Network Plug and Play

This chapter contains the following sections:

About Network Plug and Play

Network Plug and Play is a service that works in conjunction with Network Plug and Play enabled devices to allow firmware and configuration to be managed centrally, and to allow zero-touch deployment of new network devices. Devices may be deployed directly using the Network Plug and Play protocol, or indirectly if discovered by a probe that is associated with the Dashboard.

When installed, a Network Plug and Play enabled device will identify the Network Plug and Play server through one of manual configuration, DHCP, DNS, or the Plug and Play Connect service. The following sections provide more detail on the configuration of the Network Plug and Play service in Cisco Business Dashboard.

Network Requirements

A Network Plug and Play device will automatically find the address of the Network Plug and Play server using one of the following methods below. Each method will be attempted in turn until an address is found or all methods have failed. The methods used are, in order:

- **Manual configuration**—A Network Plug and Play enabled device can be manually configured with the address of the server through the administration interface
- **DHCP**—The address of the server can be supplied to the device in the Vendor-specific Information option
- **DNS**—If the DHCP Vendor-specific Information option has not been provided, then the device will perform a DNS lookup for the server using a well-known hostname
- **Plug and Play Connect Service**—If no other method has been successful, the device will attempt to contact the Plug and Play Connect service. This service will then redirect the device to your server.

Once the device has identified the server, it will contact the server and update firmware and configuration as specified by the server.

Certificate Requirements

When establishing a connection to a Network Plug and Play server, the client checks to ensure the certificate presented by the server is valid and can be trusted. For the certificate to be acceptable and the connection to proceed, the certificate must meet the following conditions:

- The certificate must be signed by a trusted Certificate Authority (CA), or the certificate itself must be trusted by the client. A certificate downloaded from the TrustpoolBundleURL learned from DHCP, or from the Plug and Play Connect service is trusted by the client
- If the server identity is discovered using manual configuration, DHCP or Plug and Play Connect, and is an IP address, then either the **Common Name** field or the **Subject-Alt-Name** field must contain that IP address
- If the server identity is discovered using manual configuration, DHCP or Plug and Play Connect, and is a hostname, then either the **Common Name** field or the **Subject-Alt-Name** field must contain that hostname
- If the server identity is discovered using DNS discovery, then either the **Common Name** field or the **Subject-Alt-Name** field must contain the IP address corresponding to the well-known hostname pnpserver.<*local domain*>

Note Some of the older Network Plug and Play client implementations do not verify the presence of the server identity in the certificate.

Setting up Discovery using DHCP

To discover the server address using DHCP, the device will send a DHCP discover message with option 60 that contains the string “ciscopnp”. The DHCP server must send a response containing the Vendor-specific Information option (option 43). The device extracts the server address from this option and uses this address to contact the server. An example of an option 43 string containing the address of a Network Plug and Play server is “5A1N;B2;K4;I172.19.45.222;J80”.

The option 43 string has the following components, delimited by semicolons:

- 5A1N—Specifies the DHCP sub-option for Plug and Play, active operation, version 1, no debug information. It is not necessary to change this part of the string.
- B2—IP address type:
  - B1 = hostname
  - B2 = IPv4
- K4—Transport protocol to be used between the Cisco Plug and Play Agent and the server:
  - K4 = HTTP (default)
  - K5 = HTTPS

- Ixxx.xxx.xxx.xxx—IP address or hostname of the server (following a capital letter i). In this example, the IP address is 172.19.45.222.
- Jxxxx—Port number to use to connect to the server. In this example, the port number is 80. The default is port 80 for HTTP and port 443 for HTTPS.
- T*trustpoolBundleURL*—Optional parameter that specifies the external URL of the trustpool bundle if it is to be retrieved from a different location than the server. For example, to download the bundle from a TFTP server at 10.30.30.10, you would specify the parameter like this: Ttftp://10.30.30.10/ca.p7b
- If you are using trustpool security and you do not specify the T parameter, the device retrieves the trustpool bundle from the server.
- Zxxx.xxx.xxx.xxx;—IP address of the NTP server. This parameter is mandatory when using trustpool security to ensure that all devices are synchronized.

Consult the documentation for your DHCP server for details on how to configure DHCP options.

Setting up Discovery using DNS

If DHCP discovery fails to get the IP address of the server, the device falls back to a DNS lookup method. Based on the network domain name returned by the DHCP server, the device constructs a fully qualified domain name (FQDN) for the server, using the preset hostname “pnpserver”.

For example, if the DHCP server returns the domain name “example.com”, the device constructs the FQDN “pnpserver.example.com”. It then uses the local name server to resolve the IP address for this FQDN.

Setting up Discovery using Plug and Play Connect

Plug and Play Connect is a Cisco-provided service that is the last resort used by a Network Plug and Play-enabled device to discover the server. To use Plug and Play Connect for server discovery, you must first create a Controller Profile representing the PnP server, and then register each of your devices with the Plug and Play Connect Service.

Accessing the Plug and Play Connect Service

To access the Plug and Play Connect Service, do the following:

1. In your web browser, navigate to *https://software.cisco.com*
2. Click the **Log In** button at the top right of the screen. Log in with a cisco.com ID associated with your Cisco Smart Account.
3. Select the **Plug and Play Connect** link under the **Network Plug and Play** heading. The main page for the **Plug and Play Connect** service is displayed.

Creating a Controller Profile

To create a Controller Profile for the PnP server, do the following:

1. Open the Plug and Play Connect web page in your browser. If necessary, select the correct Virtual Account to use.
2. Select the Controller Profiles link, and then click the Add Profile button.
3. Select a Controller Type of PNP SERVER from the drop-down list. Then click Next.

4. Specify a name, and optionally a description for the profile.
5. Under the heading for Primary Controller, use the drop-down provided to select whether to specify the server by name or IP address. Fill in the name or addresses of the server in the fields provided.
6. Select the protocol to use when communicating with the server. It is strongly recommended that HTTPS be used to ensure the integrity of the provisioning process.
7. If the protocol selected is HTTPS, the certificate used by the server should be uploaded using the controls provided. See Managing Certificates for details on downloading the certificate from Cisco Business Dashboard.
8. Optionally specify a Secondary Controller.
9. Click **Next**, and review the settings before clicking **Submit**.

Registering Devices

Certain products purchased directly from Cisco may be associated with your Cisco Smart Account at the time of order, and these will automatically be added to Plug and Play Connect. However, the majority of Cisco Business Plug and Play-enabled products will need to be registered manually. To register devices with Plug and Play Connect, do the following:

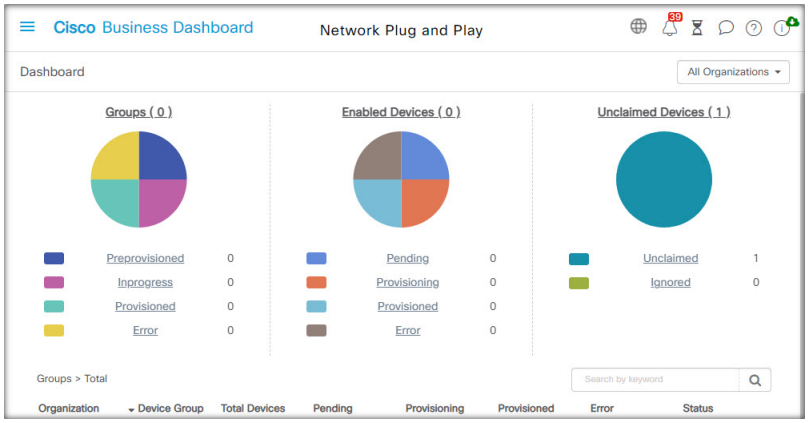
1. Open the Plug and Play Connect web page in your browser. If necessary, select the correct Virtual Account to use it.
2. Select the **Devices** link, and then click **Add Devices**. You may need to be approved to manually add devices to your account. This is a one-time process, and, if it is required, you will be notified by email once approval has been granted.
3. Choose whether to add devices manually, or to add multiple devices by uploading details in CSV format. Click the link provided to download a sample CSV file. If you choose to upload a CSV file, click the **Browse** button to select the file.
4. Click **Next**.
5. If you selected to add devices manually, click **Identify Device**. Specify the Serial Number and Product ID for the device to be added. Select a Controller Profile from the drop-down. Optionally enter a description for this device.
6. Repeat step 4 until you have added all your devices, then click **Next**.
7. Review the devices you have added, and then click **Submit**.

Configuring the Network Plug and Play Service

There are several tasks that you need to perform when setting up the Network Plug and Play service for your environment. These include uploading configurations and images, adding and configuring devices to use Network Plug and Play, and managing devices that connect to the service when they have not previously been registered with the service. The following sections describe these tasks in detail.

Using the Network Plug and Play Dashboard

The **Network Plug and Play** Dashboard provides an overview of the devices currently being provisioned using Network Plug and Play.



Three charts are displayed showing the device status broken down by:

- Device group
- PnP enabled device
- Devices that are not defined in the Cisco Business Dashboard inventory (unclaimed devices)

Each chart shows the number of devices or groups in each of the states listed. You can click on the state heading on any of the charts to see a detailed list of devices or groups that fall into that category. The following table provides a breakdown of the different statuses:

Table 1: Network Plug and Play Dashboard – Status Definitions

Status	Description
Groups	
Pre-provisioned	Device groups with PnP-enabled devices in the Pending state only.
In Progress	Device groups with some PnP-enabled devices in the Pending state and some in the Provisioning or Provisioned state.
Provisioned	Device groups where all PnP-enabled devices are in the Provisioned state.
Error	Device groups with one or more PnP-enabled devices in the Error state.
Enabled Devices	
Pending	Devices in the inventory that have been enabled for PnP, but have not yet contacted the PnP server.
Provisioning	Devices that have contacted the PnP server and begun provisioning but have not completed the provisioning process.
Provisioned	Devices that have been successfully provisioned using PnP.

Status	Description
Error	Devices where the PnP provisioning process has failed.
Unclaimed Devices	
Unclaimed	Devices that have contacted the PnP server but are not defined in the inventory.
Ignored	Unclaimed devices that have been explicitly ignored by the user.

You can restrict the data displayed to a specific organization using the organization drop-down at the top right of the page. When viewing device groups, type all or part of a group name in the search box to limit the groups displayed in the table. Or you can enter a device name, product ID or serial number in the search box when viewing provisioning rules to display the current status of an individual device.

Note The chart for unclaimed devices is only displayed to **Administrators** who are viewing data for **All Organizations**.

Managing Enabled Devices

Enabled Devices are devices in the inventory that have been configured for provisioning with an image or configuration file, or were previously discovered by Cisco Business Dashboard and have attempted to connect using the Network Plug and Play protocol. An Enabled Device that has been configured with an image or configuration file will have that image and/or configuration applied to the device at the next opportunity. If the device is connected to and managed by the Dashboard, the changes will be applied immediately. Otherwise, the changes will be applied the next time the device is connected - either via a probe or direct management, or when it checks in using the Network Plug and Play protocol. An Enabled Device may also be set to apply changes during the next change window, in which case the changes will be delayed until the next change window after the device checks in.

To create a new Enabled Device, follow the steps below.

1. Navigate to **Network Plug and Play** >**Enabled Devices**.
2. Click the ✚(plus) icon to add a new enabled device to the inventory.

Note You may also click the upload icon to add devices in bulk using a csv file. Template csv files may be downloaded from the **Network Plug and Play > Configurations** page by opening the configuration template to be used for the devices and selecting **Download CSV Template** from the **Actions** dropdown.

3. Fill out the **Add New Device** form with the requested parameters, including identifying details for the device, the organization, network and device group it should belong to, then click **Next**.
4. Optionally, select a firmware image to be applied to the device. If you choose **Default** for the image, the device will use the image that is designated as the default for the product ID at the time the device connects to the server.

Note You may use the checkbox on this page to delay the provisioning of the new device until the next change window. However, this is rarely appropriate when creating a new device, as a new device is not usually an active part of the network until after provisioning is complete.

5. Optionally, select a configuration to be applied to the device, along with the version of the configuration if there is more than one version. If the configuration is a template containing placeholders, a form will be displayed prompting for the values that should be used for this device. Complete these fields as necessary. If the template makes use of parameters defined by the system, click on the checkbox to display the values that will be used.
6. Click **Next** to proceed to the **Summary** screen. Review the data entered to ensure it is correct. You can also review the final device configuration in the preview window at the bottom. When you are satisfied, click **Finish**.

To edit an existing device, follow the steps below.

1. Navigate to **Network Plug and Play**>**Enabled Devices**.
2. Check the checkbox for the device to be modified and click **Edit**. Alternatively, you can click the name of the device.
3. Click **Next** to display the **Provision Device** screen. Change the image and/or configuration file if required and make any changes to the parameter values associated with the configuration. Optionally, check the checkbox to ensure that changes will be applied during the change window.
4. Click **Next** to proceed to the **Summary** screen. Review the data entered to ensure it is correct. You can also review the final device configuration in the preview window at the bottom. When you are satisfied, click **Finish**.

Note If the image or configuration file settings are changed for a device that has already been provisioned, that device's state will reset to pending, and the device will be re-provisioned.

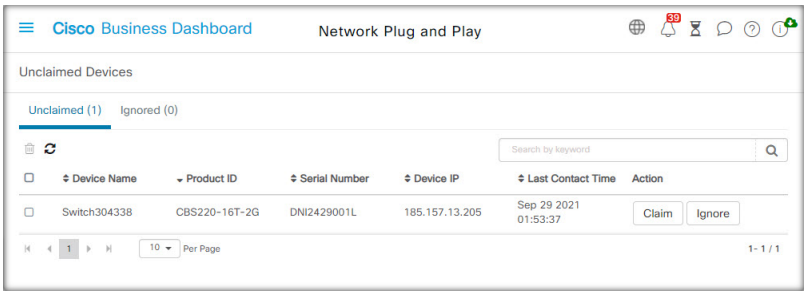
To remove an Enabled Device, follow the steps below.

1. Navigate to **Network Plug and Play** >**Enabled Devices**.
2. Check one or more checkboxes for the devices to be removed and click the **delete** icon.

Note If an Enabled Device is deleted when that device is otherwise known to the Dashboard and the device is online, only the image and configuration files settings for that device will be removed. The device will remain in the inventory similar to any other managed device. If a device subsequently connects to the Dashboard using PnP, a new entry will be added to the Enabled Devices table.

Unclaimed Devices

Note The **Unclaimed Devices** page is only available to Administrators.



An unclaimed device is one that has connected to the service, but there is no device record in the inventory that matches the device. To see a list of unclaimed devices, and to claim an unclaimed device so it can be managed using Network Plug and Play, follow the steps below.

1. Navigate to **Network Plug and Play** >**Unclaimed Devices** and select the **Unclaimed** tab.
2. Click the claim button for the device to be managed.
3. Fill out the Unclaimed Device form with the requested parameters, including the organization, network and device group it should belong to, then click **Next**.
4. Optionally, select a firmware image to be applied to the device. If you choose **Default** for the image, the device will use the image that is designated as the default for the product ID at the time the device connects to the server.
5. Alternatively, select a configuration to be applied to the device, along with the version of the configuration if there is more than one version. If the configuration is a template containing placeholders, a form will be displayed prompting for the values that should be used for this device. Complete these fields as necessary.

   If the template makes use of parameters defined by the system, you can check the checkbox to display the values that will be used.
6. Click **Next** to proceed to the **Summary** screen. Review the data entered to ensure it is correct. You can also review the final device configuration in the preview window at the bottom. When you are satisfied, click **Finish**.

To remove a device from the Unclaimed list without provisioning it, follow the steps below.

1. Navigate to **Network Plug and Play**>**Unclaimed Devices** and select the **Unclaimed** tab.
2. Click **Ignore** for the device you wish to remove from the list.

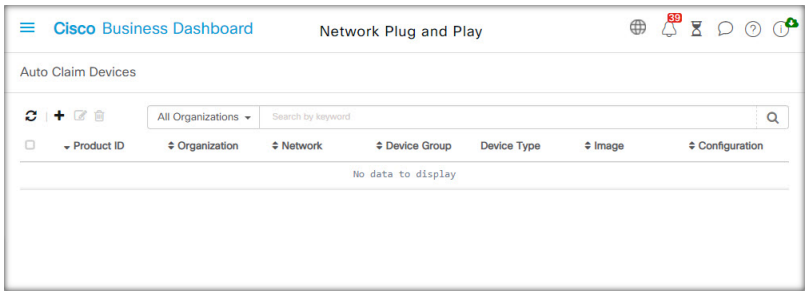
The devices will be moved to the **Ignored** list and no further action will be taken. To reclaim an ignored device, follow the steps below.

1. Navigate to **Network Plug and Play**>**Unclaimed Devices** and select the **Ignored** tab.
2. Click the **Unignore** button for the device to be reclaimed.

The devices will be moved to the **Unclaimed** list, and you can claim the devices as described above.

Auto Claiming Devices

Note The **Auto Claim** page is only available to Administrators.



Unclaimed devices can be automatically claimed and provisioned by the server by creating an Auto Claim rule for that product ID. To create an Auto Claim rule, follow the steps below.

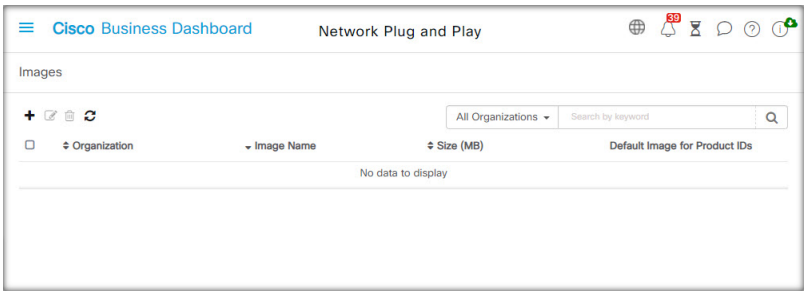
1. Navigate to **Network Plug and Play**>**Auto Claim Devices**.
2. Click the **+**(plus) icon to create a new **Auto Claim** rule.
3. Fill out the Auto Claim Device form with the requested parameters, including the Product ID (PID) to be matched, and the organization, network, and device group the newly claimed device should belong to, then click **Next**.
4. Optionally, select a firmware image to be applied to the device. If you choose **Default** for the image, the device will use the image that is designated as the default for the product ID at the time the device connects to the server.
5. Alternatively, select a configuration to be applied to the device, along with the version of the configuration if there is more than one version. If the configuration is a template containing placeholders, a form will be displayed prompting for the values that should be used for this device. Complete these fields as necessary.

   If the template makes use of parameters defined by the system, you can check the checkbox to display the values that will be used.
6. Click **Next** to proceed to the **Summary** screen. Review the data entered to ensure it is correct. You can also review the final device configuration in the preview window at the bottom. When you are satisfied, click **Finish**.

New devices that are not present in the inventory will be compared against the list of Auto Claim rules. If there is a match, a new device record will be created in the inventory with the image and configuration file defined by the **Auto Claim** rule. The device will then be provisioned accordingly. If the device does not match an **Auto Claim** rule, it will be added to the Unclaimed list and no further action will be taken.

Device Firmware Images

The **Images** page allows you to upload firmware images that can then be deployed to the devices.



Firmware images can be designated as the default image for different platforms, allowing you to update the firmware across an entire family of devices very easily. Firmware images are specific to an organization and can only be used for provisioning devices associated with the same organization.

To upload a firmware image, follow the steps below.

1. Navigate to **Network Plug and Play** > **Images**.
2. Click the ✚(plus) icon.
3. Select the organization for the image from the dropdown.
4. Drag a firmware image from your PC and drop it on the target area of the **Upload File** window. Alternatively, click the target area and select a firmware image to upload.
5. Click **Upload**.

You can change the filename or designate an image as the default image for one or more device types. To modify the filename or designate an image as a default image, follow the steps below.

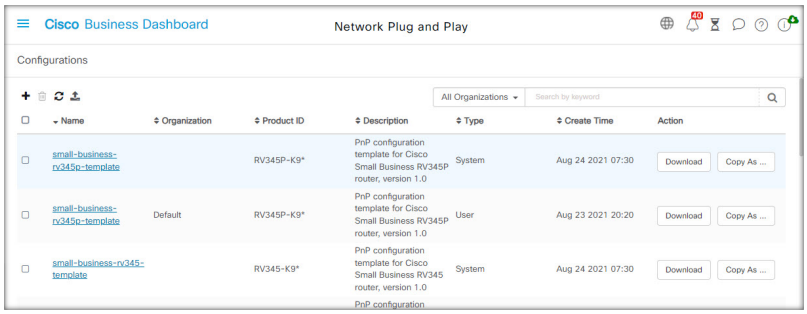
1. Navigate to **Network Plug and Play** >**Images**.
2. Select the radio button for the image in the **Images** table and click **edit**.
3. If desired, modify the filename of the image using the textbox provided.
4. Optionally enter a comma-separated list of product IDs into the **Default Image for Product IDs** field. Product IDs can contain the wildcard characters '?', representing a single character, and '*', representing a string of characters.
5. Click **Save**.

To remove an image, follow the steps below.

1. Navigate to **Network Plug and Play** >**Images**.
2. Select the radio button for the image to be deleted and click **delete**.

Device Configuration Files

The Configurations page allows you to upload or create configuration files that can then be deployed to the devices. Configuration files are specific to an organization and can only be used for provisioning devices associated with the same organization.



Configuration files can be simple text files, or can contain placeholders and associated metadata to allow the same configuration file to be used with multiple devices, while still allowing for unique parameters to be set on a device by device basis. For example, a single configuration template could be applied to multiple devices, but allow the hostname to be specified individually for each device.

Several configuration templates are included with the Dashboard application as system templates and are available to all organizations. These templates allow commonly changed settings to be modified, and can be used as is, or copied and used as a basis for new templates. For more information on the syntax of the configuration templates, See *Appendix A: Managing Configuration Templates*.

To create a new configuration manually, follow the steps below.

1. Navigate to **Network Plug and Play**>**Configurations**.
2. Click the ✚(plus) icon.
3. The template editor opens with a blank area for the configuration on the left, and a form on the right for managing the metadata associated with the template.

   Enter a name for the configuration in the field at the top left. Select an organization and enter a comma-separated list of product IDs that support this configuration in the fields on the right. Optionally, enter a description. Product IDs can contain the wildcard characters '?', representing a single character, and '*', representing a string of characters.
4. Create the configuration by typing or pasting text into the text area on the left. If necessary, make the appropriate changes to the metadata using the controls on the right.

   You can use the **Preview** button to see how the configuration template will appear when it is assigned to a device.
5. When you are satisfied with the configuration, click **Save**.

To upload a configuration file, follow the steps below.

1. Navigate to **Network Plug and Play** >**Configurations**.
2. Click the **Upload** icon.
3. Select the organization for the configuration from the dropdown. Specify a name for the configuration and optionally add a description.
4. Drag a configuration file from your PC and drop it on the target area of the **Upload File** window. Alternatively, click the target area and select a configuration file to upload.
5. Click **Upload**.

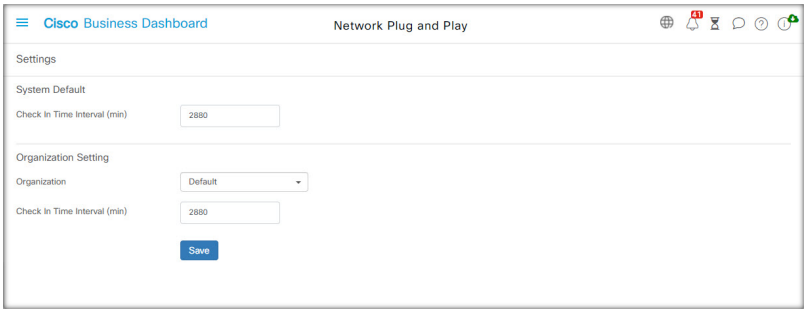
You can click on the filename of the uploaded configuration file to view the contents in the template editor, if you wish.

To remove a configuration, follow the steps below.

1. Navigate to **Network Plug and Play** >**Configurations**.
2. Check one or more checkboxes for the configurations to be removed and click the **delete** icon.

Managing Settings

The Network Plug and Play Settings page allows you to control the operation of the Network Plug and Play Protocol.



The **Check In Time Interval** controls how frequently a device will connect to the Network Plug and Play service after initial provisioning. To modify this parameter, follow the steps below.

1. Navigate to **Network Plug and Play**>**Settings**.
2. Enter the desired interval between connections in the field provided. The time is in minutes, and the default is 2880 minutes, or two days.
3. Click **Save**.

The **Check In Time Interval** is set for the system as a whole, but can be overridden at the organization level. If no interval is set for the organization, then the system value is used.

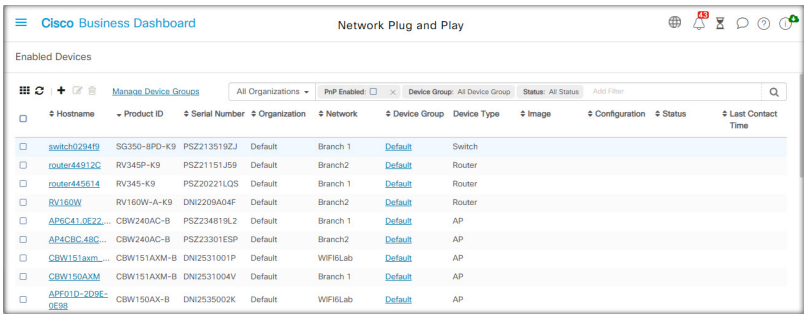
Configuring the Certificate

The certificate automatically generated by Cisco Business Dashboard during first startup is a self-signed certificate. In most cases, this will not be sufficient for the certificate to be accepted by the Network Plug and Play client, and it will be necessary to generate a new certificate. When generating a new self-signed certificate or certificate signing request (CSR), the Dashboard will include the contents of the **Common Name** field in the **Subject Alternative Name** field in addition to any values specified in the **Subject Alternative Name** field on the GUI.

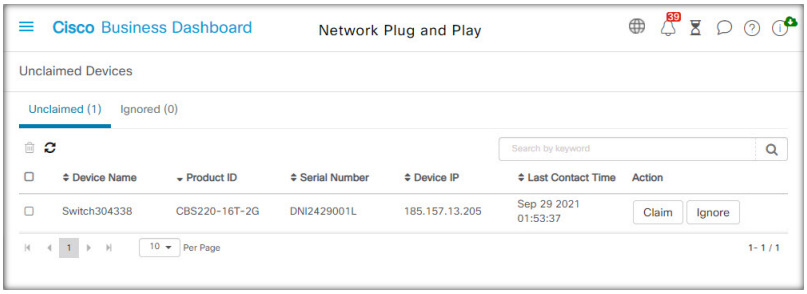
For more information on configuring the Dashboard's certificate, see Managing Certificates.

Monitoring Network Plug and Play

Each device known to the Network Plug and Play service is shown on either the **Enabled Devices** page



or the **Unclaimed Devices** page with a status displayed.



This status can also be viewed on the **Inventory** page by enabling the display of the **PnP Status** column. The status field shows the current state of the device, and will contain one of the values as listed in the following table. By clicking on the status field, you can see more detail, including a history of the state changes for this device over time.

Table 2: Network Plug and Play - Device Status

Status	Description
Pending	Device is defined but has not made contact with the service.
Provisioning	The device has made the initial connection to the service.
Provisioning_Image	A firmware image is being applied by the device.
Provisioned _Image_Rebooting	The device is rebooting to run the new firmware.
Provisioned_Image	New firmware has been applied successfully.
Provisioning_Config	A configuration file is being applied to the device.
Provisioned_Config	The configuration file has been successfully applied to the device. Depending on the type of device, it can reboot to apply the configuration.
Error	An error has occurred. Check log files for more details.
Provisioned	The provisioning process for the device is complete.