



Release Notes for Cisco Network Plug and Play

First Published: 2015-11-4

Last Updated: 2015-12-11

Contents

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

- [General Availability Release 1.0.1](#)
- [General Availability Release 1.0](#)

These release notes contain the following sections:

- [Introduction, page 1](#)
- [Supported Platforms and Software Requirements, page 1](#)
- [Limitations, page 4](#)
- [Sizing Guidelines, page 4](#)
- [Upgrading a Cisco Catalyst 3650 or 3850 Series Switch to Cisco IOS XE Denali 16.1.1 While Provisioning, page 5](#)
- [Caveats, page 5](#)
- [Related Documentation, page 7](#)
- [Obtaining Documentation and Submitting a Service Request, page 8](#)

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.

Supported Platforms and Software Requirements

The following tables list Cisco routers, switches, wireless access points, 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
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
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	3.6.3E, 3.7.2E, 16.1.1E
Cisco Catalyst 3750-X Series Switches	3750X	15.2.2E3, 15.2.4E ¹
Cisco Catalyst 3850 Series Switches	3850	3.6.3E, 3.7.2E, 16.1.1E
	3850-12X48U ² 3850-12XS ² 3850-16XS ² 3850-24XS ² 3850-32XS ²	3.7.2E
Cisco Catalyst 4500 Series Switches	Supervisor 6-E/6L-E Supervisor 7-E/7L-E Supervisor 8-E	3.6.3E, 3.7.2E, 3.8.0E
Cisco Catalyst 4500-X Series Switches	4500X-16, 32	3.6.3E, 3.7.2E, 3.8.0E
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 is supported only by using the DHCP options T and Z, and the non-VLAN 1 feature is not supported.

Table 2 Supported Cisco Routers

Platform	Models	Software Release
Cisco 800 Series Routers	819 829 866 867 881 886 887 888 891 892 896 897 898 899	15.5(3)M, 15.5(3)M1
Cisco 1900 Series Integrated Services Routers	1921 1941	15.5(3)M, 15.5(3)M1
Cisco 2900 Series Integrated Services Routers	2901 2911 2921 2951	15.5(3)M, 15.5(3)M1
Cisco 3900 Series Integrated Services Routers	3925 3925E 3945 3945E	15.5(3)M, 15.5(3)M1
Cisco 4000 Series Integrated Services Routers	4321 4331 4351 4431 4451-X	15.5(3)S, 15.5(3)S1
Cisco ASR 1000 Series Aggregation Services Routers	ASR1001 ASR1001-X ASR1002 ASR1002-X ASR1004 ASR1006 ASR1013	15.5(3)S, 15.5(3)S1
Cisco Cloud Services Router	CSR 1000V	15.5(3)S, 15.5(3)S1

Table 3 Supported Cisco Wireless Access Points

Platform	Models	Software Release
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

Limitations

Table 3 Supported Cisco Wireless Access Points (continued)

Platform	Models	Software Release
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

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
 - 4000 Series, with software release 15.5(3)S1
- Cisco Switches:
 - 3850 Series, with software release 3.6.3E or 16.1.1E
 - 3650 Series and 4500 Series with Supervisor 7-E/8-E, with software releases 3.6.3E, 3.7.2E, or 16.1.1E

Limitations

The bulk import feature function is similar to adding new rules that can set the device to the pending state. When you export the site and device database, the application displays the correct rule state. In such a scenario, the device will need to contact the APIC-EM controller again to return to the provisioned state.

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 2000 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 1.0.1 Resolved Caveats, page 6](#)
- [Release 1.0.1 Open Caveats, page 6](#)
- [Release 1.0 Open Caveats, page 7](#)

Caveats

Release 1.0.1 Resolved Caveats

Caveat ID Number	Headline
CSCUw27705	PnP should not upgrade image when same image running on router
CSCUw46498	AP PnP: PnP cert install failure during scale test
CSCUw72946	The filter is case sensitive in configuration PAge of APIC-EM
CSCUw75078	Unable to Clone PnP Project with a Space character
CSCUw76822	Bulk Import Issues : APIC EM Version 1.0.0.316
CSCUw92795	PnP UI stuck when Edit device Config with TFTP server provisioned

Release 1.0.1 Open Caveats

Caveat ID Number	Headline
CSCUt25533	PnPA: non-vlan CLI should only apply to newly bootup devices
CSCUu09487	"VTP mode Server" related config does not get applied from a saved file.
CSCUu92950	Continuous TFTP requests for config while PnP is in progress
CSCUv03573	Nonstop Autoinstall message after PnP server reloads router w/ new image
CSCUv19160	Config lock mode during redundancy prevents PnP redirection.
CSCUv23097	Trustpool fails on HA setup as certificates dont get copied over.
CSCUv42560	Trustpool bundle fails to deploy on devices with smaller nvram space.
CSCUw15272	PNP non-vlan 1 zero-touch upgrade is not working
CSCUw44673	Traceback:Sleep with expired managed timer -Process=" XEP_pnp-zero-touch"
CSCUw75002	ISR3945 router stuck in non-terminal state PKI_INSTALL_REQUESTED
CSCUw83101	CSR interface admin shutdown during PnP DHCP discovery + CD/DVD drive
CSCUw83141	PnP Image Upgrade failing on CSR 1000V
CSCUx37557	Polaris Pnp: need to support upgrade btw Nova and Polaris using APIC-EM

Release 1.0 Open Caveats

Caveat ID Number	Headline
CSCut25533	PnPA: non-vlan CLI should only apply to newly bootup devices
CSCuu09487	"VTP mode Server" related config does not get applied from a saved file.
CSCuu92950	Continuous TFTP requests for config while PnP is in progress
CSCuv03573	Nonstop Autoinstall message after PnP server reloads router w/ new image
CSCuv19160	Config lock mode during redundancy prevents PnP redirection.
CSCuv23097	Trustpool fails on HA setup as certificates dont get copied over.
CSCuv42560	Trustpool bundle fails to deploy on devices with smaller nvram space.
CSCuw15272	PNP non-vlan 1 zero-touch upgrade is not working
CSCuw27705	PnP should not upgrade image when same image running on router
CSCuw44673	Traceback:Sleep with expired managed timer -Process="XEP_pnp-zero-touch"
CSCuw46498	AP PnP: PnP cert install failure during scale test
CSCuw72946	The filter is case sensitive in configuration PAgE of APIC-EM
CSCuw75002	ISR3945 router stuck in non-terminal state PKI_INSTALL_REQUESTED
CSCuw75078	Unable to Clone PnP Project with a Space character
CSCuw76822	Bulk Import Issues : APIC EM Version 1.0.0.316
CSCuw83101	CSR interface admin shutdown during PnP DHCP discovery + CD/DVD drive
CSCuw83141	PnP Image Upgrade failing on CSR 1000V
CSCuw92795	PnP UI stuck when Edit device Config with TFTP server provisioned

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.
- [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* at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: 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. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.