Network Plug and Play Solution Guide for SMB

First Published: June 3, 2019
Last Updated: June 3, 2019

Conventions 2
Solution Overview 4
Solution Components 5
Solution Workflows 5
Planned Device Deployment in a Managed Network 6
Planned Device Deployment in an Unmanaged Network 6
Unplanned Device Deployment 7
Generic Device Deployment 8
Deploying the Cisco Network Plug and Play Solution for SMBs 8
Pre-requisites 8
Design Considerations 9
Plug and Play Server Discovery 9
Secure Connectivity 10
Device Deployment Considerations 10
Preparing FindIT Network Manager 11
Setting Up the Server Identity 11
Upload Images and Configurations 12
Create Provisioning Rules 12
Create Provisioning Rules for Unplanned Devices 12
Server Discovery 13
Configuring DHCP for PnP Server Auto-Discovery 13
Configuring DNS for PnP Server Auto-Discovery 13
Using PnP Connect for PnP Server Auto-Discovery 14
Troubleshooting 14
FindIT Network Manager PnP Server Troubleshooting 14

Verify the Service is Running 14
Verify the Server Certificate 15
View System Logs 15
PnP Device Troubleshooting 15
Verify Server Reachability 15
Verify System Clock Accuracy 16
Check Device Status in the Manager 16
Check Unclaimed Devices 16
View Device Logs 16
Logging a Support Case 16
Obtaining Documentation and Submitting a Service Request 17
Legal Information 18
Cisco Trademark 19
Cisco Copyright 19

Conventions

This document uses the following conventions.

Convention	Indication
bold font	Commands and keywords and user-entered text appear in bold font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier font`	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution: Means *reader be careful.* In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning: IMPORTANT SAFETY INSTRUCTIONS

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Solution Overview

It is well recognized in the Information and Communications Technology industry that performing network deployments for enterprises and large campuses can be challenging, and often require skilled installers to pre-stage equipment or visit each site to perform the installation. What is less well recognized is that these same challenges exist for small and medium businesses (SMBs) as well, along with the added constraints of extremely limited staff and budgets. Just like large enterprises, SMBs are looking to simplify the deployment process for new networks and offices without compromising functionality or security.

The Cisco Network Plug and Play solution provides a simple, secure, unified, and integrated offering for businesses both large and small to ease new network rollouts or for provisioning updates to an existing network. The solution provides a unified approach to provision networks comprised of Cisco routers, switches, and wireless devices with a zero-touch or near zero-touch deployment experience. An installer at the site can deploy a new device with minimal knowledge of the device being deployed, while the network administrator centrally manages the device configuration.

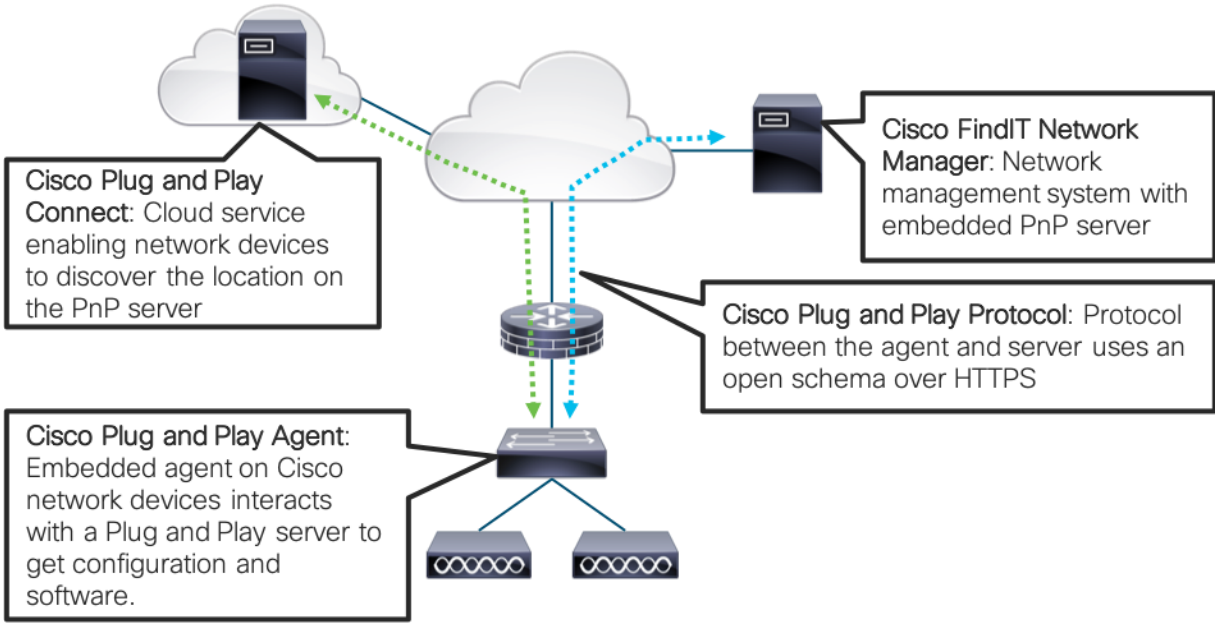
This guide will address the use of Network Plug and Play with the Cisco 100 to 500 series portfolio of routers, switches, and wireless access points. This portfolio is optimized for SMB customers who do not require the same level of functionality as is offered by the Cisco enterprise or Meraki portfolios. For more information on the use of Network Plug and Play in conjunction with the Cisco enterprise portfolio, consult the *Solution Guide for Network Plug and Play*.

Cisco Network Plug and Play used in conjunction with the Cisco 100 to 500 series portfolio offers these features:

- Simplified and consistent deployment of network devices
- Automated and centrally managed remote device deployment using Cisco FindIT Network Manager
- Converged solution for Cisco routers, switches, and wireless access point devices
- Devices can automatically discover FindIT Network Manager through DHCP, DNS, or the cloud using Plug and Play Connect, and predefined configurations and images can be pushed out as devices come online.
- Secure download of software and configuration using encrypted connections authenticated with trusted certificates. For more details on security and how it is managed, see Secure Connectivity.

Note: PnP-enabled devices from the Cisco enterprise portfolio may be used with FindIT Network Manager as the PnP server, but such deployments are outside the scope of this document.

Figure 1. Cisco Network Plug and Play Architecture



Solution Components

The Cisco Network Plug and Play solution for SMBs includes the following components:

- Cisco FindIT Network Manager–Cisco FindIT Network Manager is a network management system designed for Cisco 100 to 500 Series switches, routers, and wireless access points. As part of its functionality, FindIT Network Manager includes an embedded Network Plug and Play server.
- Cisco Network Plug and Play server–This embedded application receives Network Plug and Play requests from Cisco devices and provisions devices based on predefined rules and criteria.
- Cisco Plug and Play Agent–This agent is embedded in Cisco devices and communicates to the Cisco Network Plug and Play server using the Network Plug and Play protocol over HTTPS during device deployments.
- Plug and Play Connect–Optional cloud component for automatic PNP server discovery if the DHCP or DNS methods are not available. The Cisco network device contacts the Cisco Plug and Play Connect cloud service at devicehelper.cisco.com to obtain the IP address of the appropriate PnP server that is defined for your organization.

Solution Workflows

There are four main workflows for deploying devices in an SMB environment using Network Plug and Play:

- Planned Device Deployment in a Managed Network
- Planned Device Deployment in an Unmanaged Network
- Unplanned Device Deployment
- Generic Device Deployment

The following sections describe each of the common workflows listed above and describes the steps that should be followed for each.

Planned Device Deployment in a Managed Network

A planned device deployment occurs when the network is prepared for the device prior to the physical installation of that device occurring. A managed network is one where the network services such as DHCP or DNS are controlled by the administrator and can be used by the newly installed device to locate the PnP server. To deploy a device in a managed network, use the following procedure:

Step 1 The network administrator sets up a DHCP server in the network to respond to client discover requests with DHCP option 43, which contains information necessary to contact FindIT Network Manager.

Alternatively, DNS can be used to locate the Manager. For DHCP and DNS configuration details, see Server Discovery.

Step 2 The network administrator creates a Network Plug and Play enabled device in FindIT Network Manager.

This includes entering device information and specifying a configuration and/or image for each device to be installed. Prior to creating devices, it may also be necessary to create a new Project (FindIT Network Manager version 1.x), or a new Network and Device Group (FindIT Network Manager version 2.0 and above) to represent the network the device is to be installed in. For details on configuring Cisco Network Plug and Play in FindIT Network Manager, see the *Cisco FindIT Network Manager Administration Guide*.

Step 3 The device installer installs and powers up the Cisco network device.

Step 4 The device auto-discovers FindIT Network Manager using DHCP or DNS, identifies itself by serial number and product ID (PID) to the Cisco Network Plug and Play application, and downloads any software image and/or configuration file that were pre-provisioned by the network administrator. The device will reboot after each download.

Planned Device Deployment in an Unmanaged Network

A planned device deployment occurs when the network is prepared for the device prior to the physical installation of that device occurring. An unmanaged network is one where the network services such as DHCP or DNS are not controlled by the administrator and so cannot be used by the newly installed device to locate the PnP server. In an unmanaged network of this kind, it is typically necessary to use the PnP Connect service to locate the PnP server. This scenario is commonly encountered when deploying a new office or site, and the edge router is to be provisioned using PnP.

To deploy a device in an unmanaged network using PnP Connect, use the following procedure:

Step 1 The network administrator uses the Plug and Play Connect web portal to create a controller profile in Plug and Play Connect for the FindIT Network Manager system to be used. A Cisco Smart Account is required to use Plug and Play Connect. For more details on creating a controller profile, see Using PnP Connect for PnP Server Auto-Discovery.

Typically, the creation of a controller profile is only required once.

Step 2 In certain circumstances, Plug and Play-capable devices purchased directly from Cisco will be automatically added to Plug and Play Connect at the time of purchase. However, for the majority of SMB products and

customers, the network administrator must manually add devices.

When manually adding a device in the Plug and Play Connect web portal, the network administrator will need to provide the serial number and product ID (PID) for the device and select the appropriate controller profile to use. Multiple devices may be added in bulk by importing a CSV file.

Step 3 The network administrator creates a Network Plug and Play enabled device in FindIT Network Manager.

This includes entering device information and specifying a configuration and/or image for each device to be installed. Prior to creating devices, it may also be necessary to create a new Project (FindIT Network Manager version 1.x), or a new Network and Device Group (FindIT Network Manager version 2.0 and above) to represent the network the device is to be installed in. For details on configuring Cisco Network Plug and Play in FindIT Network Manager, see the *Cisco FindIT Network Manager Administration Guide*.

Step 4 The device installer installs and powers up the Cisco network device.

Step 5 The device contacts the Plug and Play Connect service and identifies itself by serial number and product ID (PID). The Plug and Play Connect service downloads the certificate bundle for FindIT Network Manager to the device, and then redirects the device to the Manager. The certificate bundle is supplied to the Plug and Play Connect service when creating the controller profile.

Step 6 The device contacts FindIT Network Manager, identifies itself by serial number and product ID (PID) to the Cisco Network Plug and Play application, and downloads any software image and/or configuration file that were pre-provisioned by the network administrator. The device will reboot after each download.

Note: The device will fail to contact Plug and Play Connect if the device cannot synchronize with the predefined NTP servers time-pnp.cisco.com or pool.ntp.org. To resolve this problem, unblock NTP traffic to these two host names.

Unplanned Device Deployment

In an unplanned deployment, a device is physically installed before a Network Plug and Play enabled device is created in FindIT Network Manager. In this case, the device will not be automatically provisioned with the correct image and configuration. However, this problem is easily resolved by following the Unplanned Device Deployment procedure.

Step 1 The network administrator sets up a DHCP server in the network to respond to client discover requests with DHCP option 43, which contains information necessary to contact FindIT Network Manager.

Alternatively, DNS can be used to locate the Manager. For DHCP and DNS configuration details, see Server Discovery.

Step 2 The device installer installs and powers up the Cisco network device.

Step 3 The device auto-discovers FindIT Network Manager using DHCP or DNS.

The device is listed as an Unclaimed device in FindIT Network Manager, identified by Product ID, Serial Number and IP address.

Step 4 The network administrator uses FindIT Network Manager to claim the device and provide it with a new configuration and/or image.

For more details on claiming devices in FindIT Network Manager, see the *Cisco FindIT Network Manager Administration Guide*.

Generic Device Deployment

In some networks, unique configurations are not required for each device of a particular model and it is possible to define a single, generic configuration to be used for all devices of a particular type or family. In these cases, it is often better to define generic provisioning rules for all devices of a particular model or type. To deploy devices using these generic rules, use the following procedure:

Step 1 The network administrator sets up a DHCP server in the network to respond to client discover requests with DHCP option 43, which contains information necessary to contact FindIT Network Manager.

Alternatively, DNS can be used to locate the Manager. For DHCP and DNS configuration details, see Server Discovery.

Step 2 The network administrator creates an Auto Claim rule in FindIT Network Manager for the Product ID of the devices.

In addition to specifying the Product ID, the network administrator selects an appropriate configuration and/or image for devices matching this product ID. For more details on configuring Auto Claim in FindIT Network Manager, see the *Cisco FindIT Network Manager Administration Guide*.

Step 3 The device installer installs and powers up the Cisco network device.

Step 4 The device auto-discovers FindIT Network Manager using DHCP or DNS, identifies itself by serial number and product ID (PID) to the Cisco Network Plug and Play application, and downloads the software image and/or configuration file that were specified in the Auto Claim rule. The device will reboot after each download.

Deploying the Cisco Network Plug and Play Solution for SMBs

This section discusses deploying the Cisco Network Plug and Play solution in Small and Medium Business (SMB) networks built using the Cisco 100 to 500 series product portfolio.

Pre-requisites

The following are prerequisites for using the Cisco Network Plug and Play solution in SMB networks:

- FindIT Network Manager is deployed and operational. For details, see the *Cisco FindIT Network Manager Quick Start Guide Guide*.
- The Cisco network devices to be deployed are running software releases that support the Cisco Network Plug and Play Agent. For supported platforms and software releases, see the *Cisco FindIT Network Manager - Device Support List*.
- If you are using Cisco Plug and Play Connect, the identity of the FindIT Network Manager installation is defined in the Plug and Play Connect web portal in your Cisco Smart Account, and network devices are using a

supported software release. For details on device and software release support, see the *Cisco FindIT Network Manager - Device Support List*.

Design Considerations

When deploying support for Network Plug and Play, there are a number of design considerations that should be taken in to account prior to beginning deployment. These are detailed in the following sections.

Plug and Play Server Discovery

A Network Plug and Play device will automatically find the address of the Network Plug and Play server using one of the following methods. 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 may be manually configured with the address of the server through the administration interface. Explicit configuration always takes precedence over other discovery methods.
- DHCP–The address of the server may be supplied to the device in the Vendor-specific Information option (option 43)
- DNS–If the DHCP Vendor-specific Information option has not been provided, then the device will perform discovery using DNS lookups of well-known hostnames
- Plug and Play Connect Service–Finally, 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 the correct server

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

Selecting the right discovery method to use depends on the level of control that exists over the broader network infrastructure. The use of the DHCP or DNS methods require the administration to have some level of control over the DHCP servers in the network and the domain name infrastructure. The Plug and Play Connect service requires little more than Internet access to be effective but will generally require more effort to maintain.

In most cases, the DHCP method offers the most flexibility and should be used if possible, especially if DHCP services are managed centrally and can be easily updated. DNS discovery can be more easily established in networks with many DHCP servers that are managed separately, as DNS discovery frequently only requires updates be made to one or two DNS servers. If no access is available to DHCP or DNS servers, then PnP Connect should be used.

Multiple discovery methods may also be used in combination. Setting up both DHCP and DNS discovery in the same network provides the combination of flexibility from DHCP discovery with a level of confidence that comes from having DNS discovery for devices where the DHCP server has been overlooked. A common approach is to use PnP Connect to provide discovery services for edge router deployment where DHCP and DNS are operated by the ISP and so unavailable for use, but then use DHCP for devices in the rest of the network that receive DHCP services from the router just deployed.

The manual configuration option, although reliable and flexible, is generally only used during testing of a newly deployed Manager. However, it can be used as a discovery method in environments where some pre-staging of equipment is performed.

For more details on setting up the different discovery methods, see Server Discovery below.

Secure Connectivity

The Cisco Network Plug and Play solution uses HTTPS connections between network devices and the Network Plug and Play server. This secure connectivity is implemented in one of two ways, depending on the type of transport you specify in the DHCP option or PnP Connect controller profile. DNS discovery will always attempt to use HTTPS as the transport protocol. For details on configuring DHCP discovery or PnP Connect, see Server Discovery.

Depending on the transport protocol used, secure connectivity is implemented in the following ways:

- When HTTP is specified as the transport protocol (default), secure connectivity is based on trustpoint.

  Trustpoint based secure connectivity relies on the self-signed certificate that is installed by default on FindIT Network Manager. This self-signed certificate is used to create a default trustpoint on network devices, which allows devices to connect securely over HTTPS to the Manager. HTTPS is used for communications with the Manager, despite the fact that HTTP is specified as the transport protocol. Before beginning the provisioning process, the Manager installs the certificate on the device, and then redirects the device to use HTTPS. Configuration and firmware updates are then performed through HTTPS.

- When HTTPS is specified as the transport protocol, secure connectivity is based on trustpool.

  Trustpool based secure connectivity additionally requires that you replace the self-signed certification on FindIT Network Manager with your own CA signed certificate. A trustpool is a special store of certificates signed by trusted certificate authorities and published by Cisco InfoSec. The trustpool bundle is itself signed by Cisco, allowing it to be trusted even if downloaded using an insecure transport such as HTTP or TFTP. Prior to connecting to the PnP service, the device imports the trustpool bundle into its CA store and this allows it to validate the Manager certificate, enabling secure communications over HTTPS.

  You can choose to host the trustpool bundle in a different location in your network, which you can specify in the T parameter to DHCP option 43 or using the pnptrustpool DNS name with DNS discovery. In this case, network devices would obtain your trustpool bundle instead of the default one that is installed in the Manager.

Device Deployment Considerations

There are some additional considerations that need to be taken in to account at the time devices are deployed. The considerations are about the process of deploying the devices rather than the design of the network.

Network Reachability

While it may be obvious that the devices being deployed need to be able to contact the PnP server to complete deployment, it is less obvious that there are other services that must also be reachable. Exactly which services are required will depend on the design choices made.

In an SMB environment, the most common requirement for network reachability is Internet access. Internet access is clearly required if using the PnP Connect service for discovery, but frequently Internet access will be required to access NTP services as well. It is common to rely on the default NTP service pool.ntp.org for clock synchronization, and accurate time is a pre-requisite for establishing a secure connection to the PnP server. If an accurate time source is not available, then the deployment process will fail.

Order of Deployment

When deploying multiple devices in a greenfields network, part of ensuring that network reachability is available is bring the network up in the correct order. In general, routing and upstream devices should be brought up first to provide access to the broader network. Once the router and all upstream devices are up and provisioned, switches and downstream devices can be brought up. Due consideration should also be given to the restarts performed during the provisioning process. It is wise to verify that key devices such as routers or core switches have completed provisioning

and are stable before bringing up second and third tier devices. Otherwise there is a possibility for a device to lose connectivity or even power part way through an image upgrade, potentially requiring a manual recovery to be performed.

Preparing FindIT Network Manager

There is a small amount of preparation necessary to ensure FindIT Network Manager is ready to support Network Plug and Play in a given network. First, and most importantly, it is necessary to establish the server identity so that it matches what the clients will expect. If this is not done, then the security of the process cannot be assured, and the process may fail for reasons that are not obvious to the user. Establishing the server identity is usually only done once and should generally be done at the same time as performing the initial deployment of the Manager.

Once the server identity has been correctly established, firmware and configuration files need to be uploaded and Network Plug and Play enabled devices must be created for the devices to be deployed. This is an ongoing operation, with new devices being created as the network expands, while configurations and firmware versions will be updated as network requirements change over time.

Setting Up the Server Identity

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 the Subject-Alt-Name field must contain that IP address. If the server will be reached through a NAT service, then the Subject-Alt-Name field must contain the public IP address – the same IP address the client is connecting to.
- If the server identity is discovered using manual configuration, DHCP or Plug and Play Connect, and is a hostname, then the Subject-Alt-Name field must contain that hostname
- If the server identity is discovered using DNS discovery, then the Subject-Alt-Name field must contain the well-known hostname pnpserver.<local domain>

Note: The Cisco 100 to 500 Series switch platforms do not currently check the Common Name or Server-Alt-Name fields

Note: When using DNS discovery, some older implementations of the PnP client require the Subject-Alt-Name field to contain the IP address corresponding to the well-known hostname pnpserver.<local domain>.

In release 1.1.4, FindIT Network Manager implements a number of mechanisms when generating certificates to ensure these requirements are met. In particular, when generating a Certificate Signing Request (CSR) or re-generating the self-signed certificate, the Manager automatically includes the following information in the Subject-Alt-Name field:

- The contents of the Common Name field
- The current IP address(es). If the Manager is deployed in AWS, the external, public IP address of the Manager is used.
- The hostname that was used in the web browser to connect to the administration GUI when generating the certificate or CSR

Note: When using DNS discovery, you can ensure the pnpserver.<local domain> name is included by either inserting it in the Common Name field, or by using pnpserver.<localdomain> in your web browser when generating the certificate or CSR

From release 2.0, the Subject-Alt-Name field should be specified directly along with the other parameters required when generating the certificate or CSR.

Upload Images and Configurations

Configuration and image files for the devices to be deployed must be uploaded to the Manager prior to deployment. Each file may be used for multiple devices or may be specific to a single device. Multiple files may also be uploaded for devices of the same type.

Image files may be designated as the default image for one or more product IDs. This can be used to ensure that all devices run a common software version.

See the *FindIT Network Manager Administration Guide* for detailed instructions on uploading files to the Manager.

Create Network Plug and Play Enabled Devices for Planned Devices

Network Plug and Play enabled devices are used to map individual devices to the desired image and configuration file. Devices are identified by the combination of product ID (PID) and serial number. A PnP-enabled device record should be created for each device to be deployed. When a device connects to the Manager, the PnP-enabled device records are searched, and, if a match is found, the image and configuration files specified will be pushed out to the device. The device may reboot multiple times during this process.

See the *FindIT Network Manager Administration Guide* for detailed instructions on creating provisioning rules.

Create Network Plug and Play Enabled Devices for Unplanned Devices

In some networks, it may be possible to define common configurations for all or most devices of a given type. Alternatively, there may be a requirement to ensure that any device of a particular type that is connected to the network meets a certain baseline configuration. In these cases, provisioning rules for unplanned devices – also known as Auto Claim rules – should be created.

Auto Claim rules are similar to PnP-enabled device records, but they do not match on the device serial number – only on the product ID (PID). As a result, any device with the specified PID will match this rule when connecting to the Manager so long as there is no existing device record that matches the serial number and PID of the device. When a device matches an Auto Claim rule, the image and configuration files specified in that rule will be pushed out to the device. The device may reboot multiple times during this process.

See the *FindIT Network Manager Administration Guide* for detailed instructions on creating Auto Claim rules.

Note: In FindIT Network Manager version 2.0, devices that have previously been discovered by the Manager and are already present in the inventory are effectively PnP-enabled devices without any firmware or configuration specified. They will not be visible in the PnP Enabled Device page unless and until they have connected to the Manager using PnP, but once the device connects to the Manager using PnP, they will appear on the PnP Enabled Devices page ready for configuration. This means that Auto Claim rules do not take effect for devices that are already known to the Manager at the time of initial connection.

Server Discovery

Multiple methods exist for a Network Plug and Play client to identify a Network Plug and Play server. The following sections describe each in detail.

Configuring DHCP for PnP Server Auto-Discovery

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.
- Bx—Server address type:
  - B1 = hostname
  - B2 = IPv4
- Ixxx.xxx.xxx.xxx—IP address or hostname of the server (following a capital letter i). In the example, the IP address is 172.19.45.222.
- Jxxxx—Port number to use to connect to the server. In the example, the port number is 80. The default is port 80 for HTTP and port 443 for HTTPS.
- Kx—Transport protocol to be used between the Cisco Plug and Play IOS Agent and the server:
  - K4 = HTTP (default)
  - K5 = HTTPS
- TtrustpoolBundleURL—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.

Configuring DNS for PnP Server Auto-Discovery

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.

Depending on the client type and software version, up to three names will be queried:

Table 1 Hostnames used for DNS Discovery

Name	Description
pnpserver	The PnP server to be used
pnptrustpool	A separate server for downloading a trustpool bundle. If this name does not exist, then the PnP server is used.
pnpntpserver	The server to use for clock synchronization through NTP. If this name does not exist, then the well-known service pool.ntp.org is used.

Using PnP Connect for PnP Server Auto-Discovery

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 Manager, and then register each of your devices with the Plug and Play Connect Service. 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 100 to 500 series Plug and Play-enabled products will need to be registered manually.

See the *FindIT Network Manager Administration Guide* for detailed instructions on using PnP Connect with FindIT Network Manager.

Troubleshooting

There are many components in a working Network Plug and Play solution, and the failure or misconfiguration of any one can cause a device deployment to fail. The first step in troubleshooting is to determine whether the problem is impacting one device or many, and whether this is the first use of the Manager as a PnP server or whether it has been seen to work successfully previously. Based on the answer to these questions, the troubleshooting process can focus on the Manager if the problem is widespread or this is the first use of the Manager as a PnP server, or the focus can shift to the device if there is a particular device being impacted.

The following sections describe troubleshooting techniques that focus on the Manager and the device in turn. If the problem cannot be resolved using the techniques described here, then the last section details the information that should be gathered prior to logging a support case.

FindIT Network Manager PnP Server Troubleshooting

This section provides some tips and techniques for troubleshooting the PnP server on the Manager.

Verify the Service is Running

To quickly verify that the Network Plug and Play service is operable on the Manager, enter the URL http://<server_name_or_IP>/pnp/hello in to a web browser. If the service is operating correctly, you will receive a simple response similar to the following:

```
Hello from PnP Server, d108ee3 committed at Mon Jan 07 01:49:55 UTC 2019, 2.0.0-SNAPSHOT built at Mon Feb 11 22:33:06 UTC 2019
```

The test should be repeated using HTTPS, and the server name or address used should match that being used for server discovery. This indirectly verifies that necessary infrastructure such as the DNS and routing infrastructure is operating correctly.

Verify the Server Certificate

You may view the certificate in use either through the Manager GUI, or by inspecting the certificate presented by the Manager web service using the web browser tools. However, viewing the certificate through the web browser will also show whether the certificate has been correctly signed by a public Certificate Authority (CA) and that it is otherwise a valid certificate.

Regardless of how the certificate is viewed, the Subject Alternative Name field – also known as Subject-Alt-Name or SAN – should be inspected to verify that it contains the following information:

- The server name specified in the DHCP option or PnP Connect controller profile if the server is identified by name
- The IP address specified in the DHCP option or PnP Connect controller profile if the server is identified by IP address
- The name pnpserver.<domain> if DNS discovery is being used

The validity start and end dates should also be inspected to verify that the certificate is currently valid.

View System Logs

If the PnP service is not running, it may be necessary to check the PnP logs for errors. The PnP logs are also useful for verifying that PnP requests are being received from network devices. Logs for the PnP service may be found at the following location in the file system of the Manager:

```
/var/log/findit/manager/nm-pnp-server.log
```

Note: The log files for the FindIT Network Manager application are owned by the findit user and are not world readable. To access the logs, it will be necessary to use the sudo command to gain escalated privileges.

Note: If the Manager version is 2.0 or later, the log level for the PnP service should be set to Debug. To change log levels, navigate to System > Logging in the Manager user interface. In version 2.0, log files may be directly downloaded from the System > Logging page.

PnP Device Troubleshooting

This section provides some tips and techniques for troubleshooting the PnP client on a network device.

Verify Server Reachability

Ensuring that the Manager is reachable by the device is an obvious troubleshooting step, but in many cases, the server identity used by the PnP client is not the commonly used server identity for the Manager. For example, if DNS discovery is being used, then the Manager needs to be reachable using the name pnpserver.<domain>. The built-in diagnostic tools in the network device should be used to ensure that the Manager is reachable using the same IP or name learned through the PnP server discovery process. The majority of network devices provide at least basic ping, traceroute and name lookup tools, and these will usually be sufficient to verify reachability.

Verify System Clock Accuracy

A network device must have a reasonably accurate knowledge of the current time in order to check the validity of the certificate presented by the server. If the clock is not set correctly, the device may incorrectly identify a valid certificate as being invalid based on the start and end validity dates. Because of this, a PnP client will not validate a certificate unless it has the Network Time Protocol (NTP) enabled and it has successfully synchronized the clock with one or more NTP servers. Certain PnP clients further require that the NTP servers must be learned through the PnP discovery mechanism or be from a well know default such as pool.ntp.org. Consult the network device documentation for more information.

You can visually inspect the current clock setting for the device through the user interface.

Check Device Status in the Manager

If the Manager is reachable and the clock is accurate, then it is likely that a successful connection to the PnP server will be made. If device provisioning is not proceeding correctly, then checking the PnP provisioning status can help identify a problem. Consult the *FindIT Network Manager Administration Guide* for details of how to view the provisioning status and the meaning of each of the possible values.

Check Unclaimed Devices

If the provisioning status for the device registration in the Manager remains in the Pending state, then the Unclaimed Devices page should be checked. An error in the product ID (PID) or serial number is a common reason for a device to fail to provision and in this case, the device will be listed in the Unclaimed Device table.

View Device Logs

The majority of network devices will generate detailed logs for the PnP client, although in some cases, logging may need to be explicitly enabled for each module. Many devices also allow the display of logs to be restricted to specific modules which may help when reviewing the logs. Consult the network device documentations for more details on configuring logging and the selection of appropriate modules to diagnose PnP.

Logging a Support Case

If the above tips and techniques do not provide a resolution to the problem under investigation, a support case should be opened with the Small Business Support Center. For contact details, consult https://www.cisco.com/go/sbsc and call the local access number listed.

Before opening a case, the following information should be gathered:

- Details of the PnP configuration for the device in the Manager
- The product ID and serial number of the device captured from the device user interface. Typically, this information will be found on the Status and Statistics pages in the web UI.
- Details of the DHCP offer presented to device if DHCP is in use. Ideally this should be a packet capture of the transaction, but a copy of the DHCP pool configuration from the DHCP server is generally sufficient.
- PnP service logs from the Manager
- PnP logs from the device

This information should be provided to the engineer who provides support for this case.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco Copyright