (SOAP) Serviceability AXL APIs • SOAP Call Record APIs • SOAP Diagnostic Portal (Analysis Manager) Database Service • configure trace for the audit log feature • configure Real-Time Monitoring Tool, including collecting traces	Standard RealtimeAndTraceCollection

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard SERVICEABILITY	Allows you to view and configure the following windows in Cisco Unified Serviceability or the Real-Time Monitoring Tool: • Alarm Configuration and Alarm Definitions (Cisco Unified Serviceability) • Audit Trace (marked as read/view only) • SNMP-related windows (Cisco Unified Serviceability) • Trace Configuration and Troubleshooting of Trace Configuration (Cisco Unified Serviceability) • Log Partition Monitoring • Alert Configuration (RTMT), Profile Configuration (RTMT), and Trace Collection (RTMT) Allows you to view and use the SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service. For the SOAP Call Record API, the RTMT Analysis Manager Call Record permission is controlled through this resource. For the SOAP Diagnostic Portal Database Service, the RTMT Analysis Manager Hosting Database access controlled thorough this resource.	Standard CCM Server Monitoring, Standard CCM Super Users
Standard SERVICEABILITY Administration	A serviceability administrator can access the Plugin window in Cisco Unified Communications Manager Administration and download plugins from this window.	
Standard SERVICEABILITY Administration	Allows you to administer all aspects of serviceability for the Dialed Number Analyzer.	
Standard SERVICEABILITY Administration	Allows you to view and configure all windows in Cisco Unified Serviceability and Real-Time Monitoring Tool. (Audit Trace supports viewing only.) Allows you to view and use all SOAP Serviceability AXL APIs.	

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard SERVICEABILITY Read Only	Allows you to view all serviceability-related data for components in the Dialed Number Analyzer.	Standard CCM Read Only
Standard SERVICEABILITY Read Only	Allows you to view configuration in Cisco Unified Serviceability and Real-Time Monitoring Tool. (excluding audit configuration window, which is represented by the Standard Audit Log Administration role) Allows an you to view all SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service.	
Standard System Service Management	Allows you to view, activate, start, and stop services in Cisco Unified Serviceability.	
Standard SSO Config Admin	Allows you to administer all aspects of SAML SSO configuration	
Standard Confidential Access Level Users	Allows you to access all the Confidential Access Level Pages	Standard Cisco Call Manager Administration
Standard CCMADMIN Administration	Allows you to administer all aspects of CCMAdmin system	Standard Cisco Unified CM IM and Presence Administration
Standard CCMADMIN Read Only	Allows read access to all CCMAdmin resources	Standard Cisco Unified CM IM and Presence Administration
Standard CUReporting	Allows application users to generate reports from various sources	Standard Cisco Unified CM IM and Presence Reporting