Adding Devices to Prime Infrastructure

Methods for Adding Devices

You can add devices to Cisco Prime Infrastructure in one of the following ways:

- Use an automated process—See Adding Devices Using Discovery.
- Import devices from a CSV file—See Importing Devices from Another Source.
- Add devices manually by entering IP address and device credential information—See Adding Devices Manually.

Adding Devices Using Discovery

When you run discovery, Prime Infrastructure discovers the devices and, after obtaining access, collects device inventory data. We recommend that you run discovery, when you are initially getting started with Prime Infrastructure.

Prime Infrastructure uses SNMP polling to gather information about your network devices within the range of IP addresses you specify. If you have CDP enabled on your network devices, Prime Infrastructure uses the seed device you specify to discover the devices in your network.

You can discover your devices by:

- Configuring discovery settings—This method is recommended if you want to specify settings and rerun discovery in the future using the same settings. See Running Discovery.
- Running Quick Discovery—Quick Discovery quickly ping sweeps your network and uses SNMP polling to get details on the devices. See Running Quick Discovery.

Understanding 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.

Running Discovery

Prime Infrastructure discovers devices with IPv4 and IPv6 addresses.

To run discovery, follow these steps:

Step 1 Choose **Inventory > Device Management > Discovery**.

Step 2 Click **Discovery Settings** (in the top right corner), then click **New**.

Step 3 Enter the Protocol Settings as described in Table 3-1.

Step 4 Perform one of the following:

- Click **Save** to save your discovery settings and schedule your discovery to run at a specified time.
- Click **Run Now** to run the discovery now.

Table 3-1 Discovery Protocol Settings

Field	Description
Protocol Settings	
Ping Sweep Module	Prime Infrastructure gets a list of IP address ranges from a specified combination of IP address and subnet mask, then pings each IP address in the range to check the reachability of devices. See Sample IPv4 IP Addresses for Ping Sweep for more information.
Layer 2 Protocols	
CDP Module	Prime Infrastructure reads the cdpCacheAddress and cdpCacheAddressType MIB objects in the cdpCacheTable from CISCO-CDP-MIB on every newly found device as follows: 1. The cdpCacheAddress MIB object is gathered from the current device. This provides a list of neighbor device addresses. 2. If the neighbor device addresses do not already exist in the global device list, they are added to the local cache. Select the **Enable Cross Router Boundary** check box to specify that Prime Infrastructure should discover neighboring routers.
LLDP	Similar to CDP, but it allows the discovery of non-Cisco devices.
Advanced Protocols	
Routing Table	Queries and analyzes routing tables on seed routers to discover subnets and next-hop routers. This process discovers a router for every subnet on its list of known networks.

Table 3-1 Discovery Protocol Settings (continued)

Field	Description
Address Resolution Protocol	The ARP Discovery Module depends on the Routing Table Discovery Module (RTDM), and is executed only when RTDM is processed. This precondition is identified based on the flags processed by the ARP Discovery Module, which are part of the DeviceObject. The entries coming out of the ARP Discovery Module do not need to pass through RTDM because (per the router Discovery algorithm) active routers are those that RTDM must process and identify. When the ARP table is fetched and the entries are not already discovered by RTDM, these entries (though they may represent routers) are not active routers and need not be passed on to RTDM. This is ensured by setting the ARP Discovery Module flag to Processed and leaving the RTDM flag set to Unprocessed. When the RTDM comes across an entry with the RTDM flag unset and the ARP flag set, RTDM identifies the entry as a inactive router or other device and it leaves the entry as *unprocessed*. The ARP Discovery Module also ignores the entry according to the algorithm, based on the Processed flag set against the ARP Discovery Module. When the **Enable ARP** check box is selected, the device MAC address needs to be updated in the device information. Applications can retrieve this information in the adapter through the DeviceInfo object. By scanning the device MAC address, the applications can distinguish between Cisco and non-Cisco devices. ARP cache from the device is collected using CidsARPInfoCollector. The MAC ID of the device is retrieved from this data and set in the DeviceInfo object.
Border Gateway Protocol	The BGP Discovery Module uses bgpPeerTable in the BGP4-MIB to find its BGP peer. The table contains its peers' IP addresses, which are added as clues to the local cache.
Open Shortest Path First	Open Shortest Path First (OSPF) protocol is an interior gateway routing protocol that uses the ospfNbrTable and ospfVirtNbrTable MIBs to find neighbor IP addresses.
Filters	

IP Filter	Includes or excludes devices based on IP address. For example, you can enter any of the following strings and specify whether to include or exclude the devices found during discovery:
	
	`192.0.2.89`
	`192.0.2.*`
	`192.0.[16-32].89`
	`[192-193].*.55.[16-32]`

Advanced Filters	
System Location Filter	Includes or excludes devices based on System Location.
System Object ID Filter	Includes or excludes devices based on the sysObjectID string set on the device.
DNS Filter	Includes or excludes devices based on the domain name string set on the device.
Credential Settings	
Credential Set	The credential set lists all the available credential profiles in Prime Infrastructure. You can associate credential profile with a range of IP addresses. The devices will be discovered based on the selected credential profile. For more information see, Using Credential Profiles.
SNMPv2 Credential	SNMP community string is a required parameter for discovering devices in the network using SNMPv2. You can enter multiple rows of credentials mapped to a specific IP address, or the IP address can be a wildcard; for example, *.*.*.*, 10.1.1.*. You cannot save or use the discovery settings if you do not specify SNMP credentials.

Table 3-1 Discovery Protocol Settings (continued)

Field	Description
SNMPv3 Credential	Prime Infrastructure supports SNMPv3 discovery for devices. The following SNMPv3 modes are available: • AuthPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) and AES-128 standards. • AuthNoPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. • NoAuthNoPriv—Uses a username match for authentication. • PrivType—Protocol used to secure the SNMP authentication request. • PrivPassword—Prefixed privacy passphrase for the SNMPv3 user.
Telnet Credential	You can specify the Telnet credentials during discovery so that Prime Infrastructure can collect the device configurations and fully manage the devices. If you do not specify Telnet credentials in the discovery settings, Prime Infrastructure discovers the devices but is unable to collect the full inventory of the device until you specify the Telnet credentials.
SSH Credential	For full device support via SSH, you must use SSHv2 with a 1024 bit key. You can configure SSH before running discovery. We recommend that you select SSHv2 as the protocol for communicating with the device CLI because it allows the use of Web Services Management Agent (WSMA) for configuring devices. (For more information see, Configuring the Device using WSMA.)
Preferred Management IP (how Prime Infrastructure attempts to find the preferred management address for devices)	
Use Loopback IP	Prime Infrastructure uses the preferred management IP address from the loop back interface. If the device does not have a loopback interface, Prime Infrastructure uses similar logic to the OSPF algorithm to select the router's preferred management IP address.
Use SysName	Prime Infrastructure gets the preferred management IP address for the device using DNS lookup of the SysName for the device.
Use DNS Reverse Lookup	Prime Infrastructure gets the preferred management IP address by doing a reverse DNS lookup on the device IP address, followed by a forward DNS lookup.

After running discovery, choose **Inventory > Device Management > Network Devices**.

Note When discovery job rediscovers an existing device, the original credentials will be maintained and will not be updated with the credentials entered in Discovery Settings, if Last Inventory Collection Status of the device is "completed" in the **Inventory > Device Management > Network Devices** page. However, if the status is "partial collection" or any other status, then original credentials of the existing device will be overwritten with the credentials present in the Discovery Settings.

See Monitoring Network Devices for more information.

Sample IPv4 IP Addresses for Ping Sweep

Table 3-2 Sample IPv4 Seed IP Addresses for 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	10.104.62.11	10.104.48.1	10.104.63.254
255.255.248.0	21	2046	10.104.62.11	10.104.56.1	10.104.63.254
255.255.252.0	22	1022	10.104.62.11	10.104.60.1	10.104.63.254
255.255.254.0	23	510	10.104.62.11	10.104.62.1	10.104.63.254
255.255.255.0	24	254	10.104.62.11	10.104.62.1	10.104.62.254
255.255.255.128	25	126	10.104.62.11	10.104.62.1	10.104.62.126
255.255.255.192	26	62	10.104.62.11	10.104.62.1	10.104.62.62
255.255.255.224	27	30	10.104.62.11	10.104.62.1	10.104.62.30
255.255.255.240	28	14	10.104.62.11	10.104.62.1	10.104.62.14
255.255.255.248	29	6	10.104.62.11	10.104.62.9	10.104.62.14
255.255.255.252	30	2	10.104.62.11	10.104.62.9	10.104.62.10
255.255.255.254	31	0	10.104.62.11		
255.255.255.255	32	1	10.104.62.11	10.104.62.11	10.104.62.11

Running Quick Discovery

If you want to quickly run discovery without specifying and saving your settings, you can use Quick Discovery.

You can view the guest users discovered by Prime Infrastructure by choosing **Services > Network Services > Guest Users**. To see the correct lifetime on guest user accounts after they are discovered, make sure the devices have the correct time settings specified.

To run Quick Discovery, follow these steps:

Step 1 Choose **Inventory > Device Management > Discovery**.

Step 2 In the top-right side of the page, click **Quick Discovery**.

Step 3 Complete the required fields, then click **Run Now**.

Verifying Discovery

When discovery is completed, you can verify that 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. See Table 3-1 for information about discovery settings.
- Add devices manually. See Adding Devices Manually for more information.

Importing 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 Prime Infrastructure as explained in the following steps:

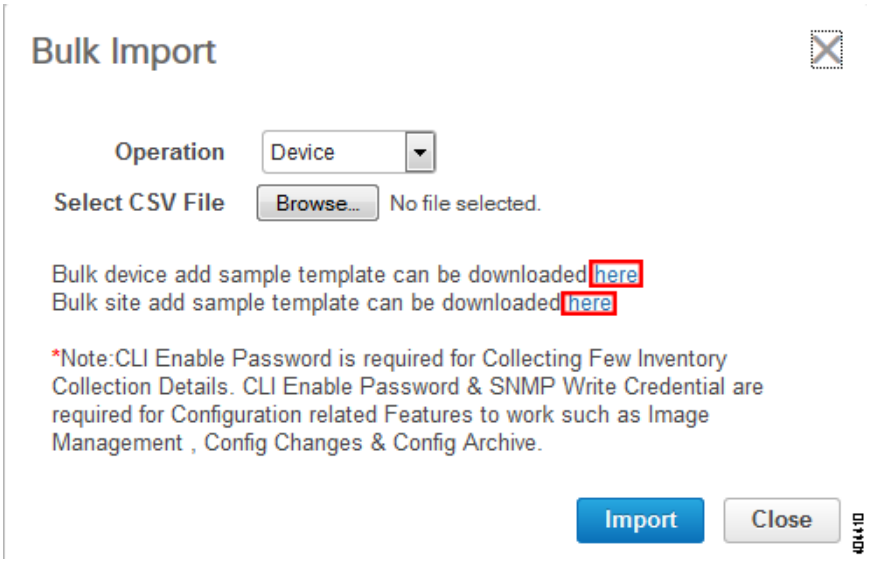
Step 1 Choose **Inventory > Device Management > Network Devices**, then click **Bulk Import**.

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

Step 3 In the **Select CSV File,** enter or browse to the CSV file that contains the devices that you want to import.

Step 4 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. See Figure 3-1.

Figure 3-1 Downloading a Sample Template for Importing Devices or Sites



Make sure that you retain the required information in the CSV file as explained in CSV File Requirements for Importing Devices.

If the importing CSV file contains any UDF parameters, ensure that UDF is configured in **Administration > Settings > System Settings > Inventory > User Defined Fields** prior to importing the devices. The UDF column in the CSV file must be begin with **UDF:** as indicated in the sample CSV template.

Step 5 Click **Import**.

Step 6 Check the status of the import by choosing **Administration > Dashboards > Job Dashboard > User Jobs > Import**.

Step 7 Click the arrow to expand the job details and view the details and history for the import job.

CSV File Requirements for Importing Devices

If you want to use a CSV file to import your devices or sites from another source into Prime Infrastructure, you can download a sample template by choosing **Inventory > Device Management > Network Devices**, then clicking **Bulk Import**. Click the link to download a sample template as shown in Figure 3-1.

When you download a sample CSV template for importing devices or sites, the extent to which Prime Infrastructure can manage your devices, depends on the information you provide in the CSV file. If you do not provide values for CLI username, password, and enable password, Prime Infrastructure will have limited functionality and cannot modify device configurations, update device software images, and perform any other valuable functions. 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, then the manually entered credentials takes high priority and the device is manged based on the combination of manually entered credentials and credential profile. For example, if the CSV file contains 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.

- For partial inventory collection in Prime Infrastructure, you must provide the following values 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 provide the following values in the CSV file:
  - Device IP address
  - SNMP version
  - SNMP read-only community strings
  - SNMP write community strings
  - SNMP retry value
  - SNMP timeout value
  - Protocol

    You must also provide values for the fields that correspond to the protocol you specify. For example, if you specify SNMPv3, you must specify values for the SNMPv3 fields in the sample CSV file such as the SNMPv3 username and authorization password.
  - CLI username

- CLI password
- CLI enable password
- CLI timeout value

Adding Devices Manually

Adding devices manually is helpful if you want to add a single device. If you want to add all devices in your network, we recommend that you run discovery (see Running Discovery) or import devices from a CSV file (see Importing Devices from Another Source).

After adding a device in the Converged view with profile, if you edit the device (which is associated with Credential Profile) in the Classic view, the Credential Profile association of the device is removed.

To add devices manually, follow these steps:

Step 1 Choose **Inventory > Device Management > Network Devices**.

Step 2 Click **Add Device**.

Step 3 Complete the required fields.

Step 4 For the License Level field, select

- **Full** to collect all device information and have Prime Infrastructure manage the device. Managed devices count against the number of managed devices in your Prime Infrastructure license. **Full** is selected by default.
- **Switch Port Trace Only** to collect partial device information (host name, device name, device type, and reachability status) and allow Prime Infrastructure to display how an AP is connected to a WLC on wireless maps. Switch Port Trace Only devices do not count against the number of managed devices in your Prime Infrastructure license. You cannot perform device management operations on devices that you designate as Switch Port Trace Only.

See Enabling IPSec Communication When Adding Devices for information about enabling IPSec.

Step 5 (Optional) Click **Verify Credentials** to verify the device credentials before adding the device.

Note Prime Infrastructure provides HTTP credentials verification support for NAM devices only.

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

Note User Defined Field (UDF) parameters are available only if you added them under **Administration > Settings > System Settings > Inventory > User Defined Fields**. Do not use the special characters : ; and # for UDF field parameters.

Enabling IPSec Communication When Adding Devices

We recommend that you use IPSec tunneling to secure wireless management traffic between your network devices and Prime Infrastructure servers. Using IPSec between the management system and the managed devices provides an additional layer of security.

To enable IPSec when adding a device to Prime Infrastructure:

Step 1 Choose **Inventory > Device Management > Network Devices**.

Step 2 Click **Add Device.**

Step 3 Complete the required fields.

Step 4 Under IPSec Parameters, click Enable IPSec Communication, then complete the required fields.

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

About Adding Wireless Devices

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

- When a controller is removed from the system, a warning message appears to confirm whether the associated access points need to be removed.
- If you are adding a controller into the Prime Infrastructure across a GRE link using IPSec or a lower MTU link with multiple fragments, you might need to adjust the Maximum VarBinds per Get PDU and Maximum VarBinds per Set PDU. If it is set too high, the controller might not be added into Prime Infrastructure.

  To adjust the Maximum VarBinds per Get PDU or Maximum VarBinds per Set PDU: Stop the Prime Infrastructure, choose **Administration > Settings > System 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 receive the error message ‘Sparse table not supported', verify that Prime Infrastructure and WLC versions are compatible and retry. For information on compatible versions, see the following URL: http://www.cisco.com/en/US/docs/wireless/controller/5500/tech_notes/Wireless_Software_Compatibility_Matrix.html.
- When a controller is added to Prime Infrastructure, Prime Infrastructure acts as a TRAP receiver and the following traps are enabled on the controller: 802.11 Disassociation, 802.11 Deauthentication, and 802.11 Authenticated.
- In the **Inventory > Network Devices > All Devices > Wireless Controllers** page, to update the credentials of multiple controllers in bulk, select the controllers you need to update and click **Edit**. Select the credential profile and click **Update** or **Update & Sync**.
- You can also update the credentials of multiple controllers in bulk by choosing a CSV file. Select the controllers and click **Bulk Import**. Browse the CSV file that contains a list of controllers to be updated, one controller per line. Each line is a comma separated list of controller attributes.
- When a controller is added, the **Reachability** of the controller will be **Unknown**, while Prime Infrastructure attempts to communicate with the controller that you added. The Reachability of the controller changes to **Reachable** or **Ping Reachable** once the communication with the controller is successful.

Validating That Devices Were Added Successfully

After collecting device information, Prime Infrastructure gathers and displays the configurations and the software images for the devices. To verify that your devices were successfully added to Prime Infrastructure, you can choose **Inventory > Device Management > Network Devices** and

- 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 Prime Infrastructure collected from the devices.
- View details about the information that was collected from the device by hovering your mouse over the **Inventory Collection Status** field and clicking the icon that appears.
- Check the **Device Reachability Status** column. See Table 3-3 for status descriptions. HTTP/HTTPS parameters are verified on NAM devices only.
- Check the Admin Status column. See Table 3-4 for descriptions of the possible Admin Status values.
- To view details about the collection job and the details and history for the import job, choose **Administration > Dashboards > Job Dashboard**.

See Troubleshooting Unmanaged Devices for information about how to resolve any errors.

Table 3-3 Descriptions of Device Reachability Status

Reachability Color	Description
Green	Prime Infrastructure is able to reach the device using SNMP.
Yellow	The device is reachable using Ping, but not via SNMP. Verify that you specified the correct SNMP parameters for read access when the device was added to Prime Infrastructure.
Red	Prime Infrastructure is unable to reach the device using Ping. Verify that the device is operational and connected to the network.

Table 3-4 Descriptions of Device Admin Status

Admin Status	Description
Managed	The device has been added successfully to Prime Infrastructure using SNMP.
Unmanaged	The device credentials are incorrect or you have exceeded the number of devices allowed by your license. Choose **Administration > Licenses** to view the status of your license. See the *Cisco Prime Infrastructure 3.0 Administrator Guide* for information about managing licenses, troubleshooting licensing issues, and verifying license details.

Verifying Device Credentials

Prime Infrastructure automatically verifies device credentials as part of the inventory process. You can view device credential verification information by choosing **Reports > Report Launch Pad > Device > Device Credential Verification**.

Editing 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 Click **Edit**.

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.

Synchronizing 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**.

Adding 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—Re-enter the password to confirm.

Step 4 Choose **Update**.

Related Topics

Enabling NAM Data Collection

Defining NAM Polling Parameters

Exporting Devices

In Prime Infrastructure, you can export device information as a CSV file. Prime Infrastructure does not export credential profiles.

To export devices, follow these steps:

Step 1 Choose **Inventory > Device Management > Network Devices**.

Step 2 Select the devices that you want to export, then click **Export Device**.

Step 3 Enter an encryption password that will be used to open the exported CSV file.

Step 4 Confirm the encryption Password and click **Export** to export the device information.

Step 5 Double-click the ExportDevice.zip file and enter the encryption password to open the ExportDevice.csv file.

Caution The device export CSV file includes all device credentials and should be handled with appropriate care. Similarly, the privilege to allow device export should be assigned to appropriate users only.

Next Steps

Now that you have added devices to Prime Infrastructure, you can create device groups and port groups to simplify management, monitoring, and configuration of similar devices and ports. See Grouping Devices.

You might also want to:

- Plan for devices that will be added to your network in the future—See Preconfiguring Devices to be Added Later.
- Configure wired and wireless features on your devices using guided, step-by-step instructions—See Getting Help Setting Up Access Switches.