



## 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](#)
- [Administrator Account Configuration, page 4](#)

## Backup/Restore

Use the following procedure to perform a backup and restore of Cisco Prime License Manager. We recommend that you perform a backup immediate 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 the **Test Connection** button to test your connection.

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

**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 the **Run Restore** button.

---

# 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 page 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 page from the main menu by selecting **Administration > License Definitions**.
- Step 2** Click the **Install New License Definition File** button. The Install License Definitions window appears.
- Step 3** Click the **Browse** button 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 will be available at the Cisco Software Download Center: <http://software.cisco.com>.

Use the following procedure to perform security updates through CLI:

## Procedure

- 
- Step 1** Enter the **license management security update** command.
- Step 2** Enter **Directory**, **Server**, **User Name**, and **Password** information when prompted, 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** Select **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 Manager. If you require licenses to be moved to a new Cisco Prime License Manager, they will need 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 need to be moved to a new Cisco Prime License Manager

License rehosts or transfers can be requested at [www.cisco.com/go/license](http://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.

To perform a rehost, the license registration from the source machine as well as license request or license registration from the target machine is required.

Use the following procedure to perform a license rehost.

### Procedure

- 
- Step 1** From Product License Registration (<https://tools.cisco.com/SWIFT/LicensingUI/Quickstart>), choose **Licenses**.
- Step 2** Under the License ID tab of a particular device, choose the license(s) that you want to rehost.
- Step 3** In the pop-up that appears, choose **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, choose 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. It must then be manually installed on 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 the **Generate Log File** button.
- 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 then send the log file to Cisco: [licensing@cisco.com](mailto:licensing@cisco.com)
- 

## Administrator Account Configuration

### Reset OS Administrator and Security Passwords

To reset a 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**

During this procedure, you must remove and then insert a valid CD or DVD in the disk drive to prove that you have physical access to the system.

---

**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.

The system tests to ensure that you removed the CD or DVD from the disk drive.

**Step 5** Insert a valid CD or DVD into the disk drive.

**Note** For this test, you must use a data CD, not a music CD. The system tests to ensure that you have inserted the disk.

**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** From the main menu in Cisco Prime License Manager, select **Administration > Administrator Accounts**.
- Step 2** Select **Add Administrator**.
- Step 3** Optionally add a name or description in the **Name/Description** field.  
Make sure you enter a name or description that is intuitive. This will help you distinguish between multiple accounts.
- Step 4** Enter a username.
- Step 5** Enter and confirm your password.  
The system will evaluate the strength of the password.
- 

## User Credential Configuration Settings

The following 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 this credential. You cannot check this check box when <b>User Must Change Credentials at Next Login</b> check box is checked.
User Must Change Credentials at Next Login	Check this check box to require the user to change this credential at next login. Use this option after you assign a temporary credential. You cannot check this check box when <b>User Cannot Change Credentials</b> check box is checked.
Credentials Do Not Expire	Check this check box to block the system from prompting the user to change this credential. You can use this option for low-security users. If checked, the user can still change this credential 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 <b>Time Locked Due to Failed Login Attempts</b> and <b>Time of Last Login Attempt</b> fields are automatically cleared. The number of failed login attempts increases whenever authentication fails for an incorrect credential.

Field	Description
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.
Time Locked by Administrator	This field displays the date and time that the administrator locked this user account. This field goes blank 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 credential change for this user.
Last Changed by User Name	This field displays the username of the administrator who made the last credential change.
Last Successful Login	This entry shows the time/date stamp of the last successful login of a particular administrator.

## Credential Policy Configuration

### Configure the Credential Policy

A 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 credential requirements. The **Credential Policy Configuration** window allows the Master Account to modify the existing credential policy for your system or site.

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).

**Note**

You cannot create or delete credential policies.

## Procedure

- 
- Step 1** From the main menu in Cisco Prime License Manager, choose **Administration > Administrator Accounts**.
- Step 2** Choose **Credential Policy**.
- Step 3** Modify the **Credential Policy Configuration** settings.  
The system provides trivial credential checks to disallow credentials that are easily accessed. Enable trivial credential 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 <b>No Limit for Failed Login Attempts</b> check box. Uncheck the check box to enter a value greater than 0. The default value is <b>No Limit for Failed Login Attempts</b> .
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 <b>Administrator Must Unlock</b> 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.



Field	Description
Number of Previous Credentials Stored	<p>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.</p> <p>Enter a number in the range 0-25. If no previous credentials should be stored, enter 0. The default value is 0.</p>
Minimum Characters Different During Credential Change	<p>Specify the minimum number of characters that must be unique when you change credentials. The default value is 0.</p>
Inactive Days Allowed	<p>Specify the number of days that an account can remain inactive before it gets locked.</p> <p>Enter a number in the range 0-5000. The default value is 0.</p>
Credential Expires After (days)/ Never Expires	<p>Specify the number of days before a credential will expire.</p> <p>Enter a number in the range 1-365. To allow credentials to never expire, check the <b>Never Expires</b> check box. Uncheck the check box to enter a value greater than 0. Use the <b>Never Expires</b> option for low-security accounts, for example. The default setting is <b>Never Expires</b>.</p>
Expiry Warning Days	<p>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.</p>
Check for Trivial Credentials	<p>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.</p>

