
# 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, page 6-1.
- Setting up access switches after they have been added to Prime Infrastructure—See Getting Help Setting Up Access Switches, page 6-6.

## 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 **Workflow** menu appears for users with the following privileges only: root, super users, and Config Managers.

When you choose **Workflows > Plug and Play Setup**, Prime Infrastructure guides you through creating a Plug and Play profile that creates a bootstrap configuration file, which creates a bootstrap configuration file and another *config* file that includes Telnet and SSH credentials, to allow new Cisco IOS devices to "call home" to Prime Infrastructure to get further configurations. Using the Plug and Play Setup Workflow eliminates the need to "console" into each device to set it up before it can be managed by Prime Infrastructure.

The Plug and Play Setup workflow is similar in functionality to **Design > Plug and Play Profiles** and **Deploy > 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 explained in Automating Device Deployment, page 9-2.

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, page 6-3

# Supported Devices and Software Images for Plug and Play Setup Workflow

Table 6-1 lists the devices and corresponding software images supported for Workflows > Plug and Play Setup.

***Table 6-1 Supported Devices and Image Versions for Workflows > Plug and Play Setup***

| 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 |
| 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 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 |

# Prerequisites

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, page 6-3. 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, page 6-3.
- 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 PI server by choosing **Administration > System Settings > Server Settings**, 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 6-2.

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 6-2 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 6-2 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. |

# 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, page 6-3.
- **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.

# Specifying Device Credentials

The **Workflows > Plug and Play Setup > 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, page 6-3, make sure that you have satisfied the necessary requirements before you specify how you want to deploy or export the Plug and Play profile.

- **Deploy 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 > 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, the Workflow Status menu at the bottom of the Prime Infrastructure interface refreshes to reflect 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, page 6-6.

# Sample Output from Plug and Play Setup

When you complete the steps in **Workflows > Plug and Play Setup**, 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, *pi2-pod1-171* is the Prime Infrastructure server hostname.

```
ip host pi2-pod1-171 192.168.138.171
cns trusted-server all-agents pi2-pod1-171
cns id hardware-serial
cns id hardware-serial event
cns id hardware-serial image
cns even pi2-pod1-171 11013 keepalive 120 2 reconnect0time 60
cns exec 80
cns image server http://pi2-pod1-171/cns/HttpMsgDispatcher status
http://pi2-pod1-171/cns/HttpMsgDispatcher
cns config partial pi2-pod1-171 80
cns config initial pi2-pod1-171 80
```

In addition to the bootstrap configuration file, another config file is created in the TFTP location which provisions the credentials you provided on the Create Profile page.

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

- **Deploy via TFTP**—Prime Infrastructure copies the bootstrap configuration file, *cisconet.cfg*, and 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 > 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

When a supported device uses the Plug and Play profile to connect to Prime Infrastructure, the device is listed in the Workflow Status window (in the Newly Registered Device column) at the bottom of the Prime Infrastructure interface. You can click a number displayed in the Workflow Status window to go directly to the Assign to Site step in the Getting Help Setting Up Access Switches workflow, which allows you to create more robust configurations for the devices.

If a device takes longer than 10 minutes to synchronize, it is not listed under the Newly Registered Device column in the Workflow Status window. However, the device is listed in the Initial Device Setup workflow with a status of N/A.

# 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 6-1.
- Supported devices for **wireless** features:
  - Catalyst 3850 switches
  - Cisco 5760 Wireless LAN Controllers

### Related Topics

- Before You Begin, page 6-7
- Assign Devices to Sites

# Before You Begin

You must create sites before you use the Initial Device Setup by choosing **Design > Site Map Design**. See Creating Sites for more information.

### Related Topic

- Assign Devices to Sites, page 6-7

# Assign Devices to Sites

The **Workflows > Initial Device Setup > Assign to Site** window allows you to specify a site 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, page 6-1) and any discovered devices that were not previously assigned are listed on this window. You must assign each device to a site.

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

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 the Device 360° View, page A-12 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 **Workflows > Initial Device Setup > Choose Other Devices** window displays all new devices you assigned to the specified site, any devices previously assigned to the same site, 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 you select.

If you select **Add wired features to my device(s)**, only applicable devices in the selected site on which you can configure wired features are displayed. After you select the devices, check the Device Readiness column and see Device Readiness Explanation, page 6-8 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 site 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 that you want to deploy and select a mobility domain.

### Device Readiness Explanation

The Readiness column indicates whether the devices 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 6-3 lists the required versions.
- Prime Infrastructure was unable to collect inventory details. Choose **Operate > Device Work Center** and make sure the Admin Status for the device is *Managed* and the Inventory Collection Status is *Completed*.

***Table 6-3 Required Cisco IOS/IOS XE Releases for Switches to Be in Ready State***

| Switch Series | Required Cisco IOS/IOS XE Releases |
|---|---|
| Catalyst 2960, 2960s | 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 3850 | IOS XE 03.02.01 SE and later |
| Catalyst 4500 | When running Sup7E and Sup7LE: IOS XE 03.03.02.SG and later<br>When running Sup6E or Sup6LE: 12.2(54)SG and later |
| 5760 Wireless LAN Controller | IOS XE 03.02.01 SE and later |

#### Related Topics

- Configuring Wired Features Using Guided Mode, page 6-8
- Configuring Wired Features Using Advanced Mode, page 6-10
- Configuring Wireless Features, page 6-11

# 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, page 6-8
2. Device Credentials, page 6-9
3. VLAN and Switching Parameters, page 6-9
4. Auto Smartports and Uplinks, page 6-9
5. Confirmation, page 6-10

## IP Address Options

During the **Workflows > Plug and Play Setup** workflow (see Preconfiguring Devices to be Added Later, page 6-1), 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 **Workflows > Plug and Play Setup** workflow (see Preconfiguring Devices to be Added Later, page 6-1), 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 Dashboard** 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 Workflow Status menu at the bottom of the Prime Infrastructure interface. 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, page 6-11
2. Wireless Parameters, page 6-11
3. Wireless LAN Security, page 6-11
4. Guest Access, page 6-11
5. Confirmation, page 6-11

## 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.

## 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" section on page 6-10.