Manage Users

Cisco Prime Collaboration supports creation of user roles. A user can be assigned the Super Administrator role. A Super Administrator can perform tasks that both system administrator and network administrator can perform.

Cisco Prime Collaboration is preconfigured with a default web client administrator user called globaladmin; globaladmin is a superuser who can access both the 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 web client for the first time.

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

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

Caution

- CLI users are not listed on the Cisco Prime Collaboration User Management page.

Globaladmin and root follow same set of password validation rules, but the rules for admin are different. See the Cisco Prime Collaboration Quick Start Guide for password validation rules for these users.

Globaladmin follows same set of password validation rules, but the rules for admin are different. See the Cisco Prime Collaboration Assurance Install and Upgrade Guide.

Add, Edit, and Delete a User

You can add a user and assign the predefined static role. The user will have access to the Cisco Prime Collaboration web client only.

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

You, as a globaladmin, must create other administrators using real user-IDs.

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

To add a user:

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

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

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

Step 4 Select the role.

Step 5 Click **Save**.
The users thus created via Add User feature are associated with the web client only and cannot log in to the Cisco Prime Collaboration Assurance server through the CLI.

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

As part of your regular system administration tasks, you sometimes must delete users from the Cisco Prime Collaboration database. However, you cannot delete the Cisco Prime Collaboration 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.

Configure an LDAP Server

You can configure Cisco Prime Collaboration 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, edit or delete a user, see Add, Edit, and Delete a User.

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

To configure an 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 If Cisco Prime Collaboration must use SSL encryption, check the Use SSL check box and specify port 636.

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.

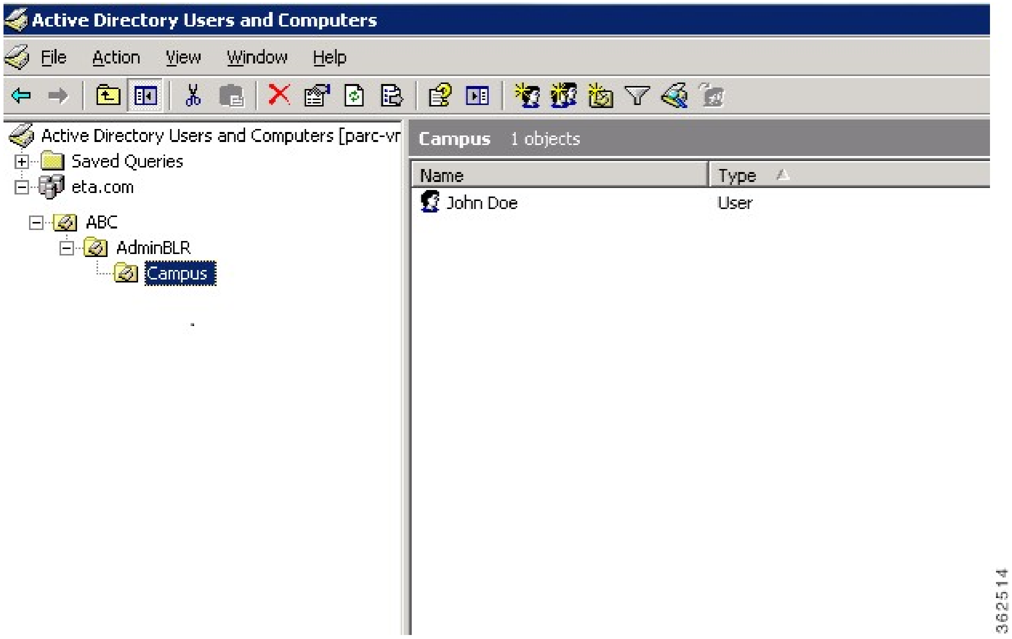
To restart Cisco Prime Collaboration Assurance Server, log in as admin user and execute the following commands:

```
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.



Name	Type
John Doe	User

Table 1: LDAP Server Configuration

Field	Description
IP Address / Hostname	Enter the LDAP server name or IP address. Optionally enter the Backup LDAP server IP address.

Field	Description
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.
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.

For a list of LDAP servers supported by Cisco Prime Collaboration 11.6, see Supported Devices for Prime Collaboration Assurance.

Reset Cisco Prime Collaboration Assurance Passwords

As a super administrator, system administrator or network operator, you can reset the password for other Cisco Prime Collaboration users.

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

To reset the Cisco Prime Collaboration Assurance globaladmin password:

Step 1 Log in as a root user.

Step 2 Execute the following:

```
#cd /opt/emms/emsam/bin/
        # ./resetGlobalAdminPassword.sh
```

Step 3 Enter a new password for the globaladmin when prompted, and also confirm the new password, when prompted. A message notifies that the globaladmin passwords has been successfully reset.

Change Passwords

To change your own password, go to **System Administration** > **User Management**, click **Change Password**, and make necessary changes.

Single Sign-On for Cisco Prime Collaboration

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

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

- Prime Collaboration Provisioning is configured to use Secure Socket Layer (SSL). SSL needs to be enabled before you enable SSO for Provisioning. For the steps to enable SSL in Prime Collaboration Provisioning, see section "**Enabling SSL for Prime Collaboration Provisioning**" in the Cisco Prime Collaboration Provisioning Guide.

Note By default, SSL is enabled in Prime Collaboration Assurance application.

- 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 11.0(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.

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 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 Prime Collaboration 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 server while enabling SSO, we recommend you to close the browser and re-launch the Cisco Prime Collaboration application. Because, though your conference expires in Cisco Prime Collaboration server, the IdP server conference might still be active.
- While enabling SSO, ensure that the hostname for Cisco Prime Collaboration 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>/ssosp/local/login.
- Disable Single Sign-On from CMD Utility.

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

- 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 By default, the recovery URL is enabled. If you want to disable it for security reasons, set it as False.