Administration

Login

To log into a standalone Cisco Prime License Manager, enter your username and password. Click **Login**.

For coresident configurations, use the following procedure to log in:

Procedure

Step 1 Select Cisco Prime License Manager from the list of installed applications.

Step 2 Enter your username and password. Click **Login**.

The initial login requires the application username and password that you created as part of the installation. If you are not sure what username and password to use for signing into Cisco Prime License Manager, see Troubleshooting.

The "Getting Started" window appears.

Initial Configuration

Follow these steps to begin using Cisco Prime License Manager:

- Add a product instance. See Add Product Instance, on page 2.

Add Product Instance

The following procedure describes how to add a product instance in Cisco Prime License Manager.

Before you begin

Before you upgrade your system, make sure that the older version of the product instance has all of the purchased licenses installed prior to upgrading to a newer version. This will ensure that those licenses are eligible for migration.

Before adding a Cisco Unified Communications Manager instance to Cisco Prime License manager, make sure that the **accountlocking** setting is **disabled**. This will help to avoid a 401 error when you attempt to add the product instance. Check the status of the account using the following command: **show accountlocking**.

Procedure

Step 1 Log in to Cisco Prime License Manager using the application username and password that you created when you completed the installation.

Step 2 Select **Product Instances**.

Step 3 Click **Add**. The Product Add dialog box appears.

Step 4 Enter the following information:

- **Name**
- **Description (optional)**
- **Product Type**
- **Hostname/IP Address**
- **Username**
- **Password**

Note Credentials are the OS Administration username and password of the product.

Step 5 Click **OK** to add the product instance.

Step 6 Once the product instance has been successfully added, the product appears in the Product Instances table.

Note On the Product Instances page, click **Synchronize Now** to request the licensing information from the new product. If you do not synchronize, current product instance information will not appear in Cisco Prime License Manager until the next scheduled synchronization is completed..

Note "Contains Migratable Licenses" appears in the Status field for all product instances whose licenses have not yet been migrated to Cisco Prime License Manager. To make any licenses that are installable at the product instance available in the Cisco Prime License Manager, they must be migrated. For information about migrating licenses, see: Migrate Licenses to Cisco Prime License Manager.

Backup/Restore

Use the following procedure to perform a backup and restore of Cisco Prime License Manager. We recommend that you perform a backup immediately before and after a successful upgrade.

Procedure

Step 1 From the main menu, select **Administration** > **Backup/Restore**.

Step 2 The Backup/Restore page opens. Enter the following information:

- IP Address/Hostname
- Username
- Password
- Directory

Note At this point, you can click **Test Connection** to test your connection.

Step 3 To perform a backup, click **Run Backup**.

Note A maximum of two backups are stored. Creating a third backup will overwrite the oldest backup.

Step 4 To restore, select the file you wish to restore and click **Run Restore**.

License Definitions

License definitions contain information about the license types managed by Cisco Prime License Manager. These definitions should be updated prior to upgrading any of your product instances to a new version or before adding a product instance of a new type. The **Administration** > **License Definitions** window provides the following information for the currently installed license definition file:

- File name
- Version
- Date Installed

You can click the **Check for Latest Version** link to access the Download Software site. From this site, you can locate the latest release and download it.

Once downloaded, the new license definition file can be installed using the following procedure:

Procedure

Step 1 Access the **License Definitions** window from the main menu by selecting **Administration** > **License Definitions**.

Step 2 Click **Install New License Definition File**.

Step 3 Click **Browse** to select the license definition file you just downloaded, then click **Install**.

Security Updates

Security updates may be required at Cisco Prime License Manager periodically to permit electronic operations with the Cisco License Office.

Security updates for your desired release are available from the https://software.cisco.com: **Downloads Home** > **Products** > **Cloud and Systems Management** > **Collaboration and Unified Communications Management** > **Prime License Manager** > **Prime License Manager 10.5**.

Use the following procedure to perform security updates through CLI:

Procedure

Step 1 Enter the **license management security update** command.

Step 2 When prompted, enter Directory, Server, User Name, and Password information, as shown in the following example:

Example:

```
Directory:
    /users/bsmith/security_update/update

Server:
    se032c-94-61

User Name:
    bsmith

Password:
    ********
```

Step 3 You are then asked to select the security update from those available in the target directory, as shown in the following example:

Example:

```
Available
    options for security update in
    "se032c-94-61:/users/bsmith/security_update/update":

1)
    SecUpd_v1.upd

q) quit
```

Step 4 Select the appropriate file from the list to download the security update. The following messages appear:

Example:

```
Installing
    security update...

Continue
    (y/n)?
```

Step 5 Enter **y** to continue the security update.

When the update is complete, the following message appears:

```
Security
    update installed.
```

TLS Setup

Transport Layer Security (TLS) provides secure and reliable signaling and data transfer between two systems or devices, by using secure ports and certificate exchange. TLS ensures a secure connection for Cisco Prime License Manager and it accepts the configured TLS version.

By default, Cisco Prime License Manager supports a minimum TLS version of 1.0. Use this procedure to reset the minimum supported TLS version for Cisco Prime License Manager to a higher version, such as 1.1 or 1.2.

Before you begin

Before you configure the minimum TLS version, make sure that your network devices and applications both support the TLS version. Also, make sure that they are enabled for TLS that you want to configure with Cisco Prime License Manager.

Note If you are upgrading from an earlier release of Cisco Prime License Manager, make sure that all your devices and applications support the higher version of TLS before you configure it. For example, Cisco Prime License Manager, Release 9.x supports TLS 1.0 only. If you are upgrading from Release 9.x, then upgrade your devices and applications before you enable the higher version of TLS.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 To confirm the existing TLS version, run the **show tls min-version** CLI command.

Step 3 Run the **set tls min-version** <*minimum*> CLI command where <*minimum*> represents the TLS version.

For example, run **set tls min-version 1.2** to set the minimum TLS version to 1.2.

Note Run **show tls min-version** command to view the minimum configured version of TLS.

Accessing Diagnostic Logs

Use the following procedure to run diagnostic logs in Cisco Prime License Manager.

Procedure

Step 1 From the main menu in Cisco Prime License Manager, select **Administration** > **Diagnostic Logs**.

Step 2 The Diagnostic Logs screen appears. Under the Log Settings tab, set the log level to **Debug** for both "Cisco Prime License Manager core services: and "Communication with product instances". Click **Save** to save your changes.

Step 3 Select the **Download Logs** tab and select the date and time range to include in your log file (the time period during which the issue occurred). Click **Generate Log File**.

Step 4 The link to the log file appears below the **Generate Log File** button. Click the link to download the log file to your computer and open a Service Request using the TAC Service Request Tool, https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case

Manage Product Instances

Edit a Product Instance

The following procedure describes how to edit a product instance in Cisco Prime License Manager.

Procedure

Step 1 To edit a product instance, select that instance from the Product Instances table.

Step 2 From the General tab of the Product Instance details page, edit the preferred settings for the product instance.

Important If the hostname or IP address of the product instance changes, you need to delete the product instance from the Cisco Prime License Manager prior to changing the hostname/IP address. You then re-add it to the Cisco Prime License Manager once you have completed the hostname/IP address change.

Delete a Product Instance

Procedure

Step 1 In the Action column for the product instance you wish to delete, click **Delete**.

Step 2 Following a successful deletion, click **Synchronize Now** to obtain the most up-to-date licensing information for all license types in the system.

Administrator Account Configuration

Add Administrator Account

During installation, the first account that is created is the Master Account. The Master Account has special privileges:

- It is the only account that can create or delete administrator accounts.
- It is the only account that can modify the credential policy.

Follow the steps below to add a new administrator account.

Procedure

Step 1 Log in to Cisco Prime License Manager using the Master Account.

Step 2 From the main menu in Cisco Prime License Manager, select **Administration** > **Administrator Accounts**.

Step 3 Select **Add Administrator**.

Step 4 Optionally add a name or description in the **Name/Description** field.

Step 5 Enter a username.

Step 6 Enter and confirm your password.
The system will evaluate the strength of the password.

Reset the Administrator or Security Password

If you lose the administrator password and cannot access your system, use this procedure to reset the password.

Before you begin

- You require physical access to the node on which you perform this procedure.
- At any point, when you are requested to insert CD or DVD media, you must mount the ISO file through the vSphere client for the VMWare server. See “Adding DVD or CD Drives to a Virtual Machine” https://www.vmware.com/support/ws5/doc/ws_disk_add_cd_dvd.html for guidance.
- The security password on all nodes in a cluster must match. Change the security password on all machines, or the cluster nodes will not communicate.

Procedure

Step 1 Sign in to the CLI on the publisher node with the following username and password:

a) Username: **`pwrecovery`**

b) Password: **`pwreset`**

Step 2 Press any key to continue.

Step 3 If you have a valid CD/DVD in the disk drive or you mounted an ISO file, remove it from the VMWare client.

Step 4 Press any key to continue.

Step 5 Insert a valid CD or DVD into the drive or mount the ISO file.

Note For this test, you must use a disk or ISO file that is data only.

Step 6 After the system verifies the last step, you are prompted to enter one of the following options to continue:

- Enter **a** to reset the administrator password.
- Enter **s** to reset the security password.

Note You must reset each node in a cluster after you change its security password. Failure to reboot the nodes causes system service problems and problems with the administration windows on the subscriber nodes.

Step 7 Enter the new password, and then reenter it to confirm.

The administrator credentials must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores.

Step 8 After the system verifies the strength of the new password, the password is reset, and you are prompted to press any key to exit the password reset utility.

If you want to set up a different administrator password, use the CLI command **set password**. For more information, see the *Command Line Interface Reference Guide for Cisco Unified Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

User Credential Configuration Settings

The following options display when you select an administrator account from the **Administrator Account** list. This table describes credential settings for each user.

Table 1: User Credential Settings

Field	Description
Account Locked By Administrator	Check this check box to lock this account and block access for this user. Uncheck this check box to unlock the account and allow access for this user.
User Cannot Change Credentials	Check this check box to block this user from changing their password. You cannot check this check box when the **User Must Change Credentials at Next Login** check box is checked.

Field	Description
User Must Change Credentials at Next Login	Check this check box to require the user to change their password at next login. Use this option after you assign a temporary password. You cannot check this check box when the **User Cannot Change Credentials** check box is checked.
Credentials Do Not Expire	Check this check box to block the system from prompting the user to change their password. You can use this option for low-security users. If checked, the user can still change their password at any time. When the check box is unchecked, the expiration setting in the associated credential policy applies.
Reset Failed Login Attempts	Check this check box to reset the number of failed login attempts for this user; The **Time Locked Due to Failed Login Attempts** and **Time of Last Login Attempt** fields are automatically cleared. The number of failed login attempts increases whenever authentication fails for an incorrect credential.
Time Locked Due to Failed Login Attempts	This field displays the date and time that the system last locked this user account due to failed login attempts. The time gets set whenever failed login attempts equal the configured threshold in the credential policy.
Time of Last Failed Login Attempt	This field displays the date and time for the most recent failed login attempt for this user credential.
IP Address of Last Failed Login Attempt	This field displays the IP address of the user who last entered an invalid username or password.
Time Locked by Administrator	This field displays the date and time that the administrator locked this user account. This field is cleared after the administrator unlocks the credential.
Failed Login Attempts	This field displays the number of failed login attempts since the last successful login, since the administrator reset the failed login attempts for this user credential, or since the last reset of failed login attempts.
Time Last Changed	This field displays the date and time of the most recent password change for this user.
Last Changed by User Name	This field displays the username of the administrator who made the last password change.

Field	Description
Last Successful Login	This entry shows the date and time of the last successful login of a particular administrator.
IP Address of Last Successful Login	This field displays the IP address of the user who last logged in successfully.

Credential Policy Configuration

Configure the Credential Policy

The credential policy defines password requirements and account lockouts for administrator accounts in Cisco Prime License Manager. The policy contains settings for failed login resets, lockout durations, expiration periods, and password requirements. The **Credential Policy Configuration** window allows the Master Account to modify the existing credential policy for your system.

Passwords can contain any alphanumeric ASCII character and all ASCII special characters. A non-trivial password meets the following criteria:

- Must contain at least one uppercase character, one lowercase character, one number (0-9), and one special character.
- Must not contain the username.
- Must not contain only consecutive characters or numbers (for example, 654321 or ABCDEFG).

Procedure

Step 1 From the main menu in Cisco Prime License Manager, select **Administration** > **Administrator Accounts**.

Step 2 Select **Credential Policy**.

Step 3 Modify the **Credential Policy Configuration** settings.

The system provides trivial credential checks to disallow passwords that are easily accessed. Enable trivial password checks by checking the **Check for Trivial Credentials** check box in the **Credential Policy Configuration** dialog box.

Customized Logon Message

In a co-resident deployment, a custom log-on message created for Cisco Unified Communications Manager automatically displays in the Cisco Prime License Manager logon window. You can upload a text file with your custom log-on message in the Cisco Unified OS Administration interface at **Software Upgrades** > **Customized Logon Message**.

Note A standalone deployment does not support a custom log-on message.