Cisco Network Plug and Play Connect Capability Overview

Customers
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 Cisco DNA-Center or APIC-EM controller.

This presentation talks about the Redirection Capabilities.
Table of Contents

I. Accessing Smart Account
II. CCW Integration
III. APIC-EM Integration
IV. Redirect Capabilities
V. Network Tab
VI. RMA
VII. Certificates
VIII. SDWAN Network Hub
IX. Transfer of Devices
X. Transaction Log
XI. Manage External Virtual Account
XII. PnP Help Tab
XIII. 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**: SA Admins, VA Admins and VA Users will be allowed to access the PnP Connect portal. Previously, only SA admins could access the tool.
Request a New Smart Account

Create Smart Accounts

You can create a new Smart Account for your company or organization, or request an account on behalf of someone else.

Account Creator

Are you authorized to create the Smart Account?

- I have the authority to create the account on behalf of my company or organization.
- Someone else will authorize the creation of the account.

Account Settings

Please provide the name and the domain identifier for the Smart Account.

- Account Name: [Cisco Systems, Inc.]
- Account Domain Identifier: [Cisco.com]

The Account Domain Identifier will be used to uniquely identify the account. The default Account Domain Identifier is based on the email address of the person specified to authorize activation of the account.

Learn More

Continue  Cancel
Request Access to an Existing 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: Vinuta Kasthuri
Email Address: vka@imc.com
Cisco ID: vka
Phone: +1 408 527 9698

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

Account Domain Identifier: 
Submit
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.

* Some of the newer devices like Catalyst 9000 series switches have the PNP license selected by default in CCW configurations.
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.

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. In case of device configurations where this item is selected by default there is a "NETWORK-PNP-NONE" option to undo this selection if the user wants to opt out.

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/Enterprise/Plug-and-Play/release/notes/pnp-release-notes14.html].
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

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

2. The entire **Message** displays above when user hovers over the line if it is wrapped.

**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
APIC-EM Integration Steps

- PnP Connect Redirection Workflow with APIC-EM.
- Configuring Smart Account Settings in APIC-EM.
- Auto-registration of APIC-EM in PnP Connect as the default controller.
- Sync devices serial numbers from PnP Connect to APIC-EM.
- Device Onboarding workflow in APIC-EM.
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 redefine 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.
**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 (continued)

Step by Step Instructions for APIC-EM:

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.
APIC-EM Integration: Configure Smart Account Setting (continued)

Step by Step Instructions for APIC-EM:

3. 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.

4. Click the **Save** button.

5. 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 (contd..)

Step by Step Instructions for APIC-EM:

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. Now your devices are ready to be pre-provisioned (moved to a project, associate with an image and/or configuration file).
Device Onboarding Workflow in APIC-EM : 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.
The device appears in the **Pre-provisioned** tab with the project that it was assigned to.
Device Onboarding Workflow in APIC-EM: 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:
- Add/Edit Devices
- Add/Edit Profile
- Delete Device
- Delete Profile
Plug and Play Connect: Devices Tab

Step by Step Instructions:

3 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. Default Virtual Account can be set up in Manage Smart Account -> Virtual Accounts.

In this example, we have selected Default VA.
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)
- 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.

CCW or Manual

Unconfigured

Redirection

Pending (Redirect)

Contacted

Redirect

Redirect Successful

Redirection Workflow

Failed

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
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.
2. **Pending (Redirection)**: Device has called PnP Connect and is associated with a Profile.
3. **Contacted**: While waiting for **Redirection**, device is in the **Contacted** status where the Device is locked so no Edit functionalities can be performed.
4. **Redirected**: This means that the Controller Profile Information is sent from PnP Connect to APIC/DNA-C 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. **Delete in Progress**
8. **Error**
Device Log

Step by Step Instructions:

1. To view the log information for any product, click the **Show Log** button for any device 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 “pnpx_redirect_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/NETWORK-PNP-LIC-O.

Note: There is no step required at Customer’s end in order to be able to add a device once the Cloud Agreement has been signed by the SA Admin.
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. Use the Sample CSV file to upload the device details with the instructions provided in the file.

3. Or click on Enter Device info manually and click the **Next** button.
Add Devices (continued)

Step by Step Instructions:

4 The Step 2: Identify Device(s) page appears. Click on “+Identify Device..” button. Here, the users can add the identified devices.

5 Enter the following values:
   • Serial Number
   • Base PID
   • Certificate Serial Number (optional)
   • Controller Profile (Optional)
   • Description (optional)
   • Add Additional SUDI (Optional)
     This field appears only if Base PID has been set as SUDI Supported in Manufacturing.
   • Note that Certificate Serial Number field is available at Device(Chassis) level and at SUDI level. Both should have different values as applicable to Device or SUDI.

6 Click the Save and Next button after all required devices have been added.
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.
Add Devices (continued)

Step by Step Instructions:

9. Device(s) added appears on the Devices tab at the top. If SUDI details are available for a device, it appears blue and underlined on hover over.

10. Click on the Serial Number to view the SUDI details.

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

11. For devices created without SUDI, there will be an alert shown along the device with a message ‘Secure UDI not available’,
Another option to add device to the account is to upload CSV File.

Download the Sample CSV File to get the list of fields and instructions.

Follow the instructions given in the CSV File and note that the instructions row should be left intact for the upload and should not be deleted.

User will be able to upload SUDI Number and Certificate Serial Number. If there are multiple SUDI & Certificate Serial number for a given Device, follow instructions.
Add Software Devices

Step by Step Instructions:

1. User can add Software only Devices on Plug and Play Portal by clicking on Add Software Devices button.

2. **Step 1:** User is taken to Add Software Devices Page, click on Add Software Device button.
Add Software Devices

**Step by Step Instructions:**

1. Identify Device pop-up is displayed. User can now enter values as shown in the screenshot. The user can add the device here.

2. Enter the Following values:
   - Base PID (Mandatory)
   - Quantity (Mandatory)
   - Controller Profile (optional)
   - Description (optional)

   Click **Save**.

3. **Step2:** Devices added are displayed for Review & Submit. Click **Next**.

**NOTE:** PnP supports only 3 types of software Routers.
- vEdge Cloud (VEDGE-CLOUD-DNA)
- Virtual ISR (ISRv) and CSR (CSRv)
Adding Software Devices

Step by Step Instructions:

5 Click Submit will display Step 3 Results.

6 Click Done. Serial Number will be generated and device is added to Devices tab in the Virtual Account.

NOTE:

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 the following error and devices will not be 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.
Edit Devices

Step by Step Instructions:

Edit can be done for a Single Device at a time or for Multiple Devices.

1. Select the checkbox corresponding to the device you want to edit or click on the drop down Menu under Actions column (Single only)

2. Click the **Edit Selected** button or Click **Edit** option from the Drop

Multiple Devices can be selected to enable Edit Selected Button as well. However, the Product Family should be the same for all devices in case of bulk edit.

Edit is applicable to both Hardware and Software Devices.
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.
Options available:
• Description
• Controller Profile

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.
In the given example, Description has been edited.
Edit Devices (continued)

Step by Step Instructions:

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

8. Certificate can be edited by double clicking on the Certificate Serial Number column at the Device Level.

9. Click on Pencil Icon will enable user to add SUDI details.

10. Click the Submit button to complete the process of editing the device. Success Message Displayed.

11. The status has now changed to Pending (Redirection) for the device that was edited.

Note: SUDI number cannot be edited. The user can delete the SUDI and add new SUDI. Only certificate serial Number can be edited by double clicking inside the column.
Delete Devices

Step by Step Instructions:

1. Under Devices tab, select one or more Devices you want to delete.

2. Click Delete Selected... Button.

For a single delete of device user can also click on the drop down under Actions Column. Choose Delete.

3. Delete Success message is displayed.

Note: 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'.
Add a Controller Profile

Step by Step Instructions:

1. In the Controller Profiles tab, the list of PNP servers is displayed with the following fields:
   - Profile name
   - Controller Type – (PNP SERVER, VBOND or WLC)
   - Default – devices that come in will be attached to the Default controller.
   - Description
   - Used By - Number of devices tied to each particular PNP Service
   - Download – Provisioning file

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

Note: In a given VA you can only have one cloud-hosted and one OnPrem VBOND Controller
Add a PNP Controller Profile

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.

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

6. The user can choose Host Name, IPv4 or IPv6 from the Primary Controller dropdown list. 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 add SSL certificate to proceed further.

7. Click the **Next** button.

**Note:** 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.

![Add Controller Profile page](image-url)
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 Controller Profiles 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

In case of Cisco Routers ordered via CCW with a SDWAN Configuration (ie PNP-CAP-VBOND in the config), then the devices will be automatically associated with a default VBOND profile if existing in the account.

Note: Customer can manually associate the devices with Controller Profile at any point of time.
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.
Downloading Provisioning file - SD WAN

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 is available or needed only for VBOND profile.

The download includes the devices associated to Vbond profile.

Before the user can download, they will have to choose which 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.
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.

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. Only WLC Servers have Secondary Controller details.

4 Click the Next button and then follow the normal process noted in the slides above for PNP Server.
Edit a Controller Profile

Step by Step Instructions:

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

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
   - Multi-Tenancy – VBOND only
   - Organization Name – VBOND only
   - SP Organization Name – VBOND only
   - Primary Controller
   - SSL Certificate
   - Secondary Controller – WLC

3. Click the **Next** button.
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.
Controller Profile – Show Log

Step by Step Instructions:

1. Select a Profile and click on **Show Log** Button

2. Controller Profile Log is displayed in a new pop-up window. The log captures all the changes that were done on the given Profile.

   Click the **X** button to close the window.
Delete Controller Profile

Step by Step Instructions:

1. Select one or more Profiles and click on **Delete Selected** Button

2. Confirmation is required from User to delete the Controller Profile(s). Click **Yes** to Proceed.

3. If Devices were associated to the Controller Profile, the device will go to unconfigured Status.

Note that in case of VBOND Profile, devices associated to the profile will have to be unconfigured first before deleting the profile.
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*
IX. RMA
RMAs in PnP

Process Flow:

If a Customer needs an RMA, TAC or a Partner will create this in SORT.

Cisco utilizes the claimed defective Serial Number to identify SA

Cisco ships the RMA and provisions it to the Customer Network

Customer logs into the vManage product and clicks “Sync”

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.*
Return Material Authorization (RMA) user experience changes

When customer initiates a Return Material Authorization (RMA), an alert will appear on the device as shown in the following screenshot:

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.
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.

User can generate new certificate using the Generate Certificate button.
Certificates (continued)

Step by Step Instructions:

2 User is taken to Step1 in Generate Certificate Page. Enter the following:

- Certificate Name - Mandatory
- Certificate Signing Request - Mandatory
- Validity Period - Mandatory
- Type – Cannot be changed
- Description

3 When Mandatory fields are entered, Next button is enabled. Click Next.
Step 2 Review & Submit page is displayed. To correct the data use the Back Button. If data is correct, click Submit button.

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

A user can add up to 100 certificates per Virtual Account.
Certificates (continued)

6 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 cannot be associated with vBond, hence a Tag for Cat9k Clouddock capable devices is created which has business rules set 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 user 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.
Cat9k - SDWAN Network Hub

Devices tab shown where the SDWAN supported device is added with cloud dock tag.
XII. Transfer of Devices
Transfer Devices from one Virtual Account to another

The user can transfer devices from one instance of his SA/VA to the same or different SA/VA based on the access for the given user.

1. Click and select one or more devices to transfer.
2. Transfer selected button is enabled.
3. Click on Transfer selected button
Transfer Devices from one Virtual Account to another (contd)

Transfer Device screen is displayed.

3. Select mandatory fields from drop down. List is displayed based on user access.

   Destination Smart Account
   Destination Virtual Account

4. User can delete any device from the current transfer only by clicking on the icon. Note this will not delete the device.

5. Note that show Log messages and SUDI Missing/RMA Alerts from the source account will not be transferred to destination account.

6. Click on ‘Transfer” Button to Initiate transfer of devices. Message displayed that Transfer request has been submitted.
Transfer Devices from one Virtual Account to another (contd)

When Transfer is in progress, Device is locked from any transaction. If Device was associated to any profile it will be automatically disassociated. Click refresh button.

Go to the destination smart account/virtual account. New devices are listed in the devices tab.
Check the Event Log in both source and destination accounts which captures the device details that were transferred.

Click on More displays the list of devices that were transferred in a separate pop up window.

For successful transfer the icon displays green with tick and if there is a failure in transfer for any reason, cross mark in Red is displayed before the device in Source Account Event log (more section).

User can click on icons in the dashboard to filter device display based on success only or failure only or all.
XIII. Transaction Log
Transaction Log

- The Transaction tab captures all transactions related to Device Provisioning for a given order (Hardware with no subscription order, Hardware + Subscription order, Change Subscription, Subscription order with Customer Devices, Disti Hardware Order with Subscription)

1. The transaction log captures the transaction date the order was provisioned in PnP. Last updated transaction will be displayed on top.

2. Click on icon in Quantity column will show all Device information that came as part of the order.

3. Hover over on Status displays all the sub-status applicable for that transaction.
Transaction Details:

Click on Transaction Date displays the Transaction Details tab.

This tab captures the details related to the transaction in sections
- “Transaction Details”,
- “Term Details”,
- “Controller Request Details”
- “Support Details”

Note that all fields will not be available at all times. Fields are displayed depending on the availability of data.
XIV. Manage External Virtual Account
Manage External Virtual Account – End Customer

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, device logs, Event Log and Transactions.
“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.
PnP Help "FAQ" tab update
PnP FAQ Help Link

1. User can access FAQ document related to PnP Connect by clicking on help link.
   Help link is not related to any tab user is in and available at all times.

2. FAQ document opens up in a pop-up window with the frequently asked questions and answers.
To open a case with GLO:

• Send an email to licensing@cisco.com or cdap-support@cisco.com

• In the body of the email, type in “Cisco.com ID:” followed by your CCO ID.

• In the message, include information like SA, SO#, Device details, specific product, questions or issues.

Sample email guideline

• Other teams to contact for urgent issues:

TO: licensing@cisco.com (or) cdap-support@cisco.com
Subject: Certificate issue

Cisco.com ID: deXXXshn
Smart Account: Sample Smart Account
Smart Account domain name: XYZuniversity.com
PAK Number - JMXXXXXXXX145
sales order number- 123456789

Description of the licensing issue faced by the customer.
XV. 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>