



Application User Configuration

The Application User Configuration window in Cisco Unified CallManager Administration allows the administrator to add, search, display, and maintain information about Cisco Unified CallManager application users.

The following topics contain information on managing application user information:

- [Finding an Application User, page 86-1](#)
- [Adding an Application User, page 86-3](#)
- [Application User Configuration Settings, page 86-4](#)
- [Changing an Application User Password, page 86-7](#)
- [Configuring Application Profiles for Application Users, page 86-7](#)
- [Associating Devices to an Application User, page 86-8](#)
- [Application Users and End Users, *Cisco Unified CallManager System Guide*](#)
- [Managing Application User and End User Configuration Checklist, *Cisco Unified CallManager System Guide*](#)

Additional Information

See the [“Related Topics”](#) section on page 86-9.

Finding an Application User

Because you may have several application users in your network, Cisco Unified CallManager lets you locate specific application users on the basis of specific criteria. Use the following procedure to locate application users.



Note

During your work in a browser session, Cisco Unified CallManager Administration retains your application user search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified CallManager Administration retains your application user search preferences until you modify your search or close the browser.

Procedure**Step 1** Choose **User Management > Application User**.

The Find and List Application Users window displays. Use the two drop-down list boxes to search for an application user.

Step 2 From the first Find application user where drop-down list box, choose the following criterion:

- User ID

From the second Find application user where drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 3 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.**Tip**

To find all application users that are registered in the database, click **Find** without entering any search text.

A list of discovered application users displays by

- User ID

**Note**

You can delete multiple application users from the Find and List application users window by checking the check boxes next to the appropriate application users and clicking **Delete Selected**. You can delete all application users in the window, except for default application users, by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records, click the application user name that matches your search criteria.

The window displays the application user that you choose.

Additional Information

See the [“Related Topics” section on page 86-9](#).

Adding an Application User

The following procedure provides instructions on adding a user.

**Note**

If you are adding an application user for Cisco Unity Administrator or Cisco Unity Connection Administrator, you must use the same user name and password that you defined in Cisco Unity and Cisco Unity Connection Administration. Refer to the *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.0* or the *Cisco Unified CallManager 5.0 SCCP Integration Guide for Cisco Unity Connection 2.1*. The user ID provides authentication between Cisco Unity or Cisco Unity Connection and Cisco Unified CallManager Administration.

Procedure

Step 1 Choose **User Management > Application User**.

The Find and List Application Users window displays. Use the two drop-down list boxes to search for an application user.

Step 2 Click **Add New**.

The Application User Configuration window displays.

Step 3 Enter the appropriate settings as described in [Table 86-1](#).

Step 4 When you have completed the user information, save your changes and add the user by clicking **Save**.

Step 5 To show the user privilege report for this application user, from the Related Links drop-down list box, choose User Privilege Report and click **Go**.

The User Privilege window displays for this application user. Refer to the [“Viewing a User’s Roles, User Groups, and Permissions” section on page 89-7](#) for details of the user privilege report.

After you display the user privilege report for this application user, you can return to the Application User Configuration window for this application user. From the Related Links drop-down list box in the User Privilege window, choose Back to Application User and click **Go**.

Next Steps

If you want to associate devices with this application user, continue with the [“Associating Devices to an Application User”](#) procedure.

Additional Information

See the [“Related Topics” section on page 86-9](#).

Application User Configuration Settings

Table 86-1 describes the application user configuration settings. For related procedures, see the “[Related Topics](#)” section on page 86-9.

Table 86-1 **Application User Configuration Settings**

Field	Description
Application User Information	
User ID	Enter the application user identification name. Cisco Unified CallManager 5.0 and subsequent releases permit modifying an existing user ID (provided synchronization with the LDAP server is not enabled). You may use the following special characters: dash (-), underscore (_), “”, and blank spaces.
Password	Enter five or more alphanumeric or special characters for the application user password.
Confirm Password	Enter the user password again.
Digest Credentials	When Cisco Unified CallManager acts as a UAS during digest authentication, the digest credentials that you specify in this field get used for challenges. Enter a string of alphanumeric characters. For information on digest authentication, refer to the <i>Cisco Unified CallManager Security Guide</i> .
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, enter the credentials in this field.
Presence Group	Configure this field with the Presence feature. Note If you are not using this application user with presence, leave the default (None) setting for presence group. From the drop-down list box, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor. The Standard Presence group gets configured at installation. Presence groups configured in Cisco Unified CallManager Administration also appear in the drop-down list box. Presence authorization works with presence groups to allow or block presence requests between groups. Refer to the “ Presence ” chapter in the <i>Cisco Unified CallManager Features and Services Guide</i> for information about configuring permissions between groups.

Table 86-1 Application User Configuration Settings (continued)

Field	Description
Accept Presence Subscription	Configure this field with the Presence feature for presence authorization. If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager performs application-level authorization. Check this check box to authorize Cisco Unified CallManager to accept presence requests that come from this SIP trunk application user. If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, refer to the “Presence” chapter in the <i>Cisco Unified CallManager Security Guide</i>.
Accept Out-of-Dialog Refer	If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager performs application-level authorization. Check this check box to authorize Cisco Unified CallManager to accept Out-of-Dialog REFER requests that come from this SIP trunk application user. For example, to use SIP-initiated transfer features and other advanced transfer-related features, you must authorize Cisco Unified CallManager to accept incoming Out-of-Dialog REFER requests for this application user. If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, refer to the <i>Cisco Unified CallManager Security Guide</i>.
Accept Unsolicited Notification	If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager performs application-level authorization. Check this check box to authorize Cisco Unified CallManager to accept unsolicited notifications that come from this SIP trunk application user. For example, to provide MWI support, you must authorize Cisco Unified CallManager to accept incoming unsolicited notifications for this application user. If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, refer to the <i>Cisco Unified CallManager Security Guide</i>.

Table 86-1 Application User Configuration Settings (continued)

Field	Description
Accept Header Replacement	If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager performs application-level authorization. Check this check box to authorize Cisco Unified CallManager to accept header replacements in messages from this SIP trunk application user. For example, to transfer an external call on a SIP trunk to an external device or party, as in attended transfer, you must authorize Cisco Unified CallManager to accept SIP requests with replaces header in REFERS and INVITES for this application user. If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CallManager sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, refer to the <i>Cisco Unified CallManager Security Guide</i>.
CAPF Information	
Associated CAPF Profiles	In the Associated CAPF Profile pane, the Instance ID for the Application User CAPF Profile displays; that is, if you configured an Application User CAPF Profile for the user. To edit the profile, click the Instance ID; then, click Edit Profile. The Application User CAPF Profile Configuration window displays. For information on how to configure the Application User CAPF Profile, refer to the <i>Cisco Unified CallManager Security Guide</i>.
Device Information	
Available Devices	This list box displays the devices that are available for association with this application user. To associate a device with this application user, select the device and click the Down arrow below this list box. If the device that you want to associate with this application user does not display in this pane, click one of these buttons to search for other devices: • Find more Phones—Click this button to find more phones to associate with this application user. The Find and List Phones window displays to enable a phone search. • Find more Route Points—Click this button to find more route points to associate with this application user. The Find and List CTI Route Points window displays to enable a CTI route point search. • Find more Pilot Points—Click this button to find more pilot points to associate with this application user. The Find and List Pilot Points window displays to enable a pilot point search.

Table 86-1 Application User Configuration Settings (continued)

Field	Description
Permissions Information	
Groups	This list box displays after an application user has been added. The list box displays the groups to which the application user belongs.
Roles	This list box displays after an application user has been added. The list box displays the roles that are assigned to the application user.

Additional Information

See the [“Related Topics” section on page 86-9](#).

Changing an Application User Password

Use the following procedure to change an application user password.

Procedure

-
- | | |
|---------------|---|
| Step 1 | Use the procedure in the “Finding an Application User” section on page 86-1 to find the application user whose password you want to change.

The Application User Configuration window displays with information about the chosen application user. |
| Step 2 | In the Password field, double-click the existing password, which is encrypted, and enter the new password. |
| Step 3 | In the Confirm Password field, double-click the existing, encrypted password and enter the new password again. |
| Step 4 | Click Save . |
-

Additional Information

See the [“Related Topics” section on page 86-9](#).

Configuring Application Profiles for Application Users

After you add a new application user, you can configure a profile for each application. These profiles allow each application user to personalize phone features, Cisco Unified CM Assistant, Cisco Extension Mobility, Cisco Unified CallManager AutoAttendant, and Cisco IP SoftPhone capability.

Before You Begin

Make sure that the application user is in the database. See the [“Finding an Application User” section on page 86-1](#) for more information.

Additional Information

See the [“Related Topics”](#) section on page 86-9.

Associating Devices to an Application User

You can associate devices over which application users will have control. Application users can control some devices, such as phones. Applications that are identified as users can control other devices, such as CTI ports. When application users have control of a phone, they can control certain settings for that phone, such as speed dial and call forwarding.

Before You Begin

To assign devices to an application user, you must access the Application User Configuration window for that user. See the [“Finding an Application User”](#) section on page 86-1 for information on finding existing application users. When the Application User Configuration window displays, perform the following procedure to assign devices.

Procedure

-
- | | |
|---------------|---|
| Step 1 | In the Available Devices list box, choose a device that you want to associate with the application user and click the Down arrow below the list box. |
| Step 2 | To limit the list of available devices, click the Find more Phones , Find more Route Points , or Find more Pilot Points button: <ul style="list-style-type: none">• If you click the Find more Phones button, the Find and List Phones window displays. Perform a search to find the phones to associate with this application user.• If you click the Find more Route Points button, the Find and List CTI Route Points window displays. Perform a search to find the CTI route points to associate with this application user.• If you click the Find more Pilot Points button, the Find and List Pilot Points window displays. Perform a search to find the pilot points to associate with this application user. |
| Step 3 | Repeat the preceding steps for each device that you want to assign to the application user. |
| Step 4 | When you complete the assignment, click Save to assign the devices to the application user. |
-

Additional Information

See the [“Related Topics”](#) section on page 86-9.

Related Topics

- [Finding an Application User](#), page 86-1
- [Adding an Application User](#), page 86-3
- [Application User Configuration Settings](#), page 86-4
- [Changing an Application User Password](#), page 86-7
- [Configuring Application Profiles for Application Users](#), page 86-7
- [Associating Devices to an Application User](#), page 86-8
- [Viewing a User's Roles, User Groups, and Permissions](#), page 89-7
- [Device Association](#), *Cisco Unified CallManager System Guide*
- [Application Users and End Users](#), *Cisco Unified CallManager System Guide*
- [Managing Application User and End User Configuration Checklist](#), *Cisco Unified CallManager System Guide*
- [Cisco Unity Messaging Integration](#), *Cisco Unified CallManager System Guide*
- [LDAP System Configuration](#), page 12-1
- [Directory Number Configuration](#), page 48-1
- [CTI Route Point Configuration](#), page 67-1
- [Cisco Unified IP Phone Configuration](#), page 70-1
- [Role Configuration](#), page 88-1
- [User Group Configuration](#), page 89-1
- [Cisco Extension Mobility](#), *Cisco Unified CallManager Features and Services Guide*
- [Presence](#), *Cisco Unified CallManager Features and Services Guide*
- [Cisco Unified CallManager Security Guide](#)

