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 allows you to create templates to define features and configurations that you can reuse and apply to new devices. You can streamline new device deployment by creating bootstrap templates, which define the necessary initial configuration, to communicate with Prime Infrastructure. You can specify (and *predeploy*) software images and configurations that will be added to the devices in the future.

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:
   - 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. 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.

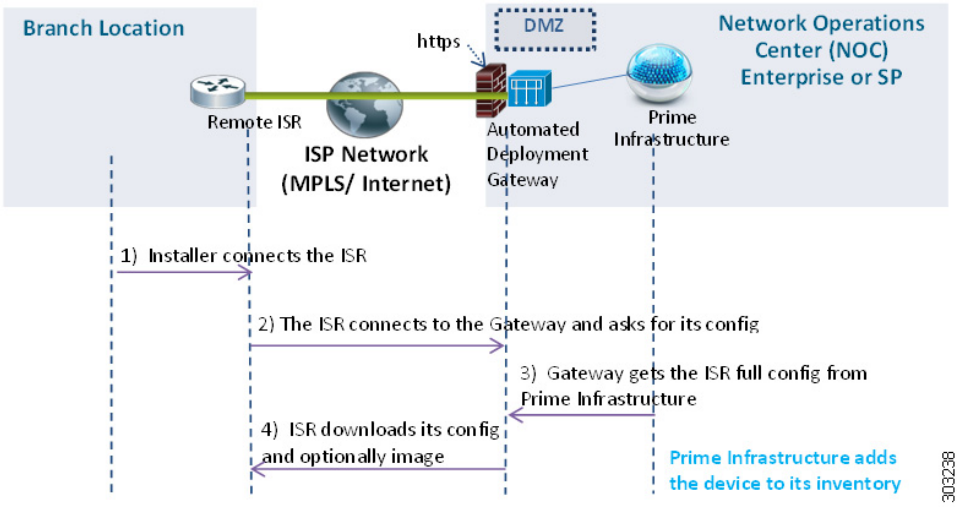
After you apply the bootstrap configuration:

1. The device uses the call-home agent capability to connect to the server you configured (either CNS or APIC-EM).
2. The Plug and Play Profile deployment is initiated.
3. The Prime Infrastructure server receives the Device Plug and Play ID / serial number of the new device and verifies if this matches with the device ID in any of the Plug and Play preprovisioning definitions. 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. 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 and adds the device to its inventory.

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 26-1).

Figure 26-1 Plug and Play Branch Deployment



Related Topics

- Exporting the Bootstrap Configuration
- Integrating APIC-EM with Prime Infrastructure

APIC-EM and Plug and Play

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, PKI certificates, 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 (including the PKI certificate) from Prime Infrastructure using APIC-EM's Plug and Play and PKI services.

With APIC-EM Plug and Play integration, devices can be provisioned with http/https. When the profile is created, you can also choose to install PKI certificates on the device to use PKI based authentication.

Related Topics

- Integrating APIC-EM with Prime Infrastructure
- Bootstrap Configuration

Integrating APIC-EM with Prime Infrastructure

Prime Infrastructure communicates with APIC-EM via HTTPs and REST API's exposed by APIC-EM. To integrate APIC-EM controller to Prime Infrastructure, follow these steps:.

Step 1 Choose **Administration > Servers > APIC-EM Controller**.

Step 2 Enter the APIC-EM controller IPv4 address.

Step 3 Enter the HTTPS port number to connect with APIC-EM.

Step 4 Enter your user name.

Step 5 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.

The global option in A**dministration > 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
- Using PKI with IWAN-DMVPN Service

Plug and Play Profiles

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 Plug and Play profiles that contain:

- Software images only.
- Configurations only.
- Both software images and configurations.
- PKI certificates (For APIC-EM only.)

Related Topic

- Creating Plug and Play Profiles

Creating Plug and Play Profiles

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 Importing Software Images for Plug and Play Profiles.
- Configuration CLI template—See Creating CLI Templates.

Step 1 Choose **Configuration > Plug and Play > PnP Profiles**, then click **Add**.

Step 2 Provide the required information.

Step 3 Click **Save as New Plug and Play Profile**.

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.

Step 5 From the **Bootstrap Template** drop-down list, select the bootstrap templates. You can also create a customized bootstrap template, but you must use the same tag names as specified in the standard bootstrap configuration provided by Prime Infrastructure.

Step 6 (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 7 (Optional) From the **Configuration Template** drop-down list, select a previously created configuration template.

Step 8 Click on **Device Details for Profile**.

Step 9 Click **Add** to add details for the devices for which you want to pre-provision the Plug and Play Profile. See Importing Device Profiles into Plug and Play Profiles for importing device information in bulk.

Step 10 After completing the required fields, click **OK**.

After you save the profile, the same configurations are added to the Plug and Play server you selected (either CNS or APIC-EM). The bootstrap configuration is for the devices to reach the Plug and Play server. When the device calls home, it discovers either the CNS or APIC-EM IP address and based on the device type (CNS only) and/or serial number (for CNS and APIC-EM), the profile is matched and the device gets provisioned based on the parameters defined in the Plug and Play profile.

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

Related Topic

- Plug and Play Profile Field Descriptions
- Importing Device Profiles into Plug and Play Profiles
- Deploying Plug and Play Profiles
- Cisco Open Plug-n-Play Agent Configuration Guide, Cisco IOS XE Release 3E

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**.

Importing Device Profiles into Plug and Play Profiles

You can import device profiles in bulk from a spreadsheet that lists all of your devices and their attributes. 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.

Prime Infrastructure provides a sample CSV which you can export, enter the required values, and then import back into Prime Infrastructure.

Step 1 Choose **Configuration > Plug and Play > PnP Profiles**.

Step 2 Select the device profile from the list and click **Left Shift** and select **Export** from the drop down list.

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. A blank csv file will be exported if there are no device profiles found in the deploy page.

Note Do not change the attribute names while editing the spreadsheet.

Step 3 Click **Import** and choose the CSV file in which you entered the device details.

All the devices in the spreadsheet are imported.

Deploying Plug and Play Profiles

To deploy a Plug and Play profile based on the device ID:

Step 1 Choose **Configuration > Plug and Play > PnP Profiles**.

Step 2 In the Plug and Play Profiles page, select a profile and click **Device details for Profile**.

Step 3 In the Device Provisioning Profiles page, click **Add**.

One profile can have multiple provisioning settings that can be applied for different devices.

Step 4 Provide the required information.

Step 5 Click **OK**, then click **Close**.

Related Topics

- Plug and Play Profile Field Descriptions
- Exporting the Bootstrap Configuration

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:

   - 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.

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 From Prime Infrastructure, choose **Configuration > Plug and Play > PnP Status**, select the Plug and Play profile you want to delete, then click **Delete**.

Step 3 Delete the provisioning profile by choosing **Configuration > Plug and Play > PnP Profiles**, select a Plug and Play profile, click **Device Details**, then delete the provisioning profile.

Step 4 Choose **Configuration > Plug and Play > PnP Profiles**, select the Plug and Play profile you want to delete, then click **Delete**.

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 DCHP option, you do not need to create a bootstrap configuration. See Using DHCP to Export Bootstrap Configurations.

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 id Hardware-Serial image
cns event OVA-VM-176 encrypt keepalive 120 2 reconnect-time 300
cns exec encrypt  443
cns image server https://OVA-VM-176:443/cns/HttpMsgDispatcher status
https://OVA-VM-176:443/cns/HttpMsgDispatcher
cns config partial OVA-VM-176 encrypt 443
cns config initial OVA-VM-176 encrypt 443
```

- APIC-EM HTTP Bootstrap

```
pnp profile network-pnp
transport http ipv4 <APIC-EM server IP>
```

- APIC-EM HTTPS Bootstrap

```
crypto ca trustpoint <APIC-EM Server IP>.cisco.com
enrollment mode ra
enrollment terminal
usage ssl-client
exit
crypto ca authenticate <APIC-EM Server IP>.cisco.com
-----BEGIN CERTIFICATE-----
Certificate detail
-----END CERTIFICATE-----
pnp profile network-pnp
transport https ipv4 <APIC-EM Server IP> port 443
!
```

  After you create a deployment profile and export it, you can download this certificate directly from Prime Infrastructure. If executing the bootstrap in a device, only the last two commands are required because the APIC-EM server will install certificates directly on the device.

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 *ciscortr.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.
- 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.

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.

Step 1 Choose **Configuration > Plug and Play > PnP Profiles**.

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

Step 3 Click **Device Details for Profile**.

Step 4 Click **Export Bootstrap > Download Bootstrap**, then click **OK**.

Step 5 After the bootstrap configuration is downloaded and applied, the Plug and Play deployment is initiated.

To check on the status, choose **Configuration > Plug and Play> PnP Status**.

Related Topic

- Plug and Play Profile Field Descriptions

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 > PnP Profiles**.

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

Step 3 Click **Device Details for Profile**.

Step 4 Click **Export Bootstrap > TFTP**.

Step 5 After the bootstrap configuration is downloaded and applied, the Plug and Play deployment is initiated.

To check on the status, choose **Configuration > Plug and Play > PnP Status**.

Related Topic

- Plug and Play Profile Field Descriptions

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 > PnP Profiles**.

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

Step 3 Click **Device Details for Profile**.

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.

To check on the status, choose **Configuration > Plug and Play> PnP Status**.

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 > PnP Profiles**.

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

Step 3 Click **Device Details for Profile**.

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.

To check on the status, choose **Configuration > Plug and Play> PnP Status**.

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_infrastucture_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"
```

Getting Help Setting Up and Configuring Devices

Cisco Prime Infrastructure provides step-by-step guidance for the following tasks:

- Preconfiguring devices that will be added to your network in the future—See Preconfiguring Devices to be Added Later.
- Setting up access switches after they have been added to Prime Infrastructure—See Getting Help Setting Up Access Switches.

Preconfiguring Devices to be Added Later

You can preconfigure devices that will be added to your network in the future. For example, if you are going to be adding a new branch office, you can use the Plug and Play Setup workflow to create an initial configuration for the branch router and switches. When the new device is added to your network, Prime Infrastructure can quickly discover, inventory, and configure the new device based on settings that you specify in a Plug and Play profile.

Note The **Bootstrap** and **Initial Device Setup** menus appear for users with the following privileges only: root, super users, and Config Managers.

The Plug and Play Setup workflow is similar in functionality to **Configuration > Templates > Features & Technologies > Plug and Play Profiles**; however, the workflow, designed more for access switches than routers, provides more guidance to set up new devices.

Note The Plug and Play Setup workflow is most helpful in setting up and configuring Cisco IOS switches and access devices. Cisco IOS devices that support auto DHCP install options can be booted up using the Plug and Play Setup workflow. All other devices (for example, routers that do not have direct network connectivity in the branch, legacy controllers, and APs) must use the Plug and Play feature.

You need to complete the Plug and Play Setup only *once*. After you complete the steps, when a new switch or access device is connected to the network, the device automatically uses the Plug and Play profile, boots up, and then Prime Infrastructure begins managing the device.

Related Topic

- Prerequisites for Delivering Plug and Play Profiles

Supported Devices and Software Images for Plug and Play Setup Workflow

Table 26-1 lists the devices and corresponding software images supported for **Configuration> Plug and Play > Initial Device Setup** for CNS gateway.

Table 26-1 Supported Devices and Image Versions for Configuration > Plug and Play > Initial Device Setup for CNS Gateway

Supported Devices for Plug and Play	Minimum Software Image Version Supported	Verified Image Version
Catalyst 2960, 2960S	Cisco IOS Release 12.2(55)SE and later	Cisco IOS Release 12.2(55)SE5 and later
Catalyst 2960C	Cisco IOS Release 12.2.55(EX) and later	Cisco IOS Release 12.2.55(EX3) and later
Catalyst 2960-SF	Cisco IOS Release 15.0(2)SE and later	Cisco IOS Release 15.0(2)SE and later
Catalyst 3560V2, 3750v2, 3560-X, 3750-X	Cisco IOS Release 12.2(55)SE and later	Cisco IOS Release 12.2(55)SE and later
Catalyst 3560C	Cisco IOS Release 12.2.55(EX) and later	Cisco IOS Release 12.2.55(EX) and later

Table 26-1 Supported Devices and Image Versions for Configuration > Plug and Play > Initial Device Setup (continued)for CNS Gateway

Supported Devices for Plug and Play	Minimum Software Image Version Supported	Verified Image Version
Catalyst 4503, 4506, 4507, and 4510 switches and 4000 Series supervisor cards supported: Sup 6E, Sup 6LE	Cisco IOS Release 151-2.SG and later	Cisco IOS Release 151-2.SG and later
Catalyst 4503, 4506, 4507, and 4510 switches and 4000 Series supervisor cards supported: Sup 7E, Sup 7LE (IOS XE)	Cisco IOS XE Release 03.04.00.SG and later	Cisco IOS XE Release 03.04.00.SG and later
Catalyst 3650, 3850 switches (IOS XE)	Cisco IOS XE Release 03.02.02.SE and later	Cisco IOS XE Release 03.02.02.SE and later
Cisco 5760 Wireless LAN Controllers (IOS XE)	Cisco IOS XE Release 03.02.02.SE and later	Cisco IOS XE Release 03.02.02.SE and later

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*.

Getting the Configuration to New Devices

You can choose how to get the bootstrap configuration that is created during the Plug and Play Setup workflow to your new devices:

- **DHCP Auto Install**—If you select the DHCP-based auto install method to deliver the Plug and Play Profile, you must have a distribution network or a network that already has an existing connection to your corporate network. See Sample DHCP Server Settings for Auto Install.
- **Prime Utilities**—If you select the Prime Utilities method to deliver the Plug and Play Profile, after connecting the new devices to the distribution layer, you must use the laptop utility to download the configuration from Prime Infrastructure and apply the configuration to the devices. You must have internet connectivity to the Prime Infrastructure server.
- **File Transfer**—If you select the File Transfer method to deliver the Plug and Play Profile, you can download the TXT file and manually apply the configuration to the devices.

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 for Auto Install. If DHCP is not available in the network, you can use a different method to apply the bootstrap configuration to your new devices as explained in Sample DHCP Server Settings for Auto Install.
- 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.

Sample DHCP Server Settings for Auto Install

If you select the DHCP-based auto install 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 26-2.

The auto install method is not supported for HTTPS with the Encrypt CNS commands. It is supported with the HTTP CNS commands.

The DHCP-based auto install 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 26-2 for more information.
2. The DCHP 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 26-2 DHCP Server Settings for Auto Install

Command to Enter	Description
`ip dhcp pool PNP`	Creates a DHCP pool named PNP.
`network 10.106.190.0 255.255.255.224`	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.
`default-router 10.106.190.17`	Configures the default route 10.106.190.17 on the new device.
`option 150 ip 10.77.240.224`	Specifies that the TFTP server IP address 10.77.240.224 is the Prime Infrastructure server IP address.

Specifying Device Credentials

The **Configuration > Plug and Play > Bootstrap > Create Profile** window is where you provide SNMP, Telnet, and SSH credentials that will be configured on the devices. Prime Infrastructure uses these credentials to contact the devices. By default, Telnet is enabled, but you can enable SSH if applicable.

The following configurations are set by the Plug and Play profile, but you can modify them using the Getting Help Setting Up Access Switches workflow:

- SNMPv2 and SSH Credentials—The SNMP, Telnet, and SSH credentials you specify will be configured on *all* devices that use the Plug and Play profile. You can consider these temporary credentials necessary to allow Prime Infrastructure to contact the devices. You can use the Getting Help Setting Up Access Switches workflow later to modify the device credentials. You can enable Telnet, SSH, or both. If you specify SSH, ensure the device has the K9 image.

  For security purposes, we recommend that do not use “public” or “private” for your community strings.
- 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.

Saving the Plug and Play Profile

As explained in Sample DHCP Server Settings for Auto Install, make sure that you have satisfied the necessary requirements before you specify how you want to apply or export the Plug and Play profile.

- **via TFTP**—The profile remains active on the TFTP server and whenever a new switch or access device is connected to the network, the device will automatically use the Plug and Play profile, boot up, and then “call home” to Prime Infrastructure for additional configuration.
- **Email to other operators**—You can email the bootstrap configuration file to an appropriate network engineer who can provision the bootstrap configuration manually to the device, or email the PIN to an appropriate network operator who can use the Prime Infrastructure iPad or laptop utility to provision the configurations on the devices.

Note 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**.

- Export the bootstrap configuration file (in TXT format) that was created and then manually apply the bootstrap configuration to the devices.

After you save the Plug and Play Profile, choose **Monitor > Workflow Status** to view newly registered devices and any devices on which the workflow failed.

Now that your devices will be able to contact the Prime Infrastructure server, you can specify further configurations that can be applied to the devices. See Getting Help Setting Up Access Switches.

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.
- Restart the Prime Infrastructure Server

For HTTPS, select the **Create Profile for https** check box in the Configuration > Plug and Play > Bootstrap page.

Sample Output from Plug and Play Setup (HTTPS)

When you complete the steps in **Configuration > Plug and Play > Bootstrap**, Prime Infrastructure creates a bootstrap configuration file, which includes the following commands to allow new Cisco IOS devices to "call home" to Prime Infrastructure.

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 4CAAA6BE
30820399 30820281 A0030201 0202044C AAA6BE30 0D06092A 864886F7 0D010105
0500307D 310B3009 06035504 06130255 53310B30 09060355 04081302 43413111
300F0603 55040713 0853616E 204A6F73 65311630 14060355 040A130D 43697363
6F205379 7374656D 73311D30 1B060355 040B1314 574E4255 20286175 746F6765
6E657261 74656429 31173015 06035504 03130E70 692D6861 74656173 742D3135
31301E17 0D313430 38303530 36313432 355A170D 31363038 30343036 31343235
5A307D31 0B300906 03550406 13025553 310B3009 06035504 08130243 41311130
0F060355 04071308 53616E20 4A6F7365 31163014 06035504 0A130D43 6973636F
20537973 74656D73 311D301B 06035504 0B131457 4E425520 28617574 6F67656E
65726174 65642931 17301506 03550403 130E7069 2D686174 65617374 2D313531
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00877EEC 985CFD97 92BAE4C4 E611B089 E4453714 844F2DEC C944F907 D53BB92A
016CA25C 007F2EF5 51CAA930 8EADF3BA 165D3A25 004FCFE3 2D0A9A92 B8165508
C4642DFA F1A0DFEE F8F1C958 7CBE7ED7 6D74195A F1E7133A 5A7EFF36 0AF8ADC1
8A829515 D91EF557 CE9F4915 B4C04FD0 F461C211 FB70A375 AA7204DC 4C025FED
72896754 53FB1F7A 9F30CC0D A0443D50 9DDB7A90 3544F345 0CAB8FDB A8009718
F8D49347 741493AD 746B3DC3 0E41D2FF 72B51816 7968D924 1F42536A 1C7B29F2
C569E111 3D126FBF 4B23F2A5 96AA446E BA9F5A94 68F1F7A3 E8C4994F BCF4B2FB
ED5589BF D222DD29 2EACFE48 DDA45116 EA2C42BA 9E37B6DA 05E7582E 1521512A
B1020301 0001A321 301F301D 0603551D 0E041604 14C05AA1 1AF06B2A D5AA67BD
226B487B 0518343B 5B300D06 092A8648 86F70D01 01050500 03820101 00741493
7B6360D5 34F7ED04 2078A847 788ACDFF A143162B 1736AB2C A8E3EA2B 1CE54E9E
AEFBE562 21D8F70E 3AD9EF0E ED782A7D 362D4D1A 9275C791 96F19584 C873DAF1
16108A59 186FD2E1 BD00F61C 2C57D6A0 0DE5E42B B76210BE EAB8C9F2 2C476091
B5F0B661 E8C8277F 5F673547 0404C863 0BE127B2 9E3FDE18 139F9BAD F5EC945A
30715BDF B72565F0 D25DBA40 216091F0 98BDB241 993662F9 248C1423 8F5417B2
69672F32 6212D37F 008A4B86 CDF280E9 2C89F1CF 9E63311D 2B349C07 43D8D02D
F9770607 9F14DF51 896BF1EF 8B2A3EC5 3B1E564E 4E079B4A CC684745 11372D92
377407E8 194EF897 5B62B38B 16B6F1EF F080A3E4 512508B8 4322C2DD 86
```

```
quit
exit
ip host pi-hateast-151 10.104.119.151
cns trusted-server all-agents pi-hateast-151
cns trusted-server all-agents 10.104.119.151
cns id hardware-serial
cns id hardware-serial event
cns id hardware-serial image
cns event pi-hateast-151 encrypt keepalive 120 2 reconnect-time 60
cns exec encrypt 443
cns image server https://pi-hateast-151/cns/HttpMsgDispatcher status
https://pi-hateast-151/cns/HttpMsgDispatcher
cns config partial pi-hateast-151 encrypt 443
cns config initial pi-hateast-151 encrypt 443
end
```

The bootstrap configuration file is delivered based on the method you specified:

- **via TFTP**—Prime Infrastructure copies the bootstrap configuration file, *cisconet.cfg*, and the *config* credentials file to the Prime Infrastructure TFTP server.
- **Email to other operators**—Prime Infrastructure emails the bootstrap configuration file to the specified email address and copies the *config* credentials file to the Prime Infrastructure TFTP server.

Note 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**.

- **Export the bootstrap configuration file**—Prime Infrastructure exports the bootstrap configuration file to the client and saves it as *Day-0 Bootstrap Configuration_NEW.txt* and copies the *config* credentials file to the Prime Infrastructure TFTP server.

Verifying Plug and Play Provisioning Status

Choose **Configuration > Plug and Play > PnP Status** to view the Plug and Play status of any devices.

Getting Help Setting Up Access Switches

After your devices are added to Prime Infrastructure, you can use the Initial Device Setup workflow to help you configure wired and wireless features on the following devices:

- Supported devices for **wired** features: See Table 26-1.
- Supported devices for **wireless** features:
  - Catalyst 3650 switches
  - Catalyst 3850 switches

- Cisco 5760 Wireless LAN Controllers

Related Topics

- Before You Begin
- Assign Devices to Location

Before You Begin

You must create a location before you use the Initial Device Setup by choosing **Inventory > Grouping > Location & Device**. See Using Location Groups for more information.

Related Topic

- Assign Devices to Location

Assign Devices to Location

The **Configuration > Plug and Play > Initial Device Setup > Assign to Location** window allows you to specify a location to which the devices you want to configure belong. *Unassigned* devices discovered using the Plug and Play Setup workflow (see Preconfiguring Devices to be Added Later) and any discovered devices that were not previously assigned are listed on this window. You must assign each device to a location.

The Initial Device Setup workflow is location-specific. To configure devices in a different location, you repeat the Initial Device Setup workflow and select that appropriate location.

To get details about any device, hover your mouse cursor over a device IP address, then click the icon that appears. See Getting Device Details from Device 360° View for more information.

If the Status column for any device is *N/A*, either the device was manually added to Prime Infrastructure (without using the Plug and Play Setup workflow), or the Plug and Play Setup workflow completed, but the synchronization took longer than 10 minutes after the device was added to Prime Infrastructure.

Choose Devices

The **Configuration > Plug and Play > Initial Device Setup > Choose Other Devices** window displays all new devices you assigned to the specified location, any devices previously assigned to the same location, and any devices that were added to Prime Infrastructure using discovery. This allows you to configure wired and wireless features on new and existing devices at the same time.

Choose whether you want to configure wired or wireless features. The devices displayed correspond to the option that you select.

If you select **Add wired features to my device(s)**, only applicable devices in the selected location on which you can configure wired features are displayed. After you select the devices, check the Device Readiness column and see Device Readiness Explanation for more information.

Choose a configuration mode:

- **Guided mode**—Gives you step-by-step guidance in creating Cisco-recommended device configurations. See Configuring Wired Features Using Guided Mode.

- **Advanced mode**—Uses templates in which you can modify and customize the device configurations. You should be comfortable with CLI templates. See Configuring Wired Features Using Advanced Mode.

If you select **Add wireless features to my device(s)**, applicable devices in the selected location on which you can configure wireless features are displayed. After you select the devices, you can choose to configure guest access as part of the wireless device configuration. Enter the number of access points and select a mobility group. See Configuring Wireless Features for step-by-step guidance in configuring wireless features.

Device Readiness Explanation

The Readiness column indicates whether the devices that you selected are ready to be configured. A device can be "not ready" for the following reasons:

- The device is not running the required Cisco IOS version. Table 26-3 lists the required versions.
- Prime Infrastructure was unable to collect inventory details. Choose **Inventory > Device Management > Network Devices** and make sure the Admin Status for the device is *Managed* and the Inventory Collection Status is *Completed*.

Table 26-3 Required Cisco IOS/IOS XE Releases for Switches to Be in Ready State

Switch Series	Required Cisco IOS/IOS XE Releases
Catalyst 2960, 2960s, 2960X	12.2(55) and later, or 15.0.1.SE and later
Catalyst 2960-SF	15.0(2)SE and later
Catalyst 3560v2, 3560X, 3750v2, 3750X	12.2(55) and later, or 15.0.1.SE and later
Catalyst 3560c, 2960c	12.2(55)-EX4 and later
Catalyst 3650, 3850	IOS XE 03.02.02 SE and later
Catalyst 4500	When running Sup7E and Sup7LE: IOS XE 03.03.02.SG and later When running Sup6E or Sup6LE: 12.2(54)SG and later
5760 Wireless LAN Controller	IOS XE 03.02.02 SE and later

Related Topics

- Configuring Wired Features Using Guided Mode
- Configuring Wired Features Using Advanced Mode
- Configuring Wireless Features

Configuring Wired Features Using Guided Mode

When you choose to configure wired features using the Guided Mode, you are guided step-by-step through configuring the following settings:

1. IP Address Options
2. Device Credentials
3. VLAN and Switching Parameters
4. Auto Smartports and Uplinks

5. Confirmation

IP Address Options

During the **Configuration > Plug and Play > Initial Device Setup** workflow (see Preconfiguring Devices to be Added Later), the DHCP server assigned IP addresses to the devices. The IP Management Options page is where you can modify the IP addresses. Select **Change Device(s) IP Management Address**, enter the necessary values for the device(s) in the Device Management Option table, then click **Save**.

You can edit IP address, hostname, subnet, and gateway values only; you cannot modify the device type and serial number.

If you have a large number of devices, you can simplify this task by exporting a CSV file of all devices, editing the file, then importing the CSV file to overwrite the Device Management Option table.

Device Credentials

During the **Configuration > Plug and Play > Initial Device Setup** workflow (see Preconfiguring Devices to be Added Later), the same SNMP, Telnet and SSH credentials you specified were be configured on *all* devices. The Credentials page is where you can modify the credentials and specify different credentials for various devices. Select **Specify new credentials** and enter the necessary values.

Click **Save Credentials** to save the credentials you entered. When you have new devices that you want to set up and you use the Initial Device Setup workflow again, you can select the credentials that you saved from the **Use Credentials** list. The fields are populated with the values that you previously saved.

When you complete the Initial Device Setup workflow, the device credentials are updated on the devices and in Prime Infrastructure.

VLAN and Switching Parameters

The VLAN and Switching page allows you to configure VLANs and switching parameters. Default VLAN values are provided. Default switching features are selected. The following options are enabled by default and you cannot modify them because they are required by Prime Infrastructure:

- Enable CDP
- Rapid PVST

By default, Spanning Tree is also enabled.

Auto Smartports and Uplinks

By default, the Initial Device Setup workflow enables Cisco Auto Smartports and quality of service (QoS) on switch downlink ports. Auto Smartport macros dynamically configure ports based on the device type detected on the port. You cannot disable Auto Smartports.

The Before You Begin page includes a link to download the supported devices for uplink configuration.

We recommend that you enable uplink-specific features such as EtherChannel and Trunking by selecting one of the options from the pulldown menu:

- Enable Layer 2 Trunking

- Enable Layer 2 Trunking with Etherchannel (PagP)
- Enable Layer 2 Trunking with Etherchannel (LACP)
- Enable Layer 2 Trunking with Etherchannel (Static)

Confirmation

The Confirmation screen is the last step in the Initial Device Setup workflow in which you can view the settings you specified. Click Deploy to deploy the configuration. A job is created and the job status information is displayed.

To view the deployed jobs, choose **Administration > Jobs** to view the status and details about the job.

If the deployment fails, the number of devices on which the deployment failed appears in the Failed column of the **Monitor > Workflow Status** window. Click the number displayed to go directly to the Choose Other Devices screen to view the device(s) that failed. You can modify necessary settings and repeat the workflow for that device.

Configuring Wired Features Using Advanced Mode

If you want to customize the configuration settings applied to your devices, select **Advanced mode** in The Choose Other Devices page. The Advanced mode uses templates in which you can modify and customize the device configurations. You should be comfortable with CLI templates.

You use the following templates to specify configuration settings:

- System—Allows you to specify new IP addresses to replace the IP addresses that were previously assigned by the DHCP server. You can edit IP address, hostname, subnet, and gateway values only; you cannot modify the device type and serial number.

  If you have many devices, it might be easier to edit these values in a spreadsheet. You can export the list of devices as a CSV file, edit the file, and then import the file to overwrite the table.
- Security—Allows you to specify authentication credentials. Whatever you select as the authentication type, your primary authentication server must match. For example, if you select RADIUS as the authentication method, the primary authentication method must be RADIUS. If you select None as the authentication type, your primary authentication method must be LOCAL. The secondary and other methods can be any authentication type.
- Layer 2—Allows you to configure Spanning Tree, VTP, LLDP, and CDP. By default, Rapid PVST and CDP are enabled because they are required by Prime Infrastructure.
- High Availability—Allows you to configure power and system redundancy. If the High Availability check box is unchecked, redundancy is disabled on the device.
- Interfaces—Allows you to configure VLANs. You can check how many ports your devices have and based on that information, you can split the interfaces into interface patterns.
- Other—Allows you to configure any other commands in the terminal configuration mode.

Configuring Wireless Features

When you choose to configure wireless features, you are guided step-by-step through configuring the following settings:

1. Create Groups
2. Wireless Parameters
3. Wireless LAN Security
4. Guest Access
5. Confirmation

Create Groups

The Create Groups page is where the Mobility Architecture group is automatically defined for the wireless devices that you selected in the Choose Other Devices page. The Mobility Group consists of Mobility Controller, Switch Peer Group, and Mobility Agents. You cannot modify the Mobility Controller and the Mobility Agent that were previously configured. Whereas, you can add Switch Peer Groups. You can configure the selected devices as Mobility Controller/Mobility Agent or delete the Mobility Controller/Mobility Agent from the mobility group.

Wireless Parameters

The Wireless Parameters page allows you to assign Wireless Management IP, Mask, and Wireless VLAN ID for the selected wireless devices. You can also choose to export the list of devices as a CSV file, edit the values, and import the file to overwrite the values for the devices. Then, click **Save**.

Wireless LAN Security

The Wireless LAN Security page allows you to add secure wireless for LAN connectivity. Default values are displayed for the Secure wireless LAN Properties. Based on the security profile and the authentication method that you choose, you must enter the primary and secondary Radius server details.

Guest Access

The Guest Access page is displayed only if you have chosen to configure guest access as part of the wireless device configuration in the Choose Other Devices page. Default values are displayed for the guest WLAN and VLAN fields. Based on the security profile and the authentication method that you select for your guest, you must enter the primary and secondary Radius server details.

Confirmation

The Confirmation page is the last step in the Guided workflow for wireless features in which you can view the settings you specified. Click Deploy to deploy the configuration. For more information about the confirmation job status and the workflow status, see the Confirmation.

Configuring Plug and Play Controller Auto Provisioning

Prime Infrastructure simplifies WLAN deployments with support for auto-provisioning. Auto provisioning allows Prime Infrastructure to automatically configure a new or replace a current Cisco Wireless LAN Controller (WLC). Prime Infrastructure auto provisioning feature can simplify deployments for customers with a large number of controllers.

Note The controller radio and b/g networks are initially disabled by the Prime Infrastructure startup configuration file. You can turn on those radio networks by using a template, which should be included as one of the automated templates.

Using the Auto Provisioning Filter List

The Auto Provision Filters page allows you to create and edit auto provisioning filters that define the list of allowable devices to be auto provisioned or auto monitored by Prime Infrastructure.

For Auto Provisioning privileges, you must have Admin, Root, or SuperUser status. To allow or disallow a user Auto Provisioning privileges, edit the permitted tasks using **Administration > Users, Roles, & AAA > User Groups >** ***group name*** **> List of Tasks Permitted** in Prime Infrastructure. Select or unselect the check box to allow or disallow these privileges.

Filter parameters include:

Parameter	Description
Filter Name	Identifies the name of the filter.
Filter Enable	Indicates whether or not the filter is enabled. Only enabled filters can participate in the Auto Provisioning process.
Monitor Only	If selected, the Cisco WLC defined in this filter is managed by Prime Infrastructure but not configured by Prime Infrastructure if the Cisco WLC contacts Prime Infrastructure during the auto provisioning process.
Filter Mode	Indicates the search mode for this filter (Host Name, MAC Address, or Serial Number).
Config Group Name	Indicates the Configuration Group name. All Config-Groups used by auto provision filters should not have any controller defined in them.

Adding an Auto Provisioning Filter

To specify the Auto Provision filter contents, you can directly enter the details in the application or import the details from a CSV file. The auto provisioning feature supports the 5500 and non-5500 series controllers. The non-5500 series controllers have AP manager interface configuration information defined, whereas 5500 series controllers do not have this information.

To add an Auto Provisioning Filter:

Step 1 Choose **Configuration >Wireless Technologies > Controller Auto Provisioning**.

Step 2 Choose **Add Filter** from the **Select a command** drop-down list, then click **Go**.

Step 3 Enter the required parameters.

You can specify the Dynamic Interface configuration and Device Specific configuration details only when you input a CSV file. These two configurations cannot be performed using the graphical user interface.

Step 4 Click **Save**.

To change the default username and password, you need to delete and then recreate the admin user and explained in Steps 5 through Step 8.

Step 5 To change the default username and password, you need to create a new read/write user on the controller using the Local Management User Template. See Creating Local Management User Templates.You must create this new user so that you can delete the default admin user as shown in Step 6.

Step 6 Choose **Inventory > Device Management > Network Devices > All Devices**, click on the controller name, click the **Configuration** tab, then select **Management > Local Management User**, select the admin user, then from the **Select a command** drop-down list, select **Delete Local Management User** and click **Go**.

Step 7 Create a new admin user on the controller using the Local Management User Template. See Creating Local Management User Templates.

Step 8 Delete the user you created in Step 5.

Related Topic

- Creating Local Management User Templates

Auto Provisioning Primary Search Key Settings

Use the Primary Search Key Setting to set the matching criteria search order.

Step 1 Choose **Configuration > Plug and Play > Controller Auto Provisioning**, then from the left sidebar menu, choose **Setting**.

Step 2 Click to highlight the applicable search key, then use the **Move Up** or **Move Down** buttons to move the search key to a higher or lower priority.

Step 3 Click **Save** to confirm the changes.