



CHAPTER 8

Managing Subscribers and Users

You can add subscribers and users, synchronize subscriber information, move the subscriber services, update user information, and domain specific user roles using Manage Subscribers and Manage Users options in Provisioning.

Managing Subscribers

A subscriber is a person who has active IP Telephony services. Provisioning treats the subscriber as the owner of all active services in the voice network. All services are tied to subscribers.



Note

Any out-of-band configurations (meaning configurations that are performed directly on the processor but not synchronized with Provisioning) can result in failed orders. You must always keep Provisioning synchronized with the processors that it is provisioning.

Creating Subscribers

-
- | | |
|---------------|--|
| Step 1 | Choose Deploy > Subscriber Management > Add Subscribers . |
| Step 2 | In the Manage Subscriber page, enter the necessary information. |
| Step 3 | Click Create . The subscriber is created. You can now update any of the subscriber information. |
-



Note

- The subscriber ID must be unique. It must not be case sensitive. Valid values are alphanumeric characters (A-Z, a-z, 0-9), underscore (_), hyphen (-), period (.), apostrophe ('), space (), and at sign (@).
- To create a subscribers name for Cisco Unified Communications Manager Express and Cisco Unity Express, enter only alphabetical characters in the First Name and Last Name fields. If you use other types of characters, orders for the subscriber will fail.
- To create a subscribers name for Call Processors, the combination of characters for First Name and Last Name cannot exceed 30 characters. If this limit is exceeded, when you place an order, the Call Processor sends an error message.
- Pseudo role allows you to provision phones without an associated user in the Call Processor.

- While selecting roles for subscriber, the default or Employee subscriber role should be configured to match the typical setup of employees in your organization. If you do not configure the default or Employee subscriber role to meet your needs, you may not see all the desired options in the employee subscriber record.
- The DefaultUserType rule (see [DefaultUserType, page 11-6](#)) controls which subscriber role is set as the default. Provisioning comes with the Employee subscriber role configured as the default subscriber role.
- The Self-Care Roles check box is enabled by default while creating a subscriber. For more information, see [Managing Password for Self-Care Account, page 9-2](#).

**Tip**

In the Manage Subscriber page, you can access a particular subscriber's Subscriber Details page. Click either View Subscriber Services or Order Subscriber Services.

Updating Subscriber Information

After a subscriber is created you can use the Manage Subscriber page to do the following:

- Change subscriber's name—Changing the subscriber's name does not also change the phone or line description field for the subscriber (if a phone or line was ordered for the previous subscriber name).

**Note**

Remember the following when entering the subscribers name:


- For Cisco Unified Communications Manager Express and Cisco Unity Express, enter only alphabetical characters in the First Name and Last Name fields. If you use other types of characters, orders for the subscriber will fail.
- For Cisco Unified Communications Manager, the combination of characters for First Name and Last Name cannot exceed 30 characters.

- Change subscriber's phone number.
- Change subscriber's email.
- Change subscriber's department.
- Change roles.
- View subscriber services.
- Order subscriber services.
- Manage passwords. (See [Resetting Subscriber Passwords, page 8-4](#).)
- Synchronize subscriber. Appears only after an order is placed for the subscriber. (See [Synchronizing a Subscriber, page 8-6](#).)

**Note**

Updating subscriber information in the converged mode is the same as in the standalone Prime Collaboration Provisioning application.

To update subscriber information:

-
- Step 1** Choose **Deploy > Subscriber Management > Add Subscribers**.
 - Step 2** In the Manage Subscriber page, click the Chooser icon () next to the Subscriber ID field.
 - Step 3** Select the subscriber that you require.
 - Step 4** Change the desired information and click **Update**.
-

Resetting Subscriber Passwords

You can reset passwords only if you have the correct privileges (see [Table 8-1](#)).

You can reset the following:

- Provisioning login password
- Cisco Unified Communications Manager password (see [Overview of Call Processor Passwords, page 8-5](#))

The Cisco Unified Communications Manager password cannot be modified when the Cisco Unified Communications Manager is configured to use external authentication. Provisioning indicates that the password is updated, even though it is not.

- Cisco Unified Communications Manager PIN
- Cisco Unified Communications Manager Express password (see [Overview of Call Processor Passwords, page 8-5](#))
- Cisco Unity Subscriber password
- Cisco Unity Connection PIN
- Cisco Unity Connection Web password



Note

When resetting the Cisco Unity Connection Web password, if the new password is not a strong password the following error message may appear:

Unity Connection Password: Failed to reset credential : The credential does not contain three of the four required character gro

The password should use a combination of at least three of the following:

- Uppercase letters
- Lowercase letters
- Numbers
- Special characters

You can either reset the password to the Provisioning system default, or specify a new password. You can obtain the default values for the user passwords on these systems from your Provisioning administrator, Managed Service Provider, or corporate IT department.

The following rules control the default passwords:

- DefaultCUPMPassword
- DefaultCallManagerPassword
- DefaultCallManagerPIN
- DefaultDigestCredentialPassword
- DefaultUnitySubscriberPassword
- DefaultWebAccessPassword

For more information about rules, see [Business Rules, page 11-2](#).


Note

After you reset a subscriber's password, you must inform the subscriber of the default value that is required to change their password.

To reset password:

-
- Step 1** Open the Manage Subscriber page for the desired subscriber (see [Updating Subscriber Information, page 8-2](#)).
- Step 2** Click **Manage Passwords**.
- Step 3** In the Password Management page, select Password/PIN/Digest Credentials to modify field. Select the password to be changed from the drop down list.
- Step 4** Do one of the following:
- To set the password to the default, click **Reset to Default**.
 - Specify a new password (and confirm), and then click **Set to New Value**.
- Step 5** Click **Done** to confirm.
-

Overview of Call Processor Passwords

Provisioning subscribers can use their passwords to log into the Call Processors, where they can view and edit the configuration details of the phones associated to them. Subscribers can do the following:

- **For Cisco Unified Communications Manager**—Using the URL `https://ccmhost_ipaddress/ccmuser`, log into a Cisco Unified Communications Manager where they have an account. Through the web interface, the subscriber can view or edit the configuration details of the phones associated to the subscriber.
- **For Cisco Unified Communications Manager Express**—Using the URL `http://cmehost_ipaddress/ccme.html`, log into the Cisco Unified Communications Manager Express through a browser in which they have an account (to access Cisco Unified Communications Manager Express through a browser, separate configurations in Cisco Unified Communications Manager Express are required). Through the web interface, the subscriber can view or edit the configuration details of the phones associated to the subscriber.

Although Cisco Unified Communications Manager Express allows a subscriber to have only one associated phone, Provisioning overcomes this limitation, allowing more than one phone to be associated to the subscriber.

In Cisco Unified Communications Manager Express, new users are created with the same username appended with a tilde (~) and sequence index (starting with 1) from the second and subsequent phones (for example, TestUser and TestUser~1). Subscribers must use the exact username to view the corresponding phone details in the Cisco Unified Communications Manager Express web interface.

When you change the password value in Provisioning, the password value is changed for all of the corresponding usernames in Cisco Unified Communications Manager Express.

Synchronizing a Subscriber


You can synchronize a single subscriber. The subscriber's data in Provisioning is synchronized with the subscriber's data in the Call Processor. For more information about synchronizing, see [Synchronizing Domains, page 4-3](#).

When synchronizing subscribers, remember the following:

- The username and phone number fields may display Unknown for subscribers who were initially created on Cisco Unified Communications Manager Express and then later synchronized to Provisioning.

You can update the subscriber information through Provisioning, but be aware that this information will be pushed to the Cisco Unified Communications Manager Express system, and will overwrite any existing information for the user in the ephone description field.

- If a Cisco Unified Communications Manager Express is the only device present in a Domain and Service Area, during Domain synchronization subscribers are not created in Provisioning if the ephone username command is not configured in Cisco Unified Communications Manager Express. Make sure the ephone username command is configured in Cisco Unified Communications Manager Express for all subscribers.
- For Cisco Unified Communications Manager Express, when using the button command in ephone configuration mode, make sure you only use a colon (:) as the separator. Provisioning only supports a colon as a separator in the button command. If any other separator is used, Provisioning does not display the line in the Subscriber Record Details page. Only the phone is displayed.

-
- Step 1** Open the Manage Subscriber page for the desired subscriber (see [Updating Subscriber Information, page 8-2](#)).
- Step 2** Click **Synchronize Subscriber**.
- A confirmation dialog box appears. The Synchronize Subscriber option does not appear for a subscriber until an order is placed for the subscriber.
-  **Note** When synchronizing a single subscriber from the Manage Subscriber page, in addition to getting the user information from the device, Provisioning runs a Domain synchronization. If the Domain contains a large number of users, the synchronization may take several minutes.
-
- Step 3** Click **OK**.
-

Removing a Subscriber

A subscriber can be removed from Provisioning whether or not it has associated services.

-
- Step 1** Open the Manage Subscriber page for the desired subscriber (see [Updating Subscriber Information, page 8-2](#)).
- Step 2** Click **Remove**.
- If you are removing a subscriber that has services associated to it, you are prompted to confirm that you want to disassociate the services before removing the subscriber.
- If the subscriber does not have any services associated to it, you are prompted to confirm removal of the subscriber.
- When a service is disassociated from a subscriber, the service is not deleted or disassociated on the device (processor); it is only disassociated within Provisioning.
- When a subsequent Domain synchronization occurs, depending on the synchronization rules, the subscriber could be created again, and the services could be associated with the subscriber.
- Step 3** Click **OK**.
-

Moving a Subscriber and the Services

You can move a subscriber from one Domain to another. You can also move a subscriber's associated services.

You cannot move a subscriber and associated services when one of the following is true:

- Subscriber is a Pseudo subscriber.
- Subscriber has pending orders.
- Synchronizations are in progress for the devices in that Domain.

-
- Step 1** Open the Manage Subscriber page for the desired subscriber (see [Updating Subscriber Information, page 8-2](#)).
- Step 2** Click **Move**.
- Step 3** In the Move Subscriber and Services page, select the new Domain for the subscriber.
You can move a subscriber only within accessible Domains.
- Step 4** Select a new Service Area.
The New Service Area drop-down list appears only for services that support change orders in Provisioning. Service Areas associated to the device are listed. A service cannot be moved to another device.
- Step 5** Check the **Apply All** check box to apply the new Service Area settings to all the services.
- Step 6** Click **Perform Move**.
If the move fails for one Service Area, the rest of the Service Area's settings are rolled back. During the subscriber move, the location in the subscriber record is displayed as NA. The Change order for products is completed, and the location on the subscriber record page is updated after a short interval.
-

Moving the Subscriber Services

Subscriber services can be moved from one Service Area to another within a Domain.



Note

When moving multiple services, if one move operation fails, a rollback order is created and all the completed move orders are rolled back to their earlier Service Area.

-
- Step 1** Choose **Deploy > Subscriber Management > Search Subscribers**.
- Step 2** Enter the subscriber details and click **Search**.
- Step 3** Click the relevant subscriber.
- Step 4** In the Subscriber Record Details page, click **Move Services**.
- Step 5** In the Move Subscriber and Services page, select the new Service Area.
- Step 6** Check the **Apply All** check box to apply the new Service Area settings to all the services or check the individual services to apply the new Service Area settings.

Step 7 Click **Perform Move** to move the subscriber services.



Note

Cisco Unity Express does not support Move operation for Voicemail.

Accessing Subscriber Records

Step 1 Choose **Deploy > Subscriber Management > Search Subscribers**.

When searching for subscribers using a subscriber's phone number, the Subscriber Search Result page only displays the contact number for a subscriber. This might not be the number that was used in the search. Also, if the subscriber is assigned multiple numbers that match the search, a record for each number is displayed.

Step 2 Enter the subscriber information and click **Search**.



Tip

Clicking the information icon (i) opens the Manage Subscriber page for the subscriber.

Step 3 Select the subscriber that you require.



Note

You can access the Subscriber Records from the Global Search tool available in the Home page. You must search with the exact name of the subscriber; it takes you to the Subscriber Record Details page.

Creating Subscriber Roles

Subscriber roles control which products and services a subscriber can order. The subscriber role also dictates which Service Areas a subscriber is entitled to access.



Note

Do not confuse subscribers with users. These two roles have different meanings in Provisioning. For a description of a user, see [Managing Users, page 8-13](#).

The default subscriber types are:

- Employee—Default role assigned to new subscribers.

The Employee subscriber role should be configured to match the typical setup of employees in your organization. If you do not configure the employee subscriber role to meet your needs, you may not see all the desired options in the employee subscriber record.

- Contractor.
- Manager.
- Senior Manager.
- Executive.

- **Pseudo**—Used to provision phones that do not have an associated user. Pseudo subscribers cannot be renamed or removed.

These subscriber types exist in each Domain in Provisioning. Each set of subscriber types may be customized in each Domain by adding, removing, or changing these predefined subscriber types.

Using the Pseudo Subscriber Role

You can use a pseudo subscriber to provision phones that do not have an associated user in a Call Processor (for more details, see [Managing Phones Without an Associated Subscriber, page 10-22](#)).

You must first create a subscriber and assign the subscriber the Pseudo subscriber role. The process is the same as creating any subscriber, during the add process you must assign the subscriber the pseudo role (see [Creating Subscribers, page 8-1](#)).

Provisioning a phone for a pseudo subscriber is the same as that for a regular subscriber, except that a user is not created in the Call Processor.

Also, a pseudo subscriber is authorized to manage phone and directory number inventory.

Creating a New Subscriber Role Type

-
- Step 1** Choose **Design > Set Up Deployment > Subscriber Roles**.
- Step 2** In the Subscriber Role Configuration page, click **New Subscriber Role**.
- Step 3** Do the following:
- Enter a name for the new subscriber role. Valid values are space, alphanumeric characters (A-Z, a-z, 0-9), underscore (_), and hyphen (-).
 - Select the appropriate Domain.
 - Click **Save**.



Note

After creating a role, you should associate products to the role (see [Associating Products to a Subscriber Role Type, page 8-11](#)).

Updating a Subscriber Role Type

The following sections describe what you can do to a subscriber role type:

- [Associating Products to a Subscriber Role Type, page 8-11](#)
- [Editing a Subscriber Role's Provisioning Attribute Precedence, page 8-11](#)
- [Changing the Name of a Subscriber Role Type, page 8-12](#)
- [Editing Provisioning Attributes for a Subscriber Role Type, page 8-12](#)
- [Removing a Subscriber Role Type, page 8-12](#)

Associating Products to a Subscriber Role Type

When products are associated to a subscriber role, the subscribers with that role can order the associated products (for information on ordering products, see [Ordering Products and Services, page 10-4](#)).

-
- | | |
|---------------|--|
| Step 1 | Choose Design > Set Up Deployment > Subscriber Roles . |
| Step 2 | In the Options pane, select the Domain where the subscriber role type exists from the View Subscriber Role in Domain field drop-down list. |
| Step 3 | Click Choose Role to View . |
| Step 4 | Click the desired subscriber role type. |
| Step 5 | Click Associate Products . |
| Step 6 | Check the check box next to the products that you want to associate to the subscriber role type. |
| Step 7 | Click Save . |
-

Editing a Subscriber Role's Provisioning Attribute Precedence

When a subscriber belongs to multiple subscriber role types, the precedence setting determines which subscriber type's provisioning attribute settings to use.



-
- | | |
|---------------|--|
| Step 1 | Choose Administration > System Setup > Provisioning Setup > Provisioning Attributes . |
| Step 2 | In the Subscriber Role in field, select the Domain where you want to edit the precedence for the subscriber roles. |
| Step 3 | Click Edit subscriber roles precedence . |

- Step 4** In the Manage Precedence page, click the arrows next to a subscriber role type to move it up or down in the order of precedence.
- Step 5** Click **Save**.
-

Changing the Name of a Subscriber Role Type

- Step 1** Choose **Design > Set Up Deployment > Subscriber Roles**.
- Step 2** In the Options pane, select the Domain where the subscriber role type exists from the View Subscriber Role in Domain field drop-down list.
- Step 3** Click **Choose Role to View**.
- Step 4** Click the desired subscriber role type.
- Step 5** In the View Subscriber Role Type page, click **Update**.
- Step 6** In the Update Subscriber Role Type page, change the subscriber role type name.
- Step 7** Click **Save**.
-

Editing Provisioning Attributes for a Subscriber Role Type

- Step 1** Choose **Design > Set Up Deployment > Subscriber Roles**.
- Step 2** In the Options pane, select the Domain where the subscriber role type exists from the View Subscriber Role in Domain field drop-down list.
- Step 3** Click **Choose Role to View**.
- Step 4** Click the desired subscriber role type.
- Step 5** In the View Subscriber Role Type page, click **Edit Provisioning Attributes**.
- Step 6** In the Provisioning Attribute Management page, click the plus sign next to the attribute heading that you want to edit.
- To edit an attribute's information, click the Edit icon () next to the attribute and make the desired changes.
 - To remove the attribute, click the Clear icon () next to the attribute.
- Step 7** Click **Done**.
-

Removing a Subscriber Role Type

- Step 1** Choose **Design > Set Up Deployment > Subscriber Roles**.
- Step 2** In the Options pane, select the Domain where the subscriber role type exists from the View Subscriber Role in Domain field drop-down list.
- Step 3** Click **Choose Role to View**.
- Step 4** Click the desired subscriber role type.

- Step 5** In the View Subscriber Role Type page, click **Remove**.
- Step 6** In the confirmation dialog box, click **OK**.
-

Managing Users

Users in Provisioning represent logins to the system for people who can access Provisioning to perform various activities. Users can be permitted to perform various roles within Provisioning. These roles can be system-wide (for example, administrators), or they can be associated to a single Domain, which limits the scope of changes that the user can make. A user can also be a subscriber.



Note

Provisioning is configured with a permanent administrator account (globaladmin).

User Roles

Two types of global Provisioning user roles are available: global and domain specific.

Based on their roles, Provisioning users are authorized to perform various tasks in Provisioning (see [Table 8-1](#)). You can create user roles in both standalone Prime Collaboration Provisioning and converged applications. When you integrate a freshly installed Provisioning server (that contains no user data) with the Assurance server, you can create common users for both Assurance and Provisioning, or create Provisioning roles only. When you attach a Provisioning server with existing user data (users and subscribers), then the globaladmin and domain-admin roles are synchronized automatically in the User Management page.

Note the following:

- Only globaladmin and domain-admin users created before attaching Provisioning to an Assurance server are synchronized automatically in the converged UI. After synchronization, the globaladmin and domain-admin receive the privileges of an Assurance Helpdesk role. See the [Cisco Prime Collaboration Administration Guide](#) for more information.
- Users other than globaladmin and domain-admin created before attaching Provisioning to an Assurance server are not synchronized. For example, users with Ordering roles, Approval roles and so on. These users cannot login to the converged UI.
- In the converged mode, multi-domain and single-domain users can be created from the User Management page.


Creating Users

To create users in the converged mode:

- Step 1

Choose **Administration > User Management**.
- Step 2

In the User Management page, click **Add**.
- Step 3

In the Add User window, enter the required user details.
- 

Note
- Since LDAP server performs authorization, specify the same user ID for LDAP server and Prime Collaboration application. To configure LDAP server, see [Configuring LDAP Server Synchronization, page 4-14](#).
 - If you select the LDAP User option, the Password and Confirm Password fields are not displayed.
- Step 4

Select the Provisioning domain.
- Step 5

Select the appropriate roles in the Provisioning Roles check box. You can select both Administration and Maintenance, or any one role.
- Step 6

To create domain specific Provisioning Roles, click **Add Row** under **Domain Specific**. You will see role settings option for General, Ordering and Activity roles. See [Table 8-1](#) for information on authorization roles.
- Step 7

Enter appropriate information, click **Done**.
- Step 8

Click **Save** to save the settings.



Note

You will not be able to view the newly added users in Cisco Unified Communications Manager unless you order any services for that user.

To create users in the standalone Prime Collaboration Provisioning application:

- Step 1

Choose **Administration > Users and Device Access Management > User Management**.
- Step 2

In the Manage User page, select appropriate roles in the Provisioning Roles check box. You can select both Administration and Maintenance, or any one role. See [Table 8-1](#) for information on authorization roles.
- Step 3

Enter the necessary field information and click **Create**.

Table 8-1 Authorization Roles

Authorization Role	Description
Global Roles	
Administration	Has access to all Provisioning functionality.

Table 8-1 Authorization Roles (continued)

Authorization Role	Description
Maintenance	Authorized to configure system cleanup activities. See Setting Up the Server, page 2-1 .
Roles for Domain	
In the drop-down list, select the Domain for which you are setting the authorization roles. The selected roles only apply to the selected Domain.	
Policy	Authorized to view phone button templates, modify subscriber roles, and add or update phone inventory.
Infrastructure Configuration Management	Authorized to provision infrastructure configuration objects. When you select this role, you must also select a profile from the Permission Profile box.
Permission Profiles	Sets the permissions for which infrastructure configuration object users assigned this authorization role can configure. (For information on setting permissions, see Managing Infrastructure Configuration Permissions, page 8-19 .)
SelfCare User	Authorized to manage his own services; set up lines, manage services, and configure phone options quickly and easily. Note In the standalone Prime Collaboration Provisioning application, you can enable or disable Self-Care while adding both subscribers and user. In the converged mode, you can enable Self-Care only while adding subscribers. The Self-Care check box is not available while adding users. However, after creating a user, you can assign Self-Care role from the Manage Subscriber page. See Creating a Self-Care Account, page 9-1 .
Ordering Roles	
Users assigned these roles are allowed to place orders for other subscribers and themselves.	
Ordering	Authorized to: <ul style="list-style-type: none"> Add, delete, or update a subscriber within a Domain. Add, delete, or update a subscriber role within a Domain (if the rule for that Domain permits it). Add, delete, or update phones in the inventory within a Domain (if the rule for that Domain permits it). Search and view detailed subscriber information within a Domain. Place an order for a subscriber within a Domain.
Advanced Ordering	Authorized to access all the functionality specified by the Ordering role; can also access Advanced Order Options in the Order Entry page.
Advanced Assignment	Authorized to access all the functionality specified by the Ordering role, and to assign the MAC address for a phone product at the time of order entry.
Activity Roles	
Users assigned one of these roles can perform activities assigned to the group during order processing.	
Approval	Authorized to accept and complete the approval for orders.

Table 8-1 Authorization Roles (continued)

Authorization Role	Description
Assignment	Authorized to accept the user activity for assigning the MAC address.
Shipping	Authorized to accept and complete shipping of orders.
Receiving	Authorized to accept and complete receiving of orders.

Editing User Roles



Note

Global roles apply system-wide and Domain roles only apply to the Domains the user belongs to.

[Table 8-1](#) lists authorization roles that are available in both standalone Prime Collaboration Provisioning, and Provisioning in the converged application.

In both standalone Prime Collaboration Provisioning and converged applications, these authorization roles can be created and managed from the User Management page.


To navigate to the User Management page:

- In the converged application, choose **Administration > User Management**.
- In the standalone Prime Collaboration Provisioning application, choose **Administration > Users and Device Access Management > User Management**

To manage authorization roles in the converged application:

-
- Step 1** Choose **Administration > User Management**.
- Step 2** Select the User Name you want to edit and click **Edit**.
- Step 3** Make necessary changes and save.
-

To manage authorization roles in the standalone Prime Collaboration Provisioning application:

-
- Step 1** Choose **Administration > Users and Device Access Management > User Management**.
- Step 2** In the Manage User page, click the Chooser icon () next to the User ID field.
- Step 3** Click **Edit** next to the assigned roles field. The Assign User Authorization Roles page appears.
-



Tip

To access the Assign User Authorization Roles page, you can also click **Manage Authorization Roles**.

- Step 4** Select the roles that you want to apply to the user.
- Step 5** Click **Update**.
- Step 6** Click **Done**.
-

You can use the User Management page to change the following information:

- User Name
- User's First Name.
- User's Last Name.
- User's email.
- Global Provisioning Roles (Administration or Maintenance).
- Provisioning Roles for Domain.


In the converged mode, the users created via Add User feature are applicable for web client only and these cannot log into the Assurance and/or Provisioning server through the CLI.

Deleting a User

To delete a user from the converged application:

-
- Step 1** Choose **Administration > User Management**.
- Step 2** Select the user you want to delete.
- Step 3** Click **OK**.
-

To remove a user from the standalone Prime Collaboration Provisioning application:

-
- Step 1** Choose **Administration > Users and Device Access Management > User Management**.
- Step 2** In the Manage User page, click the Chooser icon () next to the User ID field.
- Step 3** Open the User Management page for the desired user.
- Step 4** Click **Remove**.
- Step 5** Click **OK**.
-

Resetting User Passwords

You can reset passwords only if you have the correct privileges (see [Table 8-1](#)).

You can reset passwords for the following:

- Provisioning login password
- Cisco Unified Communications Manager password (see [Overview of Call Processor Passwords, page 8-5](#))



Note

The Cisco Unified Communications Manager password cannot be modified when the Cisco Unified Communications Manager is configured to use external authentication. Provisioning indicates that the password is updated, even though it is not.

- Cisco Unified Communications Manager PIN
- Cisco Unified Communications Manager Express password (see [Overview of Call Processor Passwords, page 8-5](#))

- Cisco Unity Subscriber password
- Cisco Unity Connection PIN
- Cisco Unity Connection Web password

**Note**

When resetting the Cisco Unity Connection Web password, if the new password is not a strong password the following error message may appear:

Unity Connection Password: Failed to reset credential : The credential does not contain three of the four required character gro

The password should use a combination of at least three of the following:

- Uppercase letters
- Lowercase letters
- Numbers
- Special characters

You can either reset the password to the Provisioning system default, or specify a new password. You can obtain the default values for the user passwords from your Provisioning administrator, Managed Service Provider, or corporate IT department.

The following rules control the default passwords:

- DefaultCUPMPassword
- DefaultCallManagerPassword
- DefaultCallManagerPIN
- DefaultCallManagerDigestCredentials
- DefaultUnitySubscriberPassword
- DefaultWebAccessPassword

For more information about rules, see [Business Rules, page 11-2](#).

**Note**


After resetting a user's password, you must inform the user of the new value that was set.

To reset user password in the converged application:

- Step 1** Choose **Administration > User Management**.
- Step 2** In the User Management page, select a user.
- Step 3** Click **Change Password**.
- Step 4** In the Reset Password window, enter the new password.
- Step 5** Click **Save**.

To reset user password in the standalone Prime Collaboration Provisioning application:

- Step 1** Choose **Administration > Users and Device Access Management > User Management**.

- Step 2** In the Manage User page, click the Chooser icon () next to the User ID field.
- Step 3** Select the user that you require, and click **Manage Passwords**.
- Step 4** In the Password Management page, select Password/PIN/Digest Credentials to modify field. Select the password to be changed.
- Step 5** Do the following:
- To set the password to the default, click **Reset to Default**.
 - Specify a new password (and confirm it) and then click **Set to New Value**.
- Step 6** Click **Done**.
-

Password Policy

Note the following points when creating a password:

- Passwords cannot be the same as, or reverse of, the username.
- Passwords cannot have a character repeated consecutively more than three times.
- Password cannot be:
 - Cisco or the reverse.
 - Cisc0 (with zero substituted for o).
 - C!sco (with exclamation mark substituted for i).
 - Ci\$co (with dollar sign substituted for s).
 - Any variation of the previous that uses variations in case (uppercase or lowercase).
- Passwords must have lowercase, uppercase, special characters, and digits.
- 8 is the minimum number of characters required (by default, but can be changed).
- 80 is the maximum number of characters allowed (by default, but can be changed).

Provisioning stores the password policy properties in a file named passwordpolicy.properties under opt/cupm/sep. You can modify the properties file to change the password policies as required. You must restart Provisioning whenever you modify the password policy configuration.



Note

If you change the password complexity policy in the properties file to be more stringent, you must update any rule-based passwords set prior to the policy change so that they meet the new password complexity policy.

Managing Infrastructure Configuration Permissions

The Infrastructure Configuration Permission Profiles page is where you set the permissions as to which infrastructure configuration products a user with the Infrastructure Configuration Management authorization role has access to for configuration purposes.

Creating an Infrastructure Configuration Permission Profile

- Step 1** Choose **Administration > Permission Profiles**. (See [Table 1-1](#) to choose the UI path in the standalone Prime Collaboration Provisioning application.)

- Step 2** In the Infrastructure Configuration Permission Profiles page, click **Add New**.
 - Step 3** In the Permission Profile Configuration page, enter a name. Valid values are alphanumeric characters (A-Z, a-z, 0-9), underscore (_), hyphen (-), period (.), and at sign (@).
 - Step 4** (Optional) Enter a description.
 - Step 5** In the Products pane, select the products that you want the profile to be able to configure.
 - Step 6** Click **Save**.
-

Updating an Infrastructure Configuration Permission Profile

-
- Step 1** Choose **Administration > Permission Profiles**. (See [Table 1-1](#) to choose the UI path in the standalone Prime Collaboration Provisioning application.)
 - Step 2** In the Infrastructure Configuration Permission Profiles page, click the profile that you want to update.

- Step 3** In the Permission Profile Configuration page, make the desired changes.
- Step 4** Click **Save**.
-

Deleting an Infrastructure Configuration Permission Profile

- Step 1** Choose **Administration > Permission Profile**. (See [Table 1-1](#) to choose the UI path in the standalone Prime Collaboration Provisioning application.)
- Step 2** In the Infrastructure Configuration Permission Profiles page, click the profile that you want to delete.
- Step 3** In the Permission Profile Configuration page, click **Delete**.
-


Synchronizing Users

If the user is also a subscriber, you can synchronize the user. The user's data in Provisioning is synchronized with the user's data in the Call Processor. For more information about synchronizing, see [Synchronizing Domains, page 4-3](#).

**Note**

When synchronizing a single subscriber from the Manage Subscriber page, in addition to getting the user information from the device, Provisioning Manager runs a Domain synchronization. If the Domain contains a large number of users, the synchronization may take several minutes.

In the standalone Prime Collaboration Provisioning application:


- Step 1** Choose **Administration > Users and Device Access Management > User Management**.
- Step 2** In the Manage User page, click the Chooser icon () next to the User ID field.
- Step 3** Select the user that you require.
- Step 4** Click **Synchronize Subscriber**.

**Note**

The Synchronize Subscriber option does not appear for a user until an order is placed for the user.

- Step 5** Click **OK** to confirm.
-

To synchronize subscriber in the converged mode:


- Step 1** Choose **Deploy > Add Subscribers**.
- Step 2** In the Manage Subscribers page, click the Chooser icon () next to the Subscriber ID field.
- Step 3** Select the user that you require.
- Step 4** Click **Synchronize Subscriber**.

**Note**

The Synchronize Subscriber option does not appear for a user until an order is placed for the user.

Accessing Subscriber Records for a User

To access subscriber records in the standalone Prime Collaboration Provisioning application:

- Step 1** Choose **Administration > Users and Device Access Management > User Management**.
- Step 2** In the Manage User page, click the Chooser icon () next to the User ID field.
- Step 3** Select the user that you require.
- Step 4** Click **View Subscriber Services**.

The Subscriber Record Details page appears.

To access subscriber records for a user in the converged mode, choose **Deploy > Add Subscribers**. Search and then select a subscriber, and view subscriber services.

Unlocking User IDs

Provisioning locks users when they enter the wrong password more times than the maximum number of permitted failed attempts.

**Note**

User ID with administrator privileges is also locked if the overall number of failed attempts is more than the maximum permitted. If an administrator is locked, only the database administrator can unlock the administrator's user ID from the postgres database.

The maximum number of login failure attempts is set in the `dfc.ipt.security.maxFailedLoginAttempt` configuration file that controls password settings; for example:

```
dfc.ipt.security.maxfailedLoginAttempt:5
```

A setting of 1 to 10 represents the number of failed login attempts allowed against a user ID before the account is locked. A setting of 0 disables this feature.

If your account is locked, only a global admin can unlock your user ID. Even when the maximum failure threshold is changed to a larger number; a locked account remains locked until a database administrator unlocks the user ID. The list of locked accounts are listed in this screen and the Unlock button can be used to unlock the locked accounts. Lock and unlock events are shown in the Audit Trail report.

To unlock locked users in the standalone Prime Collaboration Provisioning application:

Step 1 Choose **Administration > User Management > Locked Users**.

The Locked Users page appears.

Step 2 Select the User ID that you want to unlock.

Step 3 Click **Unlock**.

The selected user ID is reactivated.



Note

An entry is created in the Audit Trail report whenever an user is locked or unlocked.

In the converged mode, the unlock option is available in the home dashboard.

Viewing or Logging out Active Sessions

You can view active sessions and log out single or multiple active sessions.

Step 1 Choose **Reports > Administrative Reports > Who Is Logged On**. (See [Table 1-1](#) to choose the UI path in the standalone Provisioning.)

The Logged In Users page appears, showing the list of active sessions.

Step 2 To cancel single or multiple sessions, select the session that you want to end.

Step 3 Click **Log Out**.

The selected session and the user are logged out of the server.



Note

The Logged In Users and Locked Users can be accessed only by the globaladmin.
