Release Notes for Cisco Network Plug and Play, Release 1.6.x

First Published: 2017-10-24

Last Updated: 2018-7-10

These release notes apply to the following software releases of the Cisco Network Plug and Play Solution:

- General Availability Release 1.6.3
- General Availability Release 1.6.2
- General Availability Release 1.6.1
- General Availability Release 1.6

These release notes contain the following sections:

Introduction

The Cisco Network Plug and Play solution provides a simple, secure, unified, and integrated offering for enterprise network customers to ease new branch or campus device deployments or for provisioning updates to an existing network. The solution provides a unified approach to provision enterprise networks comprised of Cisco routers, switches, and wireless access point devices with a near zero touch deployment experience.

What's New in Release 1.6

This software release provides the following new features and functions:

- Support for the Cisco 1100 Series Integrated Services Routers
- Support for the Cisco 800 Series Industrial Integrated Services Routers
- Support for new NFVIS platforms: Cisco ENCS 5104, UCS-E180D-M3, and UCS-E1120D-M3

Supported Platforms and Software Requirements

The following tables list Cisco routers, switches, wireless access points, NFVIS platforms, and software releases that support the Cisco Plug and Play IOS Agent and the Cisco Network Plug and Play Solution.

In the case where there is a rebuild for a particular release, it is recommended to use the latest rebuild release.

Table 1 Supported Cisco Switches

Platform	Models	Software Release (Minimum Supported)
Cisco Catalyst 2960 Series Switches	2960-C 2960-Plus 2960-S 2960-SF 2960-X 2960-XR	15.2.2E3, 15.2.3E2, 15.2.4E[1]
	2960-CX[2]	15.2.3E2, 15.2.4E[1]
	2960-L	15.2.5E
Cisco Catalyst 3560 Series Switches	3560-C 3560-X	15.2.2E3
	3560-CX[2]	15.2.3E2, 15.2.4E[1]
Cisco Catalyst 3650 Series Switches	3650	3.6.5E, 3.7.4E, 16.3.3
	3650-24PDM 3650-48FQM	16.3.3
Cisco Catalyst 3750-X Series Switches	3750X	15.2.2E3, 15.2.4E[1]
Cisco Catalyst 3850 Series Switches	3850	3.6.5E, 3.7.4E, 16.3.3
	3850-12X48U[2] 3850-12XS[2] 3850-16XS[2] 3850-24XS[2] 3850-32XS[2]	3.7.4E, 16.3.3
	3850-48XS	3.7.4E, 16.3.3
Cisco Catalyst 4500 Series Switches	Supervisor 6-E/6L-E Supervisor 7-E/7L-E Supervisor 8-E	3.6.5E, 3.7.4E, 3.8.2E, 3.9.0E
	Supervisor 8L-E	3.8.1E
	Supervisor 9-E	3.10.0E
Cisco Catalyst 4500-X Series Switches	4500X-16, 32	3.6.5E, 3.7.4E, 3.8.2E, 3.9.0E
Cisco Catalyst 4900 Series Switches	4900M 4948E	15.2.2E3, 15.2.3E2, 15.2.4E[1]

Table 1 Supported Cisco Switches (continued)

Platform	Models	Software Release (Minimum Supported)
Cisco Catalyst 9300 Series Switches	9300	16.5.1a
Cisco Catalyst 9400 Series Switches	9400	16.6.1
Cisco Catalyst 9500 Series Switches	9500	16.5.1a
Cisco Industrial Ethernet 2000 Series Switches	IE2000	15.2.2E3, 15.2.3E2, 15.2.4EA[1]
Cisco Industrial Ethernet 3000 Series Switches	IE3000	15.2.2E3, 15.2.3E2, 15.2.4EA[1]
Cisco Industrial Ethernet 4000 Series Switches	IE4000	15.2.4EA5
Cisco Industrial Ethernet 5000 Series Switches	IE5000	15.2.4EA5

1. The non-VLAN 1 feature is not supported on release 15.2.4E.
2. Limited feature support: Trustpool support for devices with smaller NVRAM space is only by using the DHCP options T and Z.

Table 2 on page 3 lists software releases that have limited feature support. For software releases not listed, all features are supported.

Table 2 Limited Feature Support by Software Version for Switches

Software Release	Feature			
	DHCP Option 60	Non-VLAN1	SUDI	Trustpool
03.06.05.E	Yes	Yes[2]	Yes	Yes[1]
03.07.04.E	Yes	Yes	Yes	Yes[1]
03.08.01.E	Yes	Yes[3]	Yes[1]	Yes[1]
03.09.00.E	Yes	Yes	Yes	Yes
Denali 16.3.3	Yes	Yes	Yes	Yes
Denali 16.5.1a	Yes	Yes	Yes	Yes
Denali 16.6.1	Yes	Yes	Yes	Yes

1. The following caveats apply: CSCuv42560, CSCuw63034, CSCuy16820, CSCvb56482.
2. The following caveat applies: CSCux54515.
3. The following caveat applies: CSCux52544.

Table 3 Supported Cisco Routers

Platform	Models	Software Release (Minimum Supported)
Cisco 800 Industrial Integrated Services Routers	807 809 829	15.7(3)M1
Cisco 800 Series Routers	819	15.5(3)M1
	866 867 881 886 887 888 891 892 896 897 898 899	15.5(3)M
Cisco 1100 Series Integrated Services Routers	1111 1116 1117	16.6.2
Cisco 1900 Series Integrated Services Routers	1905 1921 1941	15.5(3)M
Cisco 2900 Series Integrated Services Routers	2901 2911 2921 2951	15.5(3)M
Cisco 3900 Series Integrated Services Routers	3925 3925E 3945 3945E	15.5(3)M
Cisco 4000 Series Integrated Services Routers	4221	16.5.1b
	4321 4331 4351 4431 4451-X	15.5(3)S
Cisco ASR 1000 Series Aggregation Services Routers	ASR1001-X/ASR1001-HX ASR1002-X/ASR1002-HX ASR1004 ASR1006/ASR1006-X ASR1009-X ASR1013	16.3.2[1] 16.4.1[2]
Cisco Cloud Services Router	CSR 1000V[3]	15.5(3)S

1. The ASR 1000 Series routers support Plug and Play discovery on the management interface beginning with Release 16.3.2.
2. The ASR 1000 Series routers support Plug and Play discovery on the non-management interfaces beginning with Release 16.4.1.
3. The CSR 1000v router supports Plug and Play discovery only on an ISO deployment, not when deployed with an OVA.

Table 4 Supported Cisco Wireless Access Points

Platform[1]	Models	Software Release (Minimum Supported)
Cisco Aironet 700 Series	702i 702w	8.2
Cisco Aironet 1600 Series	1602e 1602i	8.2
Cisco Aironet 1700 Series	1702i	8.2
Cisco Aironet 1800 Series	OEAP1810 1810w 1830i 1832i 1852e 1852i	8.3
	1815i, 1815w	8.4
	1815m, 1815t	8.5
Cisco Aironet 2600 Series	2602e 2602i	8.2
Cisco Aironet 2700 Series	2702e 2702i	8.2
Cisco Aironet 2800 Series	2802e 2802h 2802i	8.3
Cisco Aironet 3600 Series	3602e 3602i 3602p	8.2
Cisco Aironet 3700 Series	3702e 3702i 3702p	8.2
Cisco Aironet 3800 Series	3802e 3802i 3802p	8.3

1. The Flexgroup feature for the Cisco Aironet 700 Series, 1600 Series, 1700 Series, 2600 Series, 2700 Series, 3600 Series, and 3700 Series APs is available with the AireOS 8.3 release.

Table 5 Supported NFVIS Platforms

Platform	Models	Software Release (Minimum Supported)
Cisco ENCS	ENCS5104/K9	3.6.2
	ENCS5406/K9 ENCS5408/K9 ENCS5412/K9	3.5.1

Table 5 Supported NFVIS Platforms

Platform	Models	Software Release (Minimum Supported)
Cisco UCS-C Series	UCSC-C220-M4S	3.5.1
Cisco UCS-E Series	UCS-E180D-M3/K9 UCS-E1120D-M3/K9	3.6.1
	UCS-E180D-M2/K9 UCS-E160S-M3/K9 UCS-E160D-M2/K9 UCS-E140S-M2/K9	3.5.1

Note: Only official software releases obtained from the Cisco.com software download website are supported for image deployment. Engineering builds are not supported.

Cisco Network Plug and Play supports the following features, depending on the Cisco IOS software release on the device:

- IPv6 is supported in the Cisco Plug and Play IOS agent beginning with software release IOS XE 16.4.
- AAA device credential support. The AAA credentials are passed to the device securely and the password is not logged. This feature allows provisioning a device with a configuration that contains aaa authorization commands. This feature requires software release IOS 15.2(6)E1, IOS 15.6(3)M1, IOS XE 16.3.2, or IOS XE 16.4 or later on the device.
- Image install and upgrade for Cisco 3650 and 3850 Series switches is supported only when the switch is booted in Install mode. (Image install and upgrade is not supported for switches booted in Bundle mode.)

SUDI Support

The Secure Unique Device Identifier (SUDI) feature that allows secure device authentication is available on the following platforms:

- Cisco Routers:
  - Cisco 800 Series Industrial ISR with software release 15.7(3)M1 or later
  - Cisco 819 ISR with software release 15.5(3)M1 or later
  - Cisco 88x and 89x ISR models with software release 15.5(3)M or later
  - Cisco ISR 1100 Series with software release 16.6.2
  - Cisco ISR 4000 Series with software release 15.5(3)S1 or later
  - Cisco ASR 1000 Series (except for the ASR 1002-x) with software release 16.6.1
- Cisco Switches:
  - Cisco Catalyst 3850 Series with software releases 3.6.3E or 16.1.2E or later
  - Cisco Catalyst 3650 Series and 4500 Series with Supervisor 7-E/8-E, with software releases 3.6.3E, 3.7.3E, or 16.1.2E or later
  - Cisco Catalyst 4500 Series with Supervisor 8L-E with software releases 3.8.1E or later
  - Cisco Catalyst 4500 Series with Supervisor 9-E with software release 3.10.0E or later
  - Cisco Catalyst 9300 Series with software release 16.5.1a or later.
  - Cisco Catalyst 9400 Series with software release 16.6.1 or later.
  - Cisco Catalyst 9500 Series with software release 16.5.1a or later.

- NFVIS platforms:
  - Cisco ENCS 5400 Series with software release 3.5.1 or later
  - Cisco ENCS 5104 with software release 3.6.2 or later

Note: Devices that support SUDI have two serial numbers: the chassis serial number and the SUDI serial number (called the License SN on the device label). You must enter the SUDI serial number in the Serial Number field when adding a device that uses SUDI authentication. The following device models have a SUDI serial number that is different from the chassis serial number:

- Cisco Routers: ISR 88x, ISR 89x, ISR 43xx, ISR 44xx, ASR1001-X/HX, ASR1002-HX
- Cisco Switches: Catalyst 4500 Series with Supervisor 8-E/8L-E/9-E, Catalyst 9400 Series

Management Interface VRF Support

Cisco Network Plug and Play operates over the device management interface on the following platforms:

- Cisco Routers:
  - Cisco ASR 1000 Series with software release 16.3.2 or later
  - Cisco ISR 4000 Series with software release 16.3.2 or later
- Cisco Switches:
  - Catalyst 3650 Series and 3850 Series with software release 16.6.1 or later
  - Cisco Catalyst 9300 Series with software release 16.6.1 or later
  - Cisco Catalyst 9400 Series with software release 16.6.1 or later
  - Cisco Catalyst 9500 Series with software release 16.6.1 or later

4G Interface Support

Cisco Network Plug and Play operates over a 4G network interface module on the following Cisco Routers:

- Cisco 800 Series Industrial ISR with software release 15.7(3)M1 or later
- Cisco 819 ISR and C899 with software release 15.7(3)M or later
- Cisco 1100 Series ISR with software release 16.6.2 or later
- Cisco 1900, 2900, and 3900 Series ISR with software release 15.7(3)M or later

For more information, see “Cisco Network PnP Discovery Over 4G Interface” in the IOS documentation.

Upgrade and Downgrade Support

Release 1.6 Upgrade Requirements

Follow these guidelines for upgrading the Cisco Network Plug and Play application for APIC-EM to version 1.6:

- The Cisco Network Plug and Play application, which was previously bundled and enabled with the APIC-EM controller is now a separate application. You need to download and install the new application to use it with APIC-EM controller version 1.6. For information about downloading and installing an application, see the section, "Installing Cisco APIC-EM Applications," in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.
- Ensure that the APIC-EM controller software is at version 1.6 or later before upgrading the Cisco Network Plug and Play application to version 1.6.

Upgrade Support

Table 6 on page 8 lists the supported upgrade paths for each supported release.

Table 6 Upgrade Paths Supported by Switch Software Versions

From Software Version	To Software Version
03.06.05.E	03.07.04.E Denali 16.3.3 Denali 16.5.1a Denali 16.6.1
03.06.06.E	03.06.07.E 03.07.05.E Denali 16.3.3 Denali 16.5.1a Denali 16.6.1
03.07.04.E	Denali 16.3.3 Denali 16.5.1a Denali 16.6.1
03.07.05.E	Denali 16.3.3 Denali 16.5.1a Denali 16.6.1

Downgrade Support

Table 7 on page 9 lists the supported downgrade paths for each supported release.

Table 7 Downgrade Paths Supported by Switch Software Versions

From Software Version	To Software Version
03.07.05.E	03.06.05.E 03.06.06.E 03.07.04.E
03.07.04.E	03.06.05.E
Denali 16.3.3	03.06.05.E 03.06.06.E 03.06.07.E 03.07.04.E 03.07.05.E
Denali 16.5.1a	03.06.05.E 03.06.06.E 03.06.07.E 03.07.04.E 03.07.05.E Denali 16.3.3
Denali 16.6.1	03.06.05.E 03.06.06.E 03.06.07.E 03.07.04.E 03.07.05.E Denali 16.3.3 Denali 16.5.1a

Limitations

Cisco Network Plug and Play has the following limitations:

- The bulk import function is similar to adding new provisioning rules that can set a device to the pending state. When you export the project and device database, the application displays the correct device state. If you then import the saved database, the devices must contact the APIC-EM controller again to return to the provisioned state because the bulk import feature restores only the device provisioning rules and does not restore the state of devices.
- Bulk import does not support uploading template configurations.
- Virtual Switching System (VSS) is not supported.
- Configuration templates are based on the Velocity templating engine version 1.7, with the following limitations:
  - The #parse and #include directives are not supported.
  - Structured objects are not supported.
  - The #foreach element works only with lists, not maps or enumerations, and #foreach attributes like "foreach.count" are not supported.
- For stack switch functionality in Projects in the Cisco Network Plug and Play application for APIC-EM, only the Cisco Catalyst Switches 3850/3650/2960X/2960XR/2960S Series are supported. For the Cisco Catalyst 2960X/2960XR/2960S Series switches, only image upgrade with tar file and configuration upgrade are supported; license upgrade or LAN-Lite license level is not supported.
- Stack switch functionality is not supported with Cisco Catalyst 9300 Series Switches.
- Cisco switches do not support bootstrap configurations using USB drives.

Mobile App Limitations

Note the following considerations when using the Cisco Plug and Play Mobile App:

- After disconnecting the console cable from the network device, if you want to connect it to a different network device, you must first manually refresh the mobile app to reflect the correct status when connecting to the new device.
- If you have an iOS mobile device with a Redpark cable and are deploying multiple network devices, after you are done with one device, you must unplug the Redpark cable from both your mobile device and the network device to close the serial connection. If you do not disconnect the cable from your mobile device, the serial session is not closed and the wrong configuration could be deployed on the next device.
- The Cisco Plug and Play Mobile App is not be able to detect the device SUDI serial number, which is separate from the device chassis serial number. When pre-provisioning a device that will be deployed by using the mobile app, specify only the chassis serial number from the **show version** command output and do not select the SUDI Required check box in the Cisco Network Plug and Play application on APIC-EM.

Sizing Guidelines

The Cisco Network Plug and Play application on APIC-EM can support the following:

- A maximum of 10000 devices pre-provisioned in the Cisco Network Plug and Play application for APIC-EM, of which a maximum of 4000 can be router and switch devices and the remainder can be wireless access point devices
- A maximum of 50 devices of all types simultaneously contacting the server and being provisioned
- A maximum of 200 unclaimed devices of all types in the Cisco Network Plug and Play application for APIC-EM

See the *Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module* for APIC-EM device support guidelines.

Configuring Server Identity

To ensure successful controller discovery by Cisco devices running newer IOS releases, the server SSL certificate offered by the controller during the SSL handshake must contain an appropriate Subject Alternate Name (SAN) value, so that the Cisco Plug and Play IOS Agent can verify the server identity. This may require the controller administrator to upload a new server SSL certificate, which has the appropriate SAN values, to the controller. This requirement applies to all controllers that implement the Plug and Play server.

This requirement applies to devices running the following Cisco IOS releases:

- Cisco IOS Release 15.2(6)E2 and later
- Cisco IOS Release 15.6(3)M4 and later
- Cisco IOS Release 15.7(3)M2 and later
- Cisco IOS XE Denali 16.3.6 and later
- Cisco IOS XE Everest 16.5.3 and later
- Cisco IOS Everest 16.6.3 and later
- All Cisco IOS releases from 16.7.1 and later

The value of the SAN field in the controller certificate must be set according to the type of discovery being used by devices, as follows:

- For DHCP option-43/option-17 discovery using an explicit IPv4 or IPv6 address, set the SAN field to the specific IPv4/IPv6 address of the controller.
- For DHCP option-43/option-17 discovery using a hostname, set the SAN field to the controller hostname.

- For DNS discovery, set the SAN field to the hostname of the controller, in the form of pnpserver.domain.
- For Cisco Plug and Play Connect cloud portal discovery, set the SAN field to the controller IP address, if the IP address is used in the Plug and Play Connect profile. If the profile uses the controller hostname, then the SAN field must be set to the fully qualified domain name (FQDN) of the controller.

If the controller IP address that is used in the Plug and Play profile is a public IP address that is assigned by a NAT router, then this public IP address must be included in the SAN field of the server certificate.

If an HTTP proxy server is used between the devices and the controller, ensure that the proxy certificate has the same SAN fields with the appropriate IP address or hostname.

It is recommended to include multiple SAN values in the certificate, in case discovery methods vary. For example, you can include both the controller FQDN and IP address (or NAT IP address) in the SAN field. If you do include both, set the FQDN as the first SAN value, followed by the IP address.

If the SAN field in the controller certificate does not contain the appropriate value, the device will not be able to successfully complete the plug and play process.

Note: The Cisco Plug and Play IOS Agent checks only the certificate SAN field for the server identity. It does not check the common name (CN) field.

Upgrading a Cisco Catalyst 3650 or 3850 Series Switch to Cisco IOS XE Denali 16.1.1 While Provisioning

This section applies if you have a Cisco Catalyst 3650 or 3850 Series switch with a software release of Cisco IOS XE 3.6.3, 3.7.2, or earlier, it is in a factory default state (unprovisioned in the network), and at the same time as provisioning you want to upgrade it to Cisco IOS XE Denali 16.1.1E.

Such devices with older software releases fail the normal upgrade process to release 16.1.1E, however, you can use the Cisco Network Plug and Play application to do the upgrade while provisioning the device, by using the following steps:

Prerequisite: The Cisco network device to be provisioned is in a factory default state and can be auto-booted with the 16.1.1E image. If you are using a network device that was previously configured or is in an unknown state, see the reset details in the Solution Guide for Cisco Network Plug and Play.

1. Put the Cisco IOS XE Denali 16.1.1E image on a TFTP server that is accessible to the device you are upgrading.
2. Create a configuration file for the device and add the following lines to the end of the file, which will upgrade the software and reload the switch:

   ```
   ip tftp block 8192
   do software install file tftp://ip-address/dir/filename new force
   do reload in 1
   end
   ```

   The tftp URL must include the IP address of the TFTP server (*ip-address*), the directory in which the image resides (*dir*), and image filename (*filename*).
3. Upload the configuration file in the Cisco Network Plug and Play application, by using the Upload button in the Configurations tab.
4. Add the configuration file to the device information, either in the Projects tab (for a new device that you are preprovisioning) or in the Unplanned Devices tab (for an unclaimed device that is already installed but not yet provisioned).
5. If the device is unclaimed, click Claim to provision it, or if you are preprovisioning a device that is not yet installed, it is automatically provisioned when it is installed. Note that it takes about 25 minutes for the upgrade to complete and there is minimal console output from the device during the process.

6. Verify that device status is Provisioned in the Cisco Network Plug and Play GUI.
7. Verify that the device is successfully deployed by checking the log messages by clicking on the device serial number. Look for the message, “Device was successfully deployed!!”
8. Verify that the installed software release is Denali 16.1.1E by using the **show version** command on the device.

Caveats

Release 1.6.3 Resolved Caveats

Caveat ID Number	Headline
CSCvj05259	Provisioned device with additional reload showing Authentication Error
CSCvj45234	Command CorrelatorID not updated while resending to device for lost response resulting in error
CSCvj45295	PNP-service sends the certificate install request in secure mode: Error_during_Certificate_Install
CSCvj45334	Simultaneously requests to pnp-service gets blocked at message converter

Release 1.6.2 Resolved Caveats

Caveat ID Number	Headline
CSCvi63999	Unable to register with a Smart Account with TLS 1.2
CSCvi67568	2960 stack fails at license information collection in DEVICE_INFO_REQUESTED state

Release 1.6.1 Resolved Caveats

Caveat ID Number	Headline
CSCvg96408	Fails to connect to PnP Connect when controller proxy is configured
CSCvg96572	Device fails in authentication state and at times stops processing work requests
CSCvh68406	Stack switch health error timeout when show switch output is not parsed correctly
CSCvh73482	Exclude 2960 stack switch platforms from Standby bulk sync

Release 1.6 Resolved Caveats

Caveat ID Number	Headline
CSCvf48255	Server not waiting for stack switches to reach sso before pushing configuration
CSCvf53195	Device Authentication error with config push failure on PnP Connect

Release 1.6 Open Caveats

Caveat ID Number	Headline
CSCva38541	PnP vrf discovery error with Device Certification sdn-network-infra-iwan
CSCvc55317	Change Config file to Template has no effect on PnP Project Edit
CSCvg16567	Auth failure on discovered stack switch with SUDI checkbox selected on a Project flow

Related Documentation

- Solution Guide for Cisco Network Plug and Play—Solution Guide for the Cisco Network Plug and Play solution.
- Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM—Describes how to use the Network Plug and Play application in the APIC-EM to configure Cisco network devices.
- Cisco Open Plug-n-Play Agent Configuration Guide—Describes how to configure the Cisco Open Plug-n-Play Agent software application that runs on a Cisco IOS or IOS-XE device.
- Mobile Application User Guide for Cisco Network Plug and Play—Describes how to use the Cisco Network Plug and Play mobile application.
- Plug and Play Connect website—Release Notes and documentation for the Cisco Plug and Play Connect cloud service.
- Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide—Describes how to deploy and troubleshoot the Cisco APIC-EM.
- Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide—Describes how to configure settings for the Cisco APIC-EM.
- Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module—Release Notes for the Cisco APIC-EM.
- Release Notes for Cisco Intelligent Wide Area Network Application (Cisco IWAN App)—Release Notes for Cisco IWAN.
- Software Configuration Guide for Cisco IWAN on APIC-EM—Configuration Guide for Cisco IWAN.
- *Cisco APIC-EM Quick Start Guide*—Guide to getting started with the APIC-EM and including a list of related documentation (available in the APIC-EM GUI).
- Open Source Used In Cisco APIC-EM—List of open source code used in the Cisco APIC-EM.
- Open Source Used In Cisco Network Plug and Play—List of open source code used in the Cisco Network Plug and Play application for APIC-EM.

Obtain Documentation and Submit a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.