Manage Users

This section explains the following:

Manage Users

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

In Cisco Prime Collaboration Assurance, you can create users and assign roles to the users.

Cisco Prime Collaboration Assurance enables Role-based Access Control (RBAC) through these built-in static roles. Hence, the tasks a user can perform, or the device or device groups a user can view or manage is controlled by the role allocated by the Super Administrator.

You can enforce further access control of selected devices or device groups, and tasks related to those by associating the devices or device groups to domains (if you have deployed Cisco Prime Collaboration Assurance in Enterprise mode). Typically, a user with Operator role, is granted access to certain domains only.

Cisco Prime Collaboration Assurance-Advanced User Roles

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

You can be assigned one of the following roles:

- **For Cisco Prime Collaboration Release 11.5 and later**

  Report Viewer—Can view and export the reports only. The homepage of Report Viewer is CDR & CMR Reports. The global user interface components like **Search**, **Device Status Summary**, **Alarms**, and **Get Advanced** are not available for the Report Viewer user role. You can view all the reports except the following:

  - Launch CUCM Reports
  - Administrative Reports
  - Scheduled Reports

- Helpdesk — Views and accesses network status information only and cannot perform any action on a device or schedule a job that reaches the network.

- Operator — Performs all Helpdesk tasks and tasks related to the network data collection. Cannot perform any Inventory Management operations such as adding, discovering, or importing devices. Also, an operator cannot configure thresholds for Alarms and Events.
- Network administrator — Performs all Operator tasks and tasks that result in a network configuration change like credential management, threshold settings, and so on.
- System administrator — Performs the Assurance user interface-related administration tasks such as backup and restore, maintaining log files, configuring users, and so on.
- Super administrator — Can perform tasks that both system administrator and network administrator can perform.

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

For Cisco Prime Collaboration Release 11.5 and later

Report Viewer is a preselected role that is assigned to every user in Cisco Prime Collaboration Assurance.

The roles selected for a user, determines the access to data of other users. For example, a user with the Super Admin role can view all other users, however a user with the Network Administrator role cannot view the users with higher roles such as Super Administrator, or System Administrator, but can look at other user's data whose role is of Operator or Helpdesk.

If you have deployed Cisco Prime Collaboration Assurance in MSP Mode, you can look at customers belonging to another user of the same role, only if you are associated with the customer(s).

If you have deployed Cisco Prime Collaboration Assurance in ENT Mode, you can look at domains belonging to another user of the same role, only if you are associated with the domain(s).

Note: The User Management submenu is not available to the following roles:

For Cisco Prime Collaboration Release 11.5 and later

1. Report Viewer
2. Helpdesk
3. Operator

For Cisco Prime Collaboration Release 11.6 and later

The default user role selection is removed from Cisco Prime Collaboration Assurance.

Note If Report Viewer user role is selected, the system does not allow the user to choose any other roles and vice versa.

For Cisco Prime Collaboration Release 12.1 SP3 and later

The following roles are supported to provide multiple levels of authorization:

1. **Network Administrator** - Performs all Operator tasks and tasks that result in a network configuration change like credential management, and so on
2. **System Administrator** - Performs the user interface-related administration tasks.
3. **Super Administrator** - Performs tasks that both system administrator and network administrator can perform.

Related Topics

Manage Customers
Manage Domains

Single Sign-On for Cisco Prime Collaboration Assurance

Cisco Prime Collaboration Assurance provides users with admin privileges to enable Single Sign-On (SSO) in Cisco Prime Collaboration Assurance using Security Assertion Markup Language (SAML).

Cisco Prime Collaboration Assurance does not support multiserver SAN certificates and end user SAML SSO.

Ensure that the following prerequisites are met before you enable SSO:

- At least one LDAP Administrative user exists in the system—by manually creating an LDAP administrative user in Cisco Prime Collaboration Assurance.
- An Identity Provider (IdP) server that enables you to use SSO to access many other applications from a single hosted application and a Service Provider. The Service Provider is a website that hosts the applications.

  Following are the supported third-party IdP servers:

  - Open Access Manager (OpenAM)
  - Ping Identity
  - Active Directory Federation Services (ADFS)
  - Oracle Identity Manager

  For the steps to setup an IdP server, see the SAML SSO Deployment Guide for Cisco Unified Communication Applications, Release 10.0(1).

- Download the Identity Provider metadata file from the IdP server and save it in your local system.

To enable Single Sign-On:

Step 1 Choose **System Administration** > **Single Sign-On**.

Step 2 Click **Enable SSO**.

A warning message is displayed stating, Enabling SSO redirects you to the IdP server for authentication from the next login. To access the application, you will need to be authenticated successfully.

Note **Enable SSO** is disabled if the above mentioned prerequisites are not met.

Step 3 Click **Continue**.

Step 4 Follow the steps provided in the SSO wizard to enable Single Sign-On.

a) Locate the IdP metadata file from your local system and click **Import IdP Metadata**.
b) Click **Download Trust Metadata file**.
c) Launch the IdP server and import the downloaded Trust Metadata file.

Note This is a manual step for Enabling SSO. You need to create a Circle of Trust (CoT) in the IdP server and log out before you proceed with the SSO testing.

d) To run SSO Test Setup, select a username from the **Valid Administrative Usernames** drop-down. You can enter any user who is an administrator in Active Directory and is synchronized by Cisco Unified CDM under SSO user.

Note Using any other username to log in to the IdP server might lock the administrator account.

e) Click **Run SSO Test** to test the connectivity among the IdP server, Cisco Prime Collaboration Assurance Applications, and Single Sign-On.

If you are prompted with an error message, Unable to do Single Sign-On or Federation:

- Manually log in to the IdP server using the end user credentials and check if the authentication is successful.
- Verify if the Trust Metadata file is successfully uploaded in the IdP server.
- Verify if the Cisco Prime Collaboration Assurance server and the IdP server are part of the same Circle of Trust.

f) Click **Finish**.

Troubleshooting and Logs for SSO

- When you are logged out of the Cisco Prime Collaboration Assurance server while enabling SSO, it is recommended that you close the browser and re-launch the Cisco Prime Collaboration Assurance application. Because, though your conference expires in Cisco Prime Collaboration Assurance server, the IdP server conference might still be active.
- While enabling SSO, ensure that the hostname for Cisco Prime Collaboration Assurance is set and is part of DNS.

When IdP server is down, you can:

- Use the recovery URL- https://<PCserver IP address or host name that is part of DNS>:8443/ssosp/local/login.
- Disable Single Sign-On from CMD Utility.

To disable SSO from CMD utility in Cisco Prime Collaboration Assurance applications:

- Log in to Cisco Prime Collaboration Assurance server using SSH with port 26.
- Navigate to the **/opt/emms/emsam/bin** directory for Cisco Prime Collaboration Assurance. Add <Operation> and <Value> entries for **cpcmconfigsso.sh** file based on the following table:

Operations can be ..	**Values can be ..**
1-To get the Single Sign-On status	Not applicable
2-To get the recovery URL status	Not applicable
3-To set the Single Sign-On status	False **Note** You cannot enable SSO through CLI. Use the user interface procedure to enable SSO.
4-To set the recovery URL status	True or False

- To disable SSO, run the following command:

cpcmconfigsso.sh 3 false

Note The recovery URL is enabled. If you want to disable it for security reasons, set it as False by default.

Default User Accounts

Cisco Prime Collaboration Assurance is preconfigured with a default web client administrator user called globaladmin; globaladmin is a superuser who can access Cisco Prime Collaboration Assurance user interfaces.

Specify a password for globaladmin when you configure your virtual appliance. You need to use these credentials when you launch the Cisco Prime Collaboration Assurance web client for the first time.

Caution We recommend that you note down the root password, as if it is forgotten/lost you will have to open a TAC support case to reset the root password.

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

Note See the Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide for password validation rules for these users.

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

Choose . Click the Download Log button. Download the tar file and untar it. Check the /opt/emms/emsam/log/importedprovisioninguser.log file, to find the users who were not imported into Cisco Prime Collaboration Assurance database due to several reasons such as duplicate user names (user names already used in Cisco Prime Collaboration Assurance), user names with no passwords and so on.

The Cisco Prime Collaboration Assurance applications do not share inventory database. You must manage the devices separately to perform the tasks. See Manage Device Credentials to perform device management tasks using the Cisco Prime Collaboration Assurance application.

Related Topics

Manage Device Credentials
Manage Device Groups

User Roles and Tasks

The User Roles and Tasks for Cisco Prime Collaboration Assurance 11.x versions and User Roles and Tasks for Cisco Prime Collaboration Assurance 12.x versions lists the Cisco Prime Collaboration Assurance user roles and tasks they are mapped to.

Note Super administrator has access to all of the user interface menus and can perform all the tasks. Hence, the super administrator is not listed .

Related Topics

User Roles and Tasks for Cisco Prime Collaboration Assurance

Add a User

You can add a user and assign predefined static roles. The user has access to the Cisco Prime Collaboration Assurance web client only and cannot log in to the Cisco Prime Collaboration Assurance server through the CLI.

To add a user:

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

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

Step 3 In the **Add User** page, enter the required user details.

Note that because the LDAP server performs authentication, it should have the same user ID as Cisco Prime Collaboration Assurance. For more information, see Configure an LDAP Server.

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

Step 4 Select the appropriate Cisco Prime Collaboration Assurance roles.

Step 5 Click **Save**.

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

For Cisco Prime Collaboration Release 11.6 and later

To exclude Report Viewer user role from the assigned roles, you have to manually deselect the Report Viewer option and click **Save**.

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

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

Modify User Roles

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

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

For Cisco Prime Collaboration Release 11.6 and later

To exclude Report Viewer user role from the assigned roles, you have to manually deselect the Report Viewer option and click **Save**.

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

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

Configure an LDAP Server

You can configure Cisco Prime Collaboration Assurance to connect to a Lightweight Directory Access Protocol (LDAP) server, to access user information stored in the LDAP server.

You must create an LDAP user from the User Management page to enable the user to log in using LDAP credentials. To add a user, see Add a User and to edit or delete a user, see Modify User Roles.

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

To configure LDAP server:

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

Step 2 In the LDAP Settings page, enter values for all the fields. See LDAP Configuration Parameters for the field descriptions.

Note

a. If Cisco Prime Collaboration Assurance must use SSL encryption, check the Use SSL check box and specify port 636.

For Cisco Prime Collaboration Release 12.1

LDAP configuration with SSL enabled is not supported.

b. In case of invalid login, a message indicating that "Invalid Username or Password. Please try again or check LDAP server configuration if you are a LDAP user" appears. This message is applicable for both local and LDAP users.

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

Step 4 Upon successful connection, click **Apply Settings** and restart Cisco Prime Collaboration Assurance Server to log in using LDAP.

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

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

The **application stop cpcm** command takes 10 minutes to complete execution and **application start cpcm** takes 10 to 15 minutes to complete execution.

LDAP Configuration Parameters

For example, Consider Microsoft Active Directory.

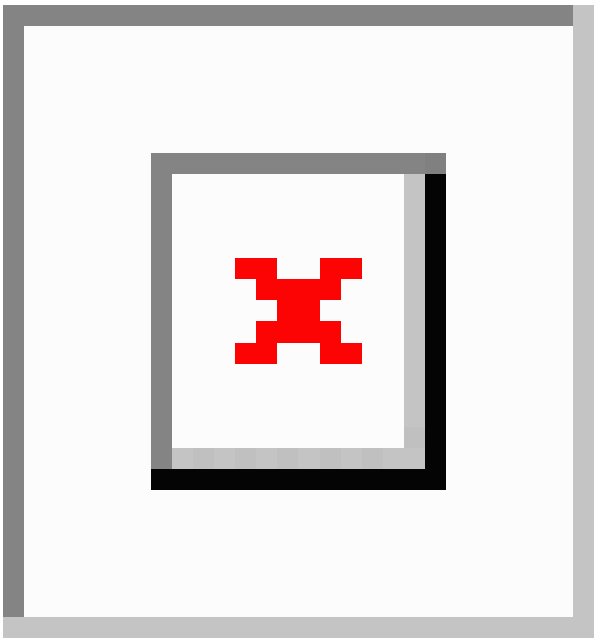

Table 1: LDAP Server Configuration

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

Field	Description
Admin Distinguished Name	Admin Distinguished Name is the distinguished name to use. For example in the preceding image there is a user whose name is John Doe in the LDAP directory, so the Admin Distinguished Name will be as follows: • CN = John Doe • OU = Campus • OU = AdminBLR • OU = ABC • DC = eta • DC = com
Admin Password	Enter the password for the LDAP server authentication and reconfirm the password. **Note** Do not use the pound sign (#) in the password, because the connectivity to the LDAP server fails if the LDAP user password contains the pound sign (#).
LDAP User Search Base	Enter the user search base. LDAP server searches for users under this base. Search Base is as follows: • DC = eta • DC = com **Note** LDAP authentication fails if you enter special characters in the search base.

Note

1. Cisco Prime Collaboration Assurance supports login to PCA with CN or sAMAccountName or uid attributes of an LDAP user as applicable.
2. uid attribute of an LDAP user should be unique.
3. The ampersand (&) character in Distinguished Names (DN) is not allowed in LDAP parameter value.

   To connect to LDAP, enter the following LDAP parameter value -

   ```
   ?CN=hq-prime,OU=Service Access Groups,DC=Megafon,DC=ru?
   ```

For a list of supported LDAP servers, see Supported Devices for Cisco Prime Collaboration Assurance.

Configure Maximum Length for Password

An authentication mechanism is only as strong as its credentials.

A strong authentication mechanism is important to force a strong password. Lack of password complexity, particularly password length, significantly reduces the search space.

Note

- The default maximum length of a password is 127 characters.
- Only the default administrator globaladmin has permissions to modify the security settings page in Cisco Prime Collaboration Assurance user interfaces.

Step 1 Choose **System Administration** > **Security Settings.**

Note Users must ensure to enter values within the range of 80-127 characters (not bytes). If the entered value is out of range then a message indicating that the value entered is out of the permissible range appears. Click **OK** to continue.

Step 2 Enter the value or click the spinners to configure the password length.

Step 3 Click **Save** to successfully update the configuration details. The application alerts that the user is modifying the maximum length of the password. Ensure compliance with this new value while setting password in other pages appears.

Click **Cancel** to exit.

Note Users cannot enter a password of length more than the configured value in any other page where password is required. An error message appears on the respective pages indicating incompliance.

Unlock Cisco Prime Collaboration Assurance Account

For Cisco Prime Collaboration Release 11.5 and later

The permissible login attempts to access the Cisco Prime Collaboration Assurance user interface is 10. If you make 10 failed attempts to log in to Cisco Prime Collaboration Assurance user interface, your account gets disabled.

A globaladmin user with administrator privileges can unlock the account.

To unlock the account:

Step 1 Log in to Cisco Prime Collaboration Assurance as globaladmin.

Step 2 Choose **System Administration** > **User Management**.

Step 3 On the **User Management** page, select the user and click **Unlock**.