Release Notes for Cisco DNA Center, Release 2.2.1.x

First Published: 2021-02-08

Last Modified: 2021-03-26

Release Notes for Cisco DNA Center, Release 2.2.1.x

Cisco DNA Center 2.2.1.x is a Commercial Availability release. Contact your Cisco sales representative to request this release.

This document describes the features, limitations, and bugs for Cisco DNA Center, Release 2.2.1.x.

For links to all of the guides in this release, see Cisco DNA Center 2.2.1 Documentation.

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Change History

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

Table 1: Document Change History

Date	Change	Location
2021-03-26	Added the list of packages in Cisco DNA Center 2.2.1.3.	New and Changed Information, on page 2
	Noted the increased scale support in Cisco DNA Center 2.2.1.3.	New and Changed Information, on page 2
	Added the Resolved Bugs table for 2.2.1.3.	Resolved Bugs, on page 20
	Added open bugs CSCvx45032, CSCvx82825.	Open Bugs, on page 18
2021-02-08	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 in Cisco DNA Center, Release 2.2.1.x.

Table 2: Updated Packages and Versions in Cisco DNA Center Release 2.2.1.x

Package Name	Release 2.2.1.3	Release 2.2.1.0
System Updates		
System	1.6.333	1.6.301
System Commons	2.1.313.62510	2.1.310.61024
Package Updates		
Access Control Application	2.1.313.62510	2.1.310.61014
AI Endpoint Analytics	1.3.331	1.3.239
AI Network Analytics	2.5.13.364	2.5.13.364
Application Hosting	1.5.1.2103220632	1.5.1.2101040747
Application Policy	2.1.313.170005	2.1.310.117202
Application Registry	2.1.313.170005	2.1.310.117202
Application Visibility	2.1.313.170005	2.1.310.117202
Assurance - Base	2.2.1.329	2.2.1.243
Assurance - Sensor	2.2.1.326	2.2.1.234
Automation - Base	2.1.313.62510	2.1.310.61014
Automation - Intelligent Capture	2.1.313.62510	2.1.310.61014
Automation - Sensor	2.1.313.62510	2.1.310.61014
Cisco DNA Center Global Search	1.4.0.15	1.4.0.11
Cisco DNA Center Platform	1.4.99.133	1.4.99.106
Cisco DNA Center UI	1.6.1.364	1.6.1.339
Cisco SD-Access	2.1.313.62510	2.1.310.61014
Cisco Umbrella	2.1.313.592337	2.1.310.590293
Cloud Connectivity - Data Hub	1.6.0.263	1.6.0.263

Package Name	Release 2.2.1.3	Release 2.2.1.0
Cloud Connectivity - Tethering	2.1.1.40	2.1.1.37
Cloud Device Provisioning Application	2.1.313.62510	2.1.310.61014
Command Runner	2.1.313.62510	2.1.310.61014
Device Onboarding	2.1.313.62510	2.1.310.61014
Disaster Recovery	2.1.313.360059	2.1.310.360409
Group-Based Policy Analytics	2.1.1.500	2.1.1.208
Image Management	2.1.313.62510	2.1.310.61014
Machine Reasoning	2.1.313.21432	2.1.310.210298
NCP - Base	2.1.313.62510	2.1.310.61014
NCP - Services	2.1.313.62510	2.1.310.61014
Network Controller Platform	2.1.313.62510	2.1.310.61014
Network Data Platform - Base Analytics	1.6.549	1.6.175
Network Data Platform - Core	1.6.571	1.6.259
Network Data Platform - Manager	1.6.537	1.6.129
Network Experience Platform - Core	2.1.313.62510	—
Path Trace	2.1.313.62510	2.1.310.61014
RBAC Extensions	2.1.313.1902010	2.1.310.1900012
Rogue and aWIPS	2.1.0.33	2.1.0.33
Stealthwatch Security Analytics	2.1.313.1090210	2.1.310.1090254
Wide Area Bonjour	2.4.311.75035	2.4.311.75035

New and Changed Features

The following table summarizes the new feature in Release 2.2.1.3.

Table 3: New Feature in Cisco DNA Center 2.2.1.3

Feature	Description
Increased scale support	Compared to earlier releases, Cisco DNA Center 2.2.1.3 supports two times the scale for wireless and wired endpoints, clients, and interfaces. For Cisco DNA Center scale numbers, see the *Cisco DNA Center Data Sheet*.

The following tables summarize the new and changed features in Release 2.2.1.0.

Table 4: New and Changed Features in Cisco DNA Center 2.2.1.0

Feature	Description
NIC bonding (LACP)	On any given Cisco DNA Center second-generation appliance, you can configure the Enterprise, Intracluster, Management, and Internet interface. Cisco DNA Center 2.2.1 supports network interface controller (NIC) bonding on a single-node cluster. As a result, each of these interfaces has two instances: The primary instance (located on either your appliance's motherboard or Intel X710-DA2 NIC) is connected to one switch, and the secondary instance (located on your appliance's Intel X710-DA4 NIC) is connected to a different switch. NIC bonding consolidates the two instances of each interface into a single logical interface, appearing as a single device with one MAC address. For details, see the Cisco DNA Center Second-Generation Appliance Installation Guide, Release 2.2.1.
Quick installation workflow	After you have installed and configured the Cisco DNA Center appliance, you can log in to its GUI. When you log in for the first time as the admin superuser (with the username *admin* and the SUPER-ADMIN-ROLE assigned), the Quick Start workflow automatically starts. Complete this new workflow to discover the devices that Cisco DNA Center will manage and enable the collection of telemetry from those devices.
Plug and Play	A new option during the Claim process lets you apply a device ID certificate to routers. You can also apply an image upgrade to Cisco Catalyst 9800 Series Wireless Controller devices during the Claim process. Plug and Play supports IPv6 addresses for switches and routers.
Cisco DNA Spaces integration	With the Cisco DNA Spaces integration, you can get the exact location of your wireless clients, rogue access points, and interferers on the floor map within the Cisco DNA Center GUI. Cisco DNA Center 2.2.1 supports the integration of Cisco DNA Spaces without the Cisco DNA Spaces Enabler package. The Cisco DNA Spaces Enabler package was introduced in Cisco DNA Center 2.1.2.4 to enable the Cisco DNA Spaces integration. If you are upgrading to 2.2.1 from an earlier release, you must uninstall the Cisco DNA Spaces Enabler package before upgrading. Otherwise, backup and restore operations will fail in 2.2.1.
View Audit Logs	Cisco DNA Center now allows you to add multiple syslog servers to receive audit logs and events from external services. Multiple syslog servers enable you to select multiple destinations for audit log export to syslog servers in case the primary syslog server data is corrupted. With this release, the Cisco DNA Center audit log feature also allows you to filter multiple audit logs by description.
ISSU compatibility matrix	Cisco DNA Center supports importing the ISSU compatibility matrix. Upgrading software images with ISSU eliminates the need to reboot and reduces the interruption of service.

Feature	Description
Change license level support for Cisco AireOS controllers	You can change the license level of the following Cisco AireOS controllers: • Cisco 3500 Series Wireless LAN Controller • Cisco 5500 Series Wireless LAN Controller • Cisco 8500 Series Wireless LAN Controller
Report license usage support for traditional devices such as Cisco Catalyst 2000, Cisco Catalyst 4000, and Cisco Catalyst 6000 devices	The Cisco DNA Center license manager checks the customer smart account and virtual account for the entitlement tags and reports the count-based usage in the **All Licenses** page.
Install Auth Code and enable HSEC license	You can install Auth Code and enable an HSEC license in a single workflow or in separate workflows as required.
Upload resource utilization details to CSSM	You can upload the resource utilization details to CSSM instantly or schedule the uploading event.
Change device throughput	You can change the throughput of smart license-enabled routers.
Transfer licenses between virtual accounts	You can transfer licenses between virtual accounts.
Reporting APs in License Manager Inventory	While exporting the data from **All Licenses** page, the number of access points connected to a wireless controller can be exported by checking the **Total APs** check box under **Select Columns to Export** in the **Export Licenses** window.
Manage customer tags to smart license-enabled devices	You can add a maximum of four customer tags to a smart license-enabled device to help identify telemetry data for a product instance. You can also update and delete the customer tags.
Support for Catalyst 9105AX Series Access Points and brownfield configuration	• Cisco DNA Center support is extended for Cisco Catalyst 9105AX series access points as embedded wireless controllers for nonfabric deployment. • Cisco DNA Center now learns and saves the brownfield configuration of embedded wireless controllers.
Support for Rogue and aWIPS	The Cisco DNA Center rogue discovery, rogue classification type, and aWIPS are now supported on Cisco Catalyst 9000 series access points, Cisco Catalyst 9800 Series Wireless Controller, and AireOS devices in IPv6 networks.
aWIPS profile	Cisco DNA Center is now supported with an aWIPS profile that enables you to configure denial of service (DoS) attacks. The **aWIPS Profile** feature is supported with **Forensic Capture** that enables you to download packets and alarms at the time of DoS attacks.

Feature	Description
Wireless maps	Cisco DNA Center now retains the preconfigured access point information in case the wireless controller is deleted from the inventory. Cisco DNA Center supports planned heatmaps that show the possible coverage of planned access points on a floor map. Cisco DNA Center supports IDS heatmaps that show the monitor mode access point coverage provided to wireless clients on a floor map. Cisco DNA Center supports GPS markers that enable you to find the actual position of the building space on the world map, providing greater accuracy of the client position. The GPS marker is exported to Cisco Connected Mobile Experiences (CMX) and Cisco DNA Spaces. Cisco DNA Center allows you to export the working floors from Cisco DNA Center as an Ekahau project and import into Ekahau Pro Tool to augment the preconfigured working floors.
Support for Discovery, Inventory, and Device controllability	• Cisco DNA Center is now supported with IPv6 for the Discovery, Inventory, and Device controllability on Cisco Catalyst 9800 Wireless Controller in nonfabric mode. • Cisco DNA Center installed in IPv6 mode does not support the workflows configured with IPv4 mode.
Inventory	With this release, when you discover a device with a Redundancy Management Interface (RMI) IP address, the inventory throws an error stating that the device is discovered with an RMI IP address and is not supported by Cisco DNA Center. Cisco DNA Center lets you disable a brownfield device that is configured for high availability. When you configure Cisco wireless controller **High Availability** from Cisco DNA Center and select the secondary controller, based on the wireless management interface IP subnet of the primary controller, redundancy management IP auto populates.
IPv6 support for application hosting and wireless automation	Application hosting, device provisioning, design, and onboarding functions are now supported with IPv6, which enables you to upgrade multiple sites at once for Cisco Catalyst 9100 Series Access Points and Cisco Catalyst 9300 devices.
Configure AAA servers	Cisco DNA Center lets you add and configure AAA servers for enterprise and guest wireless networks. Cisco DNA Center lets you override the set of AAA server configurations for SSID on the site level. You can configure a maximum of six AAA servers for an SSID of enterprise and guest wireless networks. The configure AAA feature is supported on Cisco Catalyst 9800 Series Wireless Controller and AireOS wireless controller.
Idle session timeout	If you leave the session idle, a **Session Timeout dialog box** appears 5 minutes before the session timeout. Click **Stay signed in** if you want to continue the session. You can click **Sign out** to end the session immediately.
Filter client data	In wireless maps, while filtering client data, Cisco DNA Center now shows a dotted line on the search result that indicates the association of the access point to which the client is associated on the map.

Feature	Description
IPv6 support for troubleshooting workflows	Cisco DNA Center provides support for the following troubleshooting workflows: • Ping • CPU Utilization • Power supply failure • Fabric data collection • Interface down
Model Config Design Enhancements	Model Config Design supports new **Dot11ax Configurations**. You can configure Dot11ax configuration parameters only on Wi-Fi 6 supported Cisco Catalyst 9100 series Access Points. The Dot11ax configuration supports following parameters: • BSS Color • Target Wakeup Time The Advanced SSID Model Config Design supports **802.11ax Configuration**. The following 802.11ax BSS Configuration parameters are supported: • BSS Target Wake Up Time • Downlink OFDMA • Uplink OFDMA • Downlink MU-MIMO • Uplink MU-MIMO
Configure Integration Settings	After a backup and restore of Cisco DNA Center, you need to access the Integration Settings page and update (if necessary) the **Callback URL Host Name** or **IP Address**.

Table 5: New and Changed Features in Cisco DNA Assurance

Feature	Description
Radio outage issue	A radio outage issue is triggered when certain conditions are met.
IPv6 support	Cisco DNA Center supports IPv6 addresses in canonical format only. Cisco AI Endpoint Analytics does not support IPv6 addresses.
Troubleshoot issues with MRE workflow	You can use the MRE workflow to troubleshoot wired client issues and PoE issues.

Feature	Description
IPv6 support for troubleshooting issues using MRE	Cisco DNA Center provides support for the following troubleshooting issues with MRE: • Layer 2 loop • High CPU • Power supply failure • Fabric DHCP on edge • Interface down • PoE IMAX fault • AAA authentication
FQDN support for Cisco Catalyst 9800 controllers	With this release, Cisco DNA Center supports FQDN on Cisco IOS XE 17.4 or later for Cisco Catalyst 9800 Series Wireless Controllers, ECA, and embedded wireless controllers.
Network heatmap enhancements	The following enhancements are added to the Network Heatmap: • **Search AP**: You can search and select an AP. • **Daily View**: You can determine how all the APs behave every hour in a selected day.
Compare buildings, AP models, and endpoint types	You can view and compare network performance across selected Key Performance Indicators (KPIs) by buildings, AP model families, and wireless endpoint types.
Peer comparison by network size	The peer networks that are used for comparison have a similar AP count.
Baseline tabs	The **Baseline** tabs in the **Client** health dashboard will be deprecated in the near future. These tabs are located in the **Client Onboarding Times** and **Client Count Per SSID** dashlets. For AI Network Analytics features, you must enable AI Network Analytics. See the *Configure Cisco AI Network Analytics Data Collection* and *Cisco AI Network Analytics Overview* topics in the Cisco DNA Assurance User Guide, Release 2.2.1.
Enhanced telemetry support for the Cisco Catalyst 9800 Series Wireless Controller	For the Cisco Catalyst 9800 Series Wireless Controller: If the SSIDs are mixed, that is Local mode, Flex mode, and Fabric mode, the Cisco Application Visibility and Control (AVC) basic record is configured. If all the SSIDs are in Local mode, the Optimized APM record is configured.
Issues enhancements	The following new WAN interface issues are supported: • WAN Interface Discard • WAN Interface Utilization • WAN Interface Down
Ethernet interface KPI support for APs	APs support Ethernet interface KPIs in Device 360 and network for connectivity. Ethernet interface KPIs include Utilization, Error, and Rate.

Feature	Description
Enhancements to AP issues	The AP Down issue is renamed to AP Disconnect from WLC. **AP Flap**: You can configure the new aggregation count. If the aggregation count is more than two within a time period of 15 minutes, a new AP flap issue notification is triggered.
Support for hex password in preshared key (PSK) format	For wireless sensors, support is added for the hex password in PSK format in backhaul settings.

Table 6: New and Changed Software Features in Cisco Software-Defined Access

Feature	Description
Support for VLAN ID customization	You can now assign a desired VLAN ID to a host pool VLAN and Layer 3 handoff VLAN. The VLAN IDs can be in the range of 1 to 4095. This feature provides more flexibility in segment creation for the brownfield SD-Access deployments. Delete any existing overlapping or conflicting VLANs or SVIs or AAA configurations from the device and resynchronize the device in the inventory prior to adding it to the SD-Access fabric. When you upgrade from an earlier release, the existing VLANs continue to work normally. Post upgrade, you will need to provide an external VLAN ID for new Layer 3 handoffs. Layer 2 Handoff VLAN is auto populated based on the VLAN ID assigned to the host pool. You can edit the Layer 2 Handoff VLAN ID to assign a different VLAN number. To change the VLAN ID for an existing IP pool VLAN, delete the IP pool and create the IP pool again with the desired VLAN ID. Consider the following guidelines before assigning a custom VLAN ID: • If you do not provide a custom VLAN ID, Cisco DNA Center generates a VLAN ID in the range of 1021 to 2020. • VLAN IDs 1, 1002-1005, 2046, 4095 are reserved and cannot be used. • Critical voice or pre-auth VLAN is assigned a VLAN ID of 2046 and cannot be changed. • Borders in the same Site or in different Sites can share the same Layer 3 handoff VLAN IDs.

Feature	Description
Support for Linear Daisy Chain topology on the Extended Nodes and Policy Extended Nodes	

Feature	Description

	You can expand the network connectivity, security policy, automation policy, assurance and management to the IoT endpoints by extending the SD-Access fabric with extended nodes. This release of Cisco DNA Center enhances the capability of extended nodes to cascade connectivity of multiple extended node devices or policy extended node devices in a linear daisy chain.
	
	The following devices can be cascaded in a linear daisy chain:
	
	• Extended Node Devices:
	  • Cisco Industrial Ethernet 4000, 4010, 5000 series switches that operate Cisco IOS 15.2(7)E3 or later releases.
	  • Cisco Catalyst IE3300 series switches that operate Cisco IOS XE 17.3.2a and later releases.
	• Policy Extended Node Devices: Cisco Catalyst IE3400, IE3400H series switches that operate Cisco IOS XE 17.3.2a and later releases.
	
	An extended node or policy extended node device that is added to the linear daisy chain is auto configured only if the device has the **No Authentication** template enabled.
	
	If you enable any other template, create a port channel manually, using the Cisco DNA Center GUI of the extended node or the policy extended node to which the new node is connected for onboarding.
	
	After a device is onboarded in the linear daisy chain, you can perform the following actions:
	
	• Add hosts like IP phones, laptops to the fabric.
	• Create port channels on the extended or policy extended node.
	• All existing operations supported on the extended nodes can be performed on the daisy chained nodes.
	
	Limitations of daisy chained extended nodes
	
	• A maximum of 18 devices can be onboarded in a single linear daisy chain topology. More than 18 extended nodes or policy extended nodes can be deployed under a Fabric Edge device.
	• Cascading multiple extended nodes or policy extended nodes in a ring topology is not supported.
	• Cascading a mix of extended node devices and policy extended node devices is not supported. A given linear daisy chain topology can have all devices either as extended nodes or as policy extended nodes.
	• Linear Daisy Chain topology on the extended and policy extended nodes is supported only for green field deployments. Migration from a previous release does not bring in this feature to an already onboarded extended node.
	• For a seamless software image upgrade, perform the upgrade in the order of bottom to top in the daisy chain.
	• Insertion or Deletion of a new node in between the daisy chain is not supported. You

Feature	Description
	can insert or delete a node only at the end of the daisy chain.
Support for MACsec encryption using templates	MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. Cisco DNA Center Release 2.2.1 allows you to enable switch-to-host and switch-to-switch MACsec encryption using templates. You can also configure MACsec manually on the device using the device CLI. A Catalyst 9000 Series device that runs MACsec-compatible Cisco IOS XE image supports this functionality. Refer to the device configuration guides for details on MACsec configuration and guidelines. Consider the following design aspects: • For switch-to-switch MACsec support ensure that the switch is dual-homed to avoid stranding the device. • For a classic or policy extended node, ensure that there are multiple links between the fabric edge and the extended nodes that are bundled as part of the port-channel. • For a classic or policy extended node, ensure that the template is first pushed to the extended node and then to the fabric edge.
Increase in the number of virtual networks per fabric site	Starting with Cisco DNA Center Release 2.2.1, a fabric site supports a maximum of 128 virtual networks on a 56-Core Gen 2 Cisco DNA Center appliance. For more information, see the Cisco DNA Center Data Sheet.
Increase in the number of IP pools supported per fabric site	This release supports a higher number of IP pools (includes subpools and subnets created from superpool) that can be created per fabric site. For details on the IP pool scale, see the Cisco DNA Center Data Sheet.
Configure AAA servers	Cisco DNA Center lets you add and configure AAA servers for enterprise and guest wireless networks. Cisco DNA Center lets you override the set of AAA server configurations for SSID on the site level. You can configure a maximum of six AAA servers for an SSID of enterprise and guest wireless networks. The configure AAA feature is supported on Cisco Catalyst 9800 Series Wireless Controller and AireOS wireless controller.
Note Cisco SD-Access does not support IPv6 underlay addressing.	

Table 7: New Hardware in Cisco Software-Defined Access

Device Role	Product Family	Part Number	Description
Extended Node	Cisco Catalyst Micro Series Switches	CMICR-4PT CMICR-4PC CMICR-4PS	Cisco Catalyst Micro Series switches are designed for deployments of fiber to the desk, office, and so on (FTTx). They support four 1-Gigabit Ethernet ports and two Gigabit Ethernet copper or fiber uplinks, with line-rate forwarding. CMICR-4PT is built for desktop deployments. CMICR-4PC and CMICR-4PS are built for wall-jack deployments.
Extended Node	Cisco Catalyst IE3300 Rugged Series Switch	IE-3300-8U2X	An expandable Industrial Ethernet Switch that supports 8 GE (4PPoE) ports and two 10-G SFP modules.

Deprecated Features

SNMPv3 Data Encryption Standard (DES) Privacy Mode support is undergoing a phased deprecation in Cisco DNA Center. The feature will not be supported in later Cisco DNA Center releases.

SNMPv3 DES is used to ensure data confidentiality, where the designated portion of an SNMP message is encrypted and included as part of the message sent to the recipient. DES is no longer considered secure due to its too-short key length and its proven ineffectiveness against brute force attacks. Advanced Encryption Standard (AES) is the recommended privacy mode.

Cisco SD-Access Compatibility Matrix

For information about Cisco SD-Access hardware and software support for Cisco DNA Center, see the Cisco Software-Defined Access 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 GUI 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.

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 Hardware Appliances

Cisco supplies Cisco DNA Center in the form of a rack-mountable, physical appliance. The following versions of the Cisco DNA Center appliance are available:

- First generation
  - 44-core appliance: DN1-HW-APL
- Second generation
  - 44-core appliance: DN2-HW-APL
  - 44-core promotional appliance: DN2-HW-APL-U
  - 56-core appliance: DN2-HW-APL-L
  - 56-core promotional appliance: DN2-HW-APL-L-U
  - 112-core appliance: DN2-HW-APL-XL
  - 112-core promotional appliance: DN2-HW-APL-XL-U

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 4.1(1h) for appliance model DN2-HW-APL
- Cisco IMC Version 4.1(1h) for appliance model DN2-HW-APL-L
- Cisco IMC Version 4.1(1h) 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 all later versions.

Installing Cisco DNA Center

You 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 for information about installation and deployment procedures.

Note Certain applications, like Group-Based Policy Analytics, are optional applications that are not installed on Cisco DNA Center by default. If you need any of the optional applications, you must manually download and install the packages separately.

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) 10.6.2. 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

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

Table 8: Open Bugs

Bug Identifier	Headline
CSCvt38921	Cisco DNA Center Audit log requirements: Create backup now needs a finish time and create schedule backup needs an audit log entry.

Bug Identifier	Headline
CSCvu75254	When an RMA attempt fails, the old faulty AP remains. This problem occurs under the following conditions: **1.** Mark the old AP (AP1) for replacement. A new AP (AP2) is available in the PnP page. **2.** Bring down the AP PnP by shutting down its switchport. **3.** Process the RMA for AP1 with AP2. **4.** The AP RMA fails and the Retry option appears. **5.** Bring up the AP2 via PnP. The AP RMA process begins automatically and configs are pushed based on the site assignment. The AP2 joins the eWLC; however, the old AP (AP1) remains available in the inventory. To work around this problem, click the RMA **Retry** option (under the Marked for Replacement page) to remove the old AP from the inventory.
CSCvv25434	A full synch from IOS for unmodelled commands fails due to an IP SLA CLI error.
CSCvv40358	NIC bonding (LACP) is not supported on the Cisco DNA Center first-generation, 44-core appliance (DN1-HW-APL), because the appliance does not have an extra NIC. If you do a fresh install of Cisco DNA Center 2.2.1 on a DN1-HW-APL appliance, or if you upgrade from Cisco DNA Center 2.1.x to 2.2.1 on a DN1-HW-APL appliance, you see an option to configure LACP, which is not supported.
CSCvv86095	Command Runner is present as a separate service after upgrading from Cisco DNA Center 1.3.3.0 to 2.0.x or later. Because Command Runner is integrated with the network poller service from Cisco DNA Center 2.0.x, the expected behavior after upgrade is that the Command Runner service should cease to exist and all Command Runner calls should be forwarded to the network poller service. Because Command Runner is present as a separate service after upgrading from Cisco DNA Center 1.3.3.0, commands are not executed as expected.
CSCvw03899	An error message appears on the GUI when the proxy server URL is not valid during first-time setup.
CSCvw33820	While assigning devices to sites, the DNS configuration is pushed as part of the Device Controllability workflow.
CSCvw55539	Zero touch deployment fails for IE 3400 and IE 3400H devices.
CSCvw59022	Path trace fails for IPv6 devices if the network involves a device from the NX-OS family.

CSCvw76747	The Disaster Recovery rejoin GUI action fails for the standby cluster during the replication stage with the following error:
	`Failed to configure standby system.`
	`Reason: [{'name': 'Configure managed services replication', 'status':`
	`['Maglev configure replication task failed.`
	`Reason: waiting for replication timed out\n']}]`

CSCvw79310	Customers using Cisco DNA Center 2.1.2.x releases cannot provision APs to a newly created floor in a parent site that is already managed by a wireless controller, without first provisioning the wireless controller again.
CSCvw83060	Enabling multicast on a fabric site fails with a timeout at the conversion phase.

Bug Identifier	Headline
CSCvw91472	Cisco DNA Center discovery with NETCONF of a Catalyst 9500-24Y4C with StackWise Virtual Links may cause an unexpected failover, and failure to import the sdn-network-infra-iwan certificate.
CSCvw92748	Cisco ISE integration fails when the Cisco ISE Primary Policy Administration Node (primary PAN) certificate contains an unreachable CDP.
CSCvx45017	When there is a network delay that exceeds 1 second, the Assurance Application Health page shows reduced values.
CSCvx45032	Due to a known flink issue, pipelines are not running in the cluster. No data appears in the **Assurance** UI.
CSCvx82825	During a package upgrade, the GUI displays a blank screen or the message "Updating catalog..." for a long time.

Resolved Bugs

The following table lists the resolved bugs in Cisco DNA Center, Release 2.2.1.3.

Table 9: Resolved Bugs in Cisco DNA Center, Release 2.2.1.3

Bug Identifier	Headline
CSCvt27360	Cisco DNA Center to Cisco ISE integration fails. While decrypting bad credentials are returned by credmanager service.
CSCvv02490	The Netflow collector is dropping the packets for some devices.
CSCvv74034	Cisco DNA Center upgrade to 2.1.2.x: MongoDB pod in the crash loop fails during the container creation stage.
CSCvv91822	IPDT configuration is rejected on Bluetooth interface during provision.
CSCvw20926	After system upgrade to Cisco DNA Center 2.1.2.3, download of application upgrades fail.
CSCvw31619	Elasticsearch cluster formation failure in Cisco DNA Center second-generation appliance cluster with 12 instances.
CSCvw37064	ACL_WEBAUTH_REDIRECT is not configured correctly.
CSCvw37462	AP map page loading is very slow after upgrading to Cisco DNA Center 2.1.2.3.
CSCvw47447	Custom provisioned RF profile is allowed to be deleted.
CSCvw49445	Wireless controller provisioning is blocked when RF profile is deleted from Design and not cleaned from database.
CSCvw49759	When executed manually from **Tools** > **Network Reasoner** > **CPU Utilization** workflow, an internal server error occurs during the Machine Reasoning Engine's analysis, and the cnsr-reasoner service restarts itself.
CSCvw53139	Task page doesn't load any data.

Bug Identifier	Headline
CSCvw59092	Cisco DNA Center Pkcs12 configuration failed due to internal Errors after discovering Cisco Catalyst 9800 Series Wireless Controller in cluster.
CSCvw62170	Mismatch in unassigned device count and what is seen in inventory after removal of the GPS Marker.
CSCvw62379	Cisco DNA Center to Service Now integration fails with a rate limit exceeded error.
CSCvw67029	Application upgrade failed due to RabbitMQ maximum message size.
CSCvw67480	After upgrading Cisco DNA Center, a managed wireless LAN controller may find that Flex profiles are duplicated on the device.
CSCvw72645	Cisco DNA Center 2.1.2.4: RBAC denies network hierarchy maps to load with "Error 11015".
CSCvw73184	After upgrading to Cisco DNA Center 2.1.2.3, externally authenticated users may be able to log in, but still don't have authorization to perform some functions.
CSCvw74679	Cisco SD-Access: When Cisco ISE becomes unreachable, endpoints are put into an authorized, but not authenticated state.
CSCvw76030	Cisco DNA Center 1.3.3.7: Unable to perform RMA due to field value exceeding the integer range.
CSCvw76745	The attempts to provision a Cisco Catalyst 9800 Series Wireless Controller may fail with a null pointer exception in Cisco DNA Center's network-programmer log. The wireless controller has a guest SSID with Cisco ISE authentication and a self-signed portal enabled.
CSCvx02345	Cisco DNA Center is unable to start a new LAN automation session, citing the error "NCND00006". The input payload contains an invalid key.
CSCvx02368	Cisco DNA Center may become unable to start a new LAN Automation session, citing the error, "Failed to start Network Orchestration Session: null," following a LAN automated Fabric-In-A-Box device being deleted from the system, then added again via discovery and inventory.
CSCvx08471	Restore to Cisco DNA Center 2.1.2.5 fails with error "Sentimentalized".
CSCvx09990	Cisco DNA Center pushes additional flex profiles with incorrect VLAN-name and VLAN-ID mapping.
CSCvx10390	Application upgrade failed due to contraint violation on lispcomponent table.
CSCvx12639	A managed device's inventory status in Cisco DNA Center may change to "Internal Error" when a value returned by the device that should be an IP address is null.
CSCvx12949	Support for port-channel and tunnel interfaces for tagging-based Application telemetry.
CSCvx14538	Router provisioning fails with an error "NCSP10250: Error During persistence (provision) of CFS".
CSCvx16385	Cisco DNA Center may fail to restore a backup for the Postgres service after 7200 seconds of inactivity.
CSCvx21853	Cisco DNA Center 's discovery fails to retrieve global credentials while trying to create new task.
CSCvx27169	Cisco DNA Center's inventory service may crash if the managed devices send lots of syslogs.
CSCvx34202	Assurance pod running into performance issues due to excessive logging by wireless rogue pipeline.

Bug Identifier	Headline
CSCvx41602	When Cisco DNA Center's Licensing tool tries to configure SLR reservation for stacked switches, it may get stuck at Generating Authorization code.

The following table lists the resolved bugs in Cisco DNA Center, Release 2.2.1.0.

Table 10: Resolved Bugs in Cisco DNA Center, Release 2.2.1.0

Bug Identifier	Headline
CSCvt16845	Cisco DNA Center IDM is missing some certificate validations.
CSCvt50035	The Endpoint Inventory page takes around 40 seconds to load on a Cisco DNA Center 112-core appliance when there are 75,000 or more endpoints in the system.
CSCvu39101	Cisco DNA Center fabric provision operation takes more time when multiple sites connected to transit.
CSCvu48418	The provisioning status is shown as "Pending" even when the last provision succeeded.
CSCvu96315	Cisco DNA Center's Cloud AI registration fails due to proxy authentication.
CSCvv08806	Cisco DNA Center: Extended nodes must be configured on distinct edge ports.
CSCvv22070	Cisco DNA Center 1.3.3.5: After restoring a backup, provisioning may not work if Inventory Sync is disabled.
CSCvv42973	Application Health page usage bytes does not reflect app usage on all devices.
CSCvv62098	Cisco DNA Center appliance fails to boot as maglev-system partition fails to mount by UUID.
CSCvv86302	Cisco AireOS controllers may be reported as "unmonitored", and wireless device and wireless client Assurance data may not be shown in Cisco DNA Center's UI when the wireless controllers fail to register and receive 403 error.
CSCvv95329	Cisco DNA Center's root CA certificate may expire, and will not be refreshed automatically.
CSCvw11717	Cisco DNA Center 2.1.2.0: Upgrading protocol pack for application visibility fails.
CSCvw14715	Cisco DNA Center didn't push default-site-tag-fabric configuration to Cisco Catalyst 9800 Series Wireless Controller after upgrade.
CSCvw16983	Adding Cisco Catalyst 9800 Series Wireless Controller to fabric fails if the fabric contains L3 only IP address pool segments.
CSCvw20183	Package upgrade failed due to missing deployment artifact in rogue-management.
CSCvw23564	Cert refresh script fails after etcd cert expires.
CSCvw26250	Cisco DNA Center's documentation mentions that the ENCS is supported; however, Assurance doesn't mention a Device 360 page for it.
CSCvw49759	The Cnsr-reasoner service restarts every time when executed manually from Cisco DNA Center's **Tools** > **Network Reasoner** > **CPU Utilization** and there is no issue report .

Bug Identifier	Headline
CSCvw58651	Cisco DNA Center 2.1.2.3 Policy: QoS not pushing outbound configurations.
CSCvw67029	Application upgrade failed due to RabbitMQ maximum message size.
CSCvw73184	After fixing authorization failure, AAA users are able to login but can't perform certain operations.

Limitations and Restrictions

Upgrade Limitation

If you are upgrading to Cisco DNA Center and all of the following conditions apply, the upgrade never starts:

- Cisco ISE is already configured in Cisco DNA Center.
- The version of Cisco ISE is not the required 2.6 patch 1 or 2.4 patch 7 or later.
- Cisco DNA Center contains an existing fabric site.
- The number of DNS servers must not exceed three.

Although the UI does not indicate that the upgrade failed to start, the logs contain messages related to the upgrade failure.

To work around this problem, upgrade Cisco ISE to 2.6 patch 1 or 2.4 patch 7 or later, and retry the Cisco DNA Center upgrade.

Backup and Restore Limitations

- 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.

Cisco ISE Integration Limitations

- 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.

License Limitation

The Cisco DNA Center License Manager supports Smart Licensing only for wireless LAN controller models that run Cisco IOS XE. License Manager does not support wireless LAN controller models that run Cisco AireOS.

Fabric Limitations

- Cisco DNA Center supports up to a maximum of 1.2 million interfaces on fabric devices. Fabric interfaces include physical and virtual interfaces like switched virtual interfaces, loopback interfaces, and so on.

  Physical ports cannot exceed 480,000 ports on a 112-core appliance.
- IP address pools reserved at the area level are shown as inherited at the building level on the **Design** > **Network Settings** > **IP Address Pools** window; however, these IP address pools are not listed on the **Host Onboarding** window if the fabric site is defined at the building level. If the fabric site is defined at the building level, you must reserve the IP address pools at the building level; if the fabric site is defined at the area level, you must reserve the IP address pools at the area level.

  To work around this issue, release and reserve the IP address pool at the same level (area or building) as the fabric site, or reconfigure the fabric site at the same level as the reserved IP address pool.

- Cisco DNA Center does not support multicast across multiple fabric sites that are connected by an SDA transit network.

Brownfield Feature-Related Limitations

- 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

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.

AP Limitations

- AP as a sensor is not supported in this release of Cisco DNA Center.
- 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.
- Provisioning of 100 APs takes longer in this release as compared to 3 minutes in earlier releases. 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.

IP Device Tracking on Trunk Port Limitation

Rogue-on-wire detection is impacted; Cisco DNA Center does not show all clients connected to a switch via an access point in bridge mode. The trunk port is used to exchange all VLAN information. When you enable IP device tracking on the trunk port, clients connected on the neighbor switch are also shown. Cisco DNA Center does not collect client data if the connected interface is a trunk port and the neighbor is a switch. As a best practice, disable IP device tracking on the trunk port. The rogue-on-wire is not detected if the IP device tracking is enabled on the trunk port. See Disabling IP Device Tracking for more information.

IP Address Manager Limitations

- Cisco DNA Center supports integration with an external IPAM server that has trusted certificates. In the Cisco DNA Center GUI, under **System** > **Settings** > **External Services** > **IP Address Manager**, you might see the following error:

  ```
  NCIP10282: Unable to find the valid certification path to the requested target.
  ```

  To correct this error for a self-signed certificate:

  1. Using OpenSSL, enter one of the following commands to download the self-signed certificate, depending on your IPAM type. (You can specify the FQDN [domain name] or IP address in the command.)

     ```
     openssl s_client -showcerts -connect Infoblox-FQDN:443
     ```

     ```
     openssl s_client -showcerts -connect Bluecat-FQDN:443
     ```

  2. From the output, use the content from ---BEGIN CERTIFICATE--- to ---END CERTIFICATE--- to create a new .pem file.
  3. Go to **System** > **Settings** > **Trust & Privacy** > **Trustpool**, click **Import**, and upload the certificate (.pem file).
  4. Go to **System** > **Settings** > **External Services** > **IP Address Manager** and configure the external IPAM server. (If the IPAM server is already configured, skip this step.)

  To correct this error for a CA-signed certificate, install the root certificate and any intermediate certificates of the CA that is installed on the IPAM into the Cisco DNA Center trustpool (**System** > **Settings** > **Trust & Privacy** > **Trustpool**).

- You might see the following error if a CA-signed certificate is revoked by the certificate authority:

  ```
  NCIP10286: The remote server presented with a revoked certificate. Please verify the
  certificate.
  ```

  To correct this, obtain a new certificate from the certificate authority and upload it to **System** > **Settings** > **Trust & Privacy** > **Trustpool**.

- You might see the following error after configuring the external IPAM details:

  ```
  IPAM external sync failed:
  NCIP10264: Non Empty DNAC parent pool <CIDR> exists in external ipam.
  ```

  To correct this, log in to the external IPAM server (such as BlueCat). Confirm that the parent pool CIDR exists in the external IPAM server, and remove all the child pools that are configured under that parent

pool. Then, return to the Cisco DNA Center GUI and reconfigure the IPAM server under **System** > **Settings** > **External Services** > **IP Address Manager**.

- You might see the following error while using IP Address Manager to configure an external IPAM:

```
NCIP10114: I/O error on GET request for "https://<IP>/wapi/v1.2/":
Host name '<IP>' does not match the certificate subject provided by the peer
(CN=www.infoblox.com, OU=Engineering, O=Infoblox, L=Sunnyvale, ST=California, C=US);
nested exception is javax.net.ssl.SSLPeerUnverifiedException: Host name '<IP>'
does not match the certificate subject provided by the peer (CN=www.infoblox.com,
OU=Engineering,
O=Infoblox, L=Sunnyvale, ST=California, C=US) |
```

To correct this, log in to the external IPAM server (such as Infoblox) and regenerate your external IPAM certificate with the common name (CN) value as the valid hostname or IP address. In the preceding example, the CN value is www.infoblox.com, which is not the valid hostname or IP address of the external IPAM.

After you regenerate the certificate with a valid CN value, go to **System** > **Settings** > **Trust & Privacy** > **Trustpool**. Click **Import** and upload the new certificate (.pem file).

Then, go to **System** > **Settings** > **External Services** > **IP Address Manager** and configure the external IPAM server with the server URL as the valid hostname or IP address (as listed as the CN value in the certificate).

Cisco Plug and Play Limitations

- 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>
```

Cisco Group-Based Policy Analytics Limitations

- Cisco Group-Based Policy Analytics supports up to five concurrent requests based on realistic customer data. While it is desirable for UI operations to respond within five seconds or less, for extreme cases based on realistic data, it can take upto 20 seconds. There is no mechanism to prevent more than five simultaneous requests at a time, but if it does happen, it might cause some UI operations to fail. Operations that take longer than a minute will time out.
- Data aggregation occurs at hourly offsets from UTC in Cisco Group-Based Policy Analytics. However, some time zones are at a 30-minute or 45-minute offset from UTC. If the Cisco DNA Center server is located in a time zone with a 30-minute or 45-minute offset from UTC and the client is located in a time zone with an hourly offset from UTC, or vice versa, the time ranges for data aggregation in Cisco Group-Based Policy Analytics are incorrect for the client.

  For example, assume that the Cisco DNA Center server is located in California PDT (UTC-7) where data aggregations occur at hourly offsets (8:00 a.m., 9:00 a.m., 10:00 a.m., and so on). When a client

located in India IST (UTC+5.30) wants to see the data between 10:00 - 11:00 p.m. IST, which corresponds to the time range 9:30 - 10:30 a.m. PDT in California, no aggregations are seen.

- Group changes that occur within an hour are not captured. When an endpoint changes from one scalable group to another, Cisco Group-Based Policy Analytics is unaware of this change until the next hour.
- You cannot sort the Scalable Group and Stealthwatch Host Group columns in the **Search Results** window.
- You might see discrepancies in the information related to Network Access Device (including location) between Cisco DNA Assurance and Cisco Group-Based Policy Analytics.

Application Telemetry Limitation

When configuring application telemetry on a device, Cisco DNA Center might choose the wrong interface as the source for NetFlow data.

To force Cisco DNA Center to choose a specific interface, add netflow-source in the description of the interface. You can use a special character followed by a space after netflow-source, but not before it. For example, the following syntax is valid:

```
netflow-source
MANAGEMENT netflow-source
MANAGEMENTnetflow-source
netflow-source MANAGEMENT
netflow-sourceMANAGEMENT
netflow-source & MANAGEMENT
netflow-source |MANAGEMENT
```

The following syntax is invalid:

```
MANAGEMENT | netflow-source
* netflow-source
netflow-source|MANAGEMENT
```

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