Managing Users

Managing Users

A user is a person who has active IP Telephony services. Cisco Prime Collaboration Provisioning allows you to add users, synchronize user information, reapply the services, update user information, and domain specific user roles.

The user role refers to the role that a user will have within an organization. This role dictates the services to which the user is entitled. User roles are predefined in the system.

Note

- Any out-of-band configurations (configurations that are performed directly on the processor but not synchronized with Cisco Prime Collaboration Provisioning) can result in failed orders. You must always synchronize Cisco Prime Collaboration Provisioning with the processors that it is provisioning.
- For Cisco Prime Collaboration Provisioning 12.3 and later, the admin and globaladmin users cannot be created using the User Provisioning page of Cisco Prime Collaboration Provisioning User Interface.
- User ID must contain more than one character.

Adding Users

Note To create a new user retaining the user information during system reboot, refer the following steps.

To add users:

Procedure

Step 1 Choose **User Provisioning**.

Step 2 In the **User Provisioning** page, click **Add.**

Step 3 In the Add User window, if you want to add user click **User** radio button, else click **Open Space** radio button, and enter the User ID, Domain, and Name. Also, enter values for other fields if required.

Expand the **Additional Settings** pane to enter location and contact details.

To launch quick view for a particular domain or user role, while selecting the domain and user role, click the drop-down menu and rest the mouse on quick view icon.

Note While adding or editing a user, you can select multiple user roles. In the Mulitple User Role box, if the popup quickly opens and disappears, then you need to long-press on the arrow icon for a few seconds and the popup reappears.

Step 4 In the **Save and Begin Provisioning** drop-down:

- To save the details and launch the Service Provisioning page for the user, click **Save and Begin Provisioning**.
- To save the details and add another user, click **Save and Add Another**.
- To save the details and close the Add User window, click **Save and Close**.
- To save the details and view services if you choose to Auto-Provision Parameters based on the user role, click **Save and View Services**.

Note

- If you are removing a user who has services associated, you are notified to disassociate the services before removing the user.
- To add a user, the **LDAP integration** field in **Device Setup**page must be **None**.
- The user ID must be unique and case sensitive. Valid values are alphanumeric characters (A-Z, a-z, 0-9), underscore (_), hyphen (-), period (.), apostrophe (‘), space ( ), and at sign (@).
- A user created locally in a Cisco Prime Collaboration Provisioning domain that is LDAP-integrated, will be added to Cisco Unified Communications Manager as a local user. If the Unified Communications Manager processor has a synchronization schedule that sets its LDAP directory settings, the user will be updated to LDAP-integrated after this synchronization occurs.
- For LDAP users, all fields, except Manager User ID, Directory URI, Voicemail email ID, in the **Additional Settings** pane are updated with the values in LDAP only if you perform an LDAP synchronization.
- To create a username 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 user will fail.
- To create a username for Call Processors, the combination of characters for First Name and Last Name cannot exceed 30 characters. If this limit is exceeded when you provision, the Call Processor sends an error message.
- Room role allows you to provision endpoints without an associated user in the Call Processor.
- While selecting roles for user, the default or Employee user role should be configured to match the typical setup of employees in your organization. If you do not configure the default or Employee user role to meet your needs, you may not see all the desired options in the employee user record.
- The DefaultUserType rule controls which user role is set as the default. Cisco Prime Collaboration Provisioning comes with the Employee user role configured as the default user role. If you update the default user role name for a domain in Cisco Prime Collaboration Provisioning, ensure that you update the DefaultUserType rule with the new default role name for that domain.
- Changing the username does not also change the endpoint or line description field for the user (if an endpoint or line was ordered for the previous username).
- 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 user will fail.
- For Cisco Unified Communications Manager, the combination of characters for First Name and Last Name cannot exceed 30 characters.
- If a user does not have any associated services, you are prompted to confirm removal of the user.
- When a service is disassociated from a user, 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 user could be created again, and the services could be associated with the user.

Cross-launching Related Links in Unified Communications Manager and Unity Connection from User Provisioning

Cisco Prime Collaboration Provisioning allows an administrator to cross launch Manager configuration and Assistant configuration for a selected user. As an administrator, you can cross-launch Related Links Pages for Users, Endpoints and Lines from Cisco Prime Collaboration Provisioning. When you cross-launch the Manager configuration and Assistant configuration, you can access the UI and perform any operation directly on the server. Using Single Sign-On, you can cross launch to a few of the applications.

If the Voicemail service is provisioned for the user, the cross-launch links from the Voicemail service: Notification Devices, Alternate Extensions, Greetings, Private Lists.

Rest your mouse pointer over **User Services** in the **Service Details** page (**User Provisioning** select a user), and click the quick view icon to view the Manager configuration and Assistant configuration cross launch link.

Related Topics

Overview of Authorization Roles, on page 12
Single Sign-On for Cisco Prime Collaboration Provisioning

Moving a Single User

Before you begin

Ensure the following before performing a single user move:

- You must have administration privileges to perform this task.
- User can be moved from one domain to another irrespective of the service area, provided they belong to the same call processor.
- User can be moved from one service area to another provided they belong to the same domain and call processor.
- Users cannot be moved unless they are on the same cluster. Users cannot be moved between clusters.

To move a single user from one domain to another:

Procedure

Step 1 Choose **User Provisioning**.

Step 2 In the **User Provisioning** page, select a user and click **Move**.

Move User window appears with options for single user move.

Step 3 Select a new domain from the **New Domain** drop-down list, where the user will be moved.

Step 4 Select the service area from the **New Service Area** drop-down list. This drop-down will list the service areas in a domain based on the services that are configured for a user. For example, if a user has voice mail service

enabled, service areas that are not associated with the Cisco Unified Communications Manager will not be listed in this drop-down.

Step 5 Click **Apply to All Services** to apply all services to the new service area.

If you want to update the services with new settings, you can still select a service and choose a new service area and service template for a particular service.

Check the **Keep Service Area and Template Settings** check box to apply the service area attribute settings alone to the selected service.

Note You cannot apply Service Template settings when you select this check box.

Step 6 Save the settings and click **Move User** to initiate the single user move.

Once the move is successful, a new order is created for that user.

Note To view the move status, hover over **Quick View**.

You cannot move a single user when user synchronization/domain synchronization/Cisco Unified CM synchronization is in progress.

Note **For Cisco Prime Collaboration Provisioning Release 12.5 and later**

Similar to normal users, you can move the Pseudo user IDs across domains and service areas.

Moving Bulk Users

Before you begin

Ensure the following before performing bulk user move:

- You must have administration privileges to perform this task.
- All users selected for bulk move must be from the same domain and cluster.
- Bulk move cannot be performed for multiclustered users.

To move a bulk of users from one domain to another:

Procedure

Step 1 Choose **User Provisioning**.

Step 2 In the **User Provisioning** page, select users and click **Move**.

Bulk Move window appears.

Step 3 Select a new domain from the **New Domain** drop-down list, where the user will be moved.

Step 4 Select the service area from the **New Service Area** drop-down list.

Step 5 Select the **Endpoint Settings** and **Line Settings** if you want to configure new service area settings along with the move.

This is an optional step. Skipping this step will move the users to a new service area with the existing service area settings.

Step 6 Click **Move User** to initiate the bulk move.

Once the move is successful, a new order is created for that user.

Note To view the bulk move status, you can either hover over **Quick View** or click **Bulk Move Status** to view the detailed information on the move.

You cannot move bulk users when user synchronization/domain synchronization/Cisco Unified CM synchronization is in progress.

Note **For Cisco Prime Collaboration Provisioning Release 12.5 and later**

Similar to normal users, you can move the Pseudo user IDs across domains and service areas. You can also move combinations of normal and pseudo users.

Importing Users Using a Text File

Cisco Prime Collaboration Provisioning enables you to import multiple users in a single operation in the following ways:

- Using a file in text (TXT) format
- Using an LDAP server

For information on adding individual users, see Adding Users, on page 1.

To import users using a text file:

Procedure

Step 1 Click **User Provisioning > Import Users**.

Step 2 In the Import User dialog box, click the **From File** radio button.

Step 3 Click **Browse** and select the user import file.

You can also download the sample import file available in the Import Users dialog box for your reference. You can edit the sample file (.txt) using Excel, save the updated spreadsheet as tab-delimited text file, and import the file. OrderType, UserID, LastName, and Domain are mandatory fields (rest of the fields are not mandatory; you can leave them blank).

If you want to enable auto-provisioning for a user, you must set the DoNotAutoProvisionServices field to "False". Also, you must provide the values for Auto-Provisioning ServiceArea and Auto-Provisioning Line Type fields. If you have selected the Line Type as Chosen Line, you must provide the value for Auto-Provisioning Directory Number field.

Note Valid values for user ID field are alphanumeric characters (A-Z, a-z, 0-9), underscore (_), hyphen (-), period (.), apostrophe ('), space ( ), and at sign (@).

Step 4 Click **Import**.

The Import button remains disabled, till you select a file for import. After you click the Import button, the import status of the file will be displayed in the Import Users page. To see the import status of the previously imported file, click **View Last File Import Status**.

Cisco Prime Collaboration Provisioning creates the users based on the details provided in the file. If Auto-provisioning is enabled (set to True), Cisco Prime Collaboration Provisioning will automatically provision the default services for the users based on the Auto-provisioning parameters provided in the uploaded file.

Importing Users From an LDAP Server

To import users from an LDAP server:

Procedure

Step 1 Click **User Provisioning** > **Import Users**.

Step 2 In the Import User dialog box, click the **From LDAP** radio button.

Step 3 Select the domain.

Ensure that Directory Number blocks are available in the selected domain for the users that are synchronized without DN numbers.

Step 4 Click **Import**.

To view the latest LDAP synchronization report, click **View Last LDAP Sync Report**

Note If a user is mapped to a user role for which auto-provisioning is enabled, the configured services will be automatically provisioned for that user.

See Configuring LDAP Server Synchronization for more information.

Exporting Users

Cisco Prime Collaboration Provisioning enables you to export users along with their user information. However, you cannot export the services provisioned for the user.

Note The **Export Users** button is enabled when you select one or more users.

To export users:

Procedure

Step 1 On the **User Provisioning** page, select the number of users that you want to export.

Step 2 Click **Export Users**. A tab-separated data text file is generated. This file contains details of the exported users. You can import the exported users using the **Import Users** button.

Managing User Passwords

You can change the password, reset to default, or prompt users to change their password after their initial login to the application. You must have the correct privileges to manage passwords.

You can update the following:

- Provisioning login password
- Cisco Unified Communications Manager password

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

- Cisco Unified Communications Manager PIN
- Cisco Unified Communications Manager Express password
- Cisco Unity Subscriber password
- Cisco Unity Connection PIN
- Cisco Unity Connection Web password

  When resetting the Cisco Unity Connection Web password, if the new password is not of required length, the following error occurs: `Unity Connection Password: Failed to reset credential: The credential minimum length check failed. Minimum length = 8`

- Unified CM MLPP Password

  This password can be changed using the Manage PIN/Password option only when you set the MLPP User Identification Number and MLPP Precedence Authorization Level for User Service (on the Service Provisioning page).

The Cisco Prime Collaboration Provisioning login password must be a combination of at least three of the following:

- Uppercase letters
- Lowercase letters
- Numbers
- Special characters

You can either change or reset the password to the Provisioning system default, or prompt the user to change their password when they log in to the application next time. 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 Overview of Business Rules.

Note After you reset the password of a user, you must inform the user of the default value that is required to change their password.

To change, reset password, or prompt users to change their password the next time they log in to the application:

Procedure

Step 1 Open the Manage User page for the desired user (see Adding Users, on page 1).

Step 2 Click **Manage Passwords**.

Step 3 On the Password Management page, you can select Password, PIN, or Digest Credentials to modify. Select the password to be changed from the drop-down list.

Step 4 Do one of the following:

- To change the password, specify a new password (and confirm), and then click Apply.
- To set the password to default, click **Reset Password**.
- To prompt users to change their password when they log in to the application the next time, click **Prompt User**.

Step 5 Click **Done** to confirm.

The following rules are applicable while creating a password:

- Password cannot be the same as, or reverse of, the username.
- Password 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).

- Password must have lowercase, uppercase, special characters, and digits.
- The minimum number of characters required is eight (by default, but can be changed).
- The maximum number of characters allowed is 127 (default is 80 characters).

(For Cisco Prime Collaboration Release 11.6 and later) The following enhancements have been made to the existing password policy:

- The password must contain characters from three of the following four character sets: lowercase, uppercase, number, and special character. The number of character sets is configurable (Default is three).
- The minimum number of characters required is six (Default is eight, but can be changed).
- **Allows re-use of password after <number of> changes** (minimum is 0, maximum is 24, and default is 0). This setting enables the user to reuse an existing password after the specified number of password change instances. For example, If the value is set as 0, the user can reuse the same password immediately. If the value is set as 10, the user can reuse the current password after the next ten instances of password changes, that is, if the current password is xyxy, this password can be reused after the next ten password changes.
- **Password can only be changed after <number of> hours** (minimum is 0, maximum is 48, and default is 0). If the value is set as 0, the user can change the password immediately. If the value is set as 24, the user can change the password after 24 hours since change of the last password.
- **Password expires after <number of> days** (minimum is 0, maximum is 365, and default is 0). This setting notifies the user that the password is expiring in "x" number of days and the account is disabled if the password is not changed within the specified timeframe. For example, if the value is set as 0, the password never expires.
- **Show warning message <number of> days before expiration** (minimum is 0, maximum is 31, and default is 0). This setting indicates when the user is notified about password expiration. For example, if the value is set as 0, this setting is disabled, and no warning message is displayed about expiration of the password. If the value is set as 5, a warning message is displayed five days before the expiration of the password.
- **Prompt for confirmation <number of> days before expiration** (minimum is 0, maximum is 30, and default is 0). This setting indicates when the user has to be prompted about expiration and changing of the password. When prompted, the user has to either acknowledge the password expiry or proceed to change the password. For example, if the value is set as 0, this setting is disabled, and no confirmation prompt is displayed about expiration or change of the password. If the value is set as 3, the user is prompted to change the password three days before the expiration of the password.

Cisco Prime Collaboration 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. Restart Cisco Prime Collaboration Provisioning whenever you modify the password policies.

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

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 endpoints (for example,

TestUser and TestUser~1). Use the exact username to view the corresponding endpoint details in the Cisco Unified Communications Manager Express web interface.

When you change the password in Cisco Prime Collaboration Provisioning, the password is changed for all the corresponding user names in Cisco Unified Communications Manager Express.

Resetting User Password Using Forgot Password Link

For Cisco Prime Collaboration Release 11.6 and later

To reset your password using **Forgot password?** link in the login page:

Procedure

Step 1 Click **Forgot password?** link in the login page.

Step 2 Enter your **User ID** and click **Send Email**.

Password reset email will be sent your email account.

Note If you have set security questions for password recovery, then you will be prompted to answer password reset questions. Enter the answers and click **Submit**. Go to Step 4.

Step 3 Click the link in the password reset email to initiate the password reset request.
Change password page of Cisco Prime Collaboration Provisioning appears.

Step 4 Enter your new password and click **Change Password**.
You will be redirected to login page.

Recovering User Password

For Cisco Prime Collaboration Release 11.6 and later

When you log in, you are prompted to configure the password recovery. Click **Yes** to set the recovery email ID, otherwise click **No** to return to the Home page.

To configure the password recovery:

Procedure

Step 1 Choose **Administration** > **Settings** and click **Password** tab.

Step 2 Do one of the following:

- To recover the password using email, click **Send Email** radio button. Click **email server configuration** to configure the email notification settings. For more details, see Configuring System Notifications.
- To recover the password using security questions, click **Security Questions** radio button.

  In the next login, you are prompted to set up security questions and answers after enabling the password recovery using security questions.

Step 3 Click **Update**.

Synchronizing a User

The data of a user in Cisco Prime Collaboration Provisioning is synchronized with the user data in the Call Processor and Unity Connection. For more information about synchronizing, Synchronizing Domains.

When synchronizing users, remember the following:

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

  You can update the user information through Cisco Prime Collaboration 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 users are not created in Cisco Prime Collaboration Provisioning if the ephone username command is not configured in Cisco Unified Communications Manager Express.

  Ensure that the ephone username command is configured in Cisco Unified Communications Manager Express for all users.

- For Cisco Unified Communications Manager Express, when using the button command in ephone configuration mode, ensure that you only use a colon (:) as the separator. Cisco Prime Collaboration Provisioning only supports a colon as a separator in the button command. If any other separator is used, Cisco Prime Collaboration Provisioning does not display the line in the User Record Details page. Only the endpoint is displayed.

Procedure

Step 1 Choose **User Provisioning**.

Step 2 From the list of users, mouse over QuickView, and click **Synchronize User**.

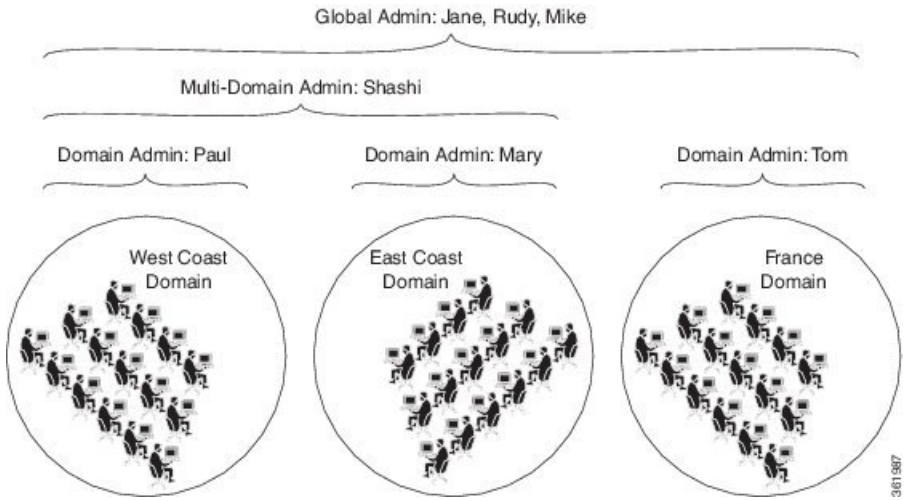
Note If the Domain contains a large number of users, the synchronization may take several minutes.

Overview of Authorization Roles

For Cisco Prime Collaboration Release 11.2 and earlier

Two types of Provisioning user roles are available: global and domain specific. Based on their roles, Provisioning users are authorized to perform various tasks in Provisioning. In the example below, the Domain administrators have administrative privileges for a specific domain. They can set polices and rules for the domain assigned to them. The multi-domain administrators have privileges for more than one domain. The global administrators have access to all Provisioning functionality.

Figure 1: Global and Domain Specific Roles in Provisioning



When you attach a Provisioning server with existing user data, then the globaladmin and domain-admin roles are synchronized automatically in the User Management page.

Note the following:

- Activity roles are available in Cisco Prime Collaboration Provisioning Advanced only. This menu is not available in Cisco Prime Collaboration Provisioning Standard.
- While creating an order for an endpoint in Cisco Prime Collaboration Provisioning Standard, MAC or dummy MAC address is mandatory.

Apart from global and domain administrator roles, a Provisioning user can also have ordering and activity roles. A provisioning user with an ordering role can place orders for users in a particular domain.

Table 1: Authorization Roles Description

Authorization Role	Description
Global Roles	
Administration	Has access to all Provisioning functionality.
Maintenance	Authorized to configure system cleanup activities. See Maintenance Mode.
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. To apply the same authorization role to all available domains, select **Apply to all domains**. **Note** If the administrator selects Apply to all domains, existing roles of the user in all the domains will be overridden with the current selection.	
Policy	Authorized to modify user roles, and add or update endpoint inventory.

Authorization Role	Description
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).
SelfCare User	Authorized to manage his own services; set up lines, manage services, and configure endpoint options quickly and easily. **Note** The SelfCareUser check box is available only if the CreateSelfCareAccounts rule is enabled for the domain.
Ordering Roles Users assigned these roles are allowed to place orders for other users and themselves.	
Ordering	Authorized to: • Add, delete, or update a user within a Domain. • Add, delete, or update a user role within a Domain (if the rule for that Domain permits it). • Add, delete, or update endpoints in the inventory within a Domain (if the rule for that Domain permits it). • Search and view detailed user information within a Domain. • Place an order for a user 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 an endpoint at the time of order entry. Available in Cisco Prime Collaboration Provisioning Advanced only.
Activity Roles Users assigned one of these roles can perform activities assigned to the group during order processing.	

Authorization Role	Description
Approval	Authorized to accept and complete the approval for orders.
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.

Access Control Groups

For Cisco Prime Collaboration Release 11.5 and later

This feature (choose **Administration > Access Control**) enables you, as an administrator, to create access control groups for granting privileges to users to access specific pages and perform specific operations on them. You can assign and restrict system access to the user by providing granular access. You can grant access rights to the users through the Access Control Group, with which the user can access the features and functions based on the granular control. All authorization roles including ordering, shipping, and maintenance are converted to access control groups if you are upgrading to Cisco Prime Collaboration Provisioning 11.5 and later. In addition, the feature enables you to export and import access control groups in different systems having same versions of Cisco Prime Collaboration Provisioning. The following table lists the default access control groups:

For Cisco Prime Collaboration Release 12.1 and later

Read-Only Access for the following administrative UIs has been implemented.

- Logging and ShowTech
- Data Maintenance
- Backup Management
- Updates
- Schedule Synchronization
- License Management
- Single Sign-On
- Rules
- Settings

Table 2: Default Access Control Groups

Name	Description
View Only	Users who only view domains, service areas, service templates, and user roles
Administrators	System Administrator with full access

Name	Description
Help Desk	User can place an order without access to advanced setting

Before you perform operations on the Access Control Group, note the following:

- Cisco Prime Collaboration Provisioning Standard does not support the creation of a new access control group. However, you can modify existing groups and assign users to groups.
- You must upload an advanced license (with delegation feature enabled) to create a new access control group. In standard license, delegation feature is disabled by default.
- You can create up to 1000 groups only.
- “globaladmin” users have full access and are not assigned to any access control groups.
- A user can be assigned more than one Access Control Group.
- A user can be given access to a particular privilege with limited or full access.
- Some privileges have domain-based restrictions.
- Each domain can be controlled with different granular access as suitable.
- Administrator users cannot change or delete the group which they belong, but can change or delete other administrators group.
- Full access groups can be created only either globaladmin or users with full access privilege. The default administrator group can be edited and deleted too.
- For the users other than administrator and full access users, Access Control Group table lists the groups which are created with access items other than full access.
- Buttons and quick view in the respective pages and operations are displayed or hidden based on the granular control.
- Access Control link in quickview of user provisioning is displayed only if the logged in user is a member of Full Access group or having Access Control privilege (either **All** or **Assign users to groups** granular access).

When the users who have access to the **Access Control** page login, they:

- Can create access control groups.
- Can assign users to groups, when the user is assigned a group that has access to access control page with All granular access or Assign users to groups or add group, edit group, delete group, or if the user has full access.
- Cannot assign or edit or delete himself to any group.
- Cannot modify the full access privileged users or globaladmin.

Creating Access Control Group

The following example details the procedure to create an Access Control Group which enable the users to perform:

- Add/Edit/Delete/Import/Move users in User Provisioning page—The user who is assigned with Add/Edit/Delete/Import/Move access can view the relevant buttons.

  For Cisco Prime Collaboration Provisioning release 12.5 and later: The available options are Add/Edit/Delete/Import/Export/Move

- View the configuration information of devices—The user who is assigned with read-only access can only view the relevant information.

To assign the members with Write (Add/Edit/Delete/Import/Move) access to the selected domains for the User Provisioning page, perform the following steps:

1. Create a group with a unique name and add members to the group.
2. Under **Privileges** section, click **Add**.
3. From the **Name** drop down in the dialog box, select **User Provisioning**.
4. Select the domains from the **Accessible Domains** check box as suitable.
5. Select the **Access** check box and the relevant details as suitable.
6. Click **Save**.

For Cisco Prime Collaboration Provisioning release 12.5 and later: The available options are Add/Edit/Delete/Import/Export/Move

To view the configuration information of devices, perform the following steps:

1. Select the group you have already created.
2. Under **Privileges** section, click **Add**.
3. From the **Name** drop down in the dialog box, select **Device Setup**.
4. Select **Read-Only**from the **Access** check box.
5. Click **Save**.

Operations of Access Control Group

You can perform the following operations using access control groups (choose **Administration > Access Control**):

Operation	Description
Add	To add a new Access Control Group • Mandatory field: Group Name. Optional fields are: Description and Members. • Save button is disabled if you do not enter a Group Name and add a Privilege. • Valid values for the Group Name field are alphanumeric characters (A-Z, a-z, 0-9), space and the following special characters: _-./:;=?@^{}[]|`~ _. • A user can be assigned to more than one Access Control Group.
Edit	To modify an existing Access Control Group • Group Name is editable. • **Members** multi-select box does not display the user who has logged in. • In the selected users box, if the logged in user is part of the group, the user is displayed.
Delete	To remove an existing Access Control Group • After deleting a group, users assigned to that group no longer have access to the system.
Copy	Creating a new group by copying Privilege from an existing group • While copying Access Control Group, user is not copied. • Group Name is a mandatory field and is prefixed with "Copy of". • Save button is disabled if Group Name or Privilege is empty.
Export	To export the groups to a tsv file • Access Control Group details are exported to a tsv file. • You can export the users only if the user is assigned to full access groups or the group is created with granular control **All** or **Assign user to groups** for Access Control access item.

Operation	Description
Import	To import the exported groups into a different Cisco Prime Collaboration Provisioning Server • While importing, if the users(which are exported in tsv file) are not available in the new system, an access control group is created and displays the message about the users which are not present in the new system. • If the user is already available in the new system and a part of other access control group, the user is also a part of new group as well during import. • If at least one valid domain is there, an access control group is created with that domain.
Quick View	Hovering over **Quick View** displays the details of the group, including the members and the access list items.

Note Changes to your access control group(s) or privilege(s) invalidates your session and you are logged out. This happens if you perform the following operations:

- Adding a new group
- Editing an existing group(changes to members and privileges)
- Deleting an existing group
- Copy an existing group
- Importing the groups
- Updating group through the user provisioning (user quick view > Access Control).

Privileges with Granular Control

Privilege Name	Description	Granular Access	Domain Control
Full Access	Relates to users who have all the access permissions in Cisco Prime Collaboration Provisioning.	All	NA

Privilege Name	Description	Granular Access	Domain Control
Access Control	Enables you, as an administrator, to configure roles, access control groups, and access privileges for roles.	• All, Read-Only • Write > Add/Edit/Delete Groups • Write > Assign users to groups	NA
Device Setup	Enables you to add or edit or delete UC devices to Cisco Prime Collaboration Provisioning.	All, Read-Only	NA

User Provisioning	Enables you to add or edit or delete or import users, and provision services.	• All, Read-Only
		• Write >
		  • Add/Edit/Delete/ Import/Move
		  • Provision Services
		  • Provision Services with Advanced
		  • Provision Services with Assignment
		  • Password Management
			Yes

Provisioning Setup	Enables you to set up all your user provisioning tasks such as adding and configuring Domains, Service Areas, User Roles, and, Service Templates.	All, Read-Only	No
Infrastructure Configuration	Enables you to view, add, edit, or delete the configuration settings of a Call Processor and Unified Message Processor.	All, Read-Only	Yes
Provisioning History	Enables you to search and view the status of an order.	All, Read-Only	Yes
Dashboard	Enables you to manage the real-time information about the operational status of your processor, device, domain, and users.	All, Logged In Users, Locked Users	NA

Privilege Name	Description	Granular Access	Domain Control
Manage Endpoints	Enables you to upload new and existing endpoints through the user interface.	All	Yes
Manage Directory Numbers	Enables you to store and manage directory numbers that are associated with each Service Area in the Provisioning inventory.	All	NA
Inventory Search	Enables you to browse and search the Provisioning inventory.	All	NA
Unified Communication Services	Lists the Unified Communication services.	All	NA
Getting Started Wizard	Ability to run the Getting Started Wizard.	All	NA
Activities	Enables you to view all the order-related activities, including System Activities.	All	Yes
Reports	Enables you to view details on Service Area, Endpoint Inventory, DNB, Audit Trial, and so on.	All	NA
Audit Trail	Enables you to view details about the user login or logout, password, account, and timeout.	All	NA
License Management and Single Sign-On	Enables you to add or import or delete licenses, and enable SSO in Cisco Prime Collaboration Provisioning to cross-launch the UC applications.	All	NA
Rules and Settings	Supports predefined business rules and allows you to manage Analog Endpoints, Password Policy, self-care feature access, FIPS and custom settings.	All	NA

Privilege Name	Description	Granular Access	Domain Control
Logging and ShowTech	Enables you to view and download application log files.	All	NA
Maintenance and Backup	Enables you to put Cisco Prime Collaboration Provisioning into maintenance mode as well as backup your data, and restore it.	All	NA
Updates and Support	Enables you to view and add endpoint bundles, localization languages, and SSL certificates.	All	NA
Schedule Synchronization	Enables you to synchronize Call Processors, Message Processors, Presence Processors, Active Directories, and Domains.	All	NA

Authorization Roles After Upgrade

For Cisco Prime Collaboration Release 11.5 and later

The following table maps the existing authorization roles with the granular access that the users have after upgrading to Cisco Prime Collaboration 11.5 and later.

Existing Role	Description	Before Upgrade		After Upgrade	
		Accessible Pages	Granular Access	Accessible Pages	Granular Access
Administration	Has access to all Provisioning functionality.	All Pages	All	All Pages	All
Maintenance	Authorized to configure system cleanup activities. See Maintenance Mode.	Dashboard	Pending Order Status	Dashboard	Welcome page
				Maintenance	All
		Data Maintenance	All	Backup Management	All
				Data Maintenance	All

Existing Role	Description	Before Upgrade		After Upgrade	
		Accessible Pages	Granular Access	Accessible Pages	Granular Access
Policy	Authorized to modify user roles, and add or update endpoint inventory.	Manage Endpoints	All	Manage Endpoints	All
		Dashboard	Pending Order Status	Dashboard	Welcome page
		Provisioning Setup	Access only to user roles of assigned domains	Provisioning Setup	Access to domains, service areas, service templates, and user role of all the domains
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.	Dashboard	Pending Order Status	Dashboard	Welcome page
		Infrastructure Configuration	All	Infrastructure Configuration	All

Existing Role	Description	Before Upgrade		After Upgrade	
		Accessible Pages	**Granular Access**	**Accessible Pages**	**Granular Access**
Ordering	Authorized to: • Add, delete, or update a user within a Domain. • Add, delete, or update a user role within a Domain (if the rule for that Domain permits it). • Add, delete, or update endpoints in the inventory within a Domain (if the rule for that Domain permits it). • Search and view detailed user information within a Domain. • Place an order for a user within a Domain.	Dashboard	• Pending Order Status • Device Sync Status • Deployment Details	Dashboard	Pending Order Status
		User Provisioning	• All buttons in User Provisioning • All actions in quick view without advanced and assignment provisioning	User Provisioning	• All buttons in User Provisioning • All actions in quick view with granular access without advanced and assignment provisioning
		Provisioning History	All	Provisioning History	All

Existing Role	Description	Before Upgrade		After Upgrade	
		Accessible Pages	Granular Access	Accessible Pages	Granular Access
Advanced Ordering	Authorized to access all the functionality specified by the Ordering role; can also access Advanced Order Options in the Order Entry page.	Dashboard	• Pending Order Status • Device Sync Status • Deployment Details	Dashboard	Pending Order Status
		User Provisioning	• All buttons in User Provisioning • All actions in quick view with advanced ordering	User Provisioning	• All buttons in User Provisioning • All actions in quick view with advanced ordering
		Provisioning History	All	Provisioning History	All
Advanced Assignment	Authorized to access all the functionality specified by the Ordering role, and to assign the MAC address for an endpoint at the time of order entry. Available in Cisco Prime Collaboration Provisioning Advanced only.	Dashboard	• Pending Order Status • Device Sync Status • Deployment Details	Dashboard	Pending Order Status
		User Provisioning	All buttons and all actions in quick view with assignment	User Provisioning	All buttons in User Provisioning and all actions in quick view with assignment
		Provisioning History	All	Provisioning History	All

Existing Role	Description	Before Upgrade		After Upgrade	
		Accessible Pages	Granular Access	Accessible Pages	Granular Access
Approval	Authorized to accept and complete the approval for orders.	Dashboard	Pending Order Status	Dashboard	Welcome page
		My Activities	Approval or Assignment or Shipping or Receiving of pending orders of the assigned domains	Activities	All (Approval, Assignment, Shipping and Receiving) of the assigned domains
Assignment	Authorized to accept the user activity for assigning the MAC address.	Dashboard	Pending Order Status	Dashboard	Welcome page
		My Activities	Approval or Assignment or Shipping or Receiving of pending orders of the assigned domains	Activities	All (Approval, Assignment, Shipping and Receiving) of the assigned domains
Shipping	Authorized to accept and complete shipping of orders.	Dashboard	Pending Order Status	Dashboard	Welcome page
		My Activities	Approval or Assignment or Shipping or Receiving of pending orders of the assigned domains	Activities	All (Approval, Assignment, Shipping and Receiving) of the assigned domains
Receiving	Authorized to accept and complete receiving of orders.	Dashboard	Pending Order Status	Dashboard	Welcome page
		My Activities	Approval or Assignment or Shipping or Receiving of pending orders of the assigned domains	Activities	All (Approval, Assignment, Shipping and Receiving) of the assigned domains

Configuring Privileges

For Cisco Prime Collaboration Release 11.5 and later

This section details steps to be followed to add or edit or delete the privileges.

Procedure

Step 1 Choose **Administration** > **Access Control** and enter or select the necessary details such as Group Name, Description, and Members.

In the Members drop-down, select the users as suitable.

Step 2 Click **Add** or **Edit** or **Delete** in the Privileges pane as suitable.

Step 3 Click **Selected** from **Accessible Domains** drop-down in the Privilege dialog box and choose the domains you want to access or click **All** to choose all the domains.

Note
- **Accessible Domains** drop-down is enabled only if you choose Provisioning Setup or User Provisioning in **Name** drop-down. For more information on domain control, see Privileges with Granular Control.
- If you select Infrastructure Setup access item, click **Selected** from **Accessible Infrastructure Objects** drop-down and choose the objects you want to access or click **All** to choose all the objects.

Step 4 Select **Access** as suitable.

Step 5 Click **Save**.

Granular Control Support for Access Control Items

The following tables describe the supported granular controls for access control items.

Table 3: Granular Control Support for Access Control Items

Access Control Item	Supported Granular Control	Description
Full Access	Not Applicable	Other than administrators and the users who are part of the full-access privileged group, **Full Access** access items are not listed in Name drop-down in the Add Access or Edit Access dialog box.

Access Control Item	Supported Granular Control	Description
Access Control	• All • Read-Only • Write > Assign Users to Groups • Write > Add/Edit/Delete Groups	Other than administrator and full access users, **Access Control** access items are not listed in Name drop-down in the Add Access or Edit Access dialog box. • With **Write > Add/Edit/Delete Groups** granular control, the user can perform all operations on Access Control page, but cannot assign users to any group. The user cannot assign groups to any user through the user provisioning quick view. While editing or copying a group, Assigned User list box is disabled or hidden. While exporting, users are not exported to the .tsv file. While importing, groups are created but users are not assigned to any group. • With **Assign Users to Groups** granular control, the user can edit the access control groups, but cannot update any items in the access list table. Apart from the Edit button, all other buttons are hidden in the Access Control Group table. In the user quick view, **Access Control** action is displayed through which the user can be assigned to any group. While editing the groups, user (other than administrator user) cannot edit or delete the **Access Control** access item for any of the groups. In addition, the Edit and Delete buttons are disabled in the Access List table.

Access Control Item	Supported Granular Control	Description
Device Setup	• All • Read-Only	• Enabled: **Dashboard**, **Device Setup** menu items, and Links for Device Name under **Device Sync Status**. • **All** and **Selected** radio buttons are disabled for the **Accessible Domains** field. • With **Read-Only** granular control, the user can view all devices in the list page of the device setup. Only **View the Detailed Log** action item is displayed in the device quick view. • The user can add, edit, delete devices, and change the services under UC Services.

Access Control Item	Supported Granular Control	Description
User Provisioning	All, Read-Only Write > • Add/Edit/Delete/Import/Move • Provision Services • Provision Services with Advanced • Provision Services with Assignment • Password Management	

Access Control Item	Supported Granular Control	Description

		• Only the **Dashboard**, and **User Provisioning** menu items are displayed. **Pending Orders** dashlet is displayed if the user has Provision Services granular control or All granular control.
		• **Accessible Domains** is a mandatory field while adding access list, with two radio buttons:
		  • **All**—All domains are accessible.
		  • **Selected**—To select specific domains.
		• With **All** granular control, all buttons are displayed in the User Provisioning table. The user can provision services through auto provisioning, quick service provisioning, add-on services, and legacy ordering flow. The User Provisioning table lists only those users which are associated with the selected domains for access items. The user can set advanced attributes while provisioning services.
		• With **Read-Only** granular control, User Provisioning table lists only those users which are associated with the selected domains in **Accessible Domains**. The user cannot provision services.
		• With **Write > Add/Edit/Delete/Import/Move** granular control, the user can add, edit, delete, import, and move users. While importing users, autoprovisioning does not happen. Only Move and Bulk Move Status buttons are displayed in the User Provisioning table. The user can navigate to the customer record page, but cannot provision services. The user can be moved with services to other domains. Only View action is visible in the service quick view.
		• With **Write > Provision Services** granular control, Provision Services

Access Control Item	Supported Granular Control	Description
		button is enabled in the User Provisioning table. Provision Services, Add User to Unified CM only, Unlock Voicemail actions are displayed in the quick view of User Provisioning. The Custom Services Wizard and Provision Services button are enabled in the customer record page and the user can provision services through quick provisioning and legacy ordering flow and add-on services. While provisioning services through Custom Service Wizard, Advanced Attribute pane is hidden. The user cannot assign the MAC address for the Endpoint service. The user can provision any services through quick service provisioning. • With **Write > Provision Services with Advanced** granular control, Provision Services button is enabled in the User Provisioning table. The Provision Services, Add User to Unified CM only, Unlock Voicemail actions are displayed in the quick view of User Provisioning. The Custom Services Wizard and Provision Services button are enabled in the customer record page. T the user can provision services through quick provisioning and legacy ordering flow and add-on services. While provisioning services through Custom Service Wizard, Advanced Attribute pane is available to perform advanced settings. The user cannot assign the MAC address for the Endpoint service.

Access Control Item	Supported Granular Control	Description
		• With **Write > Provision Services with Assignment** granular control, Provision Services button is enabled in the User Provisioning table. The Provision Services, Add User to Unified CM only, Unlock Voicemail actions are displayed in the quick view of User Provisioning. The Custom Services Wizard and Provision Services button are enabled in the customer record page. The user can provision services through quick provisioning and legacy ordering flow and add-on services. While provisioning services through Custom Service Wizard, Advanced Attribute pane is hidden. The user can assign the MAC address for the Endpoint service. • With **Password Management** granular control, only Manage Password/PIN action are displayed in the quick view of the user. All buttons in the User Provisioning table are hidden. User can navigate to the customer record page. All links for add-on services and all actions are hidden in the service quick view.

Access Control Item	Supported Granular Control	Description

Provisioning Setup	• All
	• Read-Only
		• Only the **Dashboard** and **Provisioning Setup** menu items are displayed. Only the **Deployment Details** dashlet is displayed in the dashboard.
		• Users can add Provisioning Setup access item multiple times in the access list with different domains and granular controls.
		• With **Read-Only** granular control, the user can view Domains, Service Areas, Service Templates, and User Roles in the list page of Domain, Service Area, Service Template, and User Role.
		• With **All** granular control, the user can add, edit, delete, and extract domains, service areas, service templates, and user roles.
		• You can select the domains and have write access to:
		  • Add/Edit/Delete/Export Domains
		  • Add/Edit/Delete/Copy Service Areas
		  • Add/Edit/Delete User Roles
		  • Add/Edit/Delete/Copy Service Templates
		  • With All Attributes
		  • Without Security Attributes

Access Control Item	Supported Granular Control	Description
Infrastructure Configuration	• All • Read-Only	• Only the **Dashboard** and **Infrastructure Setup** menu items are displayed. Under **Infrastructure Setup**, only the **Infrastructure Configuration** menu item is available. • Infrastructure Configuration Permission Profile is merged with Infrastructure Configuration and displayed in the Accessible Infrastructure Objects multiselect box. • With **Read-Only** granular control, the user can view all objects on the Infrastructure Configuration page. • With **All** granular control, the **Add New** button is enabled on the Schedule Configuration page. In addition, the add, edit, and copy buttons are enabled for the objects if a profile is attached, else the buttons are displayed for all the objects. If any permission profile is attached, the user can provision only those objects that are included in the profile.
Provisioning History	• All • Read-Only	• Only the **Dashboard** and **Activities** menu items are displayed. Under the **Activities** menu, only **Provisioning History** is available. • With **Read-Only** granular control, only Search and Clear buttons are enabled on the Provisioning History page. • With **All** granular control, all the buttons are enabled on the Provisioning History page and the user can perform all the operations.

Access Control Item	Supported Granular Control	Description
Dashboard	• Logged In Users • Locked Users • All	• Only the **Dashboard** menu is available with this access item. **Logged In Users** and **Locked User** dashlets are displayed along with other dashlets based on the selected granular control for this item. • **Prime Collaboration Provisioning Capacity** dashlet is displayed only for the administrator users. **Pending Order Status** dashlet is displayed if the group to which user belongs is created with User Provisioning with granular control. **Deployment Details** dashlet is displayed only if the user has access to Provisioning Setup. This dashlet lists only the domains that are selected in the **Accessible Domains** list box. **Device Sync Status** dashlet is displayed if the user has access to Device Setup. • With **Write > Logged In Users** and **Write > Locked Users** granular controls, the relevant dashlet is displayed in the dashboard along with other default dashlets. In addition, the users which are logged in to the system and the locked users are listed as suitable. • With **All** granular control, all the six dashlets are displayed in the dashboard and links for domain name, order, and device name are enabled only if the logged in user has access.

Table 4: Granular Control Support for Access Control Items (Continued)

Access Control Items	Supported Granular Control	Description
Manage Endpoints	• All	• Only **Dashboard** and **Manage Endpoints** under the **Advanced Provisioning** menu items are available. • All the buttons are enabled. The user can perform all the operations on the Manage Endpoints page. The user can assign endpoints to any users available in the system.
Manage Directory Numbers	• All	• Only **Dashboard** and **Manage Directory Numbers** are available under the **Advanced Provisioning** menu. • All the buttons are enabled. The user can perform all the operations on the Manage Directory Numbers page.
Inventory Search	• All	• Only **Dashboard** and **Inventory Search** are available under the **Advanced Provisioning** menu. • All the links for the Sample Reports are enabled. The user can create a new search and edit an existing search.
Unified Communication Services	• All	• Only **Dashboard** and **Unified Communication Services** are available under the **Advanced Provisioning** menu. • Apply button is visible and the user can perform all operations on this page.

Access Control Items	Supported Granular Control	Description
Getting Started Wizard	• All	• Only **Dashboard**, and **Getting Started Wizard** are available under the **Infrastructure Setup** menu. • The user can proceed to all the steps of GSW, and also has access to import LDAP users, and perform auto provisioning. • If only Getting Started Wizard access item is added in the access group and the user clicks **Getting Started Wizard** after logging in, the user is redirected to the dashboard. • If the access control group contains the access lists for both Getting Started Wizard and User Provisioning and the user clicks Getting Started Wizard, the user is redirected to the User Provisioning page.
Infrastructure Configuration Permissions	• All	• Only the **Dashboard**, and **Infrastructure Setup** menu items are available. Under Infrastructure Setup, only the **Infrastructure Configuration** menu is available. • The Add New button in Infrastructure Configuration Permission Profiles is visible for adding new profiles. The user can also update or delete the profiles.
Activities	• All	• Only the **Dashboard** and **Activities** menu items are available. • The user can perform all the operations.

Access Control Items	Supported Granular Control	Description
Reports	• All	• Only the **Dashboard**, and **Reports** menu items are available. • The users can generate reports for **Communication Manager Reporting**, **Service Area**, **Resource Configuration**, **Service Configuration**, **Endpoint Inventory**, **Directory Number Inventory**, **Directory Number Block**, and **Endpoint /Line Mismatch**.
Audit Trail	• All	• Only the **Dashboard**, and **Reports** menu items are available. **Audit Trail** submenu item is displayed under **Reports**. • The users can generate the Audit Trail report that contains events about every PIN or Password change, PIN or Password reset, PIN or Password change on next login, unlock voice mail of a user in a Unity or Unity Connection device, login management, user management, pin or password management, changes in access control group, user roles, self-care, system settings, and synchronization.
License Management and Single Sign-On	• All	• Only **Dashboard**, **License Management**, and **Single Sign-On** are available under the **Administrator**menu. **Audit Trail** submenu item is displayed under **Reports**. • The user can add and delete license, and have access to perform all operations on the Single Sign-On page.

Access Control Items	Supported Granular Control	Description
Rules and Settings	• All	• Only the **Dashboard**, and **Administrator** menu items are available. **Rules**, **Settings**, **System Notification Settings**, and **Domain Notification Settings** submenu items are visible under **Administrator**. • **Configure Rules in Domain** drop-down lists all the domains available in the system on the Configure Rule page. The user has access to perform all the operations on **Settings** page. The **Update** button is visible to the user. The **Test Settings** and **Save** buttons are visible on the **System Notification Settings** page. The user can perform the system configuration notification settings. The **Test Settings**, **Apply to domain template only** and **Apply to all domains**buttons are visible to the user. The user can access the notification configuration domain settings.
Maintenance and Backup	• All	• Only the **Device Setup**, and **Administrator** menu items are available. The **Data Maintenance**, **Maintenance Mode**, and **Backup Management** submenu items are visible under **Administrator**. • The user can update the configure data to be purged and **Update** button is visible on the Data Maintenance page. The user can perform all the operations. **Enter Maintenance Mode** button is visible on the **Maintenance Mode** page.

Access Control Items	Supported Granular Control	Description
Updates and Support	• All	• Only the **Dashboard**, and **Administrator** menu items are available. • The user can perform all the operations. All the buttons are visible in the **Logging and ShowTech**, **Updates**, and **Process Management** pages.
Schedule Synchronization	• All	• Only the **Dashboard**, and **Administrator** menu items are available. • All the buttons are visible and the user can schedule synchronization (**Administrator > Schedule Synchronization**).

Accessing User Records for a User

Procedure

Step 1 Choose **User Provisioning**.

Step 2 Click a specific user.

Step 3 Hover over the quick view icon next to the user in the user record page to view the user information and to perform the actions for the selected user.

In the Service Details pane, the quick view of a service displays an Add-on Service (if applicable) for quick provisioning. For example, if an existing service (called as Anchor service) is an endpoint, you can add Line service (called Add-on Service) by hovering over the quick view icon and clicking the plus symbol or the link beside the symbol. The following table lists the Add-on Service available for Anchor Service.

Anchor Service	Add-on Service
User Services	Enable Mobility, Enable SoftPhone, IM & Presence
Endpoint	Line
EM Access	EM Line
Line, EM Line, and Shared Line	Voicemail, SNR
RDP	RDP Line

Anchor Service	Add-on Service
RDP Line	Voicemail

Viewing or Logging out Active Sessions

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

Procedure

Step 1 Choose **Home** > **Dashboard** > **Logged In Users**.

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.

Using Global Search

You can use the global search field to locate any of the following:

- User ID
- Name
- MAC Address
- Directory Number
- DN Description
- Phone Description
- VM Alias Name
- EM Name

To search using the global search field at the top of the view pane:

Procedure

Step 1 Go to the search field in the top right corner of the Home page.

Step 2 Select the required option form the Search drop-down list:

- User ID

- Name
- MAC Address
- Directory Number
- DN Description
- Phone Description
- VM Alias Name
- EM Name

Step 3 Enter valid information.

Step 4 Press **Enter** to begin the search. You will be taken to the corresponding User Provisioning page if an exact match exists. If more than one match occurs, the system displays all records that matches the search criteria. When you click on a result, you will be redirected to that specific User Provisioning page.