Cisco Prime Collaboration 9.5
Administration Guide

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Text Part Number: OL-28712-01
CONTENTS

Preface v
Audience v
Related Documentation v
Obtaining Documentation and Submitting a Service Request v

CHAPTER 1
Introduction to Prime Collaboration 1-1
Prime Collaboration Assurance 1-1
Voice and Video Unified Dashboard 1-1
Device Inventory Management 1-2
Voice and Video Endpoint Monitoring 1-2
Diagnostics 1-3
Fault Management 1-4
Reports 1-4
Prime Collaboration Provisioning 1-5

CHAPTER 2
Managing Licenses 2-1
Adding and Deleting a License File 2-3

CHAPTER 3
Integrating Prime Collaboration Servers 3-1
Network Diagnostics with NAM and LMS 3-2

CHAPTER 4
Configuring System Parameters 4-1
Configuring Dashlet Label and SMTP Server 4-2
Log Levels 4-2
Configuring Prime Collaboration Assurance Server Time Zone 4-2

CHAPTER 5
Managing Users 5-1
User Roles and Tasks 5-4
Adding, Editing, and Deleting a User 5-8
Configuring an LDAP Server 5-10
Resetting and Changing Passwords 5-12
Preface

This guide is one of multiple short guides for Cisco Prime Collaboration 9.5 that are used in sequence to install, set up, administer, and manage Prime Collaboration.

After you install the Prime Collaboration applications, use this guide to:

• Set up the Prime Collaboration server with user credentials and license files.
• Integrate Cisco Prime Assurance and Cisco Prime Provisioning, if you have purchased them.
• Perform maintenance tasks, such as backup and restore.
• Configure the log files for troubleshooting.

Audience

This guide is for voice and video engineers who are responsible for the configuration, provisioning, inventory, and maintenance of infrastructure-based, real-time collaboration services such as video (TelePresence) and telephony (VoIP), including endpoints, management servers, and service-specific network devices.

Prime Collaboration is deployed on a virtual server. The user must be familiar with virtual server configuration and with UNIX commands using the CLI.

Related Documentation

This guide is one of multiple short guides for Cisco Prime Collaboration 9.5. To perform other Prime Collaboration tasks, such as user management, device management, voice provisioning, network monitoring, and fault management, see Cisco Prime Collaboration 9.5 Documentation Overview for a list of all available documents.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

Subscribe to the *What’s New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.
Introduction to Prime Collaboration

Cisco Prime Collaboration is a comprehensive video and voice assurance and management system with a set of monitoring, troubleshooting, and reporting capabilities that help ensure end users receive a consistent, high-quality video and voice collaboration experience.

Prime Collaboration:

- Provides provisioning, monitoring, diagnostics, and reporting capabilities for Unified Communications Systems.
- Supports timely, end-to-end visibility and isolates voice and video-related issues for sessions (calls), endpoints, and the network.
- Reduces time to troubleshoot and recover from service-affecting problems.
- Provides detailed analysis of the media (voice and video) path with critical fault and performance statistics that enable you to isolate network devices that cause service degradation.
- Validates large-scale deployments through comprehensive inventory, health, and status of Cisco Collaboration systems, as well as service and network infrastructure devices.
- Delivers reports that allow operators to track usage and problem history.

Prime Collaboration is delivered in two different software packages, Prime Collaboration Assurance and Prime Collaboration Provisioning, which must be deployed on two different virtual servers.

Prime Collaboration Assurance

Prime Collaboration Assurance enables you to monitor your network and perform diagnostics. In addition, you can run reports that help you identify the source of problems.

Voice and Video Unified Dashboard

The Prime Collaboration dashboards enable end-to-end monitoring of your voice and video collaboration network. They provide quick summaries of the following:

- End-User Impact: Phone status; locations with poor voice quality and call failures; TelePresence endpoints with alarms and call quality events; in-progress video sessions with alarms.
Prime Collaboration Assurance

- Endpoint Utilization: Top 10 most and least utilized endpoints; number of TelePresence sessions for one day, one week, and four weeks.
- Infrastructure: Health and status of management devices, conferencing devices, and call and session control devices. You can also view the number of infrastructure devices, with and without alarms, utilized video ports, and trunks.

See *Cisco Prime Collaboration 9.5 Assurance Guide* to learn how the dashlets are populated after deploying the Prime Collaboration servers.

Device Inventory Management

You can discover and manage all endpoints that are registered to Cisco Unified Communications Manager (phones and TelePresence), Cisco VCS (TelePresence), CTS-Manager (TelePresence) and Cisco TMS (TelePresence). In addition to managing the endpoints, you can also manage multipoint switches, application managers, call processors, routers, and switches that are part of your video collaboration network.

As part of the discovery, the device interface and peripheral details are also retrieved and stored in the Prime Collaboration database.

If you are using the Cisco Unified Management solution, you can import the managed devices from the Cisco Prime Unified Operations Manager.

After the discovery is complete, you can perform the following device management tasks:
- Group devices into predefined and user-defined groups.
- Edit visibility settings for managed devices.
- Customize event settings for devices.
- Rediscover devices.
- Update inventory for managed devices.
- Suspend and resume the management of a managed device.
- Add or remove devices from a group.
- Manage device access credentials.
- Export managed devices.

See *Cisco Prime Collaboration 9.5 Assurance Guide* to learn how to collect manage the endpoints inventory data.

Voice and Video Endpoint Monitoring

Service operators need to quickly isolate the source of any service degradation in the network for all voice and video sessions in an enterprise. Prime Collaboration provides a detailed analysis of the end-to-end media path, including specifics about endpoints, service infrastructure, and network-related issues.

For video endpoints, Prime Collaboration enables you to monitor all point-to-point, multisite, and multipoint video collaboration sessions. These sessions can be ad hoc, static, or scheduled with one of the following statuses:
- In-progress
- Scheduled
Prime Collaboration periodically imports information from:

- The management applications (CTS-Manager and Cisco TMS) and conferencing devices (CTMS, Cisco MCU, and Cisco TS) on the scheduled sessions.
- The call and session control devices (Cisco Unified CM and Cisco VCS) shown on the registration and call status of the endpoints.

For voice endpoints, Prime Collaboration provides the current operational status of the Cisco Unified Communications system. The Unified Communications (UC) Topology View displays a logical, top-level view of the IP telephony implementations. This logical view focuses on call control relationships.

The UC Topology View shows Cisco Unified Communications Manager (Unified CM) and Unity Connection clusters, devices, route groups, and route lists in the cluster. The relationships are displayed in a graphical view.

You can use the UC Topology View to:

- Display a logical or neighbor UC Topology View of your IP telephony deployment.
- Search for phones and view a summary of the IP Communications devices displayed in the UC Topology View.
- View and act on device events.
- Run other Cisco Prime Collaboration tools.
- Launch administration pages for devices.
- Open a separate window using the Detach option to view maps at the cluster level.

In addition, Prime Collaboration continuously monitors active calls supported by the Cisco Unified Communications system and provides near real-time notification when the voice quality of a call fails to meet a user-defined quality threshold. Prime Collaboration also allows you to perform call classification based on a local dial plan.

See Cisco Prime Collaboration 9.5 Assurance Guide to understand how to monitor IP Phones and TelePresence.

**Diagnostics**

Prime Collaboration uses Cisco Medianet technology to identify and isolate video issues. It provides media path computation, statistics collection, and synthetic traffic generation.

When network devices are medianet-enabled, Prime Collaboration provides:

- Flow-related information along the video path using Mediatrace.
- Snapshot views of all traffic at network hot spots using Performance Monitor.
- The ability to initiate synthetic video traffic from network devices using the IP Service Level Agreement (IP SLA) and Video Service Level Agreement Agent (VSAA) to assess video performance on a network.

In addition, for IP phones, Prime Collaboration uses the IP SLA to monitor the reachability of key phones in the network. A phone status test consists of:

- A list of IP phones to test.
• A configurable test schedule.
• IP SLA-based pings from an IP SLA-capable device (for example, a switch, a router, or a voice router) to the IP phones. Optionally, it also pings from the Prime Collaboration server to IP phones.

See *Cisco Prime Collaboration 9.5 Assurance Guide* to learn how to troubleshoot the video and voice network.

### Fault Management

Prime Collaboration ensures near real-time quick and accurate fault detection. After identifying an event, Prime Collaboration groups it with related events and performs fault analysis to determine the root cause of the fault.

Prime Collaboration allows you to monitor the events that are of importance to you. You can customize the event severity and enable severity-based notifications from Prime Collaboration.

Prime Collaboration generates traps for alarms and events and sends notifications to the trap receiver. The traps are converted into SNMPv2c notifications and are formatted according to the `CISCO-EPM-NOTIFICATION-MIB`.

See *Cisco Prime Collaboration 9.5 Assurance Guide* to learn how Prime Collaboration monitors faults.

### Reports

Prime Collaboration provides the following predefined reports and customizable reports:

• **Inventory Reports**—Provide IP phone, audio phone, video phone, SRST phone, audio SIP phone, and IP Communicator inventory details. Inventory reports also provide information about CTI applications, ATA devices, and the Cisco 1040 Sensor.

• **Call Quality Event History Reports**—Provide the history of call quality events. Event History reports can display information for both devices and clusters. You can use Event History to generate customized reports of specific events, specific dates, and specific device groups.

• **Call Quality Reports**—Enable you to examine voice transmission quality in the parts of your network that Prime Collaboration has monitored. The reports show the times when Mean Opinion Score (MOS) has been below configured thresholds, the codec in use, and the endpoints on which violations have occurred.

• **TelePresence Reports**—Provide details on completed and in-progress sessions, endpoint utilization, and No Show endpoints. TelePresence reports also provide a list of conferencing devices and their average and peak utilization in your network.

• **Activity Reports**—Provide information about IP phones and video phones that have undergone a status change during the previous 1 to 30 days.

See *Cisco Prime Collaboration 9.5 Assurance Guide* to learn the different types of reports and how to generate them.
Prime Collaboration Provisioning

Prime Collaboration Provisioning provides provisioning support for Cisco Unified Communications initial deployments and implementations, with automated processes for initial deployment and Day 2 additions and changes. It also provides ongoing operational provisioning and activation services for individual subscriber changes.

Prime Collaboration Provisioning enables you to do the following:

- Order standard services (for example a phone, line, or voicemail) for a subscriber.
- Create an order for a subscriber-level change (to a phone, a line, and so on) or an IP communications-level infrastructure change (such as provisioning a new calling search space or route pattern). All orders in the system are tracked and viewable, both across orders and by subscriber name or ID. The order records show who initiated the order, the times of various process steps, and what the order contained.
- Delegate the order management capability so that requests for service additions, changes, or deletions can be made without underlying knowledge of the voice applications that deliver those services.

See *Cisco Prime Collaboration 9.5 Provisioning Guide* to learn how to provision the Cisco Unified Communications applications.
Managing Licenses

Prime Collaboration licensing secures and enables the features and endpoint quantities for Prime Collaboration Assurance and Prime Collaboration Provisioning. You can view the already installed license details of both Prime Collaboration Assurance and Prime Collaboration Provisioning (or either one, for a standalone application) by navigating to Administration > License Management.

Prime Collaboration Assurance Licensing

Prime Collaboration Assurance licensing is based on the endpoint type and quantity. The type of an endpoint determines which licenses you need, and the quantity of the endpoints determines the tier and quantity of licenses that you need to purchase to manage your network.

Prime Collaboration Assurance provides the following license categories:

- High-end, single-codec endpoint
- High-end, multi-codec endpoint
- Midrange endpoint
- Mass endpoint

To learn the endpoint types that are mapped to each of these licenses, see the Cisco Prime Collaboration 9.5 Quick Start Guide. You can also view a list of endpoint types from the Prime Collaboration Assurance UI (Administration > License Management > Show Endpoints icon on the License Management page).

Prime Collaboration Analytics Licensing

Prime Collaboration Analytics license must be applied only after deploying the assurance license. Analytics licensing should be greater than or equal to the sum of the total assurance count. For example, if the assurance license count is 50 for each of the above listed license categories, the license count in analytics must be greater than or equal to 200.

Note

In evaluation mode, the Analytics license will be the same as that of assurance.
Prime Collaboration Provisioning Licensing

Prime Collaboration Provisioning licensing is modeled on feature-based licensing and endpoint-based licensing (in Prime Collaboration Provisioning, endpoints means phones). Prime Collaboration Provisioning licenses include a set of features that are made available for the user upon purchase. In addition, Prime Collaboration Provisioning provides licenses in terms of Image license and scale license for endpoints.

The Prime Collaboration Provisioning Northbound Interface (NBI) feature is optional, so to use this feature, you must have the appropriate license.

The image license file for Prime Collaboration Provisioning is mandatory if you wish to activate the application in the production network. Scale licenses are cumulative; you can combine licenses to increase the number of phones you support.

License Count

For Prime Collaboration Assurance, the license count is updated after a discovery task is performed. For example, for endpoints in the Managed state, a license count based on endpoint type is updated approximately 5 minutes after discovery is completed. A device in any state other than Managed or Suspended is not counted.

Clicking the Show Endpoints icon in the Prime Collaboration Assurance License Status pane displays a list of endpoints and the license category to which they belong.

Note

If the number of endpoints exceeds the license count, endpoints are randomly managed in the Prime Collaboration Assurance server.

For details on how devices are discovered and managed, see Cisco Prime Collaboration 9.5 Assurance Guide. Endpoints that are not added are listed in the discovery job.

If a number of phones have the same IP address, they are counted as a single endpoint, and only one license unit is used.

For a Prime Collaboration Provisioning scale license, the license count is updated based on the number of phones (MAC addresses) that are ordered and synchronized with the Unified CM.

Prime Collaboration Provisioning also displays the user license limit and the number of user licenses that are currently being used. If the number of users exceeds the maximum allowable limit, a warning message stating that the maximum number of users has been exceeded is displayed.

Phone Count in Prime Collaboration Assurance

Prime Collaboration Assurance follows several rules to help determine the number of license units required.

- If an IP phone shares the same phone number as a softphone, Prime Collaboration Assurance counts this pair as a single phone and thus one license unit.
- Mobile phones are counted separately.
- Analog phones connected to a voice gateway are not counted.

The Enterprise License Manager dashlet (in the Infrastructure dashboard) displays the license usage for all collaboration applications. The VCS License Usage dashlet provides information about Video Communication Server license usage. For more information about these dashlets, see the “Prime Collaboration Dashboards” chapter in Cisco Prime Collaboration 9.5 Assurance Guide.
Phone Count in Prime Collaboration Provisioning

Provisioning manages each endpoint separately; regardless of the number of lines or DN's it uses. Every single endpoint is counted for licensing even if two endpoints are shared. Provisioning runs license entitlement every minute and calculates the number of endpoints and the entitlement. It decides if it can allow more endpoints to be managed based on the licenses available in the license directory.

If you add endpoints directly through Cisco Unity CM interface, they will not show up in Provisioning. When you synchronize Cisco Unity CM, if the number of endpoints exceeds the licensing limit, synchronization will fail and the additional endpoints will be ignored. You cannot predict which ones will be left unmanaged as this is determined by Cisco Unity CM and not Provisioning.

The following phones are counted from the Provisioning database:

- IP phones (Cisco or third-party phones attached to Cisco Unified Communications Manager or Cisco Unified Communications Manager Express)
- Soft phones, Client Service Framework (CSF), or Jabber, with or without an IP phone shared
- Dual-mode phones or Cius
- Video or TelePresence endpoints
- Video or TelePresence endpoints
- Active analog ports in the ATA-186, ATA-187, or VG224 family

CTI port and EM access (device profile) are not counted.

Adding and Deleting a License File

In the License Management page (Administration > License Management), you can view the following information:

- Type of license or active image license installed—Evaluation or Image.
- Total number of licenses allowed for the license categories and the number of licenses used currently. For more details, see License Count, page 2-2.
- Expiration date—Date when the license expires. This value is applicable to the evaluation license only.
- Northbound interface licenses and northbound interface expiration date- for Prime Collaboration Provisioning application.

You must review the Cisco Prime Collaboration 9.5 Quick Start Guide to learn how to register and obtain the license file for Prime Collaboration.

Note

The image license files for Prime Collaboration Assurance and Prime Collaboration Provisioning are mandatory if you wish to activate these applications in the production network. You can add any number of scale licenses, however, the image license file is added once and added separately for Prime Collaboration Assurance and Prime Collaboration Provisioning.

To add the license file in Standalone or Converged Assurance:

Step 1 Choose Administration > License Management.
Step 2 In the License Management page, under License Files, click Add.
Step 3 In the Add License File window, choose the license type: Assurance or Provisioning.
Step 4 Upload the license file and click OK.
For the steps to add the license file in Standalone Provisioning, see *Cisco Prime Collaboration 9.5 Provisioning Guide*.

**Note**
To delete a license file, choose Administration > License Management. In the License Management page, select the license file and click **Delete**.

**Note**
When you upgrade from evaluation mode to production, perform a rediscovery of devices. For details on rediscovering devices, see *Cisco Prime Collaboration 9.5 Assurance Guide*.

The newly added license file information appears in the License Status pane of either Prime Collaboration Assurance or Prime Collaboration Provisioning based on the license type you have chosen.
Integrating Prime Collaboration Servers

Prime Collaboration provides the capability to integrate Prime Collaboration Provisioning with Prime Collaboration Assurance and configure Prime Collaboration Provisioning from Prime Collaboration Assurance. Integrating the two enables you to leverage the capabilities of both to monitor voice and video endpoints and provision Unified Communications Systems. You can also detach Prime Collaboration Provisioning from Prime Collaboration Assurance using the Prime Collaboration Assurance UI.

At Administration > System Setup > Assurance Setup > Cisco Prime 360 Integration, under Prime Collaboration Provisioning Server Setup, specify the IP address of the Provisioning application you want to attach to or detach.

You must provide the IP address of the Provisioning application server (and not the database server) while integrating Prime Collaboration Provisioning with Prime Collaboration Assurance. After you attach the Prime Collaboration Provisioning application to Prime Collaboration Assurance, you must refresh the UI for the converged UI to appear.

Note

The port used for Prime Collaboration Assurance is 26; for Prime Collaboration Provisioning it is 22.

In the converged mode, before you restart or shut down the Prime Collaboration Provisioning application, be sure to detach it from Prime Collaboration Assurance and converge it after the restart process.

When you launch the converged application through Microsoft IE 8.0, the following message is displayed, as Prime Collaboration Assurance communication is in https and Prime Collaboration Provisioning communication is in http by default: ‘Do you want to view only the webpage content that was delivered securely.’

- If you select No from the popup dialog box, the appropriate data is displayed on all Prime Collaboration Provisioning pages.
- If you select Yes from the popup dialog box, data is not displayed on all Prime Collaboration Provisioning pages.

However, with Microsoft IE 9.0, the security warning is not displayed and the appropriate data is displayed on all of the Prime Collaboration Provisioning pages.

You can also test the connectivity to the Prime Collaboration Provisioning server or change the IP address by clicking Test Connectivity.

In the converged mode, the Prime Collaboration Provisioning UI is converged with Prime Collaboration Assurance, and the Provisioning IP address is redirected to Prime Collaboration Assurance even though you log in to Prime Collaboration Provisioning application.
In converged mode, if you try to access Provisioning server when the Assurance server is shutdown, the Provisioning server must launch standalone Provisioning successfully. Restart Provisioning services and clear browser cache if you are unable to launch standalone Provisioning.

When you dissociate Prime Collaboration Provisioning from Prime Collaboration Assurance, the user roles that were applicable for Prime Collaboration Provisioning and Prime Collaboration Assurance in the converged mode also apply for the standalone applications.

**Network Diagnostics with NAM and LMS**

You can perform network diagnosis using Cisco Prime Network Analysis Module (NAM) and Cisco Prime LAN Management Solutions (LMS). While performing the troubleshooting for a session, you can cross-launch these applications to further analyze problems on the network devices that are connected between endpoints.

To launch either the Prime NAM or Prime LMS features for a particular device while troubleshooting, you must ensure that the device is managed in those applications and in Prime Collaboration.

For more details on these applications, see “Cross-Launching NMS Applications” in *Cisco Prime Collaboration 9.5 Assurance Guide*. 
Configuring System Parameters

Prime Collaboration allows you to configure system parameters for both Prime Collaboration Assurance and Prime Collaboration Provisioning. The following are the system configuration parameters for Assurance. To configure Prime Collaboration Provisioning system parameters, see Cisco Prime Collaboration 9.5 Provisioning Guide.

To configure the following Prime Collaboration Assurance system parameters, navigate to Administration > System Setup > Assurance Setup:

- Dashlet Label and SMTP Server—To configure these parameters under General Settings, see Configuring Dashlet Label and SMTP Server, page 4-2.
- CDR Trunk Utilization Settings—Allows you to configure the maximum capacity for trunks and gateways. You can either configure the maximum capacity for a particular trunk or gateway, or you can use a CSV file to import trunk utilization configuration data for all clusters. To configure this parameter, see Cisco Prime Collaboration 9.5 Assurance Guide.
- Call Quality Data Source Management—Prime Collaboration monitors voice-quality measurements in a VoIP network. This real-time, service-quality information is collected from Unified CM and Cisco NAM. To configure this parameter, see Cisco Prime Collaboration 9.5 Assurance Guide.
- LDAP Settings—To configure this parameter, see Configuring an LDAP Server, page 5-10.
- Log Settings—To configure this parameter, see Log Levels, page 4-2.
- Configuring Time Zone—To configure this parameter, see Configuring Prime Collaboration Assurance Server Time Zone, page 4-2.
- SFTP Settings—For Prime Collaboration to display phones in SRST mode and generate related events, you must configure SRST poll settings, identifying the SRST components for Prime Collaboration to test. To configure this parameter, see ‘Configuring SFTP Settings’ in Cisco Prime Collaboration 9.5 Assurance Guide.
- IP Phone Inventory Collection Settings—You can use the Phone XML Collection to schedule the phone discovery. To configure this parameter, see Cisco Prime Collaboration 9.5 Assurance Guide.
- IP Phone XML Inventory Collection Settings—To configure this parameter, see Cisco Prime Collaboration 9.5 Assurance Guide.
- Cluster Data Discovery Settings—Allows Prime Collaboration to consolidate the inventory and the device registration information it collects from Unified CMs. To configure this parameter, see Cisco Prime Collaboration 9.5 Assurance Guide.
Chapter 4 Configuring System Parameters

Configuring Dashlet Label and SMTP Server

You can shorten the endpoint or device names displayed in the Prime Collaboration dashboard using the Dashlet Label Prefix Removal Setup parameter. This is applicable only if you have used a common prefix across endpoints and devices.

To configure this parameter, specify the prefix strings separated by a semicolon (;). All special characters are supported except for the semicolon. A prefix can contain blank spaces.

You can also configure the SMTP server to send and receive e-mail notifications for alarms by specifying the SMTP server name and the sender AAA e-mail address. The value in the sender AAA E-mail address field helps you to identify the server you receive the e-mail from if there are many servers.

Log Levels

Prime Collaboration supports the following log levels:

- **Debug**—Helps you to debug the application.
- **Error**—Indicates that the application can still continue to run.
- **Information**—Indicates the progress of the application.
- **Warning**—Indicates potentially harmful situations.
- **Fatal**—Indicates critical logs.

You can set the log levels for the following features:

- Fault management—For fault management-related issues.
- Performance monitor—For performance statistics-related issues.
- Server diagnostics—For Prime Collaboration Assurance server-related issues.
- Discovery, session monitoring and others—For discovery, session management, and web server-related issues.

The log level settings can be changed from the Log Settings page (Administration > System Setup > Assurance Setup > Log Settings).

Do not change the log level settings without assistance from the Cisco Technical Assistance Center (TAC) team. The log files are also included in the backup file.

Configuring Prime Collaboration Assurance Server Time Zone

To configure the Prime Collaboration Assurance server time zone:

**Step 1**
Log into the Prime Collaboration Assurance server with the account that you have created during installation. By default, it is `admin`.

**Step 2**
Enter the following command to see the list of supported time zones:
```
cm/admin# show timezones
```

**Step 3**
Enter the following commands to set the time zone for the Prime Collaboration Assurance server:
```
cm/admin(config)# config t
cm/admin(config)# clock timezone US/Pacific
```
Step 4 Enter the following command to copy running-configuration to startup-configuration:

```
cm/admin# write memory
```

Step 5 Enter the following command to restart the Prime Collaboration Assurance server:

```
cm/admin# application stop cpcm
show application status cpcm
cm/admin# application start cpcm
```

Step 6 Wait for 10 minutes for the server to finish the restart process and enter the following command to check if the time zone is set to the new value:

```
cm/admin# show timezone
US/Pacific
```

To configure the time zones in Prime Collaboration Provisioning, see ‘Changing Time Zone Settings’ in the Cisco Prime Collaboration 9.5 Provisioning Guide.
Managing Users

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

Prime Collaboration Assurance User Roles

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

A user can be assigned one of the following roles:

- **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 network data collection. Cannot perform any Device Work Center operations such as adding, discovering, or importing devices. Also, an operator will not be able to 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 system 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 Prime Collaboration.

Prime Collaboration Provisioning User Roles

Two types of global Provisioning user roles are available: global and domain specific.

The global Provisioning user is typically an IP telephony expert who configures Prime Collaboration Provisioning business abstractions for voice applications. In Provisioning, the domain-specific user can be an administrator for a single domain and a user for multiple domains or for a single domain.

The user roles for Prime Collaboration Provisioning are explained in Table 5-1:

<table>
<thead>
<tr>
<th>Authorization Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Administration</td>
<td>Has access to all Prime Collaboration Provisioning functionality.</td>
</tr>
</tbody>
</table>
### Table 5-1 Authorization Roles (continued)

<table>
<thead>
<tr>
<th>Authorization Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance</td>
<td>Authorized to configure system cleanup activities. For more information, see “Setting up the Server” in the <em>Cisco Prime Collaboration 9.5 Provisioning Guide</em>.</td>
</tr>
</tbody>
</table>

**Roles for Domain**

In the drop-down list, select the Domain for which you are setting the authorization roles. The selected roles only apply to the selected Domain.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Authorized to view phone button templates, modify subscriber roles, and add or update phone inventory.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure Configuration Management</td>
<td>Authorized to provision infrastructure configuration objects. When you select this role, you must also select a profile from the Permission Profile box.</td>
</tr>
<tr>
<td>Permission Profiles</td>
<td>Sets the permissions for which infrastructure configuration object users assigned this authorization role can configure. For information on setting permissions, see “Managing Infrastructure Configuration Permissions” in the <em>Cisco Prime Collaboration 9.5 Provisioning Guide</em>.</td>
</tr>
<tr>
<td>SelfCare User</td>
<td>Authorized to manage his own services; set up lines, manage services, and configure phone options quickly and easily.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> In a Prime Collaboration Provisioning standalone system, you can enable or disable Self-Care while adding subscribers and users. In the converged mode, you can enable Self-Care while adding subscribers only. The Self-Care check box is not available while adding users. However, after creating a user, you can assign the Self-Care role from the Manage Subscriber page. See “Creating a Self-Care Account” in the <em>Cisco Prime Collaboration 9.5 Provisioning Guide</em>.</td>
</tr>
</tbody>
</table>

**Ordering Roles**

Users assigned these roles are allowed to place orders for other subscribers and themselves.

<table>
<thead>
<tr>
<th>Ordering</th>
<th>Authorized to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Add, delete, or update a subscriber within a Domain.</td>
</tr>
<tr>
<td></td>
<td>• Add, delete, or update a subscriber role within a Domain (if the rule for that Domain permits it).</td>
</tr>
<tr>
<td></td>
<td>• Add, delete, or update phones in the inventory within a Domain (if the rule for that Domain permits it).</td>
</tr>
<tr>
<td></td>
<td>• Search and view detailed subscriber information within a Domain.</td>
</tr>
<tr>
<td></td>
<td>• Place an order for a subscriber within a Domain.</td>
</tr>
<tr>
<td>Advanced Ordering</td>
<td>Authorized to access all the functionality specified by the Ordering role; can also access Advanced Order Options in the Order Entry page.</td>
</tr>
<tr>
<td>Advanced Assignment</td>
<td>Authorized to access all the functionality specified by the Ordering role, and to assign the MAC address for a phone product at the time of order entry.</td>
</tr>
</tbody>
</table>
Note

- globaladmin and domain admin can create Self-Care roles for any user. Self-Care role can be assigned to a user from the Manage Users page in the standalone Prime Collaboration Provisioning only. For more information, see “Creating a Self-Care Account” in the *Cisco Prime Collaboration 9.5 Provisioning Guide*.

- In the converged mode, you cannot import a user associated with a Self-Care role into the Prime Collaboration Assurance application.

The “Managing Subscribers and Users” chapter in *Cisco Prime Collaboration 9.5 Provisioning Guide* provides detailed information on how to manage users.

**Single Sign-On for Prime Collaboration**

Prime Collaboration provides the facility to login from the Prime Collaboration Assurance application to Prime Collaboration Provisioning application using the Single Sign-On feature.

In the converged mode, the Prime Collaboration Provisioning application uses the same password for authentication as is used for the Prime Collaboration Assurance application.

**Default User Accounts**

Prime Collaboration is preconfigured with a default web client administrator user called globaladmin; globaladmin is a superuser who can access both the Prime Collaboration Assurance and Prime Collaboration Provisioning UIs.

Specify a password for globaladmin when you configure your virtual appliance (for either stand-alone products or converged application). You need to use these credentials when you launch the Prime Collaboration web client for the first time.

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

You cannot create CLI users using the web client UI. 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.

We recommend that you write down the root password as it cannot be retrieved.

---

**Table 5-1 Authorization Roles (continued)**

<table>
<thead>
<tr>
<th>Authorization Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activity Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Approval</td>
<td>Authorized to accept and complete the approval for orders.</td>
</tr>
<tr>
<td>Assignment</td>
<td>Authorized to accept the user activity for assigning the MAC address.</td>
</tr>
<tr>
<td>Shipping</td>
<td>Authorized to accept and complete shipping of orders.</td>
</tr>
<tr>
<td>Receiving</td>
<td>Authorized to accept and complete receiving of orders.</td>
</tr>
</tbody>
</table>
Chapter 5      Managing Users

User Roles and Tasks

Table 5-2 lists the Prime Collaboration Assurance user roles and tasks they are mapped to.

Note that Super administrator has access to all of the UI menus and can perform all tasks listed in the table below. Thus, the super administrator is not listed in the following table.

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Task</th>
<th>System Administrator</th>
<th>Network Administrator</th>
<th>Operator</th>
<th>Helpdesk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
<td>View Video and Voice Collaboration Dashlets</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Customize Dashlets</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Launch Alarm Browser</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Launch Alarm Summary</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Operate&gt; Diagnose</td>
<td>Monitor Sessions</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Diagnose&gt; Sessions</td>
<td>Import Sessions</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Launch 360° Session View</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>From 360° Session View: Add to watch list</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>From 360° Session View: See alarms</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>From 360° Session View: Monitor Endpoint</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>From 360° Session View: Troubleshoot session or export troubleshoot data</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>From topology view (endpoints): Add to watch list or remove from watch list</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>From topology view (endpoints): See alarms</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>From topology view (endpoints): Monitor Endpoint</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>From topology view (network connection): Troubleshoot network link</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
### Table 5-2  Prime Collaboration Assurance User Roles and Task Mapping  (continued)

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Task</th>
<th>System Administrator</th>
<th>Network Administrator</th>
<th>Operator</th>
<th>Helpdesk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operate &gt; Diagnose &gt; Endpoint Diagnostics</td>
<td>Monitor endpoint</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Launch quick view</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>From quick view: Add to watch list or remove from watch list</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>From quick view: See alarms</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>From quick view: Monitor Session</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Operate &gt; Diagnose &gt; Diagnostics Summary</td>
<td>View Diagnostics Summary</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Operate &gt; Diagnose &gt; IP-SLA Diagnostics</td>
<td>Start a troubleshooting session</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Operate &gt; Diagnose &gt; Media Path Analysis</td>
<td>Start Media Path Analysis</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Operate &gt; Alarms &amp; Events &gt; Alarms</td>
<td>View Alarms</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Change Status</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Assign an Alarm</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Add an annotation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Email Notification</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Launch quick view</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>From quick view: Monitor Endpoint</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>From quick view: See Event History</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Operate &gt; Alarms &amp; Events &gt; Events</td>
<td>View Events</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Operate &gt; Device Work Center</td>
<td>Manage credentials</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Discover devices</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Update Inventory</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Manage Clusters</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Import Inventory</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Export Inventory</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Discover jobs</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Edit Visibility (Edit button)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Customize Events</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Suspend device management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Resume device management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Adding to Group</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Remove from Group</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
### Table 5-2 Prime Collaboration Assurance User Roles and Task Mapping (continued)

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Task</th>
<th>System Administrator</th>
<th>Network Administrator</th>
<th>Operator</th>
<th>Helpdesk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operate &gt; UC Topology View</td>
<td>View voice dashlets/summary</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Reports &gt;</td>
<td>Generate reports</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (excluding Administrative Reports)</td>
</tr>
<tr>
<td>Reports &gt;</td>
<td>Interactive Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reports &gt;</td>
<td>Static Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reports &gt;</td>
<td>Administrative Reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration &gt; Job Management</td>
<td>Manage jobs</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; Job Management</td>
<td>Schedule jobs</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; Job Management</td>
<td>Cancel jobs</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; User Management</td>
<td>View users</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; User Management</td>
<td>Add users</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; User Management</td>
<td>Edit users</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; User Management</td>
<td>Delete users</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; User Management</td>
<td>Reset password</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; User Management</td>
<td>Change password</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Administration &gt; License Management</td>
<td>View license details</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; License Management</td>
<td>Add license</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; License Management</td>
<td>Delete license</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; System Setup &gt; Assurance Setup</td>
<td>Configure all system parameters (General Settings, Cisco Prime 360 Integration, CDR Trunk Utilization settings, Call Quality Data Source Management, LDAP Settings, Log Settings, SFTP Settings, IP Phone Inventory Collection Settings, IP Phone XML Inventory Collection Settings, Cluster Data Discovery Settings)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; Alarm &amp; Event Configuration &gt; Event Customization</td>
<td>Customizing event monitoring and severity. Also, defining the threshold value for automatic troubleshooting.</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Table 5-3 lists the Prime Collaboration Provisioning user roles and the tasks they are mapped to. The domain roles that perform a specific task has been mentioned. The Administration user role can perform all of the Prime Collaboration Provisioning tasks while the Domain specific admins will have only restricted access to some of the pages.

### Table 5-3  Prime Collaboration Provisioning User Roles and Task Mapping

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Task</th>
<th>Domain Roles</th>
<th>Global Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home &gt; Provisioning &gt; Unified Provisioning Manager Capacity</td>
<td>View information on how much licenses that you have used from the available set.</td>
<td>No Access</td>
<td>Administration</td>
</tr>
<tr>
<td>Home &gt; Provisioning &gt; Pending Order Status</td>
<td>View pending orders</td>
<td>Ordering, advanced ordering, advanced assignment, policy, infra Config Management, assignment, approval, shipping, receiving</td>
<td>Administration</td>
</tr>
<tr>
<td>Home &gt; Provisioning &gt; Device Sync Status</td>
<td>View device sync status</td>
<td>Ordering, advanced ordering, advanced assignment</td>
<td>Administration</td>
</tr>
<tr>
<td>Home &gt; Provisioning &gt; Deployment Details</td>
<td>View deployment details</td>
<td>Ordering, advanced ordering, advanced assignment</td>
<td>Administration</td>
</tr>
<tr>
<td>Home &gt; Provisioning &gt; Locked Users</td>
<td>View locked users- users locked after a specified number of failed login attempts</td>
<td>No Access</td>
<td>Administration</td>
</tr>
<tr>
<td>Home &gt; Provisioning &gt; Logged In Users</td>
<td>View users who are logged in to the application</td>
<td>No Access</td>
<td>Administration</td>
</tr>
<tr>
<td>Design &gt; Set Up Devices</td>
<td>Set up devices, Call Processors, Unified Message Processors, Unified Presence Processors, AAA servers</td>
<td>No Access</td>
<td>Administration</td>
</tr>
<tr>
<td>Design &gt; Set Up Deployment</td>
<td>Create Domains, Service Areas, Provisioning Template, Quick Site Builder</td>
<td>No Access</td>
<td>Administration</td>
</tr>
<tr>
<td>Design &gt; Set Up Deployment</td>
<td>Create Subscriber Roles</td>
<td>Policy</td>
<td>Administration</td>
</tr>
<tr>
<td>Deploy &gt; Subscriber Management</td>
<td>Add Subscriber, Search Subscriber</td>
<td>Ordering, advanced Ordering, advanced Assignment</td>
<td>Administration</td>
</tr>
<tr>
<td>Deploy &gt; Order Management</td>
<td>Manage activities for a group and user.</td>
<td>No Access</td>
<td>Administration</td>
</tr>
<tr>
<td>Deploy &gt; Order Management</td>
<td>Search order</td>
<td>Ordering, advanced Ordering, advanced Assignment</td>
<td>Administration</td>
</tr>
<tr>
<td>Deploy &gt; Infrastructure Configuration</td>
<td>Configuring Infrastructure</td>
<td>infraConfigManagement</td>
<td>Administration</td>
</tr>
</tbody>
</table>
Adding, Editing, and Deleting a User

You can add a user via UI and assign predefined static roles. The user will have access to the Prime Collaboration web client only and not CLI.

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

You, as a globaladmin, must create other administrators using real user-IDs as they can be tracked in Audit Trail and in the Prime Collaboration Provisioning order tracking system.

Caution

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

When you integrate the Prime Collaboration Provisioning application with Prime Collaboration Assurance, you can import users with domain-specific and global Provisioning roles (who do not have Self-Care roles associated) to the Prime Collaboration Assurance application using the “Import” functionality in the Administration > User Management page. You must refresh the “User Management” page to see the list of imported users. For details on Self-Care roles, See “Using Self-Care” chapter in the Cisco Prime Collaboration 9.5 Provisioning Guide.

Note

You cannot import a Prime Collaboration Provisioning Self-Care user to the Prime Collaboration Assurance application.

You can then check the /opt/emms/emsam/log/importedprovisioninguser.log file, by logging in as a root user, to find the users who were not imported into Prime Collaboration Assurance database due to several reasons such as duplicate usernames (usernames already used in Prime Collaboration Assurance), usernames with no passwords and so on.

Table 5-3 Prime Collaboration Provisioning User Roles and Task Mapping (continued)

<table>
<thead>
<tr>
<th>Navigation</th>
<th>Task</th>
<th>Domain Roles</th>
<th>Global Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy &gt; Batch Provisioning</td>
<td>Perform batch provisioning</td>
<td>No Access</td>
<td>Administration</td>
</tr>
<tr>
<td>Deploy &gt; Provisioning Inventory</td>
<td>Manage Phones</td>
<td>Policy</td>
<td>Administration</td>
</tr>
<tr>
<td></td>
<td>Manage directory number, browse and search inventory</td>
<td>No Access</td>
<td>Administration</td>
</tr>
<tr>
<td>Report &gt; Interactive Reports &gt; Provisioning Reports</td>
<td>View Provisioning reports</td>
<td>No Access</td>
<td>Administration</td>
</tr>
<tr>
<td>Administration &gt; Provisioning Setup</td>
<td>Configure Phone Button Templates</td>
<td>Policy</td>
<td>Administration</td>
</tr>
<tr>
<td></td>
<td>Configure Provisioning Rules, Attributes, and data maintainance</td>
<td>No Access</td>
<td>Administration</td>
</tr>
<tr>
<td>Administration &gt; Notification Settings</td>
<td>Configure e-mail settings</td>
<td>No Access</td>
<td>Administration</td>
</tr>
</tbody>
</table>
However, when you integrate a freshly installed Prime Collaboration Provisioning application (that contains no user data) with the Prime Collaboration Assurance application, and you wish to create a common user for both Prime Collaboration Assurance and Prime Collaboration Provisioning, you must perform the following tasks as prerequisites:

- **Add Devices** - To learn how to create devices, see “Adding Devices to Provisioning” in the *Cisco Prime Collaboration 9.5 Provisioning Guide*.
- **Create Domains** - To learn how to create domains, see “Creating a Domain” in the *Cisco Prime Collaboration 9.5 Provisioning Guide*.

To add a user:

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

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

**Step 3** In the Add User window, enter the required user details. Note that because the LDAP server performs authentication, it should have the same user ID as Prime Collaboration. For more information, see **Configuring an LDAP Server, page 5-10**.

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

**Step 4** (Optional) If you have deployed the Managed Service Provider (MSP) version of Prime Collaboration, select a customer from the Customer drop-down list.

**Step 5** Select the appropriate Prime Collaboration Assurance roles. (If the Prime Collaboration Provisioning application is not integrated with the Prime Collaboration Assurance application, the Provisioning Domain and Provisioning Roles fields are not displayed when you perform the Add operation.)

**Step 6** If you wish to have only a Provisioning user, or a common user for Prime Collaboration Assurance and Prime Collaboration Provisioning, perform the following steps:

a. Select the appropriate roles in the Provisioning Roles check box.

b. Click **Add Row** under **Domain Specific** to create domain specific Provisioning Roles. You will see role settings option for General, Ordering and Activity roles. For information on authorization roles, see **Table 5-1: Authorization Roles, page 5-1**.

c. Enter required details and click **Done**

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

The users thus created via Add User feature are associated with the web client only and cannot log in to the Prime Collaboration Assurance or Prime Collaboration Provisioning server through the CLI.

**Note**


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 **Administration > User Management** and make the necessary changes.
As part of your regular system administration tasks, you sometimes must delete users from the Prime Collaboration database. However, you cannot delete the Prime Collaboration web client default administrator globaladmin.

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

# Configuring an LDAP Server

You can configure Prime Collaboration to connect to a Lightweight Directory Access Protocol (LDAP) server, to access user information stored in the LDAP server. In converged mode, the LDAP server specified in Prime Collaboration Assurance is used for authentication only; authorization and role-based access control (RBAC) functions are performed by Prime Collaboration.

You must create an LDAP user from the User Management page to enable the user to log in using LDAP credentials. See Adding, Editing, and Deleting a User, page 5-8 for more information.

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

To configure LDAP server:

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

**Step 2** In the LDAP Settings page, enter values for all fields (see Table 5-4 for the field descriptions).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server IP address</td>
<td>Enter the LDAP server name or IP address. Optionally enter the Backup LDAP server IP address.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Enter the Port number on which the LDAP requests for the server is received.</td>
</tr>
<tr>
<td></td>
<td>Non-secure port: 389</td>
</tr>
<tr>
<td></td>
<td>Secure SSL port: 636</td>
</tr>
<tr>
<td>Note</td>
<td>If Prime Collaboration must use SSL encryption, check the Use SSL check box.</td>
</tr>
<tr>
<td></td>
<td>Optionally enter the Backup LDAP server Port number.</td>
</tr>
<tr>
<td>Note</td>
<td>If the LDAP server is configured to use a non-standard port, that port should be entered here as well.</td>
</tr>
</tbody>
</table>
### Table 5-4 LDAP server Configuration (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Distinguished Name</td>
<td>Enter the username of the user who has access rights to the corresponding LDAP directory. For example, a user, John Doe, with userID = jdoe must enter John Doe.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If admin is a user in windows domain cisco, just enter admin (username with domain prefix such as cisco\admin will not work).</td>
</tr>
<tr>
<td>Admin Password</td>
<td>Enter the password for the LDAP server authentication and reconfirm the password.</td>
</tr>
<tr>
<td>LDAP User Search Base</td>
<td>Enter the user search base. LDAP server searches for users under this base. You must enter the CN or OU details when you enter the search base. Just dc=cisco,dc=com will not work; you must also specify the CN or OU part, for example, cn=users,dc=eta,dc=com. If you have configured two different user groups, for example, • OU=Organization, OU=Accounts, DC=aaa, DC=com • OU=Service, OU=Accounts, DC=aaa, DC=com The search base to be entered is OU=Accounts, DC=aaa, DC=com. If a user in OU=Organization user group is configured as Admin DN, then all the users in Organization user group can login to Prime Collaboration, but the users in Services user group will not be able to login. Similarly, if a user in OU=Services user group is configured as Admin DN, then all the users in Services user group can login to Prime Collaboration, but not the users in Organization user group. If you configure a user in top level as Admin DN, then all the users under that level can log into Prime Collaboration. For example, if a user in OU=Accounts user group is configured as Admin DN, then all the users in Organization and Services user groups can login to Prime Collaboration. <strong>Note</strong> LDAP authentication fails if you enter special characters in the search base.</td>
</tr>
</tbody>
</table>

**Step 3** Click **Test Connection** to check the connectivity to the LDAP server.
Step 4  
Upon successful connection, click **Apply Settings** and restart Prime Collaboration Assurance server to login using LDAP.

To restart Prime Collaboration Assurance Server, login 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** command takes 10 to 15 minutes to complete execution.

---

### Resetting and Changing Passwords

As a super administrator, system administrator or network operator, you can reset the password for other Prime Collaboration users as well as change your own password.

To reset the password for other users, select a user from **Administration > User Management** and make the necessary changes.

To change your own password, click **Change Password** and make necessary changes.

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

To reset the Prime Collaboration Assurance globaladmin password:

---

**Step 1**  
Log in as a root user.

**Step 2**  
Enter the "goemsam" command:

```
```

**Step 3**  
Execute the following:

```
# ./bin/resetGlobalAdminPassword.sh
```

**Step 4**  
Enter a new password for the globaladmin and also confirm the new password. See the *Cisco Prime Collaboration Quick Start Guide* for more information on password verification rules.

---

To reset the Prime Collaboration Provisioning globaladmin password:

---

**Step 1**  
Log in as a root user.

**Step 2**  
Execute the following commands:

```
# cd /opt/cupm/sep/ipt/bin:
# ./ResetGlobalAdminPassword.sh 'new password' <server type>
```

Enter a new password for the globaladmin and specify the server type. The server type can be one of the following:

- **ALL**—for a single machine install

---
Database—for database server
Application—for application server

Note
In case of a distributed system where database and application are in different servers, you must execute this procedure in both the servers.
Managing Customers

This section applies only to the Managed Service Provider (MSP) version of Prime Collaboration.

When you installed Prime Collaboration, you selected either the single enterprise or MSP version of Prime Collaboration. Each version provides a different customer view option.

The single enterprise version provides a single customer view, where you can only see the devices for one particular customer. This option is usually used in a standard, single enterprise environment.

The MSP version provides multiple customer views. This option is used in managed service provider environments. This view allows you to manage networks and to host services of multiple customers that are being managed by Prime Collaboration. You can associate a device to a customer by adding a customer name. All endpoints or subscribers registered to a publisher inherit the customer name from the publisher.

Adding a Customer

To add a customer:

Step 1 Choose Administration > Customer Management.
Step 2 From the Customer Management page, click Add.
Step 3 In the General Info page, enter the required details and click Next.
Step 4 In the Devices/Device Group page, select the appropriate devices and click Save.

On the Prime Collaboration home page, you can select customers and filter information accordingly.

Rest your mouse over the quick view icon next to the Customer field at the top-right corner of the Prime Collaboration user interface.

You can select one or more customers for which you want to see data for. You can also select multiple customers at the same time by selecting All Customers to see aggregate information for all customers. By default, data is displayed for all the customers.

The Prime Collaboration user interface will filter and show only the information for the selected customer(s) across all features such as dashboards, inventory table, and alarms.
Managing Jobs

Prime Collaboration allows you to view the details of all immediate and scheduled jobs in the Jobs pane. The manually scheduled jobs are discovery, update inventory, and import sessions. The polling jobs are triggered based on user-configured values.

Table 7-1 lists the details that are displayed on the Jobs page (Administration > Job Management). To get the latest information, refresh the page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Description of the job as defined in the Prime Collaboration Assurance or Prime Collaboration Provisioning server.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates the type of the job.</td>
</tr>
<tr>
<td>Description</td>
<td>Describes the job.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of a job. It can be:</td>
</tr>
<tr>
<td></td>
<td>• Completed—Job has completed. If a job has completed, it does not necessarily mean that the job has been successful. There may be instances where the job might have failed to run on a few devices. You can view the job details in the Job Instances table by clicking the arrow on the far left of the page.</td>
</tr>
<tr>
<td></td>
<td>• Cancelled—Job has been cancelled. You can cancel a scheduled job. However, you cannot cancel a running job or a system job (for example, a polling job).</td>
</tr>
<tr>
<td></td>
<td>• Scheduled—Job is scheduled to run at a specific time. It can be scheduled to run at a single time or at several times as a recurring job.</td>
</tr>
<tr>
<td></td>
<td>• Suspended—Job is halted temporarily and can be resumed later.</td>
</tr>
<tr>
<td></td>
<td>• Running—Job is executing.</td>
</tr>
<tr>
<td>Owner</td>
<td>User who created the job. If it is a predefined system job, the creator is displayed as SYSTEM.</td>
</tr>
<tr>
<td>Job Start Time</td>
<td>Time when the job is scheduled to run for the first time.</td>
</tr>
<tr>
<td>Job End Time</td>
<td>Time up to which the job remains active. The job becomes inactive after all scheduled instances of the job have been run.</td>
</tr>
<tr>
<td>Next Scheduled Time</td>
<td>Start time of a subsequent job instance. This applies to a recurring periodic job. If it is either an immediate job or one-time job, the times displayed for Job Start Time and Next Scheduled Time are the same.</td>
</tr>
<tr>
<td>Schedule Type</td>
<td>Whether the job is scheduled to run at a periodic frequency or once.</td>
</tr>
</tbody>
</table>
Table 7-1  Job Details (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run ID</td>
<td>If it is a periodic job, it displays the job instances count. If it is not a periodic job, it displays zero.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the job instance of the same job. Hover the mouse over the quick view icon in this column to view the job instance results.</td>
</tr>
<tr>
<td>Status Progress</td>
<td>Indicates the stage of the job and the percentage complete.</td>
</tr>
<tr>
<td>Results</td>
<td>Indicates whether the job succeeded or failed.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Start time of a job instance.</td>
</tr>
<tr>
<td>End Time</td>
<td>End time of a job instance.</td>
</tr>
<tr>
<td>Duration</td>
<td>Time elapsed from the start time to the end time of a job instance.</td>
</tr>
</tbody>
</table>

Scheduling a Job

You can schedule a job and set options using the Schedule and Settings tab under the Job Details pane.

Note

The schedule and settings tabs are enabled for discovery jobs only. Discovery jobs can be scheduled through the Device Work Center page only. You cannot schedule jobs through the Job Management page.

You can only modify the schedule of discovery job that has one of the following statuses:

- Running
- Scheduled
- Failed

To schedule a job:

Step 1  Choose a job under the Jobs pane, and click the Schedule tab under the Job Details pane.

Step 2  In Schedule Options, choose the start time, end time, and recurrence.

You can set the recurrence to Daily, Weekly, or Monthly to specify a day and frequency. Select Hourly to schedule a job every few hours as needed.

The schedule is defined. If you set the recurrence to None, you cannot specify other frequency details.

Step 3  Click the Settings tab and choose options.

The job runs according to the settings you have defined. The job status for the job is set to Scheduled in the Jobs pane.
Cancelling a Job

You can cancel a discovery job that is in the Scheduled state, using Cancel Job. However, you cannot cancel a job if its status is one of the following:

- Cancelled
- Completed
- Failed
- Running

Also, you cannot cancel the following jobs:

- Polling—Any job starting with the word Polling; for example, Polling_CTS-HEALTH_, Polling_TelepresenceSystem_, Polling_CtsMAN-HEALTH_, and so on).
- Purging—Any job starting with the word Purging.

Predefined Quick Filters

Prime Collaboration supports the following predefined quick filters:

- All Discovery Jobs—An example of a discovery job is DiscoveryFrmBackgroundPathtrace. Discovery jobs are listed when you perform device discovery or rediscovery or update inventory tasks, either by using Operate > Device Work Center > Discover Devices or by selecting a device and clicking Rediscover or Update Inventory.

You can view the Job Instance Result - Total Device Summary and Endpoint Device Summary by resting your mouse pointer on values in the Run ID column on the Job Details pane and clicking the Quick View icon. For more information, see ‘Discovering Devices’ in the Cisco Prime Collaboration 9.5 Assurance Guide.

- All Polling Jobs—An example of a polling job is MCU_Session.Import. Polling jobs are automatically created at system setup.

- All Report Jobs—Report jobs are listed when a report is run.

- All Session Import Jobs—An example of a session import job is MNGD_Synch_CtsMAN-MEETING. Sessions are imported from CTS-Manager and Cisco TMS. A separate job is created for each of these management applications.

- All System Jobs—System-generated jobs such as discovery, polling, and so on. System-generated jobs are listed as soon as the system performs a job.

- All User Jobs—An example of a user job is RediscoverDevices_134739631540. User jobs are listed as soon as a user runs a job.

- Jobs Run in Last 24 Hours—An example of a job run in the last 24 hours is Discovery 2012-Sep-13 10:32:40 UTC. Lists all jobs whose last complete time (the last run instance) is within the last 24 hours from the current time.
Performing Backup and Restore

Prime Collaboration allows you to back up and restore your data. You can schedule periodic backups using the Prime Collaboration user interface, or run backup commands manually by logging in to the system as an admin user (CLI user). However, you must manually run restore commands by logging in to the system as an admin user.

**Note**
- CLI is supported only through SSH; Telnet is not supported. The port used for Prime Collaboration Assurance is 26; for Prime Collaboration Provisioning it is 22.
- The `application stop cpcm` command takes 10 minutes to complete execution and `application start cpcm` command takes 10 to 15 minutes to complete execution.

Overview of Backup and Restore

Although the Prime Collaboration Assurance and Prime Collaboration Provisioning applications’ UIs are converged, you must perform backups on the respective Assurance and Provisioning servers.

Prime Collaboration Assurance backup and restore are covered in this guide. For information about Prime Collaboration Provisioning backup and restore, see ‘Provisioning Database Backup and Restore’ in *Cisco Prime Collaboration 9.5 Provisioning Guide*.

Prime Collaboration Assurance uses the following purge policy:

- All session and endpoint statistics data older than one day are purged. For more details, see “Monitoring Sessions” in *Cisco Prime Collaboration 9.5 Assurance Guide*.
- All session and troubleshooting details older than 14 days are purged every hour. For more details, see “Video Endpoints” in *Cisco Prime Collaboration 9.5 Assurance Guide*.
- Call quality event history and audio/video phone audit report data older than 30 days are purged. For more details, see “Voice Reports” in *Cisco Prime Collaboration 9.5 Assurance Guide*.
- Cleared alarms and events that are older than 14 days are purged every hour. If an alarm is purged, all associated events are also purged. Active events and alarms are not purged. For more details, see *Cisco Prime Collaboration 9.5 Assurance Guide*.
- Jobs that are older than 14 days and have a status of completed, failed, or cancelled are purged every hour.
The backup and restore service allows you back up the database, configuration files, and log files to either a remote location or a local disk. Files in the following folders are backed up by the backup service:

<table>
<thead>
<tr>
<th>Folder Name</th>
<th>Type of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>emms database</td>
<td>Database</td>
</tr>
<tr>
<td>cpcm/conf</td>
<td>Configuration files</td>
</tr>
<tr>
<td>cpcm/export</td>
<td>Troubleshooting and endpoint utilization reports</td>
</tr>
<tr>
<td>cpcm/logs and tomcat/logs</td>
<td>Assurance application and Tomcat log files</td>
</tr>
<tr>
<td>jre/lib/security</td>
<td>Keystore files</td>
</tr>
</tbody>
</table>

**Note**
The data backup may take a long time (up to 12 hours), depending on the number of managed devices in the Prime Collaboration Assurance server. It is recommended that you schedule backups during the non-business hours, because, this operation will severely slow down the Prime Collaboration Assurance UI performance.

### Scheduling a Backup Using the Prime Collaboration User Interface

You can schedule and run backup for both Assurance and Provisioning from the user interface. You can use SFTP, FTP, or a local connection to create the backup.

You must be logged in as an administrator to perform backup.

To create a new backup job:

**Step 1** Choose Administration > Backup Management.

**Step 2** In the Backup Management page, click New.

**Step 3** Enter a name for the backup job.

If you do not specify a backup name, the Backup Title field is defaulted with a date stamp.

**Step 4** Select a backup category and enter the connection settings. (You can use SFTP, FTP, or local connection to create the backup.)

**Step 5** Do one of the following:

- If you are using a local connection, specify the location at which to save the backup files on your local machine. (You can specify up to nine backup files to be saved using the Backup History drop-down list; the default is two.)

- If you selected SFTP or FTP, provide the required information and click Test to test the connection using the credentials.

**Step 6** Specify the backup start time and recurrence interval. (The time displayed in the date picker is the client browser time.)

**Step 7** (Optional) Enter the e-mail IDs to which the backup status notification are to be sent. You must separate the e-mail IDs using a comma.
Step 8  Click Save.
The scheduled backup job is listed in the Backup Management page.
You can click **Run Now** to run the backup immediately.

---

Note  You cannot take a backup of Analytics from the Backup management UI. Use CLI to take backup of Analytics.

---

### Scheduling a Backup Using the CLI

Backup and Restore using the CLI can be performed in the following ways:

- Make a backup of data in a system and restore it on the same system. For more information, see Backup and Restore Assurance Data, page 8-3.
- Make a backup of data in a system and restore it on a different system. For more information, see Restoring Data on a Different System, page 8-5.

---

### Backup and Restore Assurance Data

#### Creating a Repository on an FTP, SFTP, or TFTP Server

You must create a repository before backing up the data. By default, the backup service creates a *.tar.gpg file under the configured repository. The backed-up file is in a compressed format. The repository can be on CD-ROM, disk, HTTP, FTP, SFTP, or TFTP.

To create a repository:

---

Step 1  Log in to the Prime Collaboration Assurance server with the account that you created during installation. The default login is **admin**.

Step 2  Enter the following commands to create a repository on a disk:

```
admin# config t
admin(config)# repository RepositoryName
admin(config-Repository)# url ftp://ftpserver/directory
admin(config-Repository)# user UserName password {plain | hash} Password
admin(config-Repository)# exit
admin(config)# exit
```

Where:

- **RepositoryName** is the location to which files should be backed up. This name can contain a maximum of 30 alphanumeric characters.
- **ftp://ftpserver/directory** is the FTP server and the directory on the server to which the file is transferred. You can also use SFTP, HTTP, disk, or TFTP instead of FTP.
Scheduling a Backup Using the CLI

- **UserName** and `{plain | hash} Password` are the username and password for the FTP, SFTP, or TFTP server. `hash` specifies an encrypted password, and `plain` specifies an unencrypted plain text password.

For example:
```
admin# config t
admin(config)# repository tmp
admin(config-Repository)# url ftp://ftp.cisco.com/incoming
admin(config-Repository)# user john password plain john!23
admin(config-Repository)# exit
admin(config)# exit
```

## Backing Up Data

After creating the repository, log in to the Prime Collaboration Assurance server as `admin` and run the following command to back up the data:
```
admin# backup Backupfilename repository RepositoryName application cpcm
```

Where:
- **Backupfilename**—Name of the backup file (without the extension-.tar.gpg). This name can contain a maximum of 100 alphanumeric characters.
- **RepositoryName**—Location to which the files are be backed up. This name can contain a maximum of 30 alphanumeric characters.

The following message appears after the backup is complete:
```
% Creating backup with timestamped filename: Backupfilename-Timestamp.tar.gpg
```

The backup file is suffixed with the time stamp (YYMMDD-HHMM) and file extension .tar.gpg and saved in the repository. For example:
```
admin# backup cmbackup repository tmp application cpcm
```

The following message appears after the backup is complete:
```
% Creating backup with timestamped filename: cmbackup-110218-0954.tar.gpg
```

## Restoring Data on the Same System

To restore the data, log in to the Prime Collaboration Assurance server as `admin` and run the following command:
```
admin# restore Backupfilename repository RepositoryName application cpcm
```

Where **Backupfilename** is the name of the backup file suffixed with the timestamp (YYMMDD-HHMM) and file extension .tar.gpg.

For example:
```
admin# restore cmbackup-110218-0954.tar.gpg repository tmp application cpcm
```
Restoring Data on a Different System

Prime Collaboration allows you to back up system data and restore it on a different system in the event of total system failure.

To restore the backup from another system, the following prerequisites must be met:

- Ensure that the system to which data is restored has the same MAC address as that of the system that was backed up (the IP address and the hostname can be different).

  If you are unable to assign the MAC address of the original system (the one that was backed up) to another system, contact Cisco TAC for information on a new license file (for a new MAC address).

The procedure to backup and restore data on a different system is the same as the procedure to backup and restore data on the same system.

Note

To perform backup and restore for a single machine or distributed database setup in Provisioning, see "Performing Backup and Restore" chapter in Cisco Prime Collaboration 9.5 Provisioning guide.

Note

You must rediscover all the devices post restore.

Listing the Repository Data

You can list the data within a repository. Log in to the Prime Collaboration Assurance server as admin and run the following command:

```
admin# show repository RepositoryName
```

For example:

```
admin# show repository tmp
cmbackup-110218-0954.tar.gpg
admin#
```

Checking the Backup History

You can check the backup history. Log in to the Prime Collaboration Assurance server as admin and run the following command:

```
admin# show backup history
```

For example:

```
admin# show backup history
Fri Feb 18 09:54:39 UTC 2011: backup cmbackup-110218-0954.tar.gpg to repository temp: success
Fri Feb 18 18:29:48 UTC 2011: backup cmbackup-110218-1829.tar.gpg to repository temp: success
admin#
```
User Interface

Prime Collaboration is a thin-client, web-based application comprising the Prime Collaboration Assurance and Prime Collaboration Provisioning applications. Prime Collaboration user interface (UI) components are visible throughout the UI and enable you to set up filters, see page details in a quick view, and perform global searches.

You can install Prime Collaboration Assurance and Prime Collaboration Provisioning as standalone systems. For information about client requirements, see Cisco Prime Collaboration 9.5 Quick Start Guide.

Filters

You can use the Filter feature to display specific information on the Prime Collaboration user interface. The Filter icon is provided wherever the data is displayed in a tabular format.

The following are the types of filters available on the Prime Collaboration client:

- **Quick Filter**
- **Advanced Filter**
- **Preset Filter**

The quick filter and advanced filter are case insensitive. For these filters, you can also use the following wildcard expressions:

- **Question mark (?)**—Match any one character.
- **Asterisk (*)**—Match zero or more characters.

**Quick Filter**

This filter allows you to narrow down the data inside a table by applying a filter to a specific table column or columns. The operator used with this filter is Contains. To apply different operators, use the Advanced Filter option.

To launch the quick filter, choose Quick Filter from the Filter drop-down menu.

To clear the quick filter, click Filter.

**Advanced Filter**

This filter allows you to narrow down the data in a table by applying a filter using multiple operators, such as Does not contain, Does not equal, Ends with, Is empty, and so on.
You choose the filter pattern (table column names) and operator from the drop-down menu. In addition, you must enter filter criteria based on data available in the Prime Collaboration database.

**Launching the Advanced Filter and Saving Filter Criteria**

To launch the advanced filter, choose **Advanced Filter** from the Filter drop-down menu.

You can save the filter criteria used in the Advanced filter.

To save the filter criteria:

- **Step 1** From the Filter drop-down menu, choose **Advanced Filter**.
- **Step 2** Enter advanced filter criteria.
- **Step 3** Click **Go** and then click the **Save** icon.
- **Step 4** In the Save Preset Filter window, enter a name for the Preset Filter and click **Save**.

To clear the Advanced Filter, click the Filter button.

**Preset Filter**

Prime Collaboration provides predefined keywords to filter data. In addition, the saved advanced filter criteria are also listed in the Preset Filter drop-down list. See Advanced Filter, page A-1 for details on how to save the filter criteria.

This feature is available on some pages; for example, Device Management, Alarm browsers, and Event browsers. To launch a preset filter, choose the available values from the Show drop-down list.

**Predefined Filters**

Prime Collaboration provides a set of predefined filters that enable you to filter the data in a table.

**Quick View**

The quick view icon appears when you rest your mouse pointer on a table, specific table columns, or a topology pane. You can use quick view to cross-launch a page that you want to view in detail.

In Prime Collaboration Assurance, this option is not available for administrative tasks, reports, or diagnostic views. It is available for Prime Collaboration Provisioning when you order a product.
### Global Search Options for Prime Collaboration Assurance

**Table A-1**  
<table>
<thead>
<tr>
<th>Search</th>
<th>Variable</th>
<th>Sample String Format</th>
<th>Exceptions and Allowed Search Strings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td>DN</td>
<td>10002</td>
<td>1000*</td>
</tr>
<tr>
<td></td>
<td>IP</td>
<td>10.64.101.162</td>
<td>10.64.101.*</td>
</tr>
<tr>
<td></td>
<td>MAC</td>
<td>00260bd75cf8l</td>
<td>00260bd75cf*</td>
</tr>
<tr>
<td>Device</td>
<td>IP</td>
<td>10.78.22.129</td>
<td>10.78.22.*</td>
</tr>
<tr>
<td>DNS</td>
<td>Name</td>
<td>US-Texas</td>
<td>US*</td>
</tr>
<tr>
<td>TelePresence</td>
<td>IP</td>
<td>10.78.22.77</td>
<td>10.78.22.*</td>
</tr>
</tbody>
</table>

*Note:* When you search for phones using the MAC address in the global search option, use the format `xxxxxxxxxxxx`.

### Global Search Options for Prime Collaboration Provisioning

**Table A-2**  
<table>
<thead>
<tr>
<th>Search</th>
<th>Variable</th>
<th>Sample String Format</th>
<th>Exceptions and Allowed Search Strings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscriber</td>
<td>ID</td>
<td>AASJKUser006l</td>
<td>AAS<em>l AA</em>l</td>
</tr>
<tr>
<td>Last Name</td>
<td></td>
<td>3242#@!######## #&amp;@!@'(3)</td>
<td>AANewRDUser001*</td>
</tr>
</tbody>
</table>
**Note**

- When you search for phones using the MAC address in the global search option, use the format `xxxxxxxxxxxxx`.
- A minimum of three characters in the search string is recommended to enable faster retrieval of search results.
INDEX

A

adding
  license 2-3
  users 5-8
Adding, Editing, and Deleting a User 5-8
administration authorization role 5-1
advanced
  assignment authorization role 5-2
  ordering authorization role 5-2
approval authorization role 5-3
assignment authorization role 5-3
Assurance globaladmin password 5-12
Assurance Licensing 2-1
Assurance User Roles 5-1
Assurance user roles and tasks 5-4
authorization roles
  tasks permitted by 5-1

B

backup
  data 8-5
  history 8-6
  See also restore
Backup and Restore 8-1

C

Change Password 5-12
Configure 4-1
  Dashlet Label, SMTP server 4-2
  Log Levels 4-2

D

data
  backup 8-5
  restore 8-5
delete a user 5-10
Device Inventory Management 1-2
Diagnostics 1-3
Discovery jobs 7-2

E

edit user details 5-9
EPM MIB 1-4

F

Fault Management 1-4
files
  restore 8-5

G

globaladmin 5-3
import a user 5-8
integrate Provisioning server with Assurance 5-8
interface components
  filters A-1
  quick view A-2

job
  cancel 7-3
  management 7-1
  schedule 7-2
  status 7-1
Jobs 7-1

license
  adding 2-3
  details 2-3
license count 2-2

maintenance authorization role 5-2
Managing
  licenses 2-1
mapping, roles and tasks 5-4

ordering authorization role 5-2

password

recover 5-12
reset 5-12
Phone count in Assurance 2-2
Phone count in Provisioning 2-3
policy authorization role 5-2
port used for Assurance 8-1
Prime Collaboration Assurance 1-1
Prime Collaboration Provisioning 1-5
Provisioning globaladmin password 5-12
Provisioning Licensing 2-2
Provisioning User Roles 5-1
Provisioning user roles and the tasks 5-7

receiving authorization role 5-3
Reports 1-4
repository
  FTP 8-4
  list 8-6
  SFTP 8-4
  TFTP 8-4
restore
  data 8-5
  See also backup
roles and tasks, mapping 5-4

shipping authorization role 5-3
Single Sign-On 5-3
Super administrator 5-4

User Accounts 5-3
users
  adding 5-8
rerecovering password  5-12

V

Voice and Video Endpoint Monitoring  1-2
Voice and Video Unified Dashboard  1-1