Updating Device Inventory

Cisco Prime Infrastructure provides two ways to discover the devices in your network:

- Quick—Allows you to quickly discover the devices in your network based on the SNMP community string, seed IP address, and subnet mask you specify. Choose **Operate > Discovery**, then click **Quick Discovery**.
- Regular—Allows you to specify protocol, credential, and filter settings, and schedule the discovery job. See Changing Discovery Settings, page 12-1.

Changing Discovery Settings

Step 1 Choose **Operate > Discovery**, then click **Discovery Settings**.

Step 2 Click **New**. Enter the settings as described in Table 3-1.

Step 3 Click one of the following:

- **Save** to save the settings.
- **Run Now** to save the settings and immediately start the discovery job.

Scheduling Discovery Jobs

To create a discovery job to run at a future time:

Step 1 Choose **Operate > Discovery**, click **Discovery Settings**, then click **New**.

Step 2 Enter the required settings, then click **Save**. For descriptions of the template parameters, see the *Cisco Prime Infrastructure 2.0 Reference Guide*.

Step 3 In the Discovery Settings, select the discovery job that you just created, then click **Schedule**.

Step 4 Enter the schedule information page, then click **Save**.

Monitoring the Discovery Process

To monitor the discovery process:

Step 1 Choose **Operate > Discovery**.

Step 2 Select the discovery job for which you want to see details.

Discovery Protocols and CSV File Formats

Prime Infrastructure uses the following protocols to discover devices:

- Ping Sweep
- Cisco Discovery Protocol (CDP)
- Routing Table
- Address Resolution Protocol (ARP)
- Border Gateway Protocol (BGP)
- Open Shortest Path First (OSPF)

You can import a CSV file to add data for the protocols. Table 12-1 describes the CSV file format for each of the protocols.

Note You can import a CSV file if you are using a supported version of Mozilla Firefox only.

Table 12-1 Discovery Protocols and CSV File Formats

Protocol	CSV File Format
Ping sweep	Any valid IP address and subnet mask, separated by a comma. You can specify multiple networks in a single discovery by adding additional rows.
Cisco Discovery Protocol (CDP)	Any valid IP address and the hop count, separated by a comma.
Routing table	Any valid IP address and the hop count, separated by a comma.
Address Resolution Protocol (ARP)	Any valid IP address and the hop count, separated by a comma.

Table 12-1 Discovery Protocols and CSV File Formats

Protocol	CSV File Format
Border Gateway Protocol (BGP)	Seed device IP address for any device that is BGP enabled.
Open Shortest Path First (OSPF)	Seed device IP address for any device that is OSPF enabled.

Updating Device Inventory Manually

We recommend that you run discovery to update your device inventory. However, you can also add devices manually, if needed.

To update the device inventory manually:

Step 1 Choose **Operate > Device Work Center**, then click **Add**.

Step 2 Enter the required parameters.

Step 3 Click **Add** to add the device with the settings that you specified.

Importing Device Inventory

If you have another management system to which your devices are to be imported or if you want to import a spreadsheet that contains all your devices and their attributes, you can import device information in bulk into Prime Infrastructure.

To import device inventory:

Step 1 Choose **Operate > Device Work Center**, then click **Bulk**.

Step 2 Click the link to download a sample file that contains all of the fields and descriptions for the information that must be contained in your imported file.

Step 3 Click **Browse** to navigate to your file, then click **Import** and wait for the import to complete. (To check the status of the import, choose **Administration > Jobs Dashboard**).

Troubleshooting Unmanaged Devices

Table 12-2 describes the possible reasons a device is unmanageable by Prime Infrastructure:

Table 12-2 Reasons for Unmanageable Device

Possible Reason	Actions
Prime Infrastructure cannot reach the device because the device is down or because any device along the path from the Prime Infrastructure server to the device is down.	• Use the ping and traceroute tools to verify that Prime Infrastructure can reach the device. See Getting Device Details from the Device 360° View for more information. • If the device is reachable, verify that the retry and timeout values set for the device are sufficient. (Choose **Operate > Device Work Center**, select the device, then click **Edit**.) • Verify that SNMP is configured and enabled on the device: – If using SNMPv2, verify that the *read-write* community string configured on the device is the same as that entered in Prime Infrastructure. The read-write community string is required. – If using SMNPv3, verify that the following parameters are configured on the device, and that the configured parameters match those entered in Prime Infrastructure: Username AuthPriv mode (noAuthNoPriv, authNoPriv, authPriv) Authentication algorithm (for example: MD5, SHA) Authentication password Privacy algorithm (for example: AES, DES) Privacy password • Verify that the SNMP credentials configured on the device match the SNMP credentials configured in Prime Infrastructure. • Reenter the SNMP credentials in Prime Infrastructure, then resynchronize the device. (Choose **Operate > Device Work Center**, select the device, then click **Sync**.) See Synchronizing Devices for more information.
Prime Infrastructure cannot gather information from the device because Telnet or SSH is not configured on the device.	• Verify that Telnet or SSH is configured and enabled on the device, and that the same protocol is configured on Prime Infrastructure. (Choose **Operate > Device Work Center**, select the device, then click **Edit**.) If the device type requires HTTP, verify that the Prime Infrastructure HTTP parameters match those configured on the device. • Verify that the username, Telnet or SSH passwords, and enable mode password for Cisco IOS devices are configured correctly on the device and that the parameters entered in Prime Infrastructure match those configured on the device. (If you did not configure a username on the device for authentication, you can leave this field empty in Prime Infrastructure.) • Verify that the authorization level configured for the Telnet/SSH user is not limited to lower enable privilege levels.

Table 12-2 Reasons for Unmanageable Device (continued)

Possible Reason	Actions
Restrictions were placed for SNMP through SNMP views or access lists.	Remove any restrictions for SNMP through SNMP views or access lists.
TACACS+ "per-command authorization" is configured on the devices.	If TACACS+ is configured, verify the permissions for the Telnet/SSH user for the permitted CLI commands. We recommend that you allow all CLI commands for the Prime Infrastructure user account; or alternatively, exclude only commands that absolutely must be restricted.

For more information about configuring SNMP, Telnet, and SSH on Cisco IOS devices, see:

- Cisco IOS Software Releases 12.0 T SNMPv3
- Configuring Secure Shell on Routers and Switches Running Cisco IOS

Managing Device Groups

Device groups are logical groupings of devices. You create device groups to help you more efficiently update and manage your devices. For example, you can create a device group that includes devices that have a particular module. If you later want to configure a feature related specifically to that module, you use the device group that you created to push the configuration change to all of the devices contained in the group.

By default, Prime Infrastructure creates rule-based device groups and assigns devices to the appropriate Device Type folder. You cannot edit these device groups. You can view the rules for a device group by hovering your mouse on the device group folder.

You can create a new group that can be one of two types:

- Static—Add devices to a static group using the **Add to Group** button from **Operate > Device Work Center**.
- Dynamic—Specify the rules to which devices must comply to be added to this device group. See Creating Dynamic Device Groups for more information.

When you create a device group, you are distinguishing that group of devices from others in your network. For example, if you have devices that reside in different time zones, you can create device groups based on geographic regions so that the devices in one group can have a different time zone setting from the devices in another group.

In smaller deployments where all devices can be configured with the same settings, you may only need to create one general device group. This setup allows you to configure settings for the group, and then apply those settings consistently across all your devices.

Device groups not only save you time when configuring multiple devices, but they also ensure that configuration settings are applied consistently across your network.

Note You cannot control which users have access to which device groups. All users can see all device groups. For role-based access control (RBAC), you need to create sites and virtual domains.

Creating device groups is a two-part process:

1. Create a new device group. See Creating Dynamic Device Groups.

2. Assign devices to the device group. See Assigning Devices to a Group.

Related Topic

- Device Accessibility in Parent-Child Device Groups

Device Accessibility in Parent-Child Device Groups

When you create a child group under a parent device group, the devices accessible to the child group depend on the device group you create:

- If the parent and child group are *both dynamic* device groups, the child group can access the devices available in the parent group only.
- If the parent group is a *static* device group and the child group is a dynamic group, the child group is not limited to the devices available in the parent group.

In dynamic device groups only, the child group "inherits" its devices from the parent device group.

Related Topics

- Creating Dynamic Device Groups
- Assigning Devices to a Group

Creating Dynamic Device Groups

Before you create a dynamic device group, make sure you understand the unique properties that you want the group to contain. For example, you may want to set up two device groups that have different authentication settings or different time zone settings.

Note While there is no limit to the number of rules you can specify for a dynamic group, as the number of rules increases, the group update performance could become slower.

To create a dynamic device group:

Step 1 Choose **Operate > Device Work Center**.

Step 2 In the Groups menu on the left, click the Settings icon, then click **Create Group**.

Step 3 Enter the group name and group description, and select a parent group, if applicable.

Note The group name and description should not be more than 255 characters.

Step 4 Deselect **Static Group** so that you can specify the rules to which all devices must comply to be added to the group, or if you want to manually add the devices to the group; this means that the group will *not* be rule-based.

Step 5 Specify the rules that you want to apply to the devices in the group.

Note You can create a rule using the UDF label defined in Administration > System Settings > User Defined Field.

Step 6 Click **Save** to add the device group with the settings you specified.

The device group that you created appears under the user-defined groups.

Assigning Devices to a Group

Step 1 Choose **Operate > Device Work Center**.

Step 2 Select the device that you want to assign to a group, then click **Add To Group**.

Step 3 Select a group, then click **Save**.

Synchronizing Devices

To synchronize the Prime Infrastructure database with the configuration running on a device, you can force an inventory collection.

Step 1 Choose **Operate > Device Work Center**.

Step 2 Select the device whose configuration you want synchronized with the configuration stored in the Prime Infrastructure database.

Step 3 Click **Sync**.