Release Notes for Cisco DNA Center, Release 2.2.3.x

First Published: 2021-08-04

Last Modified: 2023-10-20

Release Notes for Cisco DNA Center, Release 2.2.3.x

This document describes the features, limitations, and bugs for Cisco DNA Center, Release 2.2.3.x.

Change History

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

Table 1: Document Change History

Date	Change	Location
2023-10-20	Added a limitation about the site hierarchy for a Rogue and aWIPS report.	Limitations and Restrictions, on page 58
2023-09-28	Added the open bug CSCwe28523.	Open Bugs, on page 36
2023-07-31	Previously, the *Cisco DNA Center Release Notes* and the *Cisco DNA Center Platform Release Notes* were separate. Now, they are combined into a single release note; the Cisco DNA Center platform content has been consolidated into this document.	—
2023-02-27	Added the open bug CSCwe27538.	Open Bugs, on page 36
2023-02-17	Added a limitation about In-Service Software Upgrade (ISSU).	Limitations and Restrictions, on page 58
2022-11-08	Added the open bug CSCwc09546.	Open Bugs, on page 36
2022-07-27	Updated the information provided for the Cisco DNA Center 2.2.3.6 System package.	Package Versions in Cisco DNA Center, Release 2.2.3.x, on page 2
2022-07-21	Added the list of packages in Cisco DNA Center 2.2.3.6.	Package Versions in Cisco DNA Center, Release 2.2.3.x, on page 2
	Noted that Cisco DNA Center 2.2.3.6 contains fixes for the Spring4Shell vulnerability.	New and Changed Features in Cisco DNA Center, on page 5
	Added the Resolved Bugs table for 2.2.3.6.	Resolved Bugs, on page 44
	Added the open bug CSCwb28540.	Open Bugs, on page 36

Date	Change	Location
2022-04-04	Added the new and changed Interactive Help information for 2.2.3.5.	New and Changed Features in Interactive Help, on page 30
	Added the list of packages in Cisco DNA Center 2.2.3.5.	Package Versions in Cisco DNA Center, Release 2.2.3.x, on page 2
	Added the Resolved Bugs table for 2.2.3.5.	Resolved Bugs, on page 44
	Added the open bugs CSCwa88686 and CSCwa99062	Open Bugs, on page 36
2021-12-23	Added the list of packages in Cisco DNA Center 2.2.3.4.	Package Versions in Cisco DNA Center, Release 2.2.3.x, on page 2
	Added the Resolved Bugs table for 2.2.3.4.	Resolved Bugs, on page 44
	Noted that Cisco DNA Center 2.2.3.4 contains fixes for the Apache Log4j vulnerability.	New and Changed Features in Cisco DNA Center, on page 5
2021-11-23	Added the open bug CSCwa30225.	Open Bugs, on page 36
2021-10-26	Added the link to download Cisco DNA Center software.	Package Versions in Cisco DNA Center, Release 2.2.3.x, on page 2
2021-10-04	Added the list of packages in Cisco DNA Center 2.2.3.3.	Package Versions in Cisco DNA Center, Release 2.2.3.x, on page 2
	Added the Resolved Bugs table for 2.2.3.3.	Resolved Bugs, on page 44
	Added the open bug CSCvy87482.	Open Bugs, on page 36
2021-08-19	Added the open bug CSCvy30606.	Open Bugs, on page 36
2021-08-04	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*.

Package Versions in Cisco DNA Center, Release 2.2.3.x

To download Cisco DNA Center software, go to https://software.cisco.com/download/home/286316341/type.

Table 2: Updated Packages and Versions in Cisco DNA Center 2.2.3.x.

Package Name	Release 2.2.3.6	Release 2.2.3.5	Release 2.2.3.4	Release 2.2.3.3	Release 2.2.3.0
System Updates					
System	1.6.718 1.6.711	1.6.706	1.6.703	1.6.551	1.6.430
System Commons	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60472	2.1.385.60720

Package Name	Release 2.2.3.6	Release 2.2.3.5	Release 2.2.3.4	Release 2.2.3.3	Release 2.2.3.0
Package Updates					
Access Control Application	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60445	2.1.385.60720
AI Endpoint Analytics	1.5.0.242	1.5.0.242	1.5.0.238	1.5.0.226	1.5.0.217
AI Network Analytics	2.7.19.612	2.7.16.588	2.7.14.582	2.7.8.528	2.7.6.515
Application Hosting	1.7.2.2204060758	1.7.2.2202011254	1.7.2.2112171046	1.7.0.2108120753	1.7.0.2107160721
Application Policy	2.1.391.172288	2.1.390.172230	2.1.389.172094	2.1.388.170155	2.1.385.117422
Application Registry	2.1.391.172288	2.1.390.172230	2.1.389.172094	2.1.388.170155	2.1.385.117422
Application Visibility	2.1.391.172288	2.1.390.172230	2.1.389.172094	2.1.388.170155	2.1.385.117422
Assurance - Base	2.2.3.506	2.2.3.457	2.2.3.408	2.2.3.337	2.2.3.276
Assurance - Sensor	2.2.3.456	2.2.3.456	2.2.3.406	2.2.3.317	2.2.3.239
Automation - Base	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60445	2.1.385.60720
Automation - Intelligent Capture	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60445	2.1.385.60720
Automation - Sensor	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60445	2.1.385.60720
Cisco DNA Center Global Search	1.6.99.12	1.6.99.12	1.6.99.11	1.6.99.10	1.6.99.9
Cisco DNA Center Platform	1.6.1.180	1.6.1.162	1.6.1.145	1.6.1.126	1.6.1.86
Cisco DNA Center UI	1.6.3.201	1.6.3.189	1.6.3.169	1.6.3.155	1.6.3.95
Cisco Umbrella	2.1.391.592253	2.1.390.592151	2.1.389.592052	2.1.388.590077	2.1.385.590131
Cloud Connectivity - Contextual Content	1.3.1.364	1.3.1.364	1.3.1.364	1.3.1.364	1.3.1.359
Cloud Connectivity - Data Hub	1.6.0.380	1.6.0.380	1.6.0.380	1.6.0.380	1.6.0.380
Cloud Connectivity - Tethering	2.13.1.4	2.13.1.4	2.13.1.4	2.13.1.4	2.1.1.43
Cloud Device Provisioning Application	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60445	2.1.385.60720
Command Runner	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60445	2.1.385.60720
Device Onboarding	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60445	2.1.385.60720
Disaster Recovery	2.1.391.3620033	2.1.390.3620020	2.1.389.3620004	2.1.388.3600024	2.1.385.36096
Disaster Recovery—Witness Site	2.1.391.3720020	2.1.390.3720019	2.1.389.3720003	2.1.388.3700006	2.1.385.37029
Group-Based Policy Analytics	2.2.3.64	2.2.3.64	2.2.3.61	2.2.3.55	2.2.3.49
Image Management	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60445	2.1.385.60720

Package Name	Release 2.2.3.6	Release 2.2.3.5	Release 2.2.3.4	Release 2.2.3.3	Release 2.2.3.0
Machine Reasoning	2.1.391.212019	2.1.390.212018	2.1.389.212015	2.1.388.210008	2.1.385.210073
NCP - Base	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60445	2.1.385.60720
NCP - Services	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60445	2.1.385.60720
Network Controller Platform	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60445	2.1.385.60720
Network Data Platform - Base Analytics	1.6.1700	1.6.1698	1.6.1696	1.6.1686	1.6.1654
Network Data Platform - Core	1.6.1720	1.6.1719	1.6.1715	1.6.1705	1.6.1677
Network Data Platform - Manager	1.6.1671	1.6.1670	1.6.1669	1.6.1662	1.6.1624
Network Experience Platform - Core	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60445	2.1.385.60720
Path Trace	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60445	2.1.385.60720
RBAC Extensions	2.1.391.192003	2.1.390.192002	2.1.389.192001	2.1.388.190003	2.1.385.1900004
Rogue and aWIPS	2.3.0.31	2.3.0.29	2.3.0.29	2.3.0.24	2.3.0.22
SD-Access	2.1.391.62945	2.1.390.62654	2.1.389.62331	2.1.388.60445	2.1.385.60720
Stealthwatch Security Analytics	2.1.391.1092249	2.1.390.1092151	2.1.389.1092057	2.1.388.1090064	2.1.385.1090063
Wide Area Bonjour	2.4.391.75000	2.4.390.75203	2.4.368.75006	2.4.364.75035	2.4.364.75035

New and Changed Information

New and Changed Features in Cisco DNA Center

Important Updates in Cisco DNA Center 2.2.3.4

Feature	Description
Fixes for the Apache Log4j Vulnerability	In December 2021, the Apache Software Foundation disclosed vulnerabilities in the open-source Log4j logging library. At this time, almost all affected Cisco products have either been remediated or have a software update scheduled for release. Cisco is committed to transparency and we have published a security advisory to make sure our customers understand the issue and how to address it. Please refer to our advisory for the latest information: Cisco Security Advisory: Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021 Cisco DNA Center 2.2.3.4 contains fixes for the Apache Log4j vulnerability. This effort is being tracked as CSCwa47322 for the Cisco DNA Center product and contains the following fixes: • CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints. • CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack. To help assess, identify, and reduce exposure to vulnerabilities, consider running a trusted vulnerability scanner. For example: • https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance • https://github.com/cisagov/log4j-scanner • https://github.com/CERTCC/CVE-2021-44228_scanner
System Health Validation Tool	Cisco DNA Center 2.2.3.4 introduces the System Health validation tool, which tests both Cisco DNA Center appliance hardware and connected external systems and identifies any issues that need to be addressed before they seriously impact your network. The validation process makes numerous checks, such as: • The ability to connect to ciscoconnectdna.com (in order to download system and package updates). • The presence of expiring certificates. • The current health of appliance hardware and back-end services. • The network components that have exceeded a scale number threshold.

Table 3: New and Changed Features in Cisco DNA Center 2.2.3

Feature	Description
3D Wireless Maps	A 3D mode has been added for viewing wireless maps. With 3D wireless maps, you can view a 3D visualization of your wireless network and key performance indicators (KPIs). 3D wireless maps offer a wide range of features and functionality, such as: • Navigate through your wireless network in a 3D environment. • Receive near real-time KPI data from the 3D wireless maps predictive model. • View the radio frequency (RF) coverage for specific elevations. • Gain insights for the areas in your wireless network where service-level agreements (SLAs) are not being met. • Create simulations of custom device configurations.
802.1x Authentication Support for Access Points	You can configure the authentication settings for the secure onboarding of access points (APs) using Plug and Play (PnP). Based on the authentication settings configured at the Global-level or Site-level hierarchy in Cisco DNA Center, PnP pushes the 802.1x (Dot1x) supplicant and certificates when claiming APs.
Application Policy Support	Application Policy support is available for Cisco Catalyst IE3300 Series and IE3400 Series switches.
Change the Protocol Order of an Image Distribution Server	You can choose the required protocol for software image distribution by changing the protocol order of an image distribution server. The protocol order helps perform verification checks on the image distribution servers.
Compliance	When Startup and Running configurations for a device are mismatched, you can run compliance checks and synchronize running configurations across multiple devices under **Action** > **Compliance** in the **Inventory** window.
Define Custom Applications for Devices Without QoS Policy	You can configure custom applications with attribute sets and maps on Cisco DNA Traffic Telemetry Appliance without configuring the quality of service (QoS) policy.
Deny RCM Clients	Cisco DNA Center prevents the clients that are using random MAC addresses from joining the network. You can choose to deny or allow the clients with random MAC addresses when creating Enterprise SSIDs and Guest SSIDs.
Different Views for Templates and Model Configs	You can view the templates and model configurations in the **Cards** view or the **Table** view when creating a network profile for Switching or Wireless.
Enable Telemetry on Switches	You can configure Switched Port Analyzer (SPAN) and Encapsulated Remote Switched Port Analyzer (ERSPAN) sessions on switches to share IP traffic for application assurance and endpoint analytics.
Fixed Versions for Security Advisories	The **Fixed Versions** column has been added to the **Security Advisories** window. This column lists the minimum known fixed version for security advisories. You can remove an advisory on your device by upgrading to the version mentioned in the **Fixed Versions** column.

Feature	Description
Flash Cleanup	You can store only the running software image and remove all the previous software images saved on a device when provisioning a software image or upgrading a software image with In-Service Software Upgrade (ISSU).
FlexConnect VLAN Mapping for AAA Override	For FlexConnect deployments, you now have the option to configure AAA override VLANs for dynamic VLAN assignment of locally switched clients.
Group-Based Access Control Policy Dashboard	With the Group-Based Access Control Policy dashboard, you can view a summary of network activity, policy-related issues, and traffic trends. In the Cisco DNA Center GUI, click the **Menu** icon and choose **Policy** > **Group-Based Access Control** > **Overview** to view this dashboard.
IPAM Trust Certificate Handling	Previously, you had to manually import the trust certificate for IP Address Manager (IPAM) integration. With this release, when you add an IPAM to Cisco DNA Center, the trust certificate is automatically added to the Cisco DNA Center trustpool.
License Manager Supports FQDN Configuration in Smart Proxy and On-Prem SSM Modes	If a satellite is configured with a fully qualified domain name (FQDN), the call-home configuration of the satellite FQDN is pushed instead of the IP address.
Manage Device Credentials - Usability Enhancements	You can view the credential status of all the devices in a site in the **Design** > **Network Settings** > **Device Credentials** window.
New Device Support for Return Material Authorization	You can replace a failed device with a new device and use the Return Material Authorization (RMA) workflow to replace the image, license, and configuration on the new device. Cisco DNA Center provides one-touch RMA support for the following switches: • Switches that are discovered and configured using LAN automation, including the seed devices (LAN automation primary and peer devices) • Devices configured as fabric in a box (standalone only)
New Model Config Design for AAA RADIUS Attributes	The AAA RADIUS **Called-station-id** parameter that is configured on Cisco AireOS Controllers and Cisco Catalyst 9800 Series Wireless Controllers is no longer restricted to be the ap-macaddress-ssid attribute value. You can now create a model configuration for AAA RADIUS attributes and choose from a list of several attribute values.
Port Actions	You can clear the MAC address of a port and shut it down. To activate an error-disabled port, clear the MAC address and then shut down the port.
RADIUS Profiling Configuration on Controllers	You can enable RADIUS client profiling on Enterprise service set identifiers (SSIDs).
Rebranding of Application Policy as Application QoS Policy	The menu navigation for Application Policies is changed from **Policy** > **Application** to **Policy** > **Application QoS**.
Replace Device Workflow	The workflow guides you step-by-step to replace a faulty device.
Retry Image Update Tasks	You can retry the image update for failed image update tasks.
Share Custom Topologies	You can mark a topology view as "shared." The shared custom topologies are viewable by other users irrespective of their role.

Feature	Description
Smart License Policy Compliance	The Smart License Policy (SLP) compliance shows a timeline graph of the license usage reports sent from Cisco DNA Center to Cisco Smart Software Manager (CSSM). Devices that are a part of the license usage reporting process are shown in a table.
Support for a New Stadium (Large Public Venue) Antenna	Cisco DNA Center now supports the C-ANT9104 antenna, which integrates with the C9130AXE to provide dual 5-GHz 4x4 radios with high gain, steerable, and switchable functions. With Cisco DNA Center, you can select the beam steering (direction) for the antennae. The following modes are available: • Wide beam • Narrow beam • Narrow beam with 10 degrees of tilt • Narrow beam with 20 degrees of tilt The beam steering configuration is available for antenna combinations ABCD (the left antennae) and EFGH (the right antennae). The antenna pattern names are set based on the selected beam. You can visualize the heatmaps on Cisco DNA Center floor maps.
Support for Cisco Wi-Fi 6 Wide Interface Pluggable Module	Cisco DNA Center now supports the Cisco Wi-Fi 6 Wide Interface Pluggable Module for Cisco Catalyst IR1800 Rugged Series Routers.
Template Editor	• The **Simulation Editor** option is available for composite templates to provide one integrated form for all the composite templates, which allows you to run a simulation for composite templates without having to go to multiple templates. • When you provision a device, the **Advanced Configuration** window displays an integrated form to all member templates in the composite template. • While creating a new template, in the **Select Device Type (s)** window, each device model in the device type hierarchy is sorted alphabetically. The Template Editor also allows you to mark a device model as a favorite to create a custom favorite list of device models.
Wireless Maps: View the KPIs of AP Neighbors	For wireless maps, you can hover your cursor over an AP to view the dBm values for the neighboring APs.

New and Changed Features in Cisco DNA Assurance

Table 4: New and Changed Features for Cisco DNA Assurance, Release 2.2.3.4

Feature	Description
Cisco AI Network Analytics — Radio Insights Based on Client Experience	Cisco AI Network Analytics uses machine learning algorithms to identify wireless APs with a potentially poor client experience. APs are continually analyzed over long periods and those suspected of providing a suboptimal client experience are grouped by underlying root cause and suggested improvements.
Power over Ethernet (PoE) AP Power Mode Distribution Dashlet	You can display the distribution of fully- and partially-powered APs. To display this information, click the menu icon and choose **Assurance** > **PoE**. The **PoE** dashboard opens.

Feature	Description
Trend View Enhancement for Wireless Clients in Client Dashboard	In the Client Health Summary, the trend view of wireless clients is enhanced. The radial bar chart provides the distribution of clients that failed to onboard, and the reason for the onboarding failure.
Virtual Network 360 Window	You can view details about a virtual network. To display this information, click the menu icon and choose **Assurance** > **Health** > **SD-Access**.
Webex Client 360	In the Webex Client 360, the client meetings table is enhanced with the following columns to indicate the overall health for each meeting: • Application: Shows the health scores and KPIs reported by the Webex Control Hub. • Network: Shows the health scores and KPIs reported by Cisco DNA Center through NetFlow exported from the managed network devices.

Table 5: New and Changed Features for Cisco DNA Assurance, Release 2.2.3.3

Feature	Description
Site Hierarchy Support for Assurance	The **Assurance** > **Health** and **Assurance** > **Issues** dashboards are enhanced to show a Site hierarchy filter and Site table for the health tabs, such as **Overall**, **Network**, and **Clients**, and issues tabs, such as **Open**, **Resolved**, and **Ignored**.

Table 6: New and Changed Features for Cisco DNA Assurance, Release 2.2.3

Feature	Description
AP 360 KPIs	The following AP details attributes are included in the Device Details area: • General Information - Power Status • Network Information - Connected Switch Under the **Connectivity** tab, the following attributes are included: • Connected Switch banner is added for Ethernet Interface KPIs. • Current Channel and Extended Channel(s) are added for Radio Specific KPIs. Under **RF** tab, Clean Air Status and Tx Power is added for Radio Specific KPIs. Tx Power and Channel Information charts are newly added for Radio Specific KPIs.
Auto Refresh	The Cisco DNA Center Assurance health window supports Auto Refresh settings. This settings option allows you to enable the auto refresh capability for the assurance windows, such as Overall health, Network, Client, Application, Device 360, Client 360 and Wi-Fi 6.
Client 360 Onboarding Times	In Client 360, the timeline slider displays the client onboarding details, such as Association, Authentication, and DHCP time.

Feature	Description
Dedicated SSID Filter Added in Application Health Dashboard	The SSID filter option is added to the **Assurance** > **Health** > **Application** dashboard. The SSID filter option allows you to choose the SSID. Depending on your selection, the information in the **Application Health** dashboard is refreshed.
IPv6 Support for Application Assurance and Telemetry	Monitors IPv6 traffic from the following devices and shows the monitored data in the **Assurance** dashboard: • Cisco Catalyst 9300 Series and Catalyst 9400 Series switches running Cisco IOS-XE software version 17.2.1 or later. • Routers running Cisco IOS-XE software version 17.3 or later. • Cisco DNA Traffic Telemetry Appliance running Cisco IOS-XE software version 17.3 or later.
Neighbor and Rogue View for AP 360	For AP 360, the Neighbors and Rogues section is displayed under the **RF** tab, which contains filters, such as **Band** (2 GHz and 5 GHz), **Type (All, Neighbor, and Rogue)**, and **RSSI Range** (0 to -100 dBm). Depending on your filter selection, the AP device and Wi-Fi analyzer graph is refreshed.
Network Heatmap Enhancements	The **Network Heatmaps** window supports **Export** of heatmap data to a CSV file.
Network Services	With this release, the **Network Services** tab is added to the **Assurance** > **Health** dashboard. The **Network Services** tab allows you to view and monitor all the transactions and latencies of **AAA** and **DHCP** servers reported by wireless controllers.
Network Services Dashlet	In the **Overall Health** dashboard, a new **Network Services** dashlet displays the total successful and failed transactions for all the **AAA** and **DHCP** servers reported by wireless controllers in your overall enterprise.
Path Trace Enhancements	Path Trace is enhanced with the **Live Traffic** to capture the network packets.
PoE Enhancements	In **Assurance > Dashboards > PoE** dashboard, a new **PoE AP Power Mode Distribution** dashlet displays the distribution of fully powered and partially powered APs. In addition, Power over Ethernet (PoE) elements for APs are now displayed in device and client detail windows.
SD-Access Landing Window and Fabric View	With this release, the **SD-Access** tab is added to the **Assurance** > **Health** dashboard. Fabric-specific health information is provided in separate windows from the network health window. You can display the overall SD-Access fabric network health and drill down to view details about site-specific and device-specific fabric health information.
Server Latency for Client Onboardings	In the **Client Onboarding Times** dashlet, the detailed view of latest client onboardings chart displays Server and Latency time for Authentication and DHCP onboardings.
Webex Client 360 Enhancements	In Client 360, use the Webex 360 to view and monitor the client webex meetings.

New and Changed Features in Cisco DNA Center Platform

Feature	Description
New API Features	
Application API	The Cisco DNA Center platform supports a new **Application** API that allows you to get a list of issues, devices, and endpoints for a combination of a specific application with site and/or device. • GET <cluster-ip>/dna/intent/api/v1/application-health Intent API to get a list of applications for a specific site, a device, or a client device's MAC address. For a combination of a specific application with site and/or device, the API gets a list of issues/devices/endpoints. To access the new application API in the Cisco DNA Center GUI, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Application**.

Feature	Description
Application Policy APIs	

Feature	Description
	The Cisco DNA Center platform supports the following new **Application Policy** APIs: • GET <cluster-ip>/dna/intent/api/v1/app-policy-default Get default application policy. • GET <cluster-ip>/dna/intent/api/v1/app-policy Get all existing application policies. • POST <cluster-ip>/dna/intent/api/v1/app-policy-intent Create, update, or delete an application policy. The Cisco DNA Center platform supports the following new **Application Policy** queuing profile APIs: • DELETE <cluster-ip>/dna/intent/api/v1/app-policy-queuing-profile/${id} Delete an existing custom application policy queuing profile by ID. • GET <cluster-ip>/dna/intent/api/v1/app-policy-queuing-profile Get all existing application policy queuing profiles, or get them by name. • GET <cluster-ip>/dna/intent/api/v1/app-policy-queuing-profile-count Get the number of all existing application policy queuing profiles. • POST <cluster-ip>/dna/intent/api/v1/app-policy-queuing-profile Create a new custom application queuing profile. • PUT <cluster-ip>/dna/intent/api/v1/app-policy-queuing-profile Update an existing custom application queuing profile. The Cisco DNA Center platform supports the following new **Quality of Service (QoS)** device interface APIs: • GET <cluster-ip>/dna/intent/api/v1/qos-device-interface-info Get all existing QoS device interfaces, or get them by network device ID. • POST <cluster-ip>/dna/intent/api/v1/qos-device-interface-info Create QoS device interface information associated with a network device ID. This allows you to mark specific interfaces as WAN, associate WAN interfaces with specific SP profiles, and define a shaper on WAN interfaces. • PUT <cluster-ip>/dna/intent/api/v1/qos-device-interface-info Update existing QoS device interface information associated with a network device ID.

Feature	Description
	- DELETE <cluster-ip>/dna/intent/api/v1/qos-device-interface-info/${id} Delete all QoS device interface information associated with a network device ID. - GET <cluster-ip>/dna/intent/api/v1/qos-device-interface-info-count Get the number of all existing QoS device interface information groups by network device ID. The Cisco DNA Center platform supports the following new **AI Endpoint Analytics** APIs to manage profiling rules for the endpoints:

Feature	Description
	- PUT <cluster-ip>/dna/intent/api/v1/endpoint-analytics/profiling-rules/${ruleId} Update the profiling rule for a given rule ID. - POST <cluster-ip>/dna/intent/api/v1/endpoint-analytics/profiling-rules/bulk Import a list of profiling rules. For each record: - If **ruleType** for a record is not **Custom Rule**, it is rejected. - If **ruleId** is provided in the input record: - If a record with the same **ruleId** exists in the system, it is replaced with new data. - If a record with the same **ruleId** does not exist, it is inserted in the database. - If a **ruleId** is not provided in the input record, the system generates a new **ruleId** and inserts it in the record. - DELETE <cluster-ip>/dna/intent/api/v1/endpoint-analytics/profiling-rules/${ruleId} Delete the profiling rule for the given rule ID. - POST <cluster-ip>/dna/intent/api/v1/endpoint-analytics/profiling-rules Create a profiling rule from the request body. - GET <cluster-ip>/dna/intent/api/v1/endpoint-analytics/profiling-rules/count Get the count of profiling rules based on the filter values provided in the query parameters. The filter parameters are the same as that of the GET /profiling-rules API, excluding the pagination and sort parameters. - GET <cluster-ip>/dna/intent/api/v1/endpoint-analytics/profiling-rules/${ruleId} Get details of the profiling rule for the given rule ID. - GET <cluster-ip>/dna/intent/api/v1/endpoint-analytics/profiling-rules Get the list of profiling rules and show those rules in client applications, or export those rules from an environment. The POST/profiling-rules/bulk API can be used to import such exported rules into another environment. If this API is used to export rules to be imported into another Cisco DNA Center system, ensure that the **includeDeleted** parameter is **true**, so that deleted rules are synchronized correctly. You must use query parameters to filter the data, as required. If no filter is provided, this API includes only rules of type **Custom Rule** in the response. By default, the response is limited to 500 records. You must use the **limit** parameter to retrieve a higher number of records, if required. The GET/profiling-rules/count API can be used

Feature	Description
	to find out the total number of rules in the system. **Note** You must enable the **AI Endpoint Analytics** bundle to view AI endpoint analytics APIs in the Cisco DNA Center platform. To access the new application policy API in the Cisco DNA Center GUI, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Policy** drop-down list and choose **Application Policy**.
Configuration Templates APIs	The Cisco DNA Center platform supports the following new **Configuration Templates** APIs with more input filter parameters: • GET <cluster-ip>/dna/intent/api/v2/template-programmer/project Get project(s) details. • GET <cluster-ip>/dna/intent/api/v2/template-programmer/template Get template(s) details. To access the new configuration template API in the Cisco DNA Center GUI, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Configuration Templates**.
Device Onboarding (PnP) API	In the PnP workflow, the Cisco DNA Center platform now allows you to bypass the provisioning workflow and provision multiple access point devices via API: • POST <cluster-ip>/dna/intent/api/v1/onboarding/pnp-device/claim Claims one or more devices with a specified workflow. To access the PnP API in the Cisco DNA Center GUI, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Device Onboarding (PnP)**.

Feature	Description
Site Design APIs	The Cisco DNA Center platform supports the following new **Site Design** APIs: • POST <cluster-ip>/dna/intent/api/v1/networkprofile/${networkProfileId}/site/${siteId} Associate a site to a network profile. • DELETE <cluster-ip>/dna/intent/api/v1/networkprofile/${networkProfileId}/site/${siteId} Disassociate a site from a network profile. To access the new site design API in the Cisco DNA Center GUI, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Site Design**.
SWIM APIs	The Cisco DNA Center platform supports the following new **SWIM** APIs: • GET <cluster-ip>/dna/intent/api/v1/image/importation/device-family-identifiers API to get device family identifiers for all device families that can be used for tagging an image as golden. • POST <cluster-ip>/dna/intent/api/v1/image/importation/golden Golden tag image. Set siteId as -1 for a global site. • DELETE <cluster-ip>/dna/intent/api/v1/image/importation/golden/site/${siteId}/family/${deviceFamilyIdentifier}/role/${deviceRole}/image/${imageId} Remove golden tag. Set siteId as -1 for a global site. • GET <cluster-ip>/dna/intent/api/v1/image/importation/golden/site/${siteId}/family/${deviceFamilyIdentifier}/role/${deviceRole}/image/${imageId} Get golden tag status of an image. Set siteId as -1 for a global site. To access the new SWIM API in the Cisco DNA Center GUI, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Software Image Management (SWIM)**.
Task API	The Cisco DNA Center platform supports the following new **Task** API: • GET <cluster-ip>/dna/intent/api/v1/dnacaap/management/execution-status/${executionId} Retrieves the execution details of a business API. To access the new task API in the Cisco DNA Center GUI, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Operational Tasks** drop-down list and choose **Task**.

Feature	Description
New ITSM Integration Features	
Network Hierarchy on Basic ITSM (ServiceNow) CMDB Synchronization	While configuring the basic ITSM (ServiceNow) CMDB synchronization bundle, the location reference field supports both area and address as additional attributes.
Webex Teams Integrations	With this release, Cisco DNA Center is integrated with **WEBEX** subscription type. To subscribe the **WEBEX** subscription type, you must have **WebEx Teams Room Id** and **WebEx Teams Bot Access Token** to list the **WEBEX** in the **Subscription Type** drop-down list. For more information, see Subscribe Cisco DNA Center Event Notifications to Cisco WebEx in Cisco DNA Center ITSM Integration Guide.
New Platform Bundle Support	
AI Endpoint Analytics	With this release Cisco DNA Center platform supports the AI Endpoint Analytics bundle that allows you to access various services provided by the AI endpoint analytics application. You must install the AI Endpoint Analytics package in Cisco DNA Center to use this bundle.
New Reports	

Feature	Description
AP Performance Report	

Feature	Description
	This release supports a new **AP Performance** report. This report provides a detailed list of key performance indicators from access points in the network. **Note** Ensure that the Cisco AI Network Analytics application is enabled. For more information, see Configure Cisco AI Network Analytics Data Collection in the *Cisco DNA Assurance User Guide*. • Supported report file formats include CSV, TDE, and JSON. • If no data is available for recent onboarding cases that are less than 7 days, Cisco DNA Center generates a successful but empty AP performance report. You must use heatmaps to view the recent data. • The AP performance report covers long intervals and internally aggregates data to a granularity of two hours. If the start and end timestamps are not aligned to two-hour slots, Cisco DNA Center still runs the report, but the actual data may not correspond to the provided start and end timestamps. • The AP performance report does not include the data from the past two hours. • In case of cloud connectivity issues, the AP performance report may fail, and you must run the report request again. • In the **Select Report Template** window, the AP performance report template displays the following KPIs from an access point in the network: • AP MAC address: Access point radio MAC address. • AP Radio Slot: Slot ID of the radio module in the access point. • AP Name: Access point name. • Frequency Band: Radio carrier band configured for the access point radio. • Average Radio Throughput (bps): Average throughput (TX+RX) per radio. • Average Cloud Apps Throughput (bps): Average throughput (TX+RX) per radio, which is limited to the **Cloud** applications group. • Average Media Apps Throughput (bps): Average throughput (TX+RX) per radio, which is limited to the **Media** applications group. • Radio Reset Count: Total number of radio resets due to failures. • Packet Failure Rate (percentage): Indicates poor radio link quality where you cannot deliver the packets even after multiple retransmissions or radio failure conditions.

Feature	Description
	• Radio Distinct Client Count: Total number of distinct clients per radio. • Radio Distinct App Count: Total number of distinct applications per radio. • Channel Change Count: External interferes cause channel changes and negatively impact the client experience. • Priority Queue Failures (Packets): Total number of packets that failed to be sent in the access point priority queue (voice/video/best effort). • Priority Queue Discards (Packets): Total number of packets discarded in the access point priority queue (voice/video/best effort). • Average Client RSSI (dBm): Indicates the radio coverage. Lower values imply bad coverage, affecting connection quality and stability. • Average Client SNR (dB): Low SNR indicates the radio link quality. Lower values imply worse connection quality. • Traffic (percentage): Traffic indicates the airtime spent by radios to serve their own clients and may not indicate a problem. If the traffic levels are consistently very high, it may indicate the area(s) served by those radios require higher capacity to provide optimal client experience. • Co-Channel Interference (percentage): Co-channel interference (CCI) is caused by Wi-Fi traffic on the same serving channel as the radio reporting it, either by neighbor or foreign APs and clients. If radios constantly report high co-channel interference even when using Radio Resource Management (RRM), it is recommended to review the RF profile settings to match the RF deployment. • Channel Utilization (percentage): Channel utilization includes percentage of the time of a busy channel, considering Wi-Fi traffic (local or neighbor APs) and non-Wi-Fi noise and interference. High channel utilization due to external factors implies that the radio may not have enough capacity to provide optimal performance to the clients associated to it. You must verify the RF profile configuration while using RRM and perform spectrum analysis capture to identify and remove interferers. Under normal conditions, channel utilization is greater than or equal to the traffic and CCI. • Average Data Rate (Mbps): Data rates are a function of the radio, client capabilities, and link quality.

Feature	Description
AP - Usage and Client Breakdown	This release supports a new **AP - Usage and Client Breakdown** report. This report provides analytics data about total usage through selected access points and breakdown of the clients and traffic by OS types, SSID, and VLAN. • Supported report file formats include PDF, CSV, TDE, and JSON. • The **Select Report Template** preview page displays the latest **AP - Usage and Client Breakdown** report sample. • In the **Setup Report Scope** window, the **AP Name** drop-down list is filtered based on the location you select in the **Location** filter. • A notification appears below the **AP Name** drop-down list that show the number of filtered access point options out of total access points for the selected location. To access the **AP - Usage and Client Breakdown** report in the Cisco DNA Center GUI, click the menu icon and choose **Report** > **Reports Templates** > **Access Point**. In the **Report** window, choose **AP - Usage and Client Breakdown**. For more information about AP reports, see the *Cisco DNA Center Platform User Guide*.
New Reports Features	

Feature	Description
New Reports GUI Features	

Feature	Description
	This Cisco DNA Center platform release supports the following new features for **Reports**: • The Cisco DNA Center platform support is extended for the dynamic lookup filter in the report. In the **Setup Report Scope** window, when you choose a filter attribute from the drop-down list, the other corresponding dependent filter attribute changes depending upon the selected filter attribute. **Note** With this release, **Client Trend - Count And Traffic** reports are supported with dynamic lookup filter. • With this release, the Cisco DNA Center platform allows you to retain the report data up to a year. In the **Schedule Report** window, the time range options are extended from last 90 days to 365 days. In the **Time Range** area, **Custom** radio button allows you to choose the date and time interval up to 365 days to generate a custom report. Cisco DNA Center uses granular data based on the selected time range to generate a report. In the **Schedule Report** window, Cisco DNA Center uses 5 minutes, hourly, daily, weekly, and monthly data intervals. Custom reports are generated in the following data intervals: • Hourly report is generated at fifth minute of each hour. • Daily report is generated at fifth minute of each day. • Weekly report is generated at fifth minute on the first day of each week. • Monthly report is generated at the 5th minute oN the first day of each month. Report does not generate any data if no data is generated within the specific time interval. For example, if you select the **Last 365 Days** option, that uses monthly data. If Cisco DNA Center runs for only few days, the generated report does not contain any data. • The Cisco DNA Center platform support is extended for the filter validation to support the reports at higher scale. You must enable the filter validation to successfully generate the report. • If the filter validation is successful, the **Schedule Report** window redirects you to the next page. • If the filter validation fails, an error message appears at the top of **Schedule Report** window. • The Cisco DNA Center platform support is extended for the following enhancements in the **Client Trend** report:

Feature	Description
	- The **Client Trend** report is renamed as **Client Trend - Count and Traffic** report. - The **Select Report Template** preview page is updated with the latest **Client Trend - Count and Traffic** report sample. - In the **Setup Report Scope** page, the **Connection Type** filter is added and allows you to choose **Wired**, **Wireless**, or **All** (wired or wireless) clients. - In the **Schedule Report** page, the last 30 days and 365 days options are added under the **Time Range** area that allows you to generate a report from last 30 and 365 days along with the data interval is used for the corresponding time range. The data interval is added in each time range option. **Note** The Cisco DNA Center platform allows you to choose 1 week data interval when you choose the time range from 90 days to 180 days. - In the **Time Range** area, the **Custom** radio button allows you to choose the date and time interval up to 365 days to generate a custom report. - Weekly aggregation support that allows you to the aggregate daily note and generate weekly note. - Monthly aggregation support that allows you to aggregate daily note and generate monthly note on the first day of each month. For more information about creating reports, see the *Cisco DNA Center Platform User Guide*.

New and Changed Features in Cisco DNA Automation

Feature	Description
Cisco AI Endpoint Analytics Enhancements	Cisco AI Endpoint Analytics assigns Trust Scores to endpoints based on the number and frequency with which the following anomalies are detected for an endpoint: - AI Spoofing Detection - Changes in Profile Labels - NAT Mode Detection - Concurrent MAC Addresses

Feature	Description
Detect Endpoints that Use Random MAC Addresses	With Cisco AI Endpoint Analytics, you can detect endpoints that use random MAC addresses. Cisco AI Endpoint Analytics enables you to handle the issue of random and changing MAC addresses by receiving from Cisco ISE a unique endpoint identifier called the DUID (also known as the GUID in Cisco ISE). Cisco AI Endpoint Analytics then uses the DUID as the identifier for an endpoint, instead of its MAC address.
Overlapping IP Address Configuration in FlexConnect Deployments	You can configure overlapping IP address in FlexConnect deployments on Cisco Catalyst 9800 Series Wireless Controller software version 17.4.x or later and Embedded Wireless Controller on Catalyst Access Point. The overlapping IP address pools feature allows you to configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP address in different address spaces.
Purge Endpoints After Inactivity	You can define an Endpoint Purge Policy to remove from your network the endpoints that have been inactive for a defined time. You can define the period of inactivity after which an endpoint must be removed. You can also customize a purge policy to act on a particular set of endpoints based on a profiling attribute.
Support for C-ANT9104 Antenna	The C-ANT9104 antenna supports the following configurations: • You can configure the beam steering for the antennae under **Design** > **Network Settings** > **Wireless** > **Antenna Radio Profile**. The beam steering configuration is available for antenna combinations ABCD (left antennae) and EFGH (right antennae). • You can configure radio antenna profiles on the antenna slots while provisioning the AP on the **Provision Devices** window. This configuration is supported on Cisco Catalyst 9130AXE Unified Access Points with Cisco Catalyst 9800 Series Wireless Controller software release 17.6 or later.
Support for Dual 4x4 Radios	In earlier releases, Cisco DNA Center leaves all Cisco Catalyst 9130 slot 2 radios in the default (disabled) mode. In this release, Cisco DNA Center enables slot 2. Enabling slot 2 in a Cisco Catalyst 9130 configures dual 5-GHz mode (dual 4x4 radios). Disabling slot 2 configures single 5-GHz mode (one 8x8 radio).
Support for New Outdoor APs	This release introduces support for the following outdoor APs: • Cisco Catalyst 9124AXE Series Unified Access Points • Cisco Embedded Wireless Controller on Catalyst 9124AX Access Points
Wireless Maps Support for a New Stadium (Large Public Venue) Antenna	Cisco DNA Center supports the C-ANT9104 antenna, which integrates with the Cisco Catalyst 9130AXE Unified Access Point to provide dual 5-GHz 4x4 radios with high gain, steerable, and switchable functions. The beam steering configuration is available for antenna combinations ABCD (the left antennae) and EFGH (the right antennae). The antenna pattern names are set based on the selected beam; you can visualize the heatmaps on Cisco DNA Center floor maps.

Feature	Description
Wireless Maps Support for New APs	This release introduces wireless maps support for the following APs: • Cisco Catalyst 9124AXE Series Unified Access Points • Cisco Embedded Wireless Controller on Catalyst 9124AX Access Points
WLAN Security Type Override	The sites, buildings, and floors inherit settings from the Global hierarchy. You can now override the level of security at the site, building, or floor level.

New and Changed Features in Cisco Software-Defined Access

Table 7: New and Changed Software Features in Cisco Software-Defined Access

Feature	Description
Configure AAA Server	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 an 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 controllers and AireOS wireless controllers in Cisco DNA Center 2.2.1.x. The configure AAA feature is supported on embedded wireless controllers on Catalyst 9000 Series Switches in Cisco DNA Center 2.2.3.x.
Dynamic Default Border	LISP Pub/Sub configuration automatically enables Dynamic Default Border. With Dynamic Default Border, an external border node tracks the presence of the default route in its routing tables and registers itself with the control plane node as a default border node. A fabric edge node or an internal border node sends its unknown destination traffic to the default border by dynamically learning about the presence and absence of the default route on the default border. If the external border node fails, loses its upstream connectivity, or otherwise no longer has the default route, its registration as a default border is withdrawn from the control plane node. This provides for an immediate convergence so that other fabric nodes cease sending traffic to that external border, thus minimizing the traffic loss. In a multisite deployment where multiple fabric sites are connected to an SD-Access transit, border nodes register themselves as default border nodes with the transit control plane node as well. Fabric sites without direct internet access learn about the presence or absence of the default route available through other fabric sites which provides the Remote Internet functionality. Fabric sites with direct internet access learn about the presence or absence of the default route available through other fabric sites providing the Backup Internet functionality.

Feature	Description
Locator/ID Separation Protocol Publish/Subscribe	Locator/ID Separation Protocol Publish/Subscribe (LISP Pub/Sub) provides native LISP support to handle the communication between the border nodes and the control plane nodes in an SD-Access fabric. LISP Pub/Sub uses the publication-subscription architecture in the control plane communications between the devices. The LISP mappings from the Mapping System are published to interested subscribers. In a fabric site with multiple borders nodes, each border node subscribes to the LISP mapping information from the control plane node. The control plane node publishes any change in the map-cache entry. With this mechanism, the mapping changes are notified faster, and it brings down the border convergence time (see *Dynamic Default Border*). A fabric edge node dynamically learns about the presence or absence of the default route on the external border. In a multisite deployment where multiple fabric sites are connected to an SD-Access transit, the transit site control plane node tracks the default route across all connected fabric sites. The border nodes of a fabric site are notified of the site-registration changes on each of the sites that they are connected to. **Note** Cisco DNA Center continues to support peering with external BGP network when LISP Pub/Sub is configured. The LISP and BGP sessions are isolated from each other, and they do not interact nor mutually redistribute. Here are some design considerations for a fabric using a LISP Pub/Sub control plane: • In Cisco DNA Center 2.2.3, LISP Pub/Sub is supported only on newly created fabric sites. Existing fabric sites can't be upgraded to a LISP Pub/Sub control plane. • Cisco IOS XE 17.6.1 is the minimum software version required to support LISP Pub/Sub. All fabric devices with the site (except Extended Nodes and Policy Extended Nodes) must be operating on Cisco IOS XE 17.6.1 and later releases. • A LISP Pub/Sub architecture cannot coexist with a LISP/BGP architecture in the same fabric site. • A fabric using a LISP/BGP control plane and a fabric using a LISP Pub/Sub control plane can’t interoperate through the same SD-Access Transit. • A virtual network anchored to a multisite remote border with a LISP Pub/Sub control plane can only be extended to fabric sites that use a LISP Pub/Sub control plane. A virtual network anchored to a multisite remote border with a LISP/BGP control plane can only be extended to fabric sites that use a LISP/BGP control plane.

Feature	Description
SD-Access Fabric UX 2.0: Automation	The GUI experience is enhanced, which integrates simplicity, flexibility, and a rich, intuitive context. Phase 1 of SD-Access UX 2.0 restructures, updates, and enhances workflows, views, and day-N management tasks for VNs. The new workflows focus on: • Gateway creation • Layer 2 VN creation • Layer 3 VN creation • Fabric site and fabric zone creation You can use the GUI toggle on the Cisco DNA Center menu bar to switch between the old GUI and the new one.
SD-Access Fabric Zones	You can create smaller fabric zones within a fabric site. A fabric zone inherits all the properties of its parent site while helping you manage the network with a lesser number of segments and devices. A fabric zone falls back on its parent site for the control plane and border. But a fabric zone can have its own edge devices and extended node devices that are independent of the parent site. Zoning is useful in networks which require large scale deployment of edge and extended nodes in a single fabric site. Here are some design considerations for a fabric zone: • In a new deployment, when a fabric zone is created, all properties of the parent fabric site (like IP pools, virtual networks, authentication profiles, multicast settings, and so on) are inherited by the fabric zone. • You can assign the required number of IP pools and virtual networks to a fabric zone. Ensure that these segments are already assigned to the parent site before assigning them to the fabric zone. • You cannot add a control plane node, a border node, or a fabric wireless controller to a fabric zone. These nodes can only be present in the parent site. You can only add edge nodes and extended nodes to a fabric zone. • If you upgrade to Cisco DNA Center 2.2.3 from an earlier release, you can create fabric zones on the existing fabric sites. All the edge nodes and extended nodes of the site are automatically added to a fabric zone when it's created.

Table 8: New Hardware Features in Cisco Software-Defined Access

Device Role	Product Family	Part Number	Description
Fabric Access Point	Cisco Catalyst 9124AXI Series Unified Access Points	C9124AXI-B	A Cisco Catalyst 9124AXI Series Unified Access Point supports Wi-Fi 6 standard and multigigabit Ethernet, among other features. It's supported in Cisco IOS XE 17.5.1 and later releases.

New and Changed Features in Interactive Help

Table 9: New and Changed Features in Interactive Help, Release 2.2.3.5

Feature	Description
Additional Interactive Help Walkthroughs	Added the following walkthroughs: • Edit a Fabric Zone • Add Layer 3 Virtual Network to Fabric Site • Add Layer 3 Virtual Network to Fabric Zone • Add Anycast Gateway to Fabric Zone • Add Layer 2 Virtual Network to Fabric Zone • Edit Layer 2 Virtual Network Properties • Edit Anycast Gateway Properties
Deprecated Walkthroughs	The following walkthrough is deprecated: Create a Fabric

Table 10: New and Changed Features in Interactive Help, Release 2.2.3

Feature	Description
Categorized Menu Items	Added categorized groups to organize menu items. Categorization is based on functional area.
Customize the Interactive Help Widget Location	You can now move the Interactive Help widget to 11 different locations besides the default location at the bottom right of the window. The possible locations are at the top, bottom, left, and right borders of the window. Simply, drag and drop the Interactive Help widget to move it. The possible locations are indicated by a green dotted-line rectangle. There is a caveat for this feature. For four locations (top left, left center, top right, and right center), when you open the widget, a part of the menu is cut off the screen.
More Walkthroughs	Added the following walkthroughs: • Create a 3D Floor Map (CAD File) • View 3D Wireless Maps • Run a Compliance Check on a Device • View the Compliance Summary of a Device • Add Scalable Groups to a Site's Virtual Network • Configure System Health Notifications

Deprecated Features

Intersite Layer 2 Handoff in a fabric site is deprecated in Cisco DNA Center 2.2.3. If you upgrade from an earlier release in which Intersite Layer 2 Handoff was configured, Cisco DNA Center 2.2.3 allows you to delete the existing Intersite Layer 2 hand off configuration.

The Common Pool attribute of a virtual network has also been deprecated in Cisco DNA Center 2.2.3. Upgrading from an earlier release, where a common pool was configured, has no effect on the virtual network in Cisco DNA Center 2.2.3.

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 Compatibility Matrix

For information about devices, such as routers, switches, wireless APs, Cisco Enterprise NFV Infrastructure Software (NFVIS) platforms, and software releases supported by each application in Cisco DNA Center, see the *Cisco DNA Center Compatibility Matrix*.

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.

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) and 4.1(2g) 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

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 an existing network firewall, see "Required Internet URLs and Fully Qualified Domain Names" in the "Plan the Deployment" chapter of the *Cisco DNA Center Installation Guide*.

About Telemetry Collection

Telemetry data is collected by default in Cisco DNA Center 2.1.x and later, but you can opt out of some data collection. The data collection is designed to help the development of product features and address any operational issues, providing greater value and return on investment (ROI). Cisco collects the following categories of data: Cisco.com ID, System, Feature Usage, Network Device Inventory, and License Entitlement. See the *Cisco DNA Center Data Sheet* for a more expansive list of data that we collect. To opt out of some of data collection, contact your Cisco account representative and the Cisco TAC.

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

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.

Support for Cisco Connected Mobile Experiences

Cisco DNA Center supports Cisco Connected Mobile Experiences (CMX) Release 10.6.2 or later. Earlier versions of Cisco CMX are not supported.

⚠

Caution 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 Catalyst IR 1800 Series with software release Cisco IOS XE 17.5.1 and later
  - Cisco ISR 1100 Series with software release Cisco IOS XE 16.6.2
  - Cisco ISR 4000 Series with software release Cisco IOS XE 3.16.1 or later, except for the ISR 4221, which requires release Cisco IOS XE 16.4.1 or later
  - Cisco ASR 1000 Series (except for the ASR 1002-x) with software release Cisco IOS XE 16.6.1
- Cisco switches:
  - Cisco Catalyst 3850 Series with software release Cisco IOS XE 3.6.3E or Cisco IOS XE 16.1.2E or later
  - Cisco Catalyst 3650 Series and 4500 Series with Supervisor 7-E/8-E, with software release 3.6.3E, Cisco IOS XE 3.7.3E, or Cisco IOS XE 16.1.2E or later
  - Cisco Catalyst 4500 Series with Supervisor 8L-E with software release Cisco IOS XE 3.8.1E or later
  - Cisco Catalyst 4500 Series with Supervisor 9-E with software release Cisco IOS XE 3.10.0E or later
  - Cisco Catalyst 9300 Series with software release Cisco IOS XE 16.6.1 or later

- Cisco Catalyst 9400 Series with software release Cisco IOS XE 16.6.1 or later
- Cisco Catalyst 9500 Series with software release Cisco IOS XE 16.6.1 or later
- Cisco Catalyst IE3300 Series with software release Cisco IOS XE 16.10.1e or later
- Cisco Catalyst IE3400 Series with software release Cisco IOS XE 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, and Cisco ASR1002-HX
- Cisco switches: Cisco Catalyst 4500 Series with Supervisor 8-E/8L-E/9-E, and 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 Cisco IOS XE 16.3.2 or later
  - Cisco ISR 4000 Series with software release Cisco IOS XE 16.3.2 or later
- Cisco switches:
  - Cisco Catalyst 3650 Series and 3850 Series with software release Cisco IOS XE 16.6.1 or later
  - Cisco Catalyst 9300 Series with software release Cisco IOS XE 16.6.1 or later
  - Cisco Catalyst 9400 Series with software release Cisco IOS XE 16.6.1 or later
  - Cisco Catalyst 9500 Series with software release Cisco IOS XE 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 Cisco IOS XE 16.6.2 or later
- Cisco Catalyst IR 1800 Series

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 Network Address Translation (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

Open Bugs

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

Bug Identifier	Headline

CSCvy24763	After successfully starting a report in Cisco DNA Center, the report may display the following error:
	`Sorry, data collection failed - this report failed because the operation timed out or the server not responding.`
	`Please try again later or create a new report.`

CSCvy30606	A wireless LAN controller stops sending telemetry data to Cisco DNA Center, so Assurance stops plotting health. This problem occurs exactly one year from the date that the wireless LAN controller is added to the site in Cisco DNA Center. The following syslog message confirms the problem: `Aug 18 02:19:05.640: %PKI-3-KEY_CMP_MISMATCH: Key in the certificate and stored key does not match for Trustpoint-sdn-network-infra-iwan.` Do the following to reconfigure the certificate: **1.** In the Cisco DNA Center GUI, choose **Provision** > **Network Devices** > **Inventory**. **2.** Choose the device and from the **Actions** drop-down list, choose **Telemetry** > **Update Telemetry Settings**. **3.** In the Update Telemetry Settings window, do the following: **a.** Check the **Force Configuration Push** check box to push the configuration changes to the device. **b.** Click **Next**. **c.** Click the **Now** radio button. **d.** Click **Apply**.
CSCvy36848	The System Health monitoring of Cisco IMC checks only DN2 parameters. Errors are seen if the Cisco DNA Center is a DN1 hardware appliance.
CSCvy49033	During the upgrade of a three-node cluster, the precheck may not determine the status of a node being down.
CSCvy61817	During sensor provisioning, wireless LAN controller devices are not provisioned with the CiscoSensorProvisioning SSID.

Bug Identifier	Headline
CSCvy61888	For wireless-enabled Cisco Catalyst switches and Catalyst 9800 devices, when there is any update on the Cisco ISE ACL rule entries (such as DHCP, DNS, or SSID ISE PSNs), Cisco DNA Center replaces the ise-acl "DNAC_ACL_WEBAUTH_REDIRECT" completely on the controller, instead of updating only the changed rule-acl entries. This problem is due to a NETCONF framework limitation, where the NETCONF RPC must contain the final configuration to be present on the device. If the NETCONF RPC for DNAC_ACL_WEBAUTH_REDIRECT contains only the updated rule-acl entries, the device is added with only new rule-acl entries under DNAC_ACL_WEBAUTH_REDIRECT. This problem occurs under the following conditions: **1.** Device types: Catalyst 9300, 9400, 9500 with wireless enabled and Catalyst 9800. **2.** Controller provisioned with guest Cisco ISE SSIDs. **3.** Modify the SSID ISE Policy Service Nodes (PSNs) on the Cisco DNA Center wireless window, or modify the DHCP/DNS address on the Cisco DNA Center Network Settings window that is part of the ise-acl "DNAC_ACL_WEBAUTH_REDIRECT." **4.** Reprovision the controller.
CSCvy62293	After APs in Local mode change to Bridge mode, they can no longer join the Cisco Catalyst 9800 Series Wireless Controller.
CSCvy62309	During the upgrade, the precheck does not validate the status of disaster recovery (DR) being in the PAUSED or NOT PAUSED state. This occurs because there is no specific validation for this part of the upgrade.
CSCvy63072	After a disaster recovery (DR) failover, when you perform a trust re-establishment operation within 15 to 20 minutes, Cisco ISE cannot reconnect the Reader role to Cisco DNA Center. This problem applies only to Cisco DNA Center being brought back to a Reader role.
CSCvy80243	The AI Analytics package does not currently support IPv6, which implies that you cannot onboard to the AI Analytics cloud.
CSCvy80587	When an overall system upgrade is triggered and the upgrade results in a failure, no notification is sent.

Bug Identifier	Headline
CSCvy81930	If an SSID is moved to a different wireless policy profile via the wireless controller GUI and has already been learned by Cisco DNA Center, the Device Config Learn workflow does not recognize that the SSID is attached to a different profile, and ignores the SSID. The behavior, which is expected, is as follows: **1.** *SSID1* is mapped to *PolicyProfileX* and learning is triggered, which creates *SSID1* in Cisco DNA Center. **2.** Modify the SSID-to-profile mapping on the device so that *SSID1* is mapped to *PolicyProfileY*. **3.** Resynchronize the device, and trigger a relearn. **4.** If the contents of *PolicyProfileX* and *PolicyProfileY* are the same, Cisco DNA Center marks *SSID1* as a duplicate, not as a new SSID. **5.** If the contents of *PolicyProfileX* and *PolicyProfileY* are different, Cisco DNA Center displays the SSID under CONFLICT. You can then choose either the device configuration or the Cisco DNA Center configuration for the SSID.

CSCvy82221	The IPAM Manager (Infoblox) is shown as **Unavailable** in the System 360 window. The System Health window shows the following error:
	`IPAM connection to Cisco DNA Center offline.`
	In addition, when you edit an existing IPAM integration or add a new IPAM Manager, the following error is shown:
	`NCIP10283: The remote server presented a certificate with an incorrect CN of the owner.`

CSCvy87482	Disaster Recovery (DR) operations performance timing increases during the DR rejoin task.
CSCvy89609	When a restore operation performed on a Cisco DNA Center system gets canceled while in progress, you might not receive the "Restore initiated" and "Restore failed" notifications.
CSCvy94699	A fabric zone that doesn't have or doesn't inherit the Fabric Site Auth Mode settings is not pushed to edge nodes.
CSCvz05135	For an endpoint with only one trust score value, if you click **Reset** for any individual section, the check box to keep or remove the ANC policy is not displayed. (The check box is displayed for a global reset.)
CSCvz06121	The Flex IP overlap model config adds an extra flex profile for each floor.

Bug Identifier	Headline
CSCvz08017	Several system monitoring events, such as "SYSTEM_SCALE_DEVICES_WIRED" and SYSTEM_SCALE_PHYSICAL_PORTS," are not shown in the System Health window.
CSCvz10683	The Fabric Overall Health score is missing for some edge and extension nodes.
CSCvz14650	For a sensor RF assessment, the data rate test case fails for a sensor image that reports a data rate of 6 Mbps or lower. This problem causes overall issues with sensor test results. This behavior is expected based on how the sensor and the AP choose data rates, and based on how Cisco DNA Center classifies data rate failures. The sensor and the AP use VHT rates (MCS0 to MCS9). When the sensor performs tests, it uses data rates higher than MCS6. However, when there's network traffic or the RF environment is busy, the sensor and the AP use MCS0 (6 Mbps). When the sensor reports data rates of 6 Mbps to Cisco DNA Center, Cisco DNA Center marks the test as a failure, because Cisco DNA Center has a failure threshold of 6 Mbps.
CSCvz17135	After an Elasticsearch restore completes, NetFlow records are not processed.
CSCvz43990	SWIM operations or any other scheduled operations might fail, indicating that the request to the back-end service timed out.
CSCvz59350	Switch 360 window doesn't show the MAC address for a switch added with an FQDN address.
CSCwa19027	Cisco DNA Center pushes the command "automate-tester username dummy ignore-acct-port probe-on" as part of its standard Cisco SD-Access configuration. Cisco DNA Center pushes the "automate-tester" configuration so that the device sends periodic RADIUS requests to the RADIUS server. The server is marked as Up if the device receives a response; the server is marked as Down if the device doesn't receive a response. It doesn't matter whether the user exists in Cisco ISE, because the device merely looks for a response from the RADIUS server, regardless of whether authentication succeeds or fails. If the corresponding Cisco ISE authentication policy uses the "Drop" action instead of the default "Access-Reject" action when the user does not exist, the AAA server might get marked as Dead when Cisco ISE drops the packet (because the dummy user does not exist on Cisco ISE). This in turn could affect CTS operation, and the following log is generated every minute: `%CTS-3-AAA_NO_RADIUS_SERVER: No RADIUS servers available for CTS AAA request for CTS env-data SM`

Bug Identifier	Headline

CSCwa30225	When you try to recover the Cisco DNA Center maglev CLI password, after selecting the Recovery mode image from the GRUB menu, the boot up hangs and never gets to the step where it prompts you to enter Rescue mode.
	This problem occurs in Cisco DNA Center 2.2.3.x when you try to recover the password as described in the Cisco DNA Center Maglev CLI Password Recovery document.
	To work around this problem, do the following:
	1. Get into Recovery mode as described in the Cisco DNA Center Maglev CLI Password Recovery.
	2. Enter the following command to SSH into the Cisco Integrated Management Controller (IMC):
	`ssh admin@<cimc>`
	3. When your KVM console hangs in Recovery mode, enter the following command to connect to the host:
	`connect host`
	4. After you connect to the host, you are prompted to change the password.

CSCwa56438	The device count is shown at the top of the Plug and Play window, but there is no device list. This problem occurs when the sort is on the Index column, which is the default option for the Plug and Play device display in this release. To work around this problem, simply click any column other than the Index column. The devices are then shown in the device list.
CSCwa86877	In an IPv6 environment, a Cisco DNA Center upgrade from 2.2.2.8 to 2.2.3.4 fails because the network-programmer service fails to start up. To work around this problem, manually upgrade the IPv6 applications from the CLI to the expected release before upgrading the network-visibility package.
CSCwa88686	Cisco DNA Center 2.2.2.x and 2.2.3.x: KGV validation failure.
CSCwa88971	The services that startup post HA node reboot were impacted as they were unable to connect to RMQ for creating some queues.
CSCwa99062	After upgrading to Cisco DNA Center 2.2.3.4, glusterfs-hostagent goes to "OOMKilled" state.

Bug Identifier	Headline
CSCwb18801	

Bug Identifier	Headline

	If you use the special character '<' in the preshared key SSID for wireless controllers, and then configure and provision the same SSID in Cisco DNA Center, Cisco DNA Center flags the '<' character with the following error:
	`< is not allowed for security reasons.`
	For security reasons, Cisco DNA Center restricts the usage of certain special characters in various API payloads. Cisco DNA Center blocks the following characters:
	`<`
	`%3C`
	`&lt`
	`&lt;`
	`&LT`
	`&LT;`
	`&#60`
	`&#060`
	`&#0060`
	`&#00060`
	`&#000060`
	`&#0000060`
	`&#60;`
	`&#060;`
	`&#0060;`
	`&#00060;`
	`&#000060;`
	`&#0000060;`
	`&#x3c`
	`&#x03c`
	`&#x003c`
	`&#x0003c`
	`&#x00003c`
	`&#x000003c`
	`&#x3c;`
	`&#x03c;`
	`&#x003c;`
	`&#x0003c;`
	`&#x00003c;`
	`&#x000003c;`
	`&#X3c`
	`&#X03c`
	`&#X003c`
	`&#X0003c`
	`&#X00003c`
	`&#X000003c`
	`&#X3c;`
	`&#X03c;`
	`&#X003c;`
	`&#X0003c;`
	`&#X00003c;`
	`&#X000003c;`
	`&#x3C`
	`&#x03C`
	`&#x003C`
	`&#x0003C`
	`&#x00003C`
	`&#x000003C`
	`&#x3C;`
	`&#x03C;`
	`&#x003C;`

Bug Identifier	Headline
	&#x0003C; &#x00003C; &#x000003C; &#X3C &#X03C &#X003C &#X0003C &#X00003C &#X000003C &#X3C; &#X03C; &#X003C; &#X0003C; &#X00003C; &#X000003C; \x3c \x3C \u003c \u003C
CSCwb28540	Cisco DNA Center 2.2.2.8: A tag mismatch is seen between the primary and secondary controllers.
CSCwb78437	When you try to configure ServiceNow for the first time, Basic ITSM (ServiceNow) CMDB Sync fails to initiate RestClient processing.
CSCwb91384	In the Cisco DNA Center **Schedule Report** page, custom time range fields (From/To) may not accept some values when you schedule a report using a custom time range with the PM option in non-English mode UI.
CSCwb96420	Cisco DNA Center formats Syslog events with the IP address of the destination configured under the Destinations menu, which causes the Syslog messages to be originated from QRadar and Splunk instead of from Cisco DNA Center.
CSCwc09007	When you upgrade from Cisco DNA Center 2.2.3.4 or earlier to 2.2.3.5 or later, the **System** > **System Health** > **Validation Tool** shows the status of a validation run executed before the upgrade as Partial Success, even when there are validations with a status of Critical or Warning. This problem occurs because the status of a validation run from 2.2.3.4 or earlier shows Partial Success if at least one of the validations is Success or Info. The status of a validation run from 2.2.3.5 and later shows Critical/Warning if at least one validation has a status of Critical/Warning. Old validation runs (executed before the Cisco DNA Center upgrade) continue to show the validation run status as before.

Bug Identifier	Headline
CSCwc09546	When you try to integrate Cisco DNA Center 2.2.3.4 with Infloblox 8.5.0 as the IPAM manager, the integration fails with the following error: `NCIP10269: IPAM external sync failed: NCIP10264: Non-empty Cisco DNA Center parent pool x.x.x.x/8 exists in external ipam` In this scenario, IP pool x.x.x.x/8 is being used on Cisco DNA Center for fabric and on the IPAM server for different servers/clients. The integration fails because duplicate IP pools are in use for the Inflobox and IPAM integration.
CSCwe27538	LLDP packets aren't forwarded to clients on Layer 2 flooding-enabled VLAN ports.
CSCwe28523	In a Cisco DNA Center disaster recovery setup, the MongoDB replication may fail with a conflict error. The log from the dr-mongodb-replicator service displays an error similar to the following: `[23:22:44 UTC 2023/02/05] [EROR] (mongoshake/executor.(*BulkWriter).doUpdate:349) detail error info with index[0] msg[Updating the path 'lastProbeCollectionTimeStamp' would create a conflict at 'lastProbeCollectionTimeStamp'] dup[false]` Other data (such as wireless maps and SWIM images) is missing after the failover.

Resolved Bugs

Cisco DNA Center 2.2.3.7

The following table lists the resolved bugs in Cisco DNA Center, Release 2.2.3.7.

Bug Identifier	Headline
CSCvy30961	Cisco DNA Center - Smart Licensing "Error in loading data".
CSCwb02969	After provisioning a switch stack (9500) and a fabric configuration, the switch displays the following error message: "Managed Internal error".
CSCwb28540	[CFD]: Cisco DNA 2.2.2.8 tag mismatch between the primary and the secondary controller.
CSCwb90766	Missing 'map-cache ::/0 map-request' under service-ipv6.
CSCwb93305	AP refresh workflow fails: "AP already part of another AP refresh task 'null'".
CSCwc23153	Cisco DNA Center is trying to provision IOx interface.
CSCwc39642	Cisco DNA Center [2.3.x.x] Event Notification using Webex, REST, and email stop working after upgrade.

Bug Identifier	Headline
CSCwc53078	Connection between config archive and broker agent service is reset, and as a result, drift is not working.
CSCwc53593	Static port assignment failure - NCSO20013: Provisioning failed due to invalid request.
CSCwc59647	Cisco DNA Center - VM: Stale entries for RD remains in DB while adding back VN to Fabric.
CSCwc64081	Incorrect TLD length check for ISE FQDN.
CSCwc78766	Removing an IP address segment from a fabric site causes the site to report an error.
CSCwc79851	Device shows not ready for ThousandEyes integration in Cisco DNA Center.
CSCwc86109	Filesystem is showing 100% utilization; found Postgres to be over 230GB in size.
CSCwd00896	The APGroup config is removed in implicit provisioning, resulting in a wireless outage while resetting AAA inheritance.
CSCwd02734	Error when adding IP Pool to fabric zone - NCSP11108: Error occurred while processing the request.
CSCwd09391	Cisco DNA Center orchestrated app hosting gets disabled on the AP when the primary WLC is changed.
CSCwd24258	Generic Provisioning Error: NCS010011: Error in generating CFS due to internal error.
CSCwd25750	Scale: Under scale kafka pod not able to handle data and slows down with gaps in Assurance.
CSCwd32998	Fabric host onboarding provisioning failure.
CSCwd40306	Cisco DNA sends SNMP trap payload field snmpTrapAddress with the external SNMP collector IP.
CSCwd46164	SWIM upgrade of 3850 switch stack may only allow active switch to recover after reboot.
CSCwd48297	If at least one flex-SSID has been configured, it is not possible to create a non-flex APGroup.
CSCwd48939	Add WLC through API call failed when the control plane in fabric site is configured with PubSub.
CSCwd53101	Cisco DNA Center 2.3.3.5: WLC provisioning fails with NCSP11001 error.
CSCwd55811	In the **Network Hierarchy** page, the filter to add the sensor on the map floor is not working.
CSCwd59216	Prov 9800 fail with NCSP11108: Error occurred while processing the request DIV:I WirelessGrouping.
CSCwd62967	Cisco DNA Center Inventory telemetry - Compute resources running out on Cloud side.
CSCwd66051	Cisco DNA Ctr shows IOS telemetry subscription as successful, irrespective of device subscription status.
CSCwd75024	Functional [2.3.3.5]: WLC provision failed due for "Device Controllability and Telemetry".
CSCwd82722	NCSP11108: ERROR: Duplicate key value violates unique constraint "wlan_bk" (DIV) - Fiab eWLC.
CSCwd84123	SDA: Enabling Fabric Pool features provision failure with error "%No policy information".
CSCwd86638	Addition of node on 2.3.3.5 fails on upgraded cluster.
CSCwd86714	Sticky-scheduler service is down after upgrade to 2.3.3.5.

Bug Identifier	Headline
CSCwd89482	SWIM internal calls going to proxy-issues with Distribution / loading Image update WF / DNAC CA push.
CSCwd90641	[CFD]: Cisco DNA Center ERROR: Duplicate key value violates unique constraint "wirelessgrouping_bk".
CSCwd91440	Functional: Alpha Ghost 70586 - 9800 ewlc provisioning fails with error NCSP11108 after intra upgrade.
CSCwe04247	Error when applying critical fix for "Closed Authentication Mode Template Update".
CSCwe10186	Wrong fabric zone is being assigned for multicast pools when bulk fabric zones are created.
CSCwe15942	Images not displayed under Image Families.
CSCwe17325	Cat3850/ 16.12.x / Base image getting deleted before SMU is copied to the switch.
CSCwe19750	Cisco DNA Center: AI RF Profile pushing 6GHz profile with non-Europe compliant channels.

Cisco DNA Center 2.2.3.6

The following table lists the resolved bugs in Cisco DNA Center, Release 2.2.3.6.

Bug Identifier	Headline
CSCvw18193	The size of the PAC key increases on every migration.
CSCvx24461	After editing an SSID previously configured in Cisco DNA Center, provisioning the Cisco Wireless Controller with the new information may fail with the following NETCONF error: `Validation failed Process DBAL response failed.`
CSCvz86051	Unable to see any devices in the Thousand Eyes Cisco DNA Center app hosting workflow window. The Manage tab shows already installed devices, but no devices are shown in the Install tab.
CSCwa21091	Cisco DNA Center may fail to provision a Cisco Catalyst 9800 Series Wireless Controller. The following error is displayed: `NCSP10001: User intent validation failed.`
CSCwa29973	CTS credentials of the device are not in synch with the Cisco ISE NAD entry.
CSCwa46093	Cisco DNA Center system certificate accepts certificates that fail the domain validator.
CSCwa59438	The Meraki dashboard and Firepower Management Center (FMC) show an internal error.
CSCwa61489	Vulnerabilities for Cisco DNA Center 2.2.3.4.
CSCwa88686	Download of latest KGV files fails due to a certificate change on tools.cisco.com.
CSCwa90857	Template provisioning of SNMP commands may fail due to special characters.
CSCwa95316	Vulnerabilities for Cisco DNA Center 2.2.2.8.
CSCwa97774	Cisco Wireless Controller provisioning fails because the snapshot doesn't exist for the namespace.
CSCwb04206	PnP connect cannot delete a profile that is not present in the PnP cloud.

Bug Identifier	Headline
CSCwb08617	Cisco Wireless Controller provisioning fails with the following error: `NCSP10250: Error during persistence (modify) of CFS & SerializedSnapshot - RfProfileCfs.`
CSCwb12382	Cisco Catalyst 9200 Switch application visibility is not seen in Cisco DNA Center because the tenant ID is SYS0 instead of a valid value.
CSCwb12514	Cisco DNA Center 2.2.3.3: The Application 360 window has gaps on the health chart.
CSCwb12871	When importing Ekahau project files, Cisco DNA Center may display the obstacle types and attenuation values as different from what is configured in the Ekahau project.
CSCwb13062	Cisco DNA Center 2.2.3.4: Unable to start LAN automation. The following error is displayed: `Error while reserving subnet : NCIP10288.`
CSCwb13771	A QoS custom application is categorized as "Default" business relevance by the device.
CSCwb15711	Fabric edge provisioning fails if you use a single-digit VLAN ID with SGT during pool addition in a virtual network.
CSCwb23176	Cisco 1800S sensors become unreachable and fail to auto register with Cisco DNA Center through the PnP flow.
CSCwb25760	Unable to view a virtual network on the Add Virtual Network window under fabric host onboarding.
CSCwb27102	Cisco DNA Center pushes the configuration on fabric edge ports for BPDU guard on its own even after it was manually removed.
CSCwb27511	A wireless grouping entry cannot be deleted, which causes a Cisco Wireless Controller provisioning failure.
CSCwb29208	In the Cisco DNA Center, the Scheduler for the ServiceNow Asset fails to synchronise.
CSCwb32387	Cisco DNA Center 2.2.2.8: A recovery site cannot be deregistered.
CSCwb35644	While unsubscribing Cisco DNA Center platform events, the following error is displayed: `Subscription already exists.`
CSCwb40106	Software image management (SWIM) does not show an activation task even after successful image transfer.
CSCwb42071	Switch provisioning fails with the following error: `Duplicate key value violates unique constraint "manageddcs_unique_key."`
CSCwb43650	Evaluation for Spring4Shell vulnerability (CVE-2022-22965).
CSCwb44246	A few IP address pools in the virtual network may be removed from the LISP configuration of edge switches.
CSCwb48383	An HTTP request to the webhook site is initiated from Cisco DNA Center.
CSCwb50439	Cisco DNA Center generates false DHCP issues for wireless clients connecting to an anchor cloud SSID.

Bug Identifier	Headline
CSCwb57463	Provisioning a single RF profile causes all the APs in the site to disjoin/join.
CSCwb68947	Unable to delete the multiple devices table snmpgroupversionsettings.
CSCwb73178	Cisco DNA Center 2.2.3.4: Disaster recovery failover hangs after you click the Pause button.
CSCwc01177	When you configure KPIs for APs in 5 GHz and disable KPIs for 2.4 GHz, Assurance for APs displays incorrect Overall Health metrics.

CSCwc40316	The Cisco DNA Center upgrade appears to hang at 0%. After some time, the upgrade times out with the following error:
	`System update failed during DOWNLOADED_SYSTEMUPDATER.`
	`Downloading systemUpdatePackage system-updater:1.6.711 failed.`

Cisco DNA Center 2.2.3.5

The following table lists the resolved bugs in Cisco DNA Center, Release 2.2.3.5.

Bug Identifier	Headline
CSCvz51440	The Switch 360 page shows the wrong interfaces from other devices.
CSCvz61877	Cisco DNA Center's neighbor topology map for an AP may show that the link status is down toward the connected device, when the link is actually up.
CSCwa03336	Cisco DNA Center does not push AAA method accounting for the accounting lists mentioned in the wireless profile policy.
CSCwa23879	When configuring integration of Cisco ISE with Cisco DNA Center, RADIUS is enabled by default, and the pxGrid connection to Cisco ISE is enabled. TACACS+ is not enabled by default. If you choose to enable TACACS+ and to also disable RADIUS, you must manually disable the pxGrid connection. Otherwise, the Cisco DNA Center System 360 windows shows the pxGrid state as Unavailable.
CSCwa25291	The Resume/Cancel configure access points workflow fails.
CSCwa40727	Fabric deploy sends an incorrect RADIUS authentication server command. Provisioning fails for Cisco AireOS wireless controllers.
CSCwa45898	NAC is not enabled via advanced SSID model config when provisioning two wireless controllers at the same time.
CSCwa51827	LISP key banner push fails for wireless devices in Cisco DNA Center 2.2.2.x.
CSCwa52917	A null pointer exception occurs when you try to access Show Task from the Image Repository window.
CSCwa56990	Cisco DNA Center has issues with displaying scalable groups on the Host Onboarding > Wireless SSIDs window. When you choose Assign SGT, the following message appears, and no SGTs are displayed: `No options are available`
CSCwa57728	Upgrading from Cisco DNA Center 2.1.2.7 to 2.2.2.x fails at 41%. The unit quagga service does not load.

Bug Identifier	Headline
CSCwa59366	For Cisco DNA Center 2.2.2.x, the following error occurs when running LAN automation for an already reserved pool for the site where the device is being provisioned through LAN automation: `NCND01134: Invalid IP Pool. IpPoolId xx-xx-xx is not a valid LAN IP pool for site yyy.`
CSCwa61159	In the Cisco DNA Center event notification, when you try to unsubscribe previously configured subscriptions from the event, the following error appears: `subscriptionDetails are wrongly configured [Field 'webExTeamsBotAccessToken' value is required] !`
CSCwa61993	A subnet is not released while removing L3 Handoff when external IPAM is integrated.
CSCwa68838	The spf-service-manager-service does not start after an upgrade to Cisco DNA Center 2.1.2.7.
CSCwa69002	Cisco AI Network Analytics stores large amounts of metadata in the credential manager, causing DR registration failure.
CSCwa69594	The Report Template for the AP report on Cisco DNA Center has the "Location (Max of 10 options allowed)" filter for Setup Report Scope in the AP report. The issue is that some Site Hierarchy locations are left out of the filter list. If the you enter "Text" for the search filter, some AP site locations are not listed in the Search Filter results.
CSCwa70463	An IPAM integration failure deletes intermediate CAs from the trustpool and Cisco ISE integration breaks.
CSCwa72663	The Update banner with a warning for wireless controller provisioning must show success before attempting a LISP key change.
CSCwa73670	SWIM_API: NCSW90008: Unable to reach Cisco.com due to an internal error (GetEULAForm).
CSCwa73823	The Assurance Client Health window does not load when Client Data Rate dashlets are deleted.
CSCwa77904	Wireless controller provisioning fails with an NCSP10246 internal error while attempting to transform.
CSCwa78331	Multiple devices display an internal error after a Cisco DNA Center upgrade to 2.2.3.4.
CSCwa82661	Port assignment in Host Onboarding does not work correctly.
CSCwa88951	After upgrading to Cisco DNA Center 2.2.3.4, the provisioning service receives DEVICE_LINE_CARD_ADDITION events for nonfabric devices and provisions those devices automatically. The auto provisioning request message in the spf-service-manager log contains the following parameter: `context={spf.corelationdata={"DEVICE_LINE_CARD_ADDITION":true}` Auto provisioning due to a DEVICE_LINE_CARD_ADDITION event is applicable for SDA deployments to be able to automatically push dot1x security configurations to the ports added to fabric devices. However, auto provisioning is not applicable for non-SDA deployment use cases.
CSCwa90595	Wireless controller provisioning fails due to an invalid $apMac configuration element.

Bug Identifier	Headline

CSCwb10620	When you try to run any inventory report under **Reports** > **Reports Templates** > **Inventory Reports**, the report fails intermittently with the following error:
	`Sorry, data collection failed - this report failed because the operation timed out or server not responding.`
	`Please try again later or create a new report.`

Cisco DNA Center 2.2.3.4

The following table lists the resolved bugs in Cisco DNA Center, Release 2.2.3.4.

Bug Identifier	Headline
CSCvw99479	The pipelineadmin service goes down and fails to restart after high availability on a three-node cluster.
CSCvx24973	When you run a full inventory report, the Cisco DNA Center 2.2.2.x build may fail to generate the report for CSV and PDF with a timeout issue.
CSCvx52786	Cisco DNA Center may not display an IP address pool or subnet when a user tries to create a segment, citing the errors, "NCIP10071: pool name can contain only alphanumeric characters, underscores and hyphens" and "NCIP10288: There was a failure in the ipam-service."
CSCvz11143	When you upgrade to Cisco DNA Center 2.2.3.x, all the existing generated reports show **0B** report size in the report GUI.
CSCvz11253	A system upgrade from Cisco DNA Center 2.2.2.x to 2.2.3.x fails with the error, "Failed to created k8s resource using file."
CSCvz24855	Fabric provisioning fails when a border device is removed.
CSCvz26522	Cisco DNA Center doesn't let you add an internal border to a fabric site when a guest border exists.
CSCvz33630	The clear port configuration succeeds from the GUI, but the configuration is still present on the device.
CSCvz36352	LAN automation doesn't release the DHCP subnet while LAN auto start fails.
CSCvz41723	Editing floor GPS markers and saving returns the error, "Error coordinates (xx, yy) of GPS marker are outside of building."
CSCvz43500	WLANs on the foreign wireless controller are disabled upon provisioning of the anchor wireless controller.
CSCvz43887	Cisco DNA Center upgrades to the desired version but the applications fail to upgrade. This results in the application upgrade failing and the device hanging at a stand still.
CSCvz48322	In the Cisco DNA Center **Event** window, the **Subject** name field in the GUI does not change for different events. When you define the **Subject** name field for an event, that defined subject name is used for all other events.
CSCvz48575	An upgrade to Cisco DNA Center removes the TACACS key to network devices from Cisco ISE.
CSCvz55757	The wrong L2 instance is pushed to the anchoring site if a different VLAN name is used.
CSCvz56988	Cisco DNA Center's Stealthwatch Security Analytics (SSA) integration should address route lookup gaps for interface selection.

Bug Identifier	Headline
CSCvz58650	While running the Smart License-Enabled workflow, usage reports are not retrieved.
CSCvz59187	The create or update floormaps API documentation does not include the payload request schema.
CSCvz59447	An empty loopbackinterface_id in the IP Address table causes a provisioning failure.
CSCvz61107	Cannot edit email parameters after the first entry in Destinations.
CSCvz62216	All WLANs are disabled when enabling application telemetry for AireOS controllers.
CSCvz62986	Allow an additional ACE in the redirect ACL and resolve all IP addresses for redirect ACLs based on URL.
CSCvz69786	The AAA configuration is removed from the wireless controller while adding a new edge node to the fabric.
CSCvz70561	While adding additional edge switches to an existing fabric, Cisco DNA Center may alter the AAA configuration of an existing wireless LAN controller from TACACS to RADIUS.
CSCvz71423	Cisco DNA Center's /dna/intent/api/v1/network-device REST API may return no more than 500 results. This impacts installations that have more than 500 managed devices.
CSCvz71424	Cisco DNA Center's GlusterFS-hostagent service may exhaust its allocated memory, causing multiple services to crash and restart.
CSCvz72857	Image import fails with the error, "File exists in Softwareimageinfo but unable to add to File Service."
CSCvz82009	Anchor controller provisioning fails.
CSCvz82017	Docker's /etc/maglev/docker-https-proxy.env gets deleted when deleting proxy settings.
CSCvz83869	Cisco DNA Center may fail to upgrade the system package due to a missing product ID (PID) for the DN1-HW-APL-U appliance in part of an upgrade hook.
CSCvz87778	Cisco DNA Center's LAN automation may fail while reserving the link subnet, citing the error, "NCIP10288: There was a failure in the ipam-service: NCIP10024: An ip pool named <UUID>_pool_dummy_31 already exists" when there are already more than 31 dummy /27 IP address pools (and more than 900 IP addresses used) from the LAN automation pool for loopbacks and L3 link configuration.
CSCvz88461	When the maps API calls Assurance APIs, the sensor API fails.
CSCvz88711	AP channel information is missing from the map view.
CSCvz89312	An interface selected from the drop-down (like GigabitEthernet0/0/0, 0/0/1) reverts to GigabitEthernet0.
CSCvz90821	Cannot enable Intelligent Capture from the AP 360 window. The wireless controller console shows APs are in Connecting state rather than in Ready state.
CSCvz98800	Cisco Aironet 1542 series APs are not listed while adding to a floor map.
CSCvz98644	Adding a segment on one new WLAN associated to one wireless controller triggers other wireless controller provisioning.

Bug Identifier	Headline
CSCvz98664	Adding and removing a fabric edge provisions wireless controllers randomly with different configurations.
CSCvz99700	Unable to delete a segment from the Host Onboarding window.
CSCwa01977	LAN automation must align to the *Cisco DNA Center Security Best Practices Guide*.
CSCwa08271	The management disaster recovery virtual IP is not reachable after a manual failover.
CSCwa16652	Manually generated reports in Cisco DNA Center result in blank pages.
CSCwa18877	Cisco DNA Center: Ekahau file import fails with the API error, "The specified group ID is null or empty."
CSCwa21212	Unable to start LAN automation due to the error, "NCND00050: An internal error occurred while processing the request."
CSCwa21789	EVENT_BASED_WIRED_WIRELESS_SYNC causes an internal error for the protocol endpoint.

CSCwa21979	Device discovery tasks remain stuck in RUNNING state for a long time, clogging up the inventory service, which in turn prevents global credentials from being displayed.
	Because the global credentials don't load, new discovery tasks cannot start. The inventory service logs contain the following error logs:
	`ERROR | covery-Pingsweep-Thread-0 | | com.cisco.nm.discovery |`
	`ERROR: [Failed to process status of ping request]. | mid=10001,`
	`MSGNAME=ERROR, ch=com.cisco.nm.discovery, sev=error`

CSCwa27606	Unable to claim a device due to a Plug and Play issue.
CSCwa39582	Unable to onboard Cisco Catalyst 3560CX running Cisco IOS 15.2(7)E4 via PnP.

CSCwa52396	CLI templates that use source binding are not able to resolve variables when provisioned on an N+1 wireless controller. An example of a template is as follows:
	`#foreach($wlanpname in $listofwlans)`
	`wlan $wlanpname['policyProfiles'] $wlanpname['wlanId'] $wlanpname['designSsid']`
	` shutdown`
	`#end`
	In the preceding example, the variable *listofwlans* is configured as follows:
	`Source = NetworkProfile`
	`Entity = SSID`
	`Attribute = wlanProfileName`
	Note that the test simulation resolves the variables correctly, but during the provisioning process of the N+1 controller, the variables do not resolve and you cannot continue with the provisioning.

Cisco DNA Center 2.2.3.3

The following table lists the resolved bugs in Cisco DNA Center, Release 2.2.3.3.

Bug Identifier	Headline
CSCvq54768	Cisco DNA Center will silently push out Identity-Based Networking Services (IBNS) 2.0 "new-style" commands to any switch that is provisioned. If there is no Cisco ISE integration to replace these commands, some port security configurations might be removed.

Bug Identifier	Headline
CSCvw80355	AAA and Cisco ISE inheritance settings are not displayed correctly between Global and sites in certain flows.
CSCvx10782	A package upgrade fails because the lispmssiteeidprefix table violates a foreign key constraint.
CSCvy69934	After a Cisco DNA Center 2.1.2.6 upgrade, Cisco DNA Center doesn't configure policy tags for modified WLANs and policies.
CSCvy77016	Reserved child pools for Layer 3 handoff are not released after a failed fabric provision.
CSCvy85887	The Cisco DNA Center Application Experience feature might attempt to configure application experience commands on an interface that isn't available, but passes through an interface that is part of a port group.
CSCvy86513	Users who have modified the interface names of the interfaces in their Cisco DNA Center appliances may encounter issues when upgrading to later versions of Cisco DNA Center that support NIC bonding. The non-default interface names cannot be bonded, and the appliances may lose connectivity.
CSCvy89652	Cisco DNA Center fails to display an ROI report.
CSCvy94920	TLS v1.2 as the minimum supported version still shows TLS v1.1 for some ports.
CSCvy98355	The Layer 3 link between the PnP agent and peer seed may not be configured while the LAN automation service is stopped.
CSCvz01073	A Cisco DNA Center system package update from 2.1.2.7 to 2.2.2.3 may fail at 49%, with the kernel-upgrade Ansible task failing to remove the older kernel image.
CSCvz07929	NetFlow table updates are too aggressive for large scale deployments.
CSCvz08578	Maglev configuration wizard complains about a conflict with the DNS address.
CSCvz10208	Cisco DNA Center may create a duplicate site tag with the default-flex-profile linked to it when an existing wireless controller is reprovisioned.
CSCvz14636	Cisco DNA Center AVC needs to restrict pushing an NBAR configuration to only access switch port.
CSCvz18219	Cisco DNA Center may fail to provision a wireless controller that had previously been removed from a fabric and inventory, citing a null pointer exception.
CSCvz18421	The NAC RADIUS configuration on the WLAN profile is lost upon wireless controller reload.
CSCvz27424	Inventory overwrites the switched virtual interface (SVI) interface description to null.
CSCvz63164	In the 3D maps view, 3D heatmaps are not displayed by default due to a missing RF calibration model entry. If no heatmap is displayed when you enter the 3D maps view, open the **KPI** section, confirm that Heatmap Type is not set to **None**, and confirm that 3D RF Model is not blank.
CSCvz76664	Under **System** > **Settings**, both the CCO ID and Device EULA acceptance are not set with fresh installations in an air gap environment.

Cisco DNA Center 2.2.3.0

The following table lists the resolved bugs in Cisco DNA Center, Release 2.2.3.0.

Bug Identifier	Headline
CSCvs50772	Cisco DNA Center's threadmanagermonitor table should be pruned periodically, to keep the size of the database from growing too large.
CSCvw37064	Cisco DNA Center may incorrectly configure ACL_WEBAUTH_REDIRECT on multiple devices at the same site.
CSCvw43696	Cisco Catalyst 9800 Series Wireless Controller inventory collection fails when the AAA authorization method length is greater than 31 characters.
CSCvw47447	Custom provisioned RF profile is allowed to be deleted.
CSCvw49445	Wireless controller provisioning is blocked due to RF profile when deleted from Design, is not cleaned from database.
CSCvw53139	Cisco DNA Center's Task page doesn't load any data.
CSCvw59092	Cisco DNA Center Pkcs12 configuration failed due to internal Errors after discovery of 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.
CSCvw62707	Updating many devices frequently could cause scheduler service restart. The updates could be multiple provisioning or updating telemetry settings.
CSCvw67480	Duplicate Flex profiles are found in a wireless controller after a Cisco DNA Center upgrade.
CSCvw72645	RBAC prevents network hierarchy maps from loading. "Error 11015" is generated.
CSCvw74679	A suboptimal closed authentication configuration is pushed when a critical VLAN/IP address pool isn't explicitly defined.
CSCvw76030	Cannot perform RMA because the field value exceeds the integer range.
CSCvw76745	Cisco Catalyst 9800 Series Wireless Controller provisioning doesn't work because FlexProfilePolicyAclConfig changes are not picked.
CSCvw95827	The default application policy configuration does not handle the IS-IS protocol correctly.
CSCvx02345	Cisco DNA Center may become unable to start a new LAN automation session, citing the error, "NCND00006: The input payload contains an invalid key."
CSCvx04343	While attempting to position APs on floor maps, Cisco DNA Center may not allow you to click on or select an AP to position it.
CSCvx04712	A fabric domain may not show in the GUI after upgrading from Cisco DNA Center 1.3.3.6 to 2.1.2.0.
CSCvx09990	Cisco DNA Center pushes additional flex profiles with an incorrect VLAN-name and VLAN-id mapping.
CSCvx10390	Application packages upgrade fails due to a constraint violation on the lispcomponent table.

Bug Identifier	Headline
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. The logs show the error, "Null value was assigned to a property of primitive type setter of com.cisco.xmp.model.foundation.connectivity.ip.IpV4Properties.directedBroadcast."
CSCvx19665	After an upgrade, the cluster interface name is shown incorrectly on the DN1-HW-APL appliance.
CSCvx21215	A Guest SSID with the Fast Transition value configured as Adaptive in an earlier release of Cisco DNA Center causes wireless controller provisioning issues in 2.1.2.5.
CSCvx21853	Cisco DNA Center discovery fails to retrieve global credentials while trying to create new task.
CSCvx22746	Cisco DNA Center's SWIM activation job may report as failed after successfully activating a new image on all the members of a stack, citing the error, "NCSW10249: Software install command execution Failed: Connection timed-out while executing the command install add file flash:cat9k_iosxe.16.09.06.SPA.bin activate commit."
CSCvx25703	An incorrect policy profile is linked with new WLANs pushed by Cisco DNA Center while provisioning.
CSCvx27169	The Cisco DNA Center Inventory Service container crashes.
CSCvx30605	An extended node device is stuck in unreachable state after renewing the IP address.
CSCvx32185	The Task web page returns an error.
CSCvx34837	After performing an existing device learn on a Cisco Catalyst 9800 Series Wireless Controller, provisioning of the same controller with SSIDs fails due to "not a valid value" in the Server Timeout and Retry count.
CSCvx41602	SLR reservation for stacked switches is stuck at the Generating Authorization code.
CSCvx43231	A wireless controller partial collection failure occurs if pmipNai is more than 32 characters.
CSCvx47878	An incorrect web auth configuration may be pushed when a PSK SSID is added. This causes a conflict in the actual configuration push to the device through Cisco DNA Center provisioning.
CSCvx47887	After a failed wireless controller provisioning attempt, Cisco DNA Center may not roll back the configuration from the wireless controller, which may cause a network outage.
CSCvx56010	Cisco SD-Access: VRF specific name-servers are removed by Cisco DNA Center.
CSCvx56258	Cisco DNA Center inventory resync results in an internal error.
CSCvx62172	Cisco DNA Center support for the AP Location field.
CSCvx62887	Cisco DNA Center doesn't configure "bandwidth remaining percentage" correctly on switches.
CSCvx64681	Can't provision an ISR Transit control plane after provisioning with a routing template.
CSCvx66928	The Cisco DNA Center postgres standby instance crashes with an error that the server forked off from that timeline.
CSCvx68948	Reconfigure device provision may not determine configuration changes for the Dot1x Auth Template.

Bug Identifier	Headline
CSCvx73110	A managed AP may not show its operational details on the Assurance Device 360 window. Additionally, clients on the wireless controller, where this AP is joined, show a blank device location.
CSCvx74221	Provisioning fails when adding a AAA server using a port number greater than 32767 to Cisco DNA Center.
CSCvx75231	After an upgrade to Cisco DNA Center 2.1.2.4 or later, the following error is displayed after a modification of IP address pools for a VN on the fabric host onboarding page. `NCWL10004: L3 Only pools are not supported. Please delete and re-create the segment.`
CSCvx76405	During an upgrade of Cisco DNA Center's application packages, the upgrade may appear to be stuck for hours at 20% with no obvious movement forward. The migration logs show a deadlock on the Postgres executionevent table.
CSCvx79755	Devices may be successfully added to Cisco DNA Center's inventory, and report being in the managed state after LAN automation. However, port information is not displayed when you click the device name in Inventory.
CSCvx86351	Device provision hangs in "In Progress" because the Cisco ISE integration is broken.
CSCvx88137	Heatmaps for the 5-Ghz band are not generated for a Cisco Catalyst 9800 Series Wireless Controller.
CSCvx88587	Image Distribution Servers won't allow a valid IP address.
CSCvx89052	When attempting to add an edge device to a fabric, Cisco DNA Center may return the error, "Provisioning failed due to invalid parameter. The interface does not exist in the device, select a valid interface."
CSCvx93717	Client Detail, Client Session, and AP Radio reports fail.
CSCvx99908	Unable to open a VN in L2 Handoff settings or click the Save button after an upgrade to Cisco DNA Center 2.1.2.6.
CSCvy00986	For Cisco Catalyst 9800 Series Wireless Controllers, the Remote Procedure Call (RPC) rfdca-removed-channel operation fails with a data missing error tag.
CSCvy06455	Nexus 7710 device provisioning may fail due to an octothorp "#" character in the login banner.
CSCvy10747	The messages in the dna.lan.common.service queue block subsequent LAN automation.
CSCvy12915	When importing an .esx file from an Ekahau project, the azimuth is always off by 90 degrees.
CSCvy16664	Device provisioning fails with a AAA update.
CSCvy19564	Cisco DNA Center's inventory service may crash when managed devices send large amounts of syslogs.
CSCvy20557	The Sensor link is missing for the 5-GHz view.
CSCvy23527	The Device 360 page takes a long time to load, or may time out due to WalkMe APIs.
CSCvy24764	Offline APs are shown as active on heatmaps.
CSCvy25460	While creating a webhook, Cisco DNA Center does not allow you to put a space in the webhook name.

Bug Identifier	Headline
CSCvy26789	When attempting to set up the integration between Cisco DNA Center and Cisco DNA Spaces, the integration may fail with the error message, "Unable to export hierarchy to the CMX DNA Spaces for one or more domain(s). An internal failure occurred while pushing an archive to the CMX."
CSCvy27260	Cisco DNA Center may fail to synchronize a Cisco Catalyst 9800 Series Wireless Controller that is configured with an access list associated to the netconfig-yang configuration.
CSCvy29574	When the appliance is configured for the first time using the express mode (install mode) of the browser-based wizard, the enterprise IP address, virtual IP address, hostname, and pnpserver.domain details are missing in the SAN field in the Cisco DNA Center certificate.
CSCvy31062	Wireless clients show the wrong SSID during onboarding.
CSCvy31186	You cannot add a second node to a Cisco DNA Center cluster installed with express mode. When using the browser-based expert mode (advanced install) to add a second node to an existing Cisco DNA Center cluster that was installed with the browser-based express mode (install mode), the process fails.
CSCvy37982	Cisco DNA Center pushes a different Anycast Gateway MAC address to some fabric edge nodes.
CSCvy42676	After a successful upgrade from Cisco DNA Center 2.1.2.3 to 2.2.2.1, all users except the user with the Admin role receive the error "Connectivity check failed" on the Software Updates window.
CSCvy43861	The config archive tries to capture data from unreachable devices.
CSCvy48594	The Assurance event notifications device parameter returns the device UUID, not the device IP address.
CSCvy53714	Wireless controller provisioning fails on IRCM version validation.
CSCvy55791	An upgrade fails due to an expired docker CA certificate.
CSCvy56987	Following a successful system upgrade of Cisco DNA Center to 2.1.2.x, the subsequent application package upgrade may fail with multiple applications.
CSCvy59061	Trend charts are empty in the Assurance Overview, Assurance Network Summary, and Assurance Client Summary windows.
CSCvy60496	NCSP10025 Provisioning failure: Unable to push the CLI command "timeout 0" to the device.
CSCvy63436	The scheduler-service gets restarted due to an out of memory error.
CSCvy63523	Cisco DNA Center Compliance flags configurations that are originally pushed by Cisco DNA Center but overridden by user templates.
CSCvy65690	Reserved child pools for Layer 3 handoff are not released after a failed fabric provision.
CSCvy66833	Cannot assign several Meraki APs to a site.
CSCvy72487	Unable to deploy SSA on a device that has more than 1000 entries in its routing table.
CSCvy73302	A heatmap is not generated for Internal-9120-Dual-2.4GHz.
CSCvy80252	Cisco ISE integration fails with the following error: `FQDN x doesn't match the common name contained in the system certificate.`

Bug Identifier	Headline
CSCvy88667	Update or delete from the protocol endpoint violates the foreign key constraint on the vxlannvesettings table.
CSCvy91546	Cisco DNA Center may fail to provision a managed fabric device if an IP address pool from the virtual network was changed, and the site name was changed to a shorter name than before, while the device is offline.
CSCvy93346	Cisco DNA Center may be unable to remove a managed device from a fabric-in-a-box installation. The network programmer service's logs contain the following error: `ERROR: update or delete on table lisprtrlocatorset violates foreign key constraint "fk9d5ac9b056ea3464" on table lisprtrlocatorsetentry.`
CSCvy94846	An appliance mismatch occurs between the main (DN2-HW-APL-XL) and the recovery (DN2-HW-APL-XL-U) appliance.
CSCvy97313	Cisco DNA Center may fail to collect the inventory from a switch that was upgraded from Cisco IOS-XE 17.3.3 to 17.5.1, because internal database entries may be missing.
CSCvy97508	While upgrading Cisco DNA Center to 2.1.2.7, the hook created to resolve defect CSCvy71772 waits indefinitely, causing the upgrade to fail.

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 2.6 patch 1, 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, 2.4 patch 7, or later, and retry the Cisco DNA Center upgrade.
- In-Service Software Upgrade (ISSU) is not supported in Cisco SD-Access deployments.

Cloud Connectivity via SSL Intercept Limitation

Some Cisco DNA Center applications, such as the Cisco AI Network Analytics agent on the Cisco DNA Center appliance, require establishing a secure communication to the cloud, with mutual authentication using X.509 certificates.

In addition to direct connectivity, use of a proxy is also supported, as long as the SSL communication is terminated directly at the agent and the cloud endpoint, without any SSL interception device in between.

Cloud connection via an SSL intercept device is not supported and could result in connectivity failures.

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 the 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.

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 Smart License registration of the Cisco 5500 Series AireOS Wireless Controller when the connection mode is smart-proxy.

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 SD-Access transit network.

- The IP-Directed Broadcast feature is supported over SD-Access transit only for unknown unicast traffic destined to silent hosts (that is, hosts present on the remote SD-Access site but not registered to the control plane). IP-Directed Broadcast over SD-Access transit does not support broadcast packets.

Existing 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 a 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 the device configuration only one time per controller.
- 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 existing device provisioning.

- The authentication and accounting servers must have the same IP addresses for them to be learned through existing device 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 Limitations

- 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.
- During wireless provisioning, Cisco DNA Center deletes any rules with an index from 1 to 99 that are configured out-of-the box or through a template. Cisco DNA Center retains rules with an index of 100 or higher. If you want to use any out-of-the-box rules, use index 100 or higher.

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 the 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

- Infoblox limitations:
  - Infoblox does not expose a name attribute; therefore, the comment field in Infoblox is populated by the IP pool name during a sync.

    - For a pool import, the first 50 characters of the comment field are used. If there are spaces in the comments, they are replaced by underscores.
    - If an IP pool name is updated for an imported pool, the comments are overwritten and the new name is reflected.

- BlueCat: There are no limitations identified with BlueCat integration at this time.
- You might see the following error when editing an existing IPAM integration or when adding a new IPAM manager.

  ```
  NCIP10283: The remote server presented a certificate with an incorrect CN of the owner
  ```

  To correct this, regenerate a new certificate for IPAM and verify that any one of the following conditions are met:

    - No values are configured in SAN field of the certificate.
    - If there is a value configured, the value and type (IP address or FQDN) must match the configured URL in the **System** > **Settings** > **External Services** > **IP Address Manager** page.

- 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).

Encryption Limitation with SNMPv3

AES192 and AES256 encryption is not fully supported for SNMPv3 configuration. If you add devices with AES192 or AES256 encryption to Cisco DNA Center, Assurance data is not collected for those devices.

As a workaround, to collect Assurance data, add a device with AES128 encryption. Cisco DNA Center supports AES128 and gathers Assurance data for devices with AES128 encryption.

IPv6 Limitations

If you choose to run Cisco DNA Center in IPv6 mode:

- Access Control Application, Group-Based Policy Analytics, and Cisco AI Endpoint Analytics packages are disabled and cannot be downloaded or installed.
- Communication through Cisco ISE pxGrid is disabled because Cisco ISE pxGrid does not support IPv6.

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 GUI operations to respond within 5 seconds or less, for extreme cases based on realistic data, it can take up to 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 GUI operations to fail. Operations that take longer than 1 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 security group to another, Cisco Group-Based Policy Analytics is unaware of this change until the next hour.
- You cannot sort the Security 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
```

Wireless Limitation

Cisco DNA Center reboots a Cisco AireOS wireless controller during site assignment if data externalization is disabled on the wireless controller.

When data externalization is disabled on a Cisco AireOS wireless controller, and Cisco DNA Center discovers the device and assigns it to a site, the device reboots.

```
(WLC-5520) >show dx summary

Data externalization status.....................................Disable
```

To avoid this problem, discover the Cisco AireOS controller with data externalization enabled, and then assign the device to a site. In this case, the device does not reboot.

Virtual Device Context Limitation

Cisco Nexus 7000 Series Switches support virtual device contexts (VDCs).

When VDC is configured on a Cisco Nexus 7000, only one VDC is discovered in the Cisco DNA Center inventory and used for Assurance.

Reports Limitations

- Reports with significant data can sometimes fail to generate in the Cisco DNA Center platform. If this occurs, we recommend that you use filters to reduce the report size to prevent such failures.
- To generate a Rogue and aWIPS report, you must choose a site hierarchy that contains a maximum of 254 floors. If you choose a site hierarchy that contains 255 floors or more, the Rogue and aWIPS report fails to generate.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

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 APs, and software releases.	*Cisco DNA Center Compatibility Matrix*
Hardware and software support for Cisco SD-Access.	*Cisco SD-Access Compatibility Matrix*
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 ITSM integration and Cisco DNA Center ITSM support.	*Cisco DNA Center ITSM Integration Guide*
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 and aWIPS functionality to monitor threats in Cisco DNA Center.	*Cisco DNA Center Rogue Management and aWIPS Application Quick Start Guide*