# CUWN release 8.2 APIC EM Wireless AP PNP Deployment Guide

**Revised: January 12, 2016,**

# Introduction

The Cisco Network Plug and Play solution provides a simple, secure, unified, and integrated offering for enterprise network customers to ease new branch or campus rollouts, or for provisioning updates to an existing network. The solution provides a unified approach to provision enterprise networks comprised of Cisco routers, switches, and wireless devices with a near zero touch deployment experience.

This deployment guide introduces the Cisco Network Plug and Play application for wireless access points. This application allows you to pre-provision the remote site or claim unplanned access points. When you provision a large site, you can use the Cisco Network Plug and Play application to pre-provision the site and add access points to the site. This includes entering access point information and setting up a bootstrap configuration. The bootstrap configuration enables the Plug and Play Agent to configure the access point primary/secondary/tertiary WLC, hostname, AP group and AP mode.

When you create small sites where pre-provisioning is not required, access points can be deployed without prior set up on the Cisco Network Plug and Play application and then claimed. When an installer installs and powers up the access point, it auto-discovers the Cisco APIC-EM controller by using the DHCP or DNS. After the auto-discovery process is complete, the AP is listed as an unplanned device in the Cisco Network Plug and Play application. You can use the Cisco Network Plug and Play application to claim the unplanned device and configure it with a new configuration.

## Components Used

- APIC-EM minimum release of 1.0.1.30 with Cisco Network Plug and Play, virtually hosted in a Cisco UCS or equivalent server.
- VMWare ESXi 5.x Virtual Machine minimum requirement:

| | | |
|---|---|---|
| Virtual Machine Options | VMware ESXi Version | 5.1/5.5 |
| | Server Image Format | ISO |

| | | |
|---|---|---|
| Hardware Specifications | Virtual CPU (vCPU) | 6 |
| | CPU (speed) | 2.4 GHz |
| | Memory | 64 GB<br>**Note** For a multi-host deployment (2 or 3 hosts) only 32 GB of RAM is required for each host. |
| | Disk Capacity | 500 GB |
| | Disk I/O Speed | 200 MBps |
| | Network Adapter | 1<br>**Note** A single network adapter or network interface controller (NIC) is the minimum requirement. For security, we recommend that you use and configure two NICs on the server. See Security in the Limitations and Restrictions section of these release notes for additional information. |
| Networking | Web Access | Required |
| | Browser | The following browsers are supported when viewing and working with the Cisco APIC-EM:<br>• Google Chrome–version 46.0 or later |

- Cisco Series Wireless LAN Controller with software release 8.x
- 802.11n Access Points with PnP agent in software release 8.2
    - 3700/2700/1700
    - 3600/2600/1600
    - 700i/700w
- Cisco Catalyst Switch
- Client computer (for example laptop) that is Windows or Mac, with an available wired Ethernet port.

# Requirement Overview

Follow these recommendations when deploying the Cisco Network Plug and Play solution:

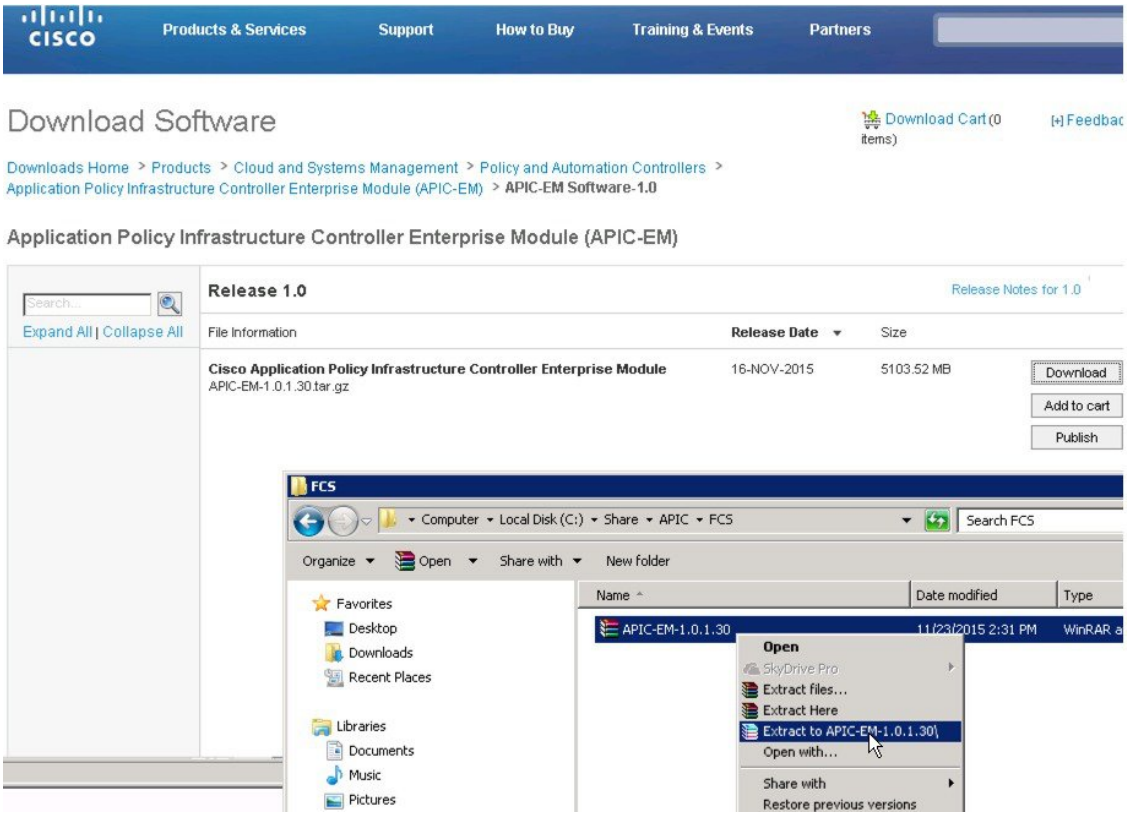
- Install APIC EM Controller VM
- Configure a DHCP server with option 43 to allow Cisco network devices to auto-discover the APIC-EM controller.
- Pre-provision the device configuration in the Cisco Network Plug and Play application for all new devices to be deployed. This includes setting up the site and devices in it with the access point info of serial numbers and bootstrap configuration.
- Device bring up order—In general, routing and upstream devices should be brought up first. Once the router and all upstream devices are up and provisioned, switches and downstream devices can be brought up. The Cisco Network Plug and Play Agent attempts to auto-discover the APIC-EM controller only during initial device startup. If at this time, the device cannot contact the controller, device provisioning fails, so upstream devices should be provisioned first.
- Cisco Router Trunk/Access Port Configuration—Typical branch networks include routers and switches. One or more switches are connected to the WAN router and other endpoints like IP phones and access points connect to the switches. When a switch connects to an upstream router, the following deployment models are supported for Cisco Network Plug and Play:
- Downstream switch is connected to the router using a switched port on the router. In this type of connection, the switched port on the router must be configured as an access port. The Cisco Network Plug and Play solution does not work for the switch if the switched port on the router is configured as a trunk port.

# APIC VM Install

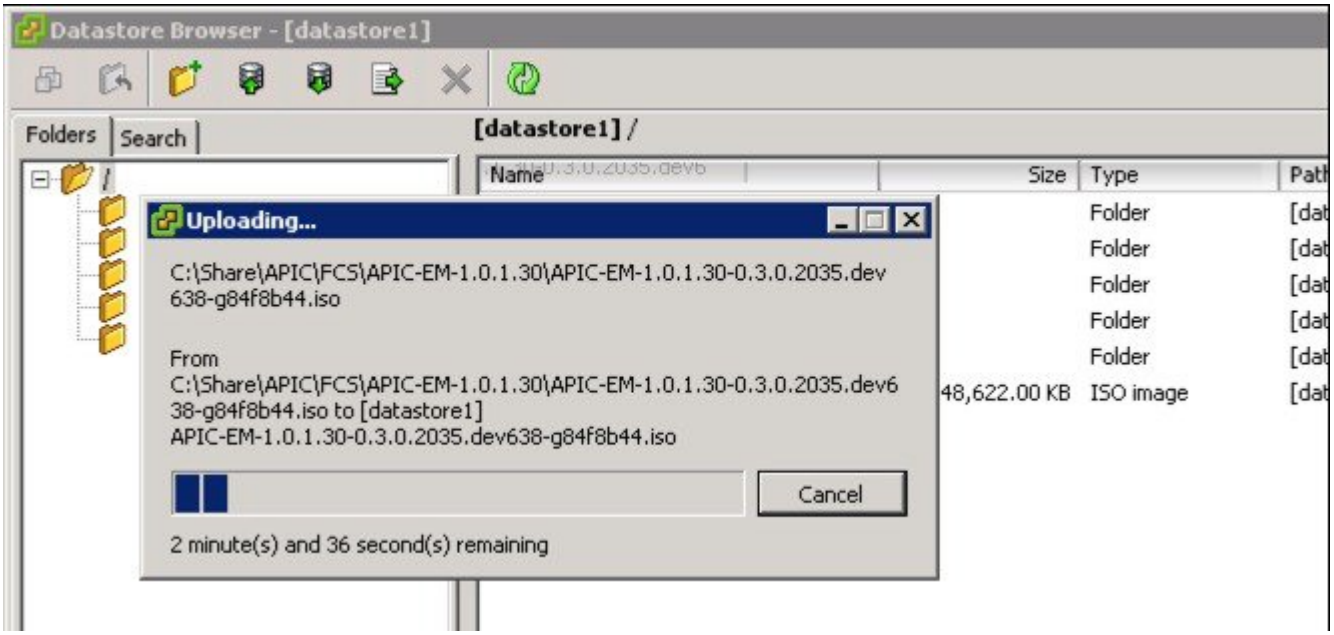
### Procedure

**Step 1** Download the APIC ISO image from Cisco website https://software.cisco.com/download/release.html?mdfid=286208072&flowid=77162&softwareid=286291196&release=1.0&relind=AVAILABLE&rellifecycle=&reltype=latest

**Step 2** Extract the **tar.gz** file to obtain the ISO image of APIC-EM.



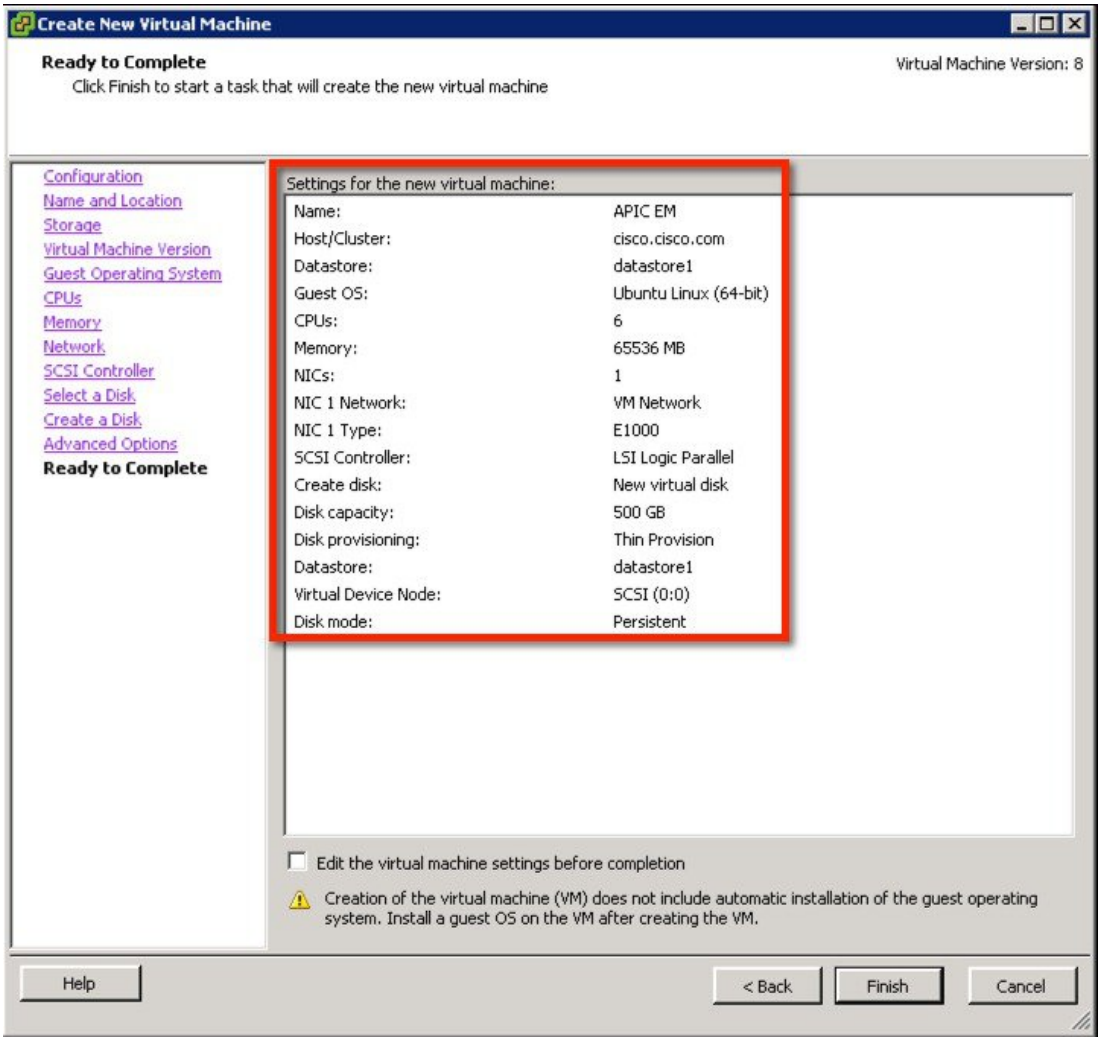

**Step 3** Upload the ISO to the ESXi 5.x server.



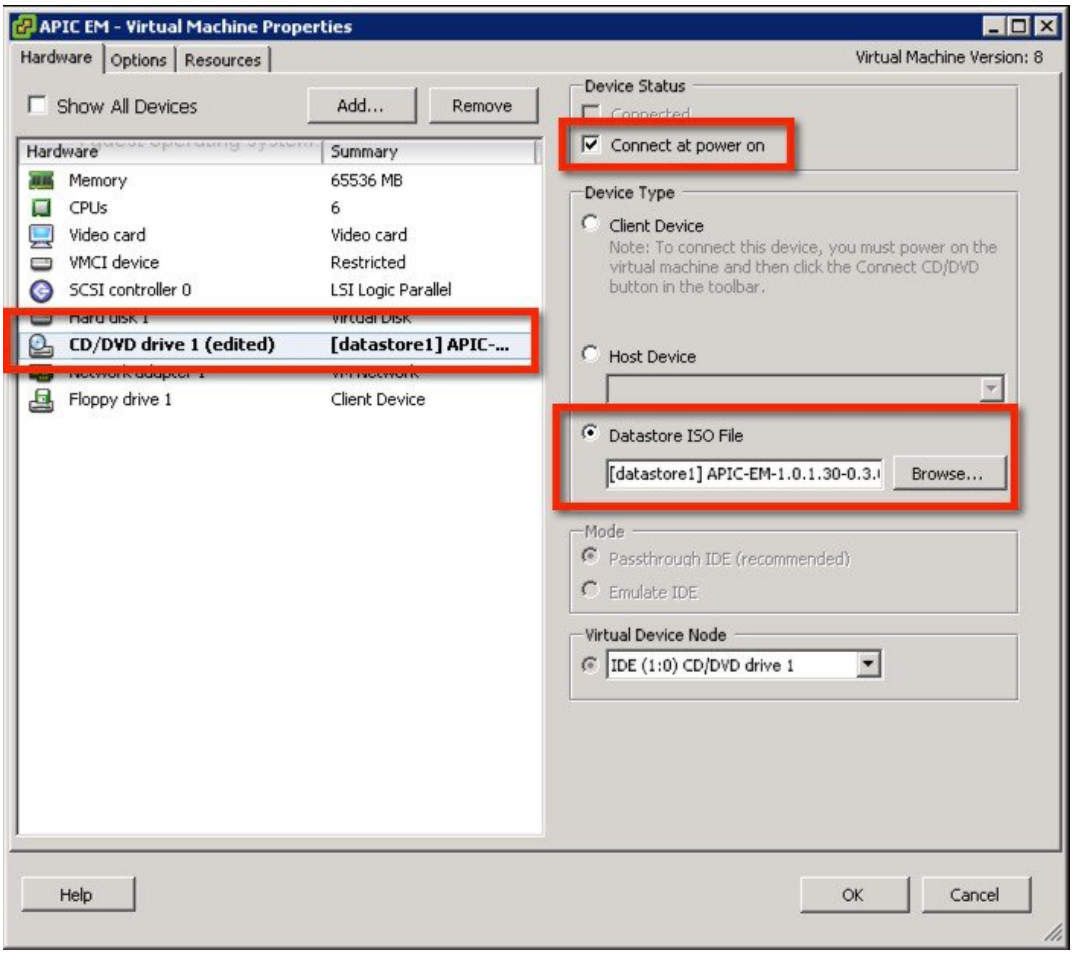
**Step 4** Create a new Virtual Machine with the following custom configuration settings:

- Guest OS: Ubuntu Linux 64bit
- CPU Cores: 6
- RAM: 64 GB
- NIC: 1
- Storage: 500 GB

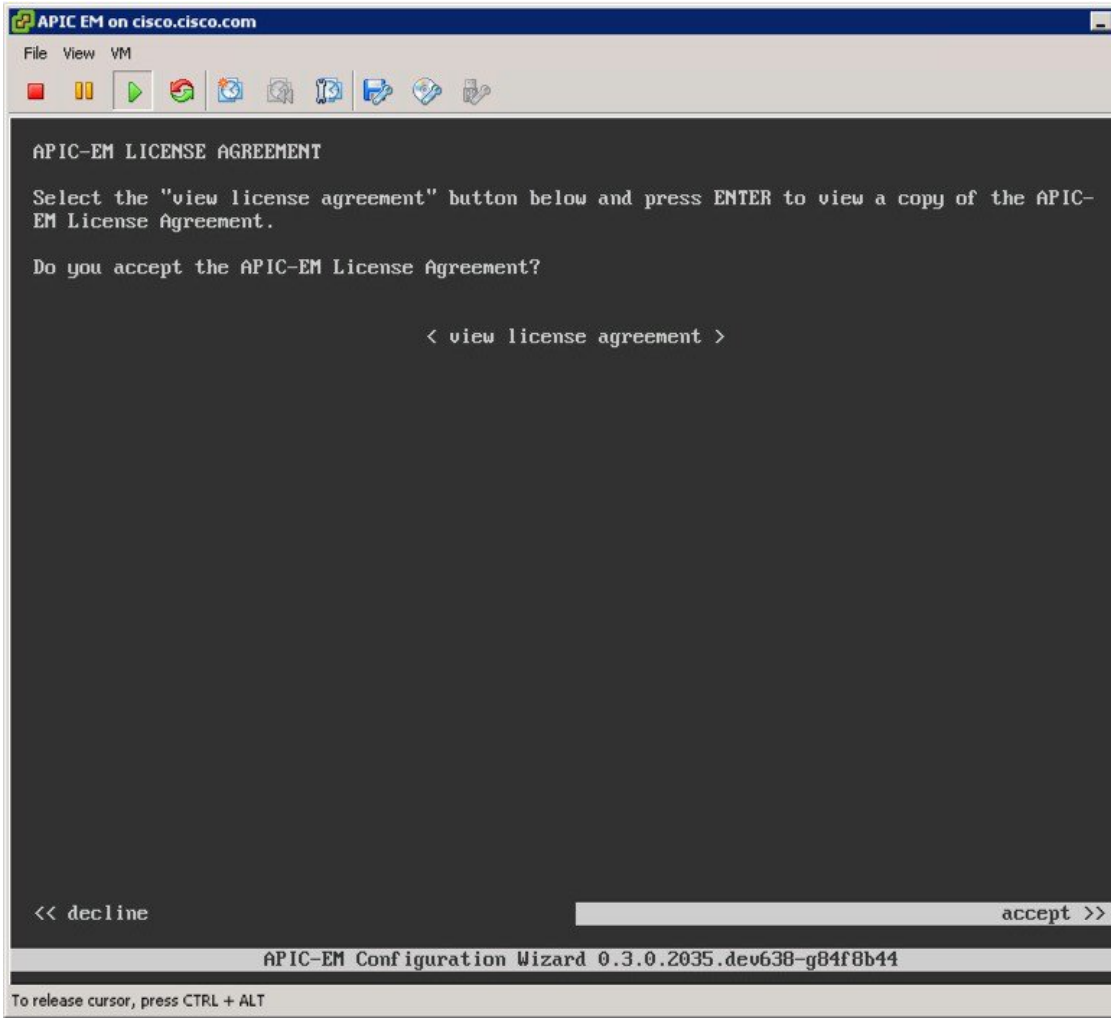
**Note** Check release notes for latest support and requirement of APIC EM.



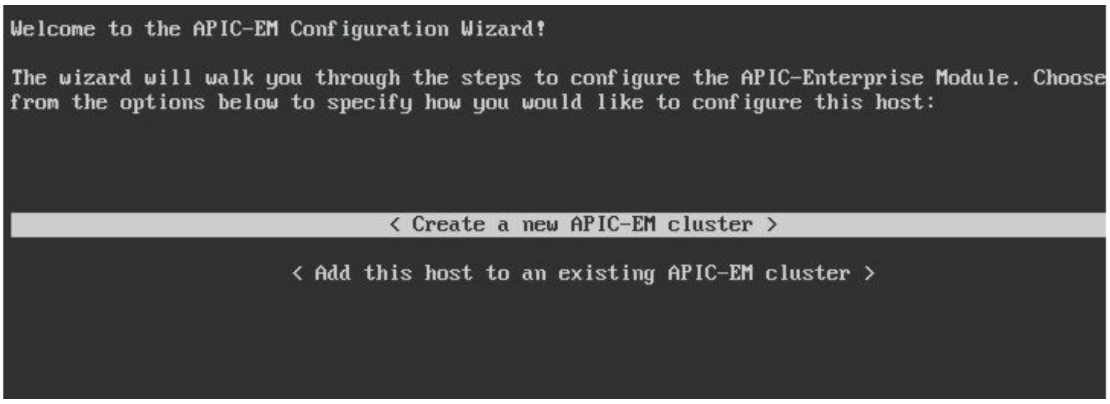

**Step 5** Mount the ISO in the CD/DVD; then, power up the VM.



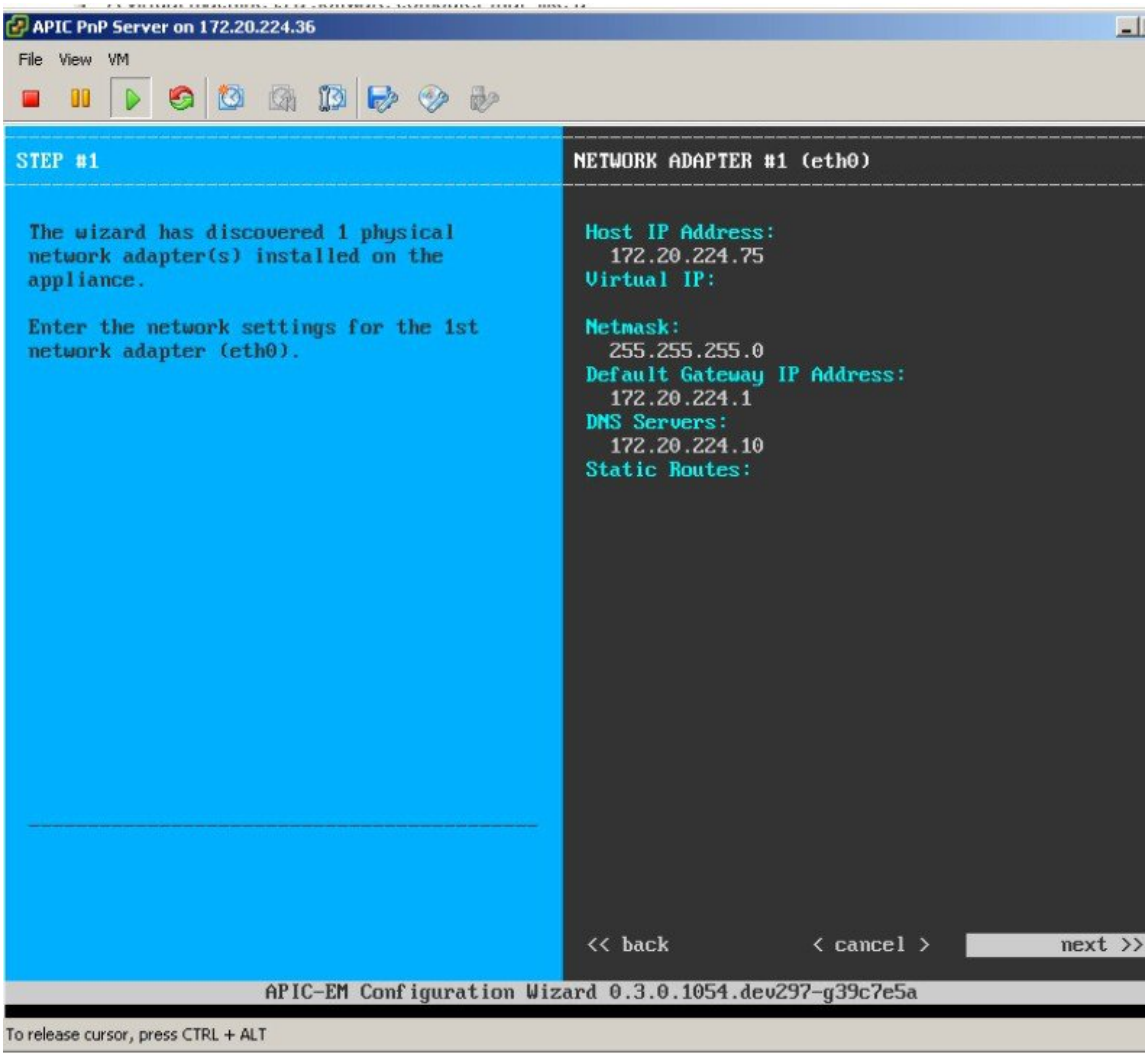

Allow the installation to complete, the VM will reboot as required. Once completed, the APIC-EM License Agreement will prompt to accept and continue (use keyboard to input and navigate).



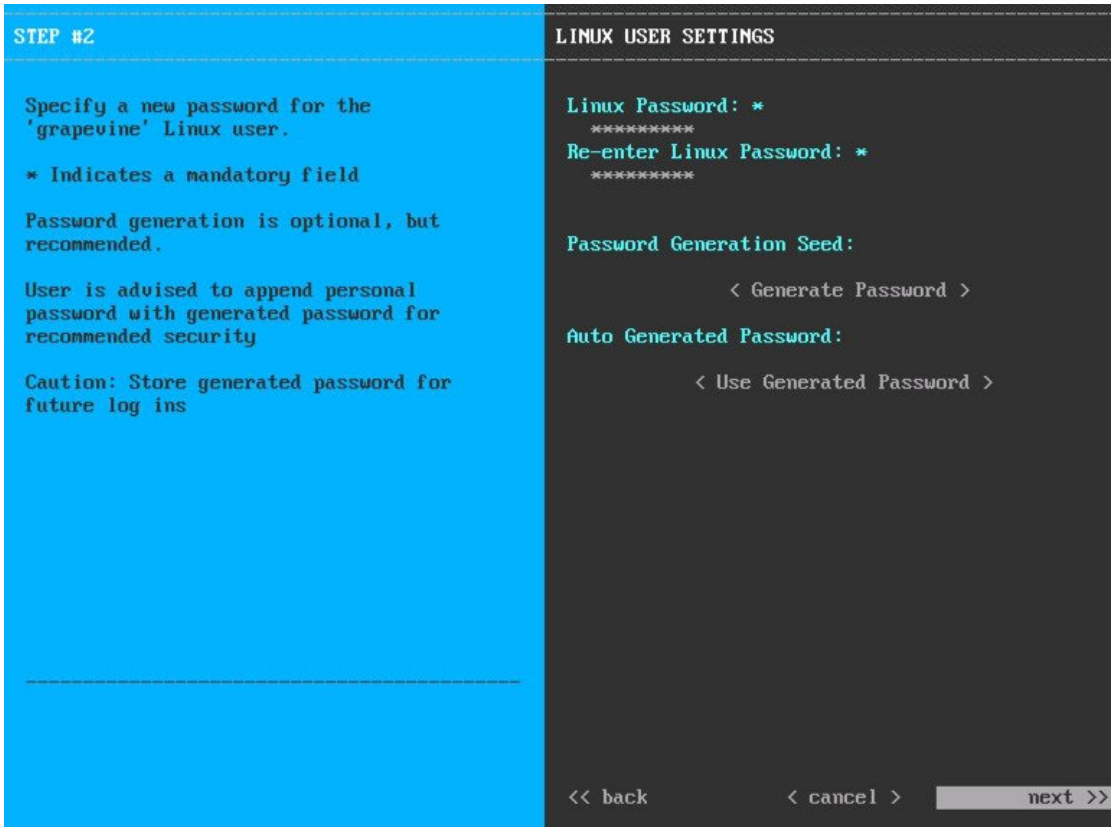

**Step 6** Select 'Create a new APIC-EM cluster'.



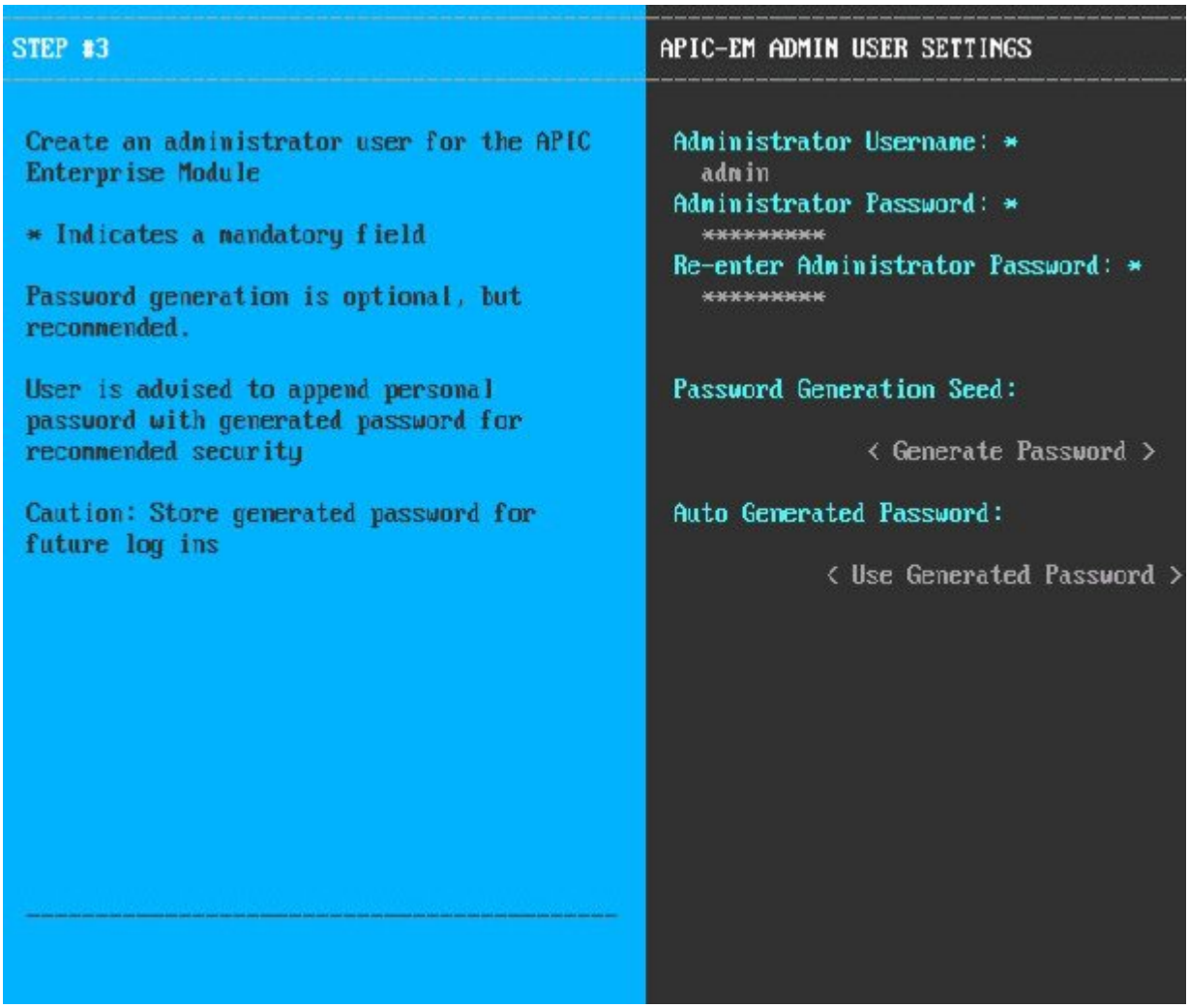

**Step 7** Enter management IP, network mask and gateway.



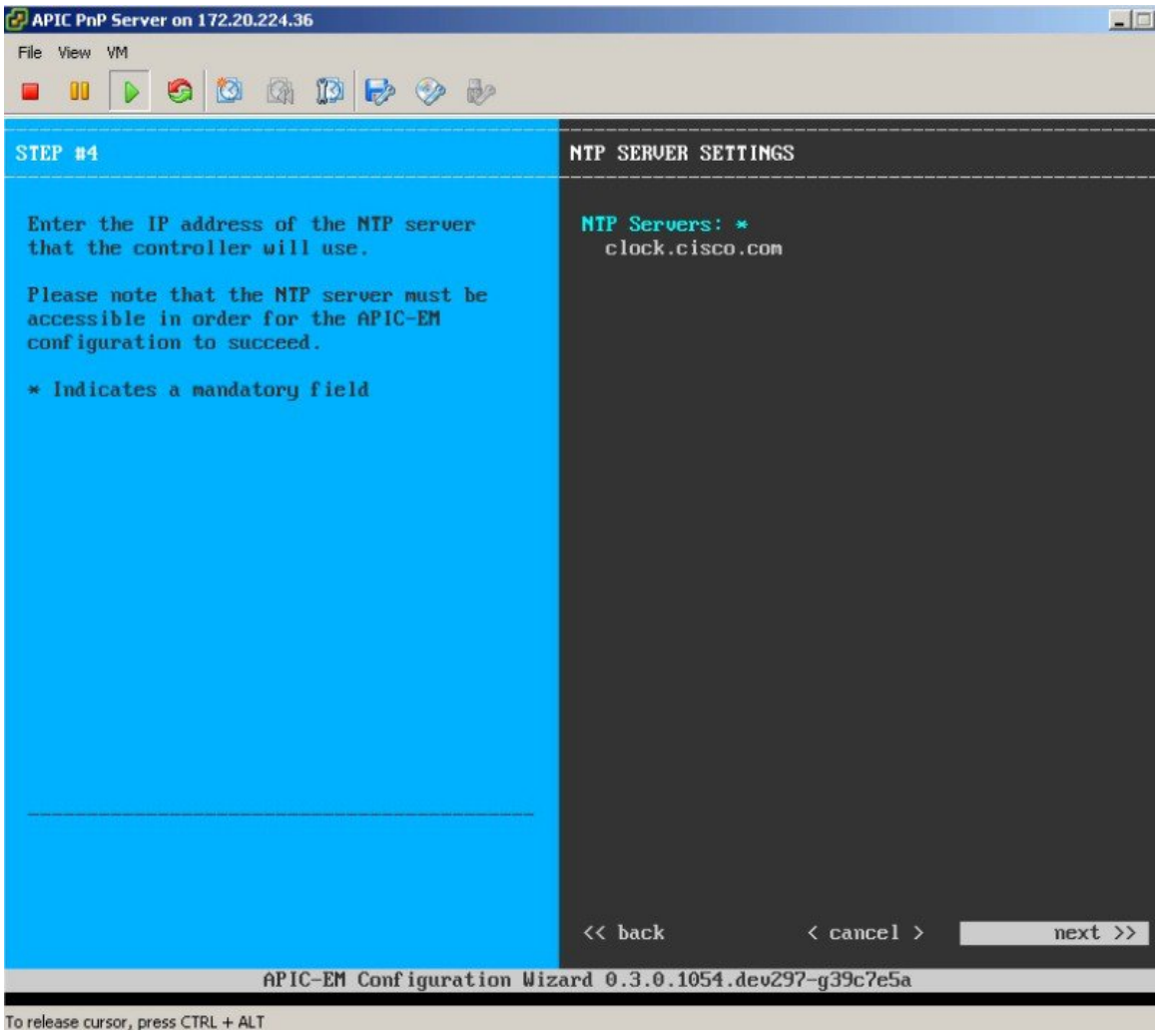

**Step 8** Enter the Linux credentials to access SSH/console of APIC-EM.



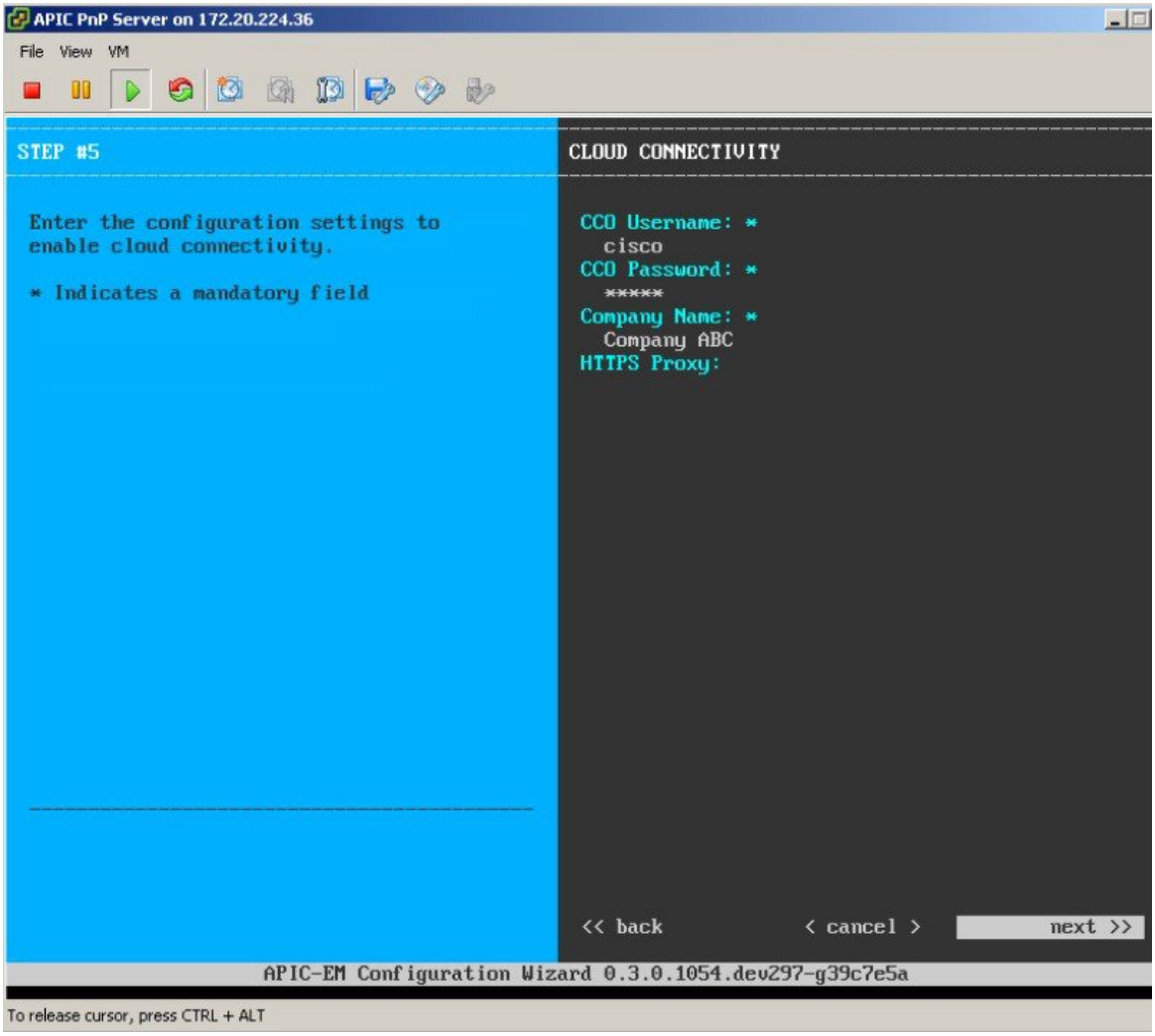

**Step 9** Enter the admin credentials to access the web application of APIC-EM.



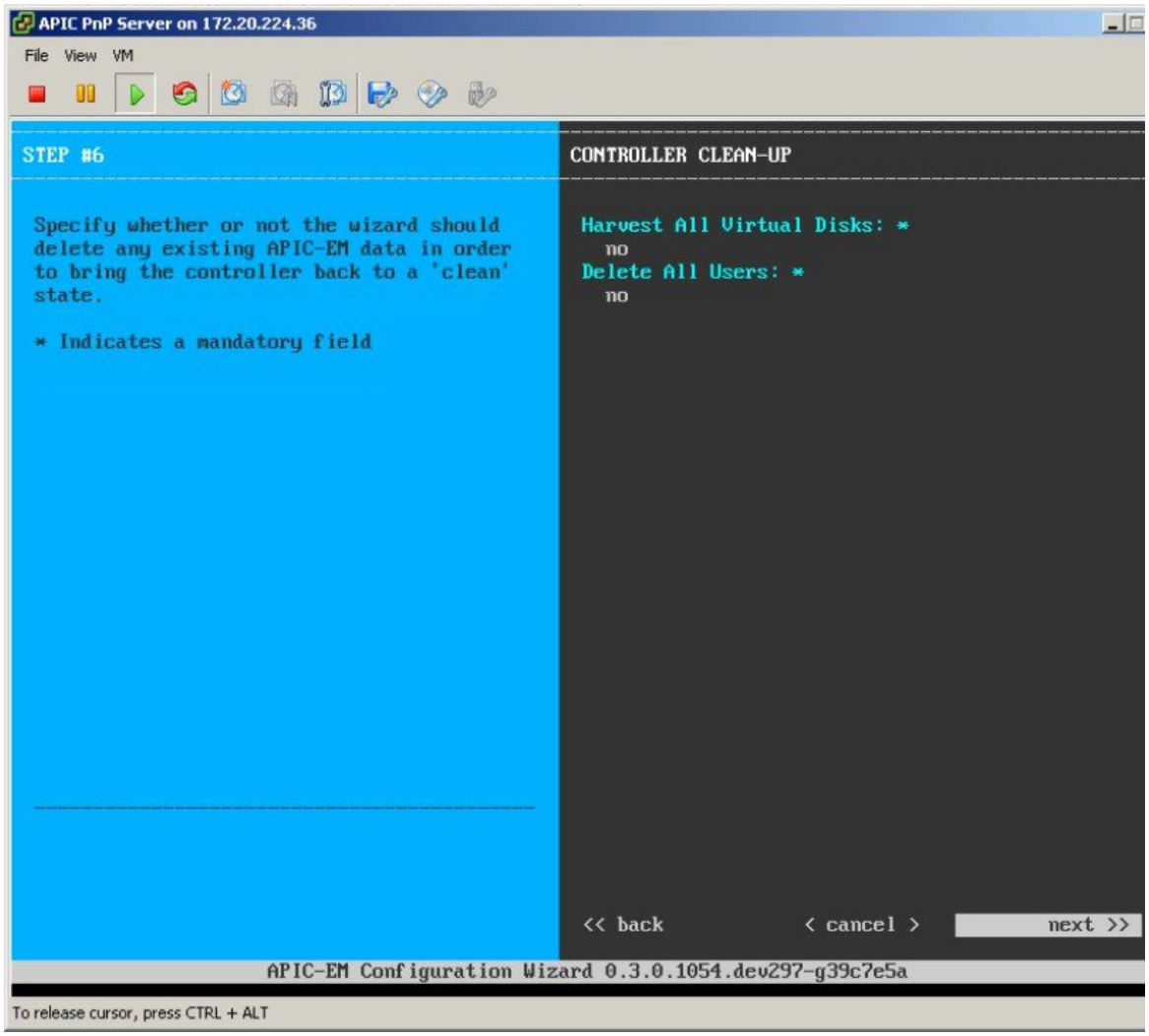

**Step 10** Enter the required or valid NTP server IP address.



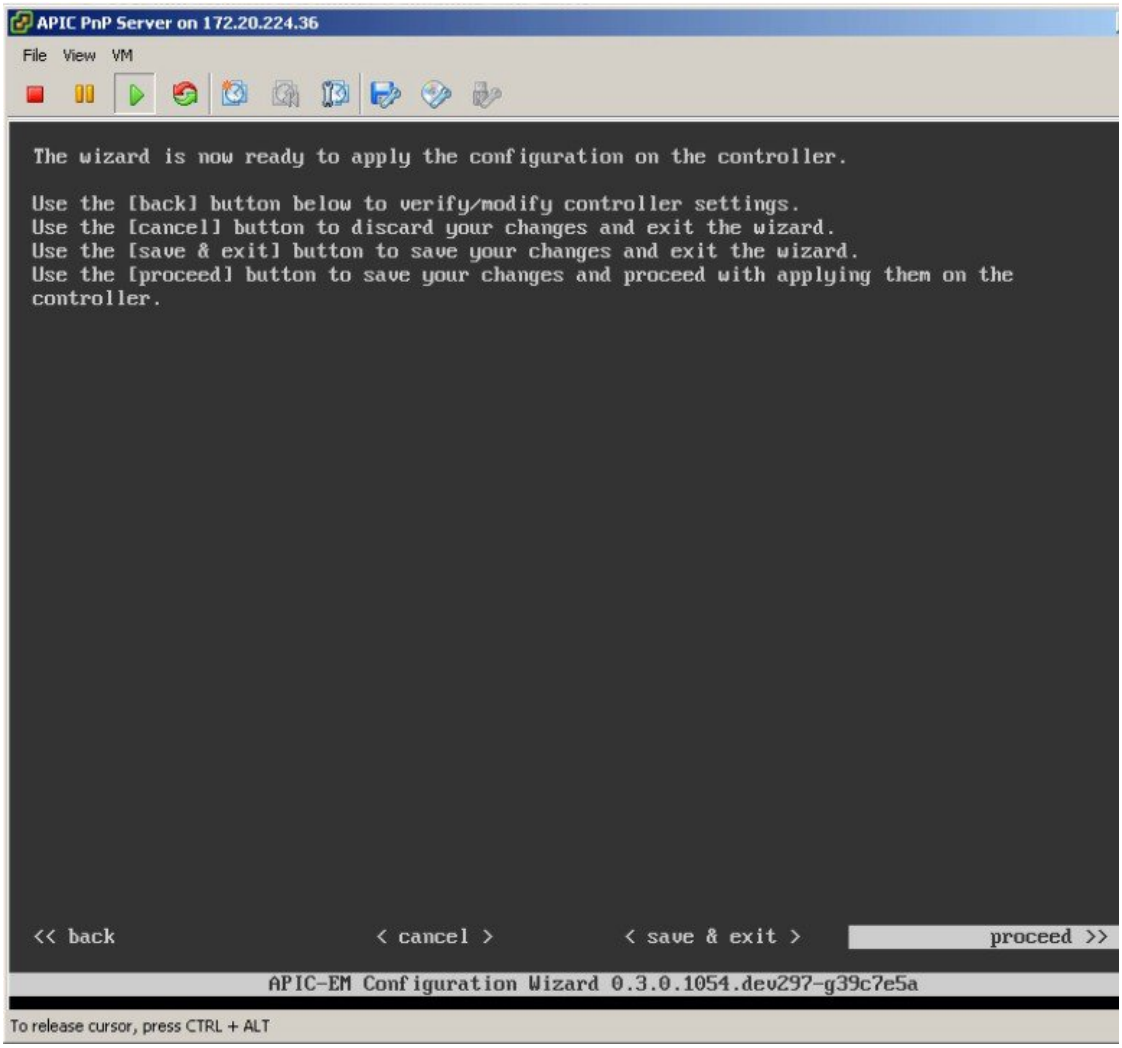

**Step 11** Enter the credentials.




**Step 12** Leave all the defaults.

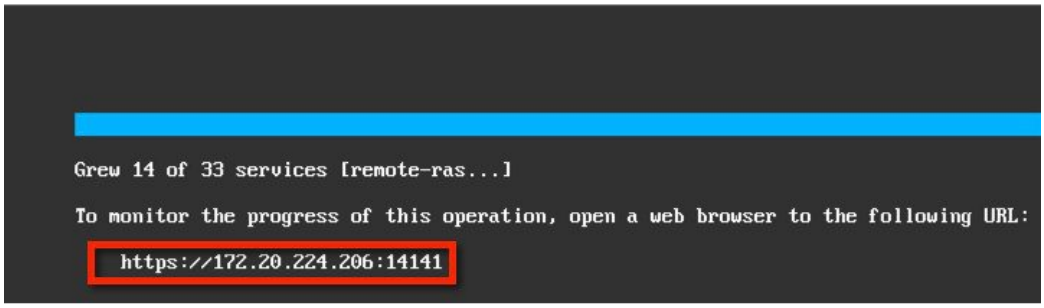



**Step 13** Select Proceed to apply the configuration.

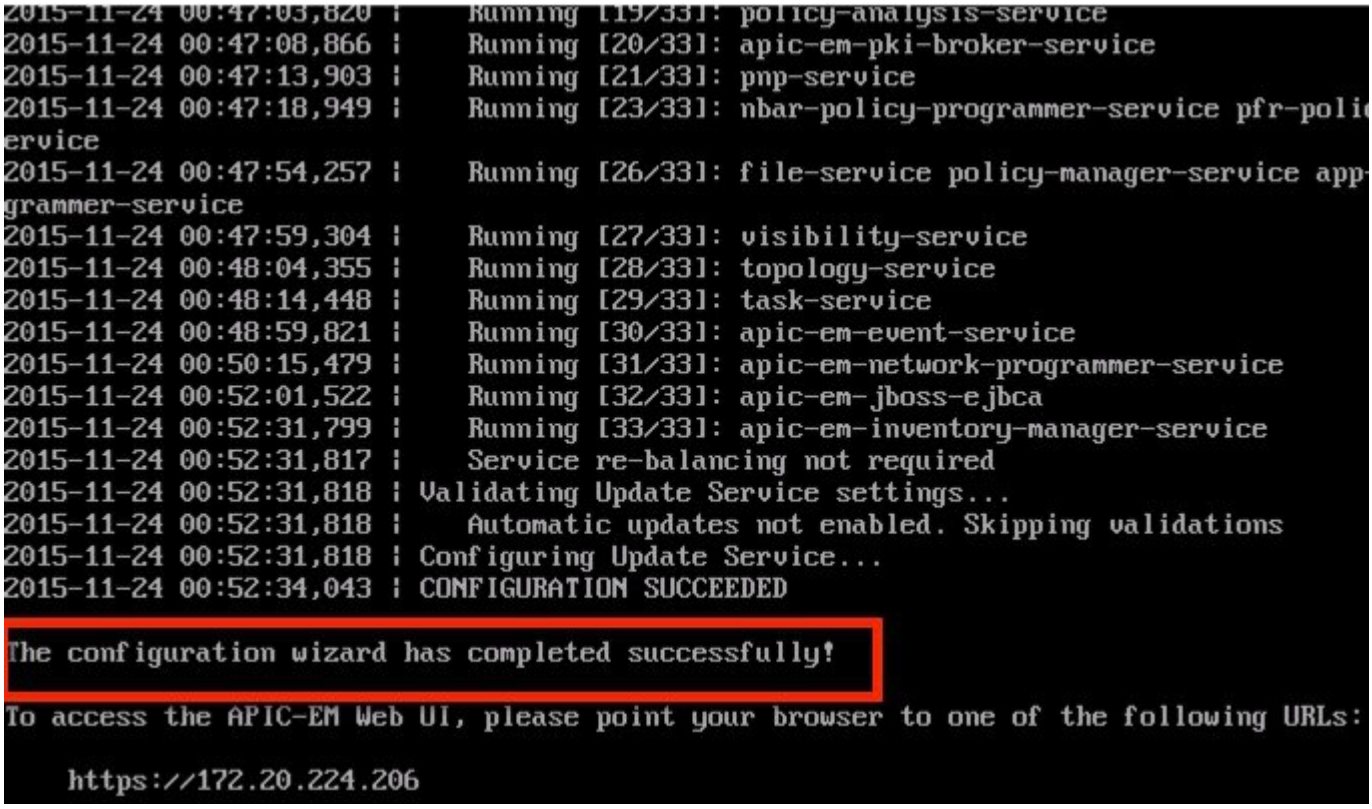



**Step 14** APIC-EM proceeds with installation, and it take a time duration of 15-30 minutes. It provides an URL to monitor the progress at HTTPS://MGT-IP-ADDRESS:14141

**Note** Port
14141

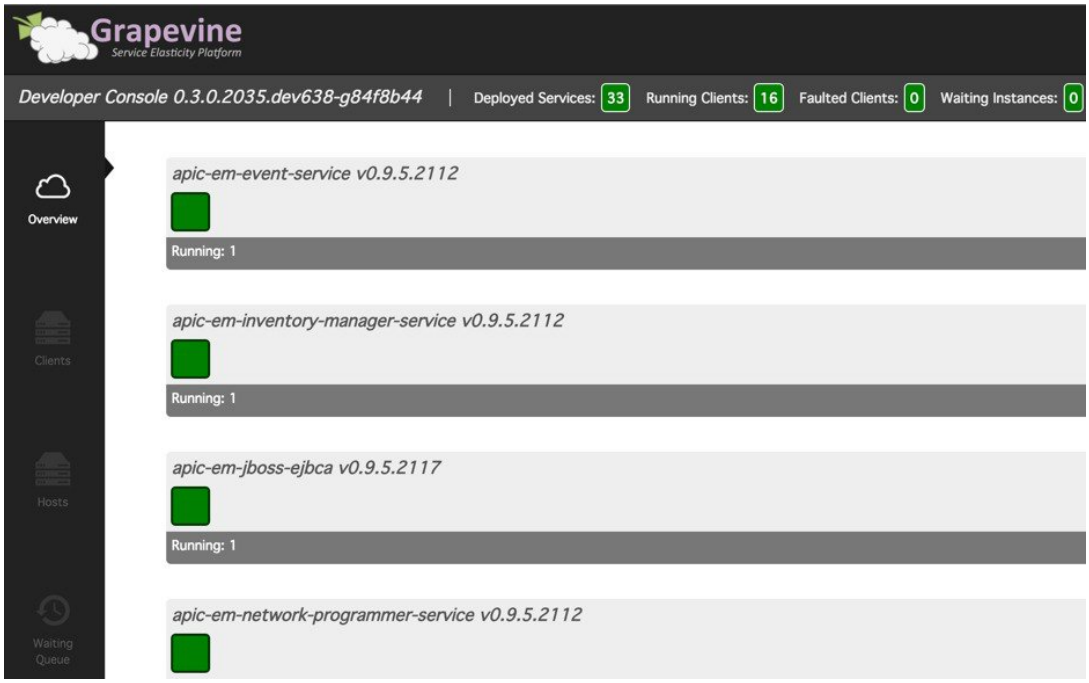



The console will also provide configuration wizard status.




**Step 15** The previous link allows to monitor services being installed or started. Log in using the admin credentials provided in the installation


In the console dashboard, when deployed services and running clients are **all showing green**, it is then ready to be used for testing.




**Step 16** When configuration is successful, log in to the management application (link: HTTPS://MGT-IP-ADDRESS) (no additional port added). Use the same admin credentials that have been created already.

## DHCP Requirement

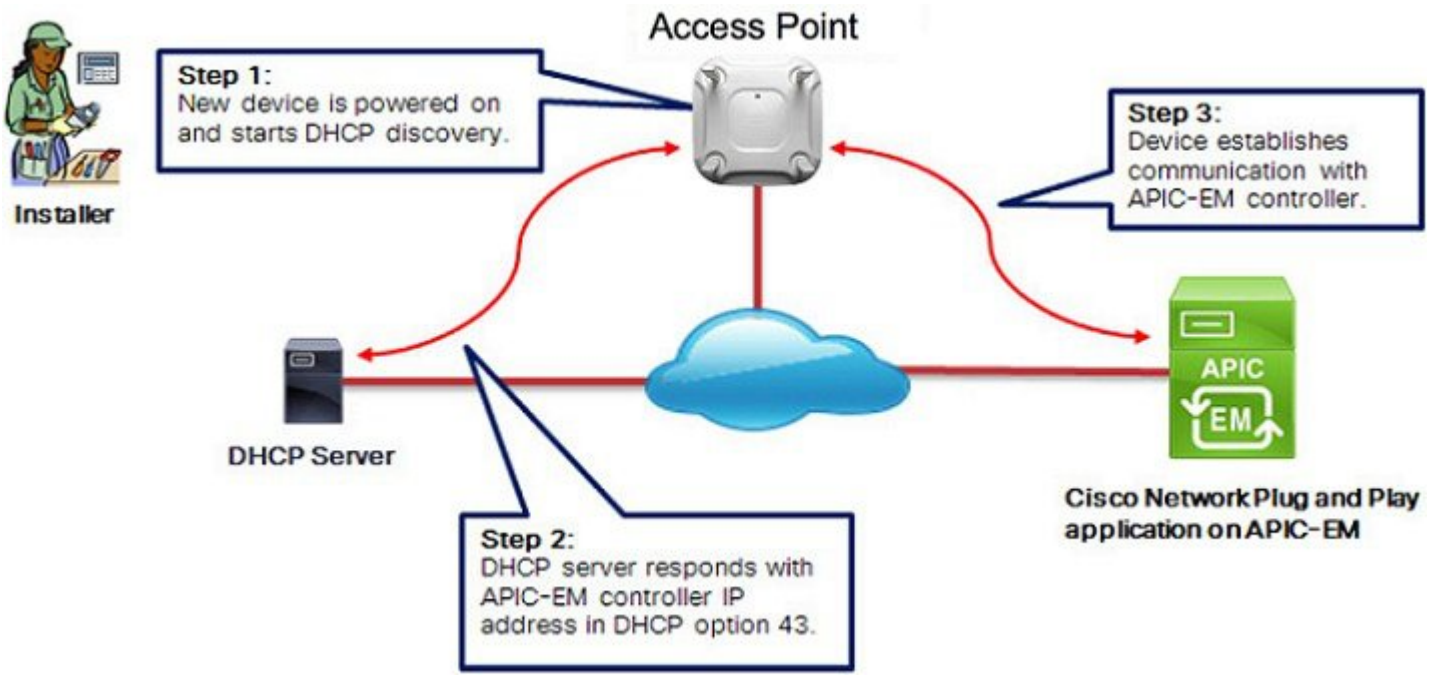
The prerequisites for the DHCP auto-discovery method are as follows:

- New devices can reach the DHCP server.
- The DHCP server is configured with option 43 for Cisco Network Plug and Play.

DHCP option 43 consists of a string value that is configured as follows on a Cisco router CLI that is acting as a DHCP server:

| | |
|---|---|
| ip dhcp pool pnp_device_pool | Name of DHCP pool |
| network 192.168.1.0 255.255.255.0 | Range of IP addresses assigned to clients |
| default-router 192.168.1.1 | Gateway address |
| option 43 ascii "5A1N;B2;K4;I<ipAddress>;J80" | **IPv4 address to APIC EM Server, access points will be directed to this pointer. |

** Option 43 string, copy/paste include quotes, insert your APIC management IP address here.



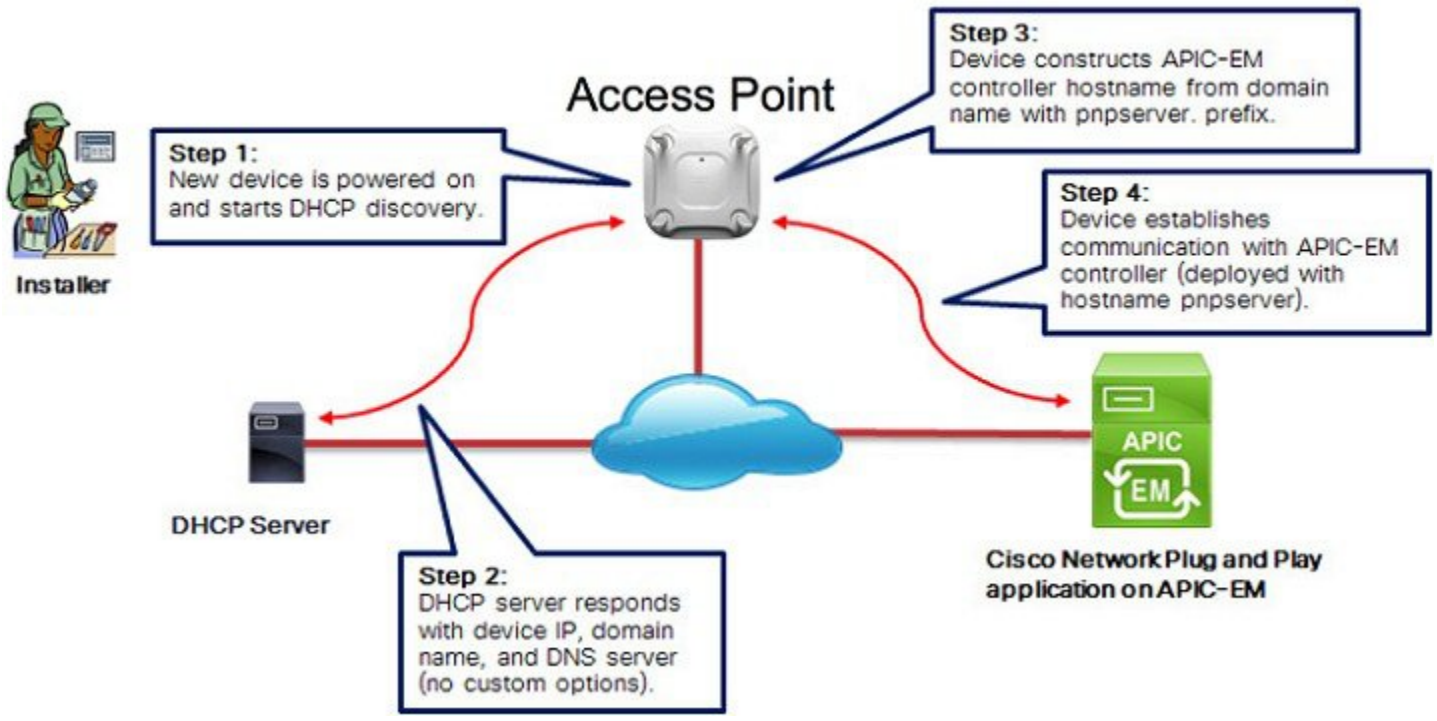
## DNS Requirement

If DHCP discovery fails to get the IP address of the APIC-EM controller, for example, because option 43 is not configured, the Cisco Plug and Play IOS Agent falls back on a DNS lookup method. Based on the network domain name returned by the DHCP server, it constructs a Fully Qualified Domain Name (FQDN) for the APIC-EM controller, using the preset hostname **pnpserver**.

For example, if the DHCP server returns the domain name " ***customer.com*** ", the Cisco Plug and Play IOS Agent constructs the FQDN "**pnpserver.*customer.com*** ". It then uses the local name server to resolve the IP address for this FQDN.

The prerequisites for the DNS auto-discovery method are as follows:

- New devices can reach the DHCP server
- The APIC-EM controller is deployed with the hostname “pnpserver”




## AP PnP Agent Requirement

Cisco CAPWAP access points with software release 8.2 provides the necessary recovery image to support PnP. An example output from the console of a NEW AP during boot up will show the following:

```
*Mar  1 00:00:13.027: %LWAPP-3-CLIENTERRORLOG: Load nvram:/lwapp_ap.cfg config failed,trying backup...
*Mar  1 00:00:13.027: %LWAPP-3-CLIENTERRORLOG: Load nvram:/lwapp_ap.cfg.bak config failed...
*Mar  1 00:00:15.035: %LINK-6-UPDOWN: Interface GigabitEthernet0, changed state to up
*Mar  1 00:00:15.107: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C3700 Software (AP3G2-RCVK9W8-M), Experimental Version 15.3(20150923:181842)[pkpanda 173]
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 23-Sep-15 11:21 by pkpanda
*Mar  1 00:00:15.107: %SNMP-5-COLDSTART: SNMP agent on host APfc5b.395a.b56c is undergoing a cold start
```

```
*Mar  1 00:00:15.191: %LWAPP-3-CLIENTERRORLOG: NumOfSlots Mismatch Reinit all Radios config rcb:0 Cfg:2
*Mar  1 00:00:15.359: %SSH-5-ENABLED: SSH 2.0 has been enabledlwapp_crypto_init: MIC Present
      and Parsed Successfully
*Mar  1 00:00:16.151: %LINEPROTO-5-UPDOWN: Line protocol on Interface BVI1, changed state to up
*Mar  1 00:00:20.003: DPAA Initialization Complete
*Mar  1 00:00:20.003: %SYS-3-HARIKARI: Process DPAA INIT top-level routine exited
*Mar  1 00:00:21.003: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0, changed state to up
*Mar  1 00:00:23.003: %LINK-6-UPDOWN: Interface BVI1, changed state to down
*Mar  1 00:00:24.003: %LINEPROTO-5-UPDOWN: Line protocol on Interface BVI1, changed state to down
*Mar  1 00:00:27.151: %LINK-6-UPDOWN: Interface BVI1, changed state to up
*Mar  1 00:00:28.151: %LINEPROTO-5-UPDOWN: Line protocol on Interface BVI1, changed state to up
*Mar  1 00:00:28.223: %PNPA-DHCP Op-43 Msg: Process state = READY
*Mar  1 00:00:28.223: %PNPA-DHCP Op-43 Msg: OK to process message
*Mar  1 00:00:28.223: XML-UPDOWN: PNPA_DHCP_OP43 XML Interface(102) UP. PID=47
*Mar  1 00:00:28.223: %PNPA-DHCP Op-43 Msg: _pdoon.1.ntf.don=47
*Mar  1 00:00:28.223: %DHCP-6-ADDRESS_ASSIGN: Interface BVI1 assigned DHCP address 10.10.50.248,
      mask 255.255.255.0, hostname APfc5b.395a.b56c
*Mar  1 00:00:28.223: %PNPA-DHCP Op-43 Msg: _pdoop.1.org=[A1D;B2;K4;I192.168.1.123;J80;]
*Mar  1 00:00:28.223: %PNPA-DHCP Op-43 Msg: _pdgfa.1.inp=[B2;K4;I192.168.1.123;J80;]
*Mar  1 00:00:28.223: %PNPA-DHCP Op-43 Msg: _pdgfa.1.B2.s12=[ ipv4 ]
*Mar  1 00:00:28.223: %PNPA-DHCP Op-43 Msg: _pdgfa.1.K4.http=[ transport http ]
*Mar  1 00:00:28.223: %PNPA-DHCP Op-43 Msg: _pdgfa.1.Ix.srv.ip.rm=[ 192.168.1.123 ]
*Mar  1 00:00:28.223: %PNPA-DHCP Op-43 Msg: _pdgfa.1.Jx.srv.rt.rm=[ port 80 ]
*Mar  1 00:00:28.223: %PNPA-DHCP Op-43 Msg: _pdoop.1.ztp=[pnp-zero-touch] host=[] ipad=[192.168.1.123]
      port=80
*Mar  1 00:00:28.223: %PNPA-DHCP Op-43 Msg: _pors.done=1
*Mar  1 00:00:28.223: %PNPA-DHCP Op-43 Msg: _pdokp.1.kil=[PNPA_DHCP_OP43] pid=47 idn=[BVI1]
*Mar  1 00:00:28.223: XML-UPDOWN: BVI1 XML Interface(102) SHUTDOWN(101). PID=47
*Mar  1 00:00:29.155: %PNPA-DHCP Op-43 Msg: _pdoon.2.ina=[BVI1]
*Mar  1 00:00:29.155: %PNPA-DHCP Op-43 Msg: _papdo.2.cot=[5A1D;B2;K4;I192.168.1.123;J80;]
      lot=[5A1D;B2;K4;I192.168.1.123;J80;]
*Mar  1 00:00:29.155: %PNPA-DHCP Op-43 Msg: Process state = READY
*Mar  1 00:00:29.155: %PNPA-DHCP Op-43 Msg: OK to process message
*Mar  1 00:00:29.155: XML-UPDOWN: PNPA_DHCP_OP43 XML Interface(102) UP. PID=34
*Mar  1 00:00:29.155: %PNPA-DHCP Op-43 Msg: _pdoon.2.ntf.don=34
```

*Mar 1 00:00:34.039: No Config Present. PNP required <— This indicates PNP process will initiate since no configuration is present.

Example that AP config is present (PNP will not start):

*Mar 1 00:00:34.043: Config Present. PNP Not required

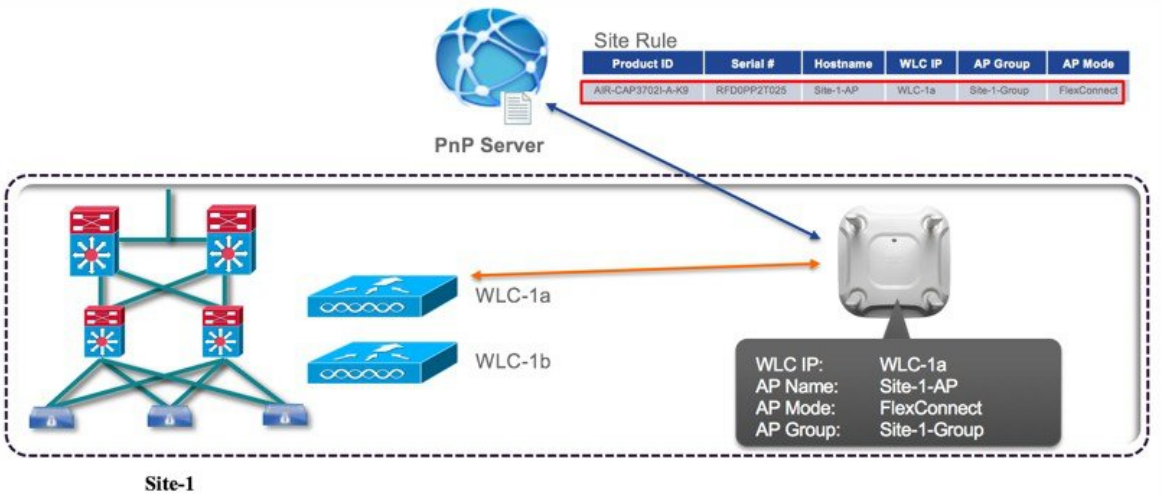
To check if AP has configuration perform the following command on the AP console:

```
AP#show capwap client rcb
AdminState :ADMIN_ENABLED
SwVer :8.2.4.4
NumFilledSlots :2
Name :APfc5b.395a.b56c
Location :default location
MwarName :<— There is no WLC name
MwarMacAddr :ff01.0000.0000
MwarHwVer :0.0.0.0<—There is no WLC IP Address
ApMode :Local
ApSubMode :Not Configured
OperationState :DISCOVERY
```

# Feature Configuration Step-by-Step

## Site Pre-Provisioning Workflow

Cisco Network Plug and Play allows you to pre-provision and plan for new sites. When you create a new site, Cisco Network Plug and Play enables you to pre-provision the access point(s) configuration file, product serial # and product ID for the selected platform. This simplifies and accelerates the time that it takes to get a site fully functional.




To pre-provision a site on your network, perform these steps:

**Procedure**

**Step 1** Create a new site.

**Step 2** Add the device to the site.

## Creating a Site or Project

To create a site, perform these steps:

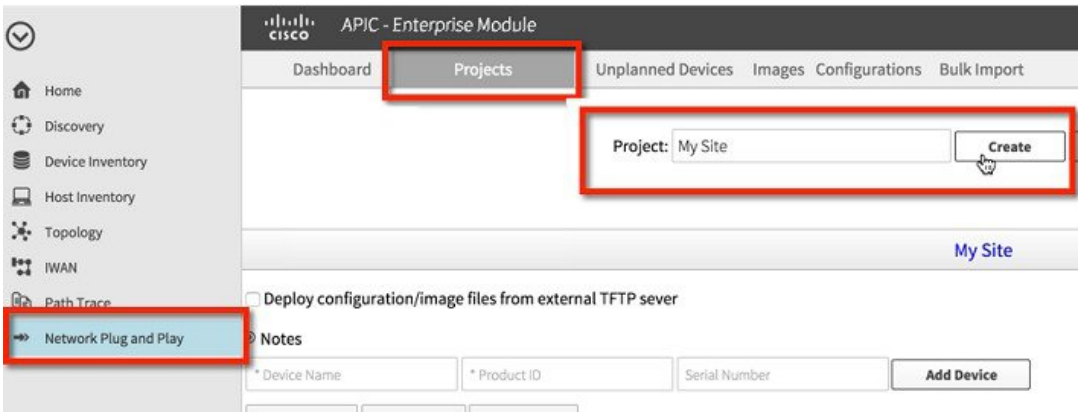
**Procedure**

**Step 1** Choose Network Plug and Play > **Projects**.

**Step 2** Enter the name for the new site.

**Step 3** Click Create to create the new site.

**Step 4** After creating the site, select the configuration file device table.




## Adding a Device

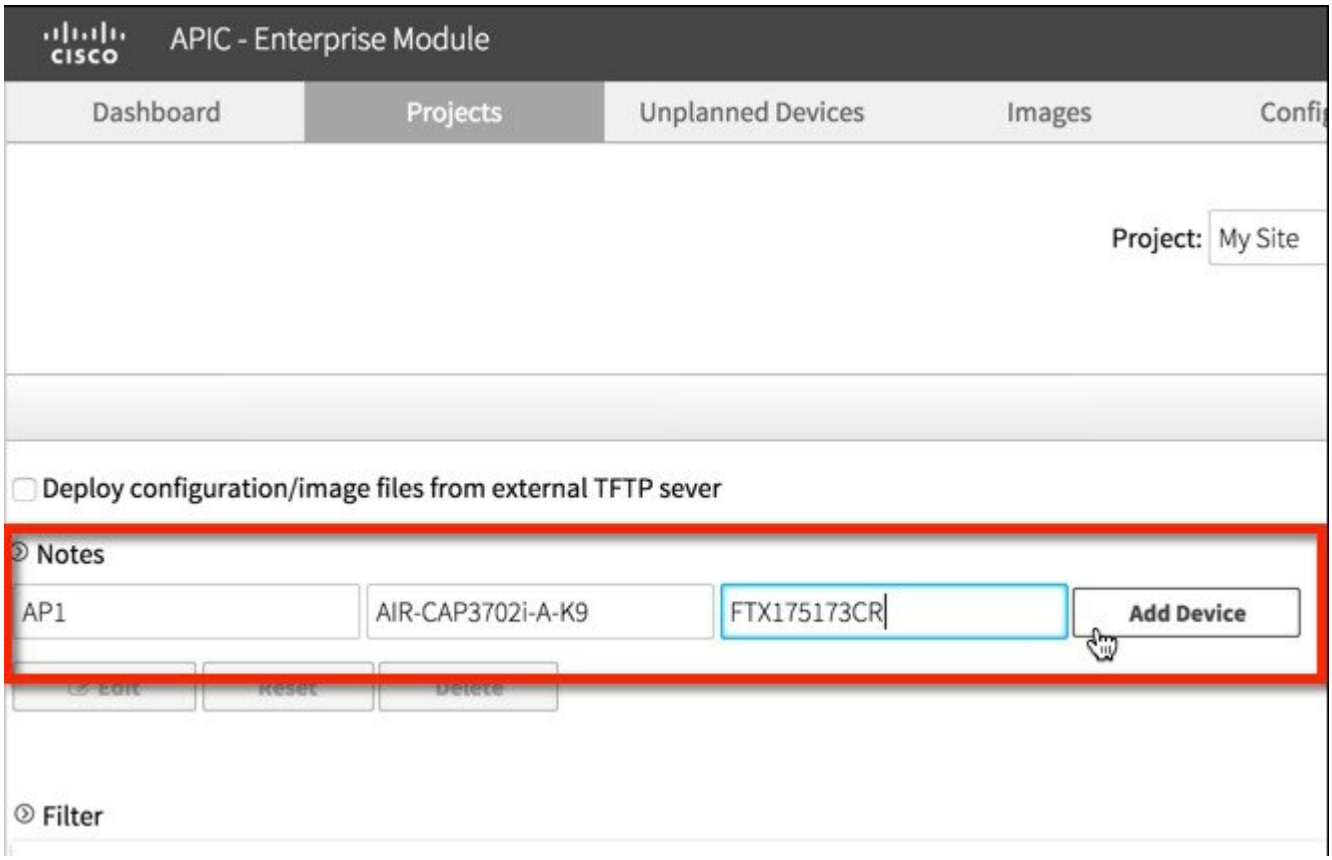
To add a device, perform these steps:

### Procedure

**Step 1** Choose **Network Plug and Play > Sites**.

**Step 2** Enter the following information:

| | |
|---|---|
| Device Name | Device name (unique for each site) |
| Product ID | Select the device product identification number from the drop-down list |
| Serial Number | Device serial number, or Mac Address (applicable only for access points) |




**Step 3** Click Add Device to add the device.

**Step 4** Apply the new configuration to the device or you can reuse the existing configuration from the list.
The configuration file contains the following 8 fields (only primary WLC IP field is mandatory field, all fields are NOT case-sensitive):

| | |
|---|---|
| apGroup | AP Group (optional, when defined APs will be placed in this group, if left blank APs will be placed in the default AP Group) |
| primaryWlcIP | Primary WLC IP address (this is a mandatory field) |
| primaryWlcName | Primary WLC Name (optional) |
| secondaryWlcIP | Secondary WLC IP address (optional) |
| secondaryWlcName | Secondary WLC Name (optional) |
| tertiaryWlcIP | Tertiary WLC IP address (optional) |
| tertiaryWlcName | Tertiary WLC Name (optional) |
| apMode | AP Mode (optional, either ‘local’ or ‘flexconnect’) |

Example of AP Configuration Text File for **Local** Mode

```
{"apGroup":"BldgA-local","primaryWlcIP":"10.10.80.5","primaryWlcName":"5508-
1","secondaryWlcIP":"10.10.80.6","secondaryWlcName":"5508-
2","tertiaryWlcIP":"10.10.10.7","tertiaryWlcName":"8500-1","apMode":"local"}
```

Example of AP Configuration Text File for **FlexConnect** Mode

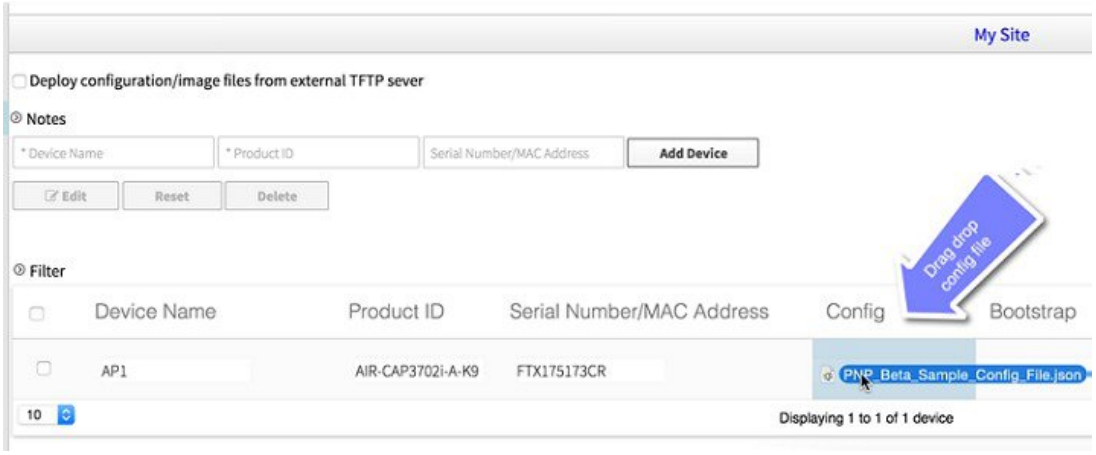
```
{"apGroup":"BldgA-local","primaryWlcIP":"10.10.80.5","primaryWlcName":"5508-
1","secondaryWlcIP":"10.10.80.6","secondaryWlcName":"5508-
2","tertiaryWlcIP":"10.10.10.7","tertiaryWlcName":"8500-1","apMode":" flexconnect"}
```

Example of AP Configuration Text File using only **MANDATORY** field (primary WLC IP)

```
{"primaryWlcIP":"10.10.10.7"}
```

**Note** The configuration file should be in text format with file extension ***.json**. Edit the configuration file(s) as needed and save it as ***.json**.

You can also drag and drop the configuration file to this screen.




## Uploading the Configuration File

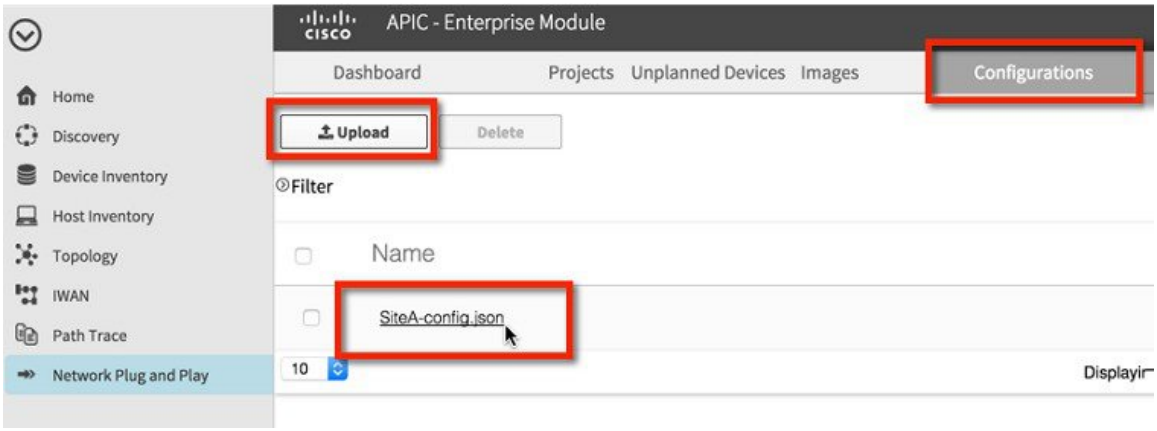
This option allows you to upload the configuration file from your local machine and supports only text format in ***.json** extension.

To upload the configuration file, perform these steps:

### Procedure

**Step 1** Choose **Network Plug and Play > Configuration**.

**Step 2** Click **Upload** and browse to the location where you saved the configuration file. Select the configuration file, and click **Open** to upload the file.




**Step 3** To view the content of the uploaded configuration file, click on the configuration file. This displays the content of the selected file.

**Step 4** You cannot delete the configuration file that is being used in any device. To delete the configuration file from the list, select the configuration file and click Delete.

a) To apply the existing configuration to the device, select the configuration file from the list. Configuration files can be uploaded to 'Configurations' in advanced.

b) To apply a new configuration to the device, you should upload the configuration file to the server, and then select the configuration file from the list. Or, as shown earlier, you can click-drag a new file to the Config field.

## Deploying Devices

After creating the site, you can initiate the provisioning process in the remote site. You should install the device and connect the power cables (or use PoE). Turn on the device, and use the Cisco Plug and Play agent to deploy devices and deliver the bootstrap configuration to the device.

**Note** When DHCP or DNS is configured in the network for automatically discovering the Cisco APIC-EM, devices can automatically discover the Cisco APIC-EM and download full configurations, when the power is turned on.

## Claiming the Device

The device is added to the unclaimed device list when the device uses the call-home agent capability to connect to the server, before it is provisioned by Cisco APIC-EM, or when the Cisco APIC-EM is not able to match the device against the existing configuration.

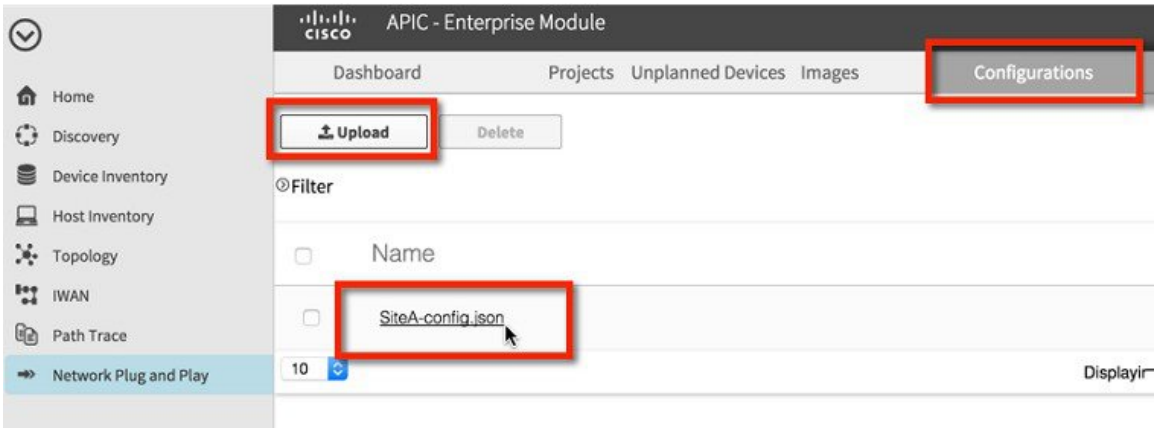
To claim the device, perform these steps:

### Procedure

**Step 1** Choose **Network Plug and Play > Unplanned Devices**.

**Step 2** Select the device from the list and associate the configuration files.

**Step 3** You can either reuse the existing configuration from the list, or apply the new configuration to the device.

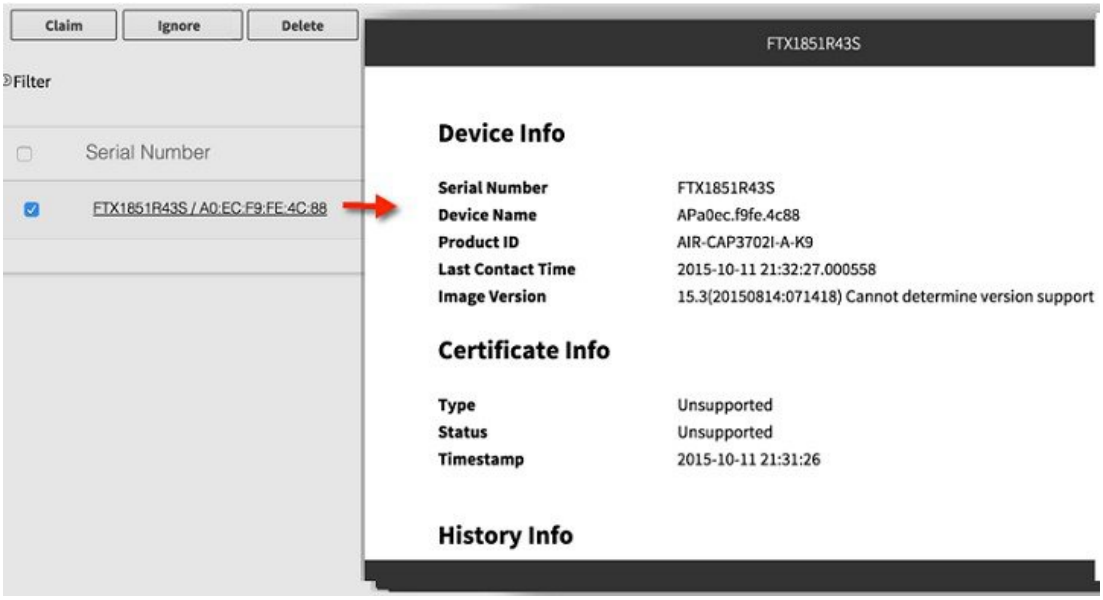



Unsupported for AP:

- Image
- Device Certificate

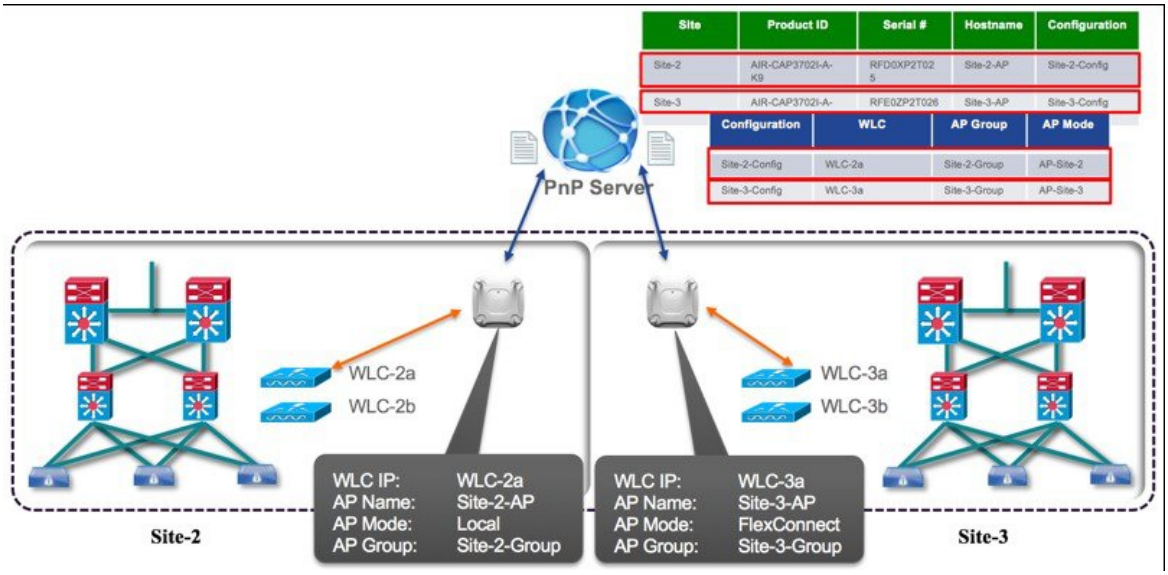
**Step 4** Click **Claim** to claim the device.

**Step 5** Click on the **device** link to view the device information.



## Bulk Import Sites and Devices

You can use the bulk import feature to import a CSV file that contains the sites and devices attributes.



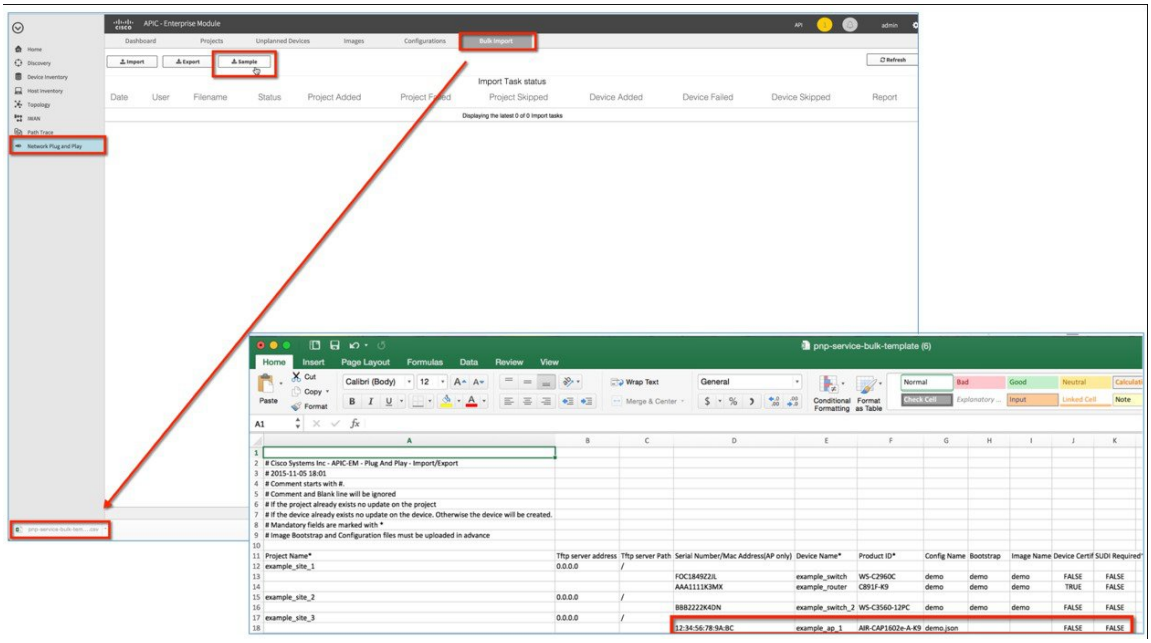

To perform a bulk import of sites and provisioned devices, perform these steps:

### Procedure

**Step 1** Choose **Network Plug and Play>Bulk Import**.

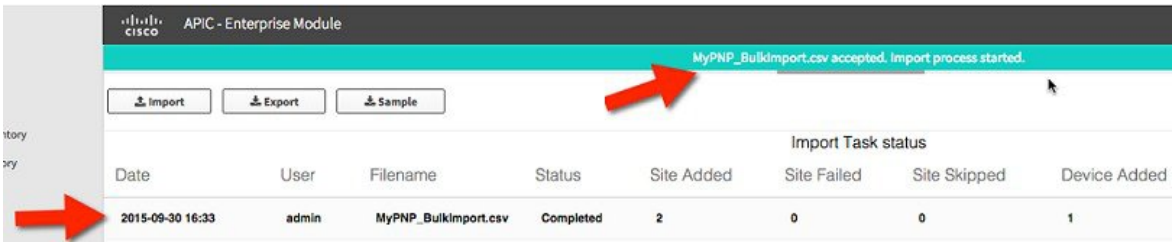
**Step 2** Click **sample** to download the sample file, and add the sites and provisioned devices information:

- Site Name
- Serial Number or Mac Address.
- Device Name (AP-NAME)
- Product ID (e.g. AIR-CAP3702I-A-K9)
- Config Name (text file already uploaded to server).
  - Note that the import will fail if the config files are not on the server.

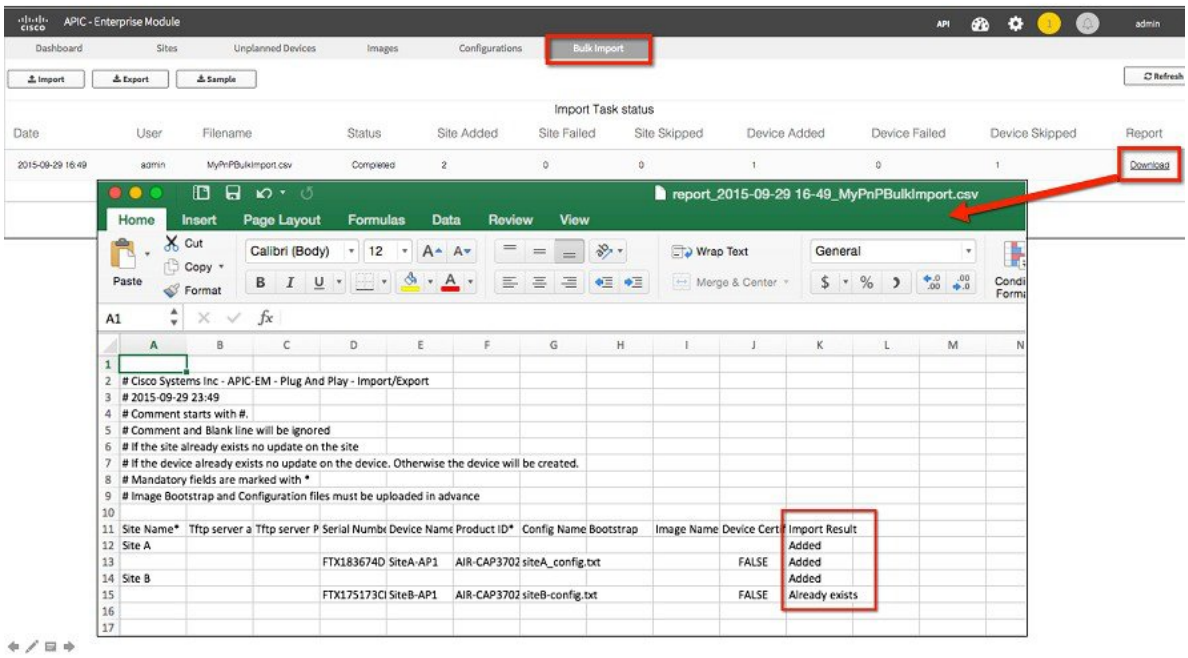



**Step 3** Click **Import** and browse to navigate to the appropriate file.

**Step 4** Select the file and click **Open** to import the CSV file.




**Step 5** To export the devices information, click **Export**. The devices information is exported in a CVS format. Use this information to analyze the devices status.




## Troubleshooting the Cisco Network Plug and Play

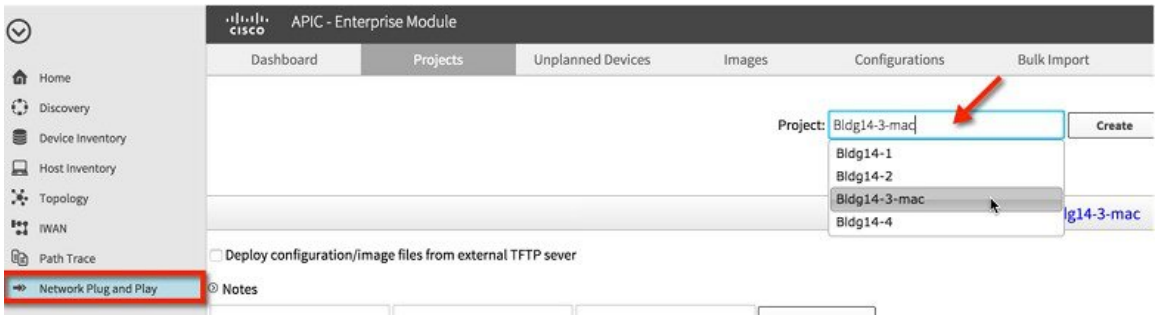
Cisco Network Plug and Play provides the following troubleshooting information for monitoring and troubleshooting the device.

## Checking Cisco Network Plug and Play Status

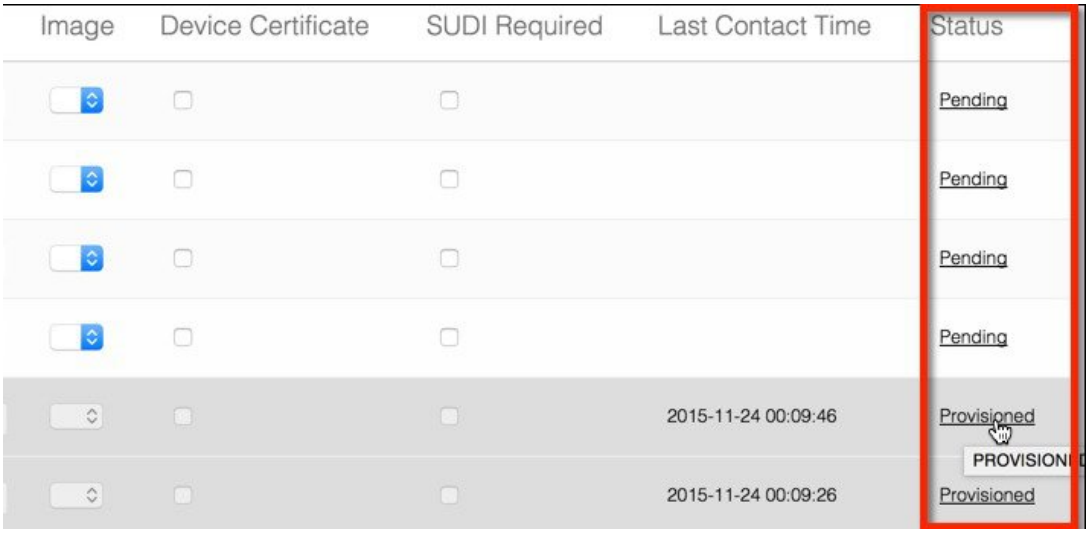
APIC polls AP through the configuration process, during and right before AP join to assigned WLC, this can be viewed in the status, perform these steps:

### Procedure

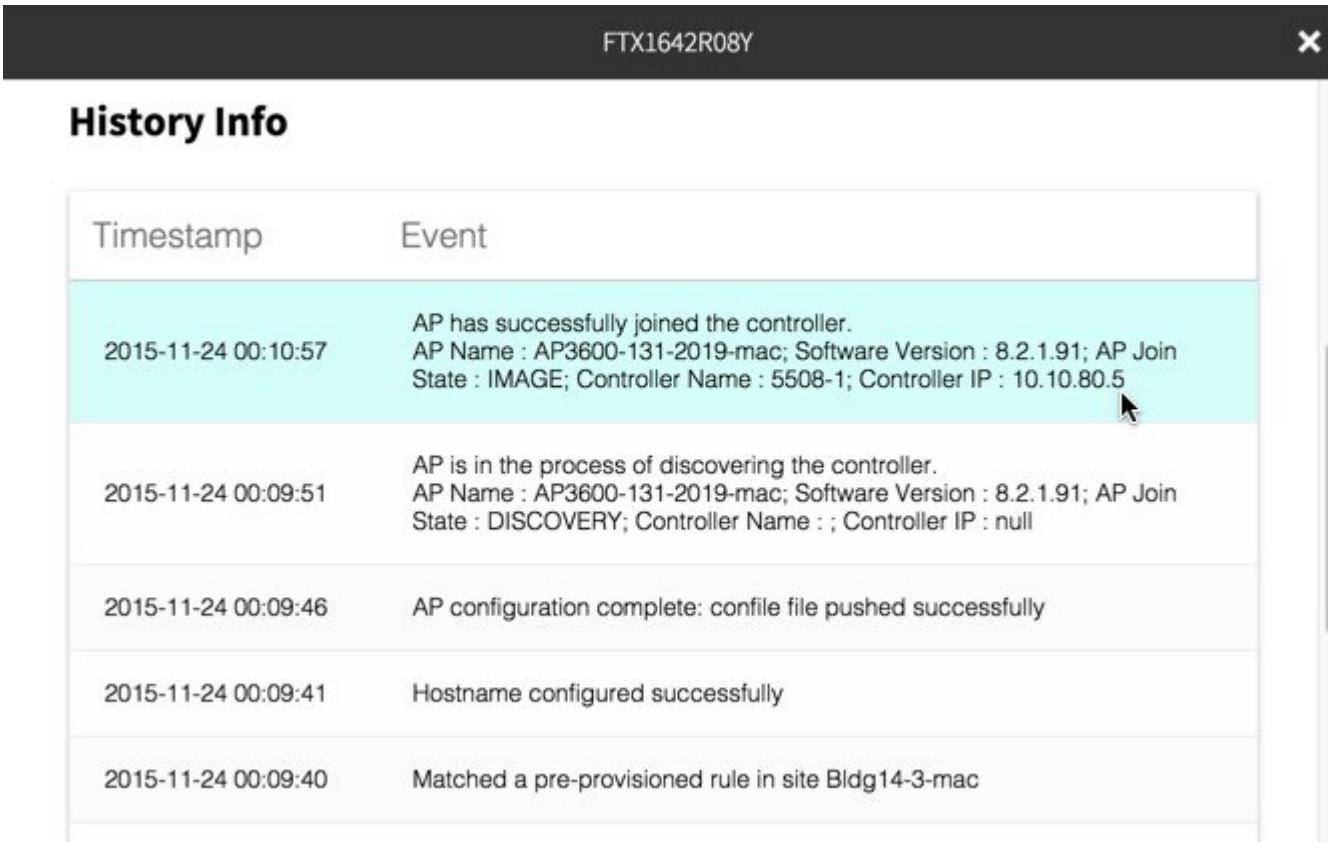
**Step 1** Choose **Network Plug and Play** select a **Project** from the drop-down list.



**Step 2** Click on **status** Link (example: Provisioned).




**Step 3** You can view this log to analyze the Cisco Network Play and Play events and take appropriate action.



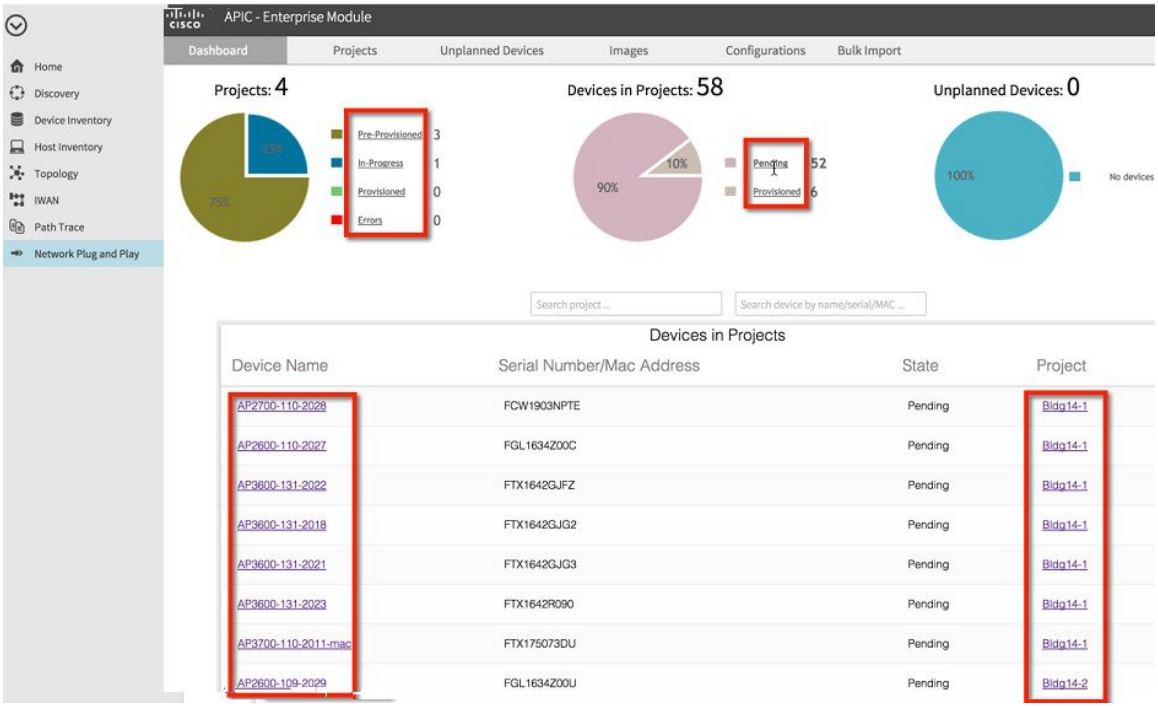
## Reviewing the Status from the Dashboard

### Procedure

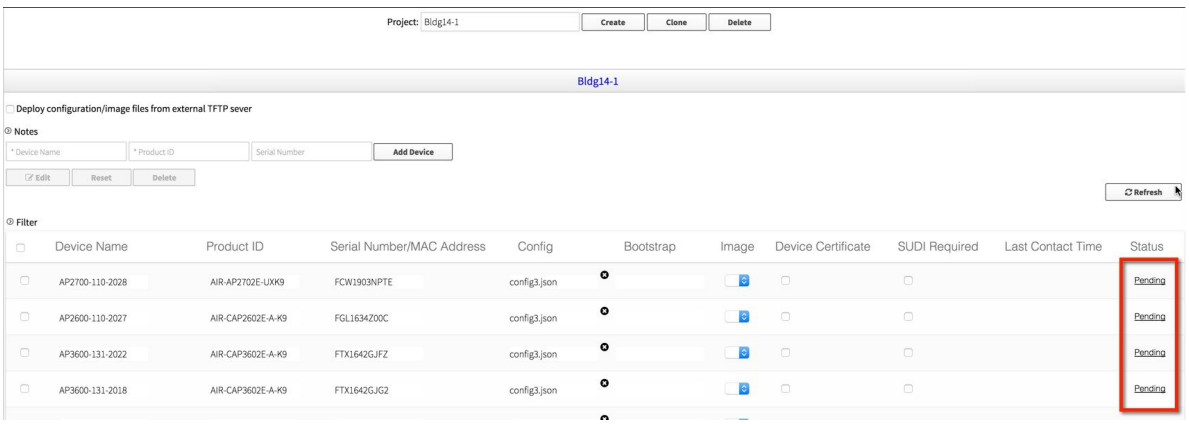
**Step 1** Choose **Network Plug and Play > Dashboard**.

**Step 2** Click on any of the Link next to the charts, e.g. Pending, Provisioned, Errors, etc. to view list of APs in relevant Projects.

**Step 3** Click on any of the AP or Project will take you to the Project view and APs.




**Step 4** Click on Status link will show detail of the PnP process.



**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV
Amsterdam, The Netherlands