
# Roles and User Groups

Cisco Unified CallManager Administration uses roles and user groups to provide varying levels of privilege (access). This technique permits granting only the required privileges for a selected group of users and limits the configuration functions that users in a particular user group can perform.

Use the following topics to understand roles and user groups:



### Related Topics

- Role Configuration, *Cisco Unified CallManager Administration Guide*
- User Group Configuration, *Cisco Unified CallManager Administration Guide*

## Overview

Roles and user groups provide multiple levels of security to Cisco Unified CallManager Administration and to other applications. The system groups the resources that are available to Cisco Unified CallManager Administration and to other applications into roles. Each application comes with standard, predefined roles. Each application defines its own access privilege for Cisco Unified CallManager Administration.

Administrators can configure additional roles for an application. A role contains, for a particular application, the list of resources that an application comprises. For each resource that a role comprises, the administrator defines the access privilege. For the Cisco Unified CallManager Administration application, the access privileges include *read* and *update*. Other applications specify their own access privileges.

After configuration of roles for an application, administrators can configure user groups. User groups define groups of users that share a common list of assigned roles. User groups comprise both application users and end users.

# Roles

A role includes a collection of resources for an application, such as the Cisco Unified CallManager Administration application. Two types of roles exist: standard roles, which are the default roles, and custom, administrator-defined roles. Standard roles for an application get created upon installation of the application. Administrators may define custom roles.

**Note** All standard roles get created at installation. You cannot modify or delete standard roles, but you can copy them to create new custom roles based on standard roles.

# Role Access Privileges

For the Cisco Unified CallManager Administration application, one of the following access privileges applies to the resources that a particular role comprises:

- Read
- Update

**Note** Other applications specify their own access privileges.

For each role that is associated with the Cisco Unified CallManager Administration application, one of these privilege levels applies for access to each of the resources. The access privileges specify the following privileges:

- Access privilege *Read* specifies that users in a user group that have this privilege defined for a particular resource can view only the windows that the resource comprises but cannot modify the windows. Access privilege *Read* limits access to windows to read operations. Buttons such as **Insert**, **Delete**, **Update**, and **Reset** do not display.
- Access privilege *Update* specifies that users in a user group that this privilege defined for a particular resource can view and change the windows that the resource comprises. Users with update privilege can perform operations such as Insert, Delete, Update, and Reset, as well as executive functions that can start or stop a process or service from the Cisco Unified CallManager Administration and Serviceability windows.

For each application, install assigns default access privileges to the roles that get created at install time.

**Note** The Standard CCM Admin Users role gives the user access to the Cisco Unified CallManager Administration user interface. This role, the base role for all administration tasks, serves as the authentication role. Cisco Unified CallManager Administration defines this role as the role that is necessary to log in to Cisco Unified CallManager Administration.

The Standard CCM Admin Users role includes no permissions beyond logging into Cisco Unified CallManager Administration. The administrator must add another authorization role to define the parts of the Cisco Unified CallManager Administration that the user can administer. The Standard CCMADMIN Administration role allows a user to access and make changes in all of Cisco Unified CallManager Administration.

**Note** A user with only the Standard CCM Admin Users role can access Cisco Unified CallManager Administration but cannot make any changes. A user with only the Standard CCMADMIN Administration role can make changes, but cannot authenticate entry to Cisco Unified CallManager Administration.

A user, therefore, must have the Standard CCM Admin User role to access Cisco Unified CallManager Administration and must have at least one other role to administer the system.

# User Groups

A user group comprises a collection of Cisco Unified CallManager application users and end users that are grouped together for the purpose of assigning a common list of roles to the members in the user group.

Various named user groups that are predefined have no members that are assigned to them at install time. The Cisco Unified CallManager super user or a user with access to user group configuration should add users to these groups. The super user or a user with access to user group configuration can configure additional named user groups as needed.

**Note** The standard CCM Super Users user group represents a named user group that always has full access permission to all named roles. You cannot delete this user group. You can only make additions and deletions of users to this group.

**Note** CCMAdministrator always represents a super user.

For the complete listing of user groups, see the "Standard Roles and User Groups" section on page 4-4.

# Access Log

The log contains a file report of access/change attempts. That is, Cisco Unified CallManager Administration generates a record of attempts to access or modify any directory or database component through Cisco Unified CallManager Administration. The change record includes the user name, date, time, window from which the change was made, and the success or failure status of the update.

# Enterprise Parameters

Roles and user groups use the Effective Access Privileges For Overlapping User Groups and Roles enterprise parameter.

### Effective Access Privileges for Overlapping User Groups and Roles

The Effective Access Privileges For Overlapping User Groups and Roles enterprise parameter determines the level of user access for users that belong to multiple user groups and have conflicting privileges.

You can set this enterprise parameter to the following values:

- Maximum—The effective privilege represents the maximum of the privileges of all the overlapping user groups.
- Minimum—The effective privilege represents the minimum of the privileges of all the overlapping user groups.

The Effective Access Privileges For Overlapping User Groups and Roles enterprise parameter specifies the Maximum default value.

**Note** This enterprise parameter does not affect the privileges for the members of the standard CCM Super Users user group.

# Standard Roles and User Groups

When you install Cisco Unified CallManager Administration, standard roles and standard user groups get created. Be aware that the list of standard roles and standard user groups is dynamic.

Standard user groups in Cisco Unified CallManager Administration provide a predefined set of roles and permissions for various functions. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users. Administrators can disable functions that they do not use or modify standard functions to increase security.

Because Cisco Unified CallManager allows administrators to manage user groups, roles, and resources, no guarantee exists that a particular user group or role goes unchanged or that administrators will use the predefined user groups or roles.

Certain user groups and roles exhibit limitations that administrators need to recognize, particularly user groups and roles that concern applications. For example, you can modify the Standard EM Authentication Proxy Rights user group by adding both application users and end users. Because authentication by proxy is intended for use by applications, end users that get added to this user group cannot authenticate by proxy.

You cannot delete standard roles and standard user groups, but the CCMAdministrator can modify a standard role or a standard user group.

# Where to Find More Information

### Related Topics

- Role Configuration, *Cisco Unified CallManager Administration Guide*
- User Group Configuration, *Cisco Unified CallManager Administration Guide*
- Application Users and End Users, page 21-1
- Application User Configuration, *Cisco Unified CallManager Administration Guide*
- End User Configuration, *Cisco Unified CallManager Administration Guide*

### Additional Cisco Documentation

- *Installing Cisco Unified CallManager*
- *Cisco Unified CallManager Administration Guide*

- *Cisco Unified CallManager Serviceability System Guide*
- *Cisco Unified CallManager Serviceability Administration Guide*