Overview

Cisco Plug and Play Connect (a component of the Cisco Network Plug and Play solution) is a cloud-based service that provides a discovery mechanism for a network device to discover its on premise APIC-EM controller or can be used for configuration provisioning of the devices directly without using APIC-EM*

This presentation talks about the Redirection Capabilities and Configuration Management.

*Note: Please note that configuration provisioning of the devices directly from Cisco Plug and Play Connect is currently a beta functionality.
Table of Contents

I. Accessing Smart Account
II. CCW Integration
III. APIC-EM Integration
IV. Redirect Capabilities
V. Configuration Management
VI. Network Tab
VII. SUDI Details
VIII. Add Software Devices
IX. RMA
X. Certificates
XI. SDWAN Network Hub
XII. Manage External Virtual Account
XIII. PnP Help Tab
XIV. References
I. Accessing Smart Account
New Smart Account Signup

Step by Step Instructions:


The following Smart Account administration functions can be accessed from Cisco Software Central (software.cisco.com):

- Request a new Smart Account
- Request access to an existing Smart Account

**Note**: VA Admins will now also be allowed to access the PnP Connect portal. Previously, only SA admins could access the tool.
Request a New Smart Account
Request Access to an Existing Smart Account

Use this page to request access to a Smart Account or Holding Account that has already been established by your company or associates. You will need to know the specific Domain Identifier that represents the Smart Account to request access.

Your Profile

Your Cisco.com profile will be included with the access request to the Account Administrators. It is very important that it is accurate before proceeding. If you need to update your profile, do it now.

Company/Organization Name: Cisco Systems, Inc.
Full Name: Vinita Karthikeyan
Email Address: vkarth@cisco.com
Cisco ID: vkarth
Phone: +1 408 527 6088

Smart Account Domain Identifier

Provide the Smart or Holding Account Domain Identifier you are requesting access to, by entering it below:

Account Domain Identifier:
II. CCW Integration
CCW Ordering of PNP Device

The Plug and Play (PNP) Connect web portal is linked to Cisco Commerce Workspace (CCW), facilitating automatic registration of the serial numbers and PIDs of purchased devices in Plug and Play Connect. The following are steps on how to enable the automated registration.

**Step by Step Instructions:**

1. **Order the major line PnP enabled device.**

2. **Click the Select Options link to order the optional license (PNP license).**

**Note:** The selection of the PnP license option will trigger a requirement to assign a Smart Account at the device level.
CCW Ordering of PNP Device (NETWORK-PNP-LIC)

Step by Step Instructions:

1. In the Option Selection tab, any applicable items appear below the Configuration Summary. Click the Network PnP License option class to access the PnP license option.

2. A PNP option item will appear to the right of the Configuration Summary. PNP option items require a Smart Account, which is noted in the warning message above the option item and next to the SKU as SA. Select the option item to configure.

3. Upon completing the configuration, you will receive applicable warning/error notifications based on configuration selections.

Note: There is also a minimum iOS requirement for each device type. These can be found here in Tables 1, 3, and 4: (http://www.cisco.com/c/en/us/td/docs/solutions/Enterpris e/Plug-and-Play/release/notes/pnp-release-notes14.html).
CCW Ordering of PNP Device (Smart Account Assignment)

Step by Step Instructions:

The screenshot shows the two ways of assigning Smart Accounts:

1a. Assign the Smart Account at the order level by clicking the **Assign Smart Account** link.

1b. Assign the Smart Account at the line level by clicking the **Assign Now** link below the line item name.

2. After clicking one of the options to assign a Smart Account, a screen will appear with two options:
   - If you already have a smart account, type the name of the Customer Smart Account to assign the device to.
   - You can also request Smart Accounts from the order directly.

3. Click **Assign** to assign the Smart Account.
CCW Ordering of PNP Device (Order Summary)

Step by Step Instructions:

1. The screenshot shows the **Order Summary** screen. It explains the following information:

   1a. Smart Account has been assigned to the major line PNP device.

   1b. The selection of the PnP license option also requires Smart Account assignment at the PnP device level.
Devices Shown in PNP Connect Portal

The screenshot shows the **Show Log** screen displaying the user information for a device.

The **Message** screen displays the message related to the Cisco user.

**Note:** Once the order is placed with the ship option as PNP, the serial numbers of the devices in the order automatically populate in the customer’s Smart Account.
III. APIC-EM Integration
Cisco Application Policy Infrastructure Controller – Enterprise Module (APIC-EM)

Defining APIC-EM

- APIC-EM is a Cisco software that delivers software-defined networking to the enterprise branch, campus, wireless, and Wide Area Network (WAN).
  - It allows automation of policy-based application profiles. With this module, IT can respond rapidly to new business opportunities.

- The PNP application is pre-installed within APIC-EM:
  - APIC-EM receives PNP requests from Cisco devices and provisions devices based on the predefined configuration and image.
  - By adding the device serial numbers to APIC-EM, a network admin can predefine the configuration and image that needs to be pushed to the device when it sends a request to the APIC-EM.
  - In the APIC-EM as well as PNP Connect service, a device is identified by its serial number.

*Note:* The minimum version of APIC-EM release that supports PNP app is 1.0.0.
PNP Connect Redirection Workflow

APIC-EM 1.4 – What’s New

**Feature**: Auto-register APIC-EM IP to PNP Connect

**Benefits**:

- Previously, an admin needed to manually define the default APIC-EM IP Address for all devices in the PNP Connect redirection service.
- Auto registration eliminates the manual task of mapping devices to the controller.

**Feature**: Cloud Inventory Sync – PNP Connect & APIC-EM

**Benefits**:

- Visibility into devices populated from sale orders (SO#) placed via Cisco Commerce Workspace (CCW).
- Simplifies serial# tracking for device provisioning.
APIC-EM Integration: Configure Smart Account Setting

Step by Step Instructions:

1. In order to sync the APIC-EM Controller as the “default controller” for the PNP Connect Redirection Service, log into the system using existing Smart Account credentials.

2. Click the **Authenticate** button to sync.
In the Cisco Smart Account screen, enter the Smart Account and APIC-EM Controller Profile settings. Check the “Register this controller under default profile” option if you want to make this the default controller for your devices in PNP Connect.

Click the Save button.

The Current Settings are displayed.
APIC-EM Integration: Auto Registration to PNP Connect as Default Controller

Step by Step Instructions:

1. Once the sync from APIC-EM settings tab is completed, the APIC-EM controller profile associated with the corresponding Smart Account displays in the PNP Connect portal.

2. To edit a controller profile, select the profile and click the **Edit** button.

3. The **Edit Controller Profile** dialog box appears. Update and save the settings here.
APIC-EM Integration: Sync Device SNs from PNP Connect

Step by Step Instructions:

1. Navigate to the Devices tab in the PNP application in APIC-EM.
2. In the Devices tab, navigate to the Cloud Synced tab.
3. Click the Sync button to sync all the devices from the PNP Connect portal.
4. The devices will now show up in the Cloud Synced tab in APIC-EM.
APIC-EM Integration: Move Devices to Project

**Step by Step Instructions:**

1. In the **Cloud Synced** tab, select the devices that you want to assign to a project.

2. Click the **Move to Project** button.

3. The **Move to Project** window appears. You can define a name for the project to which you want to assign the device.
APIC-EM Integration: Move Devices to Project (Continued)

**Step by Step Instructions:**

4 The device appears in the **Pre-provisioned** tab with the project that it was assigned to.

### Table

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>Device Name</th>
<th>Serial Number/MAC Address</th>
<th>Device IP</th>
<th>Status</th>
<th>Product ID</th>
<th>Last Contact</th>
<th>Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>4D989C01110001</td>
<td>DVSCE_1M_0101</td>
<td>FL-159240-010104</td>
<td>10.0.0.101</td>
<td>UP</td>
<td>FNDY010104</td>
<td>31/03/2021 14:00</td>
<td>Cloud</td>
</tr>
</tbody>
</table>

![Image of the APIC-EM interface showing device move to project](image-url)
APIC-EM Integration: Assign Configuration or Image to Devices in Project

Step by Step Instructions:

1. Click the **Projects** tab.

2. Select the device to which you want to assign a configuration and/or image.

3. Click the **Edit** button.
IV. Redirect Capabilities
Logging into Cisco Software Central (CSC)

Step by Step Instructions:

1. Log into the Cisco Software Central (software.cisco.com) page.
2. Click the Plug and Play Connect link.

We will now look into the following redirect capabilities:
- Adding Devices
- Adding a profile
- Editing a profile
Plug and Play Connect: Devices Tab

Step by Step Instructions:

The Plug and Play Connect page appears.

If a customer has multiple Virtual Accounts, they can select a Virtual Account from the Virtual Account dropdown.

In this example, we have selected Default.
Plug and Play Connect: Devices Tab (continued)

Step by Step Instructions:

All the devices associated with that Virtual Account will be displayed with the following values:

- Serial Number
- Product ID
- Product Group
- Controller (if associated)
- Configuration
- Last Modified
- Status
- Actions
Device Status Transition in PNP Connect

The following diagram explains the workflow and the different statuses that the device goes through for each workflow.
Device Status Transition in PnP Connect (continued)

Device Status Types

1. **Unconfigured**: Device has been added to the list on Customer account but does not have assigned Controller Profile or Configuration.
2. **Pending (Redirection)**: Device has called PnP Connect and is associated with a Profile.
3. **Contacted**: While waiting for Redirection or Configuration, device is in the Contacted status where the Device is locked so no Edit functionalities can be performed (Contacted status also comes in between # 7 and 8 below).
4. **Redirected**: This means that the Controller Profile Information is sent from PnP Connect to APIC Server and is waiting for confirmation response.
5. **Redirect Successful**: Device was successfully Redirected to the server after validations of Information.
6. **Redirect Failed**: Device has failed Redirection due to some reason.
7. **Pending (Configuration)**: Device is associated to the Configuration.
8. **Configured Successfully**: Device has been successfully Configured with the Configuration.
9. **Failed to Configure**: Device has failed to Configure with the Configuration due to some reason.
10. **Delete in Progress**
11. **Error**
Device Log

Step by Step Instructions:

1. To view the log information for any product, select the product and then click the **Show Log** button under the **Actions** tab.

2. The **Device Log** page appears for the product selected.
Troubleshooting Issues for the PNP Cloud Portal

Common Issues

- Devices can not sync with NTP servers (time-pnp.cisco.com or pool.ntp.org)
  - Possible Cause: Customer firewall may block NTP traffic inbound from Internet
  - Solution: Unblock NTP on firewall or use internal NTP servers

- Device contact PNP Connect but redirection fails.
  - Check on the log for device on PNP Connect portal.
  - Use "show run | s pnp profile" to check on device if there is a pnp profile named “pnp_redirection_profile”.
  - Get “show pnp tech” from device.
Add Devices

Step by Step Instructions:

1. To manually add devices, click the **Add Devices** button.

Users will be able to add devices even if they didn't order the NETWORK-PNP-LIC.

**Note:** There is no step required at Customer’s end in order to add a device.
Add Devices (continued)

Step by Step Instructions:

2 The Step 1: Identify Source page of the Add Device(s) wizard appears.

The users can import a device from a CSV file or enter the devices information manually.

3 Once you have entered the required information for the device, click the Next button.
Add Devices (continued)

Step by Step Instructions:

4 The Step 2: Identify Device(s) page appears.

Here, the users can add the identified devices.

5 Enter the following values:
   • Serial Number
   • Base PID
   • Configuration (optional)
   • Description (optional)

6 Click the Next button.
Add Devices (continued)

Step by Step Instructions:

7 The Step 3: Review & Submit page appears.

Review the details entered and click the Submit button.

8 The Step 4: Results page appears. The device has been added successfully. Click the Done button.
Edit Devices

Step by Step Instructions:

1. Select the check box corresponding to the device you want to edit.

2. Click the **Edit Selected** button.
Edit Devices (continued)

Step by Step Instructions:

3 The Edit Devices page appears. From the Select Device Property drop down, select the property you want to edit.

In this example, we have selected Configuration.

4 In the Provide a value text box, enter the new value for the selected property.

5 Click the Apply button.

6 The updated values appear in the table below.
Edit Devices (continued)

Step by Step Instructions:

7. Similarly, for this example, edit the **Controller Profile** property of the device.

8. Click the **Submit** button to complete the process of editing the device.

9. The status has now changed to Pending (Redirection).
Delete Devices

Step by Step Instructions:

1. Under **Devices** tab, select the Device you wish to delete.

2. Choose **Delete Selected**...
Add a Controller Profile

Step by Step Instructions:

1. In the **Controller Profiles** tab, the list of PNP servers is displayed including the following values:
   - Controller Profile name
   - Controller Type
   - Default Virtual Account
   - Description
   - Number of devices tied to each particular PNP Service (Used By column)

2. To add a Controller Profile, click **Add Profile**.

**Note:** A Default Controller is used for VAs, whenever devices come in they will be attached to a Default Controller.

**Note:** You can only edit a controller if there are no devices attached to it.

**Note:** In a given VA you can only have one cloud-hosted and OnPrem VBOND Controller.
Add a Controller Profile (continued)

Step by Step Instructions:

3 The Step 1: Profile Type page of the Add Controller Profile wizard appears.

From the Controller Type drop down, select PNP SERVER.

4 Click the Next button.
Add a PnP Controller Profile

The screenshot shows the PNP UI where the user has the capability to add a PNP controller profile:

The **Step 2: Profile Settings** page appears. Enter the required details in the page.

1. The user can choose Host Name, IPv4 or IPv6 from the Primary Controller dropdown list.
2. The user can also choose a HTTP or HTTPS for primary controller. If the user chooses HTTPS then another field for SSL opens up where the user needs to put SSL certificate to proceed further.

3. Click the Next button.

Note: A user can add a trailing dot to the Host name.
Add a Controller Profile (continued)

Step by Step Instructions:

8 The **Step 3: Review** page appears. Review the details entered on the page.

9 Click the **Submit** button.

Review the following options to make sure they are correct before you Submit the changes.

**Profile Type:**
- Controller Type: PNP SERVER

**Profile Settings:**
- Profile Name: TESTING
- Description: This is a testing profile
- Primary IPV4 Address: 121.1.1.1
- Primary Protocol: http
- Primary Port: 80

Click the **Submit** button.
Add a Controller Profile (continued)

**Step by Step Instructions:**

10 The **Step 4: Confirmation** page appears. The controller profile has been created successfully.

11 Click the **Done** button.

12 The profile added appears on the main page.
Add a Controller Profile – SD WAN

Step by Step Instructions:

If you’re adding a Controller Profile for a SD WAN product, you follow the same steps as you would with a PNP Server Product except you select a different controller type.

1. The Step 1: Profile Type page of the Add Controller Profile wizard appears.

2. From the Controller Type drop down, select VBOND.

2. Click the Next button.
Add a Controller Profile – SD WAN (continued)

Step by Step Instructions:

3. The **Step 2: Profile Settings** page appears. Enter the required details in the page. Note that the details required for VBOND differ from the previous details required for PNP Server.

4. The user can choose ‘Multitenancy’ as ‘Yes’ and it shows another field for ‘SP Organization Name’, as shown in the screenshot.

5. Click the **Next** button and then follow the normal process noted in the slides above for PNP Server.
Step by Step Instructions:

SD WAN users will need to download a provisioning file, which can be found under **Controller Profiles** tab, **Provisioning File**. It will be visible only next to the **VBOND** profile.
Add a Controller Profile - WLC

Step by Step Instructions:

If you’re adding a Controller Profile for a WLC product, you follow the same steps as you would with a PNP Server Product except you select a different controller type.

1. The Step 1: Profile Type page of the Add Controller Profile wizard appears.

2. From the Controller Type drop down, select WLC.

2. Click the Next button.
Add a Controller Profile - WLC

Step by Step Instructions:

3. The Step 2: Profile Settings page appears. Enter the required details in the page. Note that the details required for WLC differ from the previous details required for PNP Server.

4. Click the Next button and then follow the normal process noted in the slides above for PNP Server.
Customer Actions

- Log into the product in vManage, and manually click on Sync in order to sync their products.
- For On-Prem (Self-hosted) vManage, the Customer or Partner needs to login to PnP, download the new SN file and add it to the On-Prem vManage.
- For a partner led 3-way swap, the replacement shipped device is not automatically provisioned.

SD WAN Specific

*Note: Once the replacement is shipped, the data is captured in C3 and updated. It gets passed to supply chain.*
Edit a Controller Profile

Step by Step Instructions:

1. Select the profile you wish to edit and click the **Edit Selected** button.

**Note:** Each Virtual account will have different profiles associated with that account.
Edit a Controller Profile (continued)

Step by Step Instructions:

2 The Step 1: Profile Settings page appears of the Edit Controller Profile wizard. Here you can edit the following values:
   - Controller Profile Name
   - Description
   - Default Profile
   - Primary Controller
   - SSL Certificate

Once you have made the necessary updates, click the Next button.

Note: In the primary controller section, you have an option to provide the Host Name (such as cisco.com) and also another layer of security (HTTPS) for the profile.
Edit a Controller Profile (continued)

Step by Step Instructions:

4. The Step 2: Review page appears. If you see any inaccuracies on this page, click the Back button and make the required corrections.

5. Click the Submit button.

6. Once you click the Submit button, the Step 3: Confirmation page appears showing that your profile has been updated successfully.

7. Click the Done button.
V. Configuration Management
Viewing Configuration Templates

Step by Step Instructions:

1. In the Configuration Templates tab, from the Virtual Account drop down, select the account for which you want to display the templates.

   Once selected, it will display all the templates associated with that virtual account.

2. Click the template for which you want to view the template configuration. In this example, we have clicked ALL_TYPES_OF_VARIABLES. The users can view the following values in the Template Configuration pop up:

   - Variable Name
   - Type
   - Value
   - Default Value
Add a Configuration Template

Step by Step Instructions:

1. In the Configuration Templates tab, click the Add Template button.
Add a Configuration Template (continued)

Step by Step Instructions:

2 The Step 1: Template Settings page of the Template Configuration wizard appears. Here, the users can update the Template settings for the following information:
   - Template Name
   - Template Description
   - Template Code

3 Click the Next button.
Step by Step Instructions:

4 The Step 2: Define Variables page appears.

Here you can update the definitions of each variable one-by-one.

4a Once you have entered the details for one variable, you can click the Next Variable button to update the definition for the next variable.

5 Once completed, click the Next button.
Add a Configuration Template (continued)

Step by Step Instructions:

6 The Step 3: Review page appears.

Here, the users can review the information entered in the preceding pages.

7 Click the Submit button to complete the process.

8 The template added appears on the main page.
To edit a template, select the **Edit** option from the **Actions** column for the template you wish to edit.

A warning message appears. Click the **Edit Configuration Template** button to continue.
Configuration Template Edit (continued)

Step by Step Instructions:

3 The Step 1: Template Settings page of the Template Configuration wizard appears.

Enter the template settings on this page.

4 Click the Next button.
Step by Step Instructions:

5. The **Step 2: Define Variable** page appears. Define the properties of the variables in the template.

6. Click the **Next** button.
Configuration Template Edit (continued)

**Step by Step Instructions:**

1. **Step 3: Review** page appears. Review the template settings and template variables defined on this page.

2. Click the **Submit** button.
Add a Configuration

Step by Step Instructions:

1. The **Configurations** tab lists all the configurations that have been created and whether they were created via a template.

2. Click the **Add Configuration** button.
Add a Configuration (continued)

Step by Step Instructions:

The Step 1: Add Configuration page of the Configuration wizard appears. Here, the users can enter the following information:

- Configuration Name
- Configuration Description
- Configuration Source

You can add the configuration source using either of the two options. Depending on which option you select, the steps of the wizard would change.
In this example, we have selected the configuration as **Create based on a Template**.

Select the required template from the drop down.

Click the **Next** button.
Add a Configuration (continued)

Step by Step Instructions:

6 The Step 2: Variable Values page appears. You can provide values for each of the variables.

7 Once you have made the required updates, click the Next button.
Add a Configuration (continued)

Step by Step Instructions:

8 The **Step 3: Review** page appears.

Users can review the final configuration settings here.

9 Click the **Submit** button to complete the process.

10 The configuration appears in the list of configuration files on the main page.
To edit a configuration, select the **Edit** option from the **Actions** column for the file you wish to edit.

### Step by Step Instructions:

1. To edit a configuration, select the **Edit** option from the **Actions** column for the file you wish to edit.
Edit Configuration (continued)

Step by Step Instructions:

2 The Step 1: Add Configuration page of the Configuration wizard appears.

   Edit the configuration settings on this page.

3 Click the Next button.
Step by Step Instructions:

4 The Step 2: Variable Values page appears. Edit the variable values on this page.

5 Click the Next button.
The **Step 3: Review** page appears. Review the configuration settings and final configuration defined.

Click the **Submit** button.
VI. Network Tab
Network Tab

Step by Step Instructions:

1. In the **Network** tab, you should have a Network ID set. Click **Submit** to send data to ZPROV. The information is used for provisioning of the devices for SD WAN.

In a Cloud-hosted scenario, the components are sent to ZPROV.
For OnPrem installations it needs to be manually defined by customers.

**Note:** It will work only if there are devices under the Virtual Account and there is a Controller Profile in place.
VII. SUDI Details
PnP UI - Devices

Step by Step Instructions:

1. Brownfield Customers can add SUDI supported devices in PnP connect.

2. Customers then Identify the Source. They can import this using a CSV file or Enter the Device Information manually. Click Next.
PnP UI- Add SUDI Devices

Step by Step Instructions:

1. They will enter the **Serial Number**, **BASE PID**, **Controller Profile**, and **Description**.

2. If the Base PID selected is SUDI supported, PnP will automatically populate additional fields. It now asks the user to enter in the **Certificate Serial Number at chassis level** as well as **Add Additional SUDI** details. Click **Save**.
PnP UI- Add SUDI Devices

Step by Step Instructions:

5. If the Customer does not input the additional information, it is fetched from the autotest. Click Submit.

6. The Results page will show if the Device was added. Click Done.
Step by Step Instructions:

5a If the Customer decides to add the additional information requested, they will type in the **Certificate Serial Number** and then expand the **Add Additional SUDI box**.

6a The **Add Additional SUDI** box asks the Customer for the SUDI Serial Number and the Certificate Serial Number. The Customer must then click on the **plus button** which will populate the results below. Click **Save**. **Submit**.
PnP UI - Devices

Step by Step Instructions:

7 The Customer can now see the device in their Devices tab. When the Serial Number is clicked on, they see the device information.
PnP Ui- Device Info

Step by Step Instructions:

1. On the device, Hyperlink is shown. Click on it to view the SUDI details.

2. Once the User has seen the information, they can move onto the Controller Profiles tab.

Note: The serial number should be available in Auto Test. For Greenfield, if the order comes from ccw, the sno gets added in PnP UI. In case it is not available then the device will not be added in the PnP UI and a ticket will be raised in AutoTest saying that the order is not available in AutoTest. Then the AutoTest team will take care of it.

For Brownfield, there is no validation of the serial number but if the SUDI details are not getting retrieved, then an alert will be displayed saying that SUDI is not available for this device. But, it is equal to having a normal device and will be displayed in the PnP UI and can be configured to the V Bond profile. This serial number should be equal to the chassis number in AutoTest. If the Vbond profile is not created in the respective virtual account then an email notification will be sent to Cisco support.
Creating Devices without SUDI

The user can add devices without entering SUDI details while creating a device. For devices created without SUDI, there will be a alert shown along the device with a message ‘Secure UDI not available’, as shown in the following screenshot:
Editing and Deleting SUDI/Certificate Serial Numbers

Step by Step Instructions:

1. The user can edit certificate serial number by selecting the device and clicking on Edit button. While in the Selected Device page the user clicks on the Certificate serial number, it opens a text box, as shown in the screenshot, and make changes into it. The user can simply delete all the text to delete the certificate serial number.

2. The user can also edit the certificate serial number from Edit Devices page and click on pencil icon and again click on the certificate serial number text and edit.

Note: SUDI number cannot be edited. The user can delete the SUDI record from here. Only certificate serial Number can be deleted by deleting the text. After clicking on Save button, all the changes get saved.
Logs for SUDI/Certificate Serial Numbers

Step by Step Instructions:

1. When a SUDI record is added to a device, "SUDI "XXXX" is added" is displayed.
2. When a SUDI record is deleted from a device, "SUDI "XXXX" is deleted" is displayed.
3. When a SUDI record or a Certificate Serial Number is modified alone, "SUDI "XXXX" is edited from BEFORE to AFTER and "Certificate "YYYY" of SUDI "XXXX" is updated from "BEFORE" to "AFTER" is displayed respectively.
4. When Certificate Serial Number is added alone to a SUDI then "Certificate "YYYY" is added to SUDI "XXXX" is displayed.
5. When a Certificate Serial Number is deleted alone from SUDI, then "Certificate "YYYY" is deleted from SUDI "XXXX" is displayed.
PnP UI- Serial File Download

Step by Step Instructions:

1. Through the Controller Profiles tab, the User can click on the Provisioning File button to download the file. This download includes the devices associated to Vbond profile. Before the user can download, they will have to choose what Controller Version they are using.

Customer can choose to download either 17.x or 18.x version of the vManage.
18.X supports both vEdge routers and ISRs and CSRs, whereas 17.x supports only vEdge H/w and vedge S/W.

For steps on downloading and extracting the provisioning file, please go to the Reference section here.
PnP UI

Step by Step Instructions:

1. This order is visible as it has already been set up in the admin page. When the customer places an order with this PID, it means that device is getting a SUDI record.

2. The serial numbers will have an alert if the SUDI details are missing.

Note: Only devices with Vbond capability will be associated with the Vbond profile.
Request a New Smart Account

Note: For the existing functionality, if there is a Controller profile (1) which is already default, or a VBOND profile (2) which is also already default then any router switches orders coming in will be associated with the default controller profile.

In case an ISR Device is ordered in CCW with a VBOND capability then they will be associated with a VBOND profile. The Customer manually can any associate the device with Controller Profile or Vbond at any point of time.
VIII. Add Software Devices
Software Devices

Step by Step Instructions:

1. The user can add Software Devices from Add Software Devices button.

2. Once clicked, the user is taken to Add Software Devices Page and the user can click on Add Software Device button.
Adding software Only devices

Step by Step Instructions:

1. Once the Add Software Device button is clicked, a pop-up opens as shown in the screenshot. The user can enter the Base PID, Quantity, Controller Profile and Description on this page.

The Base PID and Quantity are mandatory fields.

NOTE:

2. A user (SA Admin, VA Admin and VA user) can add only 25 devices for one prefix pid in one VA. If the user tries to add more than 25 devices, it throws an error and devices are not created.

If the user wants to go beyond 25 devices, they need to ask their Cisco Sales Engineer or Account manager to drop an email to sdwan_approvals@cisco.com with the reason and count. Once BU approves, the approved counts will be added. Please note emails from domains other than Cisco.com does not get through.
Adding software Only devices

Step by Step Instructions:

When the user puts the details and click on Next and then on Submit, the record gets saved in the Devices page, as shown below:
Editing software Only devices

Step by Step Instructions:

1. The user can add/edit the Description and Controller profile details from the edit device section.

Note: A user cannot delete a software only device. If the user tries to delete a SW only device, the attempt will fail and the user will receive a message that 'Delete Software vEdge device is not allowed'.

- PnP only supports only 3 types of software Routers.
  - vEdge Cloud (VEDGE-CLOUD-DNA)
  - Virtual ISR (ISRv) and
  - CSR (CSRv)
IX. RMA
Return Material Authorization (RMA) user experience changes

When an Return Material Authorization (RMA) event is initiated and a device is identified as defective, an alert will appear on the device when a Return Material Authorization is initiated, as shown in the following screenshot:

Note: A defective device is the device for which the claim is raised by the customer for exchange. A replacement device is the device that the customer gets as replacement of the defective device.

Logs:
In addition to the above, log messages will be added for the defective and replacement device as detailed below:

1. Defective device: “The system identified this device to be defective as part of an RMA request that Cisco received: RMA Number - xxxxxxxxxx”

2. Replacement device: “Device added to virtual account “<VA Name>” as part of an RMA request that Cisco received: RMA Number – xxxxxxxxxx”
X. Certificates
Certificates

Crypto PKI is the capability for PnP connect UI portal for user to configure Certificate Signing Request (CSR). Certificates allows customers to authenticate devices and profiles in PNP for provisioning process.

The Cisco Admin, Cisco Support, Smart Account admin, Virtual Account Admin can access the Certificates tab in the PNP portal, as shown in the following screenshot:
After clicking on Certificates tab, the user is taken to the Identify Certificate tab where he can fill in details like Certificate Name, Certificate Signing Request, Validity Period and Description, as shown in the screenshot.

**Step by Step Instructions:**

1. After clicking on Certificates tab, the user is taken to the Identify Certificate tab where he can fill in details like Certificate Name, Certificate Signing Request, Validity Period and Description, as shown in the screenshot.

---

**Identify Certificate**

Enter Certificate details and click Next to proceed to the next step.

- **Certificate Name**: TEST
- **Certificate Signing Request**: Content of the certificate signing request
- **Validity Period**: Three Months
- **Type**: GO-WAN
- **Description**: Max characters not to exceed 256

---

**Generate Certificate**

1. **STEP 1**: Identify Certificate
2. **STEP 2**: Review & Submit
3. **STEP 3**: Results
After all the details are filled without any errors, the user clicks on the Submit button and the certificate is created.

After clicking on the Submit button, the Certificate is shown in the Certificates tab.

A user can add up to 100 certificates per Virtual Account.

The user can delete a Certificate by clicking on the Delete button in the Actions menu.
Certificates

Once the certificate gets successfully created, and status is Completed, the user can download the certificate from ‘Actions’ menu.

The downloaded file is .cer file which has validity details of the certificate. This validity matches the validity period entered while creating the certificate.
XI. SDWAN NETWORK HUB
Cat9k - SDWAN Network Hub

Cat9K can’t be associated with vBond, hence a Tag for Cat9k Clouddock capable devices is created which has rules to automatically include any device that is tagged as Clouddock to sync back with vManage.

The user clicks on Add Devices button, and in the Identify Device page, after entering the Serial Number and Base PID, the SDWAN Type Field and dropdown appears for the related PID. The use can choose Cloud Dock from the drop down and click on save.

Once the details are saved without any errors, the Device can be seen in the Devices listing page with the tag.
The screenshot shows the PNP Connect UI where the SDWAN supported device is added with a tag of cloud dock.
XII. Manage External Virtual Account
Manage External Virtual Account

The button “Enable External Management” is used if Customer wants to have an External Account to manage their devices.

When the Button is clicked the Account goes through a clean up activity.

Once Account is enabled for external management, view of the account will be restricted to only devices and device logs.
"Manage External Virtual Account" tab gives the ability to claim other virtual accounts of users, who want their devices to be managed.

The user claiming the virtual account to manage the devices should have access to the claimed account. For more information about access please click here.

Once an Account has been claimed for management, view of the User who is managing the new Customer Account.
XIII. PnP Help "FAQ" tab update
PnP FAQ Help Link

- A new Help link is added which redirects to a new pdf with FAQs included

The screenshot shows the PNP UI where the user can click on ‘Help’ button and a pdf FAQ file opens.
XIV. References
## References

<table>
<thead>
<tr>
<th>Reference Material</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage your Cisco Plug and Play Connect</td>
<td><a href="https://software.cisco.com/">https://software.cisco.com/</a></td>
</tr>
</tbody>
</table>

For any support, please contact [pnp-cloud-support@cisco.com](mailto:pnp-cloud-support@cisco.com).
Serial File Download

Step by Step Instructions:

1. After choosing the version, the user can click on Download button and the file gets downloaded as .viptela extension, as shown in the screenshot.

   For MAC users, the extension can be changed to .zip from .viptela and file can be extracted.

   The user can use any open-source unarchiving tool for extracting the file.

2. The user can extract the .viptela file.
   
   the extracted folder contains the following files:
The content of the file will be available in extracted file viptela_serial_file.

The extracted file shows the details of the devices including their Serial number, chassis number, SUDI, certificate serial numbers as shown in the screenshot.
## Version History (July 2018)

<table>
<thead>
<tr>
<th>Slide #</th>
<th>Details</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>74 - 82</td>
<td>SUDI Details (Secure Unique Device Identity)</td>
<td>JULY 2018</td>
</tr>
</tbody>
</table>
## Version History (Mar 2019)

<table>
<thead>
<tr>
<th>Slide #</th>
<th>Details</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>42-53</td>
<td>Add/Edit Controller Profiles</td>
<td>Jul 2018</td>
</tr>
<tr>
<td>81-82</td>
<td>Serial File Download</td>
<td>Jul 2018</td>
</tr>
<tr>
<td>85-86</td>
<td>Editing and Deleting SUDI/Certificate Serial Numbers</td>
<td>Jul 2018</td>
</tr>
<tr>
<td>87-89</td>
<td>Adding/Editing Software Only Devices</td>
<td>Aug 2018</td>
</tr>
<tr>
<td>90-93</td>
<td>RMA</td>
<td>Sep 2018</td>
</tr>
<tr>
<td>94-97</td>
<td>Crypto PKI</td>
<td>Oct 2018</td>
</tr>
<tr>
<td>99-103</td>
<td>Cat9k Clouddock</td>
<td>Nov 2018</td>
</tr>
<tr>
<td>104-109</td>
<td>PnP Help &quot;FAQ&quot; tab update</td>
<td>Dec 2018</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Jan 2019</td>
</tr>
</tbody>
</table>