Release Notes for Cisco DNA Center, Release 1.3.0.x

First Published: 2019-05-31

Last Modified: 2020-07-08

Release Notes for Cisco DNA Center, Release 1.3.0.x

This document describes the features, limitations, and bugs for Cisco DNA Center, Release 1.3.0.x.

Change History

The following table lists changes to this document since its initial release.

Table 1: Document Change History

Date	Change	Location
2020-07-08	Noted that IPv6 is not supported on Cisco Catalyst 9800 fabric devices.	New and Changed Information, on page 3
2020-04-10	Added that you can create a new AP_VLAN (2045) and template (ApAutzTemplate) on edge devices for AP connectivity.	New and Changed Information, on page 3
2020-03-18	Added an open bug: CSCvt00402.	Open Bugs—Non-High Availability
2020-02-18	Added the list of packages and resolved bugs in Cisco DNA Center 1.3.0.7.	New and Changed Information, on page 3 Resolved Bugs, on page 22
2020-02-05	Added CSCvq69305 and CSCvr12994 as resolved bugs in Cisco DNA Center 1.3.0.6.	Resolved Bugs, on page 22
2020-01-28	Added information about the **Wireless Pool** option.	Added information about the **Wireless Pool** option.
	Added CSCvs74635 as a resolved bug in Cisco DNA Center 1.3.0.6.	Resolved Bugs, on page 22
	Updated the following package version for Cisco DNA Center 1.3.0.6: • Cisco SD-Access: 2.1.46.60001	New and Changed Information, on page 3

Date	Change	Location
2020-01-09	Added the list of packages and resolved bugs in Cisco DNA Center 1.3.0.6.	New and Changed Information, on page 3 Resolved Bugs, on page 22
2019-11-05	Added the list of packages and resolved bugs in Cisco DNA Center 1.3.0.5.	New and Changed Information, on page 3 Resolved Bugs, on page 22
2019-10-16	Noted that Cisco DNA Center is not compatible with Cisco IMC 4.0(4c) and later.	Supported Firmware, on page 15
2019-10-08	Updated C9200 part numbers for fabric edge nodes with Cisco SD-Access wireless support in Cisco DNA Center 1.3.	New and Changed Information, on page 3
2019-10-07	Updated the description of CSCvr03768.	Resolved Bugs, on page 22
2019-10-03	Added CSCvr03768 as a resolved bug in Cisco DNA Center 1.3.0.4.	Resolved Bugs, on page 22
2019-09-08	Added the list of packages and resolved bugs in Cisco DNA Center 1.3.0.4.	New and Changed Information, on page 3 Resolved Bugs, on page 22
	Added open bugs: CSCvq61912, CSCvq70700, CSCvq97736, CSCvr00675, CSCvr01185, CSCvr18650, CSCvr19265, and CSCvr19604.	Open Bugs—Non-High Availability
2019-08-28	Added Cisco Catalyst 9500 High Performance switches to the list of platforms supported on the Cisco Catalyst 9800 Embedded Wireless Controller.	New and Changed Information, on page 3
2019-08-06	Added a limitation related to Cisco Connected Mobile Experiences (CMX).	Limitations and Restrictions, on page 31
	Noted that starting in Cisco DNA Center 1.3, the following Cisco Catalyst 9500 High Performance switches can be used as seed devices and PnP agents for LAN automation: • C9500-32C • C9500-32QC • C9500-24Y4C • C9500-48Y4C	New and Changed Information, on page 3
2019-08-01	Moved CSCvn69306 to the Resolved Bugs table.	Resolved Bugs, on page 22
	Added the list of packages and resolved bugs in Cisco DNA Center 1.3.0.3.	New and Changed Information, on page 3 Resolved Bugs, on page 22

Date	Change	Location
2019-07-25	Added CSCvq54634, CSCvq65765, and CSCvq65784.	Open Bugs—Non-High Availability
	Added CSCvq54357.	Resolved Bugs, on page 22
	Updated the LAN automation enhancements description.	New and Changed Information, on page 3
2019-07-03	Added limitations related to Intelligent Capture.	Limitations and Restrictions, on page 31
2019-06-21	Added the list of packages and resolved bugs in Cisco DNA Center 1.3.0.2.	New and Changed Information, on page 3 Resolved Bugs, on page 22
2019-05-31	Initial release.	—

Upgrade to the Latest Cisco DNA Center Release

For information about upgrading your current release of Cisco DNA Center, see the Cisco DNA Center Upgrade Guide.

New and Changed Information

The following table shows the updated packages and the versions.

Table 2: Updated Packages and Versions in Cisco DNA Center Release 1.3.0.x

Package Name	Release 1.3.0.7	Release 1.3.0.6	Release 1.3.0.5	Release 1.3.0.4	Release 1.3.0.3	Release 1.3.0.2	Release 1.3
System Updates							
System	1.2.0.1021	1.2.0.1013	1.2.0.1013	1.2.0.1013	1.2.0.1008	1.2.0.998	1.2.0.998
Package Updates							
Application Policy	2.1.42.170001	2.1.42.170001	2.1.42.170001	2.1.42.170001	2.1.42.170001	2.1.40.170897	2.1.40.170897
Assurance - Base	1.3.1.144	1.3.1.144	1.3.1.140	1.3.1.140	1.3.1.137	1.3.0.1345	1.3.0.1344
Assurance - Sensor	1.3.0.1313	1.3.0.1313	1.3.0.1313	1.3.0.1313	1.3.0.1313	1.3.0.1313	1.3.0.1313
Automation - Base	2.1.47.60007	2.1.45.60040	2.1.44.60004	2.1.43.60042	2.1.42.60056	2.1.41.60025	2.1.40.61847
Automation - Intelligent Capture	2.1.47.60007	2.1.45.60040	2.1.43.60042	2.1.43.60042	2.1.42.60056	2.1.41.60025	2.1.40.61847

Package Name	Release 1.3.0.7	Release 1.3.0.6	Release 1.3.0.5	Release 1.3.0.4	Release 1.3.0.3	Release 1.3.0.2	Release 1.3
Automation - Sensor	2.1.47.60007	2.1.45.60040	2.1.43.60042	2.1.43.60042	2.1.42.60056	2.1.41.60025	2.1.40.61847
Cisco DNA Center Platform	1.1.1.2	1.1.1.2	1.1.1.2	1.1.1.2	1.1.1.2	1.1.0.4	1.1.0.4
Cisco DNA Center UI	1.3.1.255	1.3.1.254	1.3.1.253	1.3.1.250	1.3.1.241	1.3.0.221	1.3.0.219
Cisco SD-Access	2.1.47.60008	2.1.46.60001	2.1.44.60004	2.1.43.60045	2.1.42.60058	2.1.41.60025	2.1.40.61847
Command Runner	2.1.45.60040	2.1.45.60040	2.1.43.60042	2.1.43.60042	2.1.41.60025	2.1.41.60025	2.1.40.61847
Device Onboarding	2.1.47.60007	2.1.45.60040	2.1.43.60042	2.1.43.60042	2.1.42.60056	2.1.40.61847	2.1.40.61847
Image Management	2.1.47.60007	2.1.45.60040	2.1.43.60042	2.1.43.60042	2.1.42.60056	2.1.41.60025	2.1.40.61847
NCP - Base	2.1.45.60040	2.1.45.60040	2.1.43.60042	2.1.43.60042	2.1.40.61847	2.1.40.61847	2.1.40.61847
NCP - Services	2.1.45.60040	2.1.45.60040	2.1.44.60004	2.1.43.60042	2.1.42.60056	2.1.41.60025	2.1.40.61847
Network Controller Platform	2.1.47.60007	2.1.45.60040	2.1.44.60004	2.1.43.60046	2.1.42.60056	2.1.41.60025	2.1.40.61847
Network Data Platform - Base Analytics	1.3.1.204	1.3.1.204	1.3.1.204	1.3.1.204	1.3.1.204	1.3.0.189	1.3.0.189
Network Data Platform - Core	1.3.1.615	1.3.1.615	1.3.1.615	1.3.1.615	1.3.1.615	1.3.0.513	1.3.0.513
Network Data Platform - Manager	1.3.1.185	1.3.1.185	1.3.1.185	1.3.1.185	1.3.1.185	1.3.0.173	1.3.0.173
Path Trace	2.1.47.60007	2.1.45.60040	2.1.43.60042	2.1.43.60042	2.1.42.60056	2.1.41.60025	2.1.40.61847

New and Changed Features

The following tables summarize the new and changed features in Release 1.3.0.x.

Table 3: New Software Feature in Cisco SD-Access, Release 1.3.0.6

Feature	Description
Ability to define an IP address pool as a wireless pool	Cisco DNA Center, Release 1.3.0.6 provides the ability to select an IP pool as a wireless pool. You can choose from only the defined wireless pool while configuring the wireless SSID for the fabric. To enable the **Wireless Pool** toggle button, from the Cisco DNA Center home page, click **Provisioning** > **Fabric** > ***Fabric Name*** > **Host Onboarding** > ***VN Name*** > **Advanced View**.

Table 4: New and Changed Features in Cisco DNA Center, Release 1.3

Feature	Description
Localization	You can view the Cisco DNA Center GUI screens in English (the default), Chinese, Japanese, or Korean. To change the default language, simply change the locale in your browser to one of the supported languages: Chinese, Japanese, or Korean. **Note** While most screens—including the home page, tools, online help, and REST APIs—are localized, the Assurance screens are not localized.
Network hierarchy	When you select an area, building, or floor on the **Network Hierarchy**, **Network Settings**, or **Provision** page, the hierarchical selection is retained when you switch between these pages.
Design usability enhancement	The options under the **Design** menu are available as a drop-down list.
Policy usability enhancement	The options under the **Policy** menu are available as a drop-down list.
Provision page navigation enhancement	The **Inventory** and **Plug and Play** menu options are available under **Provision** > **Device** as a drop-down list.
Inventory	Starting in Cisco DNA Center, the **Inventory** feature is merged with the **Provision** page. From the Cisco DNA Center home page, click **Provision**. From the **Provision Devices** page, choose **Actions** > **Inventory** to view and use the inventory features.
Image Repository	Starting in Cisco DNA Center 1.3, the **Image Repository** tool is merged with the site-based Image Repository that is available as part of the **Design** page. Starting in Cisco DNA Center 1.3, you can assign a software image to device series filtered from cisco.com as well as to custom device series.
IPv6 support	You can now create and reserve IPv6 address pools in addition to IPv4 address pools.
System 360 overview	The System 360 Overview tab is updated to provide metrics of various functions of Cisco DNA Center in dashlets. The metrics include Hosts, High Availability, Cluster Tools, System Management Updates, Backup, Application Health, Identity Services Engine (ISE), and IP Address Manager (IPAM).

Feature	Description
ROMMON upgrade	A ROMMON upgrade is included in the add-on for software image upgrade. For the ROMMON upgrade, the cisco.com configuration is mandatory. When a device is added, the latest ROMMON details are retrieved from cisco.com for applicable devices. Also, you import a base image or tag a base image, the ROMMON image is downloaded automatically from cisco.com.
Device upgrade readiness prechecks	Prechecks such as NFVIS Flash, Service Entitlement, Interface, CDP neighbors, Running Config, Spanning Tree Summary, and AP Summary are included as enhancements.
Retry option to resync Cisco ISE connectivity	If the Cisco ISE server configuration fails due to a password change, you can update the password and resync the ISE connectivity in the **Authentication and Policy Servers** page.
Ability to import new certificate file and export certificate details	You can import a new certificate file from your local system and export certificate details on the **System Settings > Settings > Trustpool** page.
Schedule discovery	You can schedule discovery for a later time.
Include SSH key information in exported device credentials	You can include information such as the SSH key and initial SSH key algorithm in the exported device credentials.
View additional device details in the Topology page	You can view additional device details such as device IP address and device name suffix in the Topology page.
View all options available in the Topology page	By clicking the **Take a Tour** link, you can view the details of all options available in the Topology page.

Table 5: New and Changed Software Features in Cisco Wireless, Release 1.3

Feature	Description
Support for N+1 High Availability	Cisco DNA Center Release 1.3 introduces support for N+1 High Availability (HA) on the Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller platforms. N+1 HA allows a single Cisco Wireless Controller to be used as a backup controller for multiple primary controllers. These wireless controllers are independent of each other and do not share configuration or IP addresses on any of their interfaces. Cisco DNA Center supports primary and secondary controller configurations for N+1 HA. N+1 HA is configured at the AP level, not at the global level. Configurations are pushed directly to the AP.
Support for guest anchor Inter-Release Controller Mobility (IRCM)	Inter-Release Controller Mobility (IRCM) supports seamless mobility and wireless services across different Cisco Wireless Controllers with different software versions. Cisco DNA Center supports guest anchor functionality for the following device combinations: • Cisco AireOS Controller as a foreign controller with a Cisco AireOS Controller as an anchor controller. • Cisco AireOS Controller as a guest anchor controller with a Cisco Catalyst 9800 Series Wireless Controller as a foreign controller. • Cisco Catalyst 9800 Series Wireless Controller as a foreign controller with a Cisco Catalyst 9800 Series Wireless Controller as an anchor controller.

Feature	Description
New platform support for Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series	The Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series supports the following platforms in this release: • Cisco Catalyst 9400 Series Switches • Cisco Catalyst 9500 Series Switches • Cisco Catalyst 9500 High Performance Series Switches
Advanced SSID configurations for enterprise and guest wireless network settings	The following advanced SSID configurations are added in this release: • Fast Transition over the DS Fast Transition over the DS is not applicable for wireless enterprise-open and guest network. • MFP Client Protection • Session Timeout • Client Exclusion • 11v BSS Transition Support: The following configurations are sent: • Max idle enable • Client user idle timeout • Directed multicast service • 11k: Neighbor list configuration is sent. This allows 11k capable clients to request neighbor reports containing information about known neighbor APs that are candidates for roaming.
AAA per SSID	**Note** The AAA per SSID feature is supported only for Cisco AireOS Controllers. The AAA per SSID feature solves the behavior of different AAA servers being mapped to different sites, buildings, and floors, which are managed by the same Cisco Wireless Controller. Cisco DNA Center pushes an SSID with respect to the AAA server. A network profile with an SSID and different sites is mapped with different AAA servers. Based on the AAA server, the SSID with a different name is pushed to the wireless controller after the wireless controller provisioning. Only two AAA servers are supported per site, building, and floor. Only one ISE server is mapped to a particular site, building, or floor. Brownfield is not supported. You cannot map the ISE server as the primary and the AAA server as the secondary to a particular site.

Table 6: New and Changed Software Features in Cisco SD-Access, Release 1.3

Feature	Description
IPv6 endpoint support in fabric	Fabric devices can now onboard IPv6 wired and wireless clients into a Cisco SD-Access fabric that has an IPv4 underlay. The following features are supported for IPv6 endpoints: • Layer 2 border handoff • Multicast, Broadcast and Link Local multicast • Layer 3 handoff • DHCP and DNS servers accept IPv6 addresses, in addition to IPv4 addresses • Client IP address assignment supports static IP, SLAAC, and DHCP • IPv6 and IPv4 clients can co-exist in the same VLAN. • IPv6 multicast support for both native and headend replication in the overlay. Note the following constraints: • IPv6 guest VN is not supported in Cisco SD-Access. • IPv6 is not supported on Cisco Catalyst 9800 fabric devices.
LAN automation enhancements	Cisco Catalyst 9400 Series Switches with 40-G ports now support LAN automation. Cisco Catalyst 9500 High Performance Series Switches running IOS XE 16.11.1 support LAN Automation. The switches now boot up in Layer 2 mode instead of Layer 3 mode. Validation of LAN subnet reachability from Cisco DNA Center: if the primary device on the LAN subnet is not reachable from Cisco DNA Center, an error message is displayed. The **LAN Automation** page now refreshes automatically.
	The following Cisco Catalyst 9500 High Performance series switches can be used as seed devices and PnP agents for LAN automation: • C9500-32C • C9500-32QC • C9500-24Y4C • C9500-48Y4C
Support for extended node	Extended nodes are those devices that run in Layer 2 switch mode and do not support fabric technology natively. You can now configure extended nodes in a Cisco SD-Access fabric. For information on configuring an extended node, see the *Configure an Extended Node* section in the *Cisco DNA Center User Guide*.
Support for port channels	You can now create or delete port channels between the fabric edge ports and the extended node uplinks.
Device support for Fabric in a Box	You can now configure a Cisco Catalyst 9500 High Performance Series Switch to function as a Fabric in a Box.

Feature	Description
Ability to create a new AP_VLAN (2045) and template (ApAutzTemplate) on edge devices for AP connectivity	In Cisco DNA Center 1.2.x, when you perform a VN-to-IP pool assignment for an AP pool under the INFRA_VN, a VLAN with a name syntax like <*ip pool*>_INFRA_VN is created in every site where the assignment occurs. In Cisco DNA Center 1.3.x, a dedicated AP VLAN with the name AP_VLAN and VLAN ID 2045 is created with a corresponding SVI interface. After you perform the VN-to-IP pool assignment under INFRA_VN for an AP pool, the IP address is assigned to the SVI interface. This can be used in Cisco ISE to assign the VLAN for AP profiling. This feature does not delete or change the existing fabric behavior for 1.2.x upgrades, which continue to use the old VLAN. If a new fabric site is created, a VLAN is created with the AP_VLAN name and VLAN ID 2045. If you want to standardize the AP_VLAN name to use in the Cisco ISE profile, you must remove the old VN-to-IP pool assignment and recreate the VN-to-IP pool assignment for the AP pool. This change requires network downtime; therefore, plan this change for a maintenance window.
Layer 2 border local endpoints: scale of 32,000	Cisco Catalyst 9500 Switches or Cisco Catalyst 9400 Switches deployed as a Layer 2 border can now have up to 32,000 local endpoints connected to them.
AAA per SSID	**Note** The AAA per SSID feature is supported only for Cisco AireOS Controllers. AAA per SSID feature solves the behavior of different AAA servers being mapped to different sites, buildings, and floors, which are managed by the same Cisco Wireless Controller. Cisco DNA Center pushes an SSID with respect to the AAA server. A network profile with an SSID and different sites are mapped with different AAA servers. Based on the AAA server, the SSID with a different profile name is pushed to the wireless controller after the wireless controller provisioning. Only two AAA servers are supported per site, building, and floor. Only one ISE server is mapped to a particular site, building, or floor. Brownfield is not supported. You cannot map an ISE server as primary and AAA server as secondary to a particular site.
New platform support for Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series	The Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series supports the following platforms in this release: • Cisco Catalyst 9400 Series Switches • Cisco Catalyst 9500 Series Switches • Cisco Catalyst 9500 High Performance Series Switches

Feature	Description
Advanced SSID configurations for enterprise and guest wireless network settings	The following advanced SSID configurations are newly added in this release: • Fast Transition over the DS Fast Transition over the DS is not applicable for wireless enterprise-open and guest network. • MFP Client Protection • Session Timeout • Client Exclusion • 11v BSS Transition Support: The following configurations are sent: • Max idle enable • Client user idle timeout • Directed multicast service • 11k: Neighbor list configuration is sent. This allows 11k capable clients to request neighbor reports containing information about known neighbor APs that are candidates for roaming.

Table 7: New Hardware in Cisco SD-Access, Release 1.3

Device Role	Product Family	Part Number	Description
Fabric border and control plane node	Cisco Catalyst 9600 Series Switches	C9600-SUP-1 C9600-LC-48YL C9600-LC-24C	Cisco Catalyst 9600 Series Switches can be configured as a fabric border node, fabric control plane node, or both.
Fabric border node	Cisco Nexus 7700 Series Switches	N77-SUP3E	The Nexus 7700 Series Switch with the Supervisor Module-3 (SUP 3E) can be configured as a fabric external border node, only with the M3 line card.
Fabric edge node	Cisco Catalyst 9200 Series Switches	C9200L-24PXG-2Y C9200L-24PXG-4X C9200L-48PXG-2Y C9200L-48PXG-4X	Cisco Catalyst 9200 Series Multigigabit switches can be configured as a fabric edge node.

Device Role	Product Family	Part Number	Description
Fabric edge node with SD-Access Wireless support	Cisco Catalyst 9200 Series Switches	-	All Cisco Catalyst 9200 Series Switches, except the Catalyst 9200L Series, support fabric edge with wireless to terminate VXLAN tunnel. Note that the Cisco Catalyst 9800 Embedded Wireless Controller is not supported on either the Cisco Catalyst 9200 Series or Cisco Catalyst 9200L Series Switches.
Access Points	Cisco Catalyst 9100 Series Wi-Fi 6 (802.11ax) Access Points	C9120AXI-x C9120AXE-x C9120AXP-x	The Cisco Catalyst 9100 Series Access Points can be configured as a Fabric Wireless node.

Table 8: New and Changed Features for Cisco DNA Assurance, Release 1.3

Feature	Description
Application Experience enhancements	Enhanced the **Health** > **Application Health** window: • Added timeline range option for 7 days. • Changed non-standard NBAR applications to display their HTTP host name or SSL common name, if available. • For the **Application** dashlet, the following data columns can be added to the table: **Jitter**, **Client Network Latency**, and **Server Network Latency**.
	Enhanced the **Application 360** window: • Added a filter for application data based on location. • Added charts for the **Application Experience** slide-in pane for the following metrics: **Jitter**, **Client Network Latency**, and **Server Network Latency**. • Added the **Observed** data column under **DSCP** to the **Application Experience** dashlet table. The **Observed** column indicates the application's current DSCP value.
	Enhanced the **Device 360** window for routers: • Added filters in the **Application Experience** category that enables you to filter application data from specific VRFs and router interfaces. • Changed non-standard NBAR applications to display their HTTP host name or SSL common name, if available. • Added the **Observed** data column under **DSCP** to the **Application Experience** category table. The **Observed** column indicates the application's current DSCP value. • Added the **Jitter** data column for the **Application Experience** category table.

Feature	Description

IPv6 address support for wireless and wired clients	Enhanced the **Health** > **Client** window:
	• Fixed the **IPv6 Address** data column to display the client's IPv6 address in the following locations:
	  • **Client Health Summary** dashlet in the slide-in panes for **Wireless Clients** and **Wired Clients**
	  • **Client Devices** dashlet
	Note Assurance supports clients with multiple IPv6 addresses. You can view the additional addresses by hovering your cursor over the tooltip link in parentheses. For example, **(1 more)**.
	• Added filtering for IPv6 addresses in the **Client Devices** dashlet table.

	Enhanced the **Client 360** window: • Fixed **IPv6** above the timeline to display the client's IPv6 address. • Added **IPv6** to the **Onboarding** category. • Added **IPv6** to the **Event Viewer** category. • Fixed **IPv6 Address** from the **Detail Information** category to display the client's IPv6 address. **Note** Assurance supports clients with multiple IPv6 addresses. You can view the additional addresses by hovering your cursor over the tooltip link in parentheses. For example, **(1 more)**.
Simplifies the health score formula for wireless clients	• Simplifies the individual health score calculation for wireless clients. • Simplifies the RSSI and SNR connectivity scores calculation for wireless clients.
Support KPIs and baselining for On-Device AI (on-premises)	Added the following enhancements: • View the issues generated by Assurance for excessive onboarding. The root causes for the excessive onboarding issues are AAA, DHCP, and Association. The issues are generated through the baseline. • In the **Global Issues** window, you can click an issue in the **Issue Type** column to open a slide-in pane with additional details. In the slide-in pane, click an issue in the **Issue Instance** column to view more details about the issue instance. • While configuring issue settings, if you set the **Device Type** as **All** and **Category** as **Onboarding** as the trigger condition, you can set the trigger condition to generate either baseline-based issues or threshold-based issues. • In the **Client Health** dashboard, for the **Client Onboarding Times** and **Client Count per SSID** dashlets, you can click the **Trend** tab to display a trend chart. Under **Trend**, you have the option to select **Baseline** to view the onboarding time baseline data (trend chart) or to view the client count data (trend chart) per SSID.

Feature	Description
Intelligent Capture	• Added the following location to manage Intelligent Capture for clients: **Assurance** > **Manage** > **Client Intelligent Capture** • Added the following location to manage Intelligent Capture for Access Points: **Assurance** > **Manage** > **AP Intelligent Capture**
Cisco ISE configuration unification	• Centralized Cisco ISE configuration for all of Cisco DNA Center in the NCP (Network Control Platform) location: **Settings** > **System Settings** > **Settings** > **Authentication and Policy Servers** After a Cisco ISE server is successfully configured, NCP sends the configuration details (that is, pxGrid nodes, keystore, and truststore files) to Network Data Platform (NDP). • Added the following location to enable anonymization for PPI (personally identifiable information): **Settings** > **System Settings** > **Settings** > **Anonymize Data**

Cisco SD-Access Compatibility Matrix

For information about Cisco SD-Access hardware and software support for Cisco DNA Center, see the Cisco SD-Access Hardware and Software Compatibility Matrix. This information is helpful for deploying Cisco SD-Access.

Cisco DNA Center-Supported Devices

For information about devices such as routers, switches, wireless access points, Cisco Enterprise NFV Infrastructure Software (NFVIS) platforms, and software releases supported by each application in Cisco DNA Center, see Supported Devices.

Compatible Browsers

The Cisco DNA Center web interface is compatible with the following HTTPS-enabled browsers:

- Google Chrome: Version 73.0 or later
- Mozilla Firefox: Version 65.0 or later

We recommend that the client systems you use to log in to Cisco DNA Center be equipped with 64-bit operating systems and browsers.

Cisco DNA Center Scale

For Cisco DNA Center scale numbers, see the Cisco DNA Center Data Sheet.

IP Address and FQDN Firewall Requirements

To determine the IP addresses and fully qualified domain names (FQDNs) that must be made accessible to Cisco DNA Center through any existing network firewall, see "Required Internet URLs and FQDNs" in the Cisco DNA Center Installation Guide.

Supported Firmware

Cisco Integrated Management Controller (Cisco IMC) versions are independent from Cisco DNA Center releases. This release of Cisco DNA Center has been validated against the following firmware:

- Cisco IMC Version 3.0(3f) for appliance model DN1-HW-APL
- Cisco IMC Version 3.1(2c) for appliance model DN2-HW-APL
- Cisco IMC Version 3.1(3a) for appliance model DN2-HW-APL-L
- Cisco IMC Version 4.0(1a) for appliance model DN2-HW-APL-XL

The preceding versions are the minimum firmware versions. While some later versions are also supported, Cisco DNA Center is not compatible with Cisco IMC 4.0(4c) and later. Do not update later than Cisco IMC 4.0(4b).

Installing Cisco DNA Center

You can install Cisco DNA Center as a dedicated physical appliance purchased from Cisco with the Cisco DNA Center ISO image preinstalled. See the Cisco DNA Center Installation Guide.

Note The following applications are not installed on Cisco DNA Center by default. If you need any of these applications, you must manually download and install the packages separately.

- Application Policy
- Assurance - Sensor
- Automation - Sensor
- Cisco DNA Center platform
- Cisco SD-Access
- Intelligent Capture

For more information about downloading and installing a package, see "Manage Applications" in the Cisco DNA Center Administrator Guide.

Cisco DNA Center Platform Support

For information about the Cisco DNA Center platform, including information about new features, installation, upgrade, and open and resolved bugs, see the Cisco DNA Center Platform Release Notes.

Support for Cisco Connected Mobile Experiences

Cisco DNA Center supports Cisco Connected Mobile Experiences (CMX) 10.6.1. Earlier versions of CMX are not supported.

Note While configuring the CMX settings, do not include the # symbol in the CMX admin password. The CMX integration fails if you include the # symbol in the CMX admin password.

Plug and Play Considerations

Plug and Play Support

General Feature Support

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

- 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 Cisco IOS 15.2(6)E1, Cisco IOS 15.6(3)M1, Cisco IOS XE 16.3.2, or Cisco IOS XE 16.4 or later on the device.
- Image install and upgrade for Cisco Catalyst 9200 Series, Catalyst 9300 Series, Catalyst 9400 Series, Catalyst 9500 Series, Catalyst 3650 Series, and Catalyst 3850 Series switches are supported only when the switch is booted in install mode. (Image install and upgrade is not supported for switches booted in bundle mode.)

Secure Unique Device Identifier Support

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

- Cisco routers:
  - Cisco ISR 1100 Series with software release 16.6.2
  - Cisco ISR 4000 Series with software release 3.16.1 or later, except for the ISR 4221, which requires release 16.4.1 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 release 3.6.3E or 16.1.2E or later
  - Cisco Catalyst 3650 Series and 4500 Series with Supervisor 7-E/8-E, with software release 3.6.3E, 3.7.3E, or 16.1.2E or later
  - Cisco Catalyst 4500 Series with Supervisor 8L-E with software release 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 16.6.1 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
- Cisco Catalyst IE3300 Series with software release 16.10.1e or later
- Cisco Catalyst IE3400 Series with software release 16.11.1a or later

- NFVIS platforms:
  - Cisco ENCS 5400 Series with software release 3.7.1 or later
  - Cisco ENCS 5104 with software release 3.7.1 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: Cisco ISR 43xx, Cisco ISR 44xx, Cisco ASR1001-X/HX, Cisco ASR1002-HX
- Cisco switches: Cisco Catalyst 4500 Series with Supervisor 8-E/8L-E/9-E, Catalyst 9400 Series

Management Interface VRF Support

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:
  - Cisco 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

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

- Cisco 1100 Series ISR with software release 16.6.2 or later

Configure Server Identity

To ensure successful Cisco DNA Center discovery by Cisco devices, the server SSL certificate offered by Cisco DNA Center 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 administrator to upload a new server SSL certificate, which has the appropriate SAN values, to Cisco DNA Center.

The SAN 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 Cisco DNA Center certificate must be set according to the type of discovery being used by devices, as follows:

- For DHCP option-43 or option-17 discovery using an explicit IPv4 or IPv6 address, set the SAN field to the specific IPv4 or IPv6 address of Cisco DNA Center.
- For DHCP option-43 or option-17 discovery using a hostname, set the SAN field to the Cisco DNA Center hostname.
- For DNS discovery, set the SAN field to the plug and play hostname, in the format **pnpserver.*domain***.
- For Cisco Plug and Play Connect cloud portal discovery, set the SAN field to the Cisco DNA Center IP address if the IP address is used in the Plug and Play Connect profile. If the profile uses the Cisco DNA Center hostname, the SAN field must be set to the FQDN of the controller.

If the Cisco DNA Center IP address that is used in the Plug and Play profile is a public IP address that is assigned by a NAT router, 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 Cisco DNA Center, ensure that the proxy certificate has the same SAN fields with the appropriate IP address or hostname.

We recommend that you include multiple SAN values in the certificate, in case discovery methods vary. For example, you can include both the Cisco DNA Center 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 Cisco DNA Center certificate does not contain the appropriate value, the device cannot 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.

Bugs

Use the Bug Search Tool

Use the Bug Search tool to search for a specific bug or to search for all bugs in this release.

Procedure

Step 1 Enter the following URL in your browser:

https://tools.cisco.com/bugsearch

Step 2 In the **Log In** window, enter your registered cisco.com username and password and click **Log In**.

The **Bug Search** window opens.

Note If you do not have a cisco.com username and password, register at https://idreg.cloudapps.cisco.com/idreg/guestRegistration.do.

Step 3 To search for a specific bug, enter the bug ID in the **Search For** field and press **Return**.

Step 4 To search for bugs in the current release:

a) In the **Search For** field, enter **Cisco DNA Center** and press **Return**. (Leave the other fields empty.)

b) When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by modified date, status, severity, and so forth.

To export the results to a spreadsheet, click the **Export Results to Excel** link.

Open Bugs—Non-High Availability

The following table lists the open non-HA bugs in Cisco DNA Center for this release.

Table 9: Open Bugs—Non-HA

Bug Identifier	Headline
CSCvj41522	Importing a Plug and Play CSV with 25 APs fails.
CSCvn32554	Wireless controller goes into unmonitored state after a restore from the backup.
CSCvo21720	Network health appears for the Cisco Catalyst 9800 wireless controller in both the monitored and unmonitored sections.
CSCvo44394	When you try to add Cisco ISE 2.4 to Cisco DNA Center 1.3, the following certificate error is generated: `"Error establishing trust with ISE: Expected phrase [Enter URI for uploading ISE certificate chain:] wasn't received from ise"` The workaround is to configure the network MTU size to 9100 between Cisco ISE and Cisco DNA Center.
CSCvo60306	Device activation fails when the image is not the minimum supported image version.

Bug Identifier	Headline
CSCvp15026	Devices remain in Partial Collection Failure state after an incomplete provision and resynch. This problem occurs only when there is an incomplete manual clearing of CLI commands on a device. When a device goes through the full removal flow, subsequent synchronizations work correctly. Related bug: CSCvj15139.
CSCvp29213	A crash occurs when the RADIUS Change of Authorization (CoA) feature is triggered for an environment data update and the **clear cts environment-data** command is issued at the same time. The problem occurs because the **clear cts environment-data** command fails to clear the environment data.
CSCvp25402	After you delete a wireless controller with 4000 APs from Cisco DNA Center, it takes 25 minutes or longer for the wireless controller to be removed from the inventory.
CSCvp38271	Cisco Software-Defined Access: Events are missing from the Event Viewer on the Device 360 page.
CSCvp48020	IR829 does not display the correct Gigabit interface in the WAN interface drop-down list.
CSCvp48160	Software image management: Catalyst 6000 image activation fails while upgrading image version 152-2.SY to 152-2.SY*.
CSCvp49120	A Cisco Catalyst 6000 ISSU upgrade from SY2 to SY3 fails when the device has **snmp-server enable traps vstack** in the running configuration.
CSCvp51880	The Maglev Cassandra service fills up the disk with index files.
CSCvp53259	A Cisco DNA Center local backup fails if the maglev password starts with special characters.
CSCvp65347	The Time API takes a very long time to respond when there are multiple user sessions browsing the Assurance GUI.
CSCvp73793	The Cisco Catalyst 9800 wireless controller neighbor topology does not update the AP count in the inventory.
CSCvp75825	Air quality is missing randomly from an AP 360 page health chart.
CSCvp80992	Provisioning fails if you choose "Do not change" and enter an interface name.
CSCvp82437	The Flex Connect SSID with Cisco Catalyst 9800 does not appear on an AP when you choose VLAN name management.
CSCvp83057	External site borders point to other external borders in a site, which causes loops.
CSCvp85827	Border Gateway Protocol (BGP) advertises Multicast Rendezvous Point (RP) /32 and /128 prefixes from non-RP borders.
CSCvp88475	AP mode and uptime don't get updated, affecting Intelligent Capture functionality.
CSCvp95386	After upgrading the embedded wireless software on Cisco Catalyst 9000 devices from 16.10.1.e to 16.11.1s, the AP country code configuration is lost.
CSCvp96088	An image change on the wireless controller causes the AP Intelligent Capture 360 page to lose all data.

Bug Identifier	Headline
CSCvp99454	After upgrading from Cisco DNA Center 1.2.3 or 1.2.6 to 1.2.8, then 1.2.10, then 1.3, the Network Plug and Play menu option is available under the Tools menu. (The Network Plug and Play menu option should not be present.) If you upgrade from Cisco DNA Center 1.2.10 to 1.3, the Network Plug and Play menu option is not available under the Tools menu, which is correct.
CSCvq02712	Cisco DNA Center 1.3 SDA end users can HTTPS to the fabric edge default gateway IP address.
CSCvq54634	Multicast does not work on an edge device that is added to a fabric on which multicast is already enabled.
CSCvq55626	The NDP package upgrade fails from 1.2.10.4 to 1.3.0.3. The Elasticsearch pod does not run in the NDP namespace.
CSCvq57083	Maglev upgrade from 1.2.12 to 1.3.0.3 fails with the error "Timeout waiting to pull system update hook bundle."
CSCvq61912	After upgrading Cisco DNA Center to 1.3.0.4, the software image update status always shows **Activation in progress**.
CSCvq65765	After upgrading to Cisco DNA Center 1.3.0.3 and enabling the Autoconf feature, macro configurations are not removed from extended nodes.
CSCvq65784	When IPv4 multicasting is enabled on an edge device, Cisco DNA Center does not push the **ip igmp explicit-tracking** command to the Layer 2 handoff VLAN on the corresponding border device.
CSCvq97736	Parent catalog settings validation fails and packages cannot be retrieved from the cloud. This problem occurs only when the proxy is not configured through the Config wizard during ISO install. To work around this problem, SSH to the cluster IP and enter **magctl service restart -d catalogserver**. Wait for 90 seconds and then enter **maglev catalog settings validate**.
CSCvr01185	After migration, extended nodes are flagged as out of compliance.
CSCvr18650	Deploying an onboarding interface fails with the following error: `"NCSP10025: UserIntentProvisioningService error."`
CSCvr19265	After upgrading or restarting a node, the API `/api/system/v1/license/credentials/cco` returns a 502 error code and CCO credentials are not set. To work around this problem, enter the following CLI command to restart the license service: `$ magctl service restart -d license-service` Related bug: CSCvq70700.
CSCvr19604	After upgrading from Cisco DNA Center 1.2.12 to 1.3.0.4, the command **no macro auto global processing** is not pushed to the edge node after enabling AVC.
CSCvt00402	Catalyst 3k switch with 1.6GB flash size unable to do software image upgrade between 16.12.x images.

Open Bugs—High Availability

The following table lists the open high availability (HA) bugs in Cisco DNA Center for this release.

Table 10: Open Bugs—HA

Bug Identifier	Headline
CSCvn32215	In a three-node setup, if you bring down the node while LAN automation is in progress, the LAN automation status shows as complete, yet without success. This problem occurs if you perform a network-orchestration service restart or a full node restart while LAN automation is in progress. The network orchestration service doesn't resume the ongoing LAN automation session. It marks LAN automation as complete and releases all IP addresses allocated from IPAM. Users are expected to perform a configuration cleanup on the seed device, write-erase/reload discovered devices, and start a new LAN automation session.
CSCvo35174	Maglev cassandra-1 goes into the crashloop state on a three-node cluster after upgrading Cisco DNA Center.
CSCvo95706	The VIP toggles between the three nodes every minute and "Invalid VRRPv3 checksum" messages are seen in keepalived.

Resolved Bugs

The following tables list the resolved bugs in Cisco DNA Center Release 1.3.0.x.

Table 11: Resolved Bugs in Cisco DNA Center, Release 1.3.0.7

Bug Identifier	Headline
CSCvp34431	The increased length of the JWT token causes a wireless controller to fail posting WSA data.
CSCvq31127	Backup fails with the error "Taskname-BACKUP.fusion:postgres.
CSCvq80742	A system upgrade fails with the error "Kubernetes upgrade to version v1.10.2 failed."
CSCvr26483	MongoDB doesn't perform write operations, causing the identitymgmt service and other dependencies to fail.
CSCvr30114	Credential manager backup fails because the upsert to MongoDB fails.
CSCvr98064	Cisco DNA Center may fail to consistently apply CLI templates for RADIUS NAC configurations on a wireless controller.
CSCvs22065	In a three-node cluster, Cisco DNA Center might become unresponsive after more than 100 days of service.
CSCvs22210	Clicking a device in the Provision tab generates the error "An unknown error occurred. Please try again."
CSCvs26491	When provisioning a new AP, the policy tag gets deleted from the associated WLAN, and clients cannot access the WLAN.
CSCvs49949	The Maglev server restarts continuously when the backup server becomes unreachable.
CSCvs74635	A wireless connectivity problem occurs for a AAA override-enabled Virtual Extensible LAN (VXLAN) network identifier.

Table 12: Resolved Bugs in Cisco DNA Center, Release 1.3.0.6

Bug Identifier	Headline
CSCvo79143	A provisioning task hangs when the device is not reachable.
CSCvp87542	Cisco Catalyst 9800 Series Wireless Controller provisioning fails when a special character is used in the Cisco ISE shared key.
CSCvq04396	If there is a failure in the template, the failed status is not shown in red.
CSCvq37639	Wireless controller provisioning fails with the error "NCWL10481: DeviceInfo with Id xxxx could not be fetched from SPR."
CSCvq41612	Even though an image is present on the device, image distribution is triggered again.
CSCvq42193	The GUI shows an inventory collection partial failure, even though the device is successfully provisioned by Cisco DNA Center.
CSCvq42795	AP provisioning fails with the error "OwningEntityId" for a wireless controller that is missing in the database.
CSCvq65767	LAN automation fails after updating the management IP address of the seed device.
CSCvq69305	A vulnerability in the web-based user interface (Web UI) of Cisco DNA Center could allow an authenticated, remote attacker to perform an arbitrary command injection attack. The vulnerability is due to incorrect input validation of user-supplied data. An attacker could exploit this vulnerability by supplying a malicious input parameter on a form in the Web UI and then submitting that form. An exploit could allow the attacker to disable a menu option on the Web UI.
CSCvq80321	Assurance API yields invalid values for client slot ID and health score.
CSCvq80558	The ca/trustpool API returns a trustpool bundle instead of 404.
CSCvq90200	A heatmap persists even after AP disassociation.
CSCvq97467	Cisco DNA Center does not display virtual network information after upgrading from 1.2.10.4 to 1.3.0.3.
CSCvq98206	Cisco DNA Center-managed fabric devices report being in "Failed" provisioning state, even though their last provisioning task completed successfully.
CSCvr00675	Unable to modify a guest wireless SSID after upgrading from Cisco DNA Center 1.2 to 1.3 when Fast Transition is null.
CSCvr01901	An unexpected "DHCP IP address obtain failure" issue occurs for IPv6-only clients.
CSCvr02827	An access tunnel goes down and does not recover after applying a security fix with an AireOS wireless controller.
CSCvr02828	Upgrade from Cisco DNA Center 1.2.12 to 1.3.0.4: Applying a security fix for Site 2 fails with errors for devices in Site 1.

Bug Identifier	Headline
CSCvr12994	A vulnerability in the web-based management interface of Cisco DNA Center could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker needs administrator credentials. Cisco has released software updates that address the vulnerability described in this advisory. There are no workarounds that address this vulnerability. This advisory is available at the following link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190205-dnac-xss
CSCvr14061	The IP address manager (IPAM) service hangs and does not process requests in the RabbitMQ queue; multiple restarts are required to recover.
CSCvr18868	Cisco DNA Center 1.3.0.3: WPA2 personal passphrase with "&" fails to provision a Cisco Catalyst 9800 Series Wireless Controller.
CSCvr21334	Under heavy load, wireless clients are missing after several days.
CSCvr28080	Unable to provision wireless controllers because AP groups are deleted from wireless controllers.
CSCvr28905	AP provisioning fails with a "character '< ' is not allowed" error.
CSCvr36410	Enhancement: Provide an option to configure the country code.
CSCvr39983	A wired client does not show the correct value for the data transmitting and receiving rate.
CSCvr41201	Cisco DNA Center image distribution to the switch expires after one hour.
CSCvr45718	Cisco DNA Center is missing a port configuration and fails to deploy an onboarding interface.
CSCvr55987	Cisco Catalyst 9800 Series Wireless Controller with scaled APs takes longer than three hours to synchronize.
CSCvr56898	The Edit Virtual Network page under Host Onboarding is blank when the SGT is not available in Cisco ISE.
CSCvr71415	Unable to delete a device from Inventory due to a constraint violation exception.
CSCvr72715	Need a descriptive and user friendly message when integration fails due to an expired certificate.
CSCvr75269	Inventory collection fails due to a ConstraintViolationException ACL.
CSCvr85956	Inventory resync takes a long time for lldp_neighbors and VLAN features.
CSCvs02116	CPU utilization goes high on a fabric-in-a-box device when the connected client is asleep and traffic comes in for a client.
CSCvs25751	After successful bulk image distribution, some devices remain in distribution pending status.

Bug Identifier	Headline
CSCvs74635	After upgrading to Cisco DNA Center 1.3.0.6, wireless connectivity problems might occur. If the IP pool association from the AAA override for a client is not defined as part of the Cisco DNA Center host onboarding, connectivity issues occur. The problem occurs because with Cisco DNA Center 1.3.0.6, all IP pools that are not associated with a fabric SSID are deleted from the wireless controller during reprovisioning.

Table 13: Resolved Bugs in Cisco DNA Center, Release 1.3.0.5

Bug Identifier	Headline
CSCvp73577	Creating virtual networks in host onboarding touches the network unnecessarily.
CSCvr03397	Cisco Catalyst 9300 macros are applied to IP phone ports.
CSCvr33678	When a configuration is pushed through Cisco DNA Center, unreachable devices should be skipped.
CSCvr42301	The SPF service (spf-service-manager-service) restarts multiple times due to a java heap space out of memory error.
CSCvr54036	Multiple template provisioning operations hang when there are unreachable devices.
CSCvr54410	The SPF service (spf-service-manager-service) goes down after associating an IP pool to a virtual network.
CSCvr71732	During provisioning, the SPF logs report a device cache lookup failure as "DeviceInfoCache: Cache lookup miss for key instanceUuid and value." The log is repeated several times because the cache is not updated with the data retrieved from the database after the initial cache lookup failure.
CSCvr86995	During provisioning, a log message such as "Providing DataSource RemoteDCacheDataSource" is logged every time a device cache lookup occurs, which fills the SPF logs.

Table 14: Resolved Bugs in Cisco DNA Center, Release 1.3.0.4

Bug Identifier	Headline
CSCvp36746	Reprovisioning of devices managed by Cisco DNA Center results in looping validating the config.
CSCvp40461	IP address management: Cannot create a global pool for IPv4.
CSCvp60708	Cisco DNA Center does not deploy a CLI template to more than one device when the firewall profile is assigned to two or more sites.
CSCvp95942	Provisioning a composite template with three templates fails before moving to success.
CSCvp97687	During an upgrade to Cisco DNA Center 1.3, the GUI appears to hang at 40% complete.
CSCvp99546	Fabric in a box: Synchronization occasionally takes longer than 30 minutes.
CSCvq02954	CommonBorder issues with INFRA_VN pool addition/names.
CSCvq09405	Cannot update the IP address pool in a virtual network.

Bug Identifier	Headline
CSCvq15441	During LAN automation, Cisco DNA Center does not push "write memory" to the peer seed.
CSCvq24092	Cisco DNA Center pushes the wrong Pre-Auth ACL.
CSCvq32466	Devices are unreachable, partial collection failures occur, and SNMP timeouts occur frequently.
CSCvq33072	IPSLA operation and reachability sessions are not cleaned up when an IP address is unprovisioned.
CSCvq33516	Cannot create custom applications in Application Policy.
CSCvq43865	Due to a large number of hung pykube connections, the Maglev server is unresponsive to services.
CSCvq45083	While provisioning an IP pool in a virtual network, the following error is generated: "java.lang.OutOfMemoryError: GC overhead limit exceeded."
CSCvq47553	Plug and Play UI: The Advanced Configuration is missing a scroll bar for templates with many attributes.
CSCvq49014	Host onboarding hangs at "fetching interfaces details... please wait..."
CSCvq49071	CMX locations of clients are missing on Cisco DNA Center floor maps.
CSCvq50166	Cisco DNA Center fails to provision a wireless controller. The error "Incorrect input!" is generated.
CSCvq53679	Assurance incorrectly reports "Excessive time lag" for a wireless controller.
CSCvq53772	Floor creation fails due to an internal server error 500.
CSCvq54768	Cisco DNA Center silently pushes IBNS 2.0.
CSCvq57415	Cisco DNA Center 1.3 upgrade fails due to tenant data migration.
CSCvq66900	The same devices belong to unassigned and to a site.
CSCvq70566	After adding a device to the fabric with Layer 3 handoff, the device domain name is lost.
CSCvq72718	Cannot provision a template that contains the string "FAILED".
CSCvq74218	Reprovisioning a wireless controller fails after site or floor deletion.
CSCvq78788	The underlay custom route-map is removed during reprovisioning.
CSCvq79255	Software upgrade shows inconsistent software upgrade status.
CSCvq79576	Border devices are deleted from the inventory without the user explicitly deleting those devices.
CSCvq81674	Cisco DNA Center cannot claim devices with the Composite Day 0 template.
CSCvq81851	Cisco DNA Center upgrade fails due to tenant data migration: duplicated entry in serialnumberipaddressmapping.
CSCvq86871	The platform exchange grid (PxGrid) service crashes due to a large number of scalable groups.
CSCvq88657	Guest ACL reprovisioning fails on the 8.5 wireless controller.

Bug Identifier	Headline
CSCvq92227	Cisco DNA Center upgrade from 1.2.12 to 1.3.0.4: Access-tunnel is gone on the access point connected to the extended node after applying the security fix.
CSCvr00693	Adding internal border/Layer 3 handoff should not push config/connect to fabric edges.
CSCvr03768	The WSDL certificate in Cisco DNA Center's EJBCA Public Key Infrastructure (PKI) broker service expired on October 4, 2019. After this server certificate expires, Cisco DNA Center clients that use the EJBCA service for secure sessions fail to connect. As a result, Cisco DNA Center fails to onboard the Embedded Wireless Controller on Cisco Catalyst 9800 series devices and 1800s wireless sensors. Apart from the Cisco Catalyst 9800 Series Wireless Controller, there is no impact to any other WLC, switch, or router onboarding, or any other feature in Cisco DNA Center. There is no workaround for this problem. You must upgrade Cisco DNA Center to a version that has been patched to include a new WSDL certificate. The following Cisco DNA Center releases have the fix with the new WSDL certificate: 1.2.10.5, 1.2.12.2, 1.3.0.4, and 1.3.1.1. The new certificate has a 20-year expiry.

Table 15: Resolved Bugs in Cisco DNA Center, Release 1.3.0.3

Bug Identifier	Headline
CSCvp17987	Device upgrade scenario must handle version changes.
CSCvp22208	Deletion of an unreachable device fails in a nonfabric Assurance-only setup.
CSCvp23733	Cisco DNA Center UI pages stop responding and display no values.
CSCvp42650	While provisioning a device to a fabric with a template applied, the "ip dhcp snooping" command is not pushed to the devices in the fabric.
CSCvp52235	Fabric in a Box does not differentiate Layer 2 from Layer 3 links.
CSCvp58052	Provisioning an AP with the High RF profile fails with an internal error.
CSCvp59968	AAA RADIUS primary Auth/Acct and secondary Auth/Acct indexes are changed when a wireless controller is provisioned.
CSCvp60199	The Authentication configuration is not pushed to newly added switch stack members.
CSCvp70381	An AP search using global search doesn't show all access points with duplicate names.
CSCvp76474	Cannot reconfigure the edge switch port after the extended node is moved.
CSCvp78285	The Template programmer service goes down.
CSCvp78852	Reprovisioning fabric devices may cause removal of CTS commands.
CSCvp79622	mongodb resource usage is 100% on a scale setup, causing performance issues.
CSCvp79623	If you use the DNS name instead of the IP address in the URL to access the Cisco DNA Center UI, inventory data does not load.

Bug Identifier	Headline
CSCvp87542	Cisco Catalyst 9800 Series Wireless Controller provisioning failure when special characters are used in the Cisco ISE shared key.
CSCvp88833	Cisco DNA Center and Meraki Dashboard integration fails because of a missing systemName value.
CSCvp89837	If you upgrade Cisco DNA Center 1.2.10 to 1.3 and make embedded wireless LAN controller image changes, the controller goes into Unmonitored state, and Assurance shows no client data.
CSCvp90804	Backup/Restore GUI becomes unresponsive (until timeout) when backup server is unreachable.
CSCvp91221	NetFlow is not pushed to the router interface when using the management IP.
CSCvp94220	Cisco DNA Center doesn't remove the map-cache command from the second border/control plane when selecting "Connected to internet."
CSCvp95641	When you create a new port channel, greyed out interfaces become selectable again via the filter output.
CSCvp95666	When the secret key is changed, the confirmation message is unclear.
CSCvp95942	Provisioning a composite template with three templates fails before moving to success.
CSCvp96021	Spanning-tree portfast is not pushed when closed auth is used in host onboarding.
CSCvp96079	After an upgrade, the compliance check fails with a false alarm for the fabric role on the Cisco Nexus 7000.
CSCvp96167	In the **Border Node Configuration** page, when you click **Details**, it shows a page with only "test" on it.
CSCvp96981	Device 360 page: Moving an issue to resolved state returns an error.
CSCvq02516	Fabric-enabled wireless is not supported with Cisco Catalyst 9200 switches.
CSCvq02799	Filtering for clients with SNR less than 9 dB fetches incorrect clients.
CSCvq03217	Wireless controller inventory collection fails due to "ERROR: value too long for type character varying (255)".
CSCvq03589	Cisco Catalyst 9000 readiness check fails for flash: "Need recommended storage but not found."
CSCvq07100	Remove polling of "show licensing" command on Cisco Catalyst 4500 during resynchronization.
CSCvq16253	In Assurance, resolving one issue updates all issues to resolved state.
CSCvq24742	Cisco ISE-reported wireless client data causes Assurance to show wireless clients as wired clients.
CSCvq28692	Physical Neighbor Topology blank, BadMessageException: 500: Request header too large.
CSCvq32539	Template provisioning doesn't show the exact CLI command that failed due to an SSH connection time out.
CSCvq33368	Wireless controller inventory collection fails with the error "unique constraint p2plinkterminationpoint_bk."
CSCvq33426	An application upgrade fails due to tenant data migration.

Bug Identifier	Headline
CSCvq54357	After enabling multicast, access points stop broadcasting their SSID and WLANs enter the down state.

Table 16: Resolved Bugs in Cisco DNA Center, Release 1.3.0.2

Bug Identifier	Headline
CSCvp85607	After an upgrade, an AireOS wireless LAN controller with TrustSec/SXP experiences partial collection failure.
CSCvp85982	After an upgrade, reprovisioning fails for embedded wireless LAN controllers and AireOS wireless LAN controllers.
CSCvp86063	Cisco DNA Center does not prevent you from removing an extended node Cisco Catalyst IE3300 or IE3400 device from the fabric and then adding it back to the fabric as an edge. In other words, you can manually add IE3300 and IE3400 extended nodes that have been removed from the fabric.
CSCvp86074	Cannot add IPv6 to the fabric if external IP address managers (IPAMs) are used for IP pools.
CSCvp86132	During an upgrade from Cisco DNA Center 1.2.8 to 1.2.10, the **Cisco DNA Center 1.3 is Here!** banner appears. However, if you upgrade to 1.3 without first upgrading the system to 1.2.10, package upgrade issues occur.
CSCvp88055	A Cisco ISR 4400 border device returns an error when the fabric is enabled with a multicast rendezvous point on the other fabric border.
CSCvp88213	After an upgrade, an embedded wireless LAN controller access point does not broadcast the SSID.
CSCvp89082	Embedded wireless LAN controller provisioning fails with a Java null pointer exception. Related bug: CSCvp88853.
CSCvp89654	A software maintenance update on a Cisco Catalyst 9000 with Release 16.9.3 fails with an "NCSW10363" error.
CSCvp90174	After an upgrade, a Cisco IE5000 loses connectivity to Cisco DNA Center after the fabric is reconfigured.
CSCvp92365	After an upgrade, the RADIUS configuration is removed and added back during reprovisioning.
CSCvp92498	After an upgrade, Cisco DNA Center pushes incorrect PSN timeout values to switches.
CSCvp92735	Deleting an extended node port channel from the edge causes the edge to lose connectivity to Cisco DNA Center.
CSCvp94448	The Image Upgrade Readiness page shows the wrong golden image for the add-on package.
CSCvp96137	After an upgrade, the first reprovisioning of an embedded wireless LAN controller fails.
CSCvp97212	The fabric banner displays the oldest extended node error instead of the newest error.
CSCvp99456	After an upgrade, reconfiguring the fabric fails with "NCSP10000: Internal error."
CSCvq01546	Cisco DNA Center configures "map-cache ::/0 map-request" on border devices that are part of an IP transit, even though that configuration is not required.

Bug Identifier	Headline
CSCvq01667	When upgrading the application packages after a Cisco DNA Center 1.3 system upgrade, the package upgrade might fail with a "tenant migration failure" error. The root cause is a missing device record in the GRT table.
CSCvq11420	When upgrading the Cisco DNA Center cluster from 1.2.10 to 1.3, the sensor goes into Unclaimed state with "Error: [lua] handler.lua:303: ACCESS DENIED."

Table 17: Resolved Bugs in Cisco DNA Center, Release 1.3

Bug Identifier	Headline
CSCvh16564	For any NFVIS with version 3.7.x or earlier, there is no API to retrieve the system uptime.
CSCvn69306	After a system update, the jboss service does not run for the next hour. After 1 hour, the service recovers automatically.
CSCvn71409	Cisco 1800s running 8.8258.2 go into error state after an upgrade from Cisco DNA Center 1.2.6 to Cisco DNA Center 1.2.8.
CSCvo07310	Purge and aggregation jobs do not run.
CSCvo16429	When editing an existing test suite by changing its location, the existing sensor's configuration is removed without warning the user.
CSCvo16662	An internal error occurs when you choose **Add VNF** and add a device to the Inventory.
CSCvo20051	A system update fails if the hook-installer is not running.
CSCvo21174	In the **Provision** > **Devices** window, uptime (the period of time that a devices has been up and running) is not shown for NFVIS 3.10 and later devices.
CSCvo24817	The Assurance topology graph does not show when a link is down, but the automation topology graph is updated.
CSCvo30065	In the Inventory window, after you change the WAN IP address to the management IP address (and vice versa), interfaces are not listed in the NFVIS provisioning flow.
CSCvo30319	After removing a failed node and adding a new node to a multihost cluster, app stack services go into a crashloop state.
CSCvo30471	The Cisco Aironet 1800S Active Sensor doesn't pull software images immediately when inventoried, but only after a nightly synch.
CSCvo34972	Cisco DNA Center and CMX 10.6 integration doesn't sync the floor and building automatically.
CSCvo36052	Sensor: Test suites disappear after removing all sensors from inventory.
CSCvo38279	During sensor test suite creation, all SSIDs are not being shown for the selected floor.
CSCvo40364	It takes a few seconds to load the heat map and AP and client details.
CSCvo42491	A Catalyst 9000 image cannot be assigned to Catalyst 9400 devices.

Bug Identifier	Headline
CSCvo42517	When embedded wireless STP is turned on (the default is off), a path trace involving embedded wireless fails at the point between the embedded wireless controller and its connected switch. The path trace returns the error "Failed to obtain complete L2 path between routers."

CSCvo43286	When updating Cisco DNA Center from 1.2.8 to 1.2.10, the following error is reported for the system update:
	`System update failed during INSTALLED_CLUSTER_UPDATES.`
	`Cluster update timed-out. Retry.`
	To work around this problem, enter the **magctl service restart -d system-updater** command.

CSCvo44418	On a restored cluster, new Assurance issues might not be generated.
CSCvo49209	A system update fails around 88% with an error that the hook download failed. To work around this problem, retry the system update.
CSCvp30313	Cisco DNA Center 1.2.10 (PxGrid client hangs): Integration fails when HA failover happens from a different Cisco ISE.
CSCvp36943	Cisco ISE Policy Administration Node (PAN) HA failover is not auto detected by Cisco DNA Center.
CSCvp42465	The NTP service does not recover from a failure on its own.
CSCvp60090	A Cisco wireless LAN controller goes to unreachable and partial collection failure (SNMP timeout) frequently.

Limitations and Restrictions

Backup and Restore Limitations

Backup and restore limitations and restrictions include:

- You cannot take a backup of one version of Cisco DNA Center and restore it to another version of Cisco DNA Center. You can only restore a backup to an appliance that is running the same Cisco DNA Center software version, applications, and application versions as the appliance and applications from which the backup was taken.
- After performing a restore operation, update your integration of Cisco ISE with Cisco DNA Center. After a restore operation, Cisco ISE and Cisco DNA Center might not be in sync. To update your Cisco ISE integration with Cisco DNA Center, choose **System Settings** > **Settings** > **Authentication and Policy Servers**. Choose **Edit** for the server. Enter your Cisco ISE password to update.
- After performing a restore operation, the configuration of devices in the network might not be in sync with the restored database. In such a scenario, you should manually revert the CLI commands pushed for authentication, authorization, and accounting (AAA) and configuration on the network devices. Refer to the individual network device documentation for information about the CLI commands to enter.
- Re-enter the device credentials in the restored database. If you updated the site-level credentials before the database restore, and the backup that is being restored does not have the credential change information, all the devices go to partial-collection after restore. You must then manually update the device credentials

on the devices for synchronization with Cisco DNA Center, or perform a rediscovery of those devices to learn the device credentials.

- Perform AAA provisioning only after adjusting network device differential changes to the restored database. Otherwise, device lockouts might occur.
- You can back up and restore Automation data only or both Automation and Assurance data. But you cannot use the GUI or the CLI to back up or restore only Assurance data.

HA Limitation

In this release, Cisco DNA Center provides HA support only for Automation and Cisco SD-Access. HA for Assurance is not supported.

Cisco ISE Integration Limitations

Cisco ISE integration limitations and restrictions include:

- ECDSA keys are not supported as either SSH keys for Cisco ISE SSH access, or in certificates in Cisco DNA Center and Cisco ISE.
- Full certificate chains must be uploaded to Cisco DNA Center while replacing an existing certificate. If a Cisco DNA Center certificate is issued by a subCA of a rootCA, the certificate chain uploaded to Cisco DNA Center while replacing the Cisco DNA Center certificate must contain all three certificates.
- Self-signed certificates applied on Cisco DNA Center must have the Basic Constraints extension with cA:TRUE (RFC5280 section-4.2.19).
- The IP address or FQDN of both Cisco ISE and Cisco DNA Center must be present in either the **Subject Name** field or the **Subject Alt Name** field of the corresponding certificates.
- If a certificate is replaced or renewed in either Cisco ISE or Cisco DNA Center, trust must be re-established.
- The Cisco DNA Center and Cisco ISE IP or FQDN must be present in the proxy exceptions list if there is a web proxy between Cisco DNA Center and Cisco ISE.
- Cisco DNA Center and Cisco ISE nodes cannot be behind a NAT device.
- Cisco DNA Center and Cisco ISE cannot integrate if the ISE Admin and ISE pxGrid certificates are issued by different enterprise certificate authorities.

  Specifically, if the ISE Admin certificate is issued by *CA server A*, the ISE pxGrid certificate is issued by *CA server B*, and the pxGrid persona is running on a node other than ISE PPAN, the pxGrid session from Cisco DNA Center to Cisco ISE does not work.
- The Cisco ISE internal certificate authority must issue the pxGrid certificate for Cisco DNA Center.

Brownfield Feature-Related Limitations

Brownfield feature-related limitations include:

- Cisco DNA Center cannot learn device credentials.
- You must enter the preshared key (PSK) or shared secret for the AAA server as part of the import flow.
- Cisco DNA Center does not learn the details about DNS, WebAuth redirect URL, and syslog.

- Cisco DNA Center can learn only one wireless controller at a time.
- For site profile creation, only the AP groups with AP and SSID entries are considered.
- Automatic site assignment is not possible.
- SSIDs with an unsupported security type and radio policy are discarded.
- For authentication and accounting servers, if the RADIUS server is present in the device, it is given first preference. If the RADIUS server is not present, the TACACS server is considered for design.
- The Cisco ISE server (AAA) configuration is not learned through brownfield provisioning.
- The authentication and accounting servers must have the same IP addresses for them to be learned through brownfield provisioning.
- When an SSID is associated with different interfaces in different AP groups, during provisioning, the newly created AP group with the SSID is associated with the same interface.
- A wireless conflict is based only on the SSID name, and does not consider other attributes.

Wireless Policy Limitation

Wireless policy limitations include:

- If an AP is migrated after a policy is created, you must manually edit the policy and point the policy to an appropriate AP location before deploying the policy. Otherwise, `Policy Deployment failed` is displayed.

Cisco Plug and Play Limitations

Plug and Play limitations and restrictions include:

- Virtual Switching System (VSS) is not supported.
- The Cisco Plug and Play Mobile app is not supported with Plug and Play in Cisco DNA Center.
- The Stack License workflow task is supported for Cisco Catalyst 3650 and 3850 Series switches running Cisco IOS XE 16.7.1 and later.
- The Plug and Play agent on the switch is initiated on VLAN 1 by default. Most deployments recommend that VLAN 1 be disabled. If you do not want to use VLAN 1 when PnP starts, enter the following command on the upstream device:

  pnp startup-vlan *<vlan_number>*

AP Provisioning Failure Limitation

Configuring APs in FlexConnect mode before provisioning the locally switched WLANs bypasses the AP provisioning error. Otherwise, the AP provisioning fails when the locally switched WLANs are provisioned on the wireless controller or APs through Cisco DNA Center.

After the provisioning failure, the AP rejoins the wireless controller. You can reprovision the AP for a successful provisioning.

AP Performance Limitation

Provisioning of 100 APs takes longer in Cisco DNA Center, Release 1.3, than compared to 3 minutes in Cisco DNA Center, Release 1.2.10. The amount of time varies depending on the "wr mem" time of the Cisco Catalyst 9800 Series Controller, which includes Cisco Catalyst 9800-40 Wireless Controller, Cisco Catalyst 9800-80 Wireless Controller, and Cisco Catalyst 9800-CL Cloud Wireless Controller devices.

Inter-Release Controller Mobility (IRCM) Limitation

The interface or VLAN configuration is not differentiated between foreign and anchor controllers. The VLAN or interface that is provided in Cisco DNA Center is configured on both foreign and anchor controllers.

CMX Limitation

When integrating Cisco DNA Center with CMX 10.6.1, the site hierarchy that is created in Cisco DNA Center might not synchronize fully with CMX.

This problem occurs when CMX 10.6.1 is used and the site hierarchy in Cisco DNA Center contains one or more area elements that are children of other area elements; for example, Global > Area1 > Area1.1 > Building > Floor. CMX version 10.6.1 (and earlier) supports only hierarchies in the form of Global > Area > Building > Floor. CMX 10.6.1 does not support nested area elements.

The workaround is to rearrange the hierarchy in Cisco DNA Center so that there are no nested area elements. In other words, make sure the hierarchy is in the form of Global > Area > Building > Floor.

Intelligent Capture Limitations

Intelligent Capture limitations and restrictions include:

- Cisco DNA Center might not receive anomaly packets.

  Under the following conditions, an AP does not send anomaly packets to Cisco DNA Center; therefore, anomaly events don't have correlated captured packets in Cisco DNA Center:

  - An anomaly event throttle limit is reached inside an AP
  - An AP consumes high CPU
  - A client roams to a non-Intelligent Capture AP
  - A wireless controller sends **delete mobile** to an AP before an anomaly timer is triggered

- Enabling live or scheduled packet capture fails because the wireless controller exceeds the 16 MAC address limit for partial packet capture.

  Because the wireless controller can support a maximum of 16 MAC addresses for partial packet capture, if the list of MAC addresses on the wireless controller is not synchronized with Cisco DNA Center, enabling live or scheduled packet capture for a client fails with the following error messages:

  ```
  Failed to enable partial packet trace. NCSP10001: User intent validation failed.

  Failed to enable partial packet trace. config icap global subscription client packet-trace
  partial filter add [CLIENT MAC] Max filters configured:Failed to add new filter.

  Failed to enable client RF statistics. NCSP10001: User intent validation failed.

  Failed to enable filter channel. NCSP10001: User intent validation failed.
  ```

  Any of the following events can cause an out-of-synch condition:

- Partial packet capture is enabled directly on the wireless controller rather than on the Intelligent Capture UI
- Cisco DNA Center is reimaged or upgraded without first disabling all Intelligent Capture features
- The wireless controller is deleted and then rediscovered on Cisco DNA Center

- Enabling data packet capture fails because there is an existing MAC address in a full packet trace subscription on the wireless controller.

  Because the wireless controller supports only one MAC address for full packet capture, if there is an existing MAC address for full packet capture on the wireless controller, enabling data packet capture fails on that wireless controller. The following warning message is displayed:

  ```
  Max filter allowed for this topic is 1. Remove existing client filter before adding a new filter.
  ```

Get Assistance from the Cisco TAC

Use this link to open a TAC case. Choose the following when opening a TAC case:

- **Technology**: Cisco DNA - Software-Defined Access
- **Subtechnology**: Cisco DNA Center Appliance (SD-Access)
- **Problem Code**: Install, uninstall, or upgrade

Related Documentation

We recommend that you read the following documents relating to Cisco DNA Center:

For This Type of Information...	See This Document...
Release information, including new features, limitations, and open and resolved bugs.	Cisco DNA Center Release Notes
Installation and configuration of Cisco DNA Center, including postinstallation tasks.	Cisco DNA Center Installation Guide
Upgrade information for your current release of Cisco DNA Center.	Cisco DNA Center Upgrade Guide
Use of the Cisco DNA Center GUI and its applications.	Cisco DNA Center User Guide
Configuration of user accounts, security certificates, authentication and password policies, and backup and restore.	Cisco DNA Center Administrator Guide
Security features, hardening, and best practices to ensure a secure deployment.	Cisco DNA Center Security Best Practices Guide
Supported devices, such as routers, switches, wireless access points, NFVIS platforms, and software releases.	Supported Devices
Hardware and software support for Cisco SD-Access.	Cisco SD-Access Hardware and Software Compatibility Matrix

For This Type of Information...	See This Document...
Use of the Cisco DNA Assurance GUI.	Cisco DNA Assurance User Guide
Use of the Cisco DNA Center platform GUI and its applications.	Cisco DNA Center Platform User Guide
Cisco DNA Center platform release information, including new features, deployment, and bugs.	Cisco DNA Center Platform Release Notes
Use of the Cisco Wide Area Bonjour Application GUI.	Cisco Wide Area Bonjour Application User Guide
Use of the Stealthwatch Security Analytics Service on Cisco DNA Center.	Cisco Stealthwatch Analytics Service User Guide
Use of Rogue Management functionality as a dashboard within Cisco DNA Assurance in the Cisco DNA Center GUI.	Cisco DNA Center Rogue Management Application Quick Start Guide

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 of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone 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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2019–2020 Cisco Systems, Inc. All rights reserved.