Administration

The following sections provide information on using the Cisco Prime License Manager administrative tools.

- Backup/Restore, page 1
- License Definitions, page 2
- Security Updates, page 2
- License Rehost, page 3
- Accessing Diagnostic Logs, page 4
- Reset the Administrator or Security Password, page 5
- Administrator Account Configuration, page 6

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.
```

License Rehost

Licenses are fulfilled to a specific Cisco Prime License Manger. If you require licenses to be moved to a new Cisco Prime License Manager, they are to be rehosted.

A rehost may be required if:

- A hardware failure occurred and new hardware is required for Cisco Prime License Manager.
- Multiple Cisco Prime License Managers are desired and a subset of fulfillment licenses are to be moved to a new Cisco Prime License Manager.

License rehosts or transfers can be requested at www.cisco.com/go/license and do not require Global Licensing Operations (GLO) support.

Note In order to use the rehost portal, you must use the same Cisco.com user ID that initially ordered or fulfilled the licenses.

Perform a rehost, the license registration ID from the source machine and the license request or license registration ID from the target machine is required.

Use the following procedure to perform a license rehost.

Procedure

Step 1 From Product License Registration (www.cisco.com/go/license), select **Devices**.

Step 2 Under the **Devices** tab of a particular device, select one or more licenses that you want to rehost.

Step 3 In the pop-up that appears, select **Rehost/Transfer**.

Step 4 In the **Quantity to Assign** field, enter the number of licenses you want to transfer.

Step 5 In the **License Request** field, enter the License Request from the Cisco Prime License Manager of the target device.

Step 6 Click **Next**.

Step 7 In the **Review** screen, review your selections.

Step 8 Enter your email address, select your name from the drop-down list next to **End User**, and indicate that you agree with the Terms of the License.

Step 9 Click **Submit**.

Step 10 The rehosted license is emailed to you. Manually install it on the target Cisco Prime License Manager.

Note The license can also be downloaded to your machine by clicking **Download Target** on the **License Request Status** window and choosing the download location.

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

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"here 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.

Administrator Account Configuration

Reset OS Administrator and Security Passwords

To reset a system password, you must connect to the system through the system console. You cannot reset a password when you connect to the system through a secure shell session.

Note 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"here for guidance.

Procedure

Step 1 Log in to the system with the following username and password:

- Username: pwrecovery
- Password: pwreset
  The **Welcome to platform password reset** window appears.

Step 2 Press any key to continue.

Step 3 If you have a CD or DVD in the disk drive, remove it now.

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 that you have inserted the disk, 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.
- Enter **q** to quit.

Step 7 Enter a new password of the type that you chose.

Step 8 Reenter the new password.
The password must contain at least six characters. The system checks the new password for strength. If the password does not pass the strength check, you are prompted to enter a new password.

Step 9 After the system verifies the strength of the new password, the password is reset. You are prompted to press any key to exit the password reset utility.

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.

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.
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.

Field	Description
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.
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.

Credential Policy Configuration Settings

The following table describes the credential policy settings.

Table 2: Credential Policy Settings

Field	Description
Maximum Failed Login Attempts / No Limit for Failed Login Attempts	Specify the number of allowed failed login attempts. When this threshold is reached, the system locks the account. Enter a number in the range 1-100. To allow unlimited failed logins, check the **No Limit for Failed Login Attempts** check box. Uncheck the check box to enter a value greater than 0. The default value is **No Limit for Failed Login Attempts**.

Field	Description
Reset Failed Login Attempts Every (minutes)	Specify the number of minutes before the counter is reset for failed login attempts. Enter a number in the range 1-120. The default value is 30.
Lockout Duration (minutes) / Administrator Must Unlock	Specify the number of minutes an account remains locked when the number of failed login attempts equals the specified threshold. Enter a number in the range 1-1440. The default value is 30. Use the check box when the credential policy specifies that an **Administrator Must Unlock** this account type after an account lockout. The account will remain locked until an administrator manually unlocks them.
Minimum Duration Between Credential Changes (minutes)	Specify the number of minutes that are required before a user can change credentials again. A value of 0 allows a user to change credentials at any time. The default value is 0.
Minimum Credential Length	Specify the minimum length for user credentials (password). Do not enter 0 because blank passwords are not allowed. The default value is 1. The minimum setting must equal at least 1.
Number of Previous Credentials Stored	Specify the number of previous user credentials to store. This setting prevents a user from configuring a recently used credential that is saved in the user list. Enter a number in the range 0-25. If no previous credentials should be stored, enter 0. The default value is 0.
Minimum Characters Different During Credential Change	Specify the minimum number of characters that must be unique when you change credentials. The default value is 0.
Inactive Days Allowed	Specify the number of days that an account can remain inactive before it gets locked. Enter a number in the range 0-5000. The default value is 0.
Credential Expires After (days)/ Never Expires	Specify the number of days before a credential will expire. Enter a number in the range 1-365.To allow credentials to never expire, check the **Never Expires** check box. Uncheck the check box to enter a value greater than 0. Use the **Never Expires** option for low-security accounts, for example. The default setting is **Never Expires**.
Expiry Warning Days	Enter a number from 0-90 to specify the number of days before a user password expires to start warning notifications. The default value is 0.

Field	Description
Check for Trivial Credentials	Check this check box to require the system to disallow credentials that are easily accessed. The password must contain at least one uppercase character, one lowercase character, one number (0-9), and one special character. The password must not contain the username or only ascending or descending characters (such as 12345). The default setting does not include a check for trivial credentials.