Network Plug and Play Troubleshooting Guide for Cisco Digital Network Architecture Center, Release 1.2.x

First Published: February 15, 2019

The Cisco Network Plug and Play (PnP) feature in Cisco DNA Center provides a simple, secure way to deploy network devices for branch or campus networks. This document provides detailed steps to troubleshoot issues you may encounter during device onboarding using Cisco DNA Center release 1.2.x and PnP.

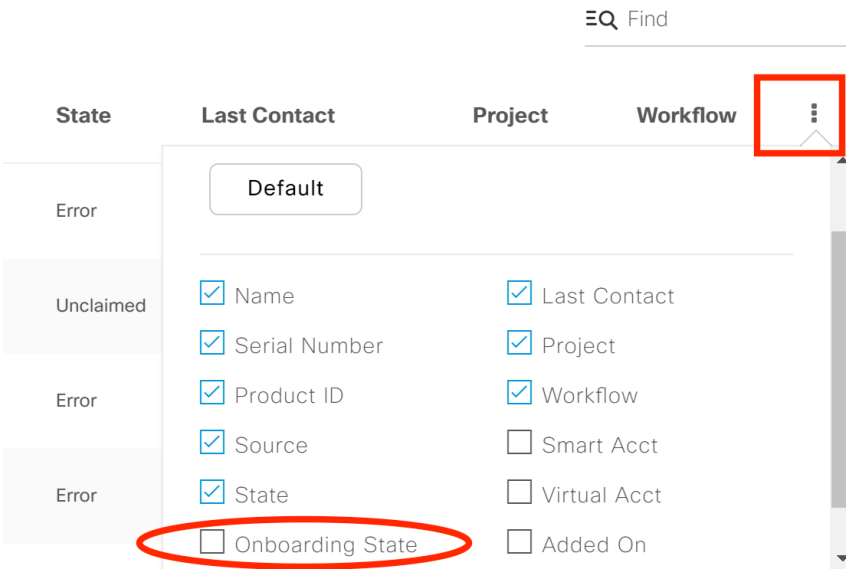
Contents

Device States Supported in PnP, Cisco DNA Center v1.2.x

The following table lists the main device states that a device goes through during onboarding.

Device State	Description
Unclaimed	No workflow assigned
Planned	User workflow added to device
Onboarding	User workflow in execution
Provisioned	Device has been provisioned/onboarded
Error	Device in one of Onboarding error state

The following table lists all the sub-states a device goes through during onboarding. By default, the “Onboarding State” column is not shown in the device list and it can be added as shown below.



Onboarding State	Description
Not Contacted	Device has not called home, but device SN added

Connecting	Device called in Securing connection (certificate install + HTTPS connection) Device Authentication
Initializing	Executing system workflow (collecting device info, CDP info, fix IOS version mismatch for stacks)
Initialized	System workflow complete
Executing Workflow	Executing user workflow
Executed Workflow	User workflow complete
Executing Reset	Executing reset workflow
Connection Error	Could not install certificates to secure connection
Authentication Error	Could not verify SUDI certificate
Authorization Error	Could not verify SUDI SN provided by user
Initialization Error	Error executing system workflow. Error details inside the workflow
Workflow Execution Error	Error executing user workflow. Error details inside the workflow
Reset Execution Error	Error executing reset workflow. Error details inside the workflow
Provisioned	Device added to inventory

Device Troubleshooting Commands

You can use the following CLI commands to troubleshoot device onboarding issues.

Description	IOS Command

Use this command to ensure that the device is running the latest software image.	show version
Make sure device is able to ping controller.	ping <controller_ip>
Make sure device has at least one IP (usually assigned by DHCP server on reload).	sh ip int br
Make sure only one PnP profile is installed.	show run | inc pnp
Make sure device is pointed to correct controller (check for the transport IP specified).	show pnp profile
Make sure device does not have startup config.	show pnp trace
Make sure device does not have left over certificates.	dir nvram:
Make sure device has a serial number (for example, prototype unit does not have one).	show pnp summary
Make sure device initiated PnP process.	show pnp tech
Use this command to view auto install trace log.	show auto install trace
Use the show boot command to display the current value for the BOOTLDR variable.	show boot
Use this command to display all CDP neighbors.	show cdp neighbor
Use this command to view the PKI trustpoint.	show crypto pki trustpoint
Use this command to view the PKI trustful.	show crypto pki trustful
Use this command to view the VLAN information.	show vlan
Use this command to view the NTP status.	show ntp status

Cisco network devices to be deployed must be in a factory default state. If you are using a network device that was previously configured or is in an unknown state, you must reset it to the factory default condition.

Device Cleanup to Manufacturing Default State

If you are using a Cisco router or switch that was previously configured or is in an unknown state, execute the following CLI commands to reset the device to the factory default condition:

```
config terminal
no pnp profile pnp-zero-touch
no crypto pki certificate pool
config-register 0x2102  (for non-default ROMMON only)
end
delete /force vlan.dat  (for switch platforms only)
delete /force nvram:*.cer
delete /force stby-nvram:*.cer  (for HA system only)
write erase  (answer no when asked to save)
reload
```

If you are using a Cisco Aironet 3700, 3600, 2700, 2600, 1700, 1600, or 700 Series Access Point device that was previously configured or is in an unknown state, execute the following CLI commands to reset the device to the factory default condition:

```
debug capwap console cli
config terminal
no crypto pki certificate pool
boot system flash:/ap3g2-rcvk9w8-mx/ap3g2-rcvk9w8-mx  (for 3700, 2700, 1700, 3600, 2600 platforms)
boot system flash:/ap1g2-rcvk9w8-mx/ap1g2-rcvk9w8-mx  (for 1600 platforms)
boot system flash:/ap1g1-rcvk9w8-mx/ap1g1-rcvk9w8-mx  (for 700 platforms)
end
clear capwap private-config
delete /force flash:capwap*
delete /force flash:private-multiple-fs
delete /force flash:lwapp*
write erase
reload
```

If you are using a Cisco Aironet 3800, 2800, or 1800 Series Access Point device that was previously configured or is in an unknown state, execute the following CLI commands to reset the device to the factory default condition:

```
capwap ap erase all
reload
```

To view active connections for the Cisco Plug and Play IOS Agent:

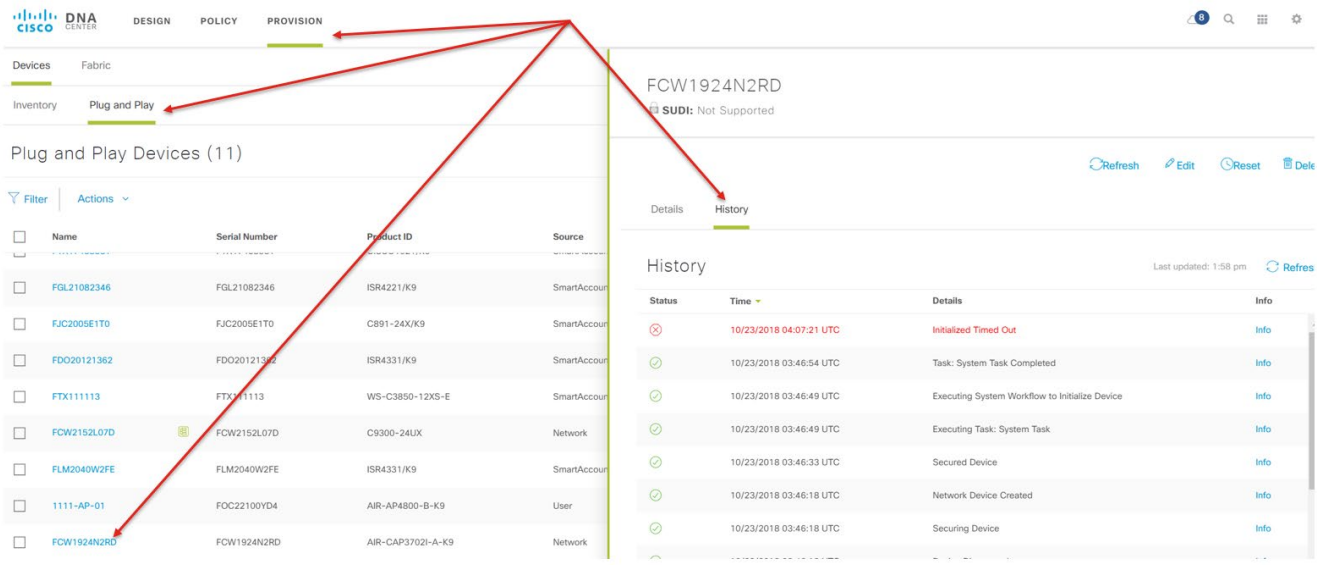
```
Router# show pnp tech-support
```

If needed, you can enable debug information and capture the output for the Cisco Plug and Play IOS Agent as follows:

```
Router> enable
Router> debug pnp all
Router> ter mon
```

Troubleshooting from the Cisco DNA Center GUI

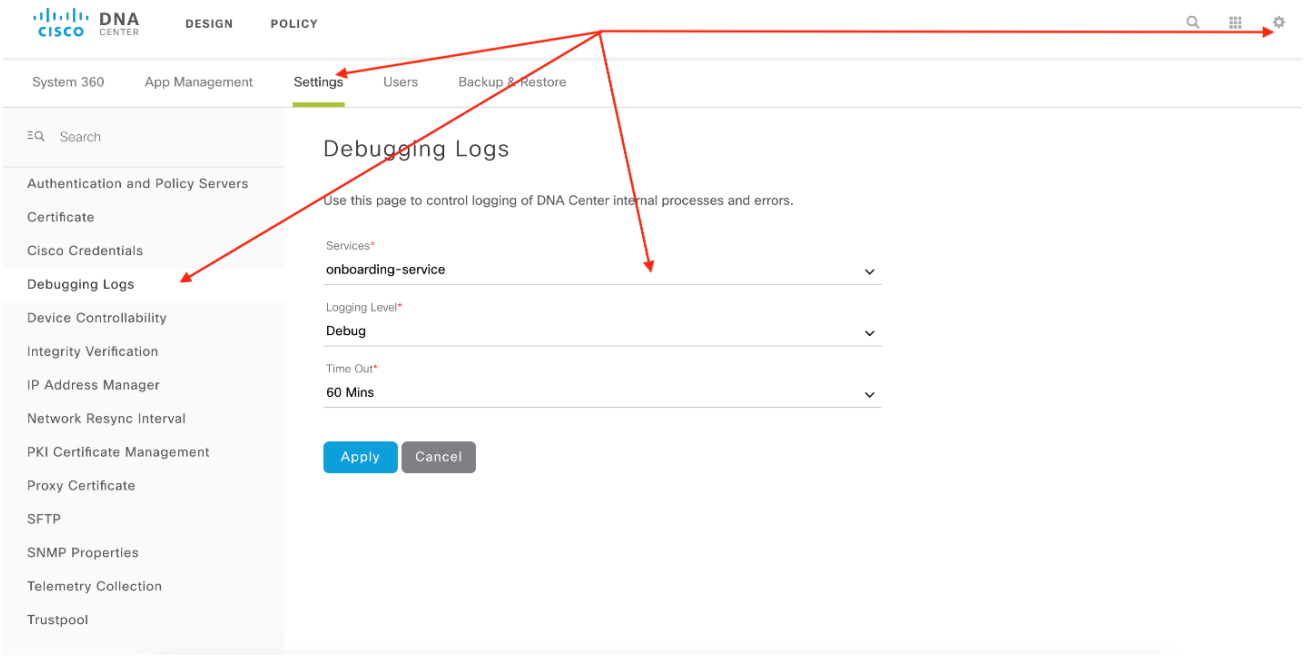
If a device ends in an error state or you want to look at the history, click on a device and then click the **History** tab. Most of the errors should be available there. You can click on **Info** to find additional information such as syntax errors.



Collecting PnP Logs from Maglev

Log Levels

Change the logging level to **Debug**. By default, the log level in Cisco DNA Center is **Info**. If you want to change the logging level and collect the logs, use **System Settings > Settings > Debugging Logs.** Change both *connection-manager-service* and *onboarding-service* to the **Debug** logging level.



Collecting All Maglev Logs

You can collect all cluster logs from Maglev using the rca command

1. Login to your cluster.

   ssh maglev@*controller-ip-address* **-p 2222**

2. Run the rca command.

   rca

   This will generate a file like */data/rca/maglev-192.0.2.11-rca-2018-04-09_23-12-00_UTC.tar.gz*. This file can be about ~200 MB

3. Copy it with **scp** it to your local folder.

   scp -P 2222 maglev@*controller-ip-address***:/data/rca/maglev-192.0.2.11-rca-2018-04-09_23-12-00_UTC.tar.gz ~/Downloads**

4. Once in your local folder, untar this file.

   tar -xvf maglev-192.0.2.11-rca-2018-04-09_23-12-00_UTC.tar.gz

   This creates a folder called data.

5. CD to the folder.

   cd data/rca/maglev-192.0.2.11-rca-2018-04-09_23-12-00_UTC

6. Untar the file var-log.tar.gz.

   tar -xvf var-log.tar.gz

   This creates a folder called **var**.

7. CD to **var/log/containers**, which contains the service logs. For example, the onboarding service logs can be a file (the name is based on service name and container ID) such as onboarding-service-1502674267-xdtjv_fusion_onboarding-service-395ff66e199c0a5797358d03a963b9612a6320c99857394ef27e588959c8a72a.log