Managing Users

Prime Collaboration supports built-in static roles for Prime Collaboration Assurance and Prime Collaboration Provisioning, with predefined access control that enables you to perform different tasks.

Prime Collaboration Assurance User Roles

User roles are used to define the authorizations of tasks that users can access.

A user can be assigned one of the following roles:

- Helpdesk—Views and accesses network status information only and cannot perform any action on a device or schedule a job that reaches the network.
- Operator—Performs all Helpdesk tasks and tasks related to network data collection. Cannot perform any Device Work Center operations such as adding, discovering, or importing devices. Also, an operator will not be able to configure thresholds for Alarms and Events.
- Network administrator—Performs all Operator tasks and tasks that result in a network configuration change like credential management, threshold settings, and so on.
- System administrator—Performs system related administration tasks such as backup and restore, maintaining log files, configuring users, and so on.
- Super administrator—Can perform tasks that both system administrator and network administrator can perform.

Helpdesk is a preselected role that is assigned to every user in Prime Collaboration.

Prime Collaboration Provisioning User Roles

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

The global Provisioning user is typically an IP telephony expert who configures Prime Collaboration Provisioning business abstractions for voice applications. In Provisioning, the domain-specific user can be an administrator for a single domain and a user for multiple domains or for a single domain.

The user roles for Prime Collaboration Provisioning are explained in Table 5-1:

Table 5-1 Authorization Roles

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

Table 5-1 Authorization Roles (continued)

Authorization Role	Description
Maintenance	Authorized to configure system cleanup activities. For more information, see "Setting up the Server" in the *Cisco Prime Collaboration 9.5 Provisioning Guide*.
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" in the *Cisco Prime Collaboration 9.5 Provisioning Guide*
SelfCare User	Authorized to manage his own services; set up lines, manage services, and configure phone options quickly and easily. **Note** In a Prime Collaboration Provisioning standalone system, you can enable or disable Self-Care while adding subscribers and users. In the converged mode, you can enable Self-Care while adding subscribers only. The Self-Care check box is not available while adding users. However, after creating a user, you can assign the Self-Care role from the Manage Subscriber page. See "Creating a Self-Care Account" in the *Cisco Prime Collaboration 9.5 Provisioning Guide*.
Ordering Roles	
Users assigned these roles are allowed to place orders for other subscribers and themselves.	
Ordering	Authorized to: • 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.

Table 5-1 Authorization Roles (continued)

Authorization Role	Description
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.
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.

Note

- globaladmin and domain admin can create Self-Care roles for any user. Self-Care role can be assigned to a user from the Manage Users page in the standalone Prime Collaboration Provisioning only. For more information, see "Creating a Self-Care Account" in the *Cisco Prime Collaboration 9.5 Provisioning Guide*.
- In the converged mode, you cannot import a user associated with a Self-Care role into the Prime Collaboration Assurance application.

The "Managing Subscribers and Users" chapter in *Cisco Prime Collaboration 9.5 Provisioning Guide* provides detailed information on how to manage users.

Single Sign-On for Prime Collaboration

Prime Collaboration provides the facility to login from the Prime Collaboration Assurance application to Prime Collaboration Provisioning application using the Single Sign-On feature.

In the converged mode, the Prime Collaboration Provisioning application uses the same password for authentication as is used for the Prime Collaboration Assurance application.

Default User Accounts

Prime Collaboration is preconfigured with a default web client administrator user called globaladmin; globaladmin is a superuser who can access both the Prime Collaboration Assurance and Prime Collaboration Provisioning UIs.

Specify a password for globaladmin when you configure your virtual appliance (for either stand-alone products or converged application). You need to use these credentials when you launch the Prime Collaboration web client for the first time.

Prime Collaboration Assurance and Prime Collaboration Provisioning servers support these CLI users: admin and root.

You cannot create CLI users using the web client UI. CLI users are created during OVA configuration. By default, the username is admin; the password is specified during OVA configuration and is used to log into the CLI to check the application status and perform backup and restore.

Caution We recommend that you write down the root password as it cannot be retrieved.

Note

- The users defined in the Prime Collaboration web client are different from the users defined on the Prime Collaboration server (CLI).
- CLI users are not listed on the Prime Collaboration User Management page.
- globaladmin and root follow same set of password validation rules, but the rules for admin are different; because the rules for admin user are predefined in the system. See the *Cisco Prime Collaboration 9.5 Quick Start Guide* for password validation rules for these users.

User Roles and Tasks

Table 5-2 lists the Prime Collaboration Assurance user roles and tasks they are mapped to.

Note that Super administrator has access to all of the UI menus and can perform all tasks listed in the table below. Thus, the super administrator is not listed in the following table.

Table 5-2 Prime Collaboration Assurance User Roles and Task Mapping

Navigation	Task	System Administrator	Network Administrator	Operator	Helpdesk
Home	View Video and Voice Collaboration Dashlets	Yes	Yes	Yes	Yes
	Customize Dashlets	Yes	Yes	Yes	Yes
	Launch Alarm Browser	Yes	Yes	Yes	Yes
	Launch Alarm Summary	Yes	Yes	Yes	Yes
Operate> Diagnose > Sessions Diagnostics	Monitor Sessions	Yes	Yes	Yes	No
	Import Sessions	Yes	Yes	Yes	No
	Launch 360^0 Session View	Yes	Yes	Yes	No
	From 360^0 Session View: Add to watch list	Yes	Yes	Yes	No
	From 360^0 Session View: See alarms	Yes	Yes	Yes	No
	From 360^0 Session View: Monitor Endpoint	Yes	Yes	Yes	No
	From 360^0 Session View: Troubleshoot session or export troubleshoot data	Yes	Yes	Yes	No
	From topology view (endpoints): Add to watch list or remove from watch list	Yes	Yes	Yes	No
	From topology view (endpoints): See alarms	Yes	Yes	Yes	No
	From topology view (endpoints): Monitor Endpoint	Yes	Yes	Yes	No
	From topology view (network connection): Troubleshoot network link	Yes	Yes	Yes	No

Table 5-2 Prime Collaboration Assurance User Roles and Task Mapping (continued)

Navigation	Task	System Administrator	Network Administrator	Operator	Helpdesk
Operate > Diagnose > Endpoint Diagnostics	Monitor endpoint	Yes	Yes	Yes	Yes
	Launch quick view	Yes	Yes	Yes	Yes
	From quick view: Add to watch list or remove from watch list	Yes	Yes	Yes	No
	From quick view: See alarms	Yes	Yes	Yes	Yes
	From quick view: Monitor Session	Yes	Yes	Yes	No
Operate > Diagnose > Diagnostics Summary	View Diagnostics Summary	Yes	Yes	Yes	Yes
Operate > Diagnose > IP-SLA Diagnostics	Start a troubleshooting session	Yes	Yes	Yes	No
Operate > Diagnose > Media Path Analysis	Start Media Path Analysis	Yes	Yes	Yes	No
Operate > Alarms & Events > Alarms	View Alarms	Yes	Yes	Yes	Yes
	Change Status	Yes	Yes	Yes	Yes
	Assign an Alarm	Yes	Yes	Yes	Yes
	Add an annotation	Yes	Yes	Yes	Yes
	Email Notification	Yes	Yes	Yes	Yes
	Launch quick view	Yes	Yes	Yes	Yes
	From quick view: Monitor Endpoint	Yes	Yes	Yes	Yes
	From quick view: See Event History	Yes	Yes	Yes	Yes
Operate > Alarms & Events > Events	View Events	Yes	Yes	Yes	Yes
Operate > Device Work Center	Manage credentials	Yes	Yes	Yes	Yes
	Discover devices	Yes	Yes	Yes	Yes
	Update Inventory	Yes	Yes	Yes	Yes
	Manage Clusters	Yes	Yes	Yes	Yes
	Import Inventory	Yes	Yes	Yes	Yes
	Export Inventory	Yes	Yes	Yes	Yes
	Discover jobs	Yes	Yes	No	No
	Edit Visibility (Edit button)	No	No	No	No
	Customize Events	Yes	Yes	Yes	Yes
	Suspend device management	Yes	Yes	Yes	Yes
	Resume device management	Yes	Yes	Yes	Yes
	Adding to Group	Yes	Yes	Yes	Yes
	Remove from Group	No	No	No	No

Table 5-2 Prime Collaboration Assurance User Roles and Task Mapping (continued)

Navigation	Task	System Administrator	Network Administrator	Operator	Helpdesk
Operate > UC Topology View	View voice dashlets/summary	Yes	Yes	Yes	Yes
Reports > • Interactive Reports • Static Reports • Administrative Reports	Generate reports	Yes	Yes	Yes	Yes (excluding Administrative Reports)
Administration > Job Management	Manage jobs	Yes	Yes	No	No
	Schedule jobs	Yes	Yes	No	No
	Cancel jobs	Yes	Yes	No	No
Administration > User Management	View users	Yes	Yes	No	No
	Add users	Yes	Yes	No	No
	Edit users	Yes	Yes	No	No
	Delete users	Yes	Yes	No	No
	Reset password	Yes	Yes	No	No
	Change password	Yes	Yes	Yes	Yes
Administration > License Management	View license details	Yes	Yes	No	No
	Add license	Yes	Yes	No	No
	Delete license	No	Yes	No	No
Administration > System Setup > Assurance Setup	Configure all system parameters (General Settings, Cisco Prime 360 Integration, CDR Trunk Utilization settings, Call Quality Data Source Management, LDAP Settings, Log Settings, SFTP Settings, IP Phone Inventory Collection Settings, IP Phone XML Inventory Collection Settings, Cluster Data Discovery Settings)	Yes	Yes	No	No
Administration > Alarm & Event Configuration > Event Customization	Customizing event monitoring and severity. Also, defining the threshold value for automatic troubleshooting.	Yes	Yes	No	No

Table 5-3 lists the Prime Collaboration Provisioning user roles and the tasks they are mapped to. The domain roles that perform a specific task has been mentioned. The Administration user role can perform all of the Prime Collaboration Provisioning tasks while the Domain specific admins will have only restricted access to some of the pages.

Table 5-3 Prime Collaboration Provisioning User Roles and Task Mapping

Navigation	Task	Domain Roles	Global Roles
Home > Provisioning > Unified Provisioning Manager Capacity	View information on how much licenses that you have used from the available set.	No Access	Administration
Home > Provisioning > Pending Order Status	View pending orders	Ordering, advanced ordering, advanced assignment, policy, infra Config Management, assignment, approval, shipping, receiving	Administration
Home > Provisioning > Device Sync Status	View device sync status	Ordering, advanced ordering, advanced assignment	Administration
Home > Provisioning > Deployment Details	View deployment details	Ordering, advanced ordering, advanced assignment	Administration
Home > Provisioning > Locked Users	View locked users- users locked after a specified number of failed login attempts	No Access	Administration
Home > Provisioning > Logged In Users	View users who are logged in to the application	No Access	Administration
Design > Set Up Devices	Set up devices, Call Processors, Unified Message Processors, Unified Presence Processors, AAA servers	No Access	Administration
Design > Set Up Depolyment	Create Domains, Service Areas, Provisioning Template, Quick Site Builder	No Access	Administration
	Create Subscriber Roles	Policy	Administration
Deploy > Subscriber Management	Add Subscriber, Search Subscriber	Ordering, advanced Ordering, advanced Assignment	Administration
Deploy > Order Management	Manage activities for a group and user.	No Access	Administration
	Search order	Ordering, advanced Ordering, advanced Assignment	Administration
Deploy > Infrastructure Configuration	Configuring Infrastructure	infraConfigManagement	Administration

Table 5-3 Prime Collaboration Provisioning User Roles and Task Mapping (continued)

Navigation	Task	Domain Roles	Global Roles
Deploy > Batch Provisioning	Perform batch provisioning	No Access	Administration
Deploy > Provisioning Inventory	Manage Phones	Policy	Administration
	Manage directory number, browse and search inventory	No Access	Administration
Report > Interactive Reports > Provisioning Reports	View Provisioning reports	No Access	Administration
Administration > Provisioning Setup	Configure Phone Button Templates	Policy	Administration
	Configure Provisioning Rules, Attributes, and data maintainance	No Access	Administration
Administration > Notification Settings	Configure e-mail settings	No Access	Administration

Adding, Editing, and Deleting a User

You can add a user via UI and assign predefined static roles. The user will have access to the Prime Collaboration web client only and not CLI.

If you are logging in for the first time to the Prime Collaboration Assurance or Prime Collaboration Provisioning web client, log in as globaladmin.

You, as a globaladmin, must create other administrators using real user-IDs as they can be tracked in Audit Trail and in the Prime Collaboration Provisioning order tracking system.

Caution You must not create a user with the name: globaladmin, pmadmin and admin.

When you integrate the Prime Collaboration Provisioning application with Prime Collaboration Assurance, you can import users with domain-specific and global Provisioning roles (who do not have Self-Care roles associated) to the Prime Collaboration Assurance application using the “Import” functionality in the **Administration > User Management** page. You must refresh the “User Management” page to see the list of imported users. For details on Self-Care roles, See “Using Self-Care” chapter in the *Cisco Prime Collaboration 9.5 Provisioning Guide*.

Note You cannot import a Prime Collaboration Provisioning Self-Care user to the Prime Collaboration Assurance application.

You can then check the */opt/emms/emsam/log/importedprovisioninguser.log* file, by logging in as a root user, to find the users who were not imported into Prime Collaboration Assurance database due to several reasons such as duplicate usernames (usernames already used in Prime Collaboration Assurance), usernames with no passwords and so on.

However, when you integrate a freshly installed Prime Collaboration Provisioning application (that contains no user data) with the Prime Collaboration Assurance application, and you wish to create a common user for both Prime Collaboration Assurance and Prime Collaboration Provisioning, you must perform the following tasks as prerequisites:

- Add Devices- To learn how to create devices, see "Adding Devices to Provisioning" in the *Cisco Prime Collaboration 9.5 Provisioning Guide*.
- Create Domains- To learn how to create domains, see "Creating a Domain" in the *Cisco Prime Collaboration 9.5 Provisioning Guide*.

To add a user:

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

Step 2 On the User Management page, click **Add**.

Step 3 In the Add User window, enter the required user details. Note that because the LDAP server performs authentication, it should have the same user ID as Prime Collaboration. For more information, see Configuring an LDAP Server, page 5-10.

If you select the LDAP User option, the Password and Confirm Password fields are not displayed.

Step 4 (Optional) If you have deployed the Managed Service Provider (MSP) version of Prime Collaboration, select a customer from the Customer drop-down list.

Step 5 Select the appropriate Prime Collaboration Assurance roles. (If the Prime Collaboration Provisioning application is not integrated with the Prime Collaboration Assurance application, the Provisioning Domain and Provisioning Roles fields are not displayed when you perform the Add operation.)

Step 6 If you wish to have only a Provisioning user, or a common user for Prime Collaboration Assurance and Prime Collaboration Provisioning, perform the following steps:

a. Select the appropriate roles in the Provisioning Roles check box.

b. Click **Add Row** under **Domain Specific** to create domain specific Provisioning Roles. You will see role settings option for General, Ordering and Activity roles. For information on authorization roles, see Table 5-1Authorization Roles, page 5-1.

c. Enter required details and click **Done**

Step 7 Click **Save**.

The users thus created via Add User feature are associated with the web client only and cannot log in to the Prime Collaboration Assurance or Prime Collaboration Provisioning server through the CLI.

Note The Prime Collaboration Assurance and Prime Collaboration Provisioning applications do not share inventory database. You must manage the devices separately to perform the assurance and provisioning-related tasks. See *Cisco Prime Collaboration Device Management Guide* to perform device management tasks using the Prime Collaboration Assurance application. See *Cisco Prime Collaboration 9.5 Provisioning Guide* to perform device management and provisioning tasks using the Prime Collaboration Provisioning application.

When the contact information, role, or account status of a user changes, the administrator must edit the corresponding details in the system.

To edit user details, select a user at **Administration > User Management** and make the necessary changes.

As part of your regular system administration tasks, you sometimes must delete users from the Prime Collaboration database. However, you cannot delete the Prime Collaboration web client default administrator globaladmin.

To delete a user, select the user from **Administration > User Management** and click **Delete**. Any jobs that are scheduled in the deleted user name continue to run until canceled.

Configuring an LDAP Server

You can configure Prime Collaboration to connect to a Lightweight Directory Access Protocol (LDAP) server, to access user information stored in the LDAP server. In converged mode, the LDAP server specified in Prime Collaboration Assurance is used for authentication only; authorization and role-based access control (RBAC) functions are performed by Prime Collaboration.

You must create an LDAP user from the User Management page to enable the user to log in using LDAP credentials. See Adding, Editing, and Deleting a User, page 5-8 for more information.

Prime Collaboration supports one primary LDAP server and one backup LDAP server.

To configure LDAP server:

Step 1 Choose **Administration > System Setup > Assurance Setup > LDAP Settings**.

Step 2 In the LDAP Settings page, enter values for all fields (see Table 5-4 for the field descriptions)

Table 5-4 LDAP server Configuration

Field	Description
Server IP address	Enter the LDAP server name or IP address. Optionally enter the Backup LDAP server IP address.
Server Port	Enter the Port number on which the LDAP requests for the server is received. Non-secure port: 389 Secure SSL port: 636 **Note** If Prime Collaboration must use SSL encryption, check the Use SSL check box. Optionally enter the Backup LDAP server Port number. **Note** If the LDAP server is configured to use a non-standard port, that port should be entered here as well.

Table 5-4 LDAP server Configuration (continued)

Field	Description
Admin Distinguished Name	Enter the username of the user who has access rights to the corresponding LDAP directory. For example, a user, John Doe, with userID = jdoe must enter John Doe. **Note** If admin is a user in windows domain cisco, just enter admin (username with domain prefix such as cisco\admin will not work).
Admin Password	Enter the password for the LDAP server authentication and reconfirm the password.
LDAP User Search Base	Enter the user search base. LDAP server searches for users under this base. You must enter the CN or OU details when you enter the search base. Just `dc=cisco,dc=com` will not work; you must also specify the CN or OU part, for example, `cn=users,dc=eta,dc=com`. If you have configured two different user groups, for example, • `OU=Organization, OU=Accounts, DC=aaa, DC=com` • `OU=Service, OU=Accounts, DC=aaa, DC=com` The search base to be entered is `OU=Accounts, DC=aaa, DC=com`. If a user in OU=Organization user group is configured as Admin DN, then all the users in Organization user group can login to Prime Collaboration, but the users in Services user group will not be able to login. Similarly, if a user in OU=Services user group is configured as Admin DN, then all the users in Services user group can login to Prime Collaboration, but not the users in Organization user group. If you configure a user in top level as Admin DN, then all the users under that level can log into Prime Collaboration. For example, if a user in OU=Accounts user group is configured as Admin DN, then all the users in Organization and Services user groups can login to Prime Collaboration. **Note** LDAP authentication fails if you enter special characters in the search base.

Step 3 Click **Test Connection** to check the connectivity to the LDAP server.

Step 4 Upon successful connection, click **Apply Settings** and restart Prime Collaboration Assurance server to login using LDAP.

To restart Prime Collaboration Assurance Server, login as admin user and execute the following commands:

```
application stop cpcm
application start cpcm
```

The **application stop cpcm** command takes 10 minutes to complete execution and **application start cpcm** command takes 10 to15 minutes to complete execution.

Resetting and Changing Passwords

As a super administrator, system administrator or network operator, you can reset the password for other Prime Collaboration users as well as change your own password.

To reset the password for other users, select a user from **Administration > User Management** and make the necessary changes.

To change your own password, click **Change Password** and make necessary changes.

You can reset the Prime Collaboration Assurance web client globaladmin password using the following procedure.

To reset the Prime Collaboration Assurance globaladmin password:

Step 1 Log in as a root user.

Step 2 Enter the "goemsam" command:

Step 3 Execute the following:

```
#./bin/resetGlobalAdminPassword.sh
```

Step 4 Enter a new password for the globaladmin and also confirm the new password. See the *Cisco Prime Collaboration Quick Start Guide* for more information on password verification rules.

To reset the Prime Collaboration Provisioning globaladmin password:

Step 1 Log in as a root user.

Step 2 Execute the following commands:

```
#cd /opt/cupm/sep/ipt/bin:
#./ResetGlobalAdminPassword.sh 'new password' <server type>
```

Enter a new password for the globaladmin and specify the server type. The server type can be one of the following:

ALL—for a single machine install

Database—for database server

Application—for application server

Note In case of a distributed system where database and application are in different servers, you must execute this procedure in both the servers.