Access Control Group Setup

This chapter provides information to configure access control groups, assign users to access control groups, and view the roles, access control groups, and permissions of a user.

About Access Control Group Setup

The role and access control group menu options in the Cisco Unified Communications Manager (Unified CM) Administration User Management menu allow users with full access to configure different levels of access for Unified CM administrators. Users with full access configure roles, access control groups, and access privileges for roles. In general, full-access users configure the access of other users to Unified CM Administration.

Access control groups comprise lists of application users and end users. A user may belong to multiple access control groups. After you add an access control group, you then add users to an access control group. After these steps, you can assign roles to an access control group. If a user belongs to multiple access control groups, the MLA permission enterprise parameter determines the effective privilege of the user.

Reduced Permissions for Access Control Groups

Problem When you add a new access control group to existing users, the level of privileges for some pre-existing access control groups is unexpectedly reduced.

Solution Users can belong to multiple access control groups. When you add a new access control group to existing users, the current level of privileges for some pre-existing access control groups may be reduced if the new access control group has the “Effective Access Privileges for Overlapping User Groups and Roles” Enterprise parameter set to minimum.

Access privilege reduction can occur inadvertently, for example, during an upgrade of Cisco Unified CM Administration. If the upgrade version supports the Standard RealTimeAndTrace Collection user group, which has the “Effective Access Privileges for Overlapping User Groups and Roles” Enterprise parameter set to minimum, all users are automatically added to that user group during the upgrade. To resolve the permissions issue in this example, you can remove users from the Standard RealTimeAndTrace Collection user group.

Find Access Control Group

Because you might have several access control groups in your network, Cisco Unified Communications Manager (Unified CM) lets you locate specific access control groups on the basis of specific criteria. Use the following procedure to locate access control group.

Note During your work in a browser session, Unified CM Administration retains your access control group search preferences. If you navigate to other menu items and return to this menu item, Unified CM Administration retains your access control group search preferences until you modify your search or close the browser.

Procedure

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

The Find and List Access Control Groups window appears. Records from an active (prior) query may also display in the window.

Step 2 To find all records in the database, ensure the dialog box is empty.

a) From the drop-down list box, select a search pattern.
b) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3 Click **Find**.

All matching records appear. You can change the number of items that appear on each page by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record, and then clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All, and then clicking Delete Selected.

Note You cannot delete the standard access control groups.

Step 4 From the list of records that appear, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Set Up Access Control Group

This section describes how to add, copy, and update an access control group in Cisco Unified CM Administration.

Note You cannot delete a standard access control group, but you can update the user membership for a standard access control group.

Procedure

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

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

Step 2 If you want to create a new access control group by copying the settings from an existing group:

a) Select the group whose settings you want to copy, and click **Copy**.
b) In the popup window, enter a name for the new group, and click **OK**.
The system creates the new access control group with identical settings to the copied group.
c) Click **Save**.

Step 3 If you want to create a new access control group from scratch:

a) Click **Add New**.
b) Enter a **Name** for the new group.
c) Click **Save**.

Step 4 If you want to update an existing access control group:

a) Click **Find** and select the appropriate group.
b) Update the appropriate settings.
c) Click **Save**.

Step 5 To add users, click **Add End Users to Group** or **Add App Users to Group**.

End users are associated with an individual and have an interactive login. End users can have administrative roles based on the user group role configuration.

Application users are associated with applications such as Cisco Unified Attendant Console, Cisco Unified Contact Center Express (UCCX), or Cisco Unified Manager Assistant. The mentioned applications need to authenticate with CUCM, but application users do not have the ability to interactively log in. Application users are leveraged for internal process-level communications between applications.

Step 6 To assign roles, from **Related Links**, select **Assign Role to Access Control Group** and click **Go**.

Roles allow Cisco Unified Communications Manager administrators who have full administration privilege (access) to configure end users and application users with different levels of privilege. Administrators with full administration privilege configure roles and user groups. In general, full-access administration users configure the privilege of other administration users and end users to Cisco Unified Communications Manager Administration and to other applications.

Delete Access Control Group

This section describes how to delete an access control group from Unified CM Administration. 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 (Unified CM) removes all access control group data from the database. To find out which roles are using the access control group, in the Access Control Group Configuration window, choose Dependency Records from the Related Links drop-down list box, and then click Go. If dependency records are not enabled for the system, the Dependency Records Summary window displays a message.

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**, Unified CM removes the access control group from the database.

Add Users to Access Control Groups

This section describes how to add end users and application users to an access control group in Cisco Unified Communications Manager (Unified CM) Administration.

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 to which you want to add users.

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

The access control group that you chose appears. The Users list shows the users that currently belong to the access control group.

Step 4 To add end users, click **Add End Users to Group**. To add application users, skip to step 8.

The Find and List Users window appears.

Step 5 Use the Find User drop-down list boxes to find the end users that you want to add, and then click **Find**.

> **Note** You can perform the search for users in a variety of ways. You can enter the first name, middle name, last name, user ID, or department of a user. Alternatively, you can leave the field blank, which results in display of all users.

A list of end users that matches your search criteria appears.

> **Note** The list of search results does not display end users that already belong to the access control group.

Step 6 In the list of search results, check the check box next to the users that you want to add to this access control group. If the list comprises multiple pages, use the links at the bottom to see more results.

Step 7 Click **Add Selected**.

The Access Control Group Configuration window reappears with the users that you added listed in the Users pane.

> **Note** After you add a user, you can view the roles by clicking the i icon in the Permission column for that user.

Step 8 To add application users, click **Add App Users to Group**.

The Find and List Application Users window appears.

Step 9 Use the Find Application User drop-down list boxes to find the application users that you want to add and click Find.

> **Note** You can perform the search for application users by searching for user ID. Alternatively, you can leave the field blank, which results in display of all application users.

A list of application users that matches your search criteria displays.

Step 10 In the list of search results, check the check box next to the application users that you want to add to this access control group. If the list comprises multiple pages, use the links at the bottom to see more results.

> **Note** The list of search results does not display application users that already belong to the user group.

Step 11 Click **Add Selected**.

The Access Control Group Configuration window reappears with the application users that you added listed in the Users pane.

> **Note** After you add an application user, you can view the roles by clicking the i icon in the Permission column for that user.

Step 12 To save your changes to this access control group, click **Save**.

Delete Users from Access Control Groups

This section describes how to delete users from an access control group in Cisco Unified Communications Manager (Unified CM) Administration.

Procedure

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

The Find and List Access Control Groups window appears.

Step 2 Find the access control group from which you want to delete users.

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

The access control group that you chose appears. The Users list shows the users that currently belong to the access control group.

Step 4 Check the check boxes next to the names of the users that you want to delete from this access control group.

Step 5 Click **Delete Selected**.

A confirmation message asks you to confirm the deletion.

Step 6 To delete the selected access control group members, click **OK** or **Cancel** to exit this window.

The Access Control Group Configuration reappears with the deleted users removed from the Users in Group pane.

Assign Roles to Access Control Group

Users with full access can assign roles to access control groups. An access control group that has assigned roles has access to the resources that the role comprises.

This section describes assigning roles to an access group in Cisco Unified Communications Manager (Unified CM) Administration.

Note When an administrator assigns roles to an access control group, the administrator should assign the Standard Unified CM Admin Users role to the access control group. This role enables the users to log into Unified CM Administration.

Procedure

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

The Find and List Access Control Groups windows appears.

Step 2 Find the access control group to which you want to assign roles.

Step 3 Click the name of the access control group for which you want to assign roles.

The access control group that you chose appears. The Users list shows the users that currently belong to the access control group.

Step 4 From the Related Links drop-down list box, choose Assign Role to Access Control Group, and then click **Go**.

The Access Control Group Configuration window changes to display the Role Assignment pane. For the access control group that you chose, the list of assigned roles appears. Choose one of the following options:

a) To assign roles to the access control group, go to step 5.
b) To delete roles from the user group, go to step 9.

Step 5 To assign additional roles to the access control group, click **Assign Role to Group**.

The Find and List Roles dialog box appears.

Step 6 If necessary, use the **Find Role** search criteria to narrow the list of roles.

Step 7 Choose the roles to assign to this access control group by checking the check boxes next to the role names. To close the Find and List Roles dialog box without assigning roles to this access control group, click **Close**.

Step 8 Click **Add Selected**.

The Find and List Roles dialog box closes. The chosen roles get added to the Role Assignment pane for this access control group. If you do not want to delete any assigned roles for this access control group, skip to step 10.

Step 9 To delete an assigned role from the access control group, select a role in the Role Assignment pane, and then click **Delete Role Assignment**. Repeat this step for each role that you want to delete from this access control group.

Step 10 Click **Save**.

The system makes the added and deleted role assignments to the access control group in the database.

View User Roles, Access Control Groups, and Permissions

This section describes how to view the roles, access control groups, and permissions that are assigned to a user who belongs to a specified access control group. Use the following procedure to view the roles, access control groups, and permissions that are assigned to a user in an access control group.

Note You can also view user roles by using **User Management** > **Application User** (for application users) or **User Management** > **End User** (for end users) to view a particular user, and then display the user roles.

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 has the users for which you want to display assigned roles.

Step 3 Click the name of the access control group for which you want to view the roles that are assigned to the users.

The Access Control Group Configuration window appears for the access control group that you chose. The Users pane shows the users that belong to the access control group.

Step 4 For a particular user, click the username.

The Application User Configuration window (for application users) or End User Configuration window (for end users) appears.

Step 5 From the Related Links drop-down list box, choose User Privilege Report, and then click **Go**.

For the user that you chose, the following information appears:

a) Access control groups to which the user belongs
b) Roles that are assigned to the user
c) Resources to which the user has access. For each resource, the following information appears:
   - Application
   - Resource
   - Permission (read and/or update)

Step 6 To return to the user, choose **Back to User** or **Back to Application User** in the Related Links drop-down list box, and click **Go**.