Cisco Plug and Play Support Guide for Cisco SD-WAN Products

June 2019

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Contents

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

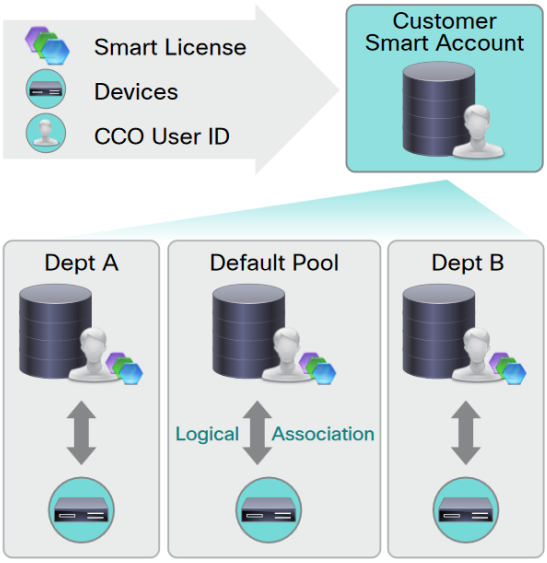
Introduction

The purpose of this document is to go through capabilities that are created on the Cisco® Plug and Play (PnP) portal to support the on-boarding of SD-WAN (formerly Viptela) products. This document will help Cisco SD-WAN customers understand the different steps that are needed to either bring up or debug on-boarding of a Cisco vEdge device or a vBond controller.

Cisco Smart Account and Virtual Account

Introduction to Cisco Smart Account and Virtual Account

After creating a Smart Account, customers can create Virtual Accounts that reflect their organizational departments, then associate licenses and devices with those departments.



Virtual Accounts

- A customer defined construct to reflect company organization, geography, budgeting, or other structure.
- Created and maintained by the customer on the Cisco Smart Software Manager with full visibility to company assets.
- Enable Delegated Authority and Differential Access.
- Flexible, allowing licenses and products to be shared between products (without contacting Cisco TAC!)

Licenses and devices are always explicitly moved, enabled or disabled by the customer administrator.

How Smart and Virtual Accounts are used for on-boarding

Smart Accounts and Virtual Accounts are essential in a successful on-boarding of a vEdge router to its corresponding network.

While placing an order on Cisco Commerce Workspace, a customer can assign the same Smart Account and Virtual Account to the order. They can log in to Cisco vManage (version 18.x and above) to find the Smart and Virtual Accounts (Administer→Setting→Organization Name→View).

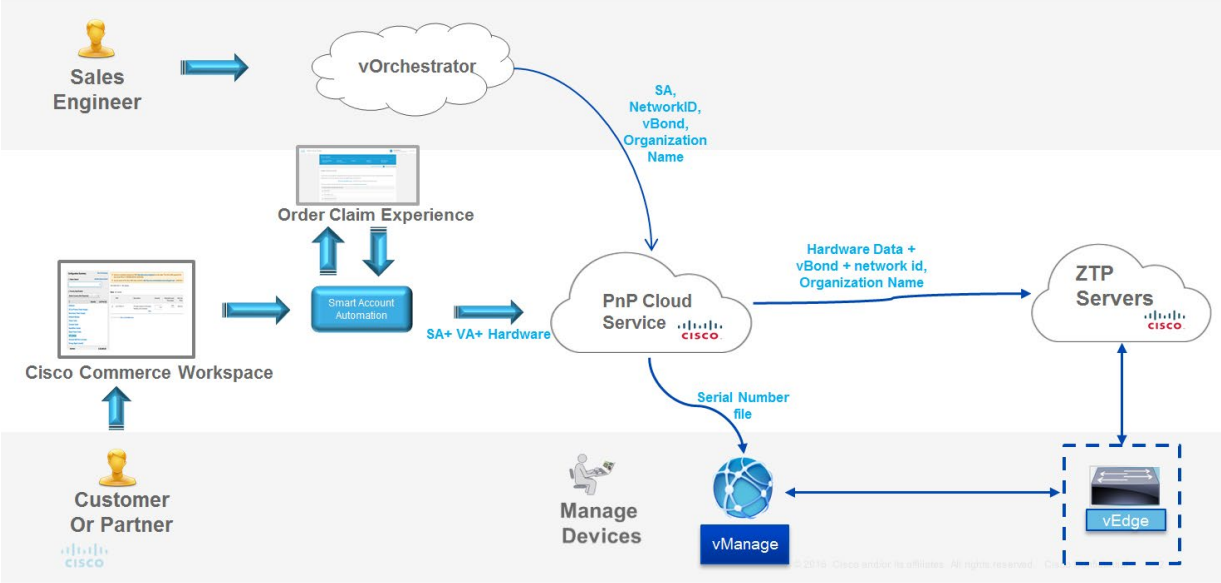
The devices manufactured as part of this order would flow into the Cisco Plug-and-Play (PnP) portal and would be associated to the vBond controller that was pushed by Cisco SD-WAN CloudOps. Once the association is successful, the data is pushed to zero-touch provisioning (ZTP).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

For on-premises deployment

The customer or sales engineer who is helping with the customer's deployment would need to enter the vBond profile information into the Plug-and-Play portal, so that the controller information can be passed to zProv. Steps to set up a vBond controller and how to associate devices to it are demonstrated later in this document.

Figure 1. PnP workflow



Note: A Smart Account and a Virtual Account are non-mandatory fields during ordering. If the values are left blank, the customer would either be assigned system-generated Smart and Virtual Accounts or would be guided through a claiming experience to select the right Smart and Virtual Accounts under his organization. This claiming experience would occur after submitting an order.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Cisco PnP terms

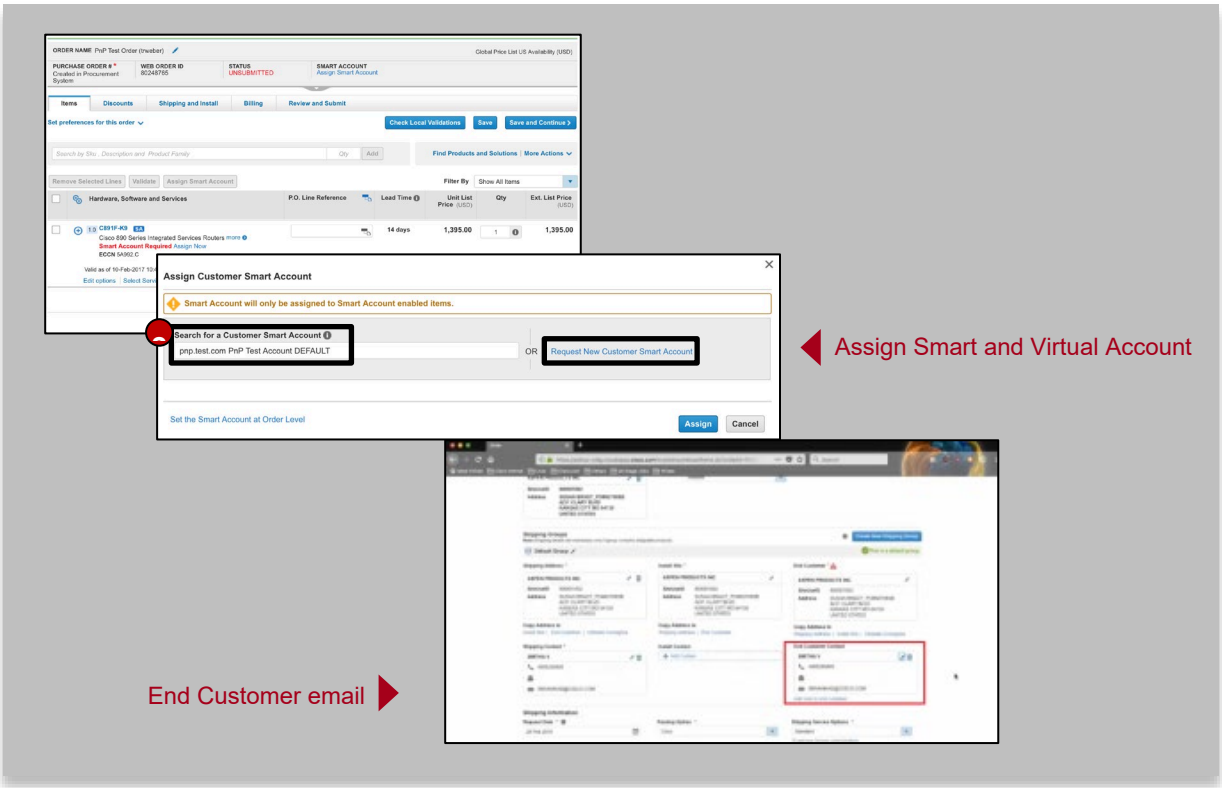
Terms	Description
Network ID	The equivalent of the overlay ID in Viptela. Auto-generated when a profile is present in PnP. Can be edited only when no profiles exist in a Virtual Account. All devices for a given organization name in ZTP should be associated to one network ID.
Organization name	An attribute that vManage used to tie all the controllers together. The organization name is associated to a vBond controller in the PnP portal.
vBond controller	Represents the vBond IP or domain name. Only IPv4 is supported today.
Base product ID (PID)	Hardware product ID that is on the label.
Ordered PID	An ordered SKU that was selected in CCW. In some cases, the ordered PID and base PID can have the same value.
Secure device ID (SUDI)	A secure board ID that is used to validate anti-tampered devices.
International Mobile station Equipment Identity (IMEI) or device IMEI	IMEI information for an LTE-enabled vEdge controller. Both of the values would be the same for vEdge devices.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

On-boarding sequence flow using PnP

For on-premises equipment

1. Place an order in CCW
    - Either the customer or the partner enters the end-customer's email address (mandatory) or the customer's Smart Account and Virtual Account numbers (not mandatory).
    - Serial number information with the Smart Account and Virtual Account is pushed to PnP.

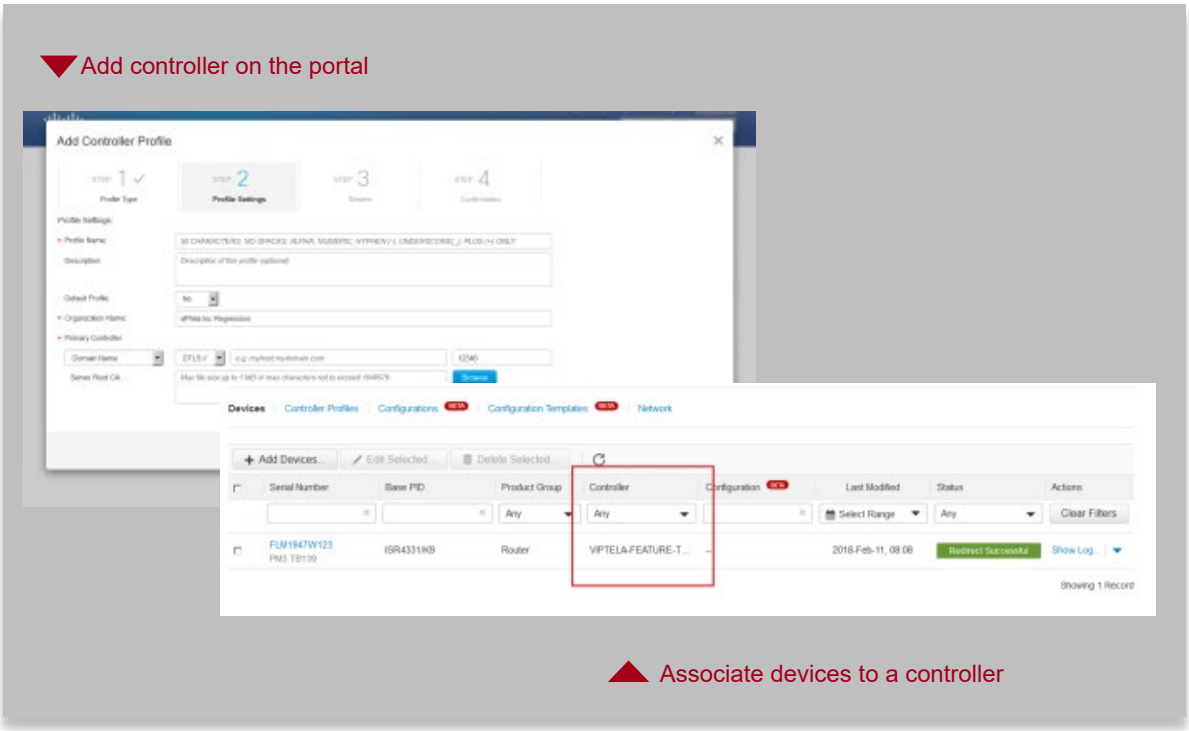


2. Customer on-premises controller
    - Make note of the organization name used to bring up the setup and also the vBond controller IP address or domain name.
    - You will be required to enter this information in PnP.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

3. Define the vBond controller in Plug and Play

- Add the vBond controller profile into PnP under the same Smart and Virtual Accounts used in Step 1 (for on premises).
- The steps to take to add a vBond controller profile are provided later in this document.
- Once the vBond Controller is added, manually associate the device to the controller.

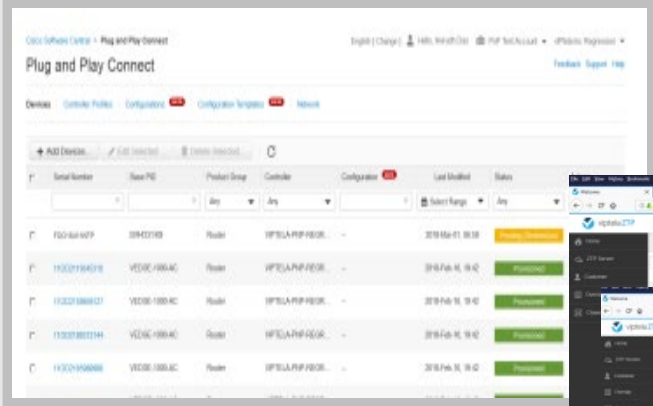


© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

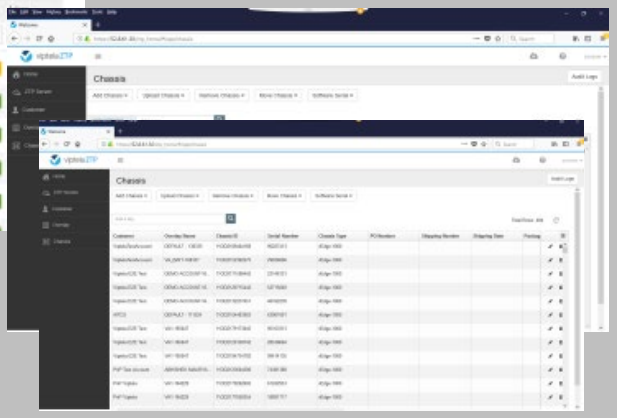
4. PnP data push to ZTP

- PnP will automatically send the data with the vBond controller information, the organization name, network ID, and associated serial numbers to ZTP.

▼ Chassis SNs in PnP from CCW associated to vBond profile from Step 3



▼Overlay data available in ZTP



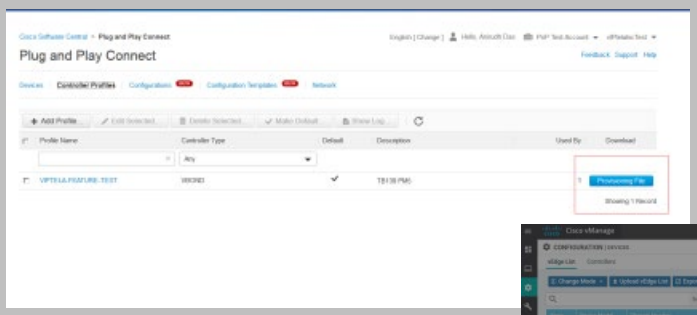
▲ Serial Numbers in ZTP

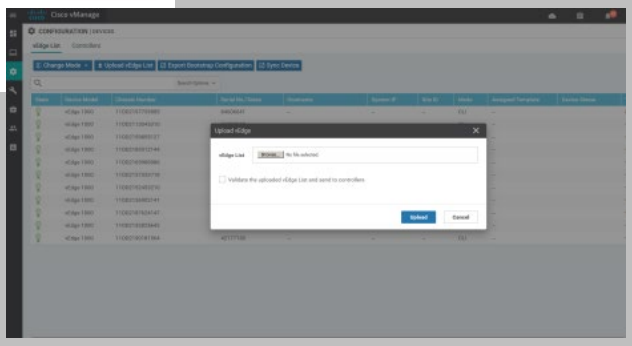
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

5. Upload the provisioning file into vManage

- Download the serial number file, also known as the provisioning file on the PnP portal.
- Upload the file in vManage (version 18.x and above).
- Devices will then be available on vManage

▼ Download Provisioning File from PnP





▲ Upload Provisioning file in vManage

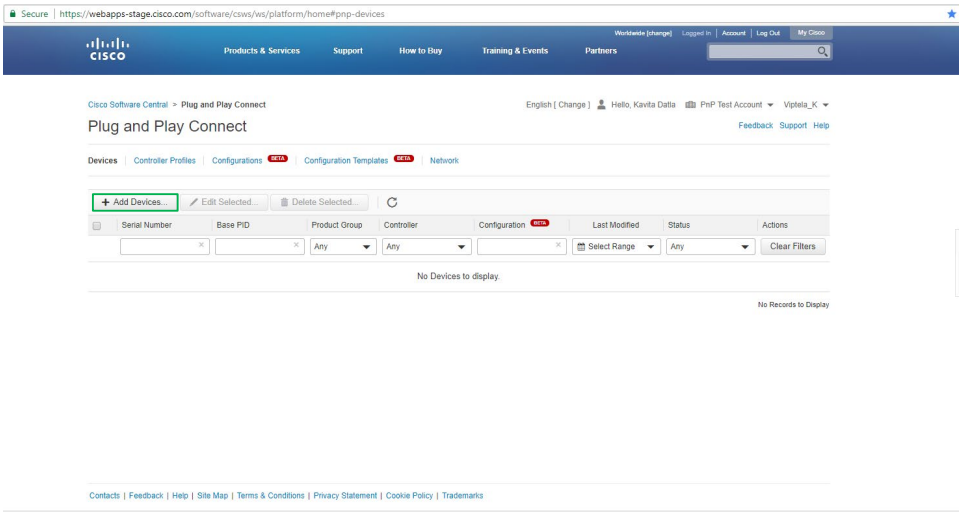
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Device management

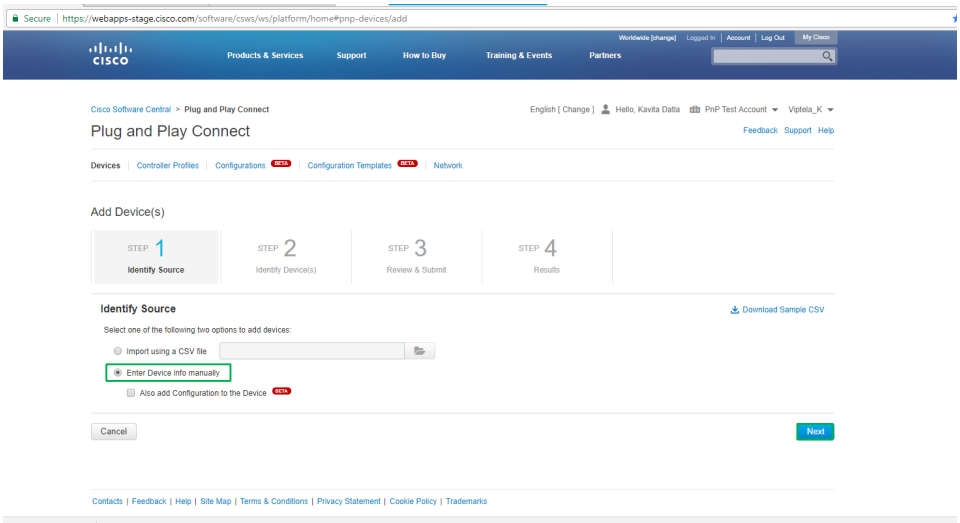
The Cisco PnP portal contains a list of devices that are associated to a given controller. For ease of issue resolution, the PnP portal provides capabilities for device management to support personnel and customers.

Steps to add a replacement device to your Virtual Account

1. Log in in to PnP with the Smart and Virtual Accounts that the user needs to add to the device. Click “Add Device”

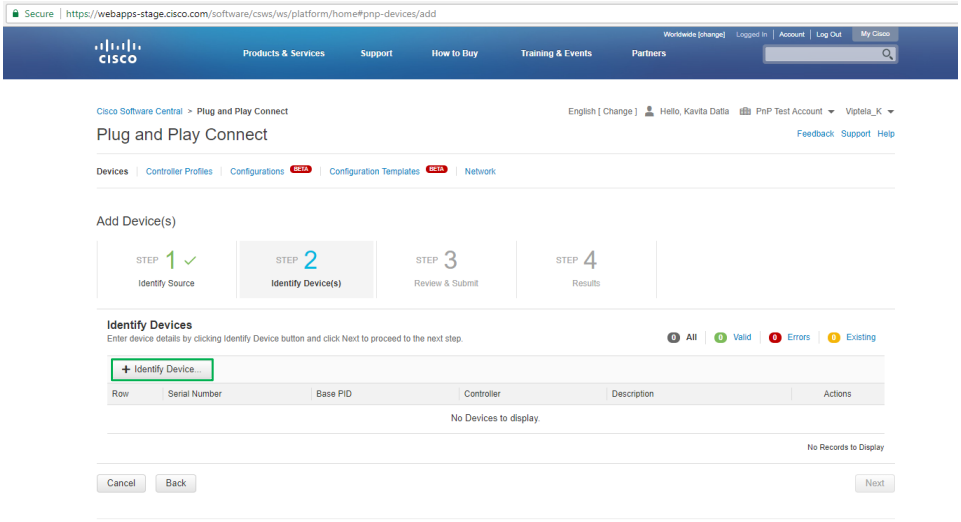


2. Choose “Enter Device Info manually” and click “Next”

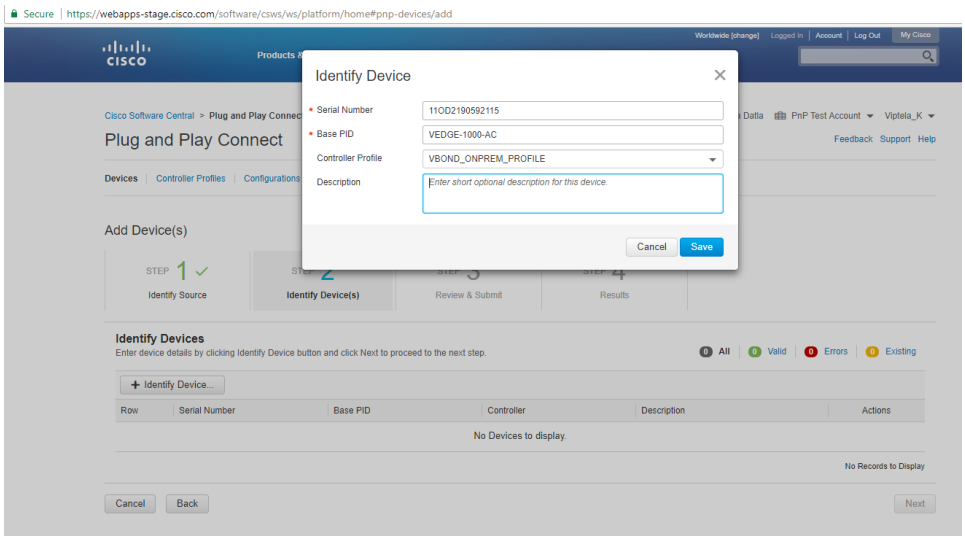


© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

3. Click on “Identify Device”



4. The “Identify Device” screen appears. Enter the device details and click “Save”, as shown in the following screenshot. Choose the base PID in the case where a vEdge device is an orderable PID or label on the hardware router called “Model Name”.



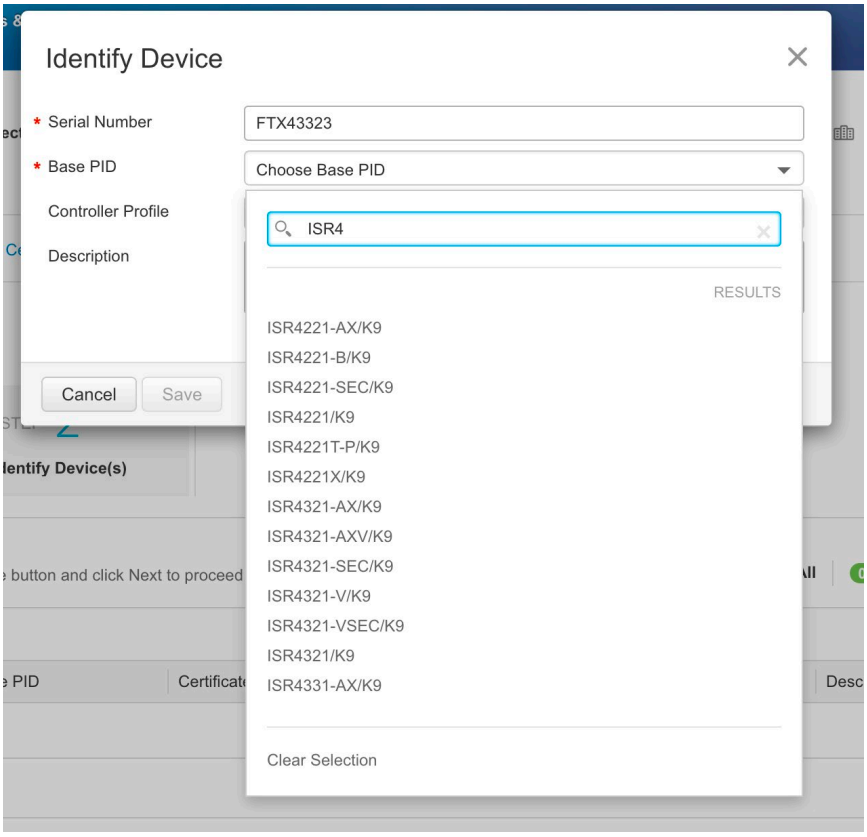
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Note: Cisco ISR 4000 Series routers use two separate serial numbers for the unique device identifier (UDI) and secure unique device identifier (SUDI). For a device with two serial numbers, you must also provide the second serial number in PnP. The device may encounter redirection problems if it is provisioned by PnP using only one serial number. The following steps provide both serial numbers, enabling PnP to provision the device correctly.

a. On the Cisco ISR 4000 Series router, display the two serial numbers (shown in bold in the output below).

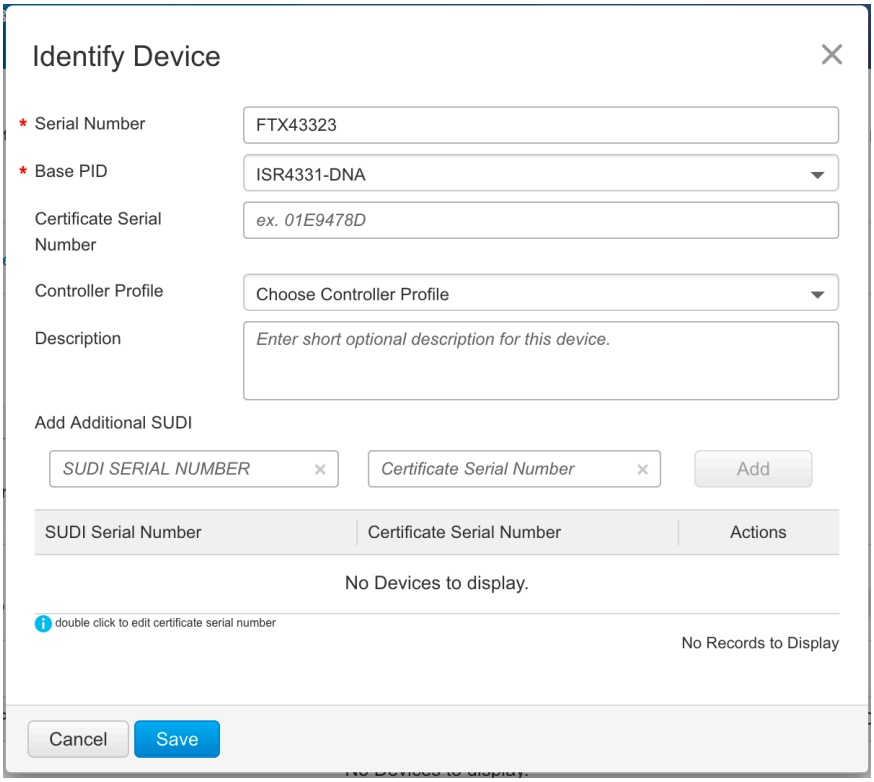
```
ISR-4331#show pnp version
------------------ show pnp version ------------------
PnP Schema Version: 1.0, Baseline Tracking: rel29.1.20190116
Device UDI: PID:ISR4331/K9,VID:V05,SN:FDO2240A1RY
UDI Checking: Yes
SID: AuthOnly:No, MustValidate:No, MustRenew:No
Security Enforced: No, PostReloadPriv'd Profile: N/A
SUDI Certificate: CISCO_IDEVID_SUDI
Device SUDI: PID:ISR4331/K9,SN:FDO22371AM5
```

b. In the "Identify Device" window, enter the PID of an ISR 4000 Series router in the “Base PID” field. When you begin typing, the field provides options based on the typed characters. Select an ISR 4000 Series router. Once the PID is selected additional fields appear in the “Identify Device” window.



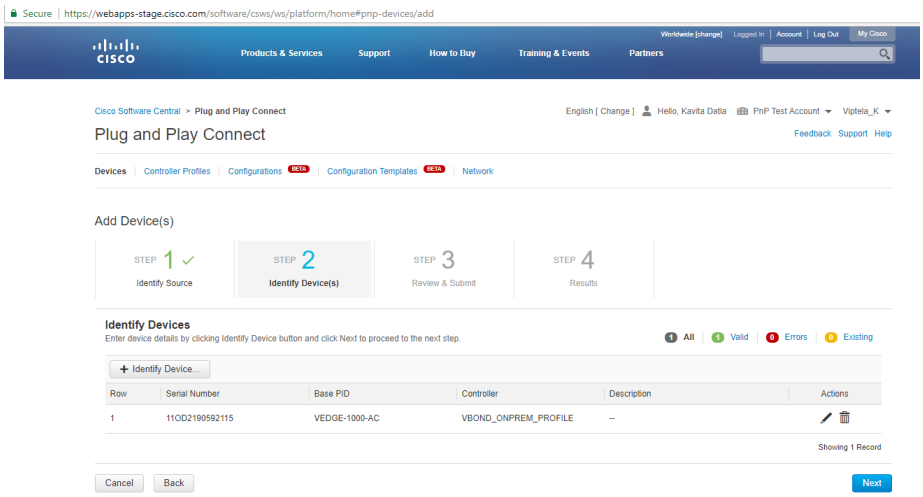
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

c. In the "SUDI Serial Number" field, enter the SUDI serial number that was displayed in a previous step and click “Add.” The "Identify Device" window now contains both serial numbers of the device.



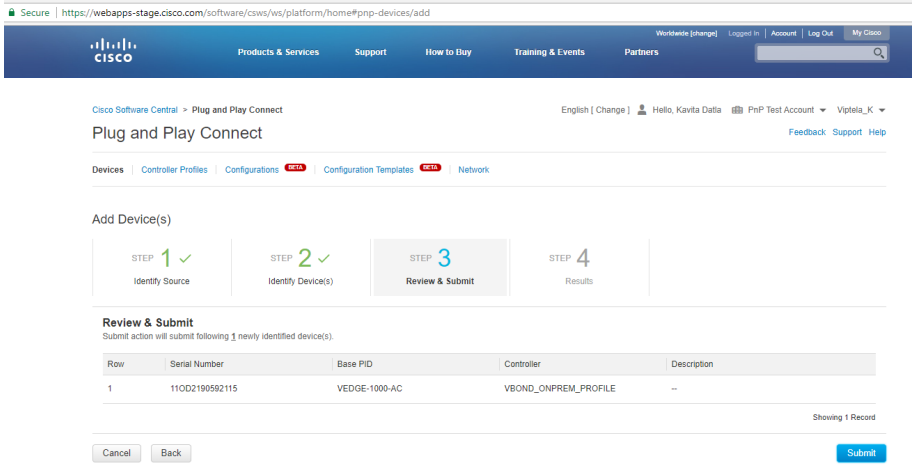
d. Click Save.

5. Click “Next”

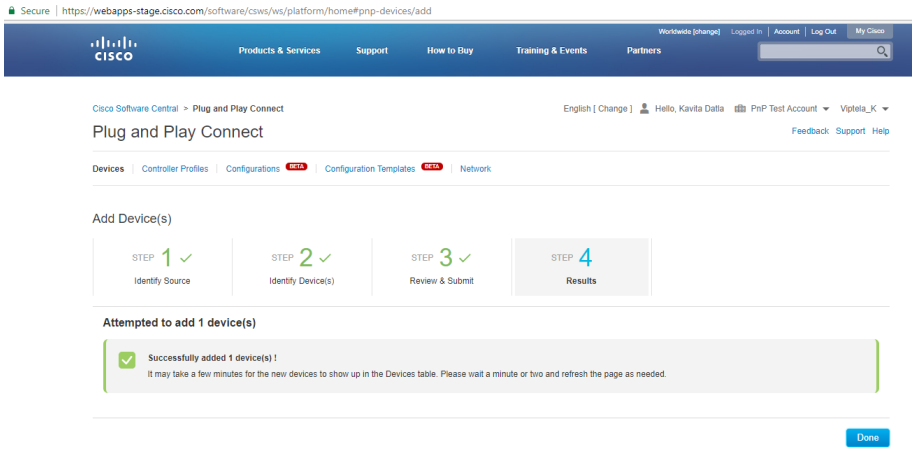


© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

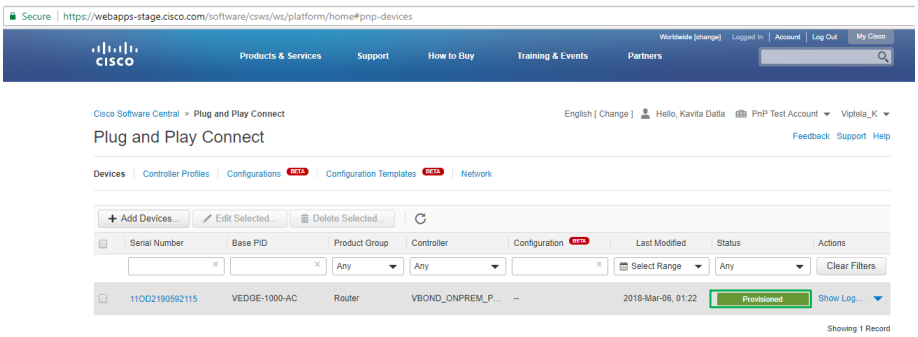
6. Click “Submit”



7. Click “Done”



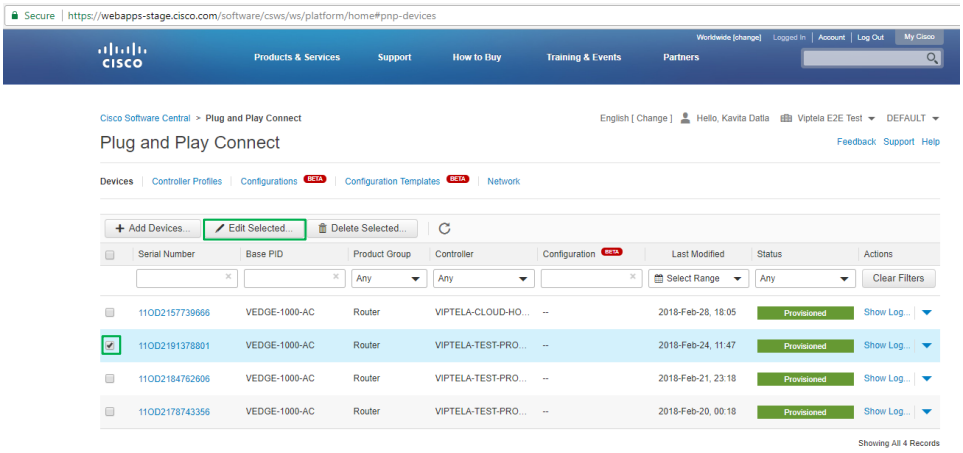
8. Devices will be provisioned automatically since the profile is already present. The status shows as “Provisioned” once the data is sent to ZTP.



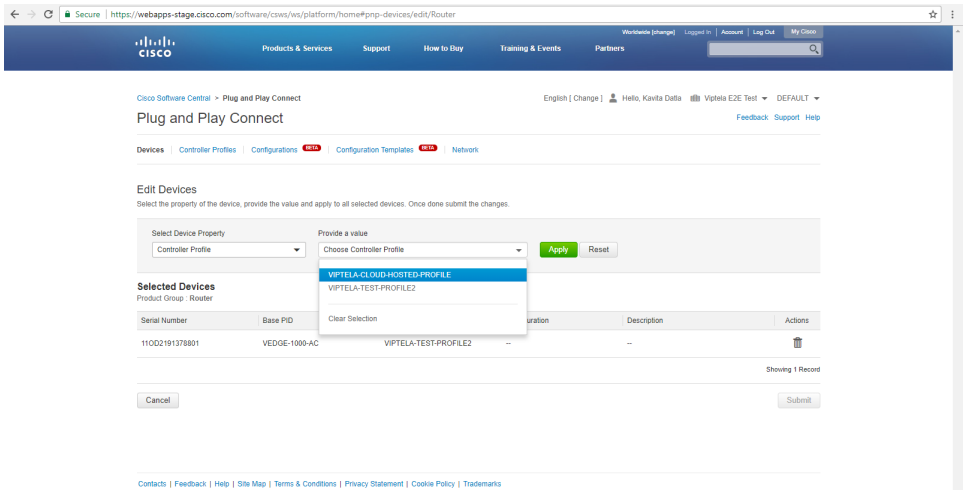
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Associate controllers to a device

1. Select the device under the “Devices” tab and Click “Edit Selected”

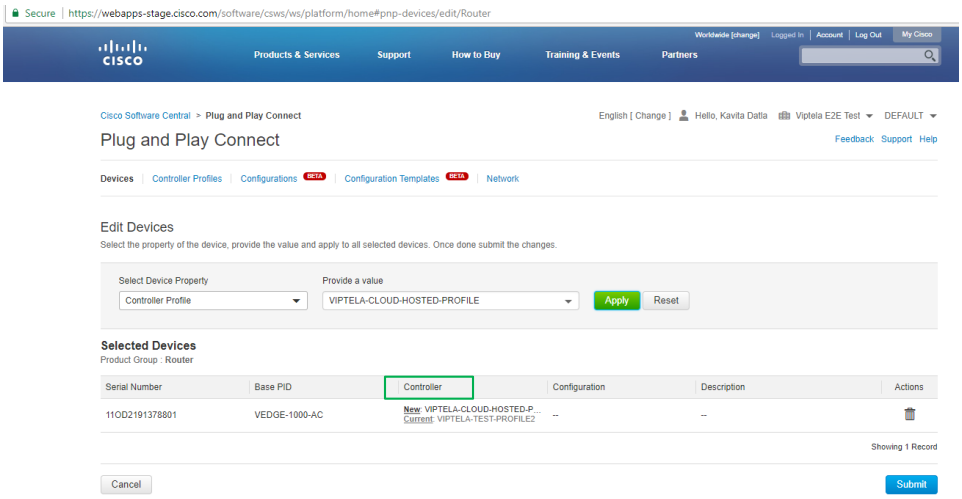


2. Select the profile that the user wants to change and click “Apply”

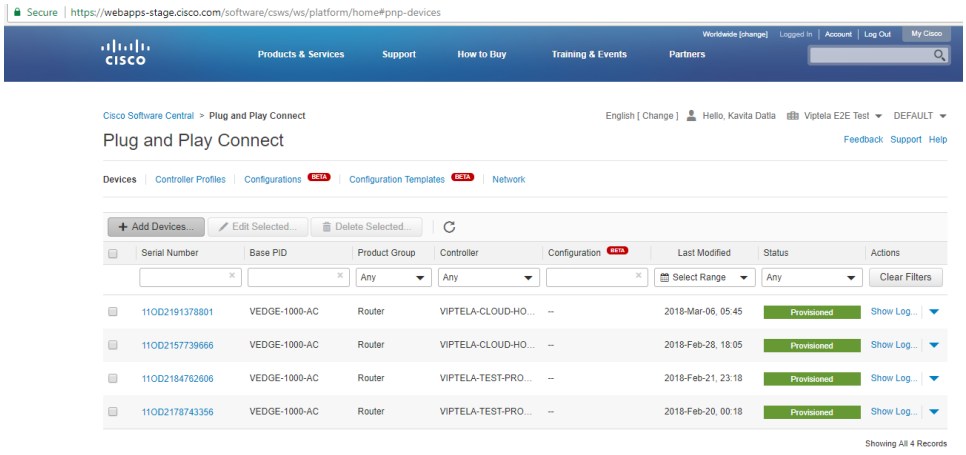


© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

3. The new and old profiles are shown under the “Controller” label



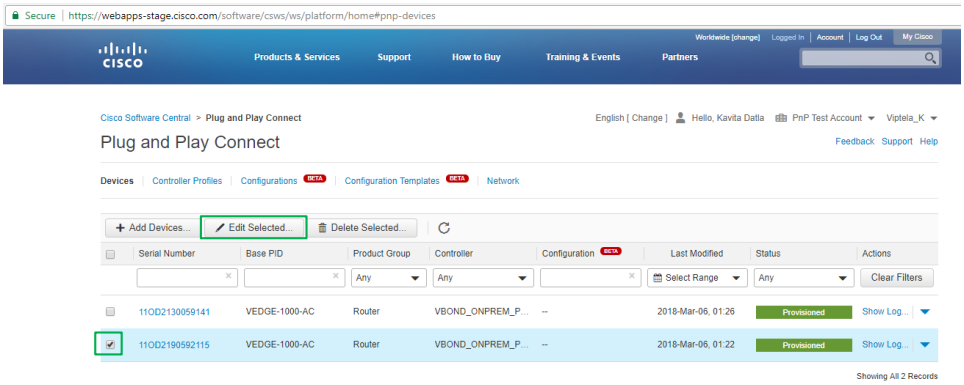
4. Click the “Submit” button. The device is now associated with a new profile (cloud-hosted in this case) as shown in the following screenshot.



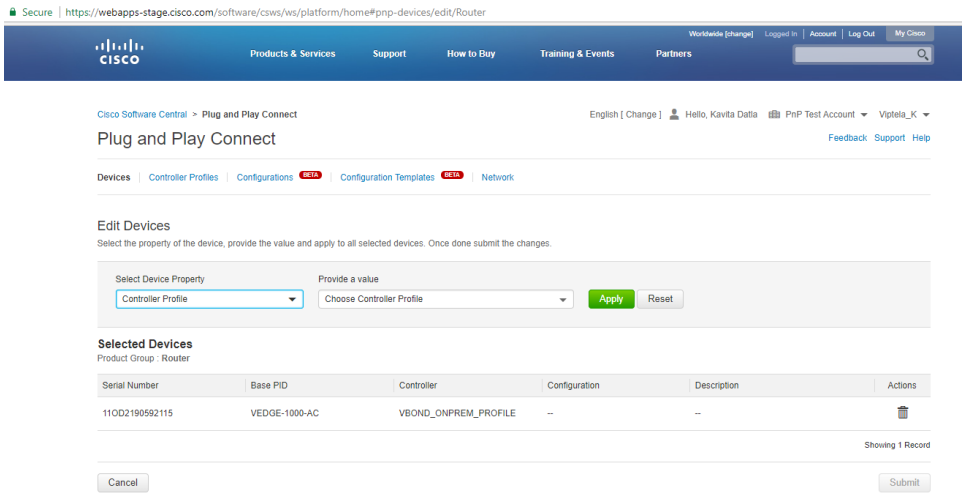
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Un-configure a device (disassociate a device from the controller)

1. Click on the device that you want to un-configure and click “Edit Selected”

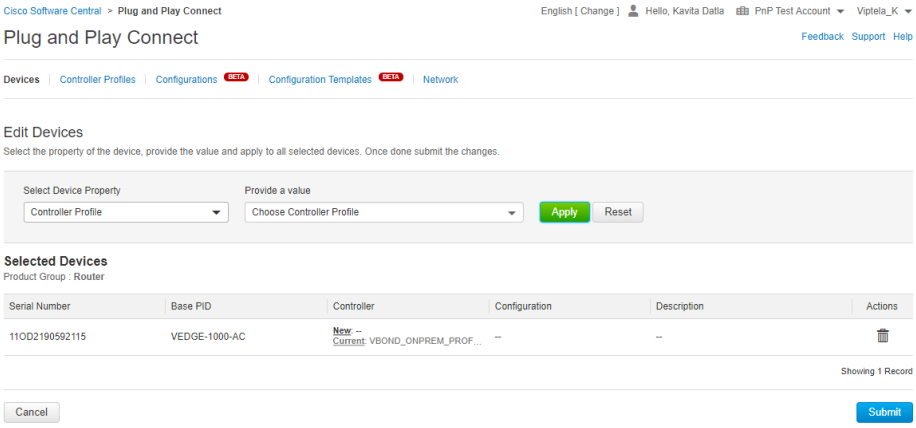


2. Click “Controller Profile” and click “Apply”

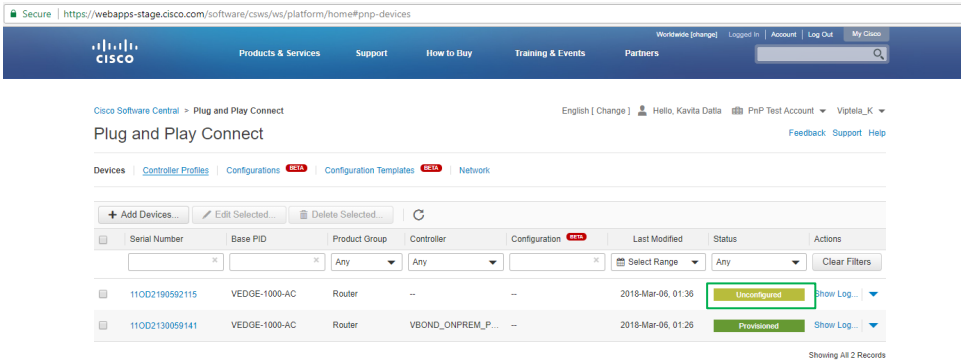


© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

3. The new and old profile will be shown



4. Click the “Submit” button. The device will be shown with an “unconfigured” status on the “Devices” tab as there is no vBond controller associated with it



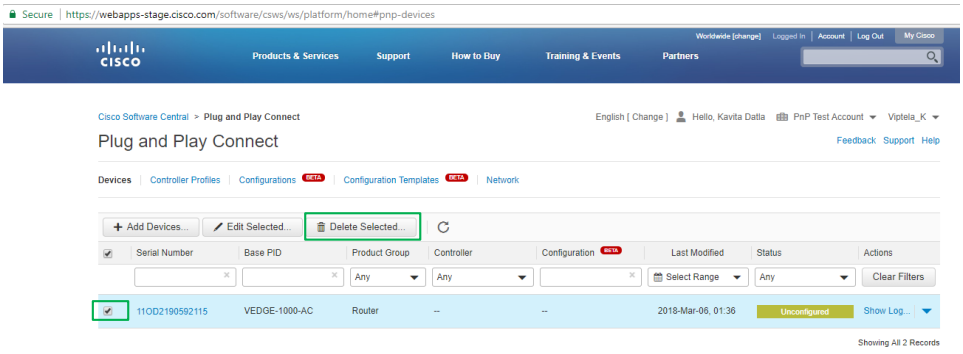
Moving devices from one Virtual Account to another Virtual Account

1. Delete the device from one Virtual Account
2. Add the device into another Virtual Account

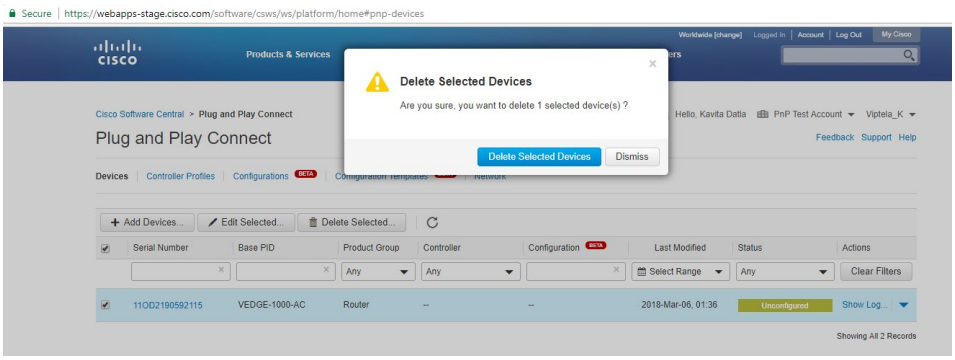
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Delete the device from one Virtual Account

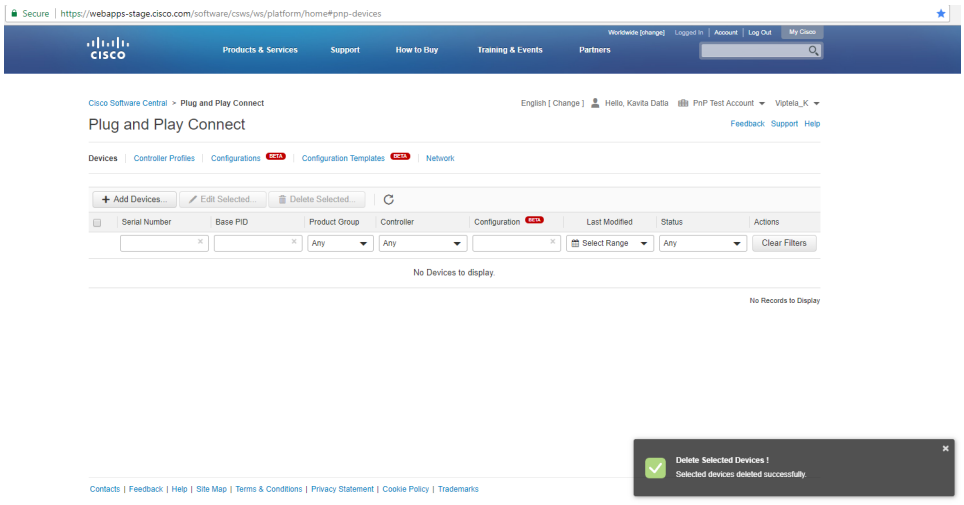
1. On the Devices tab, select the devices that need to be deleted and click the “Delete Selected” button



2. The system prompts a message, illustrated in the following screenshot. Click “Delete Selected Devices”



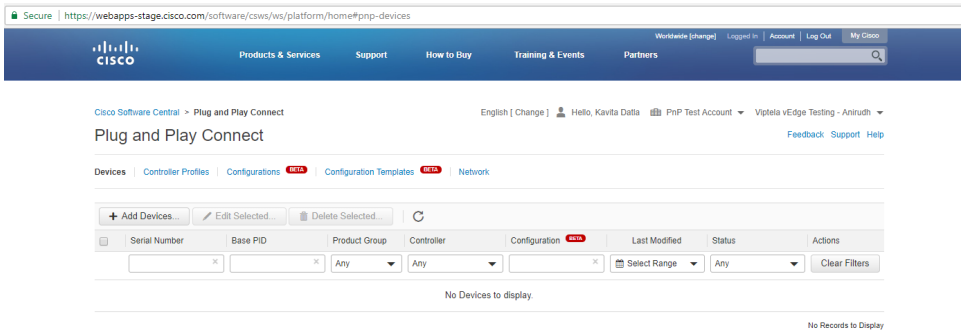
3. Devices will be deleted from the Virtual Account



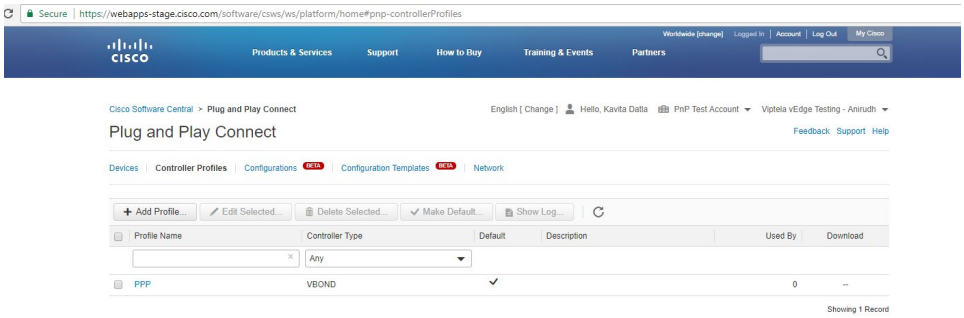
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Add a device into another Virtual Account

1. Choose another Virtual Account where you want to add a device

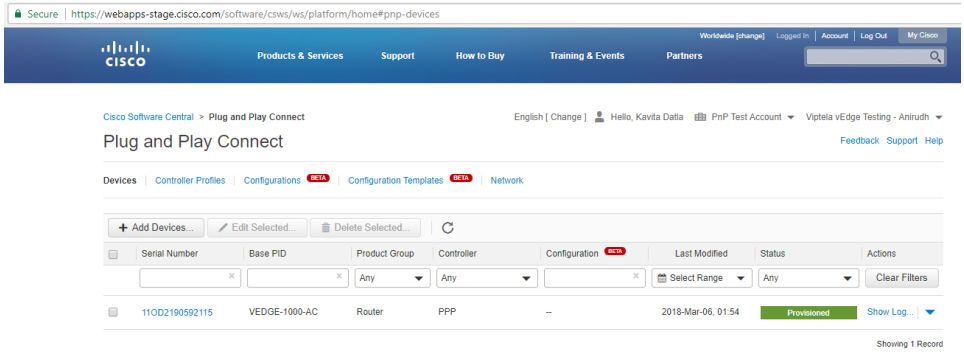


2. Make sure that there is a vBond profile in that account. If not, it needs to be created.



3. Add the device to the Virtual Account (see steps for adding the device).

   The device will be added to the new Virtual Account and be provisioned automatically as there is a vBond profile associated to it.



© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

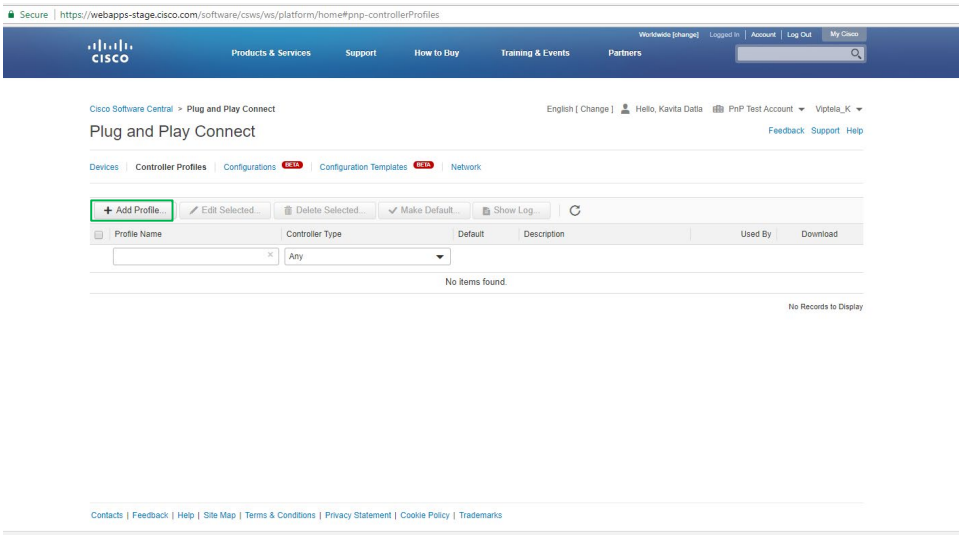
Controller management

The PnP portal allows users with the right access levels to add and modify controllers to help manage their re-direction service.

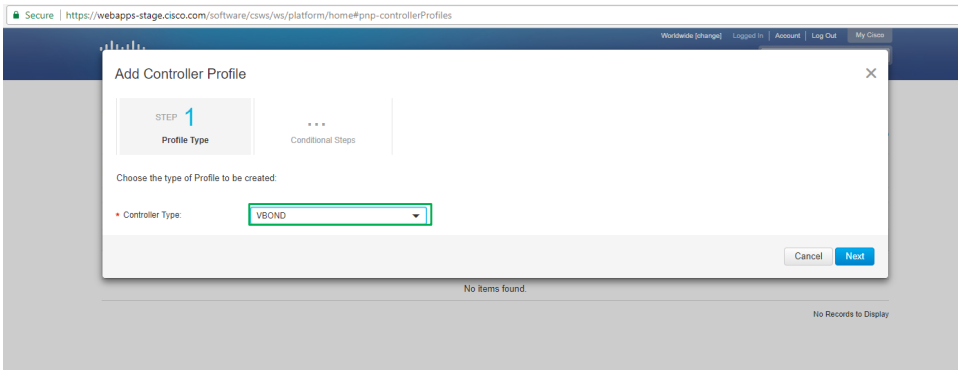
Note: There can be only one cloud-hosted and one on-premises controller in a given Virtual Account. Only one of them can be active.

Add controller

1. On the Controller Profiles tab, click “Add Profile”

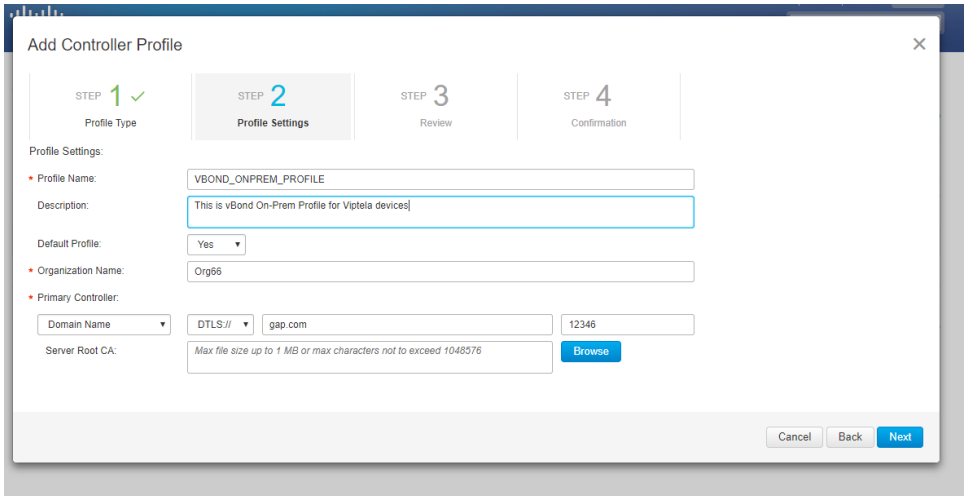


2. Enter the controller type as “vBond” and click “Next”

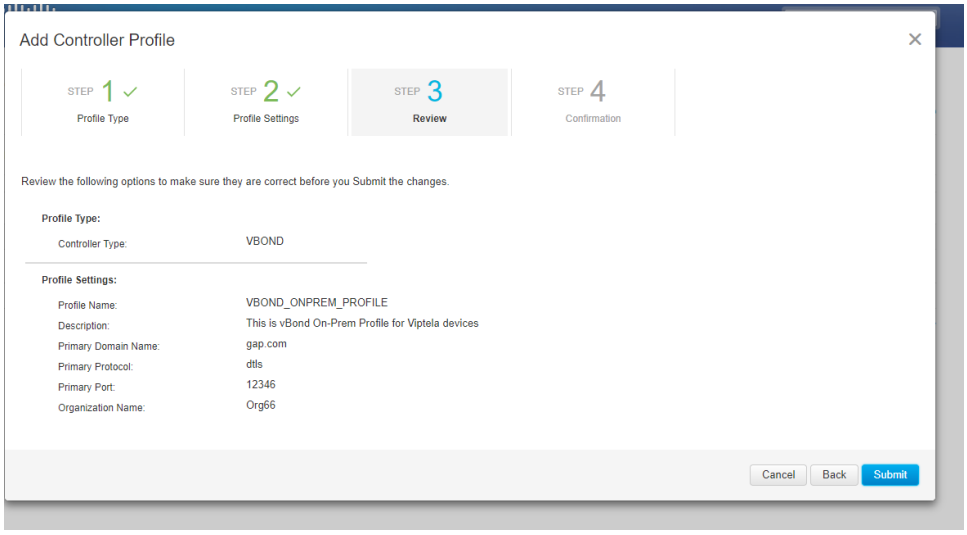


© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

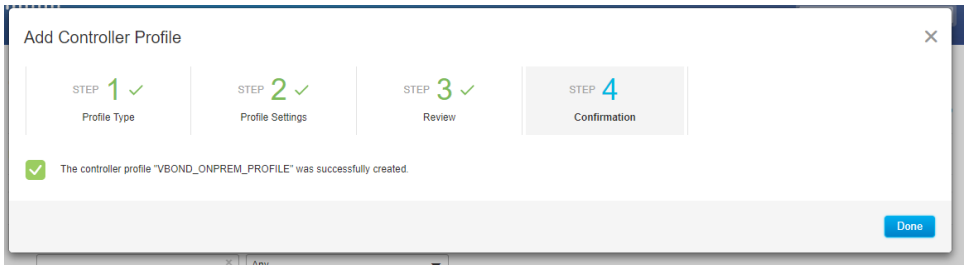
3. Enter the data in “Add Controller Profile” and click “Next”. Enter the organization name used in vManage and the domain/IP address of the vBond controller.



4. The system displays all the vBond Information as in the following screenshot.

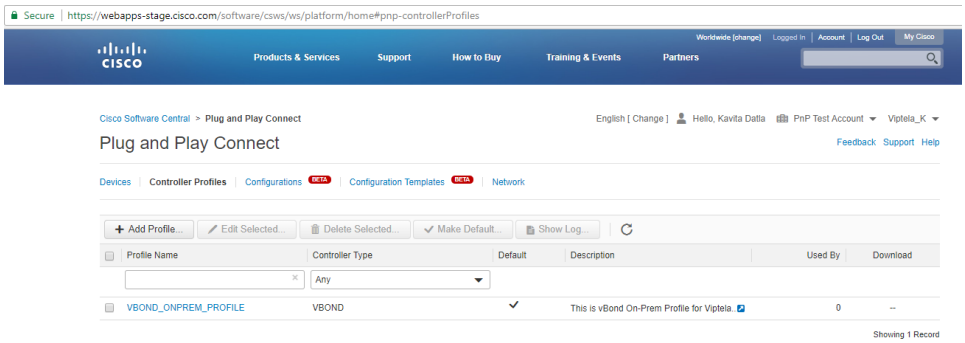


5. Click “Submit”



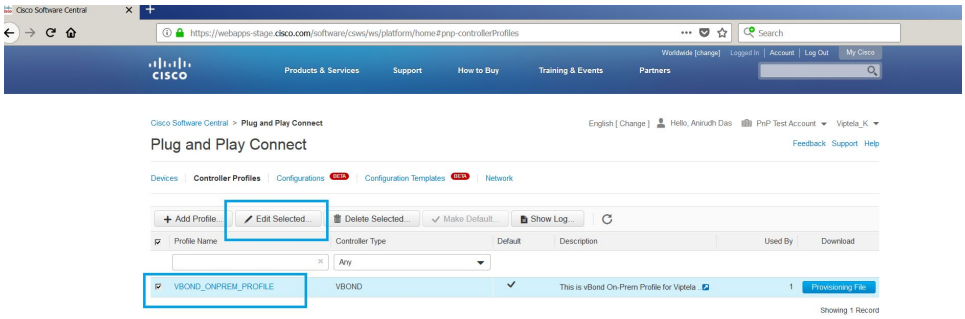
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

6. Click “Done”. The profile is created.



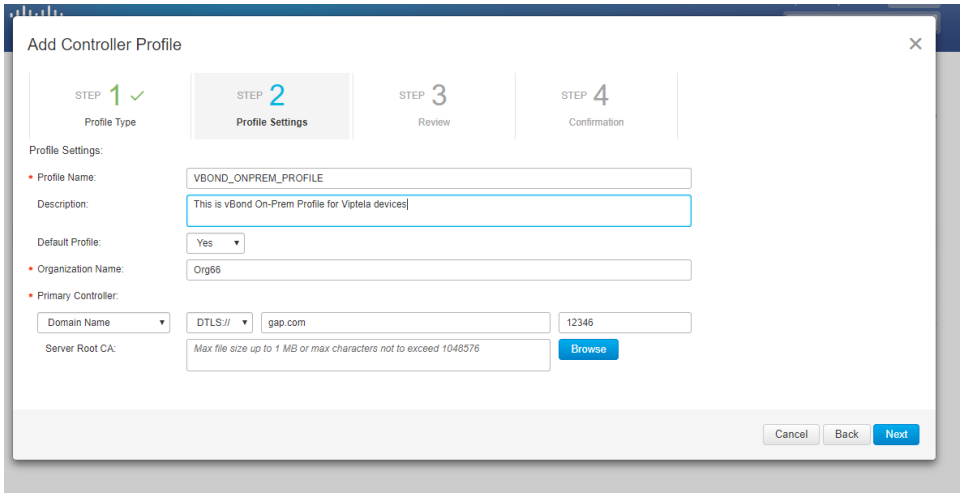
Edit controller

1. Select the controller under the Controller Profile tab and click “Edit Selected”

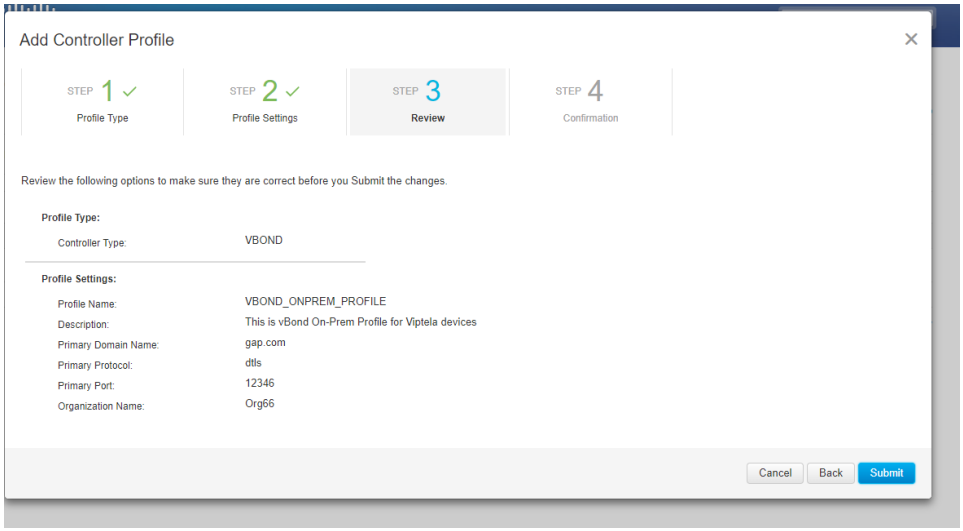


© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

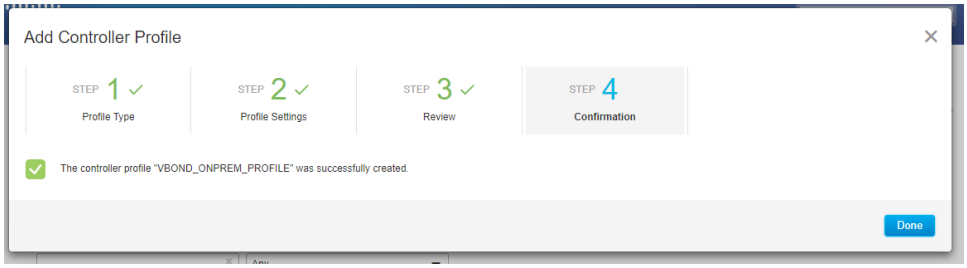
2. The existing value of the controller will be populated in editable format. Change the required value and click “Next”. Rules around editing a controller profile are explained later in this document.



3. The system displays all the vBond information, as shown in the following screenshot.

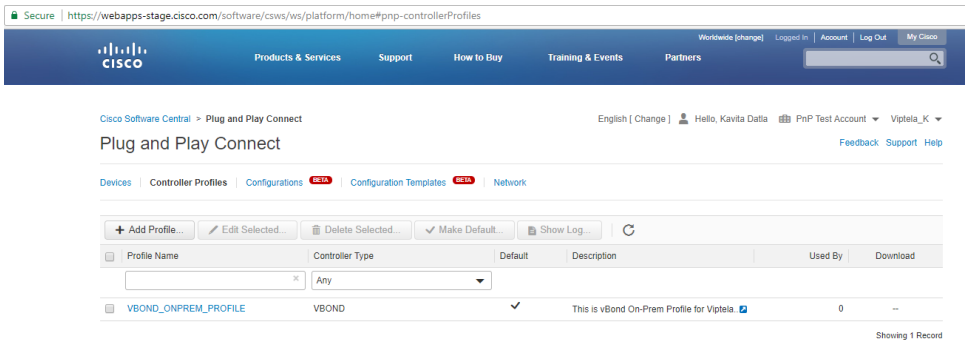


4. Click “Submit”



© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

5. Click “Done”. The profile is edited.



Rules around editing a vBond controller profile on PnP

Plug and Play enforces certain rules to ensure system integrity:

- The organization name is not editable if there are devices associated to a vBond on PnP
- The network ID is not editable when devices are present in a Virtual Account
- The default field in the vBond controller drives the active controller profile on the zProv tool. Only active profile edits will reflect in zProv.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Printed in USA 10/18

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.