Configure User Access

User Access Overview

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

- Access Control Groups
- Roles
- User Rank

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.

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:

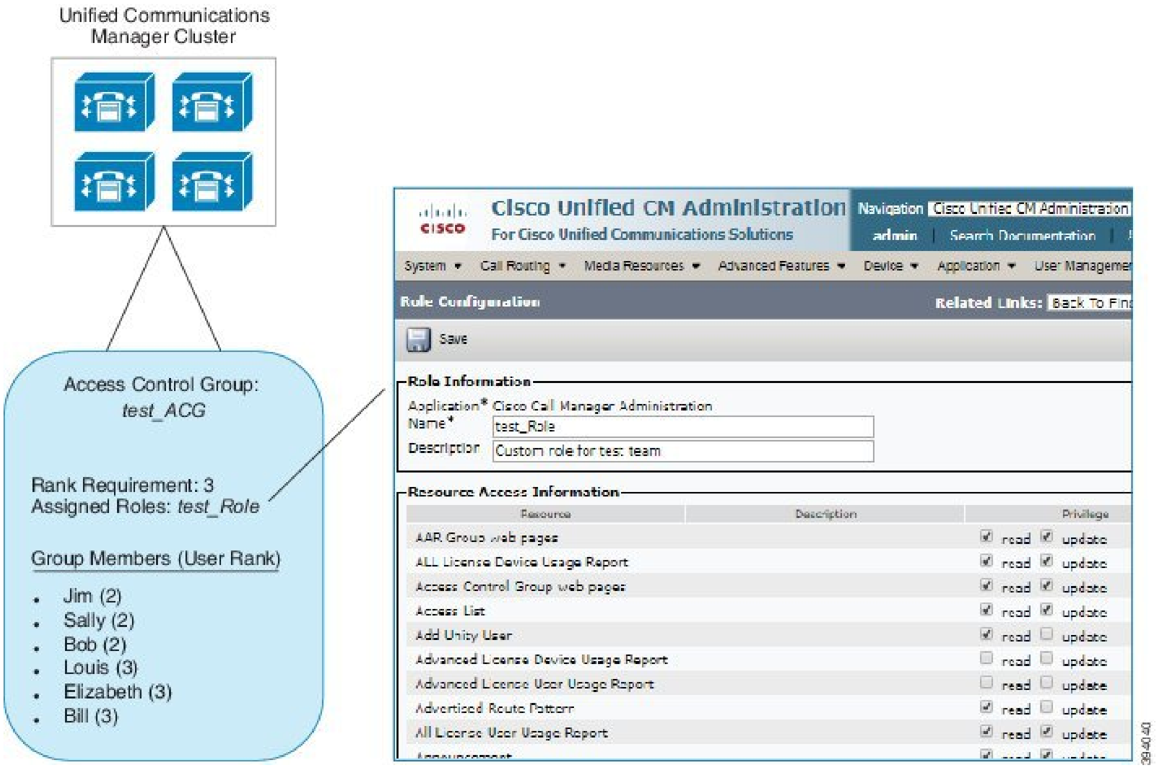
- Standard Access Control Groups—These are predefined default groups with role assignments that meet common deployment needs. You cannot edit the role assignments in a standard group. However, you can add and delete users, in addition to editing the User Rank requirement. For a list of standard access control groups, and their associated roles, see Standard Roles and Access Control Groups, on page 9.
- 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



Role Information

Application* Cisco Call Manager Administration
Name* test_Role
Description Custom role for test team

Resource Access Information

Resource	Description	Privilege
AAR Group web pages		☑ read ☑ update
ALL License Device Usage Report		☑ read ☑ update
Access Control Group web pages		☑ read ☑ update
Access List		☑ read ☑ update
Add Unity User		☑ read □ update
Advanced License Device Usage Report		□ read □ update
Advanced License User Usage Report		□ read □ update
Advertised Route Pattern		☑ read □ update
All License User Usage Report		☑ read ☑ update

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

Before you provision end users:

- Standard Roles and Access Control Groups, on page 9—Review the list of predefined roles and access control groups. Determine if you will need to configure customized roles and groups.

- Plan which user ranks you will assign to your users and groups.

User Access Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure User Rank Hierarchy, on page 4	Set up the user rank hierarchy for your system.
Step 2	If you need to create a new role, use one of the following methods: • Create a Custom Role, on page 5 • Copy an Existing Role, on page 6	Use the 'Create' procedure if you want to create and configure a new role from scratch. Use the 'Copy' procedure if the new role has similar privileges to an existing role. You can copy the privileges from the existing role into a new role, and then make edits to the privileges in the new role.
Step 3	If you need to create new access control groups, use one of the following methods: • Create Access Control Groups, on page 6 • Copy Access Control Group, on page 7	Use the 'Create' procedure to create a new access control group from scratch. Use the 'Copy' procedure if the new access control group has similar settings to an existing access control group. You can copy the settings from the existing access control group into a new group and then edit the settings.
Step 4	Assign Roles to Access Control Group, on page 8	If you created a new access control group, assign roles to your access control group.
Step 5	Configure Overlapping Privilege Policy, on page 9	Configure an enterprise policy to cover overlapping access privileges. This covers the situation where end users or application users are assigned to multiple access control groups or roles, each with conflicting privilege settings.

Related Topics

Standard Roles and Access Control Groups, on page 9

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, chooseUser 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

Create a custom role when there is no system-defined role with the privilege settings that you require.

Tip If the privileges in the new role that you want to create are similar to that of an existing role, follow the procedure Copy an Existing Role, on page 6 to copy the existing privileges into a new role that you can edit.

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**.

What to do next

Create Access Control Groups, on page 6

Copy an Existing Role

The **Copy** command allows you to create new roles that are based on the settings of existing roles. Cisco Unified Communications Manager does not allow you to edit standard roles, but you can use the **Copy** command to create a new role with the identical resources and privileges as the standard role. You can then edit the privileges in the new role that you created.

Procedure

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

Step 2 Click **Find** and select the role whose resources and privileges you want to copy.

Step 3 Click **Copy**.

Step 4 Enter the name of the new role and click **OK**.
The **Role Configuration** window displays the settings of the new role. The privileges for the new role are the same as the privileges for the role you copied.

Step 5 For any of the resources in the new role, edit the privileges as follows:

- Check the **Read** check box to allow users to view the resource.
- Check the **Update** check box to allow users to edit the resource.
- To restrict access to the resource, leave both check boxes unchecked.

Step 6 Click **Save**.

What to do next

Create a new access control group using one of the following methods:

- Create Access Control Groups, on page 6
- Copy Access Control Group, on page 7

Related Topics

Standard Roles and Access Control Groups, on page 9

Create Access Control Groups

Use this procedure is you need to create a new access control group. You may need to create a new access control group if the system-defined access control groups do not meet your deployment needs.

Before you begin

If you need to create new roles, perform one of the following procedures:

- Create a Custom Role, on page 5

- Copy an Existing Role, on page 6

Procedure

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

Step 2 Click **Add New**.

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 for a user to be assigned to this group. The default user rank is 1.

Step 5 Click **Save**.

What to do next

Assign Roles to Access Control Group, on page 8

Copy Access Control Group

Create a custom access control group by copying the settings from an existing access control group. When you copy an existing access control group, the system copies all the settings, including any assigned roles and users, to the new access control group. However, unlike default access control groups, you can make edits to the roles assigned to a custom access control group.

Before you begin

If you need to create a new role, perform either of the following steps:

- Create a Custom Role, on page 5
- Copy an Existing Role, on page 6

Procedure

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

Step 2 Click **Find** and select the access control group whose settings you want to copy.

Step 3 Click **Copy**.

Step 4 Enter a name for the new access control group and click **OK**.

Step 5 From the **Available for Users with User Rank as** drop-down, select the minimum User Rank for a user to be assigned to this group.

Step 6 Click **Save**.

What to do next

Assign Roles to Access Control Group, on page 8

Related Topics

Standard Roles and Access Control Groups, on page 9
Assign LDAP Users to Access Control Group
Assign Local Users to Access Control Group

Assign Roles to Access Control Group

For any new access control groups that you create, assign roles to the access control group. If you copied the access control group from an existing group, you may also need to delete a role.

Note You cannot edit the role assignments for any of the standard access control groups that are are configured by default.

Before you begin

Perform either of the following tasks to create a new access control group:

- Create Access Control Groups, on page 6
- Copy Access Control Group, on page 7

Procedure

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

Step 2 Click **Find** and select an access control group.

Step 3 From the **Related Links** drop-down list box, select **Assign Role to Access Control Group** and click **Go**.

Step 4 If you need to assign a role:

a) Click **Assign Role to Group**.
b) In the **Find and List Roles** window, check the roles that you want to assign to the group.
c) Click **Add Selected**.

Step 5 If you need to delete a role:

a) In the **Role** list box, highlight the role that you want to delete.
b) Click **Delete Role Assignment**.

Step 6 Click **Save**.

What to do next

Configure Overlapping Privilege Policy, on page 9

Configure Overlapping Privilege Policy

Configure how Cisco Unified Communications Manager handles overlapping user privileges in 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 access privileges.

Before you begin

Assign Roles to Access Control Group, on page 8

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**.

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