Network Simplification

Network Plug and Play for Day-0 Deployments

René and Per, Cisco DK SEs

Cisco Network Plug and Play (PnP) Solution Overview

Simple & Secure & Consistent Device Onboarding

Network Plug-n-Play

Simple, Secure & Consistent device on-boarding for Enterprise platforms

Simple

- **Zero-Touch** provisioning of Campus & Branch deployments
- **GUI** Based workflows
- Robust **Discovery Mechanisms** for all deployment types (DHCP, DNS, Mobile App, USB)
- **Cloud Redirect Service** for automated branch deployments (Roadmap)

Secure

- **SUDI** based device authentication
- CA based server (APIC-EM) authentication
- **HTTPS** for image & config. Downloads
- Installer has no access to device configuration
- Unplanned device workflow – Admin selects device

Consistent

- Support for end-to-end Enterprise platforms – **Switches, Routers, AP**
- **Consistent workflows** for all platforms
- **Backward compatible** w/ Smart-Install (Switches Only)
- Integrated w/ **PI3.x workflows**

Switches (Catalyst)

Routers (ISR/ASR)

Wireless AP

Network PnP with the Cisco APIC-EM Automates Device Provisioning

Network Admin

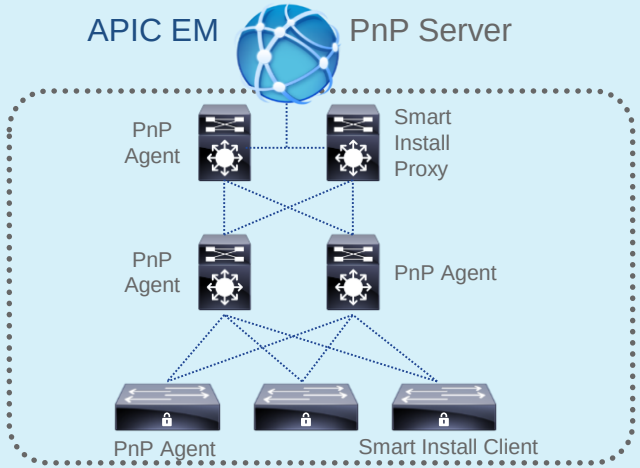
Pre-Provision Projects and Sites

- Policies
- Match rules
- Configurations, images
- IP addressing

Installer

Remote Installer

- Mount and cable devices
- Power on



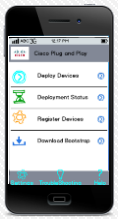
The network admin remotely monitors the installation status while in progress

Booting devices call home to the PnP server, and request instructions

Unskilled Installer	GUI-Based	Consistent for Devices and Pin (Campus, Branch)	Highly Secure	End to End	Greenfield and Brownfield

Network Plug and Play - Components

4



PnP Helper App

Delivers bootstrap status and troubleshooting checks

PnP Protocol

Runs between Agent and Server

Open schema

3

2

PnP Server

Central server - APIC-EM

Manages sites, devices, images, licenses

Provides northbound REST APIs

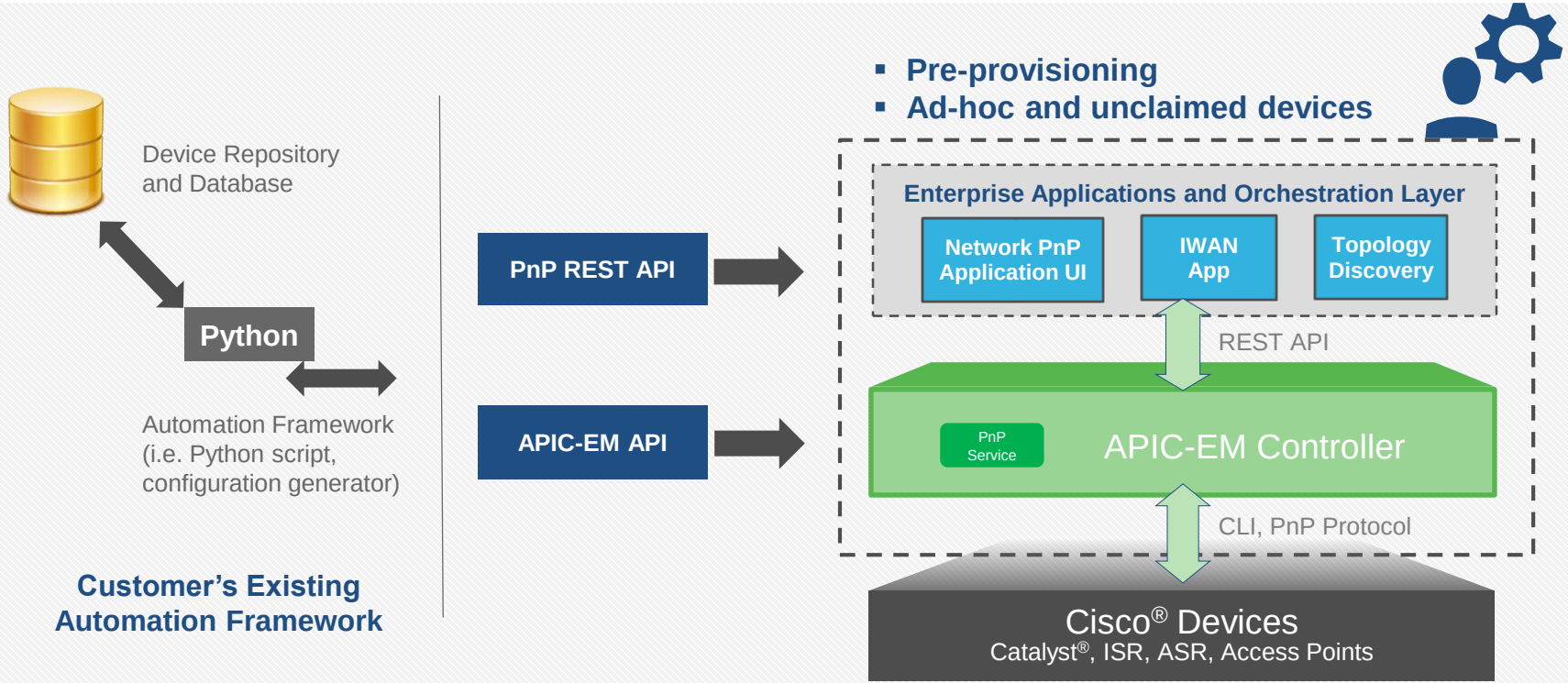
1

PnP Agent

Runs on Cisco® switches, routers, and wireless access points

Automates the deployment process

Cisco APIC EM: PnP Server Workflow-Based and REST API



Cisco PnP Agent Device Capabilities

PnP Server Discovery Options

Switches (Catalyst®)

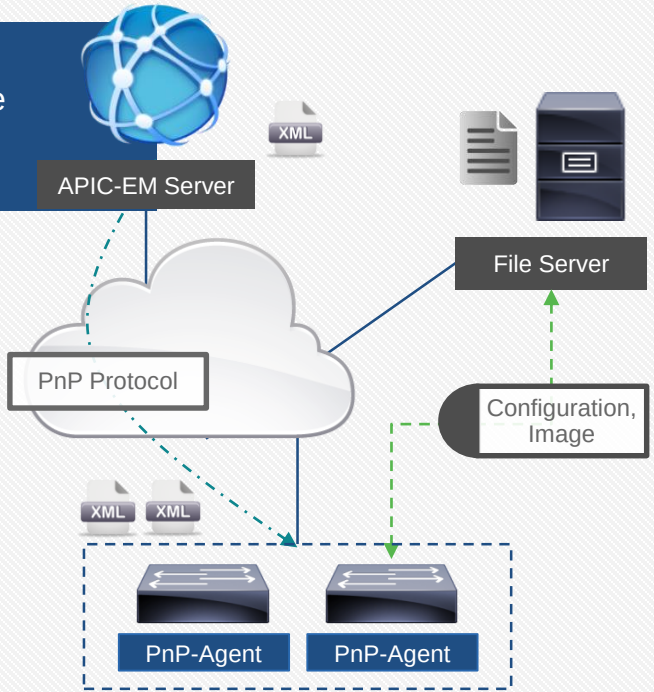
Routers (ISR, ASR)

Wireless Access Points

1	DHCP Server	**DHCP with options 60 and 43** PnP string: 5A1D;B2;K4;I172.19.45.222;J80
2	DNS Server	**DNS lookup** pnpserver.localdomain ---- 172.19.45.222 (PnP Server)
3	cisco	**Cloud re-direction - roadmap (Q3CY2016)** https://devicehelper.cisco.com/device-helper re-directs to 172.19.45.22 (PnP Server)
4		**USB-based bootstrapping**
5		**Manual - using the Cisco® Installer App** iPhone, iPad, Android, (roadmap - Windows mobile and PC)

Agent Services

Services add intelligence to the workflow and encapsulate the platform complexities from the server.



Standard Services:

- Image installation
- Configuration upgrade
- License management
- TCL script execution
- Certification installation
- Configuration CLI

Cisco Automated Device Deployment
Solution Comparison

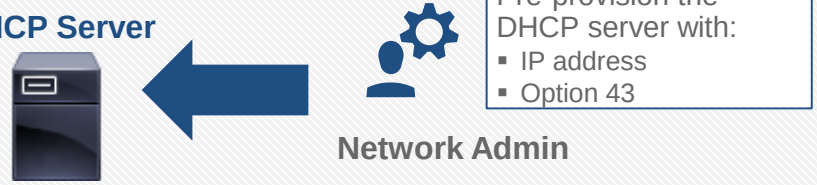
Customer Reqts for Day 1 Provisioning	Auto Install (all ENG)	Smart Install (Cat 2k/3k,4k*)	CNS/CE (Routers, switches)	PnP Solution PI 2.0 (Routers, Switches)	Network PnP Solution
Support unskilled installers (NO CLI)	✓	✓	Partial	✓	✓
Secure deployment	X	X	Partial	X	✓
Support any Place-in-Network (Campus/Branch)	Partial	Partial	✓	Partial	✓
GUI based	X	X	Partial	✓	✓
Consistent for all IOS devices	Partial	X	Partial	Partial	✓
RMA Use Case	X	✓	X	X	✓
Complete automation for branch deployments	X	X	X	X	✓

Pre-Provisioning Workflow

What Is Needed to Start a Campus Deployment

Step 1

Configure the Linux DHCP server with the PnP-specific option 43




```
sudo apt-get install isc-dhcp-server
sudo vi /etc/dhcp/dhcpd.conf

default-lease-time 600;
max-lease-time 7200;
option space CISCO_PNP;
option CISCO_PNP.pnpserver code 43 =
string;

option subnet-mask 255.255.255.0;
option broadcast-address 10.30.30.255;
```

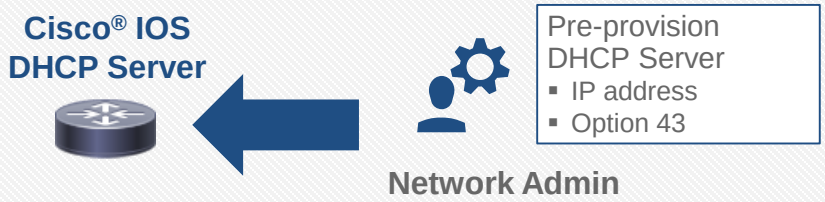
```
subnet 10.30.30.0 netmask 255.255.255.0 {
 range 10.30.30.2 10.30.30.255;
}
class "ciscopnp" {
  match if option vendor-class-identifier =
"ciscopnp";
  option vendor-class-identifier "ciscopnp";
  vendor-option-space CISCO_PNP;
  option CISCO_PNP.pnpserver
"5A;B2;K4;I172.19.210.215;J80";
}
service isc-dhcp-server start
```

What Is Needed to Start a Campus Deployment

Step 1a

- A localized, Cisco IOS® Software-based DHCP server with the PnP-specific option 43

```
ip dhcp excluded-address 10.1.1.1
!
ip dhcp pool pnp_device_pool
 network 10.1.1.0 255.255.255.0
 default-router 10.1.1.1
 option 43 ascii
"5A1D;B2;K4;I172.19.45.222;J80"
!
```

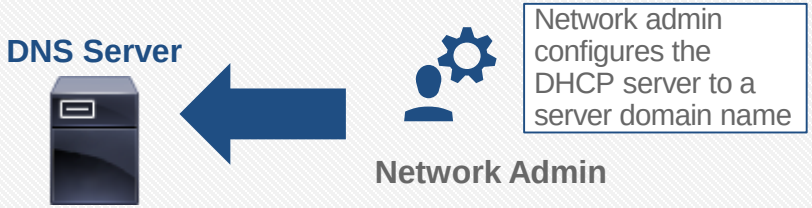


- The sample configuration uses 10.1.1.0/24 as the DHCP pool
- The DHCP server IP is 10.1.1.1
- DHCP option 43 is set with 172.19.45.222 as the PnP Server IP address

What Is Needed to Start a Campus Deployment

Step 1b

Configure the Linux DHCP server for a domain name (DNS)



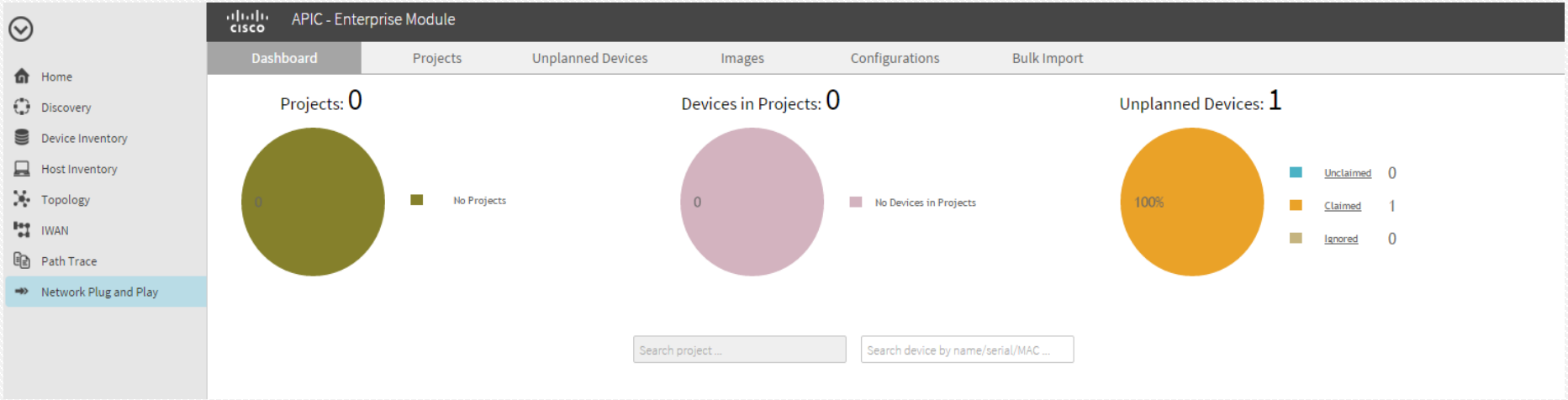

```
sudo vi /etc/dhcp/dhcpd.conf

default-lease-time 600;
max-lease-time 7200;

option subnet-mask 255.255.255.0;
option broadcast-address 10.30.30.255;
option domain-name-servers 10.30.30.1;
option domain-name "cisco.com";
```

```
subnet 10.30.30.0 netmask 255.255.255.0 {
 range 10.30.30.2 10.30.30.255;
}
service isc-dhcp-server start
```

APIC-EM PnP Login Screen

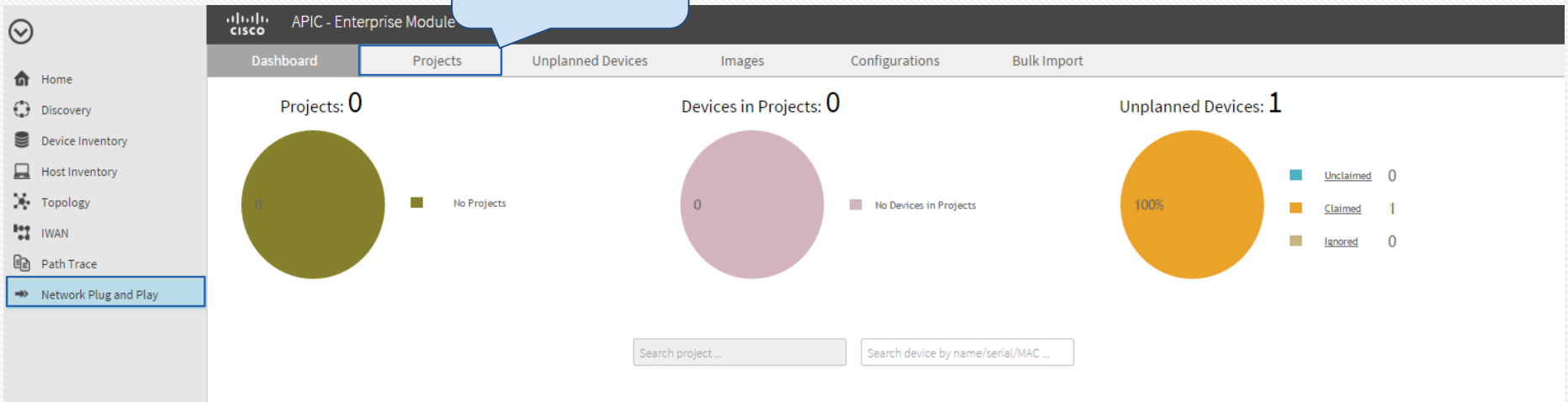


Workflow on the APIC-EM

Log in to the APIC EM and click on Cisco® Network Plug and Play

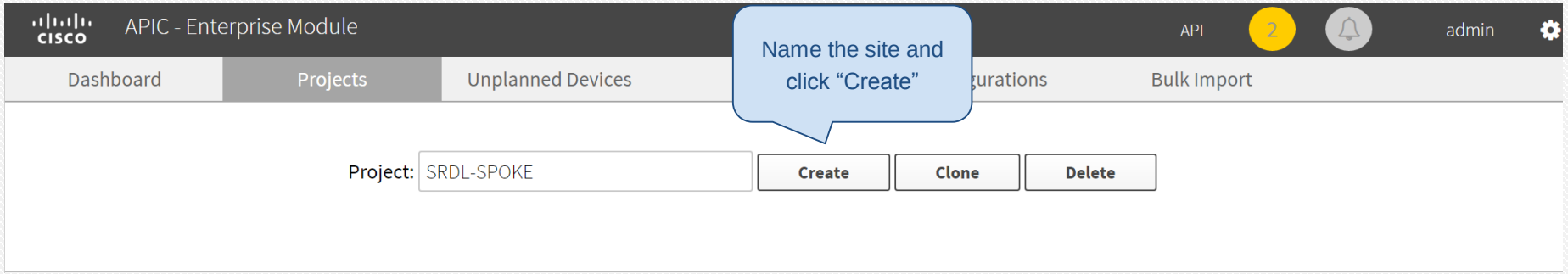
Click on “Projects” to add a new site

Step 2. The network admin creates a site for any new deployment on the APIC-EM PnP app

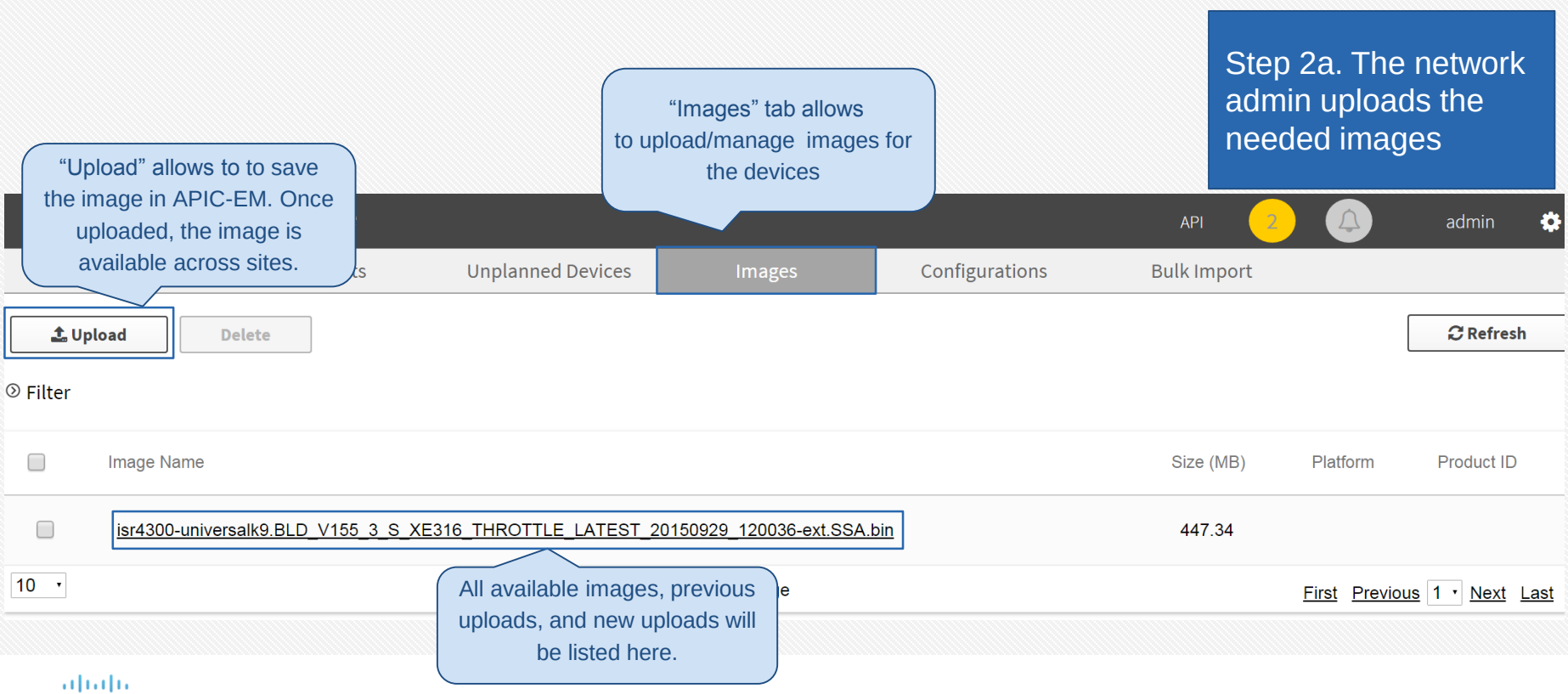


Workflow on APIC-EM

Step 2. The network admin creates a site for any new deployment on the Cisco® APIC-EM PnP app



Workflow on APIC-EM

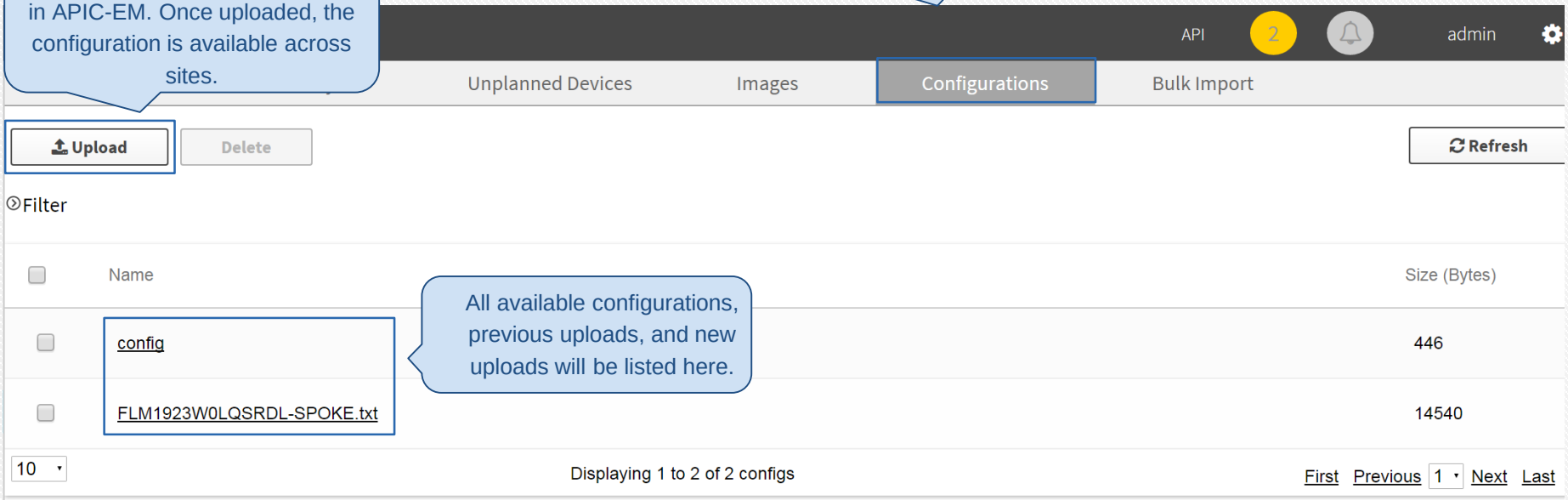


Workflow on APIC-EM

Step 2b. The network admin uploads the needed configurations

"Configurations" tab allows to upload/manage the configurations for the devices.

"Upload" saves the configuration in APIC-EM. Once uploaded, the configuration is available across sites.



All available configurations, previous uploads, and new uploads will be listed here.

Workflow on the APIC-EM

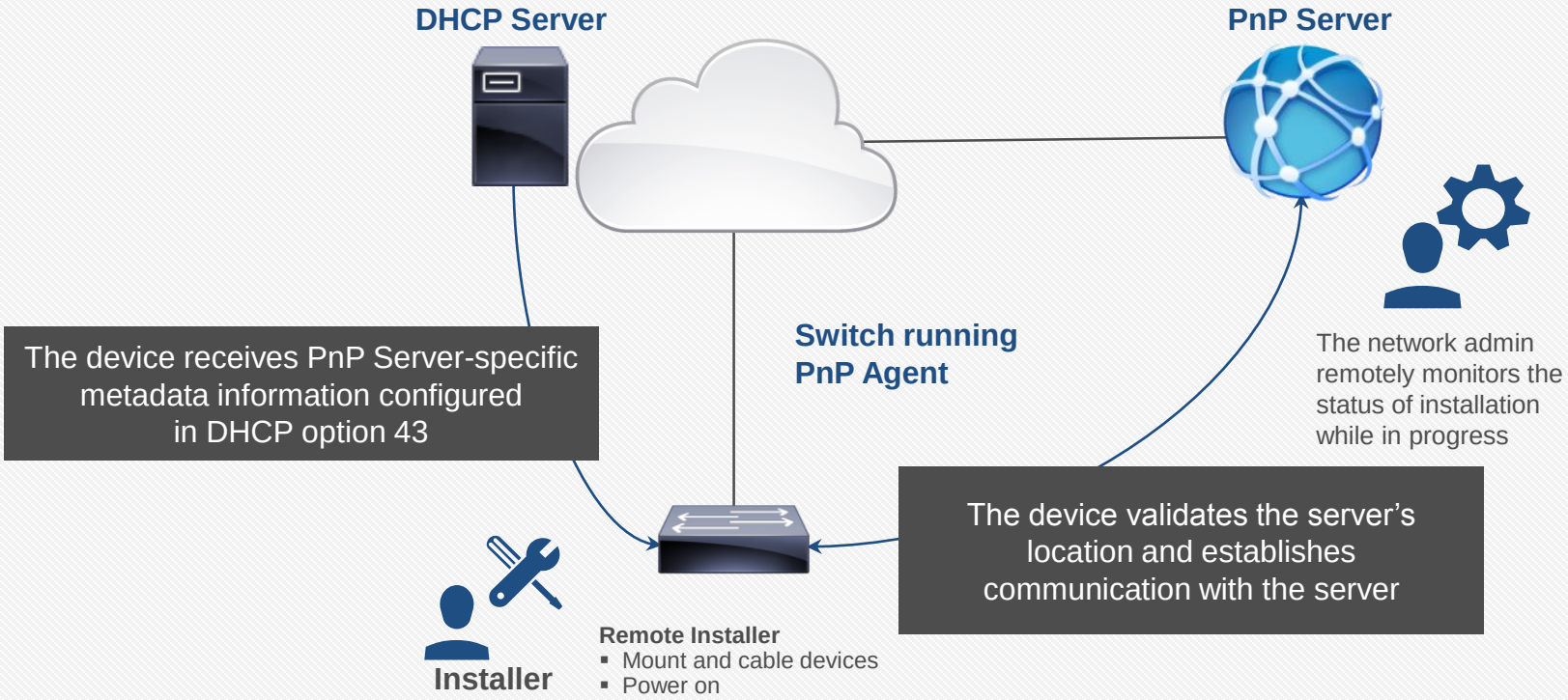
Step 3. Add devices

If any external TFTP server is used for configurations and images, for a given site information must be entered here. This is not recommended.

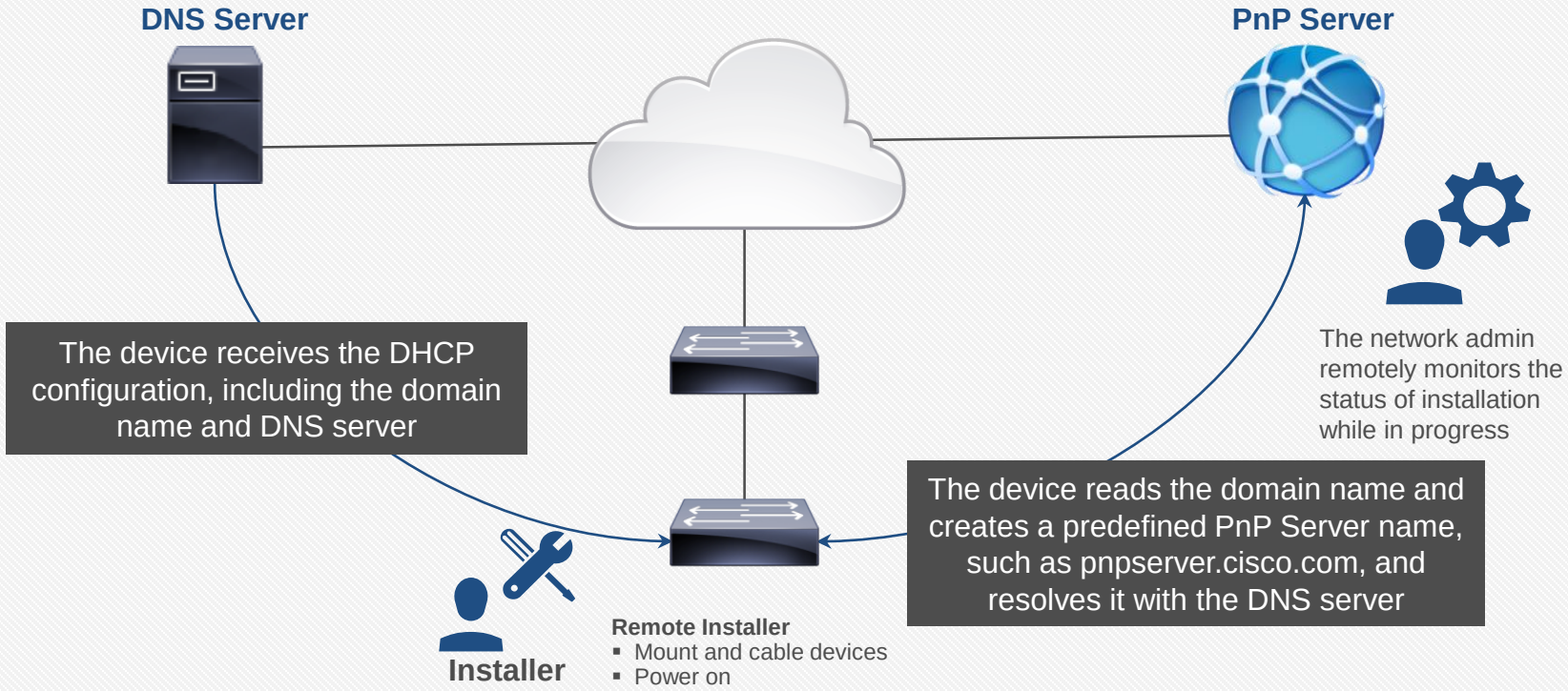
Select the image from an available list already loaded into the APIC-EM

Drag and drop the device configuration here as a txt file or select from uploaded configurations

Device Deployment - DHCP-Based Server Discovery



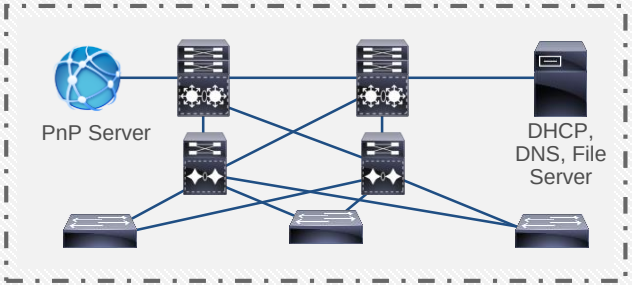
Device Deployment - DNS-Based Server Discovery



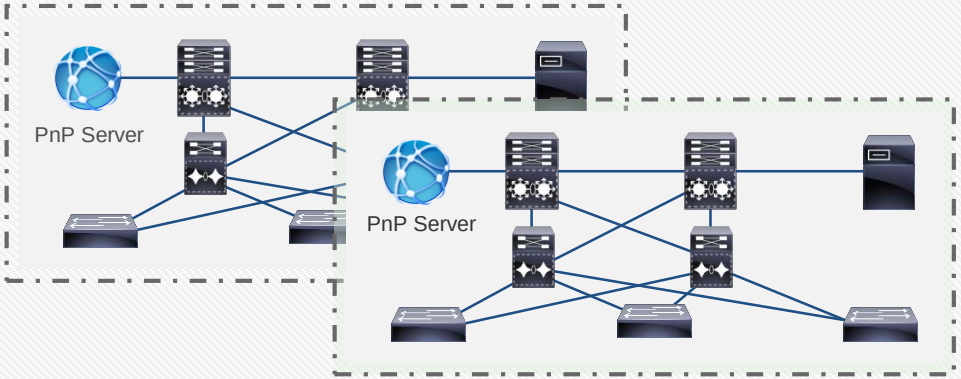
Campus - Site Bring-Up

Network Admin

Day 0
Pre-Provision Projects and Sites
- Policies
- Rules
- Configs, image
- IP addressing



Campus - Building 1



Campus - Building 3

Installer

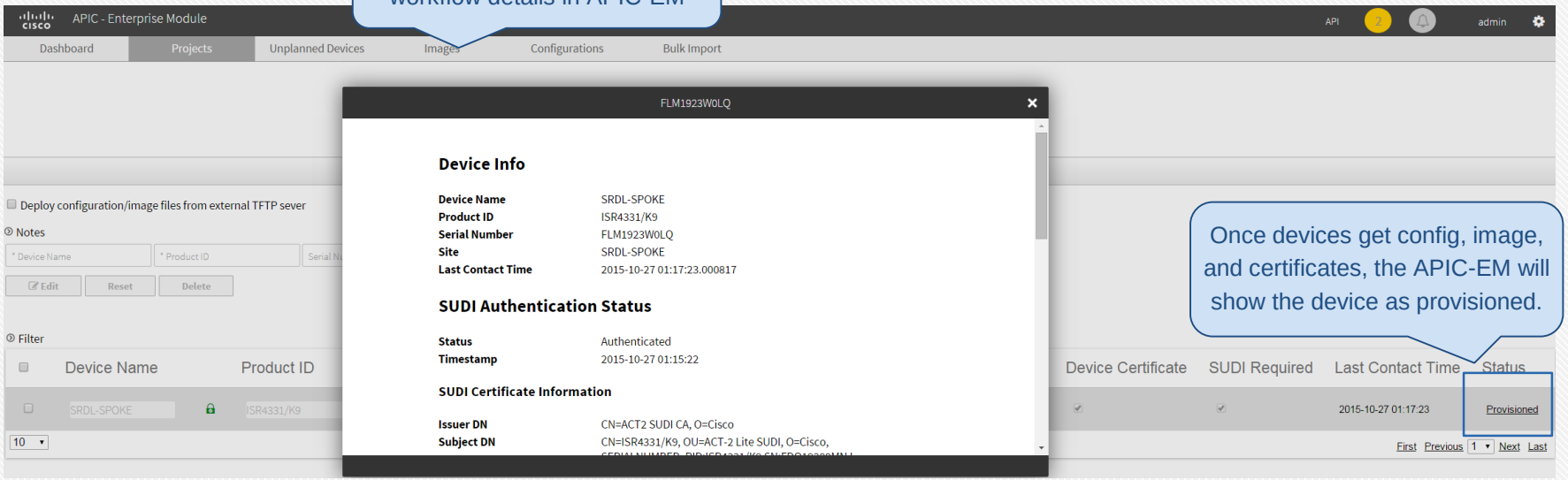
Remote Installer
- Mount and cable devices
- Power on

Day 1: The network admin remotely monitors the status of installation while in progress

Campus - Site Bring-Up

Step 4. Verify installation of devices

Click on “Details” to see full workflow details in APIC-EM



Once devices get config, image, and certificates, the APIC-EM will show the device as provisioned.

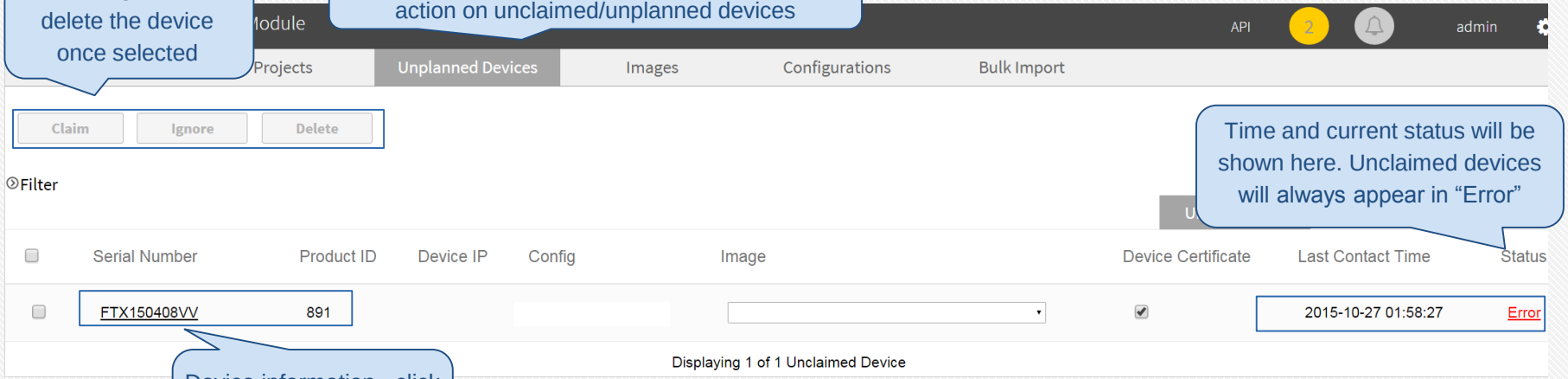
Unplanned Device Deployment

Campus - Site: Unplanned Device

In some cases when a ad-hoc device joins, is not part of any site-specific list, or has been missed for any reason, it will show up in the “Unplanned Devices” view. This is also true in scenarios where a rogue device tries to join the network. Administrators can either claim the device or reject it.

Claim, ignore, or delete the device once selected

“Unplanned Devices” tab allows admin to take action on unclaimed/unplanned devices



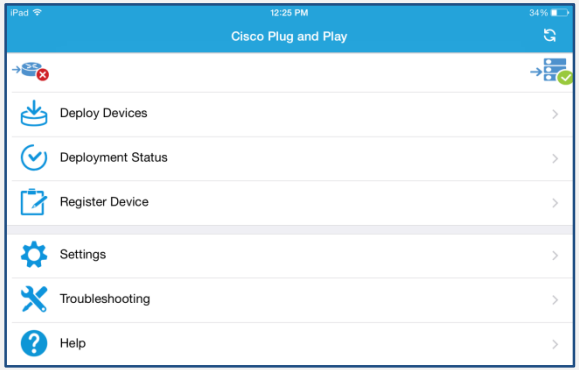
Time and current status will be shown here. Unclaimed devices will always appear in “Error”

Device information - click to get all information about the device

Mobile Application-Based Bootstrapping

Option

Network PnP: Installer App



Apple

Android

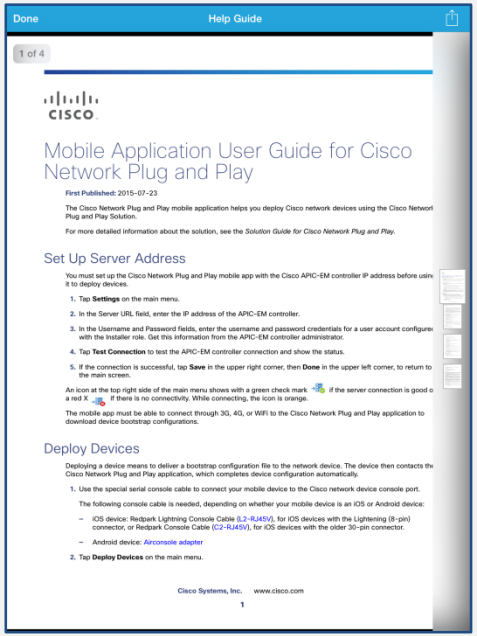
Redpark

RJ45 to Apple 8pin

RJ45 to Apple 30pin

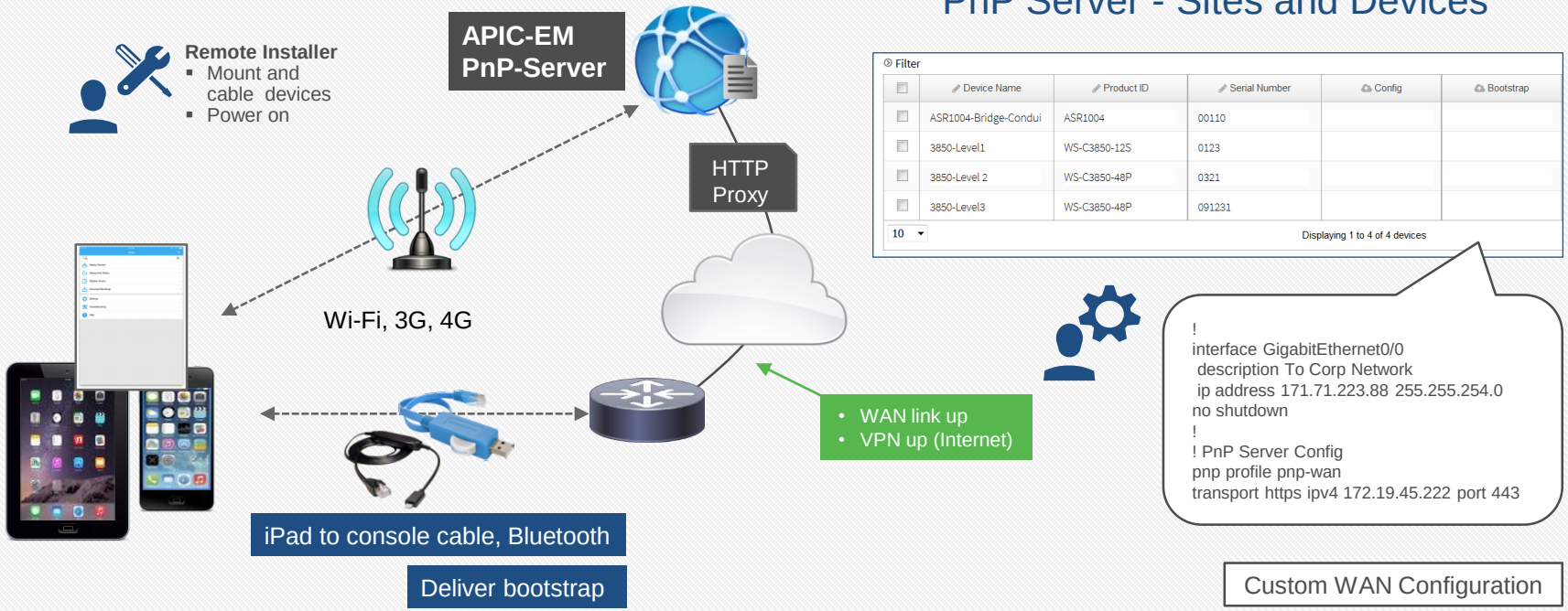
Get Console

Airconsole 2.0 Bluetooth Adapter



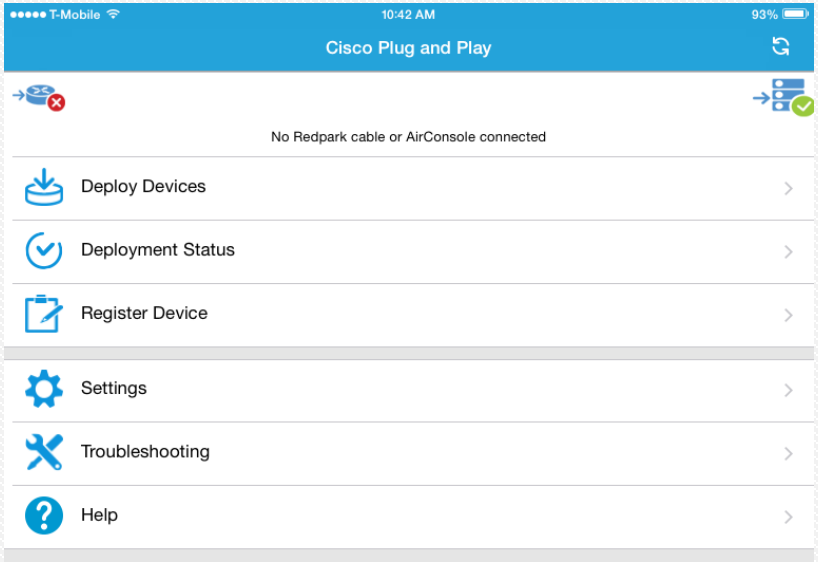
* Tested with Network-PnP Solution

Installer App - Workflow



Installer App: Home Screen

- App used by remote installer
- Runs on an iPad or iPhone



App provides:

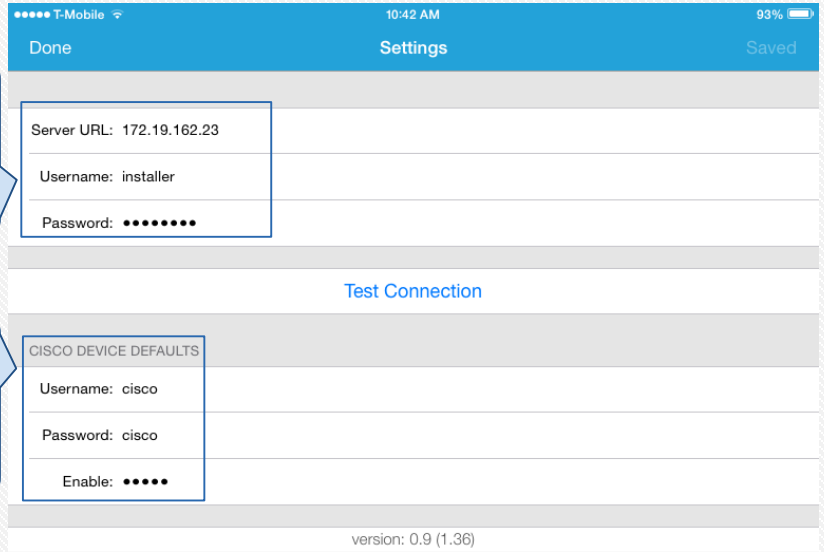
- Bootstrap configuration delivery
- PnP devices status
- Notes for the installer
- Device registration for a site
- Device installation troubleshooting

Installer App: Connecting to the APIC-EM and the Device

The installer app needs to communicate with the Cisco® APIC-EM, and needs to authenticate itself. The app provides a setting where this information can be added.

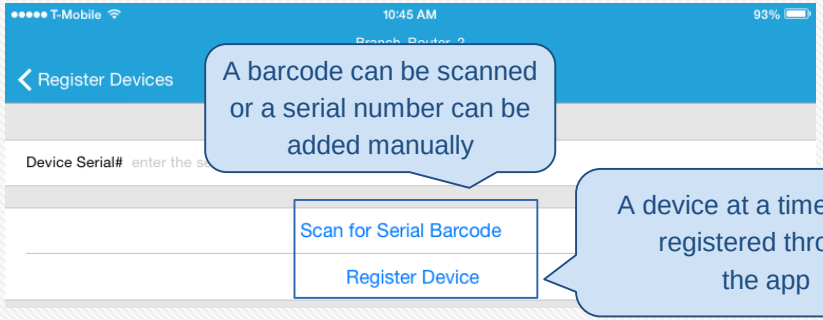
The APIC-EM URL and passwords can be added here. The app can be pre-provisioned by admins so that installers don't need to add this information.

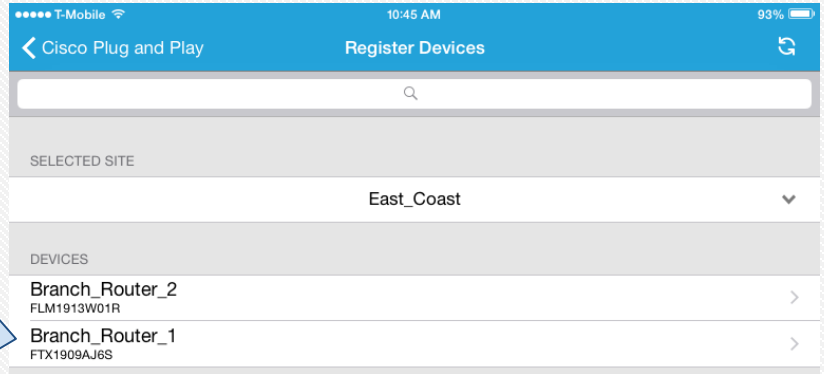
Similarly, device credentials can be added for the app to connect to the console, without sharing information with installers, if that security is required.



Installer App: Registering a Device

The installer can help install and provision new devices that are unplanned



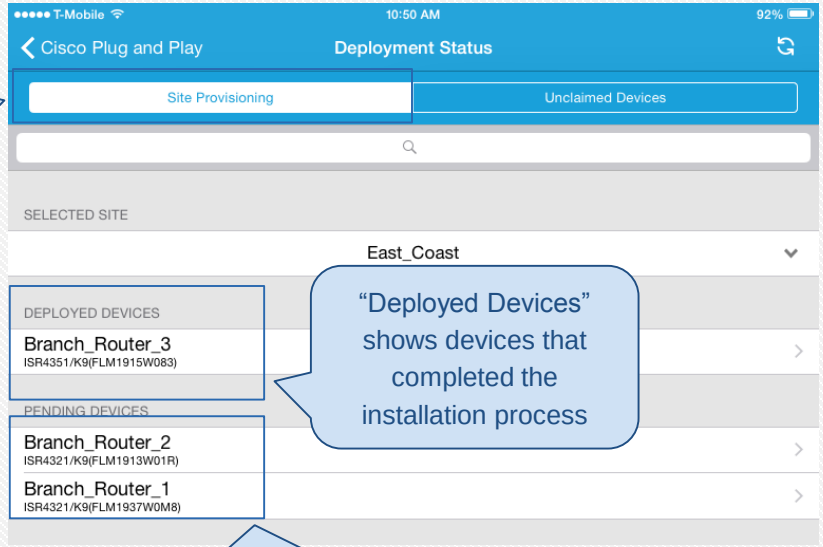


If the registration is successful, the device will show in the APIC-EM and can be provisioned accordingly

Installer App: Site Status

Installer per-device status for the site

Click on “Site Provisioning” to see the device status



“Deployed Devices” shows devices that completed the installation process

“Not Deployed” shows devices that have not started installation or are in progress for installation

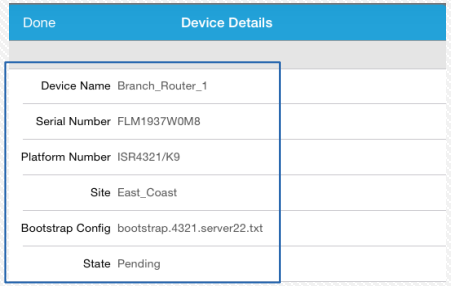
Installer App: Install Status

The installer get details on a device as it is installed. You can view:

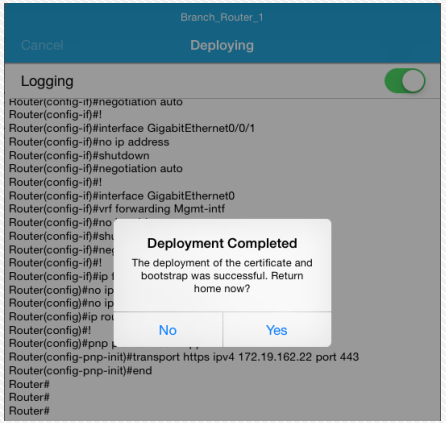
- Device details
- A log of install events and messages

If the device has any issues during this process there are a few troubleshooting methods available on the app itself.

See information on the device being provisioned

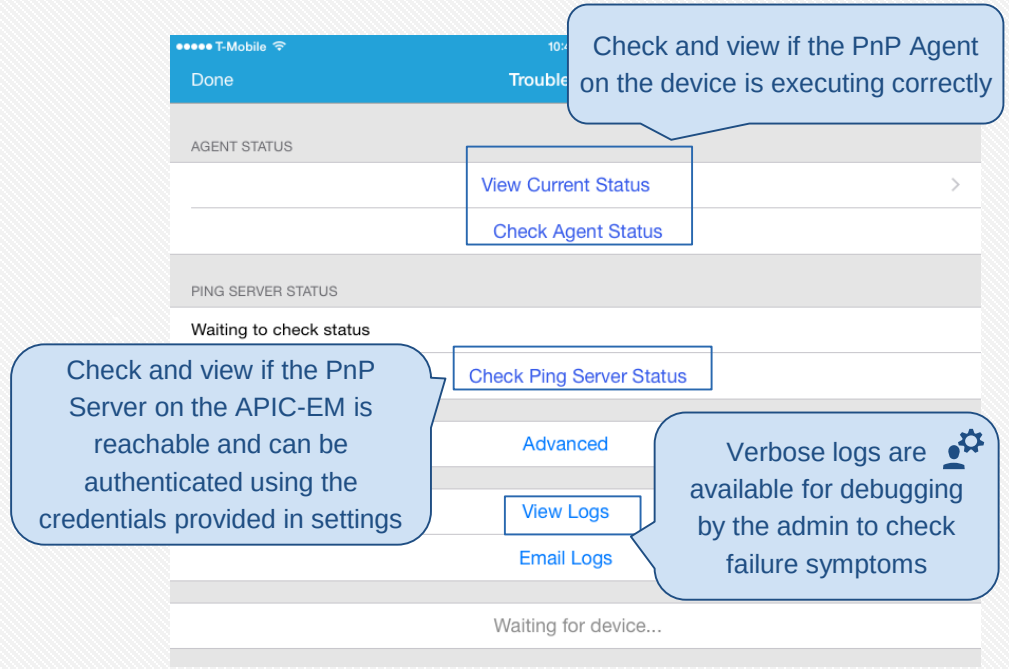


See whether the provisioning has been successfully completed



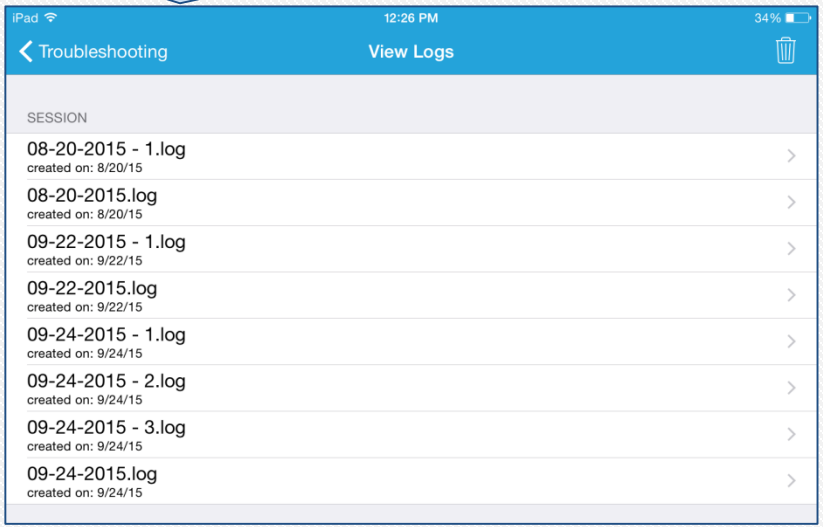
Installer App: Troubleshooting

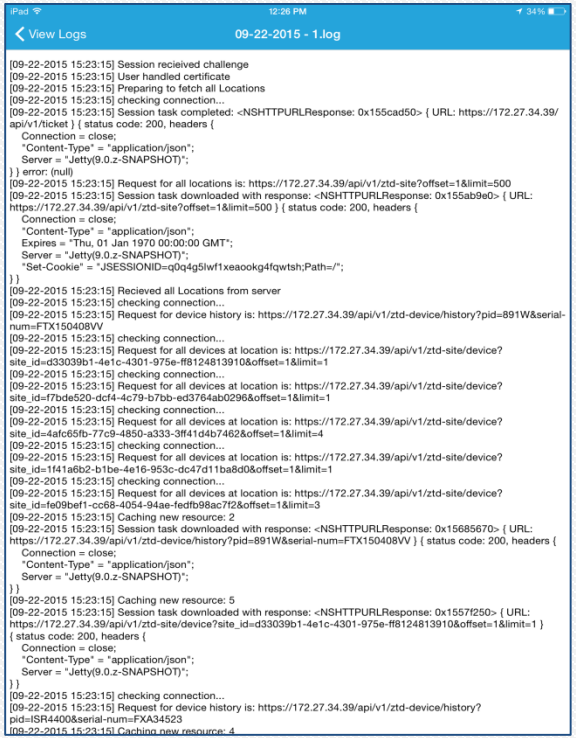
The installer can perform more troubleshooting steps after checking physical connections and power



Installer App: Logs

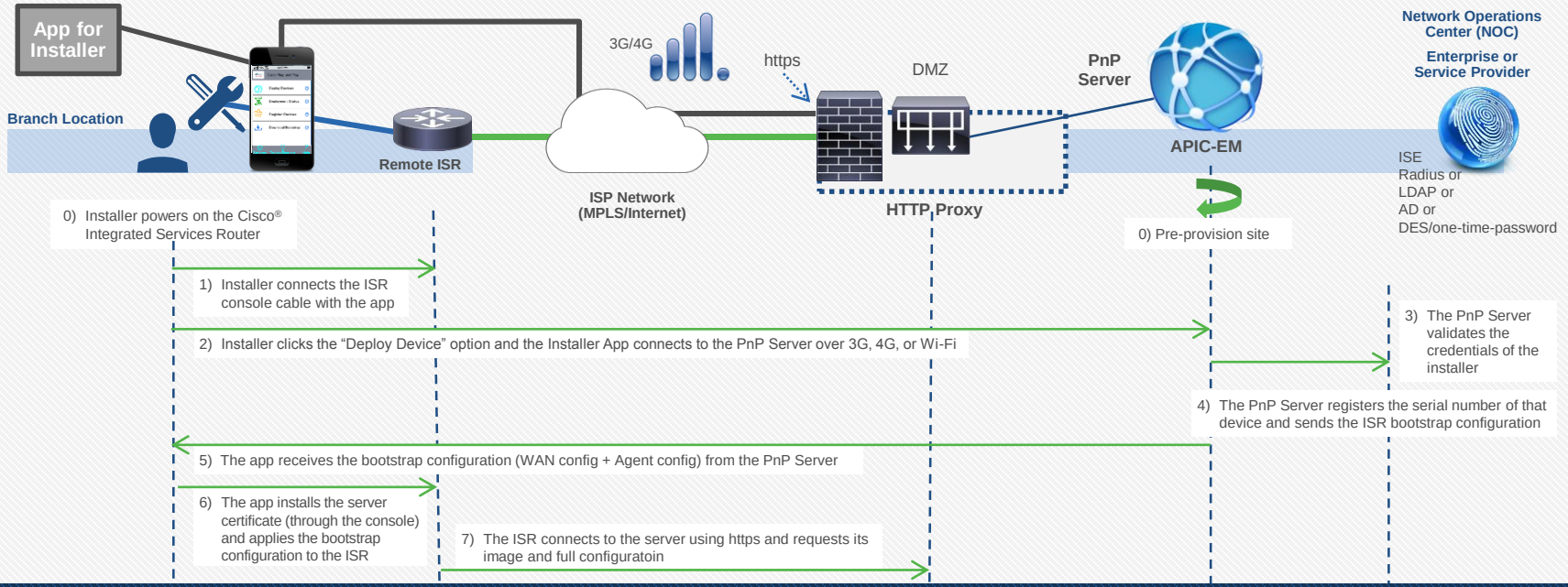
Logs can be emailed by the installer to the admin for instant troubleshooting. The per-device per-provisioning instance is saved.





Installer App-Based Automated Installation with PnP Server

Zero-Touch Configuration for the Installer

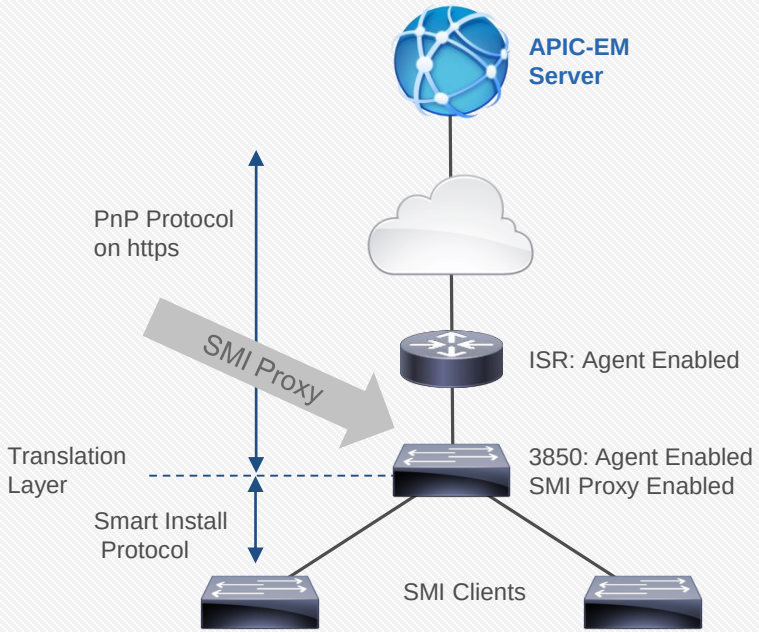


The network admin preconfigures the bootstrap prior to the installer onsite.
The bootstrap configuration is available for all ISRs supporting the agent. The installer app is supported on iPhones and iPads.

Smart Install Proxy

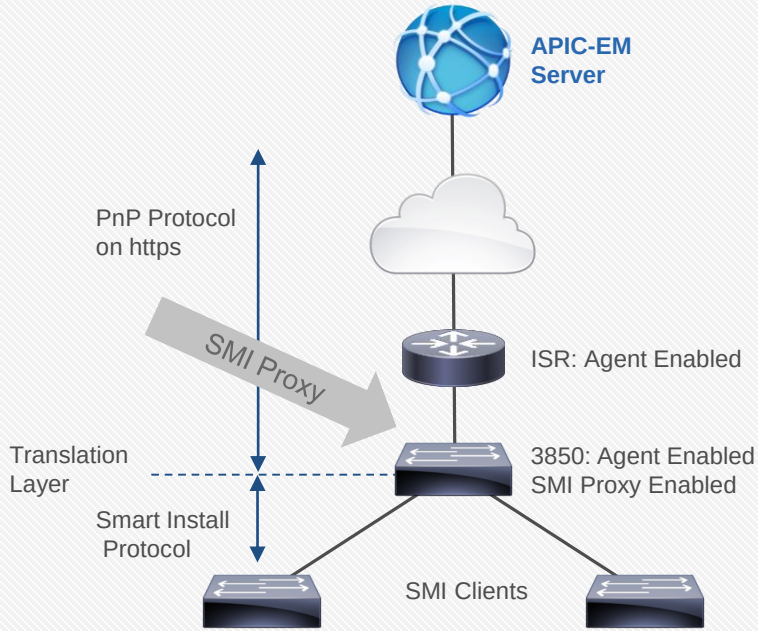
PnP Support with SMI Proxy

- Smart Install Proxy (SMI Proxy) runs on the device with the PnP Agent
- SMI Proxy translates the SMI to PnP
  - Represents SMI client to the PnP Server
- SMI Proxy must be explicitly enabled
- The PnP Server can manage legacy Cisco IOS® Software images on Cisco Catalyst® switches
- Catalyst 3000 and 4000 Series Switches with a minimum IP base support SMI Proxy



SMI Proxy: Caveats

- Non-PnP Agent images do not get all the benefits of PnP Agent support
- Caveats to a solution with older Cisco IOS® Software clients:
  - Cisco® APIC-EM discovery
  - SMI Proxy device must be explicitly enabled
    - Must be an SMI director-capable switch or release
  - Not managed by the APIC-EM as a special device
  - Scale and performance limits



PnP Support for SMI Proxy

Integrated Branch Director (IBD) Configuration Snippet

```
vstack vlan 1
vstack config tftp://10.30.30.10/cfg_new.txt
vstack group custom test product-id
 config tftp://10.30.30.10/cfg_new.txt
 match WS-C3560C-12PC-S
vstack dhcp-localserver smi
 address-pool 10.30.30.116 255.255.255.0
 file-server 10.30.30.10
 default-router 10.30.30.193
vstack director 10.30.30.193
vstack basic
vstack startup-vlan 1
no vstack backup
```

Sample configuration for IBD and SMI proxy to enable PnP

```
<pnp xmlns="urn:cisco:pnp" version="1.0"
udi="PID:7206VXR,VID:,SN:34835437">
  <info xmlns="urn:cisco:pnp:work-info" correlator="CiscoPnP-1.0-15-
1B64AE4">
    <deviceId>
      <udi>PID:7206VXR,VID:,SN:34835437</udi>

<hostname>Switch.viaProxy.PID:7206VXR,VID:,SN:34835437</hostname>
      <authRequired>false</authRequired>
      <viaProxy>true</viaProxy>
    </deviceId>
</info>
</pnp
```

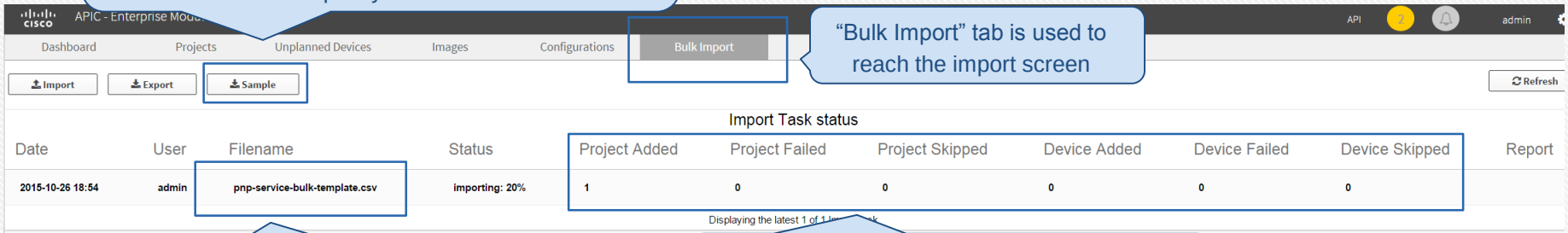
Sample XML payload sent from the device to the APIC-EM, enabled through SMI Proxy

Bulk Import and Export

Bulk Import

Bulk Import is used when there are more than 10 devices to add across sites. A CSV file can be pre-populated with device information and uploaded to the APIC-EM to enable the import process to add devices in one instance, instead of adding devices one by one.

A sample is provided, which can be downloaded to create a template for bulk imports. Any import can later be exported. Bulk Import works across sites, so caution should be used to specify the correct site name.



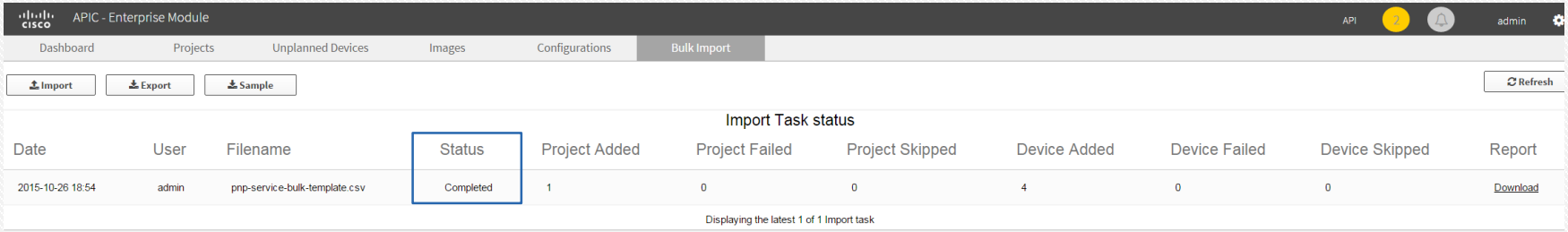
"Bulk Import" tab is used to reach the import screen

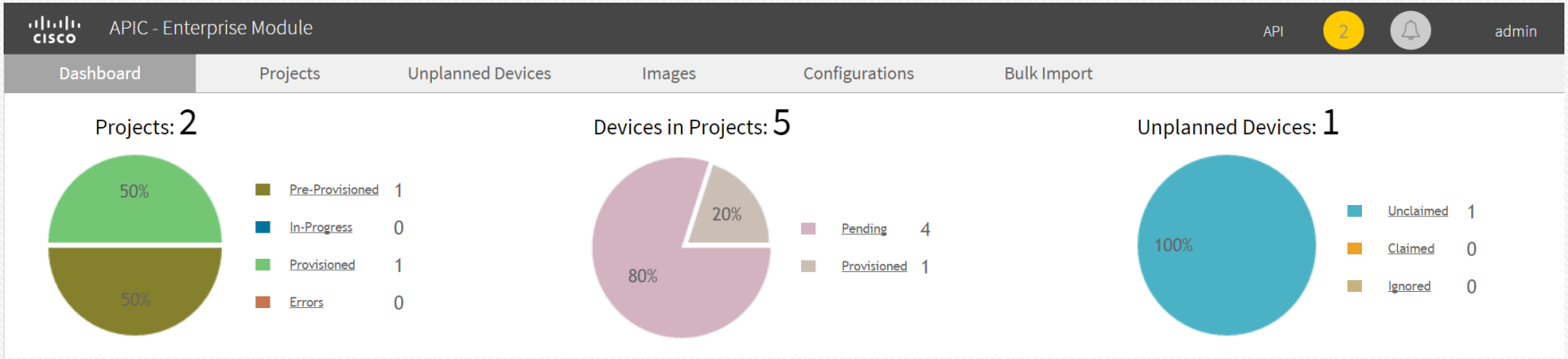
All the files being used for bulk imports are listed here.

Corresponding to each file, import information is populated. Sites and devices that are added skipped, or failed are displayed.

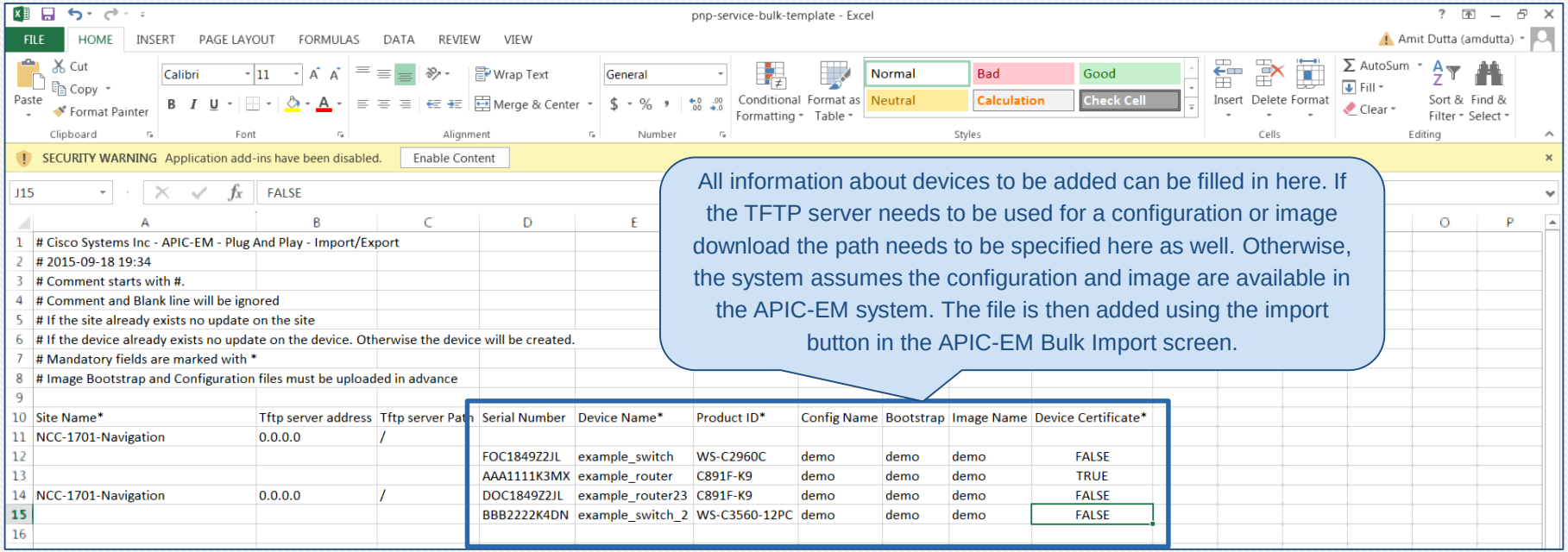
Bulk Import

New slide





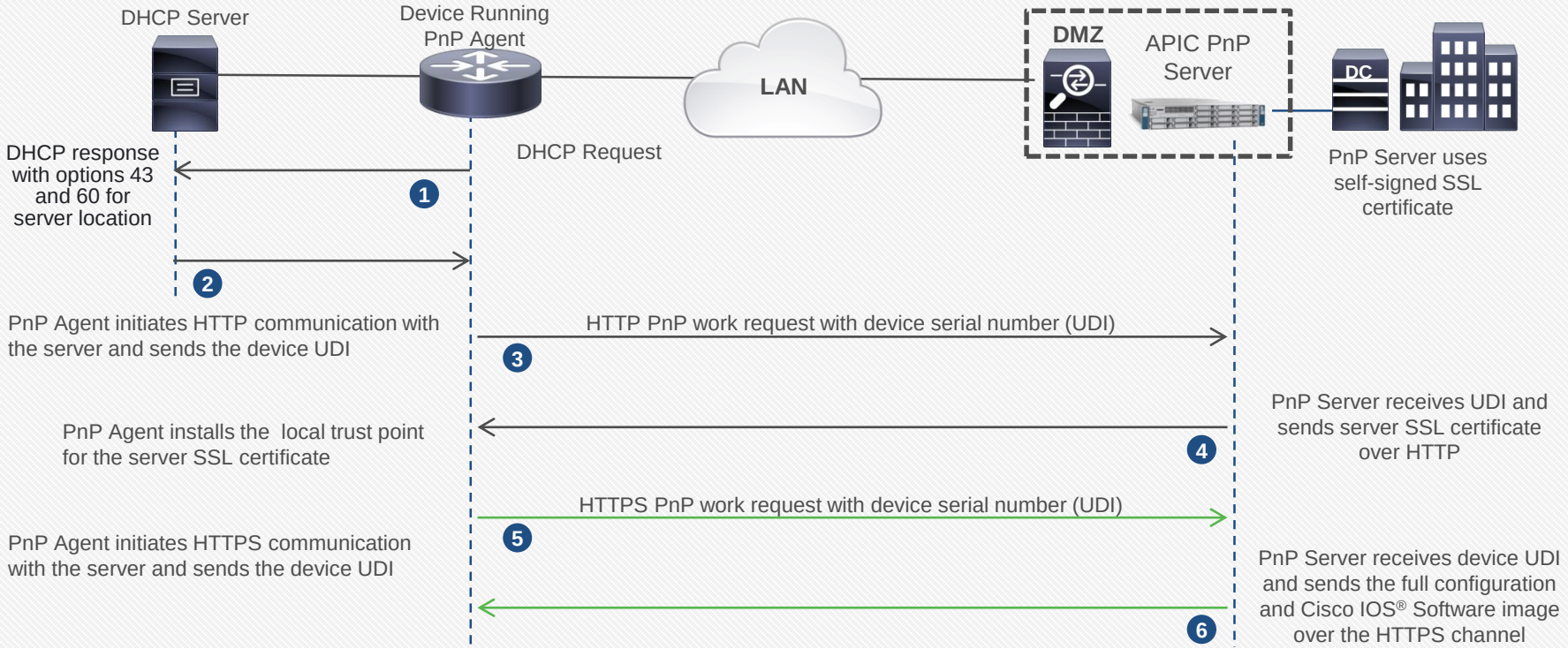
Sample Bulk Import File



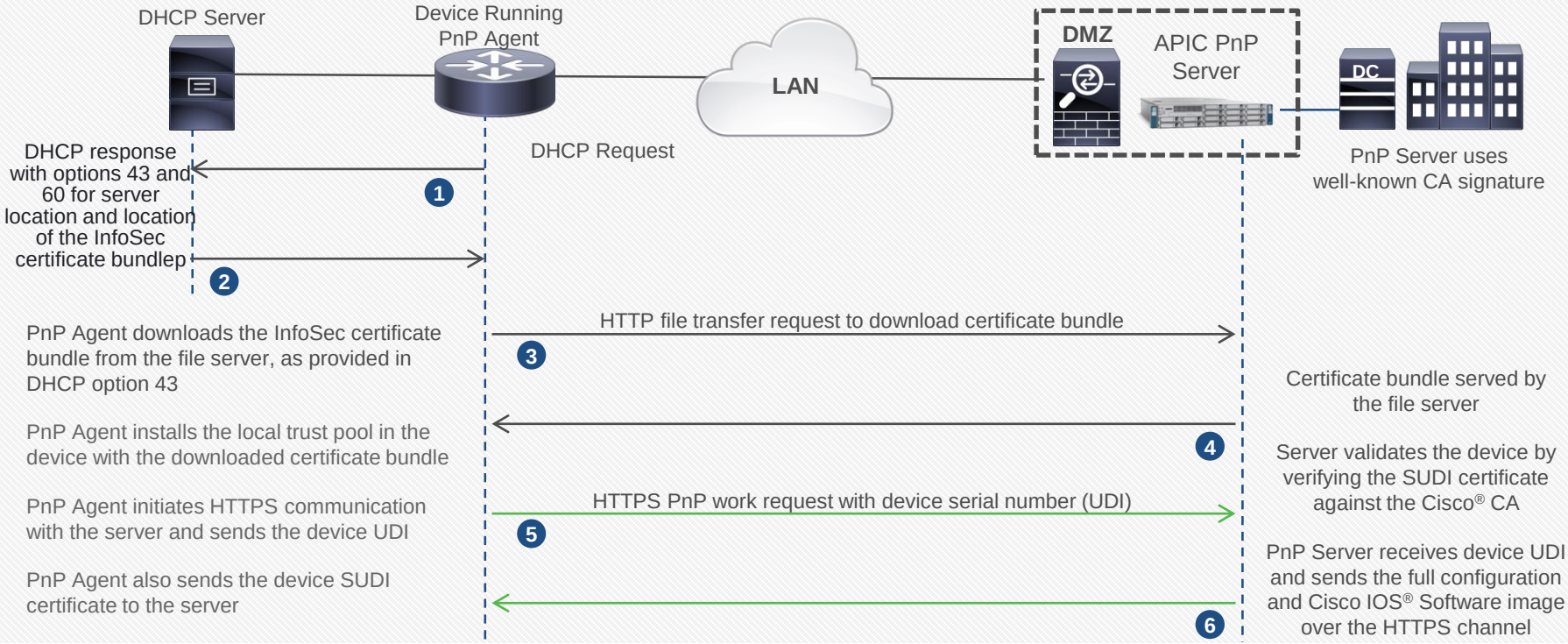
	A	B	C	D	E	F	G	H	I	J	K
1	# Cisco Systems Inc - APIC-EM - Plug And Play - Import/Export										
2	# 2015-09-18 19:34										
3	# Comment starts with #.										
4	# Comment and Blank line will be ignored										
5	# If the site already exists no update on the site										
6	# If the device already exists no update on the device. Otherwise the device will be created.										
7	# Mandatory fields are marked with *										
8	# Image Bootstrap and Configuration files must be uploaded in advance										
9											
10	Site Name*	Tftp server address	Tftp server Path	Serial Number	Device Name*	Product ID*	Config Name	Bootstrap	Image Name	Device Certificate*	
11	NCC-1701-Navigation	0.0.0.0	/								
12				FOC1849Z2JL	example_switch	WS-C2960C	demo	demo	demo	FALSE	
13				AAA1111K3MX	example_router	C891F-K9	demo	demo	demo	TRUE	
14	NCC-1701-Navigation	0.0.0.0	/	DOC1849Z2JL	example_router23	C891F-K9	demo	demo	demo	FALSE	
15				BBB2222K4DN	example_switch_2	WS-C3560-12PC	demo	demo	demo	FALSE	
16											

PnP Security Workflow

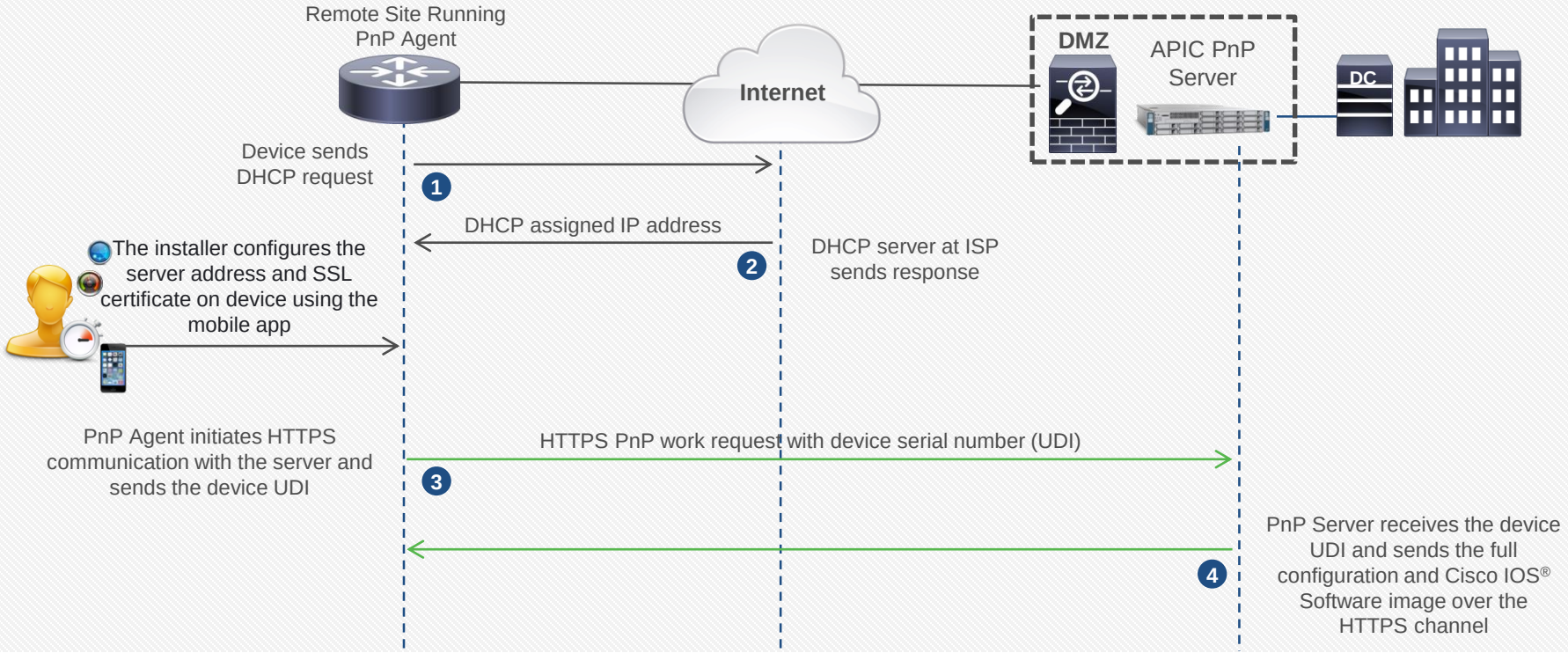
PnP Deployment for Campus - Self-Signed Certificate Method



Secured PnP Deployment for Campus - Trust Pool Method



Secured PnP Deployment for a Branch with the Mobile App



PnP Security - Secure Connection Enablement

Phase 1

Phase 1: Server certificate not authenticated	PnP Agent on device accepts certificate from the server • The server certificate is NOT authenticated	Installer App downloads the PnP Server certificate to the PnP Agent • App contains server certificate prior to delivering to the Agent • The server certificate is NOT authenticated

- HTTPS is always used

Phase 2

Phase 2: Server certificate is authenticated	PnP Agent has a built-in list of CA servers from the PKI trust pool	PnP Agent authenticates the server certificate in the trust pool	PnP Server follows the process to import the CA certificate	It is a similar process to wireless LAN controllers

Key Takeaways

Summary

Solution Summary

- Cisco® Network PnP is a simple, highly secure, and scalable automated network device deployment solution
- The agent is supported on end-to-end Cisco IOS® Software products
- The Cisco APIC-EM is the central server for the solution
- Programmability: The APIC-EM allows scripting (REST API) to automate server workflows
- Python server reference implementation in DevNet: **Give link here**
- Open-source protocol available: Customers and partners can adapt the PnP server into their own processes or build their own server based on open protocols (The schema is proprietary, even if using XMPP)

Benefits

- No pre-staging of devices
- Unskilled installer at remote sites
- GUI-based workflows
- Highly secure and scalable

NG Plug-N-Play – Supported Platforms

IOS-XE | IOS

Platform	PnP Agent Support on Products	Recommended Release
Access Switches	Cisco Catalyst 4500E Switches (Sup8-E, 7-E/7L-E, 6-E/6L-E) Cisco Catalyst 3850, 3650 Series Switches Cisco Catalyst 4500-X, 4900 Series Switches Cisco Catalyst 3750-X, 3560-X Series Switches Cisco Catalyst 2960-C, 3560-C Series Compact Switches Cisco Catalyst 2960-S/SF, 2960-X/XR Series Switches	IOS-XE 3.6.3E IOS 15.2.2E3
	Cisco Catalyst 3850XU/XS Series Switches Cisco Catalyst 2960-CX, 3560-CX Series Compact Switches	IOS-XE 3.7.2E IOS 15.2.3E2
Core Switches	Cisco Catalyst 6500 Series Switches: Sup2T/Sup720 Cisco Catalyst 6880-X, 6807-XL Series Switches	IOS 15.2(2)SY1 (Mar2016)
Access Routers	Cisco 4300/4400 Integrated Services Router Cisco ASR 1000 Series Aggregation Services Routers, Cisco CSR 1000v Cisco Cloud Services Router 1000V Series Cisco 800, 1900, 2900, 3900 Series Integrated Services Routers (ISR G2)	IOS-XE 3.16.S (ED) IOS 15.5.3M (ED)
Industrial Ethernet Switches	Cisco Industrial Ethernet 2000, 3000 Series Switches	IOS 15.2.2E3
Indoor Access Points	Gen2 802.11n AP 1600, 2600,, 3600, 702-W/I 802.11ac Wave1 - 1700, 2700, 3700, Wave 2 802.11ac & Outdoor AP support (Roadmap) WLC Supported : AireOS and IOS-XE	Nov2015


CISCO