

CallManager 5.x/6.x/7.x: Roles and Permissions

Document ID: 98796

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Cisco Unified Communications Manager User Management

Application User

- End User Configuration

Role Management

User Group Configuration

- Assigning Roles to a User Group

- Viewing a User's Roles, User Groups, and Permissions

- Assign only the Phone Web Page Access to the End Users

Troubleshoot

- Login to the Personal Directory Fails

- Users cannot Access User Options Page

- Error "User is not authorized to perform this function."

- After Changing the Locale, the Language on the CCM User Page does not Change

- Users Cannot Change Their PIN Settings on the CCM User Page

Related Information

Introduction

This document describes the roles and privileges of the different user groups in Cisco Unified Communications Manager 5.x/6.x/7.x and their management.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Cisco Unified Communications Manager Administration.

Components Used

The information in this document is based on Cisco Unified Communications Manager 5.x/6.x/7.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Cisco Unified Communications Manager User Management

In Cisco Unified Communications Manager, user groups comprise lists of **Application users** and **End users**. A user can belong to multiple user groups. After you add a user group, then you add users to a user group. Afterwards, you can proceed to assign roles to a user group. If a user belongs to multiple user groups, the **User Management Parameters Effective Access Privileges For Overlapping User Groups and Roles** enterprise parameter determines the effective privilege of the user. This parameter determines the method to resolve overlapping resource privilege when a user is a member of more than one user groups and/or a group contains multiple roles. If set to **maximum**, the user is granted the highest privilege for the resources. If set to **minimum**, the user is granted the lowest privilege for the resources. The default is **maximum**.



Application User

Application user configuration allows updates to the application users that are associated with Cisco Unified Communications Manager. By default, Cisco Unified Communications Manager Administration includes these application users:

- CCMAAdministrator
- CCMSysUser
- IPMASecureSysUser
- IPMASysUser
- WDSecureSysUser
- WDSysUser
- TabSyncSysUser
- CUCService

Note: You cannot delete these default application users, but you can change their passwords and modify the lists of devices that they control.

Note: In order to configure the application user information in Cisco Unified Communications Manager, use the **User Management > Application User** option in Cisco Unified Communications Manager Administration.

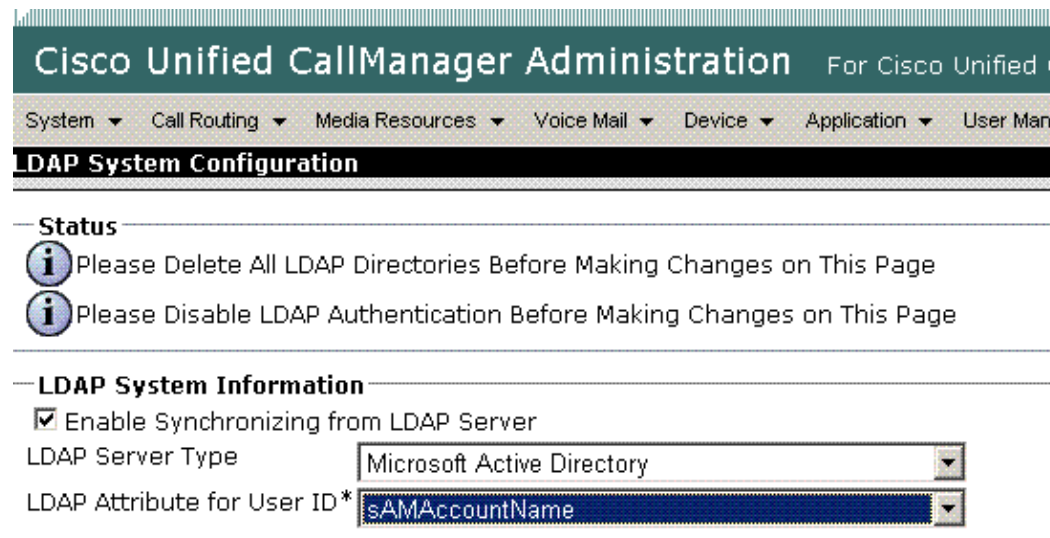
End User Configuration

The End User Configuration window in Cisco Unified CallManager Administration allows the administrator to add, search, display, and maintain information about Cisco Unified Communications Manager end users.

In order to configure end user information, choose the **User Management > End User** option in Cisco Unified Communications Manager Administration.

Note: You can add new end users through Cisco Unified CallManager Administration only when synchronization with the corporate LDAP server is disabled. When synchronization is disabled, you can add new users and you can change the settings of existing users, which includes the user ID. If synchronization is enabled, you cannot add new users and you cannot change existing user IDs. However, you can change all other settings for existing end users.

Note: In order to check whether configuration is enabled, use the **System > LDAP > LDAP System** menu option in Cisco Unified CallManager Administration. If the **Enable Synchronizing from LDAP Server** check box is not checked, synchronization is not in effect.



The screenshot shows the Cisco Unified CallManager Administration interface. The top navigation bar includes 'System', 'Call Routing', 'Media Resources', 'Voice Mail', 'Device', 'Application', and 'User Management'. The current page is 'LDAP System Configuration'. Under the 'Status' section, there are two information icons with the following messages: 'Please Delete All LDAP Directories Before Making Changes on This Page' and 'Please Disable LDAP Authentication Before Making Changes on This Page'. The 'LDAP System Information' section contains a checked checkbox for 'Enable Synchronizing from LDAP Server'. Below this, there are two dropdown menus: 'LDAP Server Type' is set to 'Microsoft Active Directory', and 'LDAP Attribute for User ID*' is set to 'sAMAccountName'.

Role Management

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.

Different levels of privilege exist for each application. For the Cisco Unified Communications Manager Administration application, two levels of privilege exist: read privilege and update privilege. These privilege levels differ:

- Users with update privilege can view and modify the Cisco Unified Communications Manager Administration windows to which the user's user group has update privilege.
- A user with read privilege can view the Cisco Unified Communications Manager Administration windows that belong to the roles to which the user's user group has read privilege. However, a user with read privilege for a window cannot make any changes on those administration windows to which the user has only read privilege. For a user with read privilege, the Cisco Unified Communications Manager Administration application does not display any update buttons or icons.

Roles comprise groups of resources for an application. At installation, default standard roles get created for various administrative functions. However, you can create custom roles that comprise custom groupings of resources for an application.

Note: Certain standard roles have no associated application or resource. These roles provide login authentication for various applications.

This section describes how to add a role to Cisco Unified Communications Manager Administration.

Complete these steps:

1. Choose **User Management > Role**.

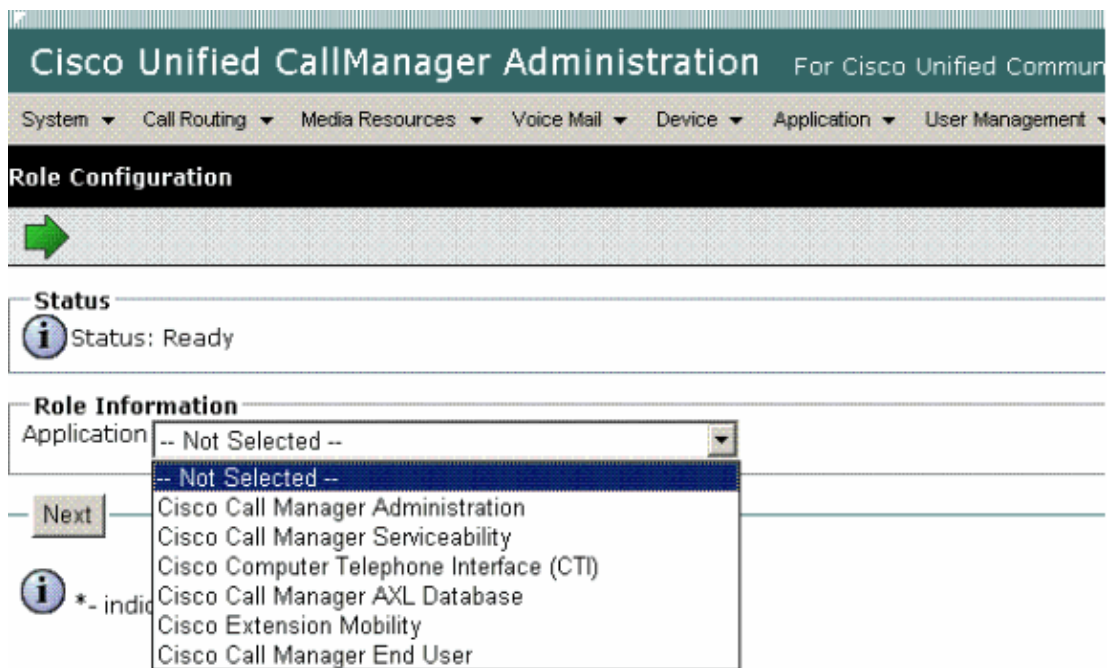
The Find and List Roles window displays.

2. Perform one of these tasks:

- ◆ In order to copy an existing role, locate the appropriate role as described in the Finding a Role section and click the **Copy** button next to the role that you want to copy. In the popup window that displays, enter a name for the new role and click **OK**. Continue with step 4.

Note: Copying a role also copies the privileges that are associated with that role.

- ◆ In order to add a new role, click the **Add New** button, and continue with step 3.
 - ◆ In order to update an existing role, locate the appropriate role as described in the Finding a Role topic and continue with step 4.
3. If you are adding a new role, choose an application from the Application drop-down list box and click **Next**.



4. In the Role Configuration window that displays, enter the appropriate settings.
5. Click **Save** in order to add the role.

The new role gets added to the Cisco Unified Communications Manager database.

User Group Configuration

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

Communications Manager Administration.

Note: The role **Standard CCM Admin Users** must be assigned to a user group to enable its members to logon to the CCMAAdmin website. The role **Standard CCM End Users** must be assigned to a user group to enable its members to logon to the CCMUser website.

Assigning Roles to a User Group

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

Note: When an administrator assigns roles to a user group, the administrator should assign the Standard CCM Admin Users role to the user group. This role enables the users to log into Cisco Unified Communications Manager Administration.

These steps should be completed to assign roles to a user group in Cisco Unified Communications Manager Administration:

1. Choose **User Management > User Group**.

The Find and List User Groups window displays.

2. Find the user group to which you want to assign roles.
3. Click the name of the user group for which you want to assign roles.

The user group that you chose displays. The Users in Group list shows the users that currently belong to the user group.

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

The User Group Configuration window changes to display the Role Assignment pane. For the user group that you chose, the list of assigned roles displays. Choose one of these options:

- ◆ In order to assign roles to the user group, go to step 5.
 - ◆ In order to delete roles from the user group, go to step 9.
5. Click **Assign Role to Group** in order to assign additional roles to the user group.

The Find and List Roles popup window displays.

6. If necessary, use the Find Role search criteria to narrow the list of roles.
7. Choose the roles to assign to this user group by clicking the check boxes next to the role names. In order to close the Find and List Roles popup window without assigning roles to this user group, click **Close**.
8. Click **Add Selected**.
9. In order to delete an assigned role from the user group, select a role in the Role Assignment pane and click **Delete Role Assignment**. Repeat this step for each role that you want to delete from this user group.
10. Click **Save**.

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

Viewing a User's Roles, User Groups, and Permissions

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

1. Choose **User Management > User Group**.

The Find and List User Groups window displays.

2. Find the user group that has the users for which you want to display assigned roles.
3. Click the name of the user group for which you want to view the roles that are assigned to the users.

The User Group Configuration window displays for the user group that you chose. The Users in Group pane shows the users that belong to the user group.

4. For a particular user, click the **i** icon in the Permission column for the user.




Standard CAR Admin Users	
Standard CCM Admin Users	
Standard CCM End Users	
Standard CCM Gateway Administration	
Standard CCM Phone Administration	
Standard CCM Read Only	
Standard CCM Server Maintenance	
Standard CCM Server Monitoring	
Standard CCM Super Users	

The User Privilege window displays. For the user that you chose, this information displays:

- ◆ User groups to which the user belongs
- ◆ Roles that are assigned to the user
- ◆ Resources to which the user has access. For each resource, this information displays:
 - ◇ Application
 - ◇ Resource
 - ◇ Permission (read and/or update)

Role Configuration

Status

 Status: Ready

Role Information

Application* Cisco Call Manager End User

Name*

Description

Resource Access Information

Resource	Privilege	
	<input type="checkbox"/> read	<input type="checkbox"/> update
CCMUser: Device	<input type="checkbox"/>	<input type="checkbox"/>
CCMUser: Directory	<input type="checkbox"/>	<input type="checkbox"/>
CCMUser: Fast Dials	<input type="checkbox"/>	<input type="checkbox"/>
CCMUser: IP Phone Services	<input type="checkbox"/>	<input type="checkbox"/>
CCMUser: Line Settings	<input type="checkbox"/>	<input type="checkbox"/>
CCMUser: Personal Address Book	<input type="checkbox"/>	<input type="checkbox"/>
CCMUser: Service URL	<input type="checkbox"/>	<input type="checkbox"/>
CCMUser: Speed Dial User	<input type="checkbox"/>	<input type="checkbox"/>
CCMUser: User Settings	<input type="checkbox"/>	<input type="checkbox"/>

5. In order to return to the user, choose **Back to User** from the Related Links drop-down list box and click **Go**.

Assign only the Phone Web Page Access to the End Users

Perform these steps in order to assign only the phone web page access to the end users:

1. Go to **User Management > End User**. Click the **Add** option to create a new end user.
2. Go to **User management > Roles**. Click the **Add** option in order to create new roles and check the **Read, Update** option for these two resources: **Directory Number web pages** and **Phone web pages** for this role.
3. Go to **User management > User groups**. Click the **Add** option to create a new user group. Go back to the find list and click the **Roles** option across the new user group created. Then assign the role that you had created and save this group.
4. Go to **User management > End user**. Use the **Add to user group** option and add these user groups: **Standard CCM admin users** and the new user group to which you had assigned the role and click **Save**.
5. Open the `<ip-address of CM>/ccmadmin` page and login with the new user. You will get access to only the phone web page and not the other pages.

Troubleshoot

Login to the Personal Directory Fails

In Cisco Unified Communications Manager 6.x, if the login to the personal directory fails with the **PD Error Message** error message, it can be because users had their pins set to change at next login. In order to resolve this issue, go to **User Management > User Groups > Standard CCM End Users > Default password** and disable it.

If the problem still persists, go to **CM administration page > Device > Device settings > Phone services** and verify that the **Personal Directory** service is enabled. If it is already enabled, restart it.

Users cannot Access User Options Page

A Cisco Unified Communications Manager user cannot login to the Cisco Unified Communications Manager user web page with a username and password. This error message is displayed: `Logon failed. Please try again.`

This issue occurs if a user in the user group does not have the corresponding permissions to log in to the Cisco Unified Communications Manager user page.

Before a user can access the User Options web pages, you must use Cisco Unified Communications Manager Administration to add the user to a standard Cisco Unified Communications Manager end user group. In order to do so, choose **User Management > User Group**. You must also associate appropriate phones with the user. In order to perform these procedures, from Cisco Unified Communications Manager Administration, choose **User Management > End User**.

If the problem still persists, then the problem is a link between the LDAP database and Cisco Unified Communications Manager. Make sure the LDAP authentication URL is correct.

Note: In order to access the CUCM User Options web page, use the `https://<CUCM IP address>/ccmuser` URL. This URL and the username are case sensitive.

Error "User is not authorized to perform this function."

When a user accesses the Options menu on the Cisco Unified Communications Manager user page, this error is received: `User is not authorized to perform this function.`

This issue can be caused by the username being case sensitive. A user logs in to Cisco Unified Communications Manager with a case other than what is specified exactly in the Cisco Unified Communications Manager database. In order to resolve this error, use the same case as is stored in the CallManager database or upgrade to the latest version.

After Changing the Locale, the Language on the CCM User Page does not Change

After choosing the locale for a language, for example Czech Republic, under `CCMUSER page > User Options > User Settings >` and **User Locale**, the Cisco Unified CM User Options web page does not change to Czech Republic. This is always shown in English. The phone and the user account are both set to use this locale.

In order to resolve this issue, open the browser, for example Internet Explorer, and go to **Tools > Internet Options > General tab > Languages**. Then, add the specified language (Czech Republic in this example), and move it to the top of the preference list. Now, the web page for the CCM User options will correctly display the new user locale.

Users Cannot Change Their PIN Settings on the CCM User Page

End users are unable to login to user settings on the CCMUser web page to change the PIN. This error message is received on the user settings option on the CCMUser page:

All features on this page have been disabled by the system administrator

This error message appears when the following parameters are set to **False**, which indicates that the user does not have access rights to change these parameters. The default value for these parameters is set to **True**.

- **Show Locale for Web Pages Settings** This parameter determines whether or not the Locale for Web Pages option appears on the Cisco Unified Communications Manager User Options (CCMUser) window. If this option is enabled, the user can view and change the User Locale Setting Extension Mobility and CCMUser web pages.
- **Show Change Password Option** This parameter determines whether or not the Change Password for a User option appears on the Cisco Unified Communications Manager User Options (CCMUser) window. If this option is enabled, the user can change the Password.
- **Show Change PIN Option** This parameter determines whether or not the Change PIN for a User option appears on the Cisco Unified Communications Manager User Options (CCMUser) window. If this option is enabled, the user can change the PIN.

Therefore, depending on which option you would like the users to change in the CCMUser page, you can set the value to **True**. If you want the PIN option to be available for the user, you would only need to change the value for **Show Change PIN Option** to **True**, and save the changes on the Enterprise Parameters. Then, login using the end user on the CCMUser web page and you should see the option available there.

Related Information

- **CUCM: Roles and Permissions for extension mobility**
- **Cisco Unified Communications Manager Administration Guide**
- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Troubleshooting Cisco IP Telephony**
- **Technical Support & Documentation – Cisco Systems**

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 25, 2007

Document ID: 98796
