CHAPTER 7

Inventory Management Tasks

This chapter provides information about managing your inventory with Cisco License Manager and contains the following sections:

Manage Devices

This section provides the following information about managing devices:

Add Cisco Devices to Your Inventory

There are several ways to add devices to the Cisco License Manager database:

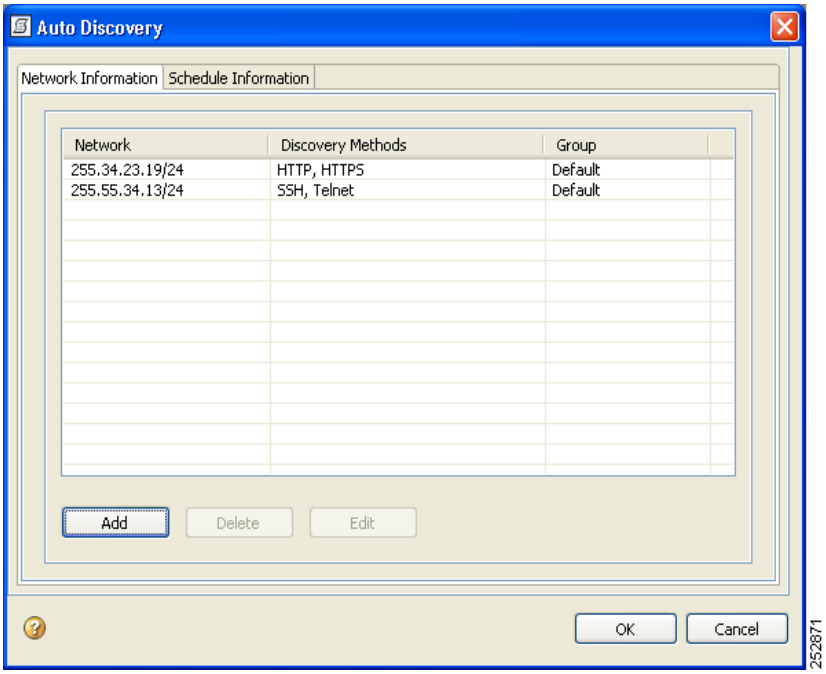
Note To create a device, you can enter either the device UDI or the device IP address in Cisco License Manager. If you use only an IP address, Cisco License Manager detects the device UDI. To obtain a license, the device UDI must be available, but for using all the licensing features, the availability of the device IP address is also mandatory.

Auto Discovery of Devices

Cisco License Manager can be set to automatically discover devices in your environment at predefined intervals. To set Cisco License Manager to discover devices automatically, complete the following steps:

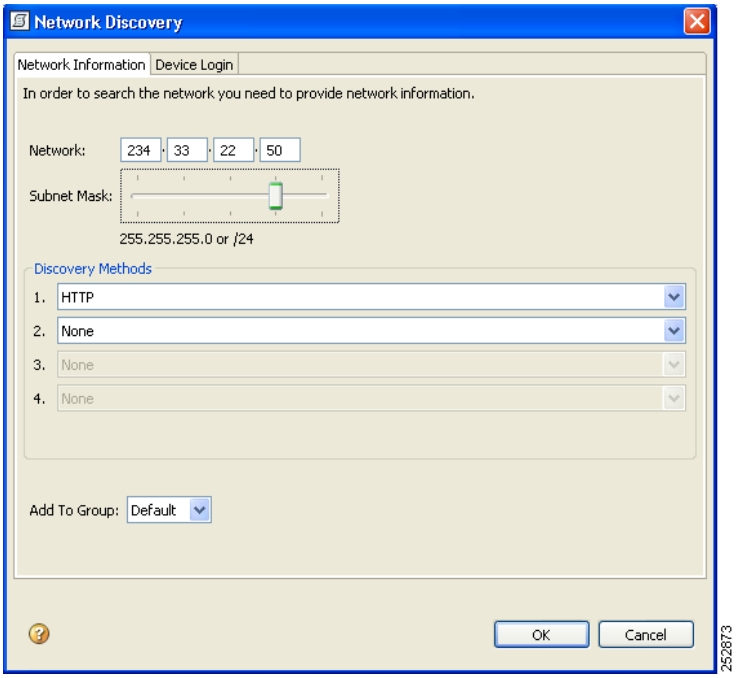
Step 1 Select **Manage > Auto Discovery**.

The Auto Discovery dialog box appears. The Network Information page shows the networks from which devices will be discovered, the discovery methods, and the device group to put the discovered devices in. If you are an administrator, you can add more networks or edit networks listed here. Other users can view the contents of this dialog box but not edit them.



Step 2 Click **Add**.

The **Network Discovery** dialog box appears.



Step 3 Enter the following information:

Field	Description
Network	The IP address of the network on which you want to discover devices; for example, 172.0.0.0. **Note** If the information turns red, that portion of the network address is not valid.
Subnet Mask	Defines which portion of the address is used to identify the network and which denotes the hosts.

Step 4 Choose your discovery methods from the drop-down menu. Your choices are HTTP, HTTPS, SSH, and Telnet. Cisco License Manager tries the choices in the order in which you select them until the operation is successful.

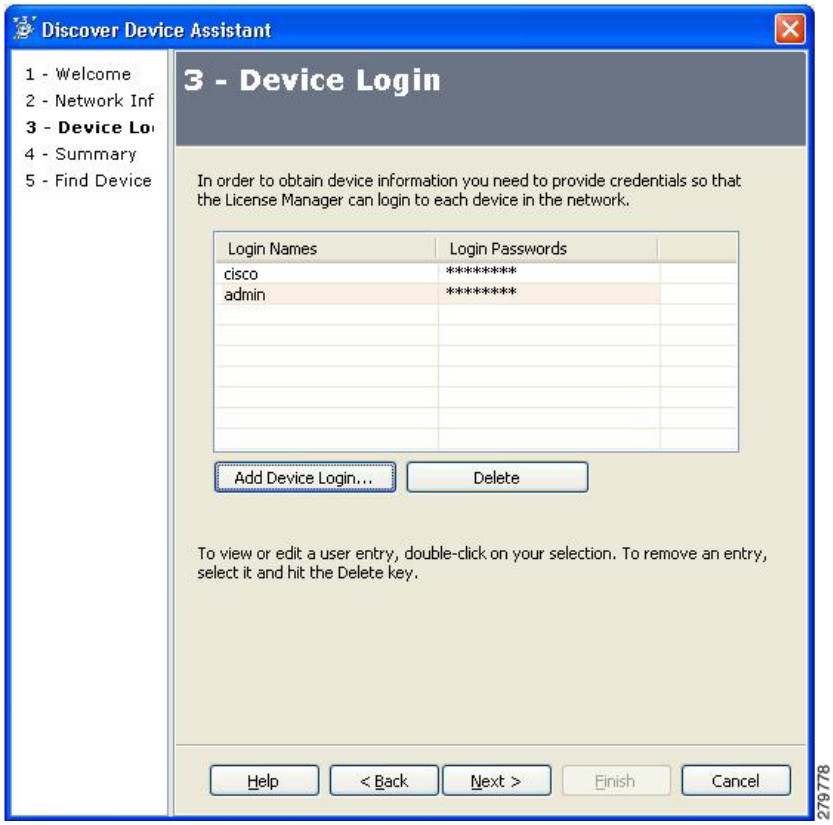
Note HTTP and HTTPS are the quickest discovery methods. Telnet is the slowest discovery method and is not secure. The most secure discovery method is SSH.

Step 5 Choose a device group for the new devices from the **Add To Group** drop-down menu.

Note This drop-down menu includes a list of existing device groups to which to add your devices. Newly discovered devices appear in the Default device group unless you create a new device group before you discover devices. To create a new device group, see "Add a Device Group" section on page 7-14.

Step 6 Click the **Device Login** tab.

The Device Login page appears.



Step 7 Provide login information for the devices in the network by clicking **Add Device Login**. The Add Device Login dialog box appears.

Note You must enter at least one valid username and password for each device. For Cisco IOS devices that do not use HTTP as the discovery method in Cisco License Manager, you must also enter enable passwords. The total number of entries for the device login name is ten.

- Enter the device login name and device login password; confirm the password.
- (For Cisco IOS devices) Enter the enable password in the Device Login Password and in the Confirm Password fields. Leave the Device Login Name field blank.
- Click **Save**.

Example: If you have two devices in your network that have the same device logins and device passwords but have different enable passwords, you make three entries in the Add Device Login dialog box: enter the single device login and password, and then enter two enable passwords (each with the device login name field blank).

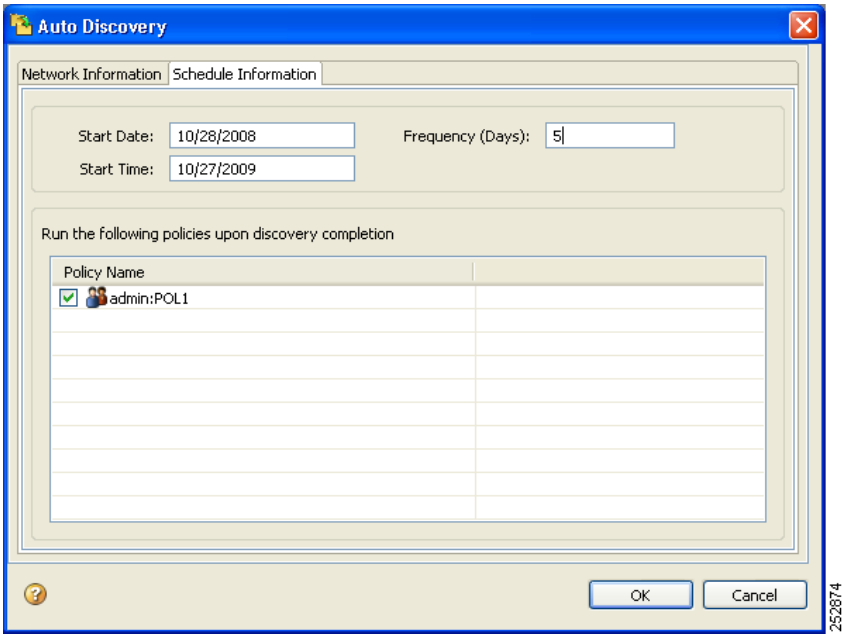
Note To edit or view an entry, double-click the entry. To delete any device login information, select the entry and click **Delete**.

Step 8 After you have entered the device login and enable password information, click **OK**.

The Auto Discovery dialog box reappears.

Step 9 Click the **Schedule Information** tab.

The Schedule Information page appears.



Step 10 To schedule the auto discovery operation:

- Enter the start date in the mm/dd/yyyy format.
- Enter the start time in the hh:mm am/pm format.
- Enter the frequency of the auto discovery operation.
- Select the policies that you want to run during auto discovery.

Step 11 Click **OK**.

While the auto discovery job is running, the job progress can be viewed in the View Job Status window. When the auto discovery operation completes, the job status of the executed policies appears in the View Job Status window. There is one job for each executed policy.

Discover Devices Using the Discover Device Assistant

You can discover devices in a specific network using the Discover Device Assistant. You can also create a new device group and collect license information on those devices during the same discovery process. You can use discovery to synchronize device license information instead of using device polling.

While a discovery operation is in progress, no other discovery operations can be started.

When you add a device using the IP address, the UDI and Device ID parameters are automatically added into the database.

Each time you perform a discovery, the device authentication information, network address, and subnet mask are stored. When you schedule discovery, Cisco License Manager uses this stored information to check if new devices are added and generates a report for each new discovery. You can also specify policies to be run after each discovery.

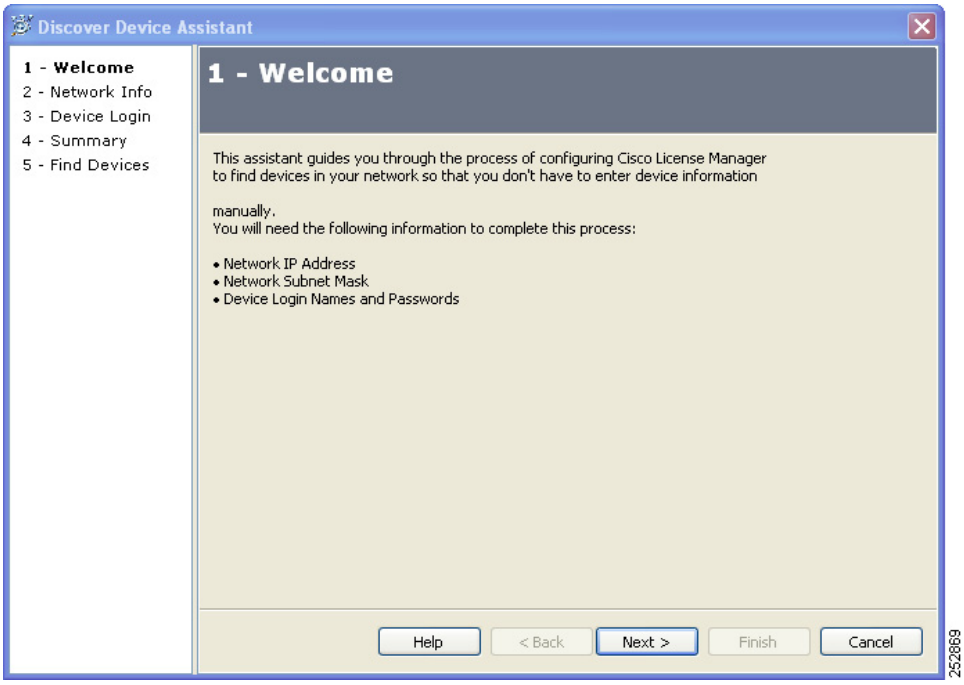
Caution A discovery will overwrite any out-of-date or manually entered data, except for the device display name.

Tip Before you get started, make sure that you have the network IP address, network subnet mask, and device login names and passwords available.

To discover a device using the Discover Device Assistant, complete the following steps:

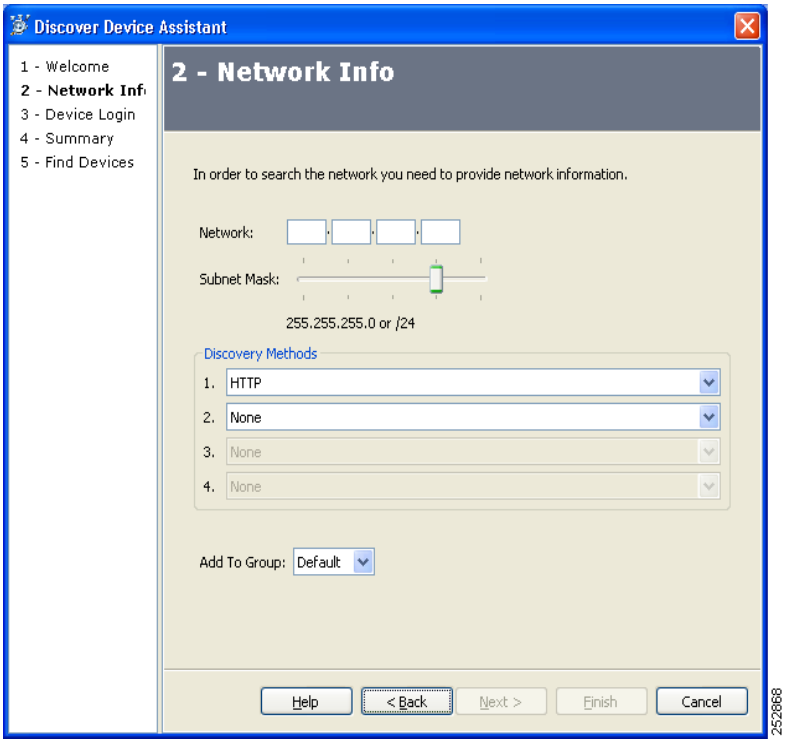
Step 1 In the Quick Links pane, click **Discover Devices**.

The Welcome screen of the Discover Devices Assistant appears. The assistant guides you through the necessary steps to discover the Cisco devices in your network.



Step 2 Click **Next**.

The Network Info screen appears.



Step 3 Enter the following information:

Field	Description
Network	The IP address of the network on which you want to discover devices; for example, 172.0.0.0. **Note** If the information turns red, that portion of the network address is not valid.
Subnet Mask	Defines which portion of the address is used to identify the network and which denotes the hosts.

Step 4 Choose your discovery methods from the drop-down menus. Your choices are HTTP, HTTPS, SSH, and Telnet. Cisco License Manager tries the choices in the order in which you select them until the operation is successful.

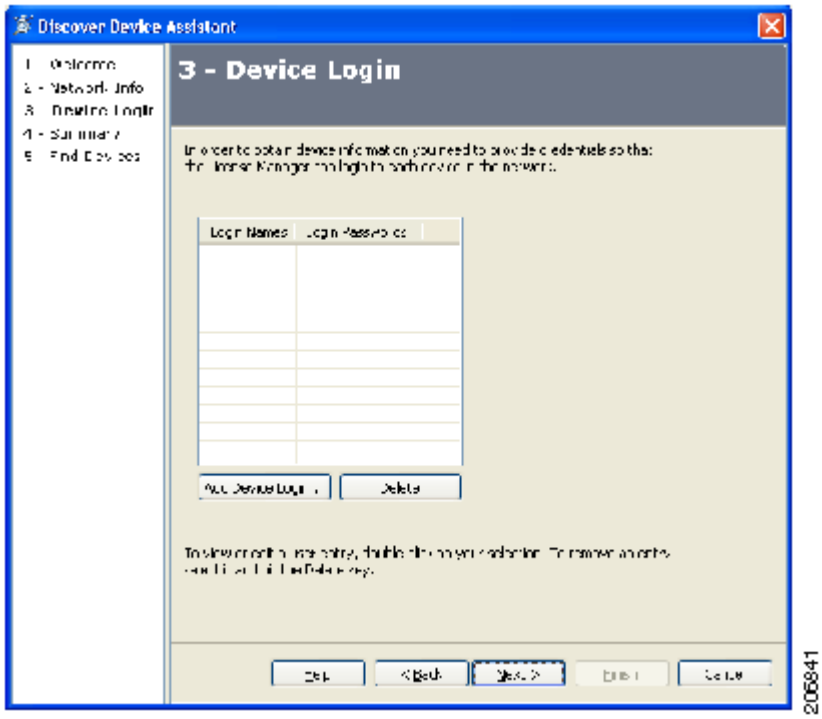
Note HTTP and HTTPS are the quickest discovery methods. Telnet is the slowest discovery method and is not secure. The most secure discovery method is ssh.

Step 5 Choose a device group for the new devices from the **Add To Group** drop-down menu.

Note This drop-down menu includes a list of existing device groups to which to add your devices. Newly discovered devices appear in the Default device group unless you create a new device group before you discover devices. To create a new device group, see "Add a Device Group" section on page 7-14.

Step 6 Click **Next**.

The Device Login screen appears.



Step 7 Provide login information for the devices in the network by clicking **Add Device Login**. The Add Device Login dialog box appears:

Note You must enter at least one valid username and password for each device. For Cisco IOS devices that do not use HTTP as the discovery method in Cisco License Manager, you must also enter enable passwords. The total number of entries for the device login name is ten.

- Enter the device login name and the device login password; confirm the password.
- (For Cisco IOS devices) Enter the enable password in the Device Login Password and in the Confirm Password fields. Leave the Device Login Name field blank.
- Click **Save**.

Example: If you have two devices in your network that have the same device logins and device passwords but have different enable passwords, you make three entries in the Add Device Login dialog box: enter the single device login and password, and then enter two enable passwords (each with the device login name field blank).

Note To edit or view an entry, double-click the entry. To delete any device login information, select the entry and click **Delete**.

Step 8 After you have entered the device login and enable password information, click **Next**.

The Summary screen appears.

Step 9 Verify that the information is correct and click **Next**. If it is not correct, click **Back** and correct the information.

The Find Devices screen appears and Cisco License Manager begins searching for Cisco devices in your network.

Step 10 Once the process is complete and a list of discovered devices appears, click **Finish**. The device status appears in the View Alert dialog box.

Add a Device Using the GUI

You must add your Cisco devices to the Cisco License Manager inventory before you can request a PAK license file. To add a new device, complete the following steps:

Tip When you add a device using the IP address, the UDI and Device ID parameters are automatically added into the database. If you add the device using only the UDI, the Device ID is automatically added into the inventory.

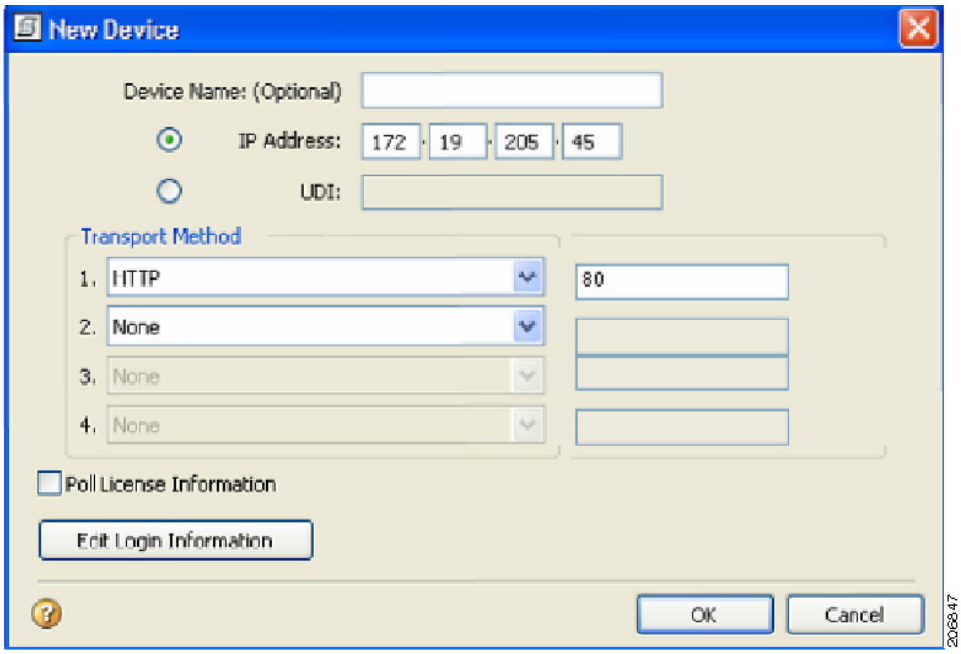
Step 1 Select **Manage > Manage Devices** or click **Devices** in the Quick Links pane.

The Manage Devices explorer appears in the Content Area.

Step 2 Select an existing device group folder to which you want to add a new device.

Make sure to select a folder that makes sense to you so that you can easily locate and retrieve device and license information at a later date.

Step 3 With the device group folder selected, right-click and select **New Device**. The New Device dialog box appears.



Step 4 Enter the following in the New Devices window:

Field	Description
Device Name	Descriptive device name, which you can assign. **Note** If no device name is assigned, the hostname or device UDI will be used.
IP Address	IP address of the device.
UDI	Unique device identifier. Cisco-wide identifier that contains product ID, serial number, and version (optional). **Note** Cisco License Manager uses a different UDI format from the UDI found on the device. The format of UDI in the Cisco License Manager inventory is <PID>:<VID>:<SN>. If you create a device using the UDI, it must be entered in this format.
Transport Method	An ordered list of transport methods. The device will try methods 1, 2, 3, and 4 in order. The approved transport methods are HTTP, HTTPS, SSH, and Telnet.
Poll License Information	Synchronizes the information in the device inventory with the device (optional).

Tip The UDI can be discovered during device discovery, so it may not have to be entered manually. If you enter the UDI manually, ensure that you use the required format. Ensure that you poll your device so that this information can be added into the device's inventory.

Note To create a device, you can enter either the device UDI or the device IP address in Cisco License Manager. If you use only an IP address, Cisco License Manager detects the device UDI. To obtain a license, the device UDI must be available, but for using all the licensing features, the availability of the device IP address is also mandatory.

Note While you create a device, you can specify port for all the supported protocols such as HTTP, HTTPS, TELNET, and SSH. This is for create device only. Discover device will always use default ports. Once the device is created, the ports are not editable in Device Properties.

Step 5 You can click **OK** now if you wish to add the device without entering login information for that device.

If the operation is successful, the device appears in the device group folder you selected. If it is unsuccessful, an error message appears.

Step 6 If you wish to edit the login information for the newly added device, click **Edit Login Information**.

Step 7 Click the **Add Device Login** button, and enter the information in the Add Device Login window:

Field	Description
Device Login Names	List of names of the users logging into the device.

Field	Description
Device Login Passwords	Passwords required for the listed users to access to the device.
Confirm Passwords	Confirmation of password.

Note You must enter at least one valid username and password for each device. For Cisco IOS devices that do not use HTTP as the transport method in Cisco License Manager, you must also enter enable passwords. The total number of entries for the device login name is ten.

- Enter the device login name and device login password; confirm the password.
- (For Cisco IOS devices) Enter the enable password in the Device Login Password and in the Confirm Password fields. Leave the Device Login Name field blank.
- Click **Save**.

Example: If you have two devices in your network that have the same device logins and device passwords but have different enable passwords, you make three entries in the Add Device Login dialog box: enter the single device login and password, and then enter two enable passwords (each with the device login name field blank).

Step 8 Perform other actions as required:

- Click the **Add Device Login Information** button to add the login information to the device configuration.
- Select a login or series of log-ins from the list and click **Delete** to disable and remove them from the device configuration.
- Select a series of passwords from the list and click **Delete** to disable and remove them from the device configuration.
- Click **Cancel** to disregard the changes indicated and return to the New Device dialog box.

Step 9 Click **OK** to save the changes to the device configuration.

Delete a Device

To delete a device, complete the following steps:

Caution This action completely removes the device from the inventory and from all associated device groups.

Step 1 Select **Manage > Manage Devices** or click **Devices** in the Quick Links pane.

The Manage Devices explorer appears in the Content Area.

Step 2 Select the device you want to delete.

Step 3 Right-click on the selected device and click **Delete**.

A Delete Device dialog box appears.

Step 4 If you want to delete the device, click **Yes**. If you do not, click **No**.

Manage Devices Using Device Groups

Use device groups to organize devices according to a scheme that is meaningful to you. For example, you can organize devices by feature, region, or work site. A device can be present in more than one device group. If you do not want to create device groups, you must use the default device group, Default. Device groups can contain any number of devices.

Device group tasks are as follows:

- Add a Device Group, page 7-14
- Rename a Device Group, page 7-14
- Delete a Device Group, page 7-15
- Refresh the Device Group, page 7-15
- Add a Device to an Existing Device Group, page 7-15
- Remove a Device from a Device Group, page 7-16
- Move a Device to a Different Device Group, page 7-16

Add a Device Group

To add a new device group, complete the following steps:

Step 1 Select **Manage > Manage Devices** or click **Devices** in the Quick Links pane.

The Manage Devices explorer appears in the Content Area.

Step 2 Click the **New Group** button or select **Manage > New Device Group**.

The New Group dialog box appears.

Step 3 Enter the name of your new device group in the dialog box and click **OK**.

Your new device group name appears in the Manage Devices explorer.

Note For details about naming device groups, see Understand Naming Rules, page 9-7.

Rename a Device Group

To rename a device group, complete the following steps:

Step 1 Select **Manage > Manage Devices** or click **Devices** in the Quick Links pane.

The Manage Devices explorer appears in the Content Area.

Step 2 Right-click the device group and select **Rename Group**.

The Rename Group dialog box appears.

Step 3 Enter the device group's new name.

Step 4 Click **OK**.

Your new device group name appears in the Manage Devices explorer.

Note For details about naming device groups, see Understand Naming Rules, page 9-7.

Delete a Device Group

To delete a device group, complete the following steps:

Step 1 Select **Manage > Manage Devices** or click **Devices** in the Quick Links pane.

The Manage Devices explorer appears in the Content Area.

Step 2 Right-click the device group and select **Delete**.

The Delete Group dialog box appears.

Step 3 If you want to delete the device group, click **Yes**. If you do not, click **No**.

Note If the device group you are deleting contains a device that does not belong to any other device group, the device will be moved to the default device group.

Refresh the Device Group

You can refresh the contents of an existing device group by selecting the device group. Right-click to select **Refresh**.

The folder redisplays with updated contents.

Add a Device to an Existing Device Group

Adding a device to an existing device group creates a copy of the device that will be placed in the device group you choose. This operation allows you to store devices in more than one device group. For example, you could create a feature-based device group and a group based on a specific work site.

To add a device to an existing device group, complete the following steps:

Step 1 Select **Manage > Manage Devices** or click **Devices** in the Quick Links pane.

The Manage Devices explorer appears in the Content Area.

Step 2 Right-click the device and select **Add to Group**.

The Select Group dialog box appears.

Step 3 From the drop-down list, select the device group to which you would like to add the device.

Step 4 Click **OK**.

Remove a Device from a Device Group

Devices are removed only from the selected device group and not from other device groups they may be in.

To remove a device from a device group, complete the following steps:

Step 1 Select **Manage > Manage Devices** or click **Devices** in the Quick Links pane.

The Manage Devices explorer appears in the Content Area.

Step 2 Right-click the device and select **Remove from Group**.

The Remove from Group dialog box appears.

Step 3 If you want to remove the device from the device group, click **Yes**. If you do not, click **No**.

Note To be removed from a device group, a device must be part of another device group.

Move a Device to a Different Device Group

You can move a device from one device group into another device group. Moving a device from one device group to another removes the device from the original device group unless you use the copy function.

To move a device to another device group, complete the following steps:

Step 1 Select **Manage > Manage Devices** or click **Devices** in the Quick Links pane.

The Manage Devices explorer appears in the Content Area.

Step 2 Right-click the device and select **Move to Group**.

The Move to Group dialog box appears.

Step 3 From the drop-down list, select the device group to which you would like to move this device.

Step 4 Click **OK**.

To move multiple devices to another device group, complete the following steps:

Step 1 Select **Manage > Manage Devices** or click **Devices** in the Quick Links pane.

The Manage Devices explorer appears in the Content Area.

Step 2 Select one or more devices in one group and drag them together into another group.

Note If you keep the Control key pressed while dragging devices, the selected devices are copied into the group to which you drag them rather than being removed from the original group.

Find a Device

Use the Find feature to locate a PAK or device. To find a PAK or device, complete the following steps:

Step 1 Click **Edit > Find**.

The Find a PAK/Device dialog box appears.

Step 2 To find a PAK, check the Find PAK check box. Type in the PAK name or ID.

Step 3 To find a device, check the Find Device check box. Type in the information you want to search for and choose device name, IP address, hostname, or UDI.

Step 4 If you want to match the case exactly, select **Match Case**.

Step 5 If you want to wrap the search text, select **Wrap Search**.

Note The search starts from the selected PAK and proceeds downward in the Manage PAK screen. If it reaches the last PAK in the tree and **Wrap Search** is enabled, the search continues from the top of the PAK tree.

Step 6 Click **Find**.

View Device Properties

Each device has properties associated with it.

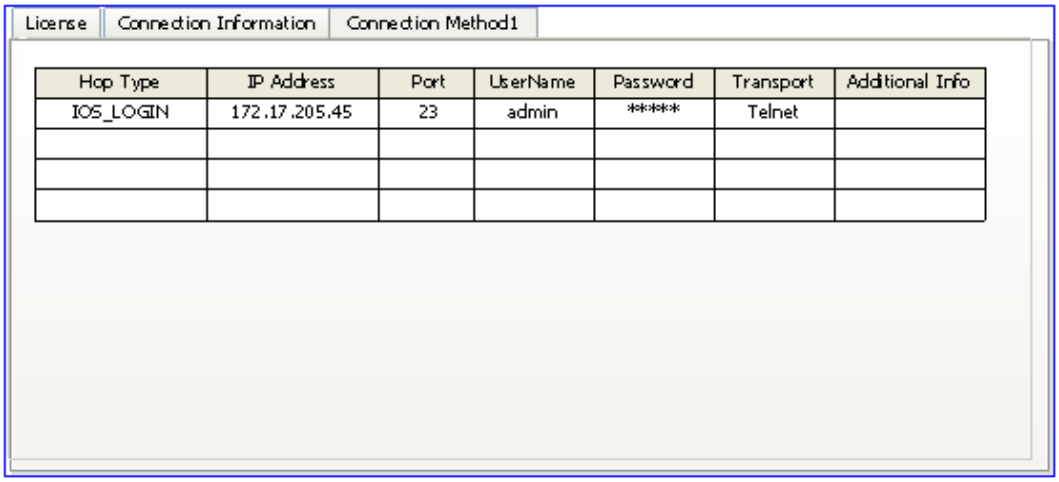
To view device properties, complete the following steps:

Step 1 Select **Manage > Manage Devices** or click **Devices** in the Quick Links pane.

The Manage Devices explorer appears in the Content Area.

Step 2 Right-click the device and select **Properties**.

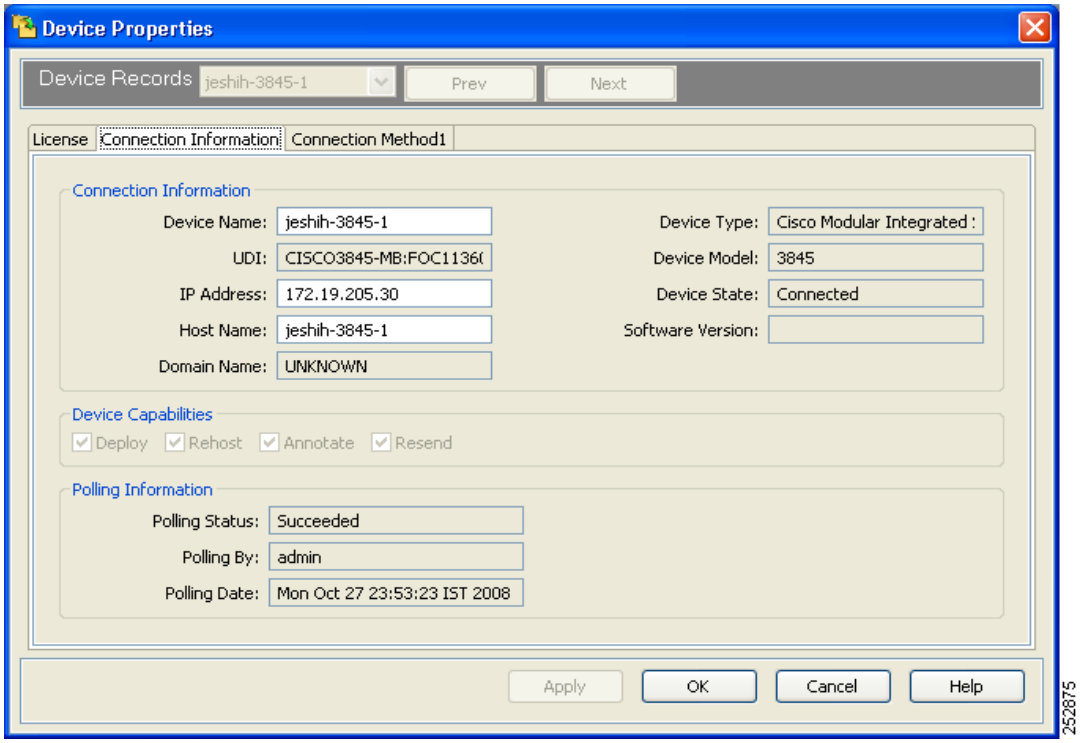
The Device Properties dialog box appears.



Step 3 To view the device's license information, select the **License** tab. The information on this tab is read-only.

Step 4 To view connection information, select the **Connection Information** tab.

The Connection Information dialog box appears.

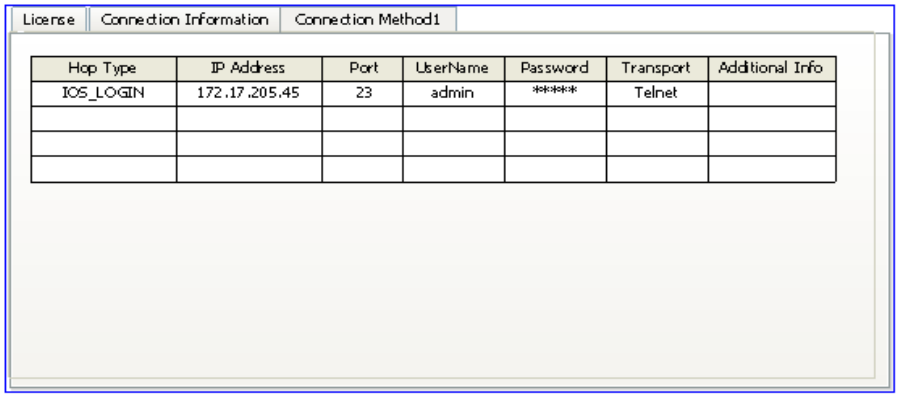


Step 5 To change connection information about the device and the capabilities that you want to provide for it, enter the new information, and click **Apply**.

Step 6 To view information about the connection method, select the **Connection Method** tab.

The Connection Method page appears. The information on this page is read-only.

Note If there are one or more connection platforms, a connection method tab is displayed for each platform.



Step 7 To close the Device Properties dialog box, click **OK**.

Update Device Information

Use Poll Licenses to collect up-to-date information (such as license expiry) on existing Cisco devices and to synchronize the information in the device inventory.

Cisco License Manager synchronizes licenses using two methods:

- GUI—Use **Poll Licenses** to update the license information.
- API—Use the PollDevicesLicenseInfo call to provide the list of devices.

To update device information, complete the following steps:

Step 1 Select **Manage > Manage Devices** or click **Devices** in the Quick Links pane.

The Manage Devices explorer appears in the Content Area.

Step 2 Right-click the device and select **Poll Licenses**.

The Poll Licenses dialog box appears.

Step 3 Click **Yes**.

A status window appears. If you get any error messages, verify that your device UDI and IP address are entered correctly.

Step 4 Once the process is complete, a confirmation window appears. Click **OK** to close the window.

Assign an Access Control List to Device Groups and Devices

The Edit Access Control List dialog box appears when you select a device or device group, right-click, and choose **Assign Access Control List**.

Use this dialog box to assign user access to devices or device groups. Only administrators can change the access list.

This dialog box displays a list of Cisco License Manager usernames, each with a check box in front of it. If the box is checked, the user has access to the devices and device groups. If it is unchecked, the user does not have access.

If no username is checked and **Allow None** is checked, only administrators are allowed access to the groups. If **Allow None** is not checked, all users are allowed access to the groups.

Check Device Connectivity

Use the Check Device Connection feature to check for connectivity between Cisco License Manger and a device using the current configuration method (HTTP, SSH, or Telnet).

To check device connectivity, complete the following steps:

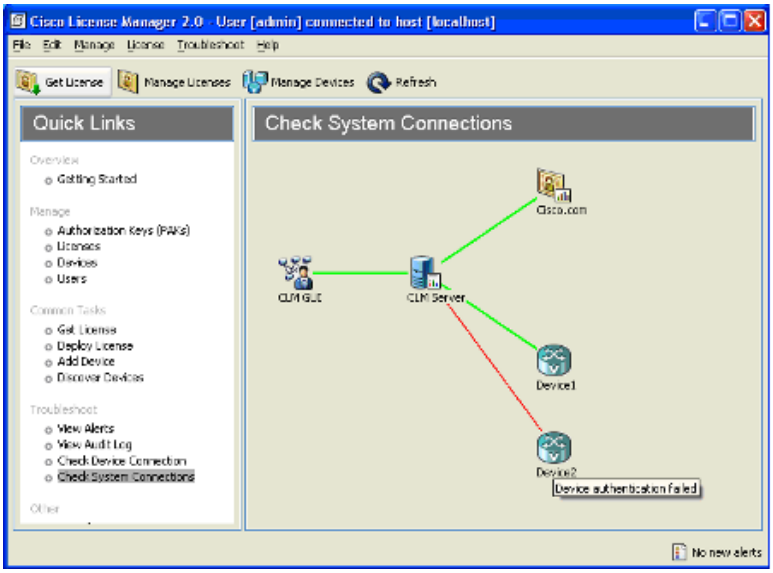
Step 1 To check device connection, either

- Click **Troubleshoot > Check Device Connection** or **Check Device Connection** in the Quick Links pane. The Select Device dialog box appears. Select the device you want to check and click **OK**.

or

- Right-click the device and select **Check System Connections**. The Check System Connections dialog box appears. Click **Yes**.

  The Check System Connections window appears.



Note From Manage Devices, you may select one or more devices to bring up Check System Connections. The graphic indicates the connections from Cisco License Manager Server to each selected device. A green link represents a successful check of the connection by the Cisco License Manager Server. A red link shows that the indication connection could not be verified by the Cisco License Manager Server.

Step 2 Once the connection has been checked, a popup window appears stating the results of the task. Click **Close**.

Manage PAKs

This section provides the following information about managing PAKs:

Add a PAK

To deploy a license to a device, you must provide a valid PAK so that a license can be obtained from Cisco.com for the device. To add a new PAK, complete the following steps:

Tip Before you do this, be sure to enter your Cisco.com password in your user profile.

Step 1 Select **Manage > Manage Authorization Keys (PAK)** or click **Authorization Keys (PAKs)** in the Quick Links pane.

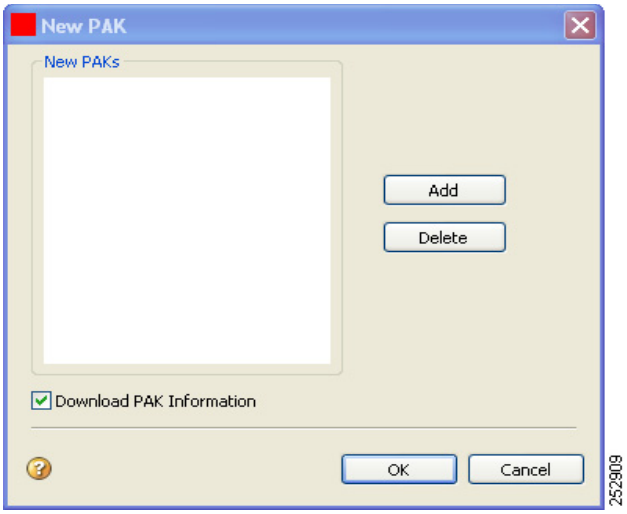
The Manage PAKs explorer appears in the Content Area.

Step 2 Select an existing PAK folder to which you want to add a new PAK.

Make sure to select a folder that makes sense to you so that you can easily locate and retrieve PAK and SKU information later.

Step 3 With the folder selected, right-click and choose **New PAK**.

The New PAK dialog box appears.



Step 4 Check the **Download PAK Information** check box if you want the PAK information to be downloaded when you add the new PAK.

Step 5 Click **Add**. The New PAK Name dialog box appears.

Step 6 Enter the PAK name and click **OK**. The new PAK appears in the New PAKs pane of the New PAK dialog box.

Note You should have received your PAK with your shipment or from Cisco via e-mail if you ordered software upgrades. If you want to add more PAKs, repeat Steps 3 and 4.

Step 7 Verify the new PAKs as they appear in the New PAKs pane of the New PAK dialog box and click **OK**.

Step 8 Enter the PAK from the device and click **OK**.

The PAK appears in the folder you selected. Passwords and PAKs stored in Cisco License Manager are encrypted.

Delete a PAK

You cannot delete a PAK that has licenses associated with it. To delete a PAK, complete the following steps:

Step 1 Select **Manage > Manage Authorization Keys (PAK)** or click **Authorization Keys (PAKs)** in the Quick Links pane.

The Manage PAKs explorer appears in the Content Area.

Step 2 Select an existing PAK that you want to delete.

Step 3 Right-click and select **Delete**.

The Delete PAK dialog box appears.

Step 4 Click **Yes** to confirm the deletion of this PAK.

The PAK is removed from the folder.

Manage PAKS Using Folders

Use folders to organize PAKs by any method that is convenient and logical to you. Folder management tasks are as follows:

Add a PAK Folder

To add a new PAK folder, complete the following steps:

Timesaver You can skip this procedure if you want to use the Default PAK folder.

Step 1 Select **Manage > Manage Authorization Keys (PAK)** or click **Authorization Keys (PAKs)** in the Quick Links pane.

The Manage PAKs explorer appears in the Content Area.

Step 2 Click the **New Folder** button.

The New Folder dialog box appears.

Step 3 Enter the name of your new PAK folder in the dialog box and click **OK**.

Your new PAK folder name appears in the Manage PAKs explorer.

Note For details about naming PAK folders, see "Naming Rules" section on page 9-7.

Rename a PAK Folder

To rename a PAK folder, complete the following steps:

Step 1 Select **Manage > Manage Authorization Keys (PAK)** or click **Authorization Keys (PAKs)** in the Quick Links pane.

The Manage PAKs explorer appears in the Content Area.

Step 2 Right-click the PAK folder and select **Rename Folder**.

The Rename Folder dialog box appears.

Step 3 Enter the folder's new name.

Step 4 Click **OK**.

Your new PAK folder name appears in the Manage PAKs explorer.

Note For details about naming device groups, see "Naming Rules" section on page 9-7.

Delete a PAK Folder

To delete a PAK folder, complete the following steps:

Step 1 Select **Manage > Manage Authorization Keys (PAK)** or click **Authorization Keys (PAKs)** in the Quick Links pane.

The Manage PAKs explorer appears in the Content Area.

Step 2 Right-click the PAK folder and select **Delete**.

The Delete Folder dialog box appears.

Step 3 If you want to delete the PAK folder, click **Yes**. If you do not, click **No**.

Note If the folder you are deleting contains a PAK that does not belong to another folder, the PAK will be moved to the default folder.

Refresh the PAK Folder

You can refresh the contents of an existing PAK folder by selecting the folder. Right-click to select **Refresh**.

The folder redisplays with updated contents.

Add a PAK to an Existing Folder

Adding a PAK to an existing folder creates a copy of the PAK that will be placed in the folder you choose. This operation allows you to store PAKs in more than one folder. For example, you could create a feature-based PAK folder and a folder based on a specific work site.

To add a PAK to an existing PAK folder, complete the following steps:

Step 1 Select **Manage > Manage Authorization Keys (PAK)** or click **Authorization Keys (PAKs)** in the Quick Links pane.

The Manage PAKs explorer appears in the Content Area.

Step 2 Right-click the PAK and select **Add to Folder**.

The Select Folder dialog box appears.

Step 3 From the drop-down list, select the PAK folder to which you would like to add the PAK.

Step 4 Click **OK**.

Remove a PAK from a Folder

PAKs are removed only from the selected folder and not from other folders they may be in.

To remove a PAK from a PAK folder, complete the following steps:

Step 1 Select **Manage > Manage Authorization Keys (PAK)** or click **Authorization Keys (PAKs)** in the Quick Links pane.

The Manage PAKs explorer appears in the Content Area.

Step 2 Right-click the PAK and select **Remove from Folder**.

The Remove from Folder dialog box appears.

Step 3 If you want to remove the PAK from the PAK folder, click **Yes**. If you do not, click **No**.

Note If the PAK you are removing is not located in another folder, it will be moved to the default folder.

Move a PAK to a Different Folder

You can move a PAK from one folder into another folder. Moving a PAK from one folder to another removes the PAK from the original folder.

To move a PAK to another PAK folder, complete the following steps:

Step 1 Select **Manage > Manage Authorization Keys (PAK)** or click **Authorization Keys (PAKs)** in the Quick Links pane.

The Manage PAKs explorer appears in the Content Area.

Step 2 Right-click the PAK and select **Move to Folder**.

The Move to Folder dialog box appears.

Step 3 From the drop-down list, select the PAK folder to which you would like to move this PAK.

Step 4 Click **OK**.

To move multiple PAKs to a different folder, complete the following steps:

Step 1 Select **Manage > Manage Authorization Keys (PAK)** or click **Authorization Keys (PAKs)** in the Quick Links pane.

The Manage PAKs explorer appears in the Content Area.

Step 2 Select one or more PAKs in one folder and drag them together into another folder.

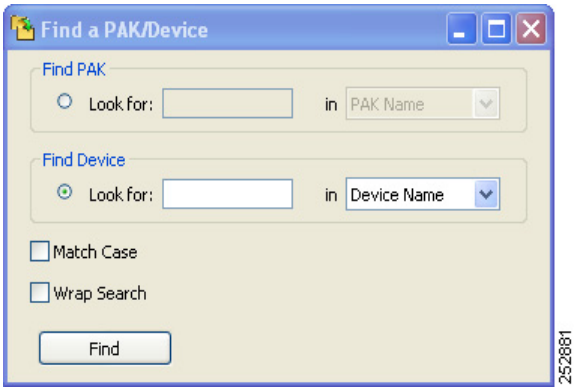
Note If you keep the Control key pressed while dragging PAKs, the selected PAKs are copied into the group to which you drag them.

Find a PAK

Use the Find feature to locate a PAK or device. To find a PAK or device, complete the following steps:

Step 1 Click **Edit > Find**.

The Find a PAK/Device dialog box appears.



Step 2 To find a PAK, check the Find PAK check box. Type in the PAK name or ID.

Step 3 To find a device, check the Find Device check box. Type in the information you want to search for and choose device name, IP address, hostname, or UDI.

Step 4 If you want to match the case exactly, select **Match Case**.

Step 5 If you want to wrap the search text, select **Wrap Search**.

Note The search starts from the selected PAK and proceeds downward in the Manage PAK screen. If it reaches the last PAK in the tree and **Wrap Search** is enabled, the search continues from the top of the PAK tree.

Step 6 Click **Find**.

View PAK Properties

Each PAK has properties associated with it.

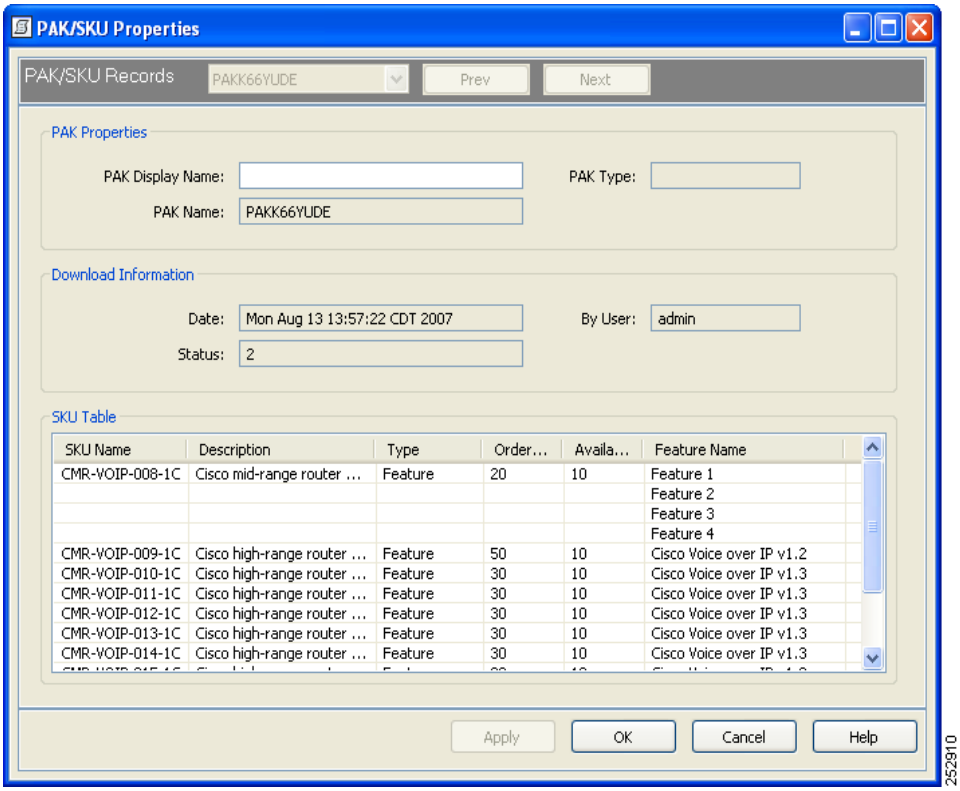
To view PAK properties, complete the following procedures:

Step 1 Select **Manage > Manage Authorization Keys (PAK)** or click **Authorization Keys (PAKs)** in the Quick Links pane.

The Manage PAKs explorer appears in the Content Area.

Step 2 Right-click the PAK and select **Properties**.

The PAK/SKU Properties dialog box appears.



The only properties field that is not read-only is the PAK Display Name.

Note For further information about the fields in the PAK Properties dialog box, see the "View PAK Properties" section on page 7-27.

Step 3 To change the PAK Display Name, enter the new information and click **Apply**.

Step 4 To close the PAK/SKU Properties dialog box, click **OK** or **Cancel**.

Download PAK Information

The PAK/SKU Properties dialog box appears when you select a PAK in the Manage PAKs explorer pane, right-click, and choose **Properties**.

Tip If you choose more than one PAK, you can scroll through the PAK properties by clicking the **Prev** and **Next** buttons in the PAK/SKU Properties dialog box.

Use this window to change a PAK display name, display PAK information, and list the SKUs associated with a PAK. The window is divided into three sections: PAK Properties, Download Information, and SKU Table.

The following table describes the fields of the PAK/SKU Properties dialog box:

Field	Description
PAK Properties	
PAK Display Name	Display name for the PAK. Can be named something unique to identify it in the Manage PAKs explorer. For information about naming rules, see the "Understand Naming Rules" section on page 9-7.
PAK Name	PAK identification that comes with each product. Can be viewed with any serial number lookup tool.
PAK Type	Type of PAK obtained from the Cisco Product License Registration Portal. Value could be SINGLE or PARTIAL. If the PAK Type is single fulfillment (SF), all the SKUs for this PAK are grouped as one. For example, if you specify any SKU, all SKUs are selected. Therefore, if a license is obtained for a device, all the SKUs will be licensed to the device specified. If the PAK Type is partial fulfillment (PF), each of the SKUs for this PAK is treated as an individual license. For example, if you specify one of these SKUs, only that SKU is selected. Therefore, if a license is obtained for a device, that one SKU will be licensed to the device specified.
Download Information	
Date	Date and time that the PAK was last downloaded. Time comes from the server system.
Status	Status of last download. Value is always 0 (not polled).
By User	Username of the person who initiated the download.
SKU Table	
SKU Name	An identification, usually alphanumeric, of a particular product that allows it to be tracked for inventory purposes. Usually maps to license features.

Field	Description
Description	Cisco device description assigned by the Cisco Product License Registration Portal. Includes SKU name and type.
Type	Defines what type of PAK information is displayed. Value will always be Feature.
Ordered Qty	Number of licenses purchased.
Available Qty	Number of licenses available for deployment.
Feature Name	Cisco IOS feature description.

Assign an Access Control List to PAKs

The Edit Access Control List window appears when you select a PAK, right-click, and choose **Assign Access Control List**.

Use this dialog box to assign user access to PAKs. Only a user with an Administrator role or a PAK owner can change the access list.

This dialog box displays a list of Cisco License Manager usernames, each with a check box in front of it. If the box is checked, the user has access to the PAKs. If it is unchecked, the user does not have access.