



Managing Users and Configuring Role-Based Access Control

This section describes how to manage users in Prime Central, 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.

Authorization of tasks is controlled by user roles within Prime Central and user roles and scopes within the applications.

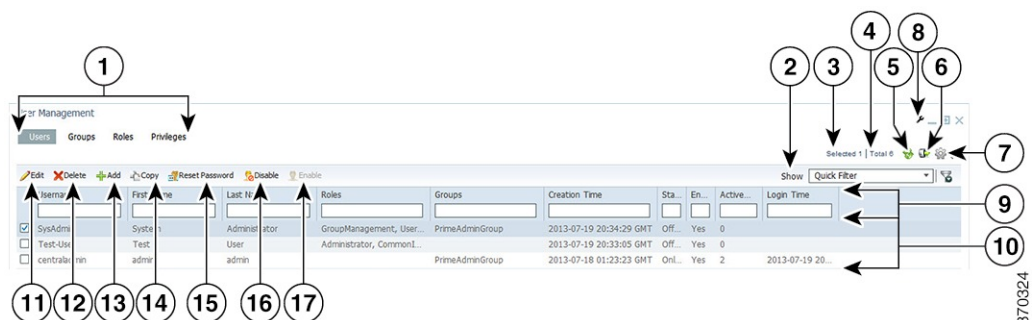
This section contains the following topics:

- [User Management Portlet, page 1](#)

User Management Portlet

The following figure shows the User Management portlet, where users with administrator-level privileges can perform all user management tasks.

Figure 1: User Management Portlet



1	User management tabs: Users, Groups, Roles, Privileges	10	Properties pane
---	--------------------------------------------------------	----	-----------------

370324

2	Show drop-down list and Filter icon	11	Edit icon
3	Number of selected table rows	12	Delete icon
4	Total table rows	13	Add icon
5	Refresh icon	14	Copy icon
6	Export icon	15	Reset Password icon
7	Settings icon	16	Disable icon
8	Options icon	17	Enable icon
9	Filter parameters area	—	—

Managing Users

You can add, edit, copy, and delete users; reset user passwords; disable and enable user accounts; and configure user security settings.

Each user can be assigned any number of roles, and each role can aggregate any number of privileges.

Prime Central includes a default user named *centraladmin* whose account cannot be deleted or disabled. The *centraladmin* user has local authentication, user management, and administrator privileges, but initially does not have any privileges on the various applications.

Adding a User

Procedure

-
- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click **Add**.
- Step 3** In the Add User window:
- a) Enter general information about the new user, including username, first and last name, password, and email address. The variables that you define must adhere to the constraints described in [Name, Password, Phone, and Note Constraints](#).
The username is display only and cannot be changed.
 - b) For the **Local Authentication Fallback** check box:
 - If Prime Central is configured to use an external authentication provider such as TACACS+, RADIUS, or LDAP, check this check box to enable user authentication to fall back to the local Prime Central database when the external authentication server is unreachable.
 - If Prime Central is not configured to use external authentication, leave this check box unchecked. (It is unchecked by default.)

- c) (Optional) For the **Concurrent User Sessions** field, do one of the following:
- To have global user settings apply to the new user, click the Use Global Settings radio button. (For details about global settings, see [Configuring User Security Settings](#).)
 - To allow the user to open an unlimited number of concurrent Prime Central sessions, click the **Unlimited** radio button.
 - To limit the user to a specific number of concurrent sessions, click the **Number of Sessions** radio button and enter the desired number in the text box.
- d) (Optional) In the **Note** field, enter any notes for the user account.

Step 4 In the Application Access Privilege area, grant user access to the appropriate applications and assign individual roles:

- a) Select an application from the list of installed applications.
The list of roles specific to that application is displayed.
- b) Select the appropriate role for the user.
After you select a role, the Grant Access to *<application>* check box is checked automatically.

Note the following:

- When you add users, the status is displayed as Enable at the end of the operation. If you want to deactivate a user, use the **Update** option to deactivate a specific user.
- Prime Central includes a set of default roles for security and access control that allow different system functions. Click [Table 3: Default Prime Central Roles](#) to view a table which lists the default roles, the privileges that each role inherits, and the portlets that each role can access.
- The application access privilege and the user role are related. For example, if you assigned the user the Prime Central Fault Management access privilege, be sure to assign the user the Prime Central Fault Management role.
- You can assign the new user additional roles as desired.
- For Prime Central and Prime Provisioning, you can assign multiple roles to a user. For Prime Central Fault Management, Prime Network, Prime Optical, and Prime Performance Manager, you can assign only one role per user.
- If your network includes multiple instances of Prime Network or Prime Optical, the new user will be created on both application instances. For example, if you grant the new user access to Prime Optical and assign the user the SysAdmin role, that SysAdmin user will be created on both Prime Optical instances. However, if a Prime Optical instance is down when you add the new user, that SysAdmin user is not created on the Prime Optical instance until 5 minutes after the instance comes back up.
- When you grant a Prime Central user access to Agora-NG, you must assign the Agora-NG Administrator role to that user.

Step 5 Add the new user as a member of one or more groups:

- a) Select **Prime Central** from the installed applications list.
- b) Click the **Groups** tab.
- c) Check the check boxes for the appropriate groups.

All users that belong to the group share the same role.

Step 6 Click **Add**.

The new user is displayed in the User Management portlet.

- Step 7** Assign device scopes (in Prime Network and Agora-NG) or NEs (in Prime Optical) to the new user:
- From the Prime Central menu, choose **Administration > Scope Management > Prime Network, Prime Optical, or Agora-NG**.
 - Launch the appropriate application and assign device scopes or NEs to the new user. See the application documentation for details:
 - Prime Network—See "Creating New Device Scopes to Control Device Access" in the [Cisco Prime Network 4.1 Administrator Guide](#), Chapter 6, "Controlling Device Access and Authorization Using Device Scopes."
 - Prime Optical—See "Modifying a Prime Optical User's Properties" in the [Cisco Prime Optical 10.0 User Guide](#), Chapter 8, "Managing Security."
 - Agora-NG—See the following [datasheet](#).

Name, Password, Phone, and Note Constraints

When adding, editing, or copying a user, the variables that you define must adhere to the constraints listed in the following table.

Table 1: Name, Password, Phone, and Note Constraints

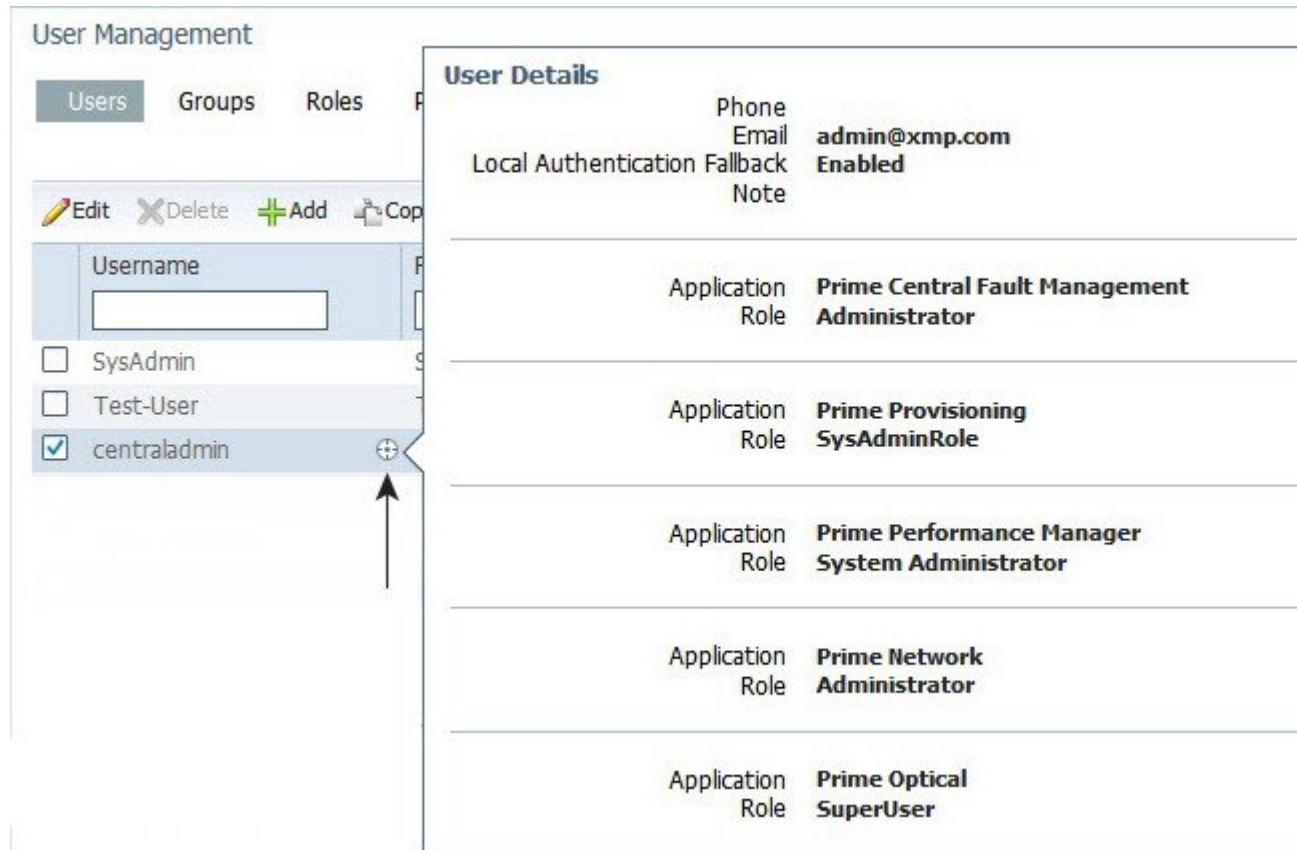
Variable	Constraints
Username	<p>The username must:</p> <ul style="list-style-type: none"> Start with a letter. Contain from 4 to 20 case-sensitive letters (A-Z, a-z), numbers (0-9), or hyphens (-), . Not contain any other special characters or spaces. Not be the reserved keywords <i>prime</i>, <i>web</i>, <i>guest</i>, <i>user</i>, <i>group</i>, <i>public</i>, or <i>private</i>, in any combination of uppercase or lowercase letters. <p>Note</p> <ul style="list-style-type: none"> Usernames are case-sensitive. Prime Central treats <i>UserA</i> and <i>userA</i> as separate users. If the username that you enter already exists in an installed application, Prime Central overwrites the existing application user with this new user.
Group name, role name, or privilege name	<p>The name must:</p> <ul style="list-style-type: none"> Start with a letter. Contain from 1 to 50 letters (A-Z, a-z), numbers (0-9), hyphens (-), or underscores (_). Not contain spaces or other special characters.

Variable	Constraints
Password	<p>The password must:</p> <ul style="list-style-type: none">• Contain from 8 to 32 characters.• Not repeat the same character three or more times.• Contain characters from at least three of the following four classes:<ul style="list-style-type: none">◦ Uppercase letters (A-Z).◦ Lowercase letters (a-z).◦ Numbers (0-9).◦ Special characters.• Not contain the username or the username in reverse.• Not contain <i>cisco</i>, <i>ocsic</i>, or any variation.
Phone	The phone number can contain up to 64 characters. All characters are allowed.
Note	The note can contain up to 1000 characters. All characters are allowed.

User Information in the Quick View

In the User Management portlet, the quick view displays additional user information when the cursor rests over the icon shown in the following figure.

Figure 2: Quick View of Additional User Details



Editing a User

Procedure

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, select the user that you want to edit and click **Edit**.
- Step 3** In the Edit User window:
 - a) Edit the user's first or last name, email address, or phone number, as required. The variables that you define must adhere to the constraints described in [Name, Password, Phone, and Note Constraints](#). The username is display only and cannot be changed.
 - b) For the **Local Authentication Fallback** check box:

- If Prime Central is configured to use an external authentication provider such as TACACS+, RADIUS, or LDAP, check this check box to enable user authentication to fall back to the local Prime Central database when the external authentication server is unreachable.
- If Prime Central is not configured to use external authentication, leave this check box unchecked. (It is unchecked by default.)

c) (Optional) For the Concurrent User Sessions field, do one of the following:

- To have global user settings apply to the new user, click the **Use Global Settings** radio button. (For details about global settings, see [Configuring User Security Settings](#).)
- To allow the user to open an unlimited number of concurrent Prime Central sessions, click the **Unlimited** radio button.
- To limit the user to a specific number of concurrent sessions, click the **Number of Sessions** radio button and enter the desired number in the text box.

d) (Optional) In the Note field, enter any notes for the user account.

Step 4 In the Application Access Privilege area, click the **Roles** tab and update the user's application access and roles, as required. If an application is not installed, it is not listed here.

Note the following:

- Application access and roles (except Prime Central roles) are all that you can edit for the *centraladmin* user.
- The application access privilege and the user role are related. For example, if you assigned the user the Prime Central Fault Management access privilege, be sure to assign the user the Prime Central Fault Management role.
- For Prime Central, all users are assigned the User role automatically. You can assign the user additional roles as desired.
- For Prime Central and Prime Provisioning, you can assign multiple roles to a user. For Prime Central Fault Management, Prime Network, Prime Optical, and Prime Performance Manager, you can assign only one role per user.
- If your network includes multiple instances of Prime Network or Prime Optical, the user will be created on both application instances. For example, if you grant the user access to Prime Optical and assign the user the SysAdmin role, that SysAdmin user will be created on both Prime Optical instances. However, if a Prime Optical instance is down when you add the user, that SysAdmin user is not created on the Prime Optical instance until 5 minutes after the instance comes back up.

Step 5 In the Application Access Privilege area, click the **Groups** tab and update the user's assigned groups and group roles, as required.

Step 6 Click **Update**. The updated user is displayed in the User Management portlet..

If you changed a user's assigned roles or access privileges, that user must log out of Prime Central and log back in to see the changes. The changes do not take effect until the user logs in next.

You can also use **Update** to deactivate an user.

Step 7 (Optional) Reassign device scopes to the user you edited:

- a) From the Prime Central menu, choose **Administration > Scope Management > Prime Network** or **Prime Optical**.

- b) Launch the appropriate application and reassign device scopes or NEs to the user. See the application documentation for details:
- Prime Network—See "Creating New Device Scopes to Control Device Access" in the [Cisco Prime Network 4.1 Administrator Guide](#), Chapter 6, "Controlling Device Access and Authorization Using Device Scopes."
 - Prime Optical—See "Modifying a Prime Optical User's Properties" in the [Cisco Prime Optical 10.0 User Guide](#), Chapter 8, "Managing Security."
-

Copying a User

You can easily create a new user by copying an existing user's assigned privileges, groups, and roles.

Procedure

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, select the user that you want to copy and click **Copy**.
- Step 3** In the Add User window, make the following entries (this information is unique to each user and is therefore not copied from the existing user):
- a) Specify a username, first and last name, password, email address, and phone number. See the constraints described in [Name, Password, Phone, and Note Constraints](#).
 - b) For the **Local Authentication Fallback** check box:
 - If Prime Central is configured to use an external authentication provider such as TACACS+, RADIUS, or LDAP, check this check box to enable user authentication to fall back to the local Prime Central database when the external authentication server is unreachable.
 - If Prime Central is not configured to use external authentication, leave this check box unchecked. (It is unchecked by default.)
 - c) (Optional) For the **Concurrent User Sessions** field, do one of the following:
 - To have global user settings apply to the new user, click the **Use Global Settings** radio button. (For details about global settings, see [Configuring User Security Settings](#).)
 - To allow the user to open an unlimited number of concurrent Prime Central sessions, click the **Unlimited** radio button.
 - To limit the user to a specific number of concurrent sessions, click the **Number of Sessions** radio button and enter the desired number in the text box.
 - d) (Optional) In the Note field, enter any notes for the user account.
- Step 4** For each of the following items, make any changes needed for the new user (the current information is copied from the existing user):
- Application access

- User roles
- Groups and group roles

Step 5 Click **Add**.

The new user is displayed in the User Management portlet.

Step 6 Assign device scopes (in Prime Network and Agora-NG) or NEs (in Prime Optical) to the new user:

- a) From the Prime Central menu, choose **Administration > Scope Management > Prime Network, Prime Optical, or Agora-NG**.
 - b) Launch the appropriate application and assign device scopes or NEs to the new user. See the application documentation for details:
 - Prime Network—See "Creating New Device Scopes to Control Device Access" in the [Cisco Prime Network 4.1 Administrator Guide](#), Chapter 6, "Controlling Device Access and Authorization Using Device Scopes."
 - Prime Optical—See "Modifying a Prime Optical User's Properties" in the [Cisco Prime Optical 10.0 User Guide](#), Chapter 8, "Managing Security."
 - Agora-NG—See the following [datasheet](#).
-

Deleting a User

Procedure

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

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

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

If the user exists on an application that is down when you delete the user from Prime Central, that user will persist on that particular application as a local user.

Resetting Another User's Password

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

Procedure

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
 - Step 2** In the User Management portlet, select the user whose password you want to reset and click **Reset Password**.
 - Step 3** In the Reset Password dialog box, enter a new password that adheres to the constraints described in [Name, Password, Phone, and Note Constraints](#).
 - Step 4** Enter the new password again to confirm the entry.
 - Step 5** Click **Save**.
-

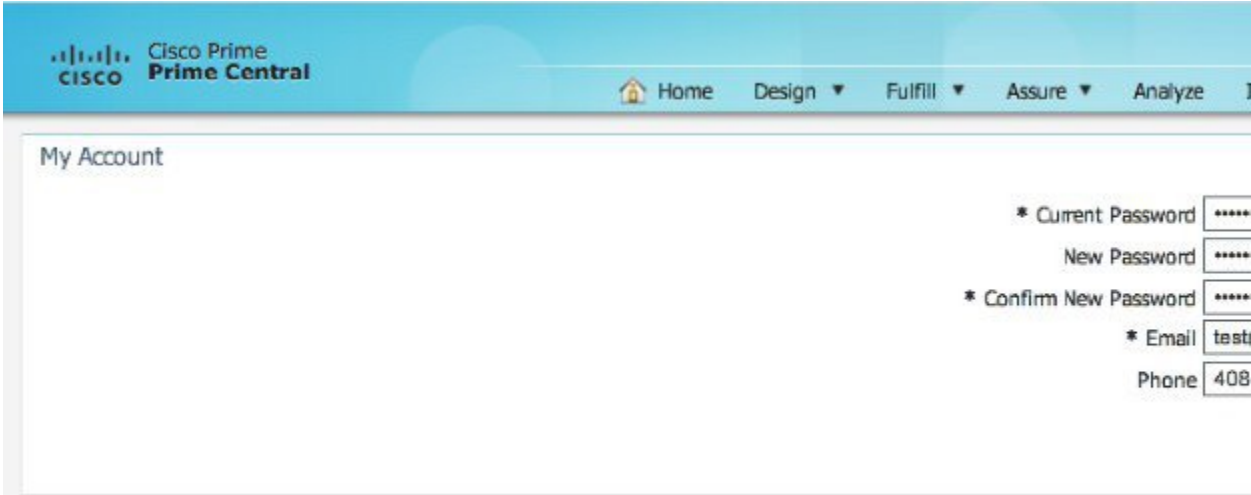
Resetting Your User Password

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

Procedure

- Step 1** On the portal home page, place your cursor over your login name (to the left of the Log Out link) and click **My Account**. In the example shown in the following figure, the name is *Test User*.
- Step 2** In the My Account portlet, enter your current password in the Current Password field.
- Step 3** In the New Password field, enter a new password that adheres to the constraints described in [Name, Password, Phone, and Note Constraints](#).
- Step 4** Enter the new password again to confirm the entry.
- Step 5** (Optional) In the Email field, edit the email 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, edit the phone number that will be displayed in the User Management portlet. This field is dimmed for the *centraladmin* user.
- Step 7** Click Save.

Figure 3: My Account Portlet



The screenshot shows the Cisco Prime Central interface. At the top, there is a navigation bar with the Cisco Prime Central logo and a menu with items: Home, Design, Fulfill, Assure, and Analyze. Below the navigation bar is the 'My Account' portlet. The portlet contains a form with the following fields:

- * Current Password
- New Password
- * Confirm New Password
- * Email (value: test)
- Phone (value: 408)

Resetting a Lost Password

From the UNIX command line, the Linux root user on the Prime Central portal can reset any Prime Central portal user's password, including an administrator password.

Complete this procedure only after trying [Resetting Another User's Password](#) and [Resetting Your User Password](#).

Procedure

- Step 1** As the primeusr user, log in to the Prime Central portal with the primeusr password that you specified during installation.
- Step 2** Enter the following command:
su root
- Step 3** When prompted, enter the root user password.
- Step 4** Change directories to the \$XMP_HOME/bin folder.
- Step 5** Enter the following command:
resetUserPassword.ksh
- Step 6** When prompted, enter the Prime Central username and the new password. In the following example, the Prime Central username is *User_XYZ*
- ```
Please enter username:
User_XYZ
Please enter new password:
Please enter confirm password:
When the script finishes, output similar to the following is displayed:

Loading USER - User_XYZ
Validating new password..
Resetting password ..
Resetting password COMPLETED.
EXECUTION STATUS : Success
```
- 

## Enabling or Disabling a User Account

Users with administrator-level privileges can enable or disable another user's account. However, you cannot disable the *centraladmin* user account.

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, select the desired user and click **Enable** or **Disable**. The User Management portlet > Enabled column displays the following value:
- Yes—The user is enabled and can log in to Prime Central.
  - No—The user is disabled and cannot log in to Prime Central.
- 

## Configuring User Security Settings

Users with the appropriate privileges can configure security settings that apply to all other users.

The following security settings do not apply to the *centraladmin* user, who has administrator-level privileges:



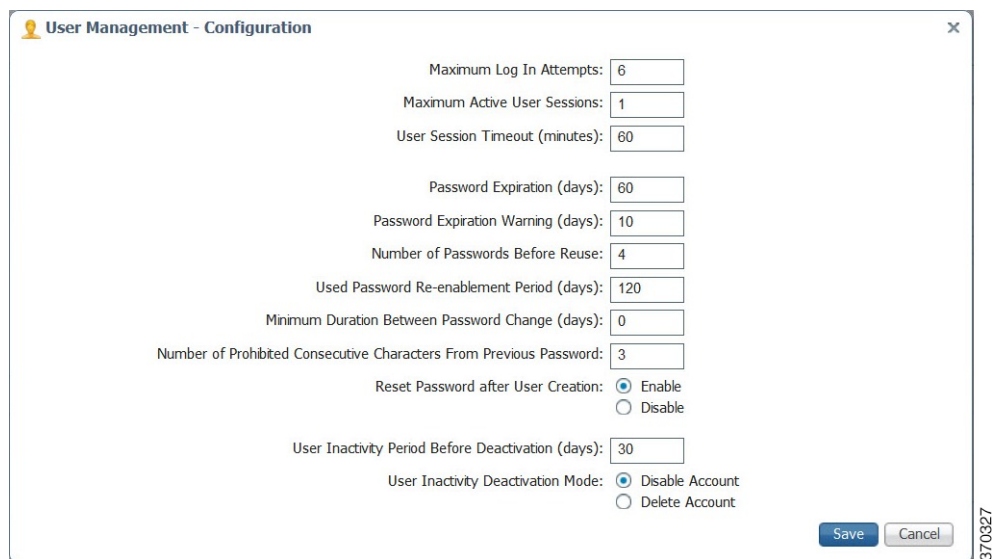
**Note**

- Maximum Log In Attempts
- Maximum Active User Sessions
- User Inactivity Period Before Deactivation (days)
- User Inactivity Deactivation Mode

**Procedure**

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the top-right corner of the User Management portlet, click the **Options** icon.
- Step 3** Click the **Configuration** link. The User Management - Configuration dialog box (see the following figure) opens.
- Step 4** Configure the security settings that will apply to all users. See the [Table 2: User Security Setting Descriptions](#) table for more information.
- Step 5** Click **Save**.

**Figure 4: User Management - Configuration Dialog Box**



**User Security Setting Descriptions**

The following table describes the security settings you can configure for the users in your network.

**Table 2: User Security Setting Descriptions**

| Setting                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum Log In Attempts                                            | The maximum number of failed login attempts allowed before the user account is denied access to Prime Central. The default is 6 retries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Maximum Active User Sessions                                       | The number of concurrent sessions allowed. The default is 1 session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| User Session Timeout (minutes)                                     | The number of minutes a user's session is inactive before Prime Central automatically locks the user out. By default, the session times out after 60 minutes of inactivity. You are prompted to extend the session 10 minutes before it times out. If you do not extend the session before the timeout, you are logged out automatically from Prime Central and from any applications.                                                                                                                                                                                                                                                                                      |
| Password Expiration (days)                                         | The number of days before the password expires. The default is 60 days.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Password Expiration Warning (days)                                 | The early warning period for password expiration. The default is 10 days. The value in this field must be less than the value in the Password Expiration field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Number of Passwords Before Reuse                                   | <p>The number of different passwords a user must use before being allowed to reuse the first password. The default is 4 passwords.</p> <p>This field takes priority over the Used Password Re-enablement Period field. For example, assume that:</p> <ul style="list-style-type: none"> <li>• Number of Passwords Before Reuse: 2</li> <li>• Used Password Re-enablement Period: 5</li> </ul> <p>If the user password is <i>test</i>, you can change it to <i>sample</i> the next day, and then to <i>basic</i> on the second day. You can then change it back to <i>test</i> before 5 days elapses, because the Number of Passwords Before Reuse field takes priority.</p> |
| Used Password Re-enablement Period (days)                          | The number of days before an old password can be reused. The default is 120 days.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Minimum Duration Between Password Change (days)                    | The number of days a user must wait between password changes. The default is 0 days.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Number of Prohibited Consecutive Characters From Previous Password | The number of consecutive characters by which the new password must differ from the previous one. The default is 3 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Reset Password after User Creation                                 | Specify whether newly added users will be prompted to reset their password before their first login.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| User Inactivity Period Before Deactivation (days)                  | The number of days a user's session is inactive before Prime Central automatically deactivates the user. The default is 30 days.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Setting                           | Description                                                                                            |
|-----------------------------------|--------------------------------------------------------------------------------------------------------|
| User Inactivity Deactivation Mode | Specify whether to disable or delete an inactive user account. The default is <i>Disable Account</i> . |

## Managing Groups

All users that belong to a particular group share the same role and have access to a specific set of functions. User groups can be tied to one or more roles. The idea is to easily create groups of users who all share the same access privileges. A user can be assigned to more than one group, but this is not typical, as a single group should define an overall operational role within the suite.

Prime Central includes a default group named *PrimeAdminGroup* that cannot be edited or deleted.

### Adding a Group

#### Procedure

- 
- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
  - Step 2** In the User Management portlet, click the **Groups** tab.
  - Step 3** Click **Add**.
  - Step 4** In the Add Group dialog box:
    - a) Enter a group name that conforms to the constraints listed in the [Table 1: Name, Password, Phone, and Note Constraints](#) table.
    - b) Enter a description that contains from 1 to 50 alphanumeric or special characters.
    - c) Check the appropriate role check boxes to assign the new group at least one role.
    - d) Click **Add**.  
The new group is displayed in the Groups tab.
- 

### Editing a Group

#### Procedure

- 
- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
  - Step 2** In the User Management portlet, click the **Groups** tab.
  - Step 3** Select the group that you want to edit and click **Edit**.
  - Step 4** Edit the group description or assigned roles, as required. The group description can contain from 1 to 50 alphanumeric or special characters.  
The group name is display only and cannot be changed.

**Step 5** Click **Update**.

---

## Deleting a Group

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click the **Groups** tab.
- Step 3** Select the group that you want to delete and click **Delete**.
- Step 4** At the confirmation prompt, click **Yes**.
- 

## Managing Roles

Users have access to functions based on the role to which they are assigned. Roles define the functions or tasks a user can perform. A user can be assigned more than one role.

Prime Central includes a set of default roles for security and access control that allow different system functions. The following table lists the default roles, the privileges that each role inherits, and the portlets that each role can access. (The default privileges are explained in [Managing Privileges](#).) The default roles cannot be edited or deleted.

User roles inherit privileges as a union of role types. For example, the Fault Management role (which has Common Inventory access) paired with the User role (which has Common Inventory access) results in Common Inventory access.

**Table 3: Default Prime Central Roles**

| Default Role Name | Privileges                | Ability to Access These Portlets: |                  |                 |                  |                  |                  |               |              |           |
|-------------------|---------------------------|-----------------------------------|------------------|-----------------|------------------|------------------|------------------|---------------|--------------|-----------|
|                   |                           | My Account                        | User Preferences | User Management | Suite Monitoring | Group Management | Common Inventory | Alarm Browser | Alarm Report | Audit Log |
| Administrator     | Admin Privilege           | Yes                               | Yes              | Yes             | Yes              | Yes              | Yes              | Yes           | Yes          | Yes       |
|                   | All Access Privilege      |                                   |                  |                 |                  |                  |                  |               |              |           |
|                   | InTracer Launch Privilege |                                   |                  |                 |                  |                  |                  |               |              |           |



| Default Role Name      | Privileges                         | Ability to Access These Portlets: |                  |                 |                  |                  |                  |               |              |           |
|------------------------|------------------------------------|-----------------------------------|------------------|-----------------|------------------|------------------|------------------|---------------|--------------|-----------|
|                        |                                    | My Account                        | User Preferences | User Management | Suite Monitoring | Group Management | Common Inventory | Alarm Browser | Alarm Report | Audit Log |
| Common Inventory Admin | Common Inventory Admin Privilege   | Yes                               | Yes              | No              | Yes              | No               | Yes              | No            | No           | No        |
|                        | Cross Launch Privilege             |                                   |                  |                 |                  |                  |                  |               |              |           |
|                        | Subsystem Inventory User Privilege |                                   |                  |                 |                  |                  |                  |               |              |           |
|                        | User Privilege                     |                                   |                  |                 |                  |                  |                  |               |              |           |
| Common Inventory User  | Common Inventory User Privilege    | Yes                               | Yes              | No              | Yes              | No               | Yes              | No            | No           | No        |
|                        | Cross Launch Privilege             |                                   |                  |                 |                  |                  |                  |               |              |           |
|                        | Subsystem Inventory User Privilege |                                   |                  |                 |                  |                  |                  |               |              |           |
|                        | User Privilege                     |                                   |                  |                 |                  |                  |                  |               |              |           |

| Default Role Name | Privileges                         | Ability to Access These Portlets: |                  |           |                  |            |                  |               |              |           |
|-------------------|------------------------------------|-----------------------------------|------------------|-----------|------------------|------------|------------------|---------------|--------------|-----------|
|                   |                                    | My Account                        | User Preferences | User Mgmt | Suite Monitoring | Group Mgmt | Common Inventory | Alarm Browser | Alarm Report | Audit Log |
| Fault Mgmt        | Cross Launch Privilege             | Yes                               | Yes              | No        | Yes              | No         | No               | Yes           | Yes          | No        |
|                   | Fault Mgmt Privilege               |                                   |                  |           |                  |            |                  |               |              |           |
|                   | Subsystem Inventory User Privilege |                                   |                  |           |                  |            |                  |               |              |           |
|                   | User Privilege                     |                                   |                  |           |                  |            |                  |               |              |           |
| Group Mgmt        | Group Mgmt Privilege               | Yes                               | Yes              | No        | No               | Yes        | No               | No            | No           | No        |
|                   | User Privilege                     |                                   |                  |           |                  |            |                  |               |              |           |
| User              | Common Inventory User Privilege    | Yes                               | Yes              | No        | Yes              | No         | Yes              | Yes           | Yes          | No        |
|                   | Cross Launch Privilege             |                                   |                  |           |                  |            |                  |               |              |           |
|                   | Fault Mgmt Privilege               |                                   |                  |           |                  |            |                  |               |              |           |
|                   | Subsystem Inventory User Privilege |                                   |                  |           |                  |            |                  |               |              |           |
|                   | User Privilege                     |                                   |                  |           |                  |            |                  |               |              |           |

| Default Role Name     | Privileges                          | Ability to Access These Portlets: |                  |                 |                  |                  |                  |               |              |           |
|-----------------------|-------------------------------------|-----------------------------------|------------------|-----------------|------------------|------------------|------------------|---------------|--------------|-----------|
|                       |                                     | My Account                        | User Preferences | User Management | Suite Monitoring | Group Management | Common Inventory | Alarm Browser | Alarm Report | Audit Log |
| User Management Admin | Cross Launch Privilege              | Yes                               | Yes              | Yes             | Yes              | No               | No               | No            | No           | No        |
|                       | Subsystem Inventory Admin Privilege |                                   |                  |                 |                  |                  |                  |               |              |           |
|                       | User Privilege                      |                                   |                  |                 |                  |                  |                  |               |              |           |
|                       | User Management Admin Privilege     |                                   |                  |                 |                  |                  |                  |               |              |           |



**Note** In the GUI, there are no spaces in the role or privilege names.

## Adding a Role

### Procedure

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click the **Roles** tab.
- Step 3** Click **Add**.
- Step 4** In the Add Role dialog box:
  - a) Enter a role name that conforms to the constraints listed in the [Table 1: Name, Password, Phone, and Note Constraints](#) table.
  - b) Enter a description that contains from 1 to 50 alphanumeric or special characters.
  - c) Check the appropriate privilege check boxes to assign the new role at least one privilege. Prime Central provides the default privileges listed in [Managing Privileges](#).
  - d) Click **Add**.  
The new role is displayed in the Roles tab.

## Editing a Role

### Procedure

- 
- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click the **Roles** tab.
- Step 3** Select the role that you want to edit and click **Edit**.
- Step 4** Edit the role description or assigned privileges, as required. The role description can contain from 1 to 50 alphanumeric or special characters.  
The role name is display only and cannot be changed.
- Step 5** Click **Update**.
- 

## Deleting a Role

### Procedure

- 
- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click the **Roles** tab.
- Step 3** Select the role that you want to delete and click **Delete**.
- Step 4** At the confirmation prompt, click **Yes**.
- 

## Managing Privileges

Privileges control the portlets, menu options, and back-end URLs that a role is authorized to access in Prime Central.

Prime Central provides the default privileges shown in the following table. The default privileges cannot be edited or deleted.

**Table 4: Default Prime Central Privileges**

| Default Privilege Name | Can...                                                                                                                              |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Admin Privilege        | <ul style="list-style-type: none"> <li>Issue all back-end operations, including create, read, update, and delete (CRUD).</li> </ul> |
| All Access Privilege   | <ul style="list-style-type: none"> <li>See all menu options.</li> </ul>                                                             |

| Default Privilege Name              | Can...                                                                                                                                                                                                                                                             |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Common Inventory Admin Privilege    | <ul style="list-style-type: none"> <li>• Access the Common Inventory portlet.</li> <li>• Access the Suite Monitoring portlet.</li> <li>• Issue all common inventory back-end operations, including CRUD.</li> </ul>                                                |
| Common Inventory User Privilege     | <ul style="list-style-type: none"> <li>• Issue GET ONLY common inventory back-end operations.</li> <li>• Access the Common Inventory portlet.</li> <li>• Access the Suite Monitoring portlet.</li> </ul>                                                           |
| Cross Launch Privilege              | <ul style="list-style-type: none"> <li>• Cross-launch applications.</li> </ul>                                                                                                                                                                                     |
| Fault Management Privilege          | <ul style="list-style-type: none"> <li>• Access the Alarm Browser portlet.</li> <li>• Access the Alarm Report portlet.</li> <li>• Access the Suite Monitoring portlet.</li> </ul>                                                                                  |
| Group Management Privilege          | <ul style="list-style-type: none"> <li>• Access the Group Management portlet.</li> <li>• See the following menu option:<br/>Administration &gt; Group Management &gt; Groups</li> <li>• Issue all group management back-end operations, including CRUD.</li> </ul> |
| InTracer Launch Privilege           | <ul style="list-style-type: none"> <li>• Cross-launch the InTracer application.</li> </ul>                                                                                                                                                                         |
| Subsystem Inventory Admin Privilege | <ul style="list-style-type: none"> <li>• Issue all subsystem inventory back-end operations, including CRUD.</li> <li>• Access the Suite Monitoring portlet.</li> </ul>                                                                                             |
| Subsystem Inventory User Privilege  | <ul style="list-style-type: none"> <li>• Issue GET ONLY subsystem inventory back-end operations.</li> </ul>                                                                                                                                                        |
| User Management Admin Privilege     | <ul style="list-style-type: none"> <li>• Issue all user management back-end operations, including CRUD.</li> <li>• Access the User Management portlet.</li> <li>• Access the Suite Monitoring portlet.</li> </ul>                                                  |

| Default Privilege Name | Can...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Privilege         | <ul style="list-style-type: none"> <li>• See most menu options, <i>except for the following</i>: <ul style="list-style-type: none"> <li>◦ Assure &gt; Prime Fault Management &gt; Alarm Browser</li> <li>◦ Assure &gt; Prime Fault Management &gt; Alarm Report</li> <li>◦ Inventory &gt; Common Inventory &gt; Devices</li> <li>◦ Administration &gt; User and Privilege Management &gt; Users</li> <li>◦ Administration &gt; System &gt; Suite Monitoring</li> </ul> </li> <li>• Access the My Account portlet.</li> <li>• Access the User Preferences portlet.</li> </ul> |



**Note** In the GUI, there are no spaces in the privilege names.

## Adding a Privilege

### Procedure

- 
- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click the **Privileges** tab.
- Step 3** Click **Add**.
- Step 4** In the Add Privilege window:
- a) Enter a privilege name that conforms to the constraints listed in the [Table 1: Name, Password, Phone, and Note Constraints](#) table.
  - b) Enter a description that contains from 1 to 50 alphanumeric or special characters.
  - c) In the URL Filter Expression field, enter a URL filter expression to enable access to a specific back-end URL pattern. This field is a free-form text field; all characters are allowed.
  - d) Assign portlets to the privilege by checking the appropriate check boxes.
  - e) Select which menu options the privilege will be able to access. Click the Expand icon and navigate to the appropriate menu options.
- Step 5** Click **Add**.
- Step 6** Create a new role and assign it the newly created privilege in the Privileges tab. See [Adding a Role](#).
-

## Editing a Privilege

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
  - Step 2** In the User Management portlet, click the **Privileges** tab.
  - Step 3** Select the privilege that you want to edit and click **Edit**.
  - Step 4** In the Edit Privilege window, update the privilege description, URL filter expressions, assigned portlets, and menu options, as required. The description can contain from 1 to 50 alphanumeric or special characters. The privilege name is display only and cannot be changed.
  - Step 5** Click **Update**.
- 

## Deleting a Privilege

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
  - Step 2** In the User Management portlet, click the **Privileges** tab.
  - Step 3** Select the privilege that you want to delete and click **Delete**.
  - Step 4** At the confirmation prompt, click **Yes**.
- 

## Exporting User Data

Prime Central allows you to export user data to Microsoft Excel. Opening the exported file with any program other than Excel is not recommended.

If you sort or filter the data before exporting it, the exported data is likewise sorted or filtered. If you check the left-most check box for a row, the exported data contains a check box for each checked row.

### Procedure

---

- Step 1** From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
- Step 2** In the User Management portlet, click the tab that contains the data you want to export.
- Step 3** Click the **Export to Excel** icon.
- Step 4** At the prompt to open or save the Excel file, click **Open**. The default filename depends on the tab you selected in Step 2.:
  - Users tab—usermgmt-Users-table.xls

- Groups tab—usermgmt-Groups-table.xls
- Roles tab—usermgmt-Roles-table.xls
- Privileges tab—usermgmt-Privileges-table.xls

**Note** By default, browser caching is enabled. If you disable caching, you might receive the following errors when you try to export user data:

*Browser cannot download file from server.*

*Browser was not able to open this Internet site. The requested site is either unavailable or cannot be found.*

*Please try again later.*

**Step 5** Click **Yes** at the following prompt:

The file you are trying to open, '*filename*', is in a different format than specified by the file extension.

Verify that the file is not corrupted and is from a trusted source before opening the file.

Do you want to open the file now?

---

## Auditing User Activity

Prime Central collects and stores security audit information, which you can use to track user activity such as logins or logouts, updates of user information, and application cross launches.

### Procedure

---

**Step 1** From the Prime Central menu, choose **Administration > System > Audit Log**. The Audit Log portlet opens, displaying user activity for the past 90 days (by default).

**Step 2** To change the default value, do the following:

- In the top-right corner of the Audit Log portlet, click the **Options** icon.
  - Click the **Configuration** link.  
The Audit Log - Configuration dialog box opens.
  - In the Number of Days of Audit Data Retention in Database field, enter the number of days for which you want Prime Central to store user activity. For example, if you enter 10, Prime Central will store activity for the past 10 days.  
After the configuration details are saved, the scheduler is triggered periodically to reflect the changes from the next day.
  - Click **Save**.
-



# Using an External Authentication Provider (LDAP or AAA Server) for User Authentication

By default, Prime Central uses internal authentication, which means passwords are stored in and verified against the data that is stored in the Prime Central database. You can also use a Lightweight Directory Access Protocol (LDAP) server or AAA server to manage user authentication externally. If you use external authentication, user information is checked against what is stored in the external LDAP or AAA server (instead of the Prime Central database). The external authentication server only stores login and password information; information pertaining to user roles is stored in the Prime Central database. The same user must exist in both the Prime Central database and the external authentication server.

## Configuring Prime Central to Communicate with an External LDAP Server

When you configure Prime Central for external user authentication via an Lightweight Directory Access Protocol (LDAP) server, you can choose to add another layer of security by enabling the use of SSL encryption. Complete one of the following procedures to configure an LDAP server connection.

### Configuring a Standard LDAP Server Connection

This procedure uses LDAP terminology, such as distinguished name (DN), common name (CN), and domain component (DC). An LDAP distinguished name uniquely identifies a user in the LDAP database, similar to a full filename but in reverse order. CNs and DCs are attributes of the domain name.

#### Procedure

- Step 1** In the User Management portlet, create a new user as described in [Adding a User](#). For example, create a Prime Central user named *test-admin*.
- Step 2** If the test-admin user does not already exist on the LDAP server, use an LDAP application to create the test-admin user.
- Step 3** Reset the test-admin user's LDAP password, ensuring that you enter this same password in Step 4d.
- Step 4** Do the following to enable LDAP authentication on the Prime Central portal:
  - a) As the primeusr user, log in to the Prime Central portal.
  - b) In the *installation-directory/XMP\_Platform/tomcat-7.0.23/webapps/SSO/WEB-INF/spring-configuration* folder, open the *cas\_xmp\_authentication\_providers.xml* file and do the following:

- Uncomment the following bean reference line:

```
<ref bean="ldapProviderPRIME" />
```

- If your *ldapUserDn* value is configured to something other than *uid*, replace *uid* with that value in the following line:

```
<constructor-arg index="1" value="(uid={0})" />
```

**Note** If your LDAP server makes use of the Windows Active Directory, run the following command to obtain the value you need to specify:

```
dsquery user -name test-admin
```

The value you are looking for is the first variable listed in the resulting output. In the following example, *CN* is the correct value.

```
"CN=test-admin,CN=Users,DC=t4,DC=local"
```

- c) Run the following script to encrypt the `ldapPassword` setting:  
**# portalAAAEncrypt**
- d) Enter the password (for example, **Cisco123**) that you want to encrypt. The script returns an encrypted value (for example, `zhEaxSqhTpJY0R2vStJJBQ==`) that you can use for the `ldapPassword` setting in the next step.
- e) In the `installation-directory/XMP_Platform/conf/prime/conf/extprovider.properties` file, configure the LDAP settings. See the [Table 5: Sample LDAP Server Settings](#) for a listing of sample settings.

**Step 5** As the `primeusr` user, enter the following commands to restart the Prime Central portal:

```
portactl stop
```

```
portactl start
```

You can now use the external authentication server for Prime Central authentication. In this example, the credentials to log in to the Prime Central portal are:

- Username: `test-admin`
- Password: *test-admin's password as configured on the external authentication server*

### Sample LDAP Server Settings

The following table provides samples of the settings you would specify when configuring an LDAP server for Prime Central authentication.

**Table 5: Sample LDAP Server Settings**

Setting	Sample Value	Description
<code>ldapServerName</code>	<code>ldap://209.165.200.254:56425</code>	LDAP server IP address or hostname and directory server port number.
<code>ldapUserDn</code>	<code>CN=test-admin,CN=Users,DC=t4,DC=local</code>	LDAP server user ID to log in to the LDAP server.  To obtain the value you need to specify for this setting, run the following command:  <b>dsquery user -name test-admin</b>  <b>Note</b> Exclude the quotation marks when you enter this value.
<code>ldapPassword</code>	(Encrypted) <code>zhEaxSqhTpJY0R2vStJJBQ==</code>	LDAP server user password to log in to the LDAP server.

Setting	Sample Value	Description
ldapBase	CN=Users,DC=t4,DC=local	LDAP base of LDAP users for authentication.

## Configuring an SSL-Encrypted LDAP Server Connection

### Procedure

- 
- Step 1** In the User Management portlet, create a new user as described in [Adding a User](#). For example, create a Prime Central user named *test-admin*.
- Step 2** If the test-admin user does not already exist on the LDAP server, use an LDAP application to create the test-admin user.
- Step 3** Enable SSL encryption on your LDAP server, following the instructions provided in the documentation for your server.
- Step 4** In the first line of the `extprovider.properties` file, which can be found in the `installation-directory/XMP_Platform/conf/prime/conf` folder:
- Replace **ldap:** with **ldaps:**
  - Ensure that the correct SSL port number is referenced

For example, if port number 10636 is designated for SSL use on your server, the first line of the `extprovider.properties` file should look like this:

```
ldapServerName=ldaps://$Your_Server:10636
```

- Step 5** Export the LDAP SSL keystore certification by entering the following command:  
**keytool -export -keystore *Your\_LDAP.ks* -alias *Your\_Domain* -file *Your\_LDAP.cer***  
 This command will create the keystore certificate (in this example, *Your\_LDAP.cer*).  
 Make sure to specify the same `.ks` file you set up when you enabled SSL encryption on your LDAP server.
- Step 6** Import the keystore certificate into the Prime Central keystore by entering the following command:  
**keytool -import -alias *Your\_Domain* -file *Your\_LDAP.cer* -keystore *\$XMP\_Home/jre/lib/security/cacerts***  
 where `XMP_Home` is the Prime Central installation directory.
- Step 7** As the root user, enter the keystore password.
- Step 8** Restart the Prime Central portal.
- Step 9** (Optional) To verify that you have set up the LDAP server connection correctly using an LDAP client, such as `jexplorer`, import the keystone certificate to your local client machine by entering the following command:  
**keytool -import -alias *Your\_Domain* -file *Your\_LDAP.cer* -keystore *\$JAVA\_Home/jre/lib/security/cacerts***  
 where `JAVA_Home` is the JDK installation directory.
-

## Configuring Prime Central to Communicate with an External AAA Server

Use this procedure to configure the Prime Central portal to communicate with the AAA (RADIUS or TACACS+) server, and to test the connection after it is configured. This procedure uses AAA terminology.

### Procedure

- 
- Step 1** In the User Management portlet, create a new user as described in [Adding a User](#). For example, create a Prime Central user named *test-admin*.
- Step 2** If the test-admin user does not already exist on the AAA server, use an AAA application to create the test-admin user.
- Step 3** Do the following to enable AAA authentication on the Prime Central portal:
- As the primeusr, log in to the Prime Central portal.
  - In the *installation-directory/XMP\_Platform/tomcat-7.0.23/webapps/SSO/WEB-INF/spring-configuration* folder, open the *cas\_xmp\_authentication\_providers.xml* file and uncomment the following bean reference line:
    - For TACACS+, uncomment:
 

```
<ref bean="jaasTacacsAuthenticationProviderPRIME" />
```
    - For RADIUS, uncomment:
 

```
<ref bean="jaasRadiusAuthenticationProviderPRIME" />
```
  - Run the following script to encrypt the JaasSecretKey setting:  
**# portalAAAEncrypt**
  - Enter the secret key (for example, **Cisco123**) that you want to encrypt. The script returns an encrypted value (for example, **zhEaxSqhTpJY0R2vStJJBQ==**) that you can use for the JaasSecretKey setting in the next step.
  - In the *installation-directory/XMP\_Platform/conf/prime/conf* folder, do one of the following:
    - For TACACS+, open the *jaas.config.tacacs* file and configure the TACACS+ settings. See the [Table 6: Sample AAA Server Settings](#) for a listing of sample settings.
    - For RADIUS, open the *jaas.config.radius* file and configure the RADIUS settings. See the [Table 6: Sample AAA Server Settings](#) for a listing of sample settings.
- Step 4** As the primeusr user, enter the following commands to restart the Prime Central portal:  
**portalctl stop**  
**portalctl start**
- Step 5** You can now use the external authentication server for Prime Central authentication. In this example, the credentials to log in to the Prime Central portal are:
- Username: test-admin
  - Password: *test-admin's password as configured on the external authentication server*
-

## Sample AAA Server Settings

The following table provides samples of the settings you would specify when configuring a AAA server for Prime Central authentication.

**Table 6: Sample AAA Server Settings**

Setting	Sample Value	Description
<b>TACACS+</b>		
server	209.165.200.254	TACACS+ server IP address or hostname
port	49	TACACS+ server port number
JaasSecretKey	(Encrypted) zhEaxSqhTpJY0R2vStJJBQ==	TACACS+ server secret key
<b>RADIUS</b>		
server	209.165.200.254	RADIUS server IP address or hostname
port	1812	RADIUS server port number
JaasSecretKey	(Encrypted) zhEaxSqhTpJY0R2vStJJBQ==	RADIUS server secret key
authenticationType	PAP	RADIUS server authentication type <b>Note</b> Only PAP authenticationType is supported by Radius.

