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

<table>
<thead>
<tr>
<th>1</th>
<th>User management tabs: Users, Groups, Roles, Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Properties pane</td>
</tr>
</tbody>
</table>
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:

- 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.

- For Prime Central, all new users are assigned the User role automatically. 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:

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:


- 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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username must:</td>
</tr>
<tr>
<td></td>
<td>• Start with a letter.</td>
</tr>
<tr>
<td></td>
<td>• Contain from 4 to 20 case-sensitive letters (A-Z, a-z), numbers (0-9), hyphens (-), or underscores (_).</td>
</tr>
<tr>
<td></td>
<td>• Not contain any other special characters or spaces.</td>
</tr>
<tr>
<td></td>
<td>• Not be the reserved keywords prime, web, guest, user, group, public, or private, in any combination of uppercase or lowercase letters.</td>
</tr>
<tr>
<td>Note</td>
<td>• Usernames are case-sensitive. Prime Central treats UserA and userA as separate users.</td>
</tr>
<tr>
<td></td>
<td>• If the username that you enter already exists in an installed application, Prime Central overwrites the existing application user with this new user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group name, role name, or privilege name</th>
<th>The name must:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Start with a letter.</td>
</tr>
<tr>
<td></td>
<td>• Contain from 1 to 50 letters (A-Z, a-z), numbers (0-9), hyphens (-), or underscores (_).</td>
</tr>
<tr>
<td></td>
<td>• Not contain spaces or other special characters.</td>
</tr>
<tr>
<td>Variable</td>
<td>Constraints</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Password | The password must:  
  - 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:  
    - Uppercase letters (A-Z).  
    - Lowercase letters (a-z).  
    - Numbers (0-9).  
    - Special characters.  
  - Not contain the username or the username in reverse.  
  - Not contain `cisco`, `ocsic`, 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.

**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:
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
**Managing Users and Configuring Role-Based Access Control**

### 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:


- 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 disabled 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 disabled for the **centraladmin** user.

**Step 7** Click **Save**.

*Figure 3: My Account Portlet*
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:

- 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**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Log In Attempts</td>
<td>The maximum number of failed login attempts allowed before the user account is denied access to Prime Central. The default is 6 retries.</td>
</tr>
<tr>
<td>Maximum Active User Sessions</td>
<td>The number of concurrent sessions allowed. The default is 1 session.</td>
</tr>
<tr>
<td>User Session Timeout (minutes)</td>
<td>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.</td>
</tr>
<tr>
<td>Password Expiration (days)</td>
<td>The number of days before the password expires. The default is 60 days.</td>
</tr>
<tr>
<td>Password Expiration Warning (days)</td>
<td>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.</td>
</tr>
<tr>
<td>Number of Passwords Before Reuse</td>
<td>The number of different passwords a user must use before being allowed to reuse the first password. The default is 4 passwords. This field takes priority over the Used Password Re-enablement Period field. For example, assume that:</td>
</tr>
<tr>
<td></td>
<td>• Number of Passwords Before Reuse: 2</td>
</tr>
<tr>
<td></td>
<td>• Used Password Re-enablement Period: 5</td>
</tr>
<tr>
<td></td>
<td>If the user password is <em>test</em>, you can change it to <em>sample</em> the next day, and then to <em>basic</em> on the second day. You can then change it back to <em>test</em> before 5 days elapses, because the Number of Passwords Before Reuse field takes priority.</td>
</tr>
<tr>
<td>Used Password Re-enablement Period (days)</td>
<td>The number of days before an old password can be reused. The default is 120 days.</td>
</tr>
<tr>
<td>Minimum Duration Between Password Change (days)</td>
<td>The number of days a user must wait between password changes. The default is 0 days.</td>
</tr>
<tr>
<td>Number of Prohibited Consecutive Characters From Previous Password</td>
<td>The number of consecutive characters by which the new password must differ from the previous one. The default is 3 characters.</td>
</tr>
</tbody>
</table>
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 no Common Inventory access) paired with the User role (which has Common Inventory access) results in Common Inventory access.
### Table 3: Default Prime Central Roles

<table>
<thead>
<tr>
<th>Default Role Name</th>
<th>Privileges</th>
<th>Ability to Access These Portlets:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>My Account</td>
</tr>
<tr>
<td><strong>Administrator</strong></td>
<td>Admin Privilege</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>All Access Privilege</td>
<td></td>
</tr>
<tr>
<td></td>
<td>InTracer Launch Privilege</td>
<td></td>
</tr>
<tr>
<td><strong>Common Inventory Admin</strong></td>
<td>Common Inventory Admin Privilege</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cross Launch Privilege</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subsystem Inventory User Privilege</td>
<td></td>
</tr>
<tr>
<td><strong>Common Inventory User</strong></td>
<td>Common Inventory User Privilege</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cross Launch Privilege</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subsystem Inventory User Privilege</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User Privilege</td>
<td></td>
</tr>
<tr>
<td>Default Role Name</td>
<td>Privileges</td>
<td>Ability to Access These Portlets:</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>My Account</td>
</tr>
<tr>
<td>Fault Management</td>
<td>Cross Launch Privilege</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Fault Management Privilege</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subsystem Inventory User Privilege</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User Privilege</td>
<td></td>
</tr>
<tr>
<td>Group Management</td>
<td>Group Management Privilege</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>User Management Privilege</td>
<td></td>
</tr>
<tr>
<td>User (assigned to all new users automatically)</td>
<td>Common Inventory User Privilege</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cross Launch Privilege</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fault Management Privilege</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subsystem Inventory User Privilege</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User Privilege</td>
<td></td>
</tr>
</tbody>
</table>
### 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.

---

<table>
<thead>
<tr>
<th>Default Role Name</th>
<th>Privileges</th>
<th>Ability to Access These Portlets:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>My Account</td>
</tr>
<tr>
<td>User Management Admin</td>
<td>Cross Launch Privilege</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Subsystem Inventory Admin Privilege</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User Privilege</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User Management Admin Privilege</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Default Privilege Name</th>
<th>Can...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Privilege</td>
<td>• Issue all back-end operations, including create, read, update, and delete (CRUD).</td>
</tr>
<tr>
<td>All Access Privilege</td>
<td>• See all menu options.</td>
</tr>
<tr>
<td>Default Privilege Name</td>
<td>Can...</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| Common Inventory Admin Privilege | • Access the Common Inventory portlet.  
• Access the Suite Monitoring portlet.  
• Issue all common inventory back-end operations, including CRUD. |
| Common Inventory User Privilege | • Issue GET ONLY common inventory back-end operations.  
• Access the Common Inventory portlet.  
• Access the Suite Monitoring portlet. |
| Cross Launch Privilege | • Cross-launch applications. |
| Fault Management Privilege | • Access the Alarm Browser portlet.  
• Access the Alarm Report portlet.  
• Access the Suite Monitoring portlet. |
| Group Management Privilege | • Access the Group Management portlet.  
• See the following menu option: Administration > Group Management > Groups  
• Issue all group management back-end operations, including CRUD. |
| InTracer Launch Privilege | • Cross-launch the InTracer application. |
| Subsystem Inventory Admin Privilege | • Issue all subsystem inventory back-end operations, including CRUD.  
• Access the Suite Monitoring portlet. |
| Subsystem Inventory User Privilege | • Issue GET ONLY subsystem inventory back-end operations. |
| User Management Admin Privilege | • Issue all user management back-end operations, including CRUD.  
• Access the User Management portlet.  
• Access the Suite Monitoring portlet. |
Can...

- See most menu options, except for the following:
  - Assure > Prime Fault Management > Alarm Browser
  - Assure > Prime Fault Management > Alarm Report
  - Inventory > Common Inventory > Devices
  - Administration > User and Privilege Management > Users
  - Administration > System > Suite Monitoring

- Access the My Account portlet.
- Access the User Preferences portlet.

<table>
<thead>
<tr>
<th>Default Privilege Name</th>
<th>Can...</th>
</tr>
</thead>
</table>
| User Privilege         | • See most menu options, except for the following:  
                          ◦ Assure > Prime Fault Management > Alarm Browser  
                          ◦ Assure > Prime Fault Management > Alarm Report  
                          ◦ Inventory > Common Inventory > Devices  
                          ◦ Administration > User and Privilege Management > Users  
                          ◦ Administration > System > Suite Monitoring  
                          • Access the My Account portlet.  
                          • Access the User Preferences portlet. |

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**

1. From the Prime Central menu, choose Administration > User and Privilege Management > Users.
2. In the User Management portlet, click the Privileges tab.
3. Select the privilege that you want to edit and click Edit.
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.
5. Click Update.

**Deleting a Privilege**

**Procedure**

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

**Importing Users in Bulk**

From the UNIX command line, you can perform a bulk import of users from an Excel file that you create.

**Procedure**

1. As the primeusr user, log in to the Prime Central portal with the primeusr password that you specified during installation.
3. Create your own Excel file that contains all the users you want to import; then, add that spreadsheet to the UtilityUsersDir folder. By default, the UtilityUsersDir folder contains a sample spreadsheet named customers.xlsx. You can structure your Excel file similarly.

The sample customers.xls file contains four sheets, each of which corresponds to a step in the User Management portlet > Add wizard.
Each sheet contains a GLOBAL SETTING row with information that will apply to all users, unless you overwrite the global setting with your specified value. If you leave a cell blank, Prime Central uses the global setting.

**Step 4** Enter the following command to import the users defined in your Excel file into the Prime Central database:

```
sh importUsers FILE Excel-filename
```

For example, to import a file named users_xyz.xlsx, enter:

```
sh importUsers FILE users_xyz.xlsx
```

**Step 5** At the following prompt, enter your Prime Central administrative username and password:

Enter Prime Central admin username:

Enter Prime Central admin user password:

**Step 6** At the following prompt:

Do you want the system to generate a random password for each imported user? [Y|N]:

Enter one of the following:

• **Y** if you want Prime Central to generate a random password for each imported user, unless overwritten by your Excel file.

• **N** if you want to choose a default password for all imported users. Then, at the following prompt, enter a password that will apply to all users

Enter a default password for all imported users:

The import begins. When it finishes, output similar to the following is displayed:

```
*** Importing user USER_3 ***
Creating USER_3 in Prime Central
User USER_3 is created successfully in Prime Central with local password password
*** Importing user USER_2 ***
Creating USER_2 in Prime Central
User USER_2 is created successfully in Prime Central with local password password
*** Importing user USER_1 ***
Creating USER_1 in Prime Central
User USER_1 is created successfully in Prime Central with local password password
Number of users requested: 3
Number of users imported: 3
```

**Note** You cannot import the same username more than once. If you try to import multiple users with the same username, Prime Central returns the following error: "User username already exists in Prime Central."

**Step 7** Log in to Prime Central and choose Administration > User and Privilege Management > Users to open the User Management portlet. Verify that the users you imported are visible in the Users tab.

---

**Reporting User Logins in Bulk**

From the UNIX command line, you can run a script to report users who logged in to (or did not log in to) Prime Central within a specific number of days.
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
Managing Users and Configuring Role-Based Access Control

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:

a) In the top-right corner of the Audit Log portlet, click the Options icon.

b) Click the Configuration link.

The Audit Log - Configuration dialog box opens.

c) 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.

d) 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 `primeuser` user, enter the following commands to restart the Prime Central portal:

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

```java
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 keystore 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. User can configure up to three TACACS+ servers.
### 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:

a)  
As the primeusr, 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 uncomment the following bean reference line:

```
• For TACACS+, uncomment:
  <ref bean="jaasTacacsAuthenticationProviderPRIME" />

• For RADIUS, uncomment:
  <ref bean="jaasRadiusAuthenticationProviderPRIME" />
```

c)  
Run the following script to encrypt the JaasSecretKey setting:

```
# portalAAAEncrypt
```

d)  
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.

e)  
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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Sample Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TACACS+</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server</td>
<td>209.165.200.254</td>
<td>TACACS+ server IP address or hostname</td>
</tr>
<tr>
<td>port</td>
<td>49</td>
<td>TACACS+ server port number</td>
</tr>
<tr>
<td>secondaryServer</td>
<td>209.165.200.253</td>
<td>TACACS+ server IP address or hostname</td>
</tr>
<tr>
<td>secondaryPort</td>
<td>49</td>
<td>TACACS+ server port number</td>
</tr>
<tr>
<td>tertiaryServer</td>
<td>209.165.200.254</td>
<td>TACACS+ server IP address or hostname</td>
</tr>
<tr>
<td>tertiaryPort</td>
<td>49</td>
<td>TACACS+ server port number</td>
</tr>
<tr>
<td>JaasSecretKey</td>
<td>(Encrypted)TACACS+ server secret key zhEaxSqhTpJY0R2vStJJBQ==</td>
<td>TACACS+ server secret key</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RADIUS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server</td>
<td>209.165.200.254</td>
<td>RADIUS server IP address or hostname</td>
</tr>
<tr>
<td>port</td>
<td>1812</td>
<td>RADIUS server port number</td>
</tr>
<tr>
<td>JaasSecretKey</td>
<td>(Encrypted)zhEaxSqhTpJY0R2vStJJBQ==</td>
<td>RADIUS server secret key</td>
</tr>
<tr>
<td>authenticationType</td>
<td>PAP</td>
<td>RADIUS server authentication type</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Only PAP authenticationType is supported by Radius.</td>
</tr>
</tbody>
</table>

### Sample TACACS Configuration:

```java
TACACS {
    com.cisco.xmp.jaas.tacacs.TacacsLoginModule required
debug=true
    JaasSecretKey="tIm+wkEvOaUgdhhWSLf+gA=="
    server="172.168.203.200"
    port="49"
    secondaryServer="172.168.203.197"
    secondaryPort="49";
};
```