Application User Setup

This chapter provides information on managing application user information.

About Application User Setup

In Cisco Unified Communications Manager Administration, use the **User Management** > **Application User** menu path to configure application users.

The Application User Configuration window allows you to add, search, display, and maintain information about application users.

Application Users Configuration Tips

Click **Add New** to set up a new application user. Complete the fields in the Application User Configuration window to configure settings for the application user. For details, see “Application User Settings”.

Note Installation provides a set of default application users for Cisco Unified Communications Manager.

Note If you are adding an administrator account for Cisco Unity or Cisco Unity Connection, you must use the same user name and password that you defined in Cisco Unity and Cisco Unity Connection Administration.The user ID provides authentication between Cisco Unity or Cisco Unity Connection and Cisco Unified Communications Manager Administration. See the applicable Cisco Unified Communications Manager Integration Guide for Cisco Unity or Cisco Unity Connection.

You can configure a Cisco Unified Communications Manager Administration application user as a Cisco Unity or Cisco Unity Connection user by using the Create a Cisco Unity Application User option in the Application User Configuration window. You can then configure any additional settings in Cisco Unity or Cisco Unity Connection Administration.

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.

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

You can associate devices with this application user, manage the application user credentials, and add an administrator user to Cisco Unity or Cisco Unity Connection.

Add Application User

To add an application user, perform the following steps:

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **Application User**.

Step 2 Click **Add New**.

Step 3 Complete the fields in the Application User Configuration window and click **Save**. For field descriptions, see Application User Settings , on page 3.

Step 4 Click **Save**.

What to do next

To associate a device to an application user, see Associate Devices to Application Users , on page 10.

Application User Deletion

Before deleting the application user, determine whether the devices or profiles that are associated with the end user need to be removed or deleted.

You can view the profiles and permissions that are assigned to the application user from the CAPF Information and Permissions Information areas of the Application User Configuration window. You can also choose Dependency Records from the Related Links drop-down list box in the Application User Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Next Steps

If this user is configured in Cisco Unity or Cisco Unity Connection, the user association to Cisco Unified Communications Manager is broken when you delete the user in Cisco Unified Communications Manager Administration. You can delete the orphaned user in Cisco Unity or Cisco Unity Connection Administration. See the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection for more information. See the applicable System Administration Guide for Cisco Unity for more Cisco Unity information.

Application User Settings

Field	Description
Application User Information	
User ID	Enter a unique application user identification name. Cisco Unified Communications Manager allows you to modify an existing user ID (provided synchronization with the LDAP server is not enabled).
Password	Enter alphanumeric or special characters for the application user password. You must enter at least the minimum number of characters that are specified in the assigned credential policy. **Note** Do not use special characters when you create an AXL password for an application user.
Confirm Password	Enter the user password again.
Digest Credentials	Enter a string of alphanumeric characters. Cisco Unified Communications Manager uses the digest credentials that you specify here to validate the SIP user agent response during a challenge to the SIP trunk. For information on digest authentication, see the *Cisco Unified Communications Manager Security Guide*.
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, enter the credentials in this field.
Edit Credential	The Edit Credential button displays after you add this user to the database. Click this button to manage credential information for this user.

Field	Description
BLF 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 Communications Manager Administration also appear in the drop-down list box. Presence authorization works with presence groups to allow or block presence requests between groups.
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 Communications Manager performs application-level authorization. Check this check box to authorize Cisco Unified Communications Manager 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 Communications Manager sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, see the *Cisco Unified Communications Manager Security Guide*.
Accept Out-of-Dialog REFER	If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager performs application-level authorization. Check this check box to authorize Cisco Unified Communications Manager 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 Communications Manager 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 Communications Manager sends a 403 error message to the SIP user agent that is connected to the trunk.

Field	Description
Accept Unsolicited Notification	If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager performs application-level authorization. Check this check box to authorize Cisco Unified Communications Manager to accept unsolicited notifications that come from this SIP trunk application user. For example, to provide MWI support, you must authorize Cisco Unified Communications Manager 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 Communications Manager sends a 403 error message to the SIP user agent that is connected to the trunk.
Accept Replaces Header	If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager performs application-level authorization. Check this check box to authorize Cisco Unified CM 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 CM 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 CM sends a 403 error message to the SIP user agent that is connected to the trunk.
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.

Field	Description
Controlled Devices	This field lists the devices that are associated with the application user. To remove a device, select the device name and click the Up arrow above this list box. To add a device, select a device in the Available Devices list box and click the Down arrow.
CAPF Information	
Associated CAPF Profiles	This pane displays the Instance ID from the CAPF Profile that you configured for this user. To view or update the profile, double-click the Instance ID or click the Instance ID to highlight it; then, click View Details. The Application User CAPF Profile Configuration window displays with the current settings. For information on how to configure the Application User CAPF Profile, see the *Cisco Unified Communications Manager Security Guide*.
Permissions Information	
Groups	This list box displays after an application user record has been saved. The list box displays the groups to which the application user belongs. To add the user to one or more user groups, click the Add to Access Control Group button. The Find and List Access Control Groups window opens as a separate window. Locate the groups to which you want to add the user, click in the check boxes beside those groups, and click Add Selected at the bottom of the window. The Find and List Access Control Groups window closes, and the Application User Configuration window displays, now showing the selected groups in the Groups list box. To remove the user from a group, highlight the group in the Groups list box and click the Remove from Access Control Group button. To view or update a group, double-click the group name or click the group name to highlight it; then, click View Details. The Access Control Group Configuration window displays with the current settings.
Roles	This list box displays after an application user has been added, the Groups list box has been populated, and the user record saved. The list box displays the roles that are assigned to the application user. To view or update a role, double-click the role name or click the role name to highlight it; then, click View Details. The Role Configuration window displays with the current settings.

Add Administrator User to Cisco Unity or Cisco Unity Connection

The Create Cisco Unity Application User link in the Application Configuration window allows you to add a user as an administrator user to Cisco Unity or Cisco Unity Connection. With this method, you configure the application user in Cisco Unified Communications Manager Administration; then, configure any additional settings for the user in Cisco Unity or Cisco Unity Connection Administration.

If you are integrating Cisco Unified Communications Manager with Cisco Unity Connection 7.x, you can use the import feature that is available in Cisco Unity Connection 7.x instead of performing the procedure that is

described in the this section. For information on how to use the import feature, see the User Moves, Adds, and Changes Guide for Cisco Unity Connection 7.x.

The Create Cisco Unity User link displays only if you install and configure the appropriate Cisco Unity or Cisco Unity Connection software. See the applicable Cisco Unified Communications Manager Integration Guide for Cisco Unity or the applicable Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection.

Before you begin

Ensure that you have defined an appropriate template for the user that you plan to push to Cisco Unity or Cisco Unity Connection. For Cisco Unity Connection users, see the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection. For Cisco Unity users, see the System Administration Guide for Cisco Unity.

Procedure

Step 1 Find the application user.

Step 2 From the Related Links drop-down list box, choose the Create Cisco Unity Application User link and click Go.

The Add Cisco Unity User dialog box displays.

Step 3 From the Application Server drop-down list box, choose the Cisco Unity or Cisco Unity Connection server on which you want to create a Cisco Unity or Cisco Unity Connection user and click Next.

Step 4 From the Application User Template drop-down list box, choose the template that you want to use.

Step 5 Click Save.

The administrator account gets created in Cisco Unity or Cisco Unity Connection. The link in Related Links changes to Edit Cisco Unity User in the Application User Configuration window. You can now view the user that you created in Cisco Unity Administration or Cisco Unity Connection Administration.

Note When the Cisco Unity or Cisco Unity Connection user is integrated with the Cisco Unified CM Application User, you cannot edit fields such as Alias (User ID in Cisco Unified Communications Manager Administration), First Name, Last Name, Extension (Primary Extension in Cisco Unified Communications Manager Administration), and so on, in Cisco Unity Administration or Cisco Unity Connection Administration. You can only update these fields in Cisco Unified Communications Manager Administration.

Note Cisco Unity and Cisco Unity Connection monitor the synchronization of data from Cisco Unified Communications Manager. You can configure the sync time in Cisco Unity Administration or Cisco Unity Connection Administration on the Tools menu. For Cisco Unity Connection, see the User Moves, Adds, and Changes Guide for Cisco Unity Connection for more information. For Cisco Unity, see the System Administration Guide for Cisco Unity.

Change Application User Password

Use the following procedure to change an application user password.

Procedure

Step 1 Find the application user whose password you want to change.

The Application User Configuration window displays information about the chosen application user.

Step 2 In the Password field, double-click the existing, encrypted password 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.

Manage Application User Credential Information

Use the following procedure to change or view credential information, such as the associated authentication rules, the associated credential policy, or the time of last password change for an application user. You can edit user credentials only after the user exists in the database.

You cannot save settings in the user Credential Configuration window that conflict with the assigned credential policy. For example, if the policy has the Never Expires check box checked, you cannot uncheck and save the Does Not Expire check box in the user Credential Configuration window. You can, however, set a different credential expiration for the user, including Does Not Expire, if the Never Expires policy setting is not checked; the user setting overrides the policy setting.

You cannot change settings in the user Credential Configuration window that conflict with other settings in the user Credential Configuration window. For example, if the User Cannot Change box is checked, you cannot check the User Must Change at Next Login check box.

The Credential Configuration window provides approximate event times; the system updates the form at the next authentication query or event.

Before you begin

Create the application user in the database.

Procedure

Step 1 Use the Finding an Application User window to find the application user configuration (**User Management** > **Application User**).

The Application User Configuration window displays the configuration information.

Step 2 To change or view password information, click the Edit Credential button next to the Password field. The user Credential Configuration window displays.

Step 3 View the credential data for the user or enter the appropriate settings, as described in Table 1: Application User and End User Credential Settings and Fields , on page 9.

Step 4 If you have changed any settings, click Save.

Credential Settings and Fields

The following table describes credential settings for application users and end users. These settings do not apply to application user or end user digest credentials.

Table 1: Application User and End User Credential Settings and Fields

Field	Description
Locked By Administrator	Check this check box to lock this account and block access for this user. Uncheck this check box to unlock the account and allow access for this user. Use this check box when the credential policy specifies that an Administrator Must Unlock this account type after an account lockout.
User Cannot Change	Check this check box to block this user from changing this credential. Use this option for group accounts. You cannot check this check box when User Must Change at Next Login check box is checked.
User Must Change at Next Login	Check this check box to require the user to change this credential at next login. Use this option after you assign a temporary credential. You cannot check this check box when User Cannot Change check box is checked.
Does Not Expire	Check this check box to block the system from prompting the user to change this credential. You can use this option for low-security users or group accounts. If checked, the user can still change this credential at any time. When the check box is unchecked, the expiration setting in the associated credential policy applies. You cannot uncheck this check box if the policy setting specifies Does Not Expire.
Reset Hack Count	Check this check box to reset the hack count for this user and clear the Time Locked Due to Failed Login Attempts field. The hack count increments whenever authentication fails for an incorrect credential. If the policy specifies No Limit for Failed Logons, the hack count always specifies 0.

Field	Description
Authentication Rule	Select the credential policy to apply to this user credential.
Time Last Changed	This field displays the date and time of the most recent credential change for this user.
Failed Logon Attempts	This field displays the number of failed login attempts since the last successful login, since the administrator reset the hack count for this user credential, or since the reset failed login attempts time expired.
Time of Last Failed Logon Attempt	This field displays the date and time for the most recent failed login attempt for this user credential.
Time Locked by Administrator	This field displays the date and time that the administrator locked this user account. This field goes blank after the administrator unlocks the credential.
Time Locked Due to Failed Logon Attempts	This field displays the date and time that the system last locked this user account due to failed login attempts. Time of hack lockout gets set whenever failed login attempts exceed the configured threshold in the applied credential policy.

Associate Devices to Application Users

Before you begin

To assign devices to an application user, you must access the Application User Configuration window for that user. Use the Finding an Application User window (**User Management** > **Application User**) to find an application user. 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. The selected device moves to the applicationuser.controlledDevices 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:

a) 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.

b) 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.

c) 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.