Release Notes for Cisco Network Plug and Play, Release 1.3x

First Published: 2016-10-25

Last Updated: 2017-1-27

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

- General Availability Release 1.3.3
- General Availability Release 1.3.2
- General Availability Release 1.3

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 1.3.3

This software release provides new functionality for configuration templates, to escape the $ character when you do not want it to be interpreted as a variable definition, such as a $ character in an encrypted password. To escape a $ character, add {esc.d} immediately following the $ in a configuration template.

For example, if you have the following line in a configuration template, you would not want the $ characters to be interpreted as variables:

```
enable secret 5 $1$cJX0$Cq6AtbQYt4owH2QTWmP4v/
```

Escape the $ characters as follows:

```
enable secret 5 ${esc.d}1${esd.d}cJX0${esc.d}Cq6AtbQYt4owH2QTWmP4v/
```

What's New in Release 1.3.2

This software release provides the following new features and functions:

- New and enhanced functionality in the Cisco Network Plug and Play application in the APIC-EM:
  - Configuration template support is enhanced with a new Template tab at the top level. Use this tab to upload and manage configuration templates.
  - When you add a device or claim an unplanned device, and are specifying the configuration file, you can now choose either Configuration or Template and then select the file to apply.

What's New in Release 1.3

This software release provides the following new features and functions:

- Configuration template support allows an administrator to define a configuration template of CLI commands that can be used to consistently configure multiple network devices, reducing deployment time. Variables in the template allow customization of specific settings per device and templates support constructs such as #set, #if, #else, and #foreach. Configuration templates are based on the open source Velocity templating engine, version 1.7.
- API support for passing the specified device management IP address to the APIC-EM discovery function. The first active device IP address is considered to be the management IP address, if the management IP address is not specified.
- IPv6 support in the Cisco Plug and Play IOS agent beginning with software release IOS XE 16.4.
- Support for Network Functions Virtualization Infrastructure Software platforms.
- New and enhanced functionality in the Cisco Network Plug and Play application in the APIC-EM:
  - Configuration template support, including text view, form view, and preview for a template.
  - Configuration file syntax validation to catch non-ASCII and control characters when a configuration file is uploaded. This functionality does not verify CLI command validity.
  - Individual device credential support, allowing the controller to manage devices that require individual TACACS or RADIUS credentials for access. The credentials are passed to the device securely and the password is not logged. This enhancement simplifies the process to provision a device with a configuration that contains **aaa authorization** commands. This feature requires software release IOS 15.6(3)M1, IOS XE 16.3.2, or IOS XE 16.4 or later on the device.
  - Bulk import improvements to handle device credentials and configuration templates.

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.

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, 16.1.3, 16.2.2, 16.3.1
	3650-24PDM 3650-48FQM	16.2.2
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, 16.1.3, 16.2.2, 16.3.1
	3850-12X48U[2] 3850-12XS[2] 3850-16XS[2] 3850-24XS[2] 3850-32XS[2]	3.7.4E, 16.1.3, 16.2.2, 16.3.1
	3850-48XS	3.7.4E, 16.2.2
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
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]
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]

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 4 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 16.1.1	Yes	Yes[1]	Yes[1]	Yes[1]
Denali 16.1.2	Yes	Yes[2]	Yes[1]	Yes[1]
Denali 16.2.1	Yes	Yes[2]	Yes[1]	Yes[1]
Denali 16.3.1	Yes	Yes[2]	Yes	Yes
Denali 16.3.1a	Yes	Yes[2]	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 Series Routers	819	15.5(3)M1
	829 866 867 881 886 887 888 891 892 896 897 898 899	15.5(3)M
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	4321 4331 4351 4431 4451-X	15.5(3)S
Cisco ASR 1000 Series Aggregation Services Routers	ASR1001 ASR1001-X ASR1002 ASR1002-X ASR1004 ASR1006 ASR1013	15.5(3)S
	ASR1001-HX ASR1002-HX	16.4.1
Cisco Cloud Services Router	CSR 1000V[1]	15.5(3)S

1. 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	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 2600 Series	2602e 2602i	8.2
Cisco Aironet 2700 Series	2702e 2702i	8.2
Cisco Aironet 3600 Series	3602e 3602i 3602p	8.2
Cisco Aironet 3700 Series	3702e 3702i 3702p	8.2

Table 5 Supported NFVIS Platforms

Platform	Models	Software Release (Minimum Supported)
Cisco ENCS	ENCS5406/K9 ENCS5408/K9 ENCS5412/K9	3.4.1
Cisco UCS-C Series	UCSC-C220-M4S	3.4.1
Cisco UCS-E Series	UCS-E180D-M2/K9 UCS-E160S-M3/K9 UCS-E160D-M2/K9 UCS-E140S-M2/K9	3.4.1

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

SUDI Support

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

- Cisco Routers:
  - 819 with software release 15.5(3)M1 or later
  - ISR 4000 Series with software release 15.5(3)S1 or later
- Cisco Switches:
  - Catalyst 3850 Series with software releases 3.6.3E or 16.1.2E or later
  - 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

Management Interface VRF Support

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

- Cisco Routers:
  - ASR 1000 Series with software release 16.3.2 or later
  - ISR 4000 Series with software release 16.3.2 or later
- Cisco Switches:
  - Catalyst 3650 Series and 3850 Series with software release 16.5 or later

Upgrade and Downgrade Support

Upgrade Support

Table 6 on page 7 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 16.1.3 Denali 16.2.2 Denali 16.3.1
03.07.04.E	Denali 16.1.3 Denali 16.2.2 Denali 16.3.1
Denali 16.1.3	Denali 16.2.2 Denali 16.3.1

Downgrade Support

Table 7 on page 8 lists the supported downgrade paths for each supported release.

Table 7 Downgrade Paths Supported by Switch Software Versions

From Software Version	To Software Version
03.07.04.E	03.06.05.E
Denali 16.1.3	03.06.05.E 03.07.04.E Denali 16.1.3 Denali 16.2.2 Denali 16.3.1
Denali 16.2.2	03.06.05.E 03.07.04.E Denali 16.1.3

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 3650 Series Switches and Cisco Catalyst 3850 Series Switches are supported.

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.

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 1.3.3 Resolved Caveats

Caveat ID Number	Headline
CSCvc53581	Bulk Import action yields no response from UI
CSCvc53590	New device rule under TFTP Project will create dummy " config"
CSCvc53599	Template files are uploaded in the Config page in Unclaimed Flow
CSCvc53606	User created template with excape ${esc.d} is being treated as variable in UI

Release 1.3.3 Open Caveats

Caveat ID Number	Headline
CSCvc68158	Template support of rendering variables inside of #set function
CSCvc68171	Non-boolean variable with no input should be be shown in the Template Preview
CSCvc84731	Skip Eula accepted check when the user edits the the switch rule from stack to single switch.
CSCvc91312	PnP UI: Edit on ztdrule with credential fails

Release 1.3.2 Resolved Caveats

Caveat ID Number	Headline
CSCvb94277	Image upgrade did not happen from 3.6.5 to 03.06.05.b, device status is shown as provisioned
CSCvc03717	Config users are forced into PnP Template flow due to $ characters
CSCvc06767	PnP App: Add 2960L supported new hardware SKUs to PNP for 1.3 Release
CSCvc09040	Snmp Priv passphrase shows encrypted string in GET
CSCvc12835	Configuration went away when deployed with Mobile App bootstrap file
CSCvc13812	PnP UI not able to accept EULA when editing previously non-stack switch device rule
CSCvc29397	PNP UI: AAA Warning when template contains AAA authorization commands

Release 1.3.2 Open Caveats

Caveat ID Number	Headline
CSCvc53581	Bulk Import action yields no response from UI
CSCvc53590	New device rule under TFTP Project will create dummy " config"
CSCvc53599	Template files are uploaded in the Config page in Unclaimed Flow
CSCvc53606	User created template with excape ${esc.d} is being treated as variable in UI
CSCvc55317	Change Config file to Template has no effect on PnP Project Edit

Release 1.3 Resolved Caveats

Caveat ID Number	Headline
CSCuu09487	" VTP mode Server" related config does not get applied from a saved file.
CSCuv19160	Config lock mode during redundancy prevents PnP redirection.
CSCuv42560	Trustpool bundle fails to deploy on devices with smaller nvram space.
CSCuw44673	Traceback:Sleep with expired managed timer -Process=" XEP_pnp-zero-touch"
CSCuw83141	PnP Image Upgrade failing on CSR 1000V
CSCux52544	PnP Fails to Initiate with Non-VLAN1 Feature Configured
CSCux54515	Cat3k Edison shows method 'manual' instead of DHCP.
CSCux86052	SMANRP-3-CMDCONNECT: Connection to local interactive relay failed
CSCuz74651	Reset does not put the Provisioned Stack Switch back to Pending state
CSCuz79238	Unable to resolve license mismatch if master has lower license level
CSCuz80826	PnPError msg " System resources could be depleted or unexpected failure
CSCuz81037	3650 stack crashes at FED when reload after V-mismatch
CSCuz81156	PNP UI - Image Conf - Used old API to get product id for platform name

Release 1.3 Open Caveats

Caveat ID Number	Headline
CSCva38541	PnP vrf discovery error with Device Certification sdn-network-infra-iwan
CSCvb31676	/ca/pem is missing Grapevine CA required by POSIX PnP Agent
CSCvb41181	DHCP ip not received on VRF interface of ASR1k devices after wr/reload
CSCvb56482	Autoinstall prevents pnp discovery - DHCP address renew loop - No set default route / gateway.
CSCvb59877	Config Template VM error not visible if the file opened was scrolled down
CSCvb71680	Not able to edit and remove the config file from project rule

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.
- 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 IWAN App Release 1*—List of open source code used in the Cisco IWAN and Cisco Network Plug and Play applications for APIC-EM.

Obtaining Documentation and Submitting 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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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.

Related Documentation