Configuring Plug and Play

Prime Infrastructure helps automate the deployment of new devices on the network by obtaining and applying the necessary software image and configuration on a new network device. Using features such as Cisco Network Services (CNS) call-home, APIC-EM (Application Policy Infrastructure Controller) call-home and Cisco IOS auto-install (which uses DHCP and TFTP), Prime Infrastructure reduces the time a new device takes to join the network and become functional.

The Plug and Play feature of Prime Infrastructure uses the templates defined in Configuration > Features and Technologies that you can reuse and apply to new devices. You can streamline new device deployment by creating bootstrap templates, which define the necessary initial configurations to enable the device to communicate with Prime Infrastructure. You can specify (and predeploy) software images and configurations that will be added to the devices in the future. See Using Templates to Configure Devices to know more on template creation.

Related Topics
- Prerequisites for Delivering Plug and Play Profiles
- Plug and Play Workflow

Prerequisites for Delivering Plug and Play Profiles

Based on the method that you select to deliver the Plug and Play profile to new devices, you must make sure that you have completed the necessary prerequisites.

- Configure DHCP with the appropriate settings in the network as described in Sample DHCP Server Settings.
- You must have an existing network connection (distribution/core) available in the branch or campus to where the new device is connecting.
- The branch must have direct connectivity to the Prime Infrastructure server, or you must use the Plug and Play external server to connect to Prime Infrastructure.
- Ensure TFTP is enabled on the Prime Infrastructure server by choosing Administration > Settings > System Settings > Server, then clicking Enable under TFTP. TFTP is enabled by default. This is an optional requirement for APIC-EM mode.
Plug and Play Workflow

Prime Infrastructure allows you to perform an initial provisioning of a software image and configuration on a new device. To automate the deployment of a new device on your network, follow this workflow:

1. Specify which of the following servers Prime Infrastructure uses for Plug and Play. If you do not specify the server, CNS gateway will be enabled by default.
   - CNS gateway—You use the CNS gateway that is bundled with Prime Infrastructure by default, or use an external CNS gateway.
   - APIC-EM—You can specify that Prime Infrastructure uses APIC-EM for Plug and Play. See Integrating APIC-EM with Prime Infrastructure for information about setting up APIC-EM.

2. Create a Plug and Play profile for your devices. The profiles are categorized as Routers, Switches, Wireless AP and Nexus Profiles. See Plug and Play Profiles.

3. Power on the device.

4. Apply a bootstrap configuration to the device. The bootstrap configuration is a minimal configuration that is required for devices to establish a connection to the Prime Infrastructure gateway (CNS or APIC-EM). See Bootstrap Configuration.
   
   In the case of Wireless AP profiles, the Primary, Secondary and Tertiary WLC details are required. See Creating Plug and Play Profiles for Wireless AP.

   **Note**

   In the case of Nexus devices, the Plug and Play workflow differs as these devices do not support bootstrap configuration. See Creating Plug and Play Profiles for Nexus Devices for more details.

After you apply the initial configuration:

1. The device communicates with the Prime Infrastructure server.

2. Based on the Device Plug and Play ID / serial number, Prime Infrastructure verifies if this matches with the device ID in any of the Plug and Play preprovisioning definitions.

3. If there is a match, Prime Infrastructure applies the software image and the configuration specified in the matched Plug and Play profile on the device.
   
   If there is no match for the device ID, Prime Infrastructure matches the device type with any of the existing type-based Plug and Play preprovisioning definitions.

4. The device is added to its inventory and is managed by Prime Infrastructure.

5. Once the device is added and managed in the inventory, Prime Infrastructure applies the post Plug and Play configurations, if specified in the Plug and Play profile, on the device.
After the bootstrap configuration is applied to the device, the installer connects the device to a WAN at the remote site. The device connects to the Plug and Play gateway using its serial number, and downloads the full configuration and (optional) Cisco IOS image (see Figure 27-1).

**Figure 27-1 Plug and Play Branch Deployment**

Related Topics

- Bootstrap Configuration
- Plug and Play Profiles

**Viewing Plug and Play Dashboard**

Choose Configuration > Plug and Play > Dashboard and select the Home tab to view the dashboard of the Plug and Play application.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Click <strong>About</strong> to know about Plug and Play feature. See <strong>Configuring Plug and Play</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Click <strong>Monitoring</strong> to view the details of devices in a map view. See <strong>Integrating Map View</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Click <strong>Errors / Progress / Success</strong> to navigate to <strong>Device Status</strong> page. The details will be filtered and displayed accordingly.</td>
</tr>
<tr>
<td>4</td>
<td>Click to navigate to <strong>Device Status</strong> page to monitor the devices and its status.</td>
</tr>
<tr>
<td>5</td>
<td>Click to navigate to <strong>Bootstrap</strong> page to create bootstrap templates for profiles.</td>
</tr>
<tr>
<td>6</td>
<td>Click to navigate to <strong>Administration &gt; Servers &gt; APIC-EM Controller</strong> page.</td>
</tr>
<tr>
<td>7</td>
<td>Click to navigate to <strong>Plug and Play Profiles</strong> page to create profile for a device type.</td>
</tr>
<tr>
<td>8</td>
<td>Click to navigate to <strong>Profile Activation</strong> page to activate by providing values specific to device/type.</td>
</tr>
<tr>
<td>9</td>
<td>Click to navigate to <strong>Device Status</strong> page.</td>
</tr>
<tr>
<td>10</td>
<td>Click to navigate to <strong>Map View</strong> page to view the devices and their site locations.</td>
</tr>
<tr>
<td>11</td>
<td>Click to navigate to <strong>Plug and Play Profiles</strong> page.</td>
</tr>
<tr>
<td>12</td>
<td>Click to navigate to <strong>Administration &gt; Dashboard &gt; Jobs Dashboard</strong> page to view the job status.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Integrating APIC-EM with Prime Infrastructure
- Integrating Map View
- Plug and Play Profiles
- Activating Device Profiles
- Bootstrap Configuration
- Verifying Device Status
Chapter 27      Configuring Plug and Play

APIC-EM and Plug and Play

Prime Infrastructure supports APIC-EM GA Release 1.0.0.x. You can specify to have Prime Infrastructure use the APIC-EM for Plug and Play. You must preconfigure a profile which determines what is deployed on the devices (configurations, images, etc.). When the device calls home, based on the device’s serial number, the profile is matched and the device is provisioned with the same pre-configured image and configuration from Prime Infrastructure using APIC-EM’s Plug and Play.

With APIC-EM Plug and Play integration, devices can be provisioned with http/https. If applicable, when the profile is created, you can also choose to install PKI (Public Key Infrastructure) and SUDI (Secure Unique Device Identifier) certificates on the device to use PKI and SUDI based authentication.

Note
Prime Infrastructure supports only APIC-EM for Wireless AP profiles.

Related Topics
• Integrating APIC-EM with Prime Infrastructure
• Plug and Play Workflow

Integrating APIC-EM with Prime Infrastructure

Prime Infrastructure communicates with APIC-EM via HTTPs and REST API’s exposed by APIC-EM.

Note
Prime Infrastructure requires a dedicated APIC-EM server. Hence you must not integrate the APIC-EM server with more than one Prime Infrastructure server to prevent data corruption and out of sync condition.

To integrate APIC-EM controller to Prime Infrastructure, follow these steps:

Step 1 Choose Configuration > Plug and Play > Dashboard.
Step 2 In the Home tab, click on Server to view the Administration > Servers > APIC-EM Controller page.
Step 3 Click Add.
Step 4 Enter the APIC-EM controller IPv4 address.
Step 5 Enter the HTTPS port number to connect with APIC-EM.
Step 6 Enter your user name.
Step 7 Enter your password and confirm it.

The polling interval is not editable. The APIC-EM controller is polled periodically (every 5 minutes) to check the status of its connection / integration with Prime Infrastructure.

After the APIC-EM controller is added to Prime Infrastructure, you can view the reachability status of the APIC controller in same page. You can select a specific APIC-EM controller to view the history of the connection polling status. Make sure the APIC-EM connection is successful before using the service.

To navigate to Configuration > Plug and Play > Dashboard, click the link Please Click here to create Plug and Play Profiles.
Chapter 27 Configuring Plug and Play

Plug and Play Profiles

The global option in Administration > Servers > APIC-EM Controller > Global PnP/ZTD Settings is automatically set to APIC-EM when you add a valid APIC-EM controller into Prime Infrastructure.

Related Topics
- Plug and Play Profiles
- Bootstrap Configuration
- Viewing Plug and Play Dashboard

Plug and Play Profiles

Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles. The detailed summary of the list of plug and play profiles are displayed.

Prime Infrastructure helps you create a Plug and Play Profile that allows any newly connected device to “call home” to the Prime Infrastructure server so that the device can be discovered, added to the inventory, and configured. This profile, also known as a Bootstrap Profile, places credentials on the device, eliminating the need to “console” into every device to setup before the device can be managed by Prime Infrastructure.

You can create any of the following Plug and Play profiles under the specific folders:
- Router profiles - See Creating Plug and Play Profiles for Routers and Switches
- Switch profiles - See Creating Plug and Play Profiles for Routers and Switches
- Wireless AP profiles - See Creating Plug and Play Profiles for Wireless AP
- Nexus profiles - See Creating Plug and Play Profiles for Nexus Devices

Depending on the type, you can create Plug and Play profiles that contain:
- Software images only.
- Configurations only.
- Both software images and configurations.
- PKI certificates and SUDI certificates (For APIC-EM only.)
- Primary and Secondary Controllers, AP and Flexconnect groups (For Wireless AP only.)

The profile can include additional post Plug and Play configurations (optional), that can be applied on the device only after the device is managed by Prime Infrastructure.

Note
You cannot create a profile under the root Plug and Play Profiles folder. Depending on the profile-type, you can create profiles only under the specific folders - Nexus Profiles, Switch Profiles, Router Profiles and Wireless AP Profiles.

Note
PnP scale supports any number of devices distributed across profiles, but a profile can support maximum of 100 devices per profile instance. If you want to increase this scale, create additional profile and add devices to the new profile.
Creating Plug and Play Profiles for Routers and Switches

A Plug and Play profile must have at least one of the following:

- A bootstrap configuration—Prime Infrastructure provides a standard bootstrap configuration, or you can create your own. See Bootstrap Configuration.
- Software image—See Managing Software Images.
- Configuration CLI template (PnP and Post PnP configuration)—See CLI Templates.

---

**Step 1** Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles.

**Step 2** Select the required profile (Router Profiles or Switch Profiles) from the left navigation pane, then click Add to view the details in Profile Summary tab.

**Step 3** Provide the required information in the Profile Basic section.
- If you select Router or Switch from the Device Type drop-down list, then you will be required to select the required credential profile from the Credential Profile drop-down list to associate the credentials common to the device. See Using Credential Profiles.

**Step 4** (Optional) If you selected APIC-EM for Plug and Play, in the Profile Detail section, check the Enable PKI check box to provision devices with PKI certificates. PKI certificates are installed on the device after the Image provision and configuration are complete. See Cisco Open Plug-n-Play Agent Configuration Guide, Cisco IOS XE Release 3E for more information.

This option is available for users who have selected APIC-EM as the Plug and Play server. You cannot select this option if you selected CNS as the Plug and Play server.

If the Enable PKI check box is unchecked, the device is not provisioned with PKI certificates.

**Note** Enable PKI check box will be disabled for Switch Profiles.

**Step 5** (Optional) If you selected APIC-EM for Plug and Play, in the Profile Detail section, check the Enable SUDI check box to provision devices with SUDI certificates. By enabling this option, you can specify that the APIC-EM controller must validate the SUDI certificate to authenticate the device.

**Step 6** From the Bootstrap Template drop-down list, select the bootstrap templates. You can also create a customized bootstrap template which will be saved in PnP Bootstrap Templates (User Defined). See Bootstrap Configuration.

**Step 7** (Optional) From the Software Image drop-down list, select the required software images. This step is required only if you want to provision the device with images. See Importing Software Images for Plug and Play Profiles.

The Image Location text box is disabled if you selected APIC-EM for Plug and Play.
Step 8  (Optional) From the **Configuration Template** drop-down list, select a previously created configuration template.

Step 9  (Optional) From the **Post PnP Configuration Template** drop-down list, select the required configuration template. This configuration is applied on the device once it is managed by Prime Infrastructure.

Step 10  Click **Save as New Plug and Play Profile**.

Step 11  The profile is created and the details in **Profile Summary** tab is displayed. You can edit the details and click **Save** to save the details in the same profile and click **Save as New** to create a new profile.

Step 12  Click **Profile Instances** tab.

Step 13  Click **Add** to add details for the devices for which you want to pre-provision the Plug and Play Profile. See **Adding Device Profiles into Router and Switches Plug and Play Profiles**.

**Related Topics**

- Adding Device Profiles into Router and Switches Plug and Play Profiles
- Importing Device Profiles into Plug and Play Profiles
- Activating Device Profiles
- Cisco Open Plug-n-Play Agent Configuration Guide, Cisco IOS XE Release 3E
- Bootstrap Configuration

**Importing Software Images for Plug and Play Profiles**

You can import a software image to include it as part of a Plug and Play profile.

Step 1  Choose **Inventory > Device Management > Software Images**.

Step 2  Click **Import**, then specify the source from which the software image is to be imported.

Step 3  Specify the collection options and when to import the image file. You can run the job immediately or schedule it to run at a later time.

The image import job will run only once.

Step 4  Click **Submit**.

Step 5  To view the details of image management job, choose **Administration > Dashboards > Job Dashboard**.

**Creating Plug and Play Profiles for Wireless AP**

You can create a plug and play profile for a wireless AP to provision thousands of devices at a time.

Step 1  Choose **Configuration > Plug and Play > Dashboard** and in the **Home** tab, click **PnP Profiles**.

Step 2  Select **Wireless AP Profiles** from the left navigation pane and click **Add** to view the details in the **Profile Summary** tab.

Step 3  Provide the required information in the Profile Basic section.
In the Device Type field, Autonomous AP is auto-populated and is non-editable. It is mandatory to provide the PID value for Wireless AP profiles.

**Step 4** Provide the required information in the Profile Detail section.

**Step 5** Click **Save as New Plug and Play Profile**.

**Step 6** The profile is created and the details in **Profile Summary** tab is displayed. You can edit the details and click **Save** to save the details in the same profile and click **Save as New** to create a new profile.

**Step 7** Click **Profile Instances** tab.

**Step 8** Click **Add** to add details for the devices for which you want to pre-provision the Plug and Play Profile. See **Adding Device Profiles into Wireless AP Plug and Play Profiles**.

---

**Related Topics**
- Adding Device Profiles into Wireless AP Plug and Play Profiles
- Bootstrap Configuration
- Verifying Device Status

---

**Prerequisites for Connecting a Nexus Device in the Network**

The following prerequisites should be met before connecting the Nexus device to the network:

- A DHCP server to bootstrap the interface IP address, gateway address, script server (Cisco Prime Infrastructure 3.1) and script file (Plug and Play). See **Configuring DHCP Server**.
- A TFTP or HTTP server containing the configuration script used to automate the software image installation and configuration process. See **Configuring HTTP Server**.
- Cisco Prime Infrastructure 3.1 server with created Plug and Play Nexus profile containing the software images and configuration files. See **Creating Plug and Play Profiles for Nexus Devices**.

**Configuring DHCP Server**

The Nexus device sends out DHCP discover messages on all of the active interfaces (including the management interface) soliciting DHCP offers from the DHCP server or servers. The DHCP client on the Nexus device uses the device serial number or its MAC address in the client-identifier option to identify itself to the DHCP server. The DHCP server uses this identifier to send information, such as the IP address and script file name, back to the DHCP client.

The DHCP discover message also mandates the following options:

- Option 66 (TFTP server name) or Option 150 (TFTP server address)—The DHCP server relays the TFTP server name or TFTP server address to the DHCP client. The DHCP client uses this information to contact the TFTP server to obtain the script file.
- IP address
- Default Gateway
- Option 67 (Bootfile name)—The DHCP server relays the bootfile name to the DHCP client. The bootfile name includes the complete path to the bootfile on the TFTP server which is used by the DHCP client to download the script file.
Chapter 27 Configuring Plug and Play

Plug and Play Profiles

Related Topics

- Configuring HTTP Server
- Creating Plug and Play Profiles for Nexus Devices
- Prerequisites for Connecting a Nexus Device in the Network
- Adding Device Profiles into Nexus Plug and Play Profiles

Configuring HTTP Server

Choose Administration > Settings > System Settings > General and select Server from the left navigation menu.

In the HTTP Forward section, select Enable to enable the device to contact the Plug and Play Gateway for downloading initial configuration and image. The default port is 80 but you can still change the port configuration on the device.

Note
Restart Prime Infrastructure for the changes to reflect.

Related Topics

- Configuring DHCP Server
- Creating Plug and Play Profiles for Nexus Devices
- Adding Device Profiles into Nexus Plug and Play Profiles
- Prerequisites for Connecting a Nexus Device in the Network

Creating Plug and Play Profiles for Nexus Devices

To create a Plug and Play profile for Nexus devices, follow these steps:

**Step 1** Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles.

**Step 2** Select Nexus Profiles from the left navigation pane and click Add to view the details in the Profile Summary tab.

**Step 3** Provide the required information in the Profile Basic section.
Select the required credential profile from the Credential Profile drop-down list to associate the credentials common to the device. See Using Credential Profiles.

**Step 4** From the System Image and Kick Start Image drop-down lists, select the required software images. See Importing Software Images for Plug and Play Profiles.

Note
While downloading from Cisco.com, ensure that both system and kick start images have the same image version.

**Step 5** From the Configuration Template drop-down list, select either the system-defined Nexus POAP Configuration Template or a previously created configuration template and make additional changes.

**Step 6** Click Save as New Plug and Play Profile.
Activating Device Profiles

You can pre-provision a device on any defined profile, and activate by providing values specific to device/type. To add devices in bulk, see Importing Device Profiles into Plug and Play Profiles.

You can perform either one of the following:

- Create a new plug and play profile and add device profiles to the created plug and play profile. See Creating New Plug and Play Profiles and Adding Device Profiles.
- Add device profiles to an existing plug and play profile. See Adding Device Profiles to an Existing Plug and Play Profile.

Alternatively, you can choose Configuration > Plug and Play > Dashboard, in the Home tab, click PnP Profiles to create a new Plug and Play profile. After creating the required Plug and Play profile, click Add in the Profile Instances tab to add device profiles.

Related Topics

- Adding Device Profiles into Router and Switches Plug and Play Profiles
- Adding Device Profiles into Wireless AP Plug and Play Profiles
- Adding Device Profiles into Nexus Plug and Play Profiles

Creating New Plug and Play Profiles and Adding Device Profiles

Step 1 Choose Configuration > Plug and Play > Dashboard and in the Home tab, click Profile Activation.
Step 2 In the Select PnP Profile page, select Add device by creating new Profile.
Step 3 Select the type of profile you want to create from the Profile Type drop-down list.
Step 4 Enter the required information in the Profile Basic and Profile Detail sections. See Plug and Play Profiles for information on profile creation.
Step 5 Click the arrow icon in the right to navigate to the Plug and Play Profile page to add device profiles to the created plug and play profile.
Related Topics

- Adding Device Profiles to an Existing Plug and Play Profile
- Adding Device Profiles into Router and Switches Plug and Play Profiles
- Adding Device Profiles into Wireless AP Plug and Play Profiles
- Adding Device Profiles into Nexus Plug and Play Profiles

Adding Device Profiles to an Existing Plug and Play Profile

Step 1 Choose Configuration > Plug and Play > Dashboard and in the Home tab, click Profile Activation.

Step 2 In the Select PnP Profile page, select Add device to an existing profile.

Step 3 Select the required profile from the Select Profile drop-down list, for which you need to add device profiles. See Plug and Play Profiles for information on profile creation.

Step 4 The details of the profile you selected gets auto-populated and are non-editable.

Step 5 Click the arrow icon in the right to navigate to the Plug and Play Profile page to add device profiles to the created plug and play profile.

Related Topics

- Creating New Plug and Play Profiles and Adding Device Profiles
- Adding Device Profiles into Router and Switches Plug and Play Profiles
- Adding Device Profiles into Wireless AP Plug and Play Profiles
- Adding Device Profiles into Nexus Plug and Play Profiles

Adding Device Profiles into Router and Switches Plug and Play Profiles

To add a device profile to the required Plug and Play profile, follow these steps:

Step 1 In the Plug and Play Device Provisioning Profile page, provide the required information.

- Select the site location to which the device will be mapped from the Location drop-down list. This detail will be displayed in the Map View.

Note Before you add a device to a specific location, create a location group in Inventory > Device Management > Network Devices or Inventory > Group Management > Network Device Groups. See Using Location Groups.

Step 2 Click the arrow icon in the right to navigate to the Bootstrap Selection page.

Step 3 In the Bootstrap Selection page, the bootstrap template you selected in the profile creation phase will get auto-populated. You can edit the values as required.

- Plug and Play Gateway Location—By default, the Prime Infrastructure server acts as the Plug and Play gateway server. You can modify the server by providing the external Plug and Play gateway IP address.
Click CLI to view the CLI summary of the bootstrap configured.

**Step 4** Click the arrow icon in the right to navigate to the next pages.

**Note** If you had selected Software Image and Configuration Template in the profile creation phase, the Software Image, Configuration and Post PnP Configuration tabs will be displayed in the Profile Activation page.

**Step 5** (Optional) In the Software Image page, provide the required information.

**Step 6** (Optional) In the Configuration page, the configuration template you selected in the profile creation phase will be auto-populated. Provide the required information and navigate to the next page.

Click CLI to view the CLI summary.

**Step 7** (Optional) In the Post PnP Configuration page, the configuration template you selected in the profile creation phase will be auto-populated. Provide the required information and navigate to the next page.

Click CLI to view the CLI summary.

**Step 8** In the Management Credentials page, provide the required information. These device parameters will be applied on the devices on provisioning.

**Note** If the device type is a router or switch, then in the Management Credentials page, the credential profile you selected in the profile creation phase will be auto-populated and the values cannot be edited.

**Step 9** In the Profile Activation Summary page, the device details with their configurations is displayed.

**Step 10** Click Finish to provision the device profile.

On successful provisioning, the device profile will be displayed in the Profile Instances page of the specific profile. Alternatively, the provisioning status of the device can be viewed at the Device Status page.

After the device is provisioned successfully, the device is added to the Prime Infrastructure inventory so that the device can be managed. The device is added to the Prime Infrastructure inventory based on the management parameters provided in the Plug and Play Profile. After the device is added successfully to the inventory, additional post Plug and Play configurations (if applicable) are applied on the device.

If there is a mismatch in credentials, the device is added to the inventory, but it will not have “Managed” status.

**Related Topics**

- Importing Device Profiles into Plug and Play Profiles
- Plug and Play Profiles
- Creating Plug and Play Profiles for Routers and Switches
- Adding Device Profiles into Wireless AP Plug and Play Profiles
- Adding Device Profiles into Nexus Plug and Play Profiles
Importing Device Profiles into Plug and Play Profiles

You can perform import and export operations on device profiles in bulk. Instead of adding devices and specifying their attributes one at a time, you can import a CSV file that includes all the devices and their attributes. By performing bulk import, you can update the existing profiles and add new profiles. To update more than one device profile at a time, you can perform bulk export.

**Step 1** Choose **Configuration > Plug and Play > Dashboard** and in the **Home** tab, click **PnP Profiles**.

**Step 2** Select the required Plug and Play profile from the left navigation menu. The details in **Profile Summary** tab is displayed.

**Step 3** Click **Profile Instances** tab.

**Step 4** Select the device profiles check-boxes you need to edit and click **Export**.

The CSV file with the device properties will be exported. You can add devices or edit the properties of the existing devices in the spreadsheet. Do not change the attribute names while editing the spreadsheet.

**Note** If you want to export a blank CSV file, click **Export** without selecting any device profiles. A blank csv file will be exported even if there are no device profiles in the **Profile Instances** page.

**Step 5** Click **Import** and choose the CSV file in which you entered the device details. Click **Upload**.

The CSV file is uploaded and a link to **Administration > Dashboard > Jobs Dashboard** is displayed.

**Step 6** In the **Jobs Dashboard** page, click **Import** from the left navigation menu to view the job status of the bulk imported file.

**Related Topics**
- Creating Plug and Play Profiles for Routers and Switches
- Adding Device Profiles into Wireless AP Plug and Play Profiles
- Adding Device Profiles into Nexus Plug and Play Profiles

**Deployment Based on Device Type**

If you are using a CNS gateway only for Plug and Play, to deploy a Plug and Play profile based on the device type, you do not have to associate the device ID with the deployment profile. Device type-based deployment is useful primarily for switches that use the same set of images and configurations. Matching profiles are identified by the device type (PID) of the incoming device that is specified in the profile during the design phase.

During device type-based deployment:

1. The device type is matched hierarchically; Prime Infrastructure searches for a profile with the same device type as that of the incoming device. If the profile does not match the device type, Prime Infrastructure searches for a profile that is defined for a higher level of the device type in the hierarchy.

For example:
2. If the ‘switch_profile’ in Prime Infrastructure is defined for ‘Switches and Hubs’ and the incoming device is of type Switches and Hubs > Catalyst 2928 Series Switches > Catalyst 2928-24TC-C switch, and

- If there is no profile defined specifically for this switch (Catalyst 2928-24TC-C or Catalyst 2928 Series Switches), then the ‘switch_profile’ is considered for deployment.

2. If Prime Infrastructure has multiple matching deployment profiles for a given device type, then Prime Infrastructure chooses the deployment profile that is created or has been recently updated.

---

Adding Device Profiles into Wireless AP Plug and Play Profiles

Prime Infrastructure supports only APIC-EM for Wireless AP profiles. You must preconfigure a plug and play profile which determines the primary, secondary and tertiary WLC details that is required to be provisioned on the devices. See Creating Plug and Play Profiles for Wireless AP.

When the AP (Access Point) is connected to a network, the AP contacts the DHCP of the network to know the APIC-EM details. The AP then contacts the APIC-EM and based on the device’s serial number and PID, the profile is matched. AP contacts WLC which then pushes the image and configurations to the device.

To add a device profile to the required Plug and Play profile, follow these steps:

---

**Step 1**

In the **Plug and Play Device Provisioning Profile** page, provide the required information.

- Select the site location to which the device will be mapped from the **Location** drop-down list. This detail will be displayed in the Map View.

---

**Note**

Before you add a device to a specific location, create a location group in **Inventory > Device Management > Network Devices** or **Inventory > Group Management > Network Device Groups**. See Using Location Groups.

---

**Step 2**

In the **Profile Activation Summary** page, the device details with their configurations is displayed.

**Step 3**

Click **Finish** to provision the device profile.

On successful provisioning, the device profile will be displayed in the **Profile Instances** page of the specific profile. Alternatively, the provisioning status of the device can be viewed at the **Device Status** page.

---

**Related Topics**

- Activating Device Profiles
- Plug and Play Profiles
- Creating Plug and Play Profiles for Wireless AP
- Adding Device Profiles into Router and Switches Plug and Play Profiles
- Adding Device Profiles into Nexus Plug and Play Profiles
Adding Device Profiles into Nexus Plug and Play Profiles

Before you begin, there is a set of prerequisites to be met. See Prerequisites for Connecting a Nexus Device in the Network.

When a Nexus device is connected to the network, it follows the below workflow:

1. Locates the configured DHCP server and establishes communication to get the IP Address, gateway, script server (Cisco Prime Infrastructure 3.1) and the script file (Nexus Plug and Play profile).
2. The device then communicates with the Cisco Prime Infrastructure and downloads the created Plug and Play profile for Nexus device. See Creating Plug and Play Profiles for Nexus Devices.
3. The device then obtains the IP address of a TFTP server or URL of an HTTP server from which it downloads the image and the necessary configuration files.

To add a device profile to the required Plug and Play profile, follow these steps:

**Step 1**
In the **Plug and Play Device Provisioning Profile** page, provide the required information.
- Select the site location to which the device will be mapped from the **Location** drop-down list. This detail will be displayed in the Map View.

**Note**
Before you add a device to a specific location, create a location group in **Inventory > Device Management > Network Devices** or **Inventory > Group Management > Network Device Groups**. See Using Location Groups.

**Step 2**
Click the arrow icon in the right to navigate to the **Image Selection** page.

The selected system and kick start images are auto-populated and cannot be edited.

**Step 3**
Click the arrow icon in the right to navigate to the **Configuration** page.

The configuration template you selected in the profile creation phase will be auto-populated. You should provide the Management Interface IP Address, Management Route IP Address and the other required information. This management IP address is configured to enable Cisco Prime Infrastructure to reach the Nexus device.

Click **CLI** to view the CLI summary.

**Step 4**
Click the arrow icon in the right to navigate to the **Management Credentials** page.

For Nexus devices, it is mandatory to specify the **Management IP Address** so that the device can be managed. Provide the other required information and navigate to the next page. These device parameters will be applied on the devices on provisioning.

**Step 5**
In the **Profile Activation Summary** page, the device details with their configurations is displayed.

**Step 6**
Click **Finish** to provision the device profile.

On successful provisioning, the device profile will be displayed in the **Profile Instances** page of the specific profile. Alternatively, the provisioning status of the device can be viewed at the **Device Status** page. The device is added to the Prime Infrastructure inventory so that the device can be managed.

**Related Topics**
- Viewing Plug and Play Dashboard
- Plug and Play Profiles
Supported Devices and Software Images for Plug and Play

Table 27-1 lists the devices and corresponding software images supported for CNS gateway.

<table>
<thead>
<tr>
<th>Supported Devices for Plug and Play</th>
<th>Minimum Software Image Version Supported</th>
<th>Verified Image Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 2960, 2960S</td>
<td>Cisco IOS Release 12.2(55)SE and later</td>
<td>Cisco IOS Release 12.2(55)SE5 and later</td>
</tr>
<tr>
<td>Catalyst 2960C</td>
<td>Cisco IOS Release 12.2.55(EX) and later</td>
<td>Cisco IOS Release 12.2.55(EX3) and later</td>
</tr>
<tr>
<td>Catalyst 2960-SF</td>
<td>Cisco IOS Release 15.0(2)SE and later</td>
<td>Cisco IOS Release 15.0(2)SE and later</td>
</tr>
<tr>
<td>Catalyst 3560V2, 3750v2, 3560-X, 3750-X</td>
<td>Cisco IOS Release 12.2(55)SE and later</td>
<td>Cisco IOS Release 12.2(55)SE and later</td>
</tr>
<tr>
<td>Catalyst 3560C</td>
<td>Cisco IOS Release 12.2.55(EX) and later</td>
<td>Cisco IOS Release 12.2.55(EX) and later</td>
</tr>
<tr>
<td>Catalyst 4503, 4506, 4507, and 4510 switches and 4000 Series supervisor cards supported: Sup 6E, Sup 6LE</td>
<td>Cisco IOS Release 151-2.SG and later</td>
<td>Cisco IOS Release 151-2.SG and later</td>
</tr>
<tr>
<td>Catalyst 4503, 4506, 4507, and 4510 switches and 4000 Series supervisor cards supported: Sup 7E, Sup 7LE (IOS XE)</td>
<td>Cisco IOS XE Release 03.04.00.SG and later</td>
<td>Cisco IOS XE Release 03.04.00.SG and later</td>
</tr>
<tr>
<td>Catalyst 3650, 3850 switches (IOS XE)</td>
<td>Cisco IOS XE Release 03.02.02.SG and later</td>
<td>Cisco IOS XE Release 03.02.02.SG and later</td>
</tr>
<tr>
<td>Cisco 5760 Wireless LAN Controllers (IOS XE)</td>
<td>Cisco IOS XE Release 03.02.02.SG and later</td>
<td>Cisco IOS XE Release 03.02.02.SG and later</td>
</tr>
</tbody>
</table>

Refer Release Notes for Cisco Network Plug and Play to know the devices and the corresponding software images supported for APIC-EM.

For more Details on all the supported devices and the corresponding sysObjectIDs, see Cisco Prime Infrastructure 3.0 Supported Devices.

Related Topics
- Plug and Play Workflow
- Plug and Play Profiles
Prerequisites for Deploying Bootstrap Configuration into a Device

To deploy bootstrap configuration into a device in a Prime Infrastructure Server:

- Enable Cipher in Admin mode of the server by entering the following command:
  
  ncs run pnp-ciphers enable

- Click Enable in the HTTP Forward section of the Administration > Settings > System Settings > Server Settings page.

- If you are going to use email to deliver either the bootstrap configuration or the PIN, you must have previously configured the mail server settings under Administration > Settings > System Settings > Mail Server Configuration.

- Ensure TFTP is enabled on the Prime Infrastructure server by choosing Administration > Settings > System Settings > Server, then clicking Enable under TFTP. TFTP is enabled by default.

Bootstrap Configuration

A bootstrap configuration is a minimal configuration that is required for devices to establish a connection to the Prime Infrastructure gateway (CNS or APIC-EM). Prime Infrastructure provides a standard bootstrap configuration that you can use.

If you are using the DHCP option, you do not need to create a bootstrap configuration. See Using DHCP to Export Bootstrap Configurations.

To create a user-defined bootstrap template, follow these steps:

1. Choose Configuration > Plug and Play > Dashboard and in the Home tab, click Bootstrap.
   By default, an APIC Bootstrap and Plug and Play Bootstrap template will be displayed. These templates cannot be deleted.

2. Select the specific Bootstrap check-box and click Clone to clone a similar template. This new template will be displayed as APIC Bootstrap_1, APIC Bootstrap_1_1, and so on or Plug and Play Bootstrap_1, Plug and Play Bootstrap_1_1 and so on, depending on the bootstrap you cloned.

   Note: You can rename the cloned template. Once renamed, you cannot change the template name again.

3. Click Save.

4. Click the pointer beside the Bootstrap template to view or edit the details.

5. Click Update to save the changes. Click CLI to view the CLI summary.

6. To delete any bootstrap template, select the specific bootstrap template check-box and click Delete.

These templates that you create will be saved in PnP Bootstrap Templates (User Defined).
You can choose this newly created bootstrap template when adding a profile instance by selecting the specific bootstrap template from PnP Bootstrap Templates (User Defined). The details will automatically be displayed and will be editable.

You can also use the Configuration > Templates > Features & Technologies > CLI Templates > System Templates-CLI > Plug And Play Bootstrap to create a customized bootstrap template.

The bootstrap configurations that Prime Infrastructure provides have the following content:

- **CNS HTTP Bootstrap**

  ip host OVA-VM-176 10.104.118.176
cns trusted-server all-agents OVA-VM-176
cns trusted-server all-agents 10.104.118.176
cns id Hardware-Serial
cns id Hardware-Serial event
cns event OVA-VM-176 encrypt keepalive 120 2 reconnect-time 300
cns exec encrypt 443
cns config partial OVA-VM-176 encrypt 443
cns config initial OVA-VM-176 encrypt 443

- **CNS HTTPS Bootstrap**

  In the following example, pi-hateast-151 is the Prime Infrastructure server hostname.
crypto pki trustpoint pi-hateast-151
enrollment mode ra
enrollment terminal
usage ssl-client
revocation-check crl
exit
crypto pki certificate chain pi-hateast-151
certificate ca 4CAAA6BE30 0D060906 10.104.118.176

cns config partial OVA-VM-176 encrypt 443
cns config initial OVA-VM-176 encrypt 443
Methods of Installing Bootstrap Configurations

A bootstrap configuration is a minimal configuration that is required for devices to establish a connection to the Prime Infrastructure gateway (CNS or APIC-EM). The bootstrap configuration can be installed on the devices using any of the bootstrap delivery methods that Prime Infrastructure supports:
• Export and download the bootstrap—If you have access to the device console, you can export the bootstrap, and then copy and paste the bootstrap configuration to the device. See Exporting the Bootstrap Configuration.

• Export and save the bootstrap to a USB flash drive—You can save the bootstrap configuration to a USB drive with the file name `ciscort.cfg`. Connect the USB drive to the device, and then boot the device. The device will retrieve the bootstrap configuration from the USB drive. See Exporting the Bootstrap Configuration Using TFTP.

• Email the bootstrap. See Emailing the Bootstrap Configuration.

• DHCP options based on the server you specified. See Using DHCP to Export Bootstrap Configurations.
  – For CNS gateway—DHCP option 150
  – For APIC-EM—DHCP option 43. You can configure option 43 on the APIC-EM server IP under DHCP Configuration. When a device gets its IP address from DHCP, it will get the bootstrap configuration also.

• Mobile application—You can use the Cisco Network Plug and Play mobile application.

Related Topics
• Prerequisites for Deploying Bootstrap Configuration into a Device
• Bootstrap Configuration
• Exporting the Bootstrap Configuration
• Exporting the Bootstrap Configuration Using TFTP
• Emailing the Bootstrap Configuration
• Using DHCP to Export Bootstrap Configurations

Exporting the Bootstrap Configuration

You can export a bootstrap configuration and then manually apply the bootstrap on the device. After the bootstrap configuration is applied, the Plug and Play deployment is initiated and the administrator can view the configuration status on Prime Infrastructure.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Configuration &gt; Plug and Play &gt; Dashboard</strong> and in the <strong>Home</strong> tab, click <strong>PnP Profiles</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the Plug and Play Profiles page, select a profile from the list.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Profile Instances</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Export Bootstrap &gt; Download Bootstrap</strong>, then click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>After the bootstrap configuration is downloaded and applied, the Plug and Play deployment is initiated.</td>
</tr>
</tbody>
</table>

Related Topics
• Exporting the Bootstrap Configuration Using TFTP
• Emailing the Bootstrap Configuration
• Using DHCP to Export Bootstrap Configurations
• Bootstrap Configuration
Exporting the Bootstrap Configuration Using TFTP

If you are using a CNS gateway only for Plug and Play, you can use the TFTP protocol to deliver the bootstrap configuration to the Prime Infrastructure TFTP server. You can specify the file name that should be created on the TFTP server; this file is used by the auto-install enabled devices to get the IP address and other Prime Infrastructure details through the DHCP. In the DHCP server, the TFTP server must be configured as the Prime Infrastructure TFTP server. For more information, please see Cisco Open Plug-n-Play Agent Configuration Guide, Cisco IOS XE Release 3E.

Step 1  Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles.
Step 2  From the Plug and Play Profiles page, select a profile from the list.
Step 3  Click Profile Instances.
Step 4  Click Export Bootstrap > TFTP.
Step 5  After the bootstrap configuration is downloaded and applied, the Plug and Play deployment is initiated.

Related Topics
- Emailing the Bootstrap Configuration
- Bootstrap Configuration
- Emailing the PIN for the Bootstrap Configuration
- Using DHCP to Export Bootstrap Configurations

Emailing the Bootstrap Configuration

You can email the bootstrap configuration and then manually apply the bootstrap on the device. After the bootstrap configuration is applied, the automated deployment is initiated. The administrator can view the configuration status on Prime Infrastructure.

Note
Before you can email the bootstrap configuration, you must set the email settings under Administration > Settings > System Settings > Mail and Notification > Mail Server Configuration.

To email the bootstrap configuration to the operator:

Step 1  Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles.
Step 2  From the Plug and Play Profiles page, select a profile from the list.
Step 3  Click Profile Instances.
Step 4  Click Export Bootstrap > Email Bootstrap.
Step 5  Enter the email address to which the bootstrap configuration is be sent, then click OK.
Step 6  After the bootstrap configuration is downloaded and applied, the Plug and Play deployment is initiated.
Emailing the PIN for the Bootstrap Configuration

Prime Infrastructure generates a random Personal Identification Number (PIN) per device. This PIN can be used to identify the device and the Plug and Play profile (bootstrap configuration) associated with it. After the pre-provisioning tasks are complete, the administrator must use the Email PIN option (available in the pre-provisioning task of the Prime Infrastructure) to email the unique PIN to the deployment engineer. During installation, the deployment engineer uses this PIN to download the bootstrap configuration from the server.

To deliver the PIN for the bootstrap configuration:

Step 1
Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles.

Step 2
From the Plug and Play Profiles page, select a profile from the list.

Step 3
Click Profile Instances tab.

Step 4
Click CNS Email PIN.

Step 5
Enter the email address to which the PIN should be sent and click OK.

Step 6
Use one of the following methods to apply the bootstrap configuration:

- If you are applying the bootstrap configuration using the deployment application, the Prime Infrastructure Plug and Play deployment application communicates to the Prime Infrastructure and applies the bootstrap configuration on the device.

- If you are manually applying the bootstrap configuration using the PIN:
  - Use the PIN to download the bootstrap configuration from the Prime Infrastructure Plug and Play gateway: https://<pnp-gateway-server>/cns/PnpBootstrap.html. You can also register the ISR’s serial number during this process.
  - Apply the bootstrap configuration on the device manually, using a console or USB flash.

For detailed information about Plug and Play deployment, see the Cisco Plug and Play Application User Guide.

Step 7
After the bootstrap configuration is applied, the Plug and Play deployment is initiated.
Using DHCP to Export Bootstrap Configurations

To use the DHCP option to export a bootstrap configuration, you must have the following configuration on your devices:

- For CNS gateway—DHCP option 150

  ```
  ip dhcp pool <DHCP pool name>
  network <subnet> <subnet mask>
  default-router <default gateway>
  option 150 ip <prime_infrastructure_server_IP>
  ```

- For APIC-EM—DHCP option 43

  ```
  ip dhcp pool <DHCP pool name>
  network <subnet> <subnet mask>
  default-router <default gateway>
  option 43 ascii "5A1D;B2;K4;I<APIC-EM_server_IP>;J80"
  ```

Sample DHCP Server Settings

If you select the DHCP-based method to deliver the Plug and Play Profile, you must configure the DHCP server to redirect the switch to the TFTP server by entering the commands described in Table 27-2. This method is not supported for HTTPS with the Encrypt CNS commands. It is supported with the HTTP CNS commands.

The DHCP-based method follows these steps:

1. The new switch contacts the DHCP server. You must configure the DHCP server to redirect the switch to the TFTP server. See Table 27-2 for more information.
2. The DHCP server points the switch to the new TFTP server where the Plug and Play bootstrap profile resides.
3. The switch loads the bootstrap configuration file, boots up, and then contacts the Plug and Play Gateway.

### Table 27-2  DHCP Server Settings

<table>
<thead>
<tr>
<th>Command to Enter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp pool PNP</td>
<td>Creates a DHCP pool named PNP.</td>
</tr>
<tr>
<td>network 10.106.190.0 255.255.255.224</td>
<td>Defines the network 10.106.190.0 and subnet mask 255.255.255.224. DHCP uses this pool of IP addresses to assign an IP address to the new device.</td>
</tr>
<tr>
<td>default-router 10.106.190.17</td>
<td>Configures the default route 10.106.190.17 on the new device.</td>
</tr>
<tr>
<td>option 150 ip 10.77.240.224</td>
<td>Specifies that the TFTP server IP address 10.77.240.224 is the Prime Infrastructure server IP address.</td>
</tr>
</tbody>
</table>

---

Cisco does not support these non-Cisco DHCP products. However if you are using other DHCP servers please note the following:

- Both the CNS-based Cisco Plug and Play Agent and the APIC-EM based Cisco Open Plug-N-Play Agent use a VPN-ID option (Option 221) of "Mgmt-intf" in their DHCP packets. An enterprise level DHCP server will not be able to process these packets without properly handling that VPN-ID.
• Both the CNS-based Cisco Plug and Play Agent and the APIC-EM based Cisco Open Plug-N-Play Agent expect the TFTP server address to be returned as a string. Enterprise level DHCP servers return Option 150 as an IP address, and Option 66 as a string.
• Both the CNS-based Cisco Plug and Play Agent and the APIC-EM based Cisco Open Plug-N-Play Agent expect a default route (Option 33). Enterprise level DHCP servers return Option 33 as a default route, not just the address of the router as provided by Option 3.

Related Topics
• Viewing Plug and Play Dashboard
• Plug and Play Profiles
• Bootstrap Configuration
• Methods of Installing Bootstrap Configurations

Verifying Device Status

Choose Configuration > Plug and Play > Dashboard and in the Home tab, click Status Information. The device details (Serial ID, hostname, IP address, type, profile name, location), current and post Plug and Play statuses, and the graphical representation of the provisioning status are displayed in a List view.

Click Map in the upper right corner to view the device details and their statuses in map view. See Integrating Map View.

You can choose Administration > Dashboards > Job Dashboard > User Jobs > Post PnP Status to view the status of post Plug and Play configuration job on a device.

Integrating Map View

You can view the details in a map view in any of the following ways:
• Choose Configuration > Plug and Play > Dashboard and click Monitoring tab.
• Choose Configuration > Plug and Play > Dashboard and click Home tab. Click Status Information and click Map from the upper right corner of the Device Status page.
• Choose Configuration > Plug and Play > Dashboard and click Home tab. Click Locations.
Verifying Device Status

1. Click to view the map in full screen.
2. You can perform zooming operations using mouse or keyboard. With keyboard, click the + or - signs to zoom in or zoom out. With mouse, use the mouse scroll wheel to zoom in or zoom out or double-click to zoom in.
3. Click to view the provisioning status of the device in detail.
4. Click to view the sites that do not have geographical coordinates specified.
5. Click to view the devices that are not mapped to any location. Drag and drop the devices to a location in the map. The device automatically gets mapped to that location group.
6. Toggle the button to enable edit mode. Once enabled, you can drag and drop the unmapped devices to a location in the map. Before you map a device to a location, create location groups. See Using Location Groups.
7. Select a location from the list.
8. Click to view the cluster details. A cluster represents two or more locations in a geographical area. Hover the mouse over the site to view the number of devices mapped to it. Click the number hyperlink to view the device details.
9. Click List to view the Device Status page.

Related Topics
- Verifying Device Status
- Deleting Plug and Play Profiles
- Viewing Plug and Play Dashboard
- Plug and Play Profiles
- Activating Device Profiles
- Bootstrap Configuration
Deleting Plug and Play Profiles

If you are using APIC-EM for Plug and Play, you might need to delete a plug and play profile that is incorrect or outdated.

Step 1  Execute the following command from the router CLI to remove the Plug and Play profile from the router:

```
no pnp profile plug_and_play_profile_name
```

Step 2  Delete the provisioning profile by choosing Configuration > Plug and Play > Dashboard and click PnP Profiles. Select a Plug and Play profile, click Profile Instances, then delete the required provisioning profile.

Step 3  Choose Configuration > Plug and Play > Dashboard and click PnP Profiles. Select the Plug and Play profile you want to delete, then click Delete.

Related Topics

- Viewing Plug and Play Dashboard
- Plug and Play Profiles
- Activating Device Profiles
- Bootstrap Configuration
- Verifying Device Status