CHAPTER 3

Managing Users and Configuring Role-Based Access Control

This chapter describes how to manage users in Prime Central for HCS, including defining users and passwords and configuring role-based access control (RBAC).

Prime Central provides role-based access to various functions. Through RBAC, Prime Central allows a user to access some resources but not others, and to perform specific tasks based on the logged-in user's roles. This chapter contains the following sections:

Understanding Prime Central for HCS Roles

Prime Central for HCS has two categories of roles that are based on the type of their privileges. It follows the Role Based Access Control (RBAC) policy. RBAC is a method of restricting or authorizing system access for users, based on their assigned roles. A role can contain one or more system privileges, wherein each privilege defines the right to access or modify certain objects and components or the types of objects and components. Roles can also contain privileges related to running certain tasks and test within the assurance system. Prime Central for HCS supports the following two roles:

- Administrator user—An administrator can make configuration changes. The administrator can manage users and administer domain managers by cross-launching to the specific domain manager as an administrator user.
- SP operator—SP operator has privileges to perform all tasks that involve collecting and viewing data and initiating test and maintenance actions, such as initiating diagnostic test between HCS system devices. SP operator does not have the privilege to make any configuration-related changes onPrime Central for HCS platform, except to change its user password. The actions that are specific to operator is restricted to view-only. The operator cannot manage users.

To provision users for single sign-on, at the time of Prime Central for HCS installation, you must provision Cisco Prime Unified Operations Manager and DCNM-SAN with one Super Administrator user. Also, a user with Operator role must be created for use when a user cross-launches from SP Operator group.

For other domain managers (DCNM-LAN, Infrastructure Monitoring, Cisco Unified Computing System Manager) you must provision users at the time of installation. These domain managers do not support single sign-on. When you cross-launch to the domain manager, a login window appears. Supply the appropriate credentials that you provided at the time of the installation.

Understanding the User Management Portlet

Figure 3-1shows the User Management portlet, where you perform all user management tasks.

Figure 3-1 User Management Portlet

1	User management tabs: Users, Groups, Roles, Privileges	**7**	Disable icon
2	Show drop-down list and Filter icon	**8**	Reset Password icon
3	Refresh icon	**9**	Add icon
4	Export icon	**10**	Delete icon
5	Filter parameters area	**11**	Copy icon
6	Enable icon	**12**	Edit icon

Managing Users

This section explains the various procedures that are involved in managing users.

Creating New Users in Prime Central for HCS

The first time you log in to Prime Central for HCS, you have to use the default login username **centraladmin**. Once you log in, you can create new users and assign them roles and add them to groups. Each user, by default, has to be associated to a group. By default, Prime Central for HCS has two groups—Prime Central administrator and Prime Central for HCS operator. All domain managers will also have operator and administrator user and Prime Central for HCS fetches this data from SDR. Prime Central for HCS uses these credentials to facilitate single sign-on.

This section describes the various administrative operations that you can perform. Refer to the HCM-F user guide for instructions on adding domain manager details, domain manager user credentials and other domain manager information to the SDR. Prime Central for HCS uses the domain manager information (such as domain manager IP address, username, password and other information) in the SDR to perform cross launches. All the administrative tasks are listed in the **Administration** tab.

Step 1 From the Prime Central menu, choose **Administration > User and Group Management > Users**.

Step 2 In the User Management portlet, click **Add User**.

Step 3 Enter general information about the user in the Enter User Info screen.

Field	Description
Username	Enter a username for logging in. The username must: • Start with an alphabetic character. • Contain from 4 to 20 alphanumeric characters. • Not contain any spaces or special characters, except for hyphens.
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
Password	Enter a unique password, which is then stored in the Prime Central for HCS database. The password must: • Contain at least one character from at least three of the following four classes: – Alphabetic characters in uppercase (A-Z) – Alphabetic characters in lowercase (a-z) – Numerics (0-9) – Special characters (! " # $ % & ' () * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~) • Minimum of 8 characters and maximum 64 characters. • Not contain the username or the username in reverse. • Not repeat the same character three or more times. • Must not contain the word `cisco` or any other combination of the word.
Confirm Password	Enter the new password again to confirm the entry.
Email	Enter an e-mail address for the user.
Phone	(Optional) Enter a phone number for the user. Do not enter any spaces or hyphens between numbers.
Note	(Optional) Enter any additional information as a note for the user. You can click and drag the notes field if you want to add more information.

Step 4 Click **Next** and assign the domain manager access privileges in the Domain Manager Access Privilege screen.

Field	Description
Domain Manager Access Privilege	By default, Prime Fault Management check box is checked. This allows you to access the domain manager. You cannot edit this setting.

Step 5 Click **Next** and associate the new user as a member of one or more groups in the Assign Groups & Group Roles screen. Currently, Prime Central for HCS solution supports two groups: PrimeAdminGroup (Administrators) and SPOperators (Operators)

Field	Description
Groups	Check the appropriate check box(es) to grant the user access to the desired group: • Name—Shows the group name. • Description—Shows the group description. • Role—Shows the group role. All users that belong to the group share the same role.

Step 6 Click **Next** and assign individual roles in the Assign Additional Individual User Roles screen.

Two tabs—Prime Central and Prime Fault Management—are available.

- Under the Prime Central tab, by default, the role User will be selected. Based on your selection in the previous step, choose a role appropriately:

If your selection in previous step was...	In this step, select...
PrimeAdminGroup	Administrator
SPOperators	DMLaunchOperatorRole

- If you chose Administrator in the previous step, check Administrator in this step as well or if you chose the If operator in the previous step, select SP Operator as the value in this step.
- Under the Prime Fault Management tab, check the appropriate check box to choose the role again. The roles that you can choose are: Administrator and Operator.

An Administrator user in Prime Central for HCS maps to admin user in Cisco Prime Unified Operations Manager and sanadmin user in DCNM-SAN. The admin and sanadmin users have to be created at the time of installation of domain managers. When you log in as an Administrator user in Prime Central for HCS and cross-launch to Cisco Prime Unified Operations Manager and DCNM-SAN, the credentials of admin and sanadmin users will be used, respectively.

Note DCNM is an optional component in Prime Central for HCS 9.2.1. If you are not using DCNM in your deployment, skip tasks and sections related to DCNM.

Step 7 Click **Next**; the summary of the new user is displayed.

Step 8 Click **Finish**.

Creation of a new user takes few minutes. Once the new user is created, the details are displayed in the Users tab.

Using the Quick View

In the User Management portlet, hover your mouse cursor over the icon to view user information in a *quick view*.

Editing a User

Step 1 From the Prime Central menu, choose **Administration > User and Group Management > Users**.

Step 2 In the User Management portlet, select the user that you want to edit and click **Edit**.

Step 3 Modify the following fields in the Enter User Info screen, as required.

Field	Description
Username	*Display only.* Username to be used for logging in.
First Name	First name of the user.
Last Name	Last name of the user.
Email	E-mail address of the user.
Phone	Phone number of the user. Do not enter any spaces or hyphens between numbers.
Note	Enter any additional information as a note for the user. You can click and drag the notes field if you want to add more information.

Step 4 Click **Next** and update the user's domain manager access privileges, as required. If a domain manager is not yet installed, it does not appear as an option.

Field	Description
Domain Manager Access Privilege	By default, Prime Fault Management check box is checked. This grants the user access to the domain manager. You cannot edit this setting.

Step 5 Click **Next** and update the user's assigned groups and group roles, as required.

Field	Description
Groups	Check the appropriate check box(es) to grant the user access to the desired group(s): • Name—Shows the group name. • Description—Shows the group description. • Role—Shows the group role. All users that belong to the group share the same role.

Step 6 Click **Next** and update the user's individual roles, as required. To assign individual roles, follow the procedure outlined in the section Creating New Users in Prime Central for HCS, page 3-2.

The domain manager access privilege (assigned in Step 4) and the user role are related. For example, In Step 4, you have assigned Prime Fault Management domain manager access privilege, then you have to assign the user with Fault Management role in this screen.

Click the tabs at the top to update roles per domain manager. If a domain manager is not yet installed, it does not appear as a tab.

Field	Description
Roles	Check the appropriate check box (or radio button) to grant the user access to the desired role(s): • Name—Shows the individual user role name. • Description—Shows the user role description. • Privileges—Shows the privilege assigned to each individual user role. **Note** In Prime Central for HCS, you can assign multiple roles to a user.

Step 7 Click **Next** and confirm your updates in the Summary screen.

Step 8 Click **Finish**. The updated user is displayed in the Users tab.

Copying a User

You can easily create a new user by copying an existing user's assigned privileges, groups, and roles. However, you can also edit the user's profile, as required, at every step.

Step 1 From the Prime Central menu, choose **Administration > User and Group Management > Users**.

Step 2 In the User Management portlet, select the user that you want to copy and click **Copy**.

Step 3 In the Enter User Info screen, the information is unique to each user and is therefore not copied from the existing user. Fill in the new user's username, first and last name, password, e-mail address, and phone number. Then, click **Next**.

Note Copy option is disabled when you log in as a Central Admin. You are not allowed to copy the Central Admin user privileges.

Step 4 The information in the following screens is copied from the existing user. In each screen, make any necessary changes for the new user; then, click **Next**:

- Domain Manager Access Privilege
- Assign Groups & Group Roles
- Assign Additional Individual User Roles

Step 5 The Summary screen shows your selections. Click **Finish**. The new user is displayed in the Users tab.

Deleting a User

Step 1 From the Prime Central menu, choose **Administration > User and Group Management > Users**.

Step 2 In the User Management portlet, select the user that you want to delete and click **Delete**.

A confirmation message appears.

Step 3 At the confirmation prompt, click **Yes**.

Changing Another User's Password

Users with administrator-level privileges can change another user's password.

Step 1 From the Prime Central menu, choose **Administration > User and Group Management > Users**.

Step 2 In the User Management portlet, select the user whose password you want to change and click **Reset Password**.

Step 3 In the Change Password dialog box, follow the password guidelines mentioned below and enter a password:

- Contains at least one character from at least three of the following four classes:
  - Alphabetic characters in uppercase (A-Z)
  - Alphabetic characters in lowercase (a-z)
  - Numerics (0-9)
  - Special characters (! " # $ % & ' () * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~)
- Minimum of 8 characters and maximum 12 characters.
- Not contain the username or the username in reverse.
- Not repeat the same character three or more times.
- Not begin with a special character.
- Must not contain the word `cisco` or any other combination of the word.

Step 4 Enter the new password again to confirm the entry.

Step 5 Click **Save**.

Changing Your User Password

Users of any privilege level can use the My Account portlet to change their Prime Central password. The password change applies to the Prime Central user who is currently logged in.

Step 1 On the portal home page, click your login name link.

The My Account portlet opens.

Step 2 In the Old Password field, enter your current password.

Step 3 In the New Password field, enter a new password. For password related guidelines see Step 3 of Changing Another User’s Password.

Step 4 Enter the new password again to confirm.

Step 5 (Optional) In the Email field, enter an e-mail address that will be displayed in the User Management portlet. This field is dimmed for the *centraladmin* user.

Step 6 (Optional) In the Phone field, enter a phone number that will be displayed in the User Management portlet. This field is dimmed for the *centraladmin* user.

Step 7 Click **Save**.

Enabling a User Account

This section explains the procedure to enable a user account. This can be performed only by an Administrator user.

Step 1 From the Prime Central menu, choose **Administration > User and Group Management > Users**.

Step 2 In the User Management portlet, select the user whose account you want to enable and click **Enable**.

The User Management portlet > Active column displays *Yes*, meaning that user is enabled and can log into Prime Central.

Disabling a User Account

This section explains the procedure to disable a user account. This can be performed only by an Administrator user.

Step 1 From the Prime Central menu, choose **Administration > User and Group Management > Users**.

Step 2 In the User Management portlet, select the user whose account you want to disable and click **Disable**.

The User Management portlet > Active column displays *No*, meaning that user is disabled and cannot log into Prime Central.

Changing the Time Zone Preferences

By default, the creation time in the User Management portlet is UTC time. To update the time zone to a local time zone:

Step 1 Click **Add Application > Cisco Prime > User Preferences**.

Step 2 Select time zone from the Time Zone drop-down, and click **Save** to save the changes.