User Management

User Management Overview

Users are added to Cisco Unified Communications Domain Manager 10.6(1) from the following potential sources:

- Synched in from LDAP
- Synched from Cisco Unified Communications Manager
- Bulk loader template
- Manually created

Typically users are associated with a Site. You can create move filters to automatically assign users to Sites when they are synched from LDAP or Cisco Unified Communications Manager. Bulk loaded and manually created users can be moved using filters or by individually selecting users.

If an IdP server is deployed at a given hierarchy node above Site, then Cisco Unified Communications Domain Manager 10.6(1) can be configured to provide Single Sign On support for users created or synched in at that hierarchy node.

Conflicts between users synched from different sources are handled according to the strategy described in Manage Duplicate User Names, on page 11. For information about user password management, depending on the source of the user, see Password Management, on page 15.

Users associated with a site can be pushed to the Cisco Unified Communications Manager that appears in the Network Device List assigned to that site. Once pushed to Cisco Unified Communications Manager, users become subscribers that can be provisioned with various collaboration services.

When a user is added to Cisco Unified Communications Domain Manager 10.6(1) by any of the above methods, if the user's language is not set, the user's language is inherited from nearest hierarchy node (at or above the user's node) that has a default language set. If no default language is set anywhere in the hierarchy at or above the user's node, the user's language is set to English.

Create User

To manually create a user do the following:

Procedure

Step 1 Log in as the admin at the hierarchy node where you want to create the user.

Step 2 Select **User Management** > **Users**.

Step 3 Click **Add**.

Step 4 At a minimum, complete the following fields:

Fields	Description
Username	Login username. This field is mandatory.
Role	Select the user's role. This field is mandatory.

Fields	Description
Surname	User's family name. This field is mandatory.
Email Address	User email address. This field is mandatory.

Step 5 Click **Save**.

A user is created. If SSO is enabled for the hierarchy node where the user is added, the corresponding SSO user is created.

Note Because IdPs are not configured at the site hierarchy node, SSO can be enabled for a user created at the site level only by selecting **Single Sign On** > **SSO User**, clicking **Add**, and choosing the appropriate IdP that can authenticate the user.

Manage Local Administrators and Operators

Default local Cisco Unified Communications Domain Manager 10.6(1) administrators are created when provider, reseller, customer, and site hierarchy nodes are established. Use this procedure to modify or create additional local administrators or operators. Also use this procedure to create administrators for intermediate nodes.

An administrator for a particular hierarchy level can create or modify the administrators and operators at that hierarchy level and any level below. For example, a Customer XYZ administrator can create other Customer XYZ administrators as well as site administrators for Customer XYZ.

Procedure

Step 1 Log in as an administrator.

Step 2 To create or modify an admin or operator at a level below your current level, set the hierarchy path at the top of the window.
For example, if you have logged in as provider admin, and want to create a customer admin, set the hierarchy path to the customer for which you want to create the admin.

Step 3 Select **User Management** > **Local Admins**.

Step 4 At a minimum, complete the following fields:

Fields	Description
Username	Login username. This field is mandatory.
Email Address	User email address. This field is mandatory.
Password	Set the password. This field is mandatory.

Step 5 To modify an existing administrator or operator, click the administrator or operator.

a) Modify the appropriate settings for the admin or operator.
b) Click **Save**.

Define a Filter

You can define a Filter to easily select multiple users to move according to one or more user attributes.

If you specify multiple attributes, a user will match the filter only if the user matches all of the attributes in the filter. For example, a filter with State=Missouri and City=Kansas City, would not match a user in Kansas City, Kansas.

Procedure

Step 1 Select **User Management** > **Define Filters**.

Step 2 Click **Add**.

Step 3 Provide the following information:

Field	Description
Name	Enter a name for the filter. This field is mandatory.
Move To Hierarchy	Select the target hierarchy node. This field is mandatory.
Move To Role	Select the role to be assigned to the user after the move. The available roles depend on the target hierarchy node selected. This field is mandatory.
Condition	Select a condition for a filter. This field should be set for at least one of the available filters.
Value	Specify the value to evaluate for the condition. This field should be set for at least one of the available filters.

Example:
Set the City Filter to Condition = isexactly and Value = Toronto to move users located in Toronto to the target hierarchy node and give them the target user role.

Step 4 Click **Save**.

The Filter is available to be used to manually move users by selecting **User Management** > **Move Users**. Filters are automatically applied during LDAP and Cisco Unified Communications Manager user synchronization, if the User Move mode is set to automatic.

Methods to Push Users to Cisco Unified Communications Manager

When you manage users in Cisco Unified Communications Domain Manager 10.6(1) there are several steps required to process the new users introduced into the system from the three sources: a synchronization from LDAP directory, a synchronization from Cisco Unified Communications Manager, and a manual configuration in Cisco Unified Communications Domain Manager 10.6(1).

One of these steps is to push the user to the Cisco Unified Communications Manager assigned to the customer and site where the user was added. You can push the user to Cisco Unified Communications Manager from Cisco Unified Communications Domain Manager 10.6(1) in two ways:

1. **Automatic Push—**Enabled or disabled using the **Auto Push to CUCM** checkbox from **Site Management > Sites**
2. **Manual Push—**Performed from **User Management > Manage Users**

There are a variety of options available in Cisco Unified Communications Domain Manager 10.6(1) for configuring users with phones, lines, and features. Depending on the option you choose, you may, or may not, want to automatically push users to Cisco Unified Communications Manager.

To determine if you should automatically push users to Cisco Unified Communications Manager, consider the following guidelines:

- When users are synchronized into Cisco Unified Communications Domain Manager 10.6(1) from an LDAP server, or the users are configured locally on Cisco Unified Communications Domain Manager 10.6(1), and then the **Subscriber Management > Subscribers** menu is used to provision phones, lines, and features for those users, we recommend an automatic user push to Cisco Unified Communications Manager. It does not matter whether you perform the Subscribers configuration through the GUI, bulk loaders, or API; we recommend automatic user push to Cisco Unified Communications Manager in all cases.
- When users are configured locally on Cisco Unified Communications Manager and synchronized into Cisco Unified Communications Domain Manager 10.6(1), the users are already on Cisco Unified Communications Manager, so automatic push to Cisco Unified Communications Manager is not required.

Automatic User Push to Cisco Unified Communications Manager

You can enable Automatic User Push to Cisco Unified Communications Manager by checking the **Auto Push Users to CUCM** box on the **Site Management > Sites > Site Details** page. Automatic User Push is disabled by default.

Users are automatically pushed to a Cisco Unified Communications Manager in the following situations:

- When users are moved to a site hierarchy level (either by filters, username, or usernames):
  - If a Network Device List (NDL) is configured on that site and contains a Cisco Unified Communications Manager, the users are pushed to the Cisco Unified Communications Manager.
  - If an NDL is configured on that site with no Cisco Unified Communications Manager, nothing happens.

    - If an NDL is not configured on that site, nothing happens.

- When an NDL is added to a site after the site was created:
    - If the NDL is configured with a Cisco Unified Communications Manager, the users at the associated site are pushed.
    - If the NDL is not configured with a Cisco Unified Communications Manager, nothing happens.
- When a Cisco Unified Communications Manager is added to an NDL:

  If the NDL is associated with a site, the users on that site are pushed to the new Cisco Unified Communications Manager.
- When a new user is created at the site level:
    - If an NDL is configured on that site and contains a Cisco Unified Communications Manager, the user is pushed to the Cisco Unified Communications Manager.
    - If an NDL is configured on that site with no Cisco Unified Communications Manager, nothing happens.
    - If an NDL is not configured on that site, nothing happens.

Manual User Push to Cisco Unified Communications Manager

You can manually push users to Cisco Unified Communications Manager from hierarchy nodes between customer and site, inclusive.

Note The following limitations exist when pushing users to Cisco Unified Communications Manager:

- A user may be pushed to only one Cisco Unified Communications Manager.
- Users with the SelfService role may be pushed only from a site.

Note For users that have been synched from LDAP, you can use **Subscriber Management** > **Quick Add Subscriber** to push the users to Cisco Unified Communications Manager, instead of this procedure.

Procedure

Step 1 Log in as a provider, reseller, customer, or site admin.

Step 2 Set the hierarchy path to the hierarchy node where the users are located.

Step 3 Select **User Management** > **Manage Users**.

Step 4 Select **Add or update users to CUCM** from the Action drop down list.

Step 5 Select a Network Device List that contains the target Cisco Unified Communications Manager server.

Step 6 Select the users to move, or click **Select All**.

Step 7 Click **Save** to move the selected users to Cisco Unified Communications Manager.

Step 8 Verify the users are in Cisco Unified Communications Manager:

a) Select **User Management** > **Provisioning Status**.

b) Verify the users are assigned to the Cisco Unified Communications Manager server.

Step 9 Verify that users are available as subscribers. After the users are pushed to Cisco Unified Communications Manager, they appear as subscribers to be assigned phones, lines, and features.

a) Select **Subscriber Management** > **Subscriber**.

b) Verify all the pushed users are listed.

c) Click on one of the users to display the Subscriber page.

What to Do Next

Once users are pushed to Cisco Unified Communications Manager they can be managed with subscriber templates.

Automatic Cisco Unified Communications Manager User Move

Use this procedure to automatically move users synced from Cisco Unified Communications Manager using previously-defined move filters.

Procedure

Step 1 Navigate to **Device Management** > **CUCM** > **Servers**.

Step 2 Click the Cisco Unified Communications Manager server to modify.

Step 3 Click the **Publisher** tab.

Step 4 From the User Move Mode drop-down list, select **Automatic**.

Step 5 Click **Save**.

Subsequently synced Cisco Unified Communications Manager users are automatically moved based on previously-defined user management move filters.

Move Users

Users can be moved between any hierarchy nodes, with the exception of hierarchy nodes above the hierarchy level at which they were originally created or synced in. For example, customer users cannot be moved to a reseller hierarchy node. A common practice might be to move users synced in at a customer hierarchy node to various customer sites.

Note The following additional limitations exist when moving users that have been pushed to Cisco Unified Communications Manager:

- Cisco Unified Communications Manager users can be moved only down the hierarchy.
- An NDL containing the same Cisco Unified Communications Manager that the users were pushed to must be referenced at or below the target hierarchy node.

You can select the users to be moved in the following three ways:

- Move users by filters—allows you to select the users depending on one or more user attributes, for example City or Street
- Move users by usernames—allows you to select multiple users by their usernames
- Move user by username—allows you to move an individual user

When you move users, you select a Move To Role for the users that is appropriate for the target hierarchy node.

Procedure

Step 1 Log in at the appropriate hierarchy level.

Step 2 Select **User Management** > **Move Users**.

Step 3 In the Action field, select the move method.

- If you select **Move users by filters**:
  1. Select one or more Move Filters from the **Available** list and click **Select** to move them to the **Selected** list. You can select filters in a different order to change the order in which they are applied.
  2. Click **Save** to move the users that are defined by the move filters.
- If you select **Move users by usernames**:
  1. Select the target hierarchy node from the Move To Hierarchy menu. The Move To Role field appears.
  2. Select the target user role from the Move To Role menu.
  3. Select the users you want to move or click **Select All**.
  4. Click **Save** to move the users.
- If you select **Move user by username**:
  1. Select the username from the User menu. The Move To Hierarchy field appears.
  2. Select the target hierarchy node from the Move To Hierarchy menu. The Move To Role field appears.

3 Select the target user role from the Move To Role menu.
4 Click **Save** to move the user.

For information about user roles, see Roles.

Step 4 Select **User Management** > **Users** to verify that the users are moved to the target hierarchy.

Check User Provisioning Status

Procedure

Step 1 Login as a provider, reseller, or customer admin.
Step 2 Select **User Management** > **Provisioning Status**.
Step 3 The following information is displayed for each user that is visible to the admin:

Field	Description
Username	User's username
CUCM Server	Cisco Unified Communications Manager to which the user is synched
LDAP Server	LDAP from which the user is synched
Synced To	Hierarchy level where the user was originally synched to or created from
Hierarchy	User's current hierarchy node

You can sort the table by clicking on the field headings. You can search any field where a magnifying glass appears when the cursor is on the field heading.

Sync and Purge LDAP Users

Use this procedure to sync or purge Users synced from an LDAP server.

Procedure

Step 1 Set the hierarchy path to the hierarchy node where the LDAP server is.
Step 2 Click **User Management** > **Sync & Purge** > **LDAP Users**.
Step 3 Provide the information as shown below:

Field	Description
Remove Log Messages	Select if you want to remove user management logs prior to the action.
Remove Log Direction	Select Local to remove logs at the hierarchy of the LDAP server. Select Down to remove logs at and below the hierarchy of the LDAP server. This field appears only if Remove Log Messages is checked.
Action	Select synchronize or purge. This field is mandatory.

Step 4 Click **Save** to initiate the sync or purge action.

Sync Cisco Unified Communications Manager Users, Lines, and Phones

Use this procedure to sync Users, Lines, and Phones from Cisco Unified Communications Manager.

Note Syncing of lines and phones is meant only for self-provisioning and is not intended for a full migration scenario. Only Jabber and desk phones are supported for sync from Cisco Unified Communications Manager. Single Number Reach and Extension Mobility are not supported in terms of adding to Cisco Unified Communications Manager first and then syncing into Cisco Unified Communications Domain Manager.

Procedure

Step 1 Set the hierarchy path to the hierarchy node where the Cisco Unified Communications Manager server is.

Step 2 Click **User Management** > **Sync & Purge** > **CUCM Users, Lines, and Phones**.

Step 3 Provide the information as shown below:

Field	Description
Remove Log Messages	Select if you want to remove user management logs prior to the action.
Remove Log Direction	Select Local to remove logs at the hierarchy of the selected Cisco Unified Communications Manager. Select Down to remove logs at and below the hierarchy of the selected Cisco Unified Communications Manager. This field appears only if Remove Log Messages is checked.
Action	Select synchronize. This field is mandatory.

Field	Description
Cisco Unified CM	Select the Cisco Unified Communications Manager server. Data will be synced from the selected Cisco Unified Communications Manager. This field is mandatory.

Step 4 Click **Save** to initiate the sync action.

Manage Duplicate User Names

Users are created in an LDAP sync, a Cisco Unified Communications Manager sync, or manually in the Cisco Unified Communications Domain Manager 10.6(1) GUI. All users are created according to the following duplicate username guidelines:

- The username of a user cannot be updated if another user in the current hierarchy has the same username. This includes **above, below, or at the same level** in the current hierarchy.
- A user cannot be added if another user that is **above, or was originally above before being moved,** in the current hierarchy has the same username.
- A user cannot be manually added if another user that is **at the same level or below** in the current hierarchy has the same username.
- A user may or may not be synched in from LDAP or Cisco Unified Communications Manager if another user that is **at the same level or below** in the current hierarchy has the same username, depending on the source of the existing user as shown in the tables below:

Table 1: Users created in an LDAP Sync

Original source of existing user	Action
LDAP	Simple user update, if the user is coming from the same LDAP server.
Cisco Unified Communications Manager	Update user + update provisioning status with LDAP server and SyncTo info
Manually created	Update user + update provisioning status with LDAP server and SyncTo info

Table 2: Users created in a Cisco Unified Communications Manager Sync

Original source of existing user	Action
LDAP	User is not synced.

Original source of existing user	Action
Cisco Unified Communications Manager	Simple user update, if the user is coming from the same Cisco Unified Communications Manager server.
Manually created	Update user + update provisioning status with Cisco Unified Communications Manager server and SyncTo info

Note If a user cannot be created or updated during an LDAP or Cisco Unified Communications Manager sync, a log is created in **User Management > Log Messages** and the sync completes successfully. If a user cannot be created or updated manually, an error message is generated.

Important An update is blocked if two duplicate users are from the same source but originate from different servers.

Assign a Credential Policy to a User

In general, a user will inherit a credential policy from the nearest hierarchy node at or above the user's location that has a default credential policy set. However, you can explicitly assign a credential policy to a user.

Procedure

Step 1 Log in as provider, reseller, or customer admin.

Step 2 Select **User Management** > **Users**.

Step 3 Click the user that you want to assign a credential policy to.

Step 4 Click the **Account Information** tab.

Step 5 In the Credential Policy field, select the credential policy from the pulldown menu.
The menu contains all the credential policies available at or above the user's node in the hierarchy.

Step 6 Click **Save**.

Note If a user is already logged in when the credential policy is changed, changes do not take effect until the user logs out and logs in again.

Assign a Credential Policy to an Administrator

In general, an administrator will inherit a credential policy from the nearest hierarchy node at or above the administrator's location that has a default credential policy set. However, you can explicitly assign a credential policy to an administrator.

Procedure

Step 1 Log in as provider, reseller, or customer administrator.

Step 2 Select **User Management** > **Local Admins**.

Step 3 Click the administrator that you want to assign a credential policy to.

Step 4 Click the **Account Information** tab.

Step 5 In the Credential Policy field, select the credential policy from the pulldown menu.
The menu contains all the credential policies available at or above the administrator's node in the hierarchy.

Step 6 Click **Save**.

Note If an administrator already logged on when the credential policy is changed, changes do not take effect until the administrator logs out and logs on again.

Unlock a Locked Out User

If a user is locked out on account of a credential policy violation, an administrator responsible for the user can unlock the user's account.

Procedure

Step 1 Login as provider, reseller, or customer admin.

Step 2 Select **User Management** > **Users**.

Step 3 Click the user whose account you want to unlock.

Step 4 Click the **Account Information** tab.

Step 5 Uncheck the **Locked** check box.

Step 6 Click **Save**.

Unlock a Locked Out Administrator

If an administrator is locked out on account of a credential policy violation, an administrator at a hierarchy node above the locked out administrator can unlock the administrator's account.

Procedure

Step 1 Login as provider, reseller, or customer admin, depending on the location of the locked out administrator.
Step 2 Select **User Management** > **Local Admins**.
Step 3 Click the administrator whose account you want to unlock.
Step 4 Click the **Account Information** tab.
Step 5 Uncheck the **Locked** check box.
Step 6 Click **Save**.

Manually Disable User Account

Usually, a user account is disabled when the password has expired. However, an administrator can manually disable a user account at any time.

Note Manually disabling a user is preferred to manually locking out a user as you can provide the reason for disabling.

Procedure

Step 1 Log in as provider, reseller, or customer admin.
Step 2 Select **User Management** > **Users**.
Step 3 Click the user whose account you want to disable.
Step 4 Click the **Account Information** tab.
Step 5 Check the **Disabled** check box.
Step 6 Enter the reason the account is disabled in the **Reason for Disabled** field. This reason will be displayed to the user when the next login attempt fails.
Step 7 Click **Save**.

Manually Disable Administrator Account

Usually, an administrator account is disabled when the password has expired. However, an administrator at a higher hierarchy level can manually disable an administrator account at any time.

Note Manually disabling an administrator is preferred to manually locking out an administrator as you can provide the reason for disabling.

Procedure

Step 1 Log in as provider, reseller, or customer admin.
Step 2 Select **User Management** > **Local Admins**.
Step 3 Click the administrator whose account you want to disable.
Step 4 Click the **Account Information** tab.
Step 5 Check the **Disabled** check box.
Step 6 Enter the reason the account is disabled in the **Reason for Disabled** field. This reason will be displayed to the administrator when the next login attempt fails.
Step 7 Click **Save**.

Password Management

The following sections describe the various ways passwords are set by default and can be configured between LDAP, Cisco Unified Communications Domain Manager 10.6(1), and Cisco Unified Communications Manager.

User Synced from LDAP to Cisco Unified Communications Domain Manager 10.6(1)

LDAP Authentication can be enabled on Cisco Unified Communications Domain Manager 10.6(1) and if enabled, when the user is synced, the LDAP password is used to log in. If the user is synced from LDAP to Cisco Unified Communications Domain Manager 10.6(1), the password is not synced with other user information that is pulled from LDAP. However, the password can be used to log in and the local password is ignored for users synced in from LDAP.

User Synced from LDAP to Cisco Unified Communications Domain Manager 10.6(1) (SSO Enabled)

If the user is synced from LDAP to Cisco Unified Communications Domain Manager 10.6(1) with SSO enabled, the passwords are defined and enforced at the IdP.

User Synced from LDAP to Cisco Unified Communications Manager

When a user is synced from LDAP to Cisco Unified Communications Manager, the password is not synced like other user information that is pulled from LDAP. If LDAP Authentication is enabled, the password in the LDAP Server is used unless the password was changed locally in Cisco Unified Communications Manager, forcing the Cisco Unified Communications Manager password to be used. However, if LDAP Authentication is not enabled, the default password is whatever was configured in Cisco Unified Communications Manager as the Default. If there is no default password defined, then one needs to be configured manually.

User Synced from Cisco Unified Communications Domain Manager 10.6(1)

When users are synced from Cisco Unified Communications Manager to Cisco Unified Communications Domain Manager 10.6(1), the password is not transferred over. The passwords are blank and need to be configured by an admin before the accounts can be used.

This applies to Cisco Unified Communications Manager users that were originally added manually to Cisco Unified Communications Manager or synced from LDAP.

User Added Manually from User Management

When a user is added manually through User Management, the password is set to the local Cisco Unified Communications Domain Manager 10.6(1) password that was specified when the user was created. When this type of user is pushed to Cisco Unified Communications Manager, the password is not pushed. Instead the password can be configured in one of the following ways:

Create a Default Password with Cisco Unified Communications Manager

1. Log in to Cisco Unified Communications Manager as an admin.
2. Navigate to **User Management > User Settings > Credential Policy Default**.
3. Select the line item that has the **Credential User** to 'End User' and **Credential Type** to 'Password'.
4. Enter the default password in the confirmation box and click **Save**.

Note Ensure the user has the correct role defined.

Or

Manually Set the Password in the CUCM End User Page

1. Log in to Cisco Unified Communications Manager as an admin.
2. Navigate to **User Management > End User**.
3. Filter for the user you wish to modify.
4. Change password fields for the specified user.

Force User Password Change

You can use a credential policy to force users to change their passwords on initial login. However, an administrator can manually force a user password change on the next login attempt.

Procedure

Step 1 Log in as provider, reseller, or customer admin.
Step 2 Select **User Management** > **Users**.
Step 3 Click the user whose password you want to be changed on the next login attempt.
Step 4 Click the **Account Information** tab.
Step 5 Check the **Change Password on Next Login** check box.
Step 6 Click **Save**.

When the user next attempts to login, the user will be prompted to change the password. Once the password is changed the **Change Password on Next Login** check box is cleared.

Force Administrator Password Change

You can use a credential policy to force administrators to change their passwords on initial login. However, an administrator at a higher hierarchy level can manually force an administrator to change password on the next login attempt.

Procedure

Step 1 Log in as provider, reseller, or customer admin.
Step 2 Select **User Management** > **Local Admins**.
Step 3 Click the administrator whose password you want to be changed on the next login attempt.
Step 4 Click the **Account Information** tab.
Step 5 Check the **Change Password on Next Login** check box.
Step 6 Click **Save**.

When the administrator next attempts to login, the administrator will be prompted to change the password. Once the password is changed the **Change Password on Next Login** check box is cleared.

Manage Your Own Account Password

Logged in users or administrators can manage their own account passwords.

Note Users who are configured for Single Sign On or through LDAP do not manage their account passwords in Cisco Unified Communications Domain Manager 10.6(1).

Change Password

To change your own password when you are logged in to Cisco Unified Communications Domain Manager 10.6(1).

Reset My Password

To reset your password from the Login page when you have forgotten your password.

Password Reset Questions

To configure your own password reset questions.

Change Your Own Password

Follow this procedure to change your own password if required:

1. Log in to Cisco Unified Communications Domain Manager 10.6(1) .
2. Click the arrow next to the logged in user at the top right-hand side of the screen.
3. Choose the Change Password option from the drop-down menu. The Change Password screen is displayed.
4. Enter your existing password in the Old Password field.
5. Enter your new password in the New Password field.
6. Confirm your new password by re-entering it in the Repeat New Password field.
7. Click **Change Password** in the button bar. Your password is changed.

Reset Your Own Password

You can reset your password only if you have already provided answers to the security questions created by your administrator.

If you forget your password while attempting to log in to Cisco Unified Communications Domain Manager 10.6(1):

1. Enter your username in the Username field on the Log in screen.
2. Click the **Forgot Password?** hyperlink located below the Log in button.
3. Enter your username again.
4. Click **Reset my password**.
5. Click in each security question field and type the correct answer.
6. Click in the **New Password** field and type your new password.
7. Click in the **Repeat Password** field and re-type your new password.
8. Click **Reset my Password**. Your password is changed.
9. Click the **Login** hyperlink if you want to attempt to log in again.

Configure Your Own Password Reset Questions

Note Configuring your own password reset questions is available only if the credential policy applied to your user account has **Number of Questions Asked During Password Reset** set to > 0.

1. Log in to Cisco Unified Communications Domain Manager 10.6(1).
2. Click the arrow next to the logged in user at the top right-hand side of the screen.
3. Choose the **Password Reset Questions** option from the drop-down menu. The Password Reset Questions screen is displayed.
4. Type your password in the **Current Password*** field.
5. Choose the required security question from the **Question*** drop-down list.
6. Enter your answer to the above question in the **Answer*** field.
7. Repeat steps 5 and 6 until you have configured the required amount of security questions (as determined by your administrator).
8. Click the **Update Security Questions** button in the button bar when complete. Your security questions and answers are updated.

Self Service

Using the Cisco Unified Communications Domain Manager 10.6(1) Self Service interface, end users can configure their own phone settings, including voicemail, call forwarding, availability, and speed dials. For detailed information about the Self Service interface, see *Cisco Unified Communications Domain Manager, Release 10.6(1) Self Service Guide*.

To access the Self Service interface, a user must be assigned a SelfService role in Cisco Unified Communications Domain Manager 10.6(1). A user may get a SelfService role in one of the following ways:

- Automatically when synced from LDAP, if the LDAP Sync has User Role configured to a SelfService role.
- By default when synced from Cisco Unified Communications Manager.
- Manually assigned by an administrator using **User Management** > **Users**.

To access the Self Service interface, the user should enter *https://<service-ip-or-node-name>/selfservice/#//login?theme=cisco_selfservice* in the browser URL field.

Note Access to the Self Service interface and the Cisco Unified Communications Domain Manager 10.6(1) administrative GUI are mutually exclusive. Therefore, if an administrator needs access to the Self Service interface, the administrator will need a second user configured in Cisco Unified Communications Domain Manager 10.6(1) with a SelfService role assigned to it.

Self Service and End User Configuration

As an Administrator, you can:

- Configure various aspects of the Self Service interface
- Provide end user access to Self Service
- Configure services for the end users as required

The following table provides a summary of the configurable items in Self Service.

Table 3: Configurable Items in Self Service Interface

Task or Item	Description	For More Information
End user access	An end user can log into the Self Service GUI if a 'System User' entry exists for the user. A 'System 'User entry is created automatically when a user is added as a subscriber.	See Subscriber Management
End user access	You can grant an end user access to Self Service is by creating a user, with a Self Service role, directly in the System user interface. Note that such a user will not be able to view devices or any services associated with the devices, nor will a manually-added user be able to view personal information such as first name, last name, address, department, and so on.	See Create User, on page 2
User Authentication	Self Service authentication is controlled by the administration interface using the same three authentication methods: Standard, LDAP, and SSO.	See "System User" in the User Authentication Management chapter of *Cisco Unified Communications Domain Manager, Release 10.6(1) Planning and Install Guide*
GUI Themes and Branding	The Self Service GUI interface can be branded by configuring Cascading Style Sheets and images and logos. It uses the same theme upload and download interface used for the Admin GUI. The theme itself however, is different between the Admin and Self Service interface (based on the user role). The login page theme is also loaded from the URL: `https://<host>/selfservice/#/login?theme=mytheme`	See Download, Edit and Update a Theme

Task or Item	Description	For More Information
Personal Phones (Remote Destinations)	You must allocate a remote destination profile (RDP) to an end user for them to be able to manage their own personal phones and simultaneous ring settings. If no RDP is associated to the end user, the Personal Phones management interface in self service is hidden. Note that multiple RDP's per end user is not supported. The Personal Phones management interface in Self Service is also hidden if an end user has more than one RDP associated.	See *Cisco Unified Communications Domain Manager, Release 10.6(1) Self Service Guide*
Dual Mode Phones - Mobile ID	If a user has a dual mode device associated, they can manage the phone number and simultaneous ring settings for the device. If no dual mode device is associated, the relevant settings are hidden in the Self Service interface.	See Configure Phones
Voicemail	Voicemail settings are only visible in the Self Service interface if the user has a Voicemail box.	See Voicemail