



Add and Organize Devices

This chapter contains the following topics:

- [Add Devices to , on page 1](#)
- [Import Devices from Another Source, on page 5](#)
- [Create Device Import CSV Files, on page 6](#)
- [Add Devices Manually \(New Device Type or Series\), on page 7](#)
- [Prerequisites for Adding Wireless Controllers, on page 10](#)
- [Validate Added Devices and Troubleshoot Problems, on page 10](#)
- [Add NAM HTTP/HTTPS Credentials, on page 14](#)
- [Export Device Information to a CSV File, on page 15](#)
- [Apply Device Credentials Consistently Using Credential Profiles, on page 16](#)
- [Create Groups of Devices for Easier Management and Configuration, on page 18](#)

Add Devices to

uses device, location, and port groups to organize elements in the network. When you view devices in a table or on a map (network topology), the devices are organized in terms of the groups they belong to. When a device is added to , it is assigned to a group named Unassigned Group. You can then move the device into the desired groups as described in [Create Groups of Devices for Easier Management and Configuration, on page 18](#).

Table 1: Methods for Adding Devices

Supported Methods for Adding Devices	See:
Add multiple devices by discovering the neighbors of a seed device using:	Add Devices Using Discovery, on page 2 .
<ul style="list-style-type: none"> • Ping sweep and SNMP polling (Quick Discovery) 	<ul style="list-style-type: none"> • Run Quick Discovery, on page 3
<ul style="list-style-type: none"> • Customized protocol, credential, and filter settings (useful when you will be repeating the discovery job) 	<ul style="list-style-type: none"> • Run Discovery with Customized Discovery Settings, on page 4
Add multiple devices using the settings specified in a CSV file	

Supported Methods for Adding Devices	See:
Add a single device (for example, for a new device type)	Add Devices Manually (New Device Type or Series), on page 7

Understand the Discovery Process

Prime Infrastructure performs the following steps during the discovery process:

1. Using ICMP ping, determine if each device is reachable. If Prime Infrastructure is unable to reach the device, the device Reachability status is Unreachable.
2. Verify the SNMP credentials. If the device is reachable by ICMP, but the SNMP credentials are not valid, the device Reachability status is Ping Reachable.
If the device is reachable by both ICMP and SNMP, the device Reachability status is Reachable .
3. Verify Telnet and SSH credentials.
4. Modify the device configuration(s) to add a trap receiver in order for Prime Infrastructure to receive the necessary notifications.
5. Start the inventory collection process to gather all device information.
6. Add the devices to the Inventory > Network Devices page.

After running discovery, choose Inventory > Device Management > Network Devices to verify that discovery is complete.

Add Devices Using Discovery

supports two discovery methods:

- Ping sweep from a seed device (Quick Discovery). The device name, SNMP community, seed IP address and subnet mask are required. See [Run Quick Discovery, on page 3](#)
- Using customized discovery methods (Discovery Settings)—This method is recommended if you want to specify settings and rerun discovery in the future. See [Run Discovery with Customized Discovery Settings, on page 4](#).



Note

- If a discovery job rediscovers an existing device and the device's last inventory collection status is Completed, does not overwrite the existing credentials with those specified in the Discovery Settings. For all other statuses (on existing devices), overwrites the device credentials with those specified in the Discovery Settings.
- Service discovery might take longer than usual when a large number of devices is added during database maintenance windows. Therefore, we recommend that you avoid large-scale operations during the night and on weekends.
- Autonomous APs are filtered out of the discovery process to optimize the discovery time. You need to manually add Autonomous APs using Import Devices or Credential Profile.

The discovery process of a device is carried out in the sequence of steps listed below. As performs discovery, it sets the reachability state of a device, which is: Reachable, Ping Reachable, or Unreachable. A description of the states is provided in [Device Reachability and Admin States, on page 12](#).

1. determines if a device is reachable using ICMP ping. If a device is not reachable, its reachability state is set to Unreachable.
2. Server checks if SNMP communication is possible or not.
 - If a device is reachable by ICMP but its SNMP communication is not possible, its reachability state is set to Ping Reachable.
 - If a device is reachable by both ICMP and SNMP, its reachability state is Reachable.
3. Verifies the device's Telnet and SSH credentials. If the credentials fail, details about the failure are provided in the Network Devices table in the Last Inventory Collection Status column (for example, Wrong CLI Credentials). The reachability state is not changed.
4. Modifies the device configuration to add a trap receiver so that can receive the necessary notifications (using SNMP).
5. Starts the inventory collection process to gather all device information.
6. Displays all information in the web GUI, including whether discovery was fully or partially successful.



Note When verifies a device's SNMP read-write credentials, the device log is updated to indicate that a configuration change has been made by (identified by its IP address).

Specify the Management IP Address Type (IPv4/IPv6) for Discovered Devices

For discovered dual-home (IPv4/IPv6) devices, specify whether you want to use IPv4 or IPv6 addresses for management IP addresses.

-
- Step 1** Choose Administration > Settings > System Settings, then choose Inventory > Discovery.
- Step 2** From the IPv4/IPv6 Preference for Management Address drop-down list, choose either v4 or v6.
- Step 3** Click Save.
-

Run Quick Discovery

Use this method when you want to perform a ping sweep using a single seed device. Only the device name, SNMP community, seed IP address and subnet mask are required. If you plan to use the configuration management features, you must provide the protocol, user name, password, and enable password.

-
- Step 1** Choose Inventory > Device Management > Discovery, then click the Quick Discovery link at the top right of the window.
- Step 2** At a minimum, enter the name, SNMP community, seed IP address, and subnet mask.

Step 3 Click Run Now.

What to do next

Click the job hyperlink in the Discovery Job Instances area to view the results.

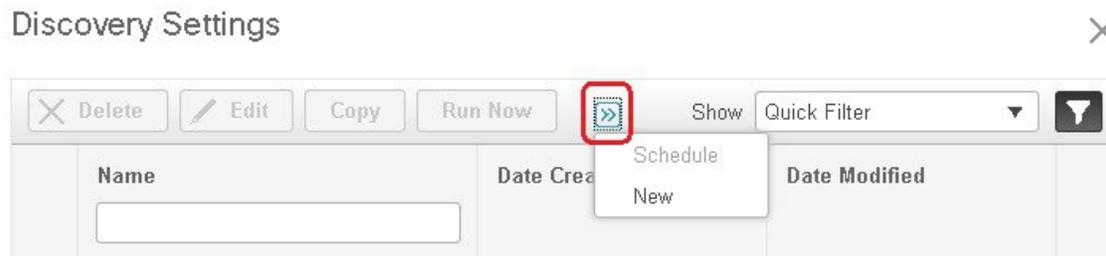
Run Discovery with Customized Discovery Settings

can discover network devices using discovery profiles. A discovery profile contains a collection of settings that instructs how to find network elements, connect to them, and collect their inventory. For example, you can instruct to use CDP, LLDP, OSPF to discover devices, or just perform a simple ping sweep (an example of the results of a ping sweep is provided in [Sample IPv4 IP Addresses for Ping Sweep, on page 4.](#)) You can also create filters to fine-tune the collection, specify credential sets, and configure other discovery settings. You can create as many profiles as you need.

After you create a profile, create and run a discovery job that uses the profile. You can check the results of the discovery job on the Discovery page. You can also schedule the job to run again at regular intervals.

Step 1 Choose Inventory > Device Management > Discovery, then click the Discovery Settings link at the top right of the window. (If you do not see a Discovery Settings link, click the arrow icon next to the Quick Discovery link.)

Step 2 In the Discovery Settings pop-up, click New.



Step 3 Enter the settings in the Discovery Settings window. Click "?" next to a setting to get information about that setting. For example, if you click "?" next to SNMPv2 Credential, the help pop-up provides a description of the protocol and any required attributes.

Step 4 Click Run Now to run the job immediately, or Save to save your settings and schedule the discovery to run later.

Sample IPv4 IP Addresses for Ping Sweep

The following table provides an example of the results of a ping sweep.

Subnet Range	Number of Bits	Number of IP Addresses	Sample Seed IP Address	Start IP Address	End IP Address
255.255.240.0	20	4094	205.169.62.11	205.169.48.1	205.169.63.254
255.255.248.0	21	2046	205.169.62.11	205.169.56.1	205.169.63.254
255.255.252.0	22	1022	205.169.62.11	205.169.60.1	205.169.63.254

255.255.254.0	23	510	205.169.62.11	205.169.62.1	205.169.63.254
255.255.255.0	24	254	205.169.62.11	205.169.62.1	205.169.63.254
255.255.255.128	25	126	205.169.62.11	205.169.62.1	205.169.63.127
255.255.255.192	26	62	205.169.62.11	205.169.62.1	205.169.63.62
255.255.255.224	27	30	205.169.62.11	205.169.62.1	205.169.63.30
255.255.255.240	28	14	205.169.62.11	205.169.62.1	205.169.63.14
255.255.255.248	29	6	205.169.62.11	205.169.62.9	205.169.63.14
255.255.255.252	30	2	205.169.62.11	205.169.62.9	205.169.63.10
255.255.255.254	31	0	205.169.62.11		
255.255.255.255	32	1	205.169.62.11	205.169.62.11	205.169.62.11

Verify Discovery

When discovery is completed, you can verify if the process was successful.

To verify successful discovery, follow these steps:

-
- Step 1** Choose Inventory > Device Management > Discovery.
 - Step 2** Choose the discovery job for which you want to view details.
 - Step 3** Choose User Jobs > Discovery from the left navigation pane and select the specific job.
 - Step 4** Under Discovery Job Instances, expand the arrow to view details about the devices that were discovered.

If devices are missing:

- Change your discovery settings, then rerun the discovery.
- Add devices manually. See [Add Devices Manually \(New Device Type or Series\)](#), on page 7 for more information.

The Discovery Job Instances section now displays Export and Refresh buttons. You can export the job information as both PDF and CSV.

Import Devices from Another Source

If you have another management system from which you want to import your devices, or if you want to import a spreadsheet that lists all of your devices and their attributes, you can add device information into by importing a bulk device file. You must ensure that the CSV file you plan to import is complete and properly formatted, as explained in [Create Device Import CSV Files](#), on page 6.

-
- Step 1** Choose Inventory > Device Management > Network Devices, click the + icon above the Network Devices table and then click Bulk Import.
- Step 2** From the Operation drop-down list, choose Device.
- Step 3** Next to Select CSV File, click Browse to navigate to and select the CSV file that contains the devices that you want to import.
- Step 4** Click Import.
- Step 5** Check the status of the import by choosing Administration > Dashboards > Job Dashboard > UserJobs > Device Bulk Import.
- Step 6** Click the arrow to expand the job details and view the details and history for the import job.
-

Create Device Import CSV Files

If you want to use a CSV file to import your devices from another source into , you should prepare the CSV file using the device template, which you can download from as follows:

1. Choose Inventory > Device Management > Network Devices Inventory > Device Management >. Then click Bulk Import.
2. Click the [here](#) link next to "Bulk device add sample template can be downloaded" (as highlighted in the figure below). The template contains all of the fields and descriptions for the information that must be contained in the CSV device file you plan to import.

Bulk Import

Operation

Select CSV File No file selected.

Bulk device add sample template can be downloaded [here](#)

Bulk site add sample template can be downloaded [here](#)

*Note: CLI Enable Password is required for Collecting Few Inventory Collection Details. CLI Enable Password & SNMP Write Credential are required for Configuration related Features to work such as Image Management, Config Changes & Config Archive.

Please note that when you add devices by importing a CSV file, the extent to which can manage these devices will depend on the information you provide in the CSV file. For example: If you do not provide values for the CLI username, CLI password, CLI enable password, and CLI timeout value fields for a device in the CSV file, will be unable to modify that device's configurations, update device software images, or perform other useful functions.

This will also affect collection of complete device inventory. For partial inventory collection in , you must provide values for at least the following fields in the CSV file:

- Device IP address
- SNMP version
- SNMP read-only community strings
- SNMP write community strings
- SNMP retry value
- SNMP timeout value

For full inventory collection in Prime Infrastructure, you must also provide a value for the Protocol field, as well as values for the fields that correspond to the protocol you specify. For example: If you specify a value of **SNMPv3** in the Protocol field, you must also specify values for the SNMPv3 fields in the sample CSV file (such as the SNMPv3 username and authorization password).

You can specify the credential profile in the CSV file to apply the credentials to a set of devices. If you specify the credential profile and also enter the values manually in the CSV file, the device will be managed based on a combination of the manually entered credentials and the credential profile, with the manually entered credentials taking higher priority. For example, if the CSV file contains a credential profile with SNMP and Telnet credentials in addition to manually entered SNMP credentials, then the device is managed based on the manually entered SNMP credentials and the Telnet credentials in the credential profile.

If the CSV file you plan to import contains any User Defined Field (UDF) parameters, you must ensure that you add these UDF parameters before importing the CSV file. You can do this by selecting Administration > Settings > System Settings > Inventory > User Defined Fields and then adding each of the UDF parameters. The UDF column in your CSV file must begin with **UDF:**, as indicated in the CSV template. Do not use the special characters **:**, **;** and **#** for UDF field parameters.



Note During bulk import, the CSV file must contain only the IP Address and Credential Profile Name information.

Add Devices Manually (New Device Type or Series)

Use this procedure to add a new device type and to test your settings before applying them to a group of devices.

-
- Step 1** Choose Inventory > Device Management > Network Devices.
- Step 2** Click the **+** icon above the Network Devices table, then choose Add Device.
- Step 3** In the Add Device dialog box, complete the required fields. Click the ? icon next to a field for a description of that field.
- Note** Telnet/SSH information is mandatory for devices .
- Step 4** (Optional) Click Verify Credentials to validate the credentials before adding the device.
- Step 5** Click Add to add the device with the settings you specified.
- Note** For NCS 2000 devices, the Enable Single Session TL1 setting takes effect only for devices running release 11.0 onwards.

Note , by default, does not accept UCS with self-signed certification. User can enable it manually by adding the following lines in the /opt/CSColumos/xmp_inventory/xde-home/inventoryDefaults/ncsCIMC.def file.

```
<default attribute="HTTPS_TRUST_CONDITION">always</default>
<default attribute="HTTPS_HOSTNAME_VERIFICATION_STRATEGY">allow_all</default>
```

Add a Virtual Device Context Device

In , Cisco NX-OS software supports Virtual Device Contexts (VDCs), which partition a single physical device into multiple logical devices that provide fault isolation, management isolation, address allocation isolation, service differentiation domains, and adaptive resource management. A VDC allows a switch to be virtualized at the device level. It runs as a separate logical entity within the switch that maintains its own set of running software processes, has its own configuration, and is managed by an administrator. VDC1 is the default (Admin) VDC and has a special role: It allows you to configure child VDCs and allocate resources.

manages all Cisco Nexus switch features (including VDCs) on devices running Cisco NX-OS software release 6.2(12) or later.

To add the device with the default VDC, complete the following procedure:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 From the Add Device drop-down list, choose Add Device.

Step 3 Specify the required settings in the various tabs.

To view a description of a particular parameter, place your cursor over its ? icon.

Step 4 (Optional) Click Verify Credentials to confirm that the credentials you entered are valid before adding the device.

Step 5 Click Add to add the device with the settings you specified.

After successful inventory collection, the device with the default VDC is added. Subsequently, child VDCs are added automatically and the configuration is stored in the database.

Add a Meraki Device to Prime Infrastructure

You can monitor all Meraki Access Point, Meraki Security Appliances and Meraki switches in Cisco Prime Infrastructure. Cisco Prime Infrastructure uses SNMP protocol to extract information about the Meraki devices, from Cloud, for both monitoring and inventory purposes.

Integrating Cisco Meraki into Cisco Prime Infrastructure requires the following:

- Enable SNMP on the Dashboard
- Add the Meraki Dashboard to the Cisco Prime Infrastructure Server
- Verify Connectivity

To add a Meraki device to Prime Infrastructure, perform the following steps :

- Step 1** Choose Inventory > Device Management > Network Devices.
- Step 2** Click the + icon above the Network Devices table, then choose Add Device.
- Step 3** Enter the IP Address or DNS Name of the Meraki Dashboard.
- Step 4** Enter the SNMP v2/v3 credentials in the Add Device screen.
- Step 5** (Optional) Click Verify Credentials to validate the credentials before adding the device.
- Step 6** Click Add to add the devices with the settings you specified. The device details will be displayed in the right pane. Some of which include:
- Device Name
 - Reachability/Status
 - IP address/DNS name
 - Device Type or Model
 - MAC address
 - Client Count
 - Serial Number
 - Mesh Status
 - Network Name.

Inventory / Device Management / Network Devices

Device Groups / Device Type / Meraki Dashboard

Meraki Dashboard

Selected 0 / Total 1

Device Name	Reacha...	IP Address/...	Device Type	Admin Status	Inventory Collectio...	Last Successf...	Software Ve
meraki-dashbo...	✓	2.36.1.1	Meraki Dashboard	Managed	Completed	March 26, 201...	

The Meraki Dashboard remains the single point of configuration for Meraki devices. Cisco Prime makes it very easy to get to any specific device by including a device link next to the IP Address of the device. These links will launch a browser window that will bring the administrator right to the device in the Meraki Dashboard which helps you to extract comprehensive information about a particular device.

Note You must select an appropriate device group from the group selector/object selector in the Network Devices page to view the required the Access Points, Switches, and Security Appliances.

Prerequisites for Adding Wireless Controllers

Note the following information when adding wireless devices to Prime Infrastructure:

- When you remove a wireless controller from Prime Infrastructure, a warning message appears to confirm whether the access points associated with that controller also need to be removed.
- If you are adding a controller across a GRE link using IPsec or a lower MTU link with multiple fragments, you may need to adjust the values of Maximum VarBinds per Get PDU and Maximum VarBinds per Set PDU. If these values are too high, the controller might not be added to Prime Infrastructure.

To adjust the Maximum VarBinds per Get PDU or Maximum VarBinds per Set PDU values: Stop the Prime Infrastructure server, choose Administration > Settings > Network and Device > SNMP, and edit the Maximum VarBinds per Get PDU and Maximum VarBinds per Set PDU values to 50 or lower.

- If you are adding a wireless controller and receive the error message "Sparse table not supported", verify that you are running compatible versions of both Prime Infrastructure and WLC before retrying. For information on compatible versions of the two products, see the [Cisco Wireless Solutions Software Compatibility Matrix](#) entry for Prime Infrastructure, on Cisco.com.
- Prime Infrastructure acts as a trap receiver for controllers you add. The following traps are enabled on the controller: 802.11 Disassociation, 802.11 Deauthentication, and 802.11 Authenticated.
- When you add a new controller, the Reachability of the controller will be listed as "Unknown" while Prime Infrastructure attempts to communicate with the new controller. The controller's Reachability changes to "Reachable" or "Ping Reachable" once the communication with the controller is successful.
- When Compliance is enabled, the WLC can go to partial inventory collection state due to the following reasons:
 - CLI credential does not have read-write privilege.
 - WLC closes the connection during synchronization.
 - WLC does not respond in the configured time out period.
- To update the credentials of multiple controllers in bulk, choose Inventory > Network Devices > Wireless Controllers. Then select the controllers you need to update and click the Edit icon. Finally, select the credential profile and click Update or Update & Sync.
- You can also update the credentials of multiple controllers in bulk by creating a CSV file that contains a list of controllers to be updated. Make sure there is one controller per line, with each line a comma-separated list of the controller attributes you want updated.
 - Choose Inventory > Network Devices > Wireless Controllers.
 - Click the + icon above the table.
 - Choose Bulk Import and browse to the CSV file.

Validate Added Devices and Troubleshoot Problems

To monitor the discovery process, follow these steps:

-
- Step 1** To check the discovery process, choose Inventory > Device Management > Discovery.
- Step 2** Expand the job instance to view its details, then click each of the following tabs to view details about that device's discovery:
- **Reachable**—Devices that were reached using ICMP. Devices may be reachable, but not modeled, this may happen due to various reasons as discussed in [Add Devices Using Discovery, on page 2](#). Check the information in this tab for any failures.
 - **Filtered**—Devices that were filtered out according to the customized discovery settings.
 - **Ping Reachable**—Devices that were reachable by ICMP ping but could not be communicated using SNMP. This might be due to multiple reasons: invalid SNMP credentials, SNMP not enabled in device, network dropping SNMP packets, etc.
 - **Unreachable**—Devices that did not respond to ICMP ping, with the failure reason.
 - **Unknown**— cannot connect to the device by ICMP or SNMP.
- Note** For devices that use the TL1 protocol, make sure that node names do not contain spaces. Otherwise, you will see a connectivity failure.
- Step 3** To verify that devices were successfully added to , choose Inventory > Device Management > Network Devices. Then:
- Verify that the devices you have added appear in the list. Click a device name to view the device configurations and the software images that collected from the devices.
 - View details about the information that was collected from the device by hovering your mouse cursor over the Inventory Collection Status field and clicking the icon that appears.
 - Check the device's Reachability and Admin Status columns. See [Device Reachability and Admin States, on page 12](#).
-

Check a Device's Reachability State and Admin Status

Use this procedure to determine whether can communicate with a device (reachability state) and whether it is managing that device (admin status). The admin status also provides information on whether the device is being successfully managed by .

- Step 1** Choose Inventory > Device Management > Network Devices.
- Step 2** Locate your device in the Network Devices table.
- a) From the Show drop-down list (at the top right of the table), choose Quick Filter.
 - b) Enter the device name (or part of it) in the text box under the Device Name column.
- Step 3** Check the information in the Reachability and Admin Status columns. See [Device Reachability and Admin States, on page 12](#) for descriptions of these states.
-

Device Reachability and Admin States

Device Reachability State—Indicates whether can communicate with the device using all configured protocols.

Table 2: Device Reachability State

Icon	Device Reachability State	Description	Troubleshooting
	Reachable	can reach the device using SNMP, or the NCS 2K device using ICMP.	—
	Ping reachable	can reach the device using Ping, but not via SNMP.	Although ICMP ping is successful, check for all possible reasons why SNMP communication is failing. Check that device SNMP credentials are the same in both the device and in , whether SNMP is enabled on the device, or whether the transport network is dropping SNMP packets due to reasons such as mis-configuration, etc. .
	Unreachable	cannot reach the device using Ping.	Verify that the physical device is operational and connected to the network.
	Unknown	cannot connect to the device.	Check the device.

Device Admin State—Indicates the configured state of the device (for example, if an administrator has manually shut down a device, as opposed to a device being down because it is not reachable by Ping).

Table 3: Device Admin State

Device Admin State	Description	Troubleshooting
Managed	is actively monitoring the device.	Not Applicable.
Maintenance	is checking the device for reachability but is not processing traps, syslogs, or TL1 messages.	To move a device back to Managed state, see Move a Device To and From Maintenance State, on page 13 .

Unmanaged	is not monitoring the device.	<p>In the Network Devices table, locate the device and click the "i" icon next to the data in the Last Inventory Collection Status column. The popup window will provide details and troubleshooting tips. Typical reasons for collection problems are:</p> <ul style="list-style-type: none"> • Device SNMP credentials are incorrect. • The deployment has exceeded the number of devices allowed by its license. • A device is enabled for switch path tracing only. <p>If a device type is not supported, its Device Type will be Unknown. You can check if support for that device type is available from Cisco.com by choosing Administration > Licenses and Software Updates > Software Update and then clicking Check for Updates.</p>
Unknown	cannot connect to the device.	Check the device.

Move a Device To and From Maintenance State

When a device's admin status is changed to Maintenance, will neither poll the device for inventory changes, nor will it process any traps or syslogs that are generated by the device. However, will continue to maintain existing links and check the device for reachability.

See [Device Reachability and Admin States, on page 12](#) for a list of all admin states and their icons.

-
- Step 1** From the Network Devices table, choose Admin State > Set to Maintenance State.
- Step 2** To return the device to the fully managed state, choose Admin State > Set to Managed State.
-

Edit Device Parameters

You can edit the device parameters of a single device or multiple devices by choosing Inventory > Device Management > Network Devices.

To edit device parameters, follow these steps:

-
- Step 1** Choose Inventory > Device Management > Network Devices.
- Step 2** Select a single device or multiple devices and then click the Edit icon.
- Editing more than 9 devices triggers a job in the Job Dashboard page. The status of the bulk edit is displayed in that page.
- Step 3** Update the required parameters.
- Step 4** Click Update to update the parameters of all of the selected devices or Update & Sync to update and synchronize the devices with the updated parameters.
-

Synchronize Devices

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

To synchronize devices, follow these steps:

-
- Step 1** Choose Inventory > Device Management > Network Devices.
- Step 2** Select the device whose configuration you want synchronized with the configuration stored in the Prime Infrastructure database.
- Step 3** Click Sync.
- Note** If the synchronized device is a default/Admin VDC, then all the configuration of all the child VDCs are synchronized automatically and the configuration is updated in the Prime Infrastructure database. Admin VDC sync will also add the newly added VDC in hardware to the user interface or delete the deleted VDC in hardware from the user interface.
-

Smart Inventory

Smart Inventory allows only limited features to be collected if the commit id on the device is not changed. Otherwise, full collection of features will happen. Smart Inventory aims to reduce the amount of data transferred between Prime Infrastructure and the device in a smart way. Prime Infrastructure will do a major inventory collection and full config archive only when there is a change in the configuration of the device. If there is no change in the running configuration of the device, only the physical information like images, flash, files, interface status, etc will be collected from the device. If there is no change in the running config of the device, config archive will not be triggered.

To enable Smart Inventory:

-
- Step 1** Choose Administration > System Settings > Inventory > Smart Inventory.
- Step 2** Select the Enable Smart Inventory Globally check box. All the supported devices will be listed.
- Note** You can also enable/disable Smart Inventory for the individual devices. Select the required devices and click Enable or Disable button.
-

Add NAM HTTP/HTTPS Credentials

If you are using Cisco Network Analysis Modules (NAMs) to monitor your network, you must add HTTPS credentials so that Prime Infrastructure can retrieve data from them. This is especially important for users who have licensed Assurance features, as most Assurance features depend on NAM data to work.

Prime Infrastructure polls NAMs directly via HTTP (or HTTPS) to collect their data. This type of polling requires Prime Infrastructure to store each NAMs' HTTP credentials. Unlike with SNMP community strings

and Telnet/SSH credentials, you cannot enter NAM HTTP credentials during the discovery process. You can only specify NAM HTTP credentials after the modules are discovered or added to inventory.

Follow these steps to add HTTP credentials for a single NAM. You can repeat this task for all NAMs from which you want Prime Infrastructure to collect data.

-
- Step 1** Choose Inventory > Device Management > Network Devices > Device Type > Cisco Interfaces and Modules > Network Analysis Modules.
- Step 2** Select one of the NAMs and click Edit.
- Step 3** In the Edit Device window, under Http Parameters:
- Protocol—Select the HTTP protocol, HTTP or HTTPS. The TCP Port will change automatically to the default port for the protocol that you have selected.
 - TCP Port—Enter a different TCP Port if you want to override the default.
 - Username—Enter the name of a user who can access the NAM via HTTP or HTTPS.
 - Password—Enter the password for the username that you entered.
 - Confirm Password—Enter the password a second time to confirm.
- Step 4** Choose Update.
-

Export Device Information to a CSV File

When you export the device list to a file, all device information is exported into a CSV file. The file is then compressed and encrypted using a password you select. The exported file contains information about the device's SNMP credentials, CLI settings, and geographical coordinates. The exported file includes device credentials but does not include credential profiles.



Caution Exercise caution while using the CSV file as it lists all credentials for the exported devices. You should ensure that only users with special privileges can perform a device export.

-
- Step 1** Choose Inventory > Device Management > Network Devices.
- Step 2** Select the devices that you want to export, then click Export Device (or click  and choose Export Device).
- Step 3** In the Export Device dialog box, enter a password that will be used to encrypt the exported CSV file. Users will need to supply this password to open the exported file.
- Step 4** Enter the password, confirm password, or export file name and click Export. Depending on your browser configuration, you can save or open the compressed file.
-

Apply Device Credentials Consistently Using Credential Profiles

Credential profiles are collections of device credentials for SNMP, Telnet/SSH, HTTP, and TL1. When you add devices, you can specify the credential profile the devices should use. This lets you apply credential settings consistently across devices.

If you need to make a credential change, such as changing a device password, you can edit the profile so that the settings are updated across all devices that use that profile.

To view the existing profiles, choose Inventory > Device Management > Credential Profiles.

Create a New Credential Profile

Use this procedure to create a new credential profile. You can then use the profile to apply credentials consistently across products, or when you add new devices.

-
- Step 1** Select Inventory > Device Management > Credential Profiles.
- Step 2** If an existing credential profile has most of the settings you need, select it and click Copy. Otherwise, click Add.
- Step 3** Enter a profile name and description. If you have many credential profiles, make the name and description as informative as possible because that information will be displayed on the Credential Profiles page.
- Step 4** Enter the credentials for the profile. When a device is added or updated using this profile, the content you specify here is applied to the device.
- The SNMP read community string is required.
- Step 5** Click Save Changes.
-

Apply a New or Changed Profile to Existing Devices

Use this procedure to perform a bulk edit of devices and change the credential profile the devices are associated with. This operation overwrites any existing association between a device and a credential profile. You can also use this operation to synchronize device configurations with the new settings.



Note Make sure the profile's credential settings are correct before following this procedure and selecting Update and Sync. That operation will synchronize the devices with the new profile.

- Step 1** Configure the credential profile using one of these methods:
- Create a new credential profile by choosing Inventory > Device Management > Credential Profiles, and clicking Add.
 - Edit an existing profile by choosing Inventory > Device Management > Credential Profiles, selecting the profile, and clicking Edit.

- Step 2** When you are satisfied with the profile, choose Inventory > Device Management > Network Devices.
- Step 3** Filter and select all of the devices you want to change (bulk edit).
- Step 4** Click Edit, and select the new credential profile from the Credential Profile drop-down list.
- Step 5** Save your changes:
- Update saves your changes to the database.
 - Update and Sync saves your changes to the database, collects the device's physical and logical inventory, and saves all inventory changes to the database.
-

Delete a Credential Profile

This procedure deletes a credential profile from . If the profile is currently associated with any devices, you must disassociate them from the profile.

- Step 1** Check whether any devices are using the profile.
- a) Go to Inventory > Device Management > Credential Profiles.
 - b) Select the credential profile to be deleted.
 - c) Click Edit, and check if any devices are listed on the Device List page. If any devices are listed, make note of them.
- Step 2** If required, disassociate devices from the profile.
- a) Go to Inventory > Device Management > Network Devices.
 - b) Filter and select all of the devices you want to change (bulk edit).
 - c) Click Edit, and choose --Select-- from the Credential Profile drop-down list.
 - d) Disassociate the devices from the old profile by clicking OK in the warning dialog box.
- Step 3** Delete the credential profile by choosing Inventory > Device Management > Credential Profiles, selecting the profile, and clicking Delete.
-

Export and Import a Credential Profile

You can export and import the credentials profile from device management using the following steps:

- Step 1** Choose Inventory > Device Management > Credential Profiles
- Step 2** Select the credential profile that you want to export, click Export Profile.
- Step 3** Enter the following credentials in the Export Profile pop-up window:
- Password
 - Confirm Password
 - Export File Name
- Step 4** Click Export to save the zip file which contains Profile and Profile associated with devices csv files.

- Step 5** To import the credential profile, use the following steps:
- Step 6** Login to the Prime Infrastructure Server.
- Step 7** Choose Inventory > Device Management > Credential Profiles.
- Step 8** Click Bulk Import.
- Step 9** In the Bulk Import pop-up, browse the credential profile .csv file and Click Import.
- Caution** You should not import Profile_associated_devices .csv files during bulk import.
- Step 10** Once the import is completed, the credential profile bulk import job is created. You can navigate to Administration > Dashboard > Job Dashboard > User Jobs > Credential Profile Bulk Import to check the job.
-

Create Groups of Devices for Easier Management and Configuration

- [How Groups Work, on page 18](#)
- [Create User-Defined Device Groups, on page 21](#)
- [Create Location Groups, on page 22](#)
- [Create Port Groups, on page 26](#)
- [Make Copies of Groups, on page 27](#)
- [Hide Groups That Do Not Have Any Members, on page 28](#)
- [Delete Groups, on page 28](#)

Organizing your devices into logical groupings simplifies device management, monitoring, and configuration. As you can apply operations to groups, grouping saves time and ensures that configuration settings are applied consistently across your network. In smaller deployments where all devices can be configured with the same settings, you may only need to create one general device group. The grouping mechanism also supports subgroups. You will see these groups in many of the GUI windows.

When a device is added to , it is assigned to a location group named Unassigned. If you are managing a large number of devices, be sure to move devices into other groups so that the Unassigned Group membership does not become too large.

How Groups Work

For information on how elements are added to groups, see [How Elements Are Added to Groups: Dynamic, Manual, and Mixed Groups, on page 20](#).

Network Device Groups

The following table lists the supported types of network device groups. The device groups can be accessed from the Inventory.

Network Device Group Type	Membership Criteria	Can Be Created or Edited By Users?
Device Type	<p>Devices are grouped by family (for example, Routers, Switches and Hubs, and so forth). Under each device family, devices are further grouped by series. New devices are automatically assigned to the appropriate family and series groups. For example, a Cisco ASR 9006 would belong to Routers (family) and Cisco ASR 9000 Series Aggregation Services Routers (series).</p> <p>Note the following:</p> <ul style="list-style-type: none"> • You cannot create a device type group; these are dynamic groups that are system-defined. Instead, use device criteria to create a user-defined group and give it an appropriate device name. • Device type groups are not displayed in Network Topology maps. • Unsupported devices discovered by are automatically assigned the Unsupported Cisco Device device type and are listed under Device Type > Unsupported Cisco Device Family. 	No
Location	<p>Location groups allow you to group devices by location. You can create a hierarchy of location groups (such as theater, country, region, campus, building, and floor) by adding devices manually or by adding devices dynamically.</p> <p>A device should appear in one location group only, though a higher level “parent” group will also contain that device. For example, a device that belongs to a building location group might also indirectly belong to the parent campus group.</p> <p>By default, the top location of the hierarchy is the All Locations group. All devices that have not been assigned to a location appear under the Unassigned group under All Locations.</p>	Yes
User Defined	<p>Devices are grouped by a customizable combination of device and location criteria. You can customize group names and use whatever device and location criteria you need.</p>	Yes

Port Groups

The following table lists the supported types of port groups.

Port Group Type	Membership Criteria	Can be created or edited by users?
Port Type	<p>Grouped by port type, speed, name, or description. Ports on new devices are automatically assigned to the appropriate port group.</p> <p>You cannot create Port Type groups. Instead, use device criteria to create a user-defined group, and create subgroups under the user-defined group.</p>	No; instead create a User Defined Group

System Defined	<p>Grouped by port usage or state. Ports on new devices are automatically assigned to the appropriate port group.</p> <p>Link Ports—Ports that are connected to another Cisco device or other network devices and are operating on “VLAN” mode and are assigned to a VLAN.</p> <p>Trunk Ports—Ports that are connected to a Cisco device or other network devices (Switch/Router/Firewall/Third party devices) and operating on “Trunk” mode in which they carry traffic for all VLANs.</p> <p>If the status of a port goes down, it is automatically added to Unconnected Port group. You cannot delete the ports in this group, and you cannot re-create this group as a sub group of any other group.</p> <p>You cannot create System Defined Port groups. Instead, use device criteria to create a user-defined group, and create subgroups under the user-defined group.</p> <p>Note As the WAN Interfaces is a static group, automatic port addition is not applicable. Hence, you must add the ports manually to the group.</p>	No; instead create a User Defined Group
User Defined	Grouped by a customizable combination of port criteria, and you can name the group. If the group is dynamic and a port matches the criteria, it is added to the group.	Yes

Data Center Groups

The following table lists the supported types of data center groups.

Table 4: Data Center Group Supported Types

Data Center Group Type	Membership Criteria	Can be created or edited by users?
System Defined	<p>Grouped by type (Data Center, Cluster, Virtual Machine (VM), Host).</p> <p>You cannot create System Defined Data Center Groups. Instead, use device criteria to create a user-defined Data Center group, and create subgroups under the user-defined group.</p>	No. Can create User Defined Groups for VMs and Hosts
User Defined	Grouped by customizable combination of device and location criteria. You can customize group names and use whatever device criteria you need.	Yes

How Elements Are Added to Groups: Dynamic, Manual, and Mixed Groups

How elements are added to a group depends on whether the group is dynamic, manual, or mixed.

Method for Adding Devices	Description
Dynamic	automatically adds a new element to the group if the element meets the group criteria. While there is no limit to the number of rules that you can specify, the performance for updates may be negatively impacted as you add more rules.
Manual	Users add the elements manually when creating the group or by editing the group.
Mixed	Elements are added through a combination of dynamic rules and manual additions.

The device inheritance in parent-child user defined and location groups are as follows:

- User Defined Group—When you create a child group:
 - If the parent and child groups are both dynamic, the child group can only access devices that are in the parent group.
 - If the parent group is static and the child group is dynamic, the child group can access devices that are outside of the parent group.
 - If the parent and child groups are dynamic and static, the child group "inherits" devices from the parent device group.
- Location Group—The parent group inherits the child group devices.

Groups and Virtual Domains

While groups are logical containers for elements, access to the elements is controlled by virtual domains. This example shows the relationship between groups and virtual domains.

- A group named SanJoseDevices contains 100 devices.
- A virtual domain named NorthernCalifornia contains 400 devices. Those devices are from various groups and include 20 devices from the SanJoseDevices group.

Users with access to the NorthernCalifornia virtual domain will be able to access the 20 devices from the SanJoseDevices group, but not the other 80 devices in the group. For more details, see [Create Virtual Domains to Control User Access to Devices](#).

Create User-Defined Device Groups

To create a new device type group, use the user-defined group mechanism. You must use this mechanism because device type groups are a special category used throughout . The groups you create will appear in the User Defined category.

To create a new group, complete the following procedure:

-
- Step 1** Choose Inventory > Group Management > Network Device Groups.
- Step 2** In the Device Groups pane, click the + (Add) icon and then choose Create User Defined Group.

View All Groups to Which a Device Belongs

Step 3 Enter the group's name and description. If other user-defined device type groups already exist, you can set one as the parent group by choosing it from the Parent Group drop-down list. If you do not select a parent group, the new group will reside in the User-Defined folder (by default).

Step 4 Add devices to the new group:

If you want to add devices that meet your criteria automatically, enter the criteria in the Add Devices Dynamically area. To group devices that fall within a specific range of IP addresses, enter that range in square brackets. For example, you can specify the following:

- IPv4-10.[101-155].[1-255].[1-255] and 10.126.170.[1-180]
- IPv6-2014::5217:[0000-ffff]:fe22:[1e40-1f41]

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

If you want to add devices manually, do the following:

- a. Expand the Add Devices Manually area and then click Add.
- b. In the Add Devices dialog box, check the check boxes for the devices you want to add, then click Add.

Step 5 Click the Preview tab to see the members of your group.

Step 6 Click Save.

The new device group appears in the folder you selected in Step 3.

View All Groups to Which a Device Belongs

To view the list of device groups to which a device belongs, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices or Inventory > Group Management > Network Device Groups.

Step 2 Enter an IP address or device name in the Search field in the Device Group pane on the left, to view the list of all groups to which the device belongs.

You can also search the group by entering the group name in the search field.

Create Location Groups

Step 1 Choose Inventory > Group Management > Network Device Groups.

Step 2 In the Device Groups pane on the left, click the Add icon, then choose Create Location Group.

Step 3 Enter the name and description, and choose a group from the Parent Group drop-down list. By default, the group will be an All Locations subgroup (that is, displayed under the All Locations folder).

Step 4 If you are creating a device group based on geographical location, for example, all devices located in a building at a specific address, select the Geographical Location check box and specify the GPS coordinates of the group or click the

View Map link and click on the required location in the map. The GPS coordinates will be populated automatically in this case. Note that location groups defined with a geographic location are represented by a group icon in the geo map. The devices you add to the group will inherit the GPS coordinates of the group. Note that if geographical location is the primary reason for grouping a set of devices, it is recommended that the devices you add to the group do not have their own GPS coordinates that are different from the group's.

Step 5

If you want devices to be added automatically if they meet certain criteria, enter the criteria in the Add Device Dynamically area. Otherwise, leave this area blank.

▼ Add Devices Dynamically ⓘ **Match operation using ***

And ▼ Device Name ▼ matches ▼ rou* - +

Device Name ▲	IP Address/DNS	Device Type
<input type="text"/>	<input type="text"/>	<input type="text"/>
Router.Cisco.com	10.104.62.154	Cisco ASR 1002 Router

▼ Add Devices Dynamically ⓘ **Doesn't match operation using ***

And ▼ Device Name ▼ doesn't match (... ▼ *uter - +

Device Name ▲	IP Address/DNS	Device Type
<input type="text"/>	<input type="text"/>	<input type="text"/>
bgl12-ssi9	10.106.183.128	Unsupported Cisco Device
C2851	10.126.168.154	Cisco 2851 Integrated Services Router

▼ Add Devices Dynamically ⓘ **Match operation using ?**

And ▼ Device Name ▼ matches ▼ r??ter - +

Device Name ▲	IP Address/DNS	Device Type
<input type="text"/>	<input type="text"/>	<input type="text"/>
Router	10.197.70.47	Cisco Cloud Services Router 1000V
Router	10.197.70.49	Cisco Cloud Services Router 1000V

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

Step 6

If you want to add devices manually:

- a) Under Add Devices Manually, click Add.
- b) In the Add Devices dialog box, locate devices you want to add, then click Add.

Step 7 Click the Preview tab to see the group members.

Step 8 Click Save, and the new location group appears under the folder you selected in Step 3 (All Locations, by default).

Note Numeric alone Floor Group name is considered as floor index automatically. Please make sure that the planned "Numeric alone Floor Group name" index is not used in any of the existing floors of that building using the Edit view option of the existing floors in Maps GUI.

To create numeric/digits value as Floor Group:

- launch Maps GUI, click Building.
- Edit the existing floors in Maps GUI, change the existing floor index value from **1** to other value.
- Click Save

launch the Maps GUI. click building.

When you edit a location group, you may change the group type if the following conditions are met:

- The group type is Default.
- The group does not have any subgroups.

Create Groups Using CSV Files

To import a group using a CSV file that lists all attributes of the group that you want to add into Prime Infrastructure, follow these steps.

Step 1 Choose Inventory > Group Management > Network Device Groups, then click Import Groups.

Step 2 Click the [here link](#) to download the sample template for the CSV file.

Make sure that you retain the required information in the CSV file as mentioned in the Template.

Step 3 Click Choose File in the Import Groups dialog box, and select the CSV file that contains the group that you want to import.

Step 4 Click Import.

Step 5 Choose Administration > Dashboards > Job Dashboard, then click Import Groups to view the status of the job.

Export Groups to CSV Files

To export group information as a CSV file, follow these steps.

Step 1 Choose Inventory > Group Management > Network Device Groups.

Step 2 Select PI or APIC-EM.

Step 3 Click Export Groups to download the CSV file including the details of all location groups, into your local system.

Add APs to Device Groups and Location Groups

SUMMARY STEPS

1. Choose Inventory > Group Management > Network Device Groups.
2. In the Device Groups pane on the left, hover the mouse over the expand icon next to User Defined or Location and click Add SubGroup.
3. Enter the name, description, and parent group (if any).
4. Add APs in one of the following ways:
5. Click Preview to view the APs that are automatically added to the group based on the specified rule and the manually added APs.
6. Click Save.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Choose Inventory > Group Management > Network Device Groups.	
Step 2	In the Device Groups pane on the left, hover the mouse over the expand icon next to User Defined or Location and click Add SubGroup.	
Step 3	Enter the name, description, and parent group (if any).	
Step 4	Add APs in one of the following ways:	<ul style="list-style-type: none"> • Manually—Click Add under Add Devices Manually and select the APs you want to add to the group. • Dynamically—Specify rules to which APs must comply before they are added to this port group. You do not add APs to dynamic groups. Prime Infrastructure adds APs that match the specified rules to the dynamic group. <p>If you select any type of Location group other than Default, the APs will not be added dynamically.</p>
Step 5	Click Preview to view the APs that are automatically added to the group based on the specified rule and the manually added APs.	
Step 6	Click Save.	If the group has Unified AP or Third Party AP as a member, a new tab is added in the right hand table in the Device Work Center, to display the APs.

Create Port Groups

To create a port group, follow these steps:

-
- Step 1** Choose Inventory > Group Management > Port Groups.
- Step 2** From Port Groups > User Defined, hover your cursor over the "i" icon next to User Defined and click Add SubGroup from the popup window.
- Step 3** Enter the name and description, and choose a group from the Parent Group drop-down list. By default, the port group will be under the User Defined folder.
- Step 4** Choose the devices a port must belong to in order to be added to the group. From the Device Selection drop-down list, you can select:
- Device—To choose devices from a flat list of all devices.
 - Device Group—To choose device groups (Device Type, Location, and User Defined groups are listed).
- Step 5** If you want ports to be added automatically if they meet your criteria, enter the criteria in the Add Ports Dynamically area. Otherwise, leave this area blank.
- While there is no limit on the number of rules that you can specify for a dynamic group, the group update performance could become slower as the number of rules increases.
- Step 6** If you want to add devices manually:
- a) Under Add Ports Manually, click Add.
 - b) In the Add Ports dialog box, locate devices you want to add, then click Add.
- Step 7** Click the Preview tab to see the group members.
- Step 8** Click Save, and the new port group appears under the folder you selected in Step 3 (User Defined, by default).
-

Create User-Defined Data Center Groups

In addition to the out-of-box data center and cluster groups, you can create user-defined groups for VMs and hosts. To create a user-defined group, complete the following procedure:

-
- Step 1** Choose Inventory > Device Management > Compute Devices.
- Step 2** From the Compute Resources pane, locate User Defined Hosts and VMs and place your cursor over its i (information) icon.
- Step 3** From the Actions area, click Add Subgroup.
- The Add Device Subgroup page opens.
- Step 4** Enter the group's name and description, and then choose the folder the group will reside in from the Parent Group drop-down list.
- Step 5** Add devices to the location group:
- If you want to add devices that meet your criteria automatically, enter the criteria in the Add Devices Dynamically area.

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

- If you want to add devices manually, do the following:
 - a. Expand the Add Devices Manually area and then click Add.
 - b. In the Add Devices dialog box, check the check boxes for the devices you want to add, then click Add.

Step 6 Click the Preview tab to see the devices that will belong to the group.

Step 7 Click Save. The new group appears in the folder you selected in Step 4.

Edit User-Defined Groups

You can change the parent group, add devices, and modify device rules using the edit option.

Procedure

	Command or Action	Purpose
Step 1	Choose Inventory > Group Management > Network Device Groups.	
Step 2	In the Device Groups pane on the left, click the name of the group you want to edit.	
Step 3	Click Edit and modify the details.	When you are editing a location group, you can change the group type to Campus, if: <ul style="list-style-type: none"> • The group type is Default. • The group does not have any subgroups.
Step 4	Click Preview to view the updated device details.	
Step 5	Click Save to save the updated device details.	

Make Copies of Groups

When you create a duplicate of a group, names the group CopyOfgroup-name by default. You can change the name, if required.

To duplicate a group follow these steps:

Step 1 Choose Inventory > Group Management > Network Device Groups.

Step 2 Choose the group from the Device Groups pane on the left.

Step 3 Locate the device group you want to copy, then click the "i" icon next to it to open the pop-up window.

Step 4 Click Duplicate Group (do not make any changes yet) and click Save. creates a new group called CopyOfgroup-name.

- Step 5** Configure your group as described in [Create User-Defined Device Groups, on page 21](#) and [Create Location Groups, on page 22](#).
- Step 6** Verify your group settings by clicking the Preview tab and examining the group members.
- Step 7** Click Save to save the group.

Copy User-Defined and Location Groups

You can duplicate any user-defined or location group using the Duplicate Group option. The duplicated group will contain all of the values from the original group, which you can modify. The populated group name will have a prefix of "CopyOf" by default. You can change the name, if required.

If you duplicate a child group, a copy of the child group is created under the same parent group.

If you duplicate a parent group, a copy of the respective child groups are created.

Procedure

	Command or Action	Purpose
Step 1	Choose Inventory > Group Management > Network Device Groups.	
Step 2	In the Device Groups pane on the left, locate the device group you want to duplicate. Then click the "i" icon next to the name of the group to display the popup menu.	
Step 3	Click Duplicate Group and update the group details.	
Step 4	Click Preview to view the duplicate group details.	
Step 5	Click Save to save the duplicate group.	

Hide Groups That Do Not Have Any Members

By default, will display a group in the web GUI even if the group has no members. Users with Administrator privileges can change this setting so that empty groups are hidden—that is, they are not displayed in the web GUI. (Hidden groups are not deleted from .)

- Step 1** Choose Administration > Settings > System Settings, then choose Inventory > Grouping.
- Step 2** Uncheck Display groups with no members, and click Save.

We recommend that you leave the Display groups with no members check box selected if you have a large number of groups and devices. Unselecting it can slow system performance.

Delete Groups

Make sure the group you want to delete has no members, otherwise will not allow the operation to proceed.

-
- Step 1** Choose Inventory > Group Management > Network Device Groups.
- Step 2** Locate the device group you want to delete in the Device Groups pane on the left, then click the "i" icon next to it to open the pop-up window.
- Step 3** Click Delete Group and click OK.
-

Create Compute Resource Groups

In addition to out-of-box groups for Compute Services devices such as Data Centers and clusters, you can create user-defined groups for UCS servers, hosts and VMs.

Procedure

	Command or Action	Purpose
Step 1	Choose Inventory > Compute Device Groups	
Step 2	In the Compute Resources at left, hover the mouse over the expand icon next to User Defined UCS or User Defined Hosts and VMs and click Add SubGroup.	
Step 3	Enter the group name and description, and select a parent group, if applicable.	
Step 4	In the Add Devices Dynamically pane, specify the rules that you want to apply to the devices in the group.	
Step 5	In the Add Devices Manually pane, choose the compute resources that you want to assign to the group.	
Step 6	Click Preview to view the devices that are automatically added to the group based on the specified rule and the manually added devices.	
Step 7	Click Save to add the compute resource group with the settings that you specified.	

