Manage Administrators

The Packaged CCE deployment of Unified CCE Administration offers extensive flexibility in the configuration of administrator users and in ways to limit their system access.

Administrator access is controlled by the roles and department tools available from the **System** menu. Only administrators with the SystemAdmin role can access these tools.

Note Administrator password and role changes can take up to 30 minutes to take effect.

Note If the system administrator is assigned to "None" (no role), then that administrator has access all the tools in the Configuration Manager.

Add and Maintain Administrators

This procedure explains how to add an administrator. For information on maintaining administrators, see Update Objects and Delete Objects.

To add, edit, or delete administrators, an administrator must have the SystemAdmin role. Administrators cannot add, update, or delete themselves.

Procedure

Step 1 Navigate to **Unified CCE Administration** > **System** > **Administrators**.

This opens a **List of Administrators** that shows all administrators who are currently configured.

Step 2 Click **New** to open the **New Administrator** window.

Step 3 Complete the following fields:

Field	Required?	Description
Domain	no	From the drop-down menu, select the domain for this administrator.
Username	yes	Enter a unique name for the administrator, using a maximum of 64 characters. The account must already exist in Active Directory under the selected domain.
Description	no	Enter a maximum of 255 characters to describe the role. See Native Character Sets for details on valid characters for this field.
Role	no	*ConfigAdmin* is the default role for a new administrator. Click the **magnifying glass** icon to open the **List of Roles** pop-up window. Select a role for this administrator. For more infromation see the topic
Read only	no	This check box defaults to unchecked, indicating that the administrator has full access to the tools this role allows. Check this check box to limit the administrator to read-only access.
Access to All Departments	no	This check box defaults to checked. You cannot uncheck it for the *SystemAdmin* role—SystemAdmins are always Global administrators. For all other roles, you can leave the check box checked to configure the new administrator as a Global administrator. Or you can uncheck the check box to configure the administrator as a Department Administrator and then: • Click **Add** to open the **List of Allowed Departments** pop-up window. • Click one or more departments to select them; then close the popup window. The administrator is now a Department administrator who is associated with those departments. • Click the **x** icon to remove a department. **Note** Department Administrator will have read-only access to non-departmental entities such as SIP Server Group, Media Routing Domain, Routing Pattern, and so on, even if the associated role grants full access.

Step 4 Click **Save** to return to the list, where a message confirms the successful creation of the administrator.

Related Topics

Important Considerations Regarding User Accounts
Administrators and System Access, on page 3
Departments, on page 7
Roles, on page 5

Administrators and System Access

Administrators' access to the system can be restricted by their roles, the departments to which they are assigned, and whether they have full or read-only permission.

An administrator must have a role, which specifies which menus and tools an administrator sees .

Packaged CCE offers the option to create departments. A contact center for a university might have a department for each academic area, a department for admissions, a department for alumni, and so forth. An administrator can be associated with one or more departments or can be a global administrator who is assigned to no departments and who therefore has access to all departments. Departmental administrators can add and edit objects only for the departments they administer.

An administrator's role and department associations are configured when the administrator is created. A SystemAdmin can change them.

Note If user's Use logon name (pre-Windows 2000) changes in Active Directory, you must update the same in Packaged CCE. Choose **Unified CCE Administration** > **System** > **Administrator**. Select the user to open the details and click **Save**.

Related Topics

Roles, on page 5
Departments, on page 7

Limit Administrator Access

Limit Administrator Access by Departments

Packaged CCE allows you to create departments and to associate an object with one department. For example, a university might have department for Admissions, Billing, and each academic area.

The add/edit pages for those objects have a Department field. If you do not want an object to have a department association, you have two options:

- Do not create departments.
- Create departments, but select *Global* from the Department drop-down menu to give the object “global” status.

In the table below, Skill Group One is associated with the Admissions department. Skill Group Two is associated with the History department. Skill Group Three is global and belongs to no department.

Table 1: Object and Departments

Department	Object
Admissions	Skill Group One
History	Skill Group Two
Global	Skill Group Three

When you create or edit an administrator, you can either check **Access to All Departments**, which gives an administrator "global" access to all departments, or associate the administrator with one or more departments. To establish a department association for an administrator, click **Add** next to the **List of Allowed Departments** and select one or multiple departments.

Note An administrator with the SystemAdmin role cannot be a departmental administrator.

In the following table, Administrator One can work with objects in the Admissions department. Administrator Two can work with objects in the History department. Administrator Three is a global administrator and can work with all objects in all departments.

Table 2: Administrators and Departments

Department	Administrator
Admissions	Administrator One
History	Administrator Two
Global	Administrator Three

Limit Administrator Access by Role and Permissions

An administrator must be assigned a role to be allowed to sign in to the Unified CCE Administration.

These roles specify which menus and tools an administrator sees. Every administrator has a **Read only** check box. This means that two administrators could have a role that allows them to see the tools under **Manage** > **Agents**, but with different permissions. One could have that role with **Read only** checked; this administrator could see the lists in each tool, unless restricted by departmental association. The other administrator could have that role with **Read only** unchecked; this administrator could see the lists in each tool and could also add, edit, and delete objects on those lists, unless restricted by departmental association.

Table 3: Impact of Role and Permissions

Role	Permissions	Administrator
Agent Tools	Read-only	Administrator One
Agent Tools	Full	Administrator Two
Script and Call Tools only	Full	Administrator Three

Administrator One, whose role and administrator settings allow Read-Only access to Agent tools and who is associated with the Admissions department, can see Skill Group One and Skill Group Three.

Administrator Two, whose role and administrator settings allow full access to Agent tools and who is associated with the History department, can see, edit, and delete Skill Group Two. This administrator can add History Department agents to Skill Group Two, add global agents to Skill Group Two, and see Skill Group Three but cannot edit or delete it.

Administrator Three, who is not associated with any department, cannot access the **Manage** > **Agents** menu and cannot work with any of the skill groups—this administrator's role allows access to Script and Call tools only.

Roles

Roles specify which menus and tools an administrator can see and use. An administrator can be assigned to a built-in role or to a custom role. (An administrator who has no role cannot sign in.)

Every administrator has a **read-only** check box. If read-only is checked, the administrator has read-only access to the tools available in their role.

Features access for roles are defined by check boxes. You cannot alter the features access for built-in roles (all allowed features are checked). But, you can create custom roles to define customized sets of features access.

Note Role changes can take up to 30 minutes to take effect.

Built-In Roles

Administrators with this role	Can access
AgentAdmin	Agent Tools only: • Agents • Attributes • Desk Settings • Precision Queues • Reason Codes • Skill Groups • Teams

Administrators with this role	Can access
ScriptAdmin	All Agent Tools, plus these Script and Call Tools: • Bucket Intervals • Bulk Jobs • Call Types • Dialed Numbers • Expanded Call Variables • Multichannel tools. These include Media Routing Domains, and these Configuration Manager tools: Application Instance, Application Path, Media Class List, Media Routing Domain List. • Network VRU Scripts • Outbound Campaigns (Configuration Manager) • Script Editor
ConfigAdmin	All the Tools for the roles listed previously, plus these System Tools: • Agent Targeting (Configuration Manager) • Agent Trace • Context Service • Deleted Objects (Configuration Manager) • Deployment • Log Collection • Outbound Dialer (Configuration Manager) • Single Sign-On • System Information • System Settings
SystemAdmin	All the Tools for the roles listed previously, plus these Access Tools: • Administrators • Departments • Roles

Add and Maintain Custom Roles

To add, edit, or delete custom roles, an administrator must have the SystemAdmin role.

This procedure explains how to add a role. For information on maintaining roles, see Update Objects and Delete Objects.

Procedure

Step 1 Navigate to **Unified CCE Administration** > **System** > **Roles**.

This opens a **List of Roles** that shows all roles currently configured.

Step 2 Click **New** to open the **New Role** page.

Step 3 Complete the fields on the **General** tab:

Field	Required?	Description
Name	Yes	Enter a unique name for the role, using a maximum of 32 characters.
Description	No	Enter a maximum of 255 characters to describe the role. See Native Character Sets.
Access fields	No	When you create a new (custom) role, check the tools that you want administrators with that role to be able to see and use. Checking a category of tools checks all tools in that category. You can uncheck individual tools. For example, you can select Agent Tools and then uncheck Precision Queues and Skill Groups. **Note** You cannot add Access tools (Administrators, Departments, Roles) to a custom role.

Step 4 Continue to the **Administrators** tab to add administrators to the role.

Step 5 Click **Add** to open the **Add Administrators** pop-up window.

The row for each administrator has three columns: a column that is either blank or that shows an “i” icon, a column with the administrator's username, and a column with the administrator's domain.

If an administrator already has an "i" icon indicating that the administrator has a role, hover over the icon to see the name of that role. Clicking an administrator who already has a role removes that role and reassigns this role.

Step 6 Click **Save** to return to the list of roles, where a message confirms the successful creation of the role.

Departments

You have the option to create departments to facilitate contact center operation and maintenance. A contact center for a hospital might create departments for Surgery, Radiology, Obstetrics, and other operational units. A contact center for a university might create departments for Admissions, Alumni, and Registration. Departments are not required, and there are no built-in departments.

If you do not create departments, all administrators and objects are *global*, meaning that they are not associated with a department.

If you create departments, you have the option to associate a department with each administrator and object. These are called *departmental* administrators and objects. Your Packaged CCE configuration can include a mix of global and departmental administrators and objects.

You can creating routing scripts for a department by referencing objects from that department in the scripts.

You can also create custom reporting collections in Cisco Unified Intelligence Center to report on departmental objects. See the *Cisco Unified Intelligence Center Report Customization Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.html for directions on customizing reports.

Departmental Objects

The following objects can be associated with a single department. If departments are configured, the List screens for these objects have a Department column. The New and Edit windows for these objects have a Department field.

- Agents
- Attributes
- Bucket intervals
- Call types
- Desk settings
- Dialed numbers
- Network VRU scripts
- Precision queues
- Skill groups
- Teams

Relationships Between Global and Departmental Objects

You can create relationships between objects in your configuration. For example, you can associate an agent with skill groups, a call type with a dialed number, and so on. An object's department assignment controls the relationships it can have to other objects.

The rules for creating relationships between objects are as follows:

- A **global** object can be associated with any global or departmental objects. For example, when you are assigning skill groups to a global agent, the skill group selection list includes global skill groups and skill groups in all departments to which you have access.
- A **departmental** object can be associated with global objects or with objects in the same department. For example, when you are assigning skill groups to an agent in Department A, the skill group selection list includes global skill groups and skill groups in Department A.

These rules are summarized in the following table.

Table 4: Rules for Relationships Between Global and Departmental Objects

Object Type	Can be associated with Global object?	Can be associated with Departmental object?
Global	yes	yes, with objects from any department
Departmental	yes	yes, with objects from same department only

The only exceptions to these rules are for the relationships between the following objects:

- **Teams and agent:** A global agent can belong only to a global team. A departmental agent can belong either to a global team or to a team that is associated with the same department.
- **Teams and supervisors:** Global supervisors can supervise both global and departmental teams. Departmental supervisors can supervise only teams that are associated with the same department.

These exceptions prevent departmental supervisors from modifying global agents, and are summarized in the following table.

Table 5: Rules for Relationships Between Teams and Agents and Teams and Supervisors

	Agent - Global	Agent - Departmental	Supervisor - Global	Supervisor - Departmental
Team - Global	yes	yes	yes	no
Team - Departmental	no	yes (same department only)	yes	yes (same department only)

Change Departments for an Object

When you change the department for an object, relationships with objects in the original department are cleared; relationships with global objects and objects in the new department remain intact. For example, if you change an agent from Department A to Department B, any skill groups in Department A that had been associated with the agent are cleared.

For some objects, such as call type, the Edit window does not show all related objects. If you try to change the department for those objects, you see an error indicating that you cannot change the department because a related object is in the original department. For example, you see this error if you try to change a call type from Department A to Department B and it is related to a dialed number in Department A. You must change the department of the dialed number before you can change the department of the call type.

System-wide Settings and Global Objects

Only global objects can be selected for system-wide settings in the **System** > **Settings** tool.

Global and Departmental Administrators

When you create administrators, you can configure them as global administrators or associate them with departments. See Add and Maintain Administrators, on page 1.

Global administrators

Global administrators:

- Have read and write access to departmental objects and global objects on all tools and menus that are allowed for their role. Administrators configured as **read-only** have read-only access to those objects.
- Can use Script Editor or Internet Script Editor to modify routing scripts.

Departmental administrators

Departmental administrators:

- Can be associated with multiple departments. They have read and write access and objects in their departments on all tools and menus that are allowed for their role. Administrators configured as **read-only** have read-only access to those objects.
- Have read-only access to global objects.
- A departmental administrator with the ConfigAdmin role has read-only access to the General tools on the System menu: Information, Settings, Deployment, and Agent Trace.
- Can use Internet Script Editor to modify scripts that reference objects associated with their departments. Departmental administrators cannot log into Script Editor.

Add and Maintain Departments

To add, edit, or delete departments, an administrator must have the SystemAdmin role.

This procedure explains how to add a department. For information on maintaining departments, see Update Objects and Delete Objects.

Procedure

Step 1 Navigate to **Unified CCE Administration** > **System** > **Departments**.

A **List of Departments** window opens.

Step 2 Click **New** to open the **New Department** window.

Step 3 Complete the fields on the **General** tab:

a) **Name** (Required) Enter a unique name for the department, using a maximum of 32 characters.

b) **Description** (Optional) Enter a maximum of 255 characters to describe the department. See Native Character Sets for details on valid characters for this field.

Step 4 Click the **Administrators** tab.

This tab shows the Username and Domain of the administrators who currently serve as department administrators and allows you to add or remove administrators.

a) Click **Add** to open the **Add Administrators** popup window.

b) Click one or more rows to select administrators; then close the popup window. The administrators are now on the List of Administrators.

c) Click the **x** icon to remove an administrator from the list.

Step 5 Click **Save** to return to the list window, where a message confirms the successful creation of the department.