Release Notes for Cisco DNA Center, Release 2.3.3.x

First Published: 2022-04-26

Last Modified: 2024-02-22

Release Notes for Cisco DNA Center, Release 2.3.3.x

This document describes the features, limitations, and bugs for Cisco DNA Center, Release 2.3.3.x.

For links to all of the guides in this release, see *Cisco DNA Center 2.3.3 Documentation.*

Change History

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

Date	Change	Location
2024-02-22	Added the open bug CSCwh06255.	Open Bugs, on page 35
2024-02-06	Noted that in 2.3.3.0, Cisco TrustSec (CTS) role-based enforcement is now the same for SD-Access edge nodes and border nodes. In earlier releases, CTS role-based enforcement is configured globally on SD-Access edge nodes only.	New and Changed Features in Cisco Software-Defined Access, on page 25
2023-11-01	Added the Resolved Bugs table for the 2.3.3.7-72328-HF5 hot fix.	Resolved Bugs, on page 39
	Updated the list of packages for 2.3.3.7-72328-HF5.	Package Versions in Cisco DNA Center, Release 2.3.3.x, on page 3
2023-10-20	Added a limitation about the site hierarchy for a Rogue and aWIPS report.	Guidelines and Limitations, on page 59
2023-10-12	Added the Resolved Bugs table for the 2.3.3.7-72328-HF4 hot fix, which includes CSCwe15923 with a modified fix for explicit restart of etcd containers. This hook explicitly restarts the etcd container if it's still using the old etcd certificate that was renewed before an upgrade to 2.3.3.7.	Resolved Bugs, on page 39
2023-09-29	Added the open bug CSCwh58183 for 2.3.3.7.	Open Bugs, on page 35
2023-09-27	Updated the list of packages in 2.3.3.7.	Package Versions in Cisco DNA Center, Release 2.3.3.x, on page 3
	Added the open bugs CSCwe28523 and CSCwe42201.	Open Bugs, on page 35

Date	Change	Location
2023-09-22	Added the resolved bug CSCwe15923, which is fixed as a hook for 2.3.3.7. If you renewed your etcd certificate after upgrading to 2.3.3.7, the fix installed by the hook handles the certificate renewal for 2.3.3.7.	Resolved Bugs, on page 39
2023-08-18	Added a limitation about custom applications.	Guidelines and Limitations, on page 59
2023-08-03	Added the open bug CSCwh15353.	Open Bugs, on page 35
2023-08-01	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.	—
2023-07-06	Noted that if you run Cisco DNA Center in IPv6 mode, wireless controller provisioning is not supported.	Guidelines and Limitations, on page 59
2023-06-26	Added the open bug CSCwf73998.	Open Bugs, on page 35
2023-06-07	Noted that if you run Cisco DNA Center in IPv6 mode, LAN automation is not supported.	Guidelines and Limitations, on page 59
2023-04-19	Added the list of packages in the latest version of Cisco DNA Center 2.3.3.7.	Package Versions in Cisco DNA Center, Release 2.3.3.x, on page 3
	Added the resolved bug CSCwe44726, which is resolved when you install the latest 2.3.3.7 package version for the Automation – Base package.	Resolved Bugs, on page 39
2023-03-09	Added the list of packages in Cisco DNA Center 2.3.3.7.	Package Versions in Cisco DNA Center, Release 2.3.3.x, on page 3
	Added the Resolved Bugs table for 2.3.3.7.	Resolved Bugs, on page 39
	Added the open bugs CSCwb66336, CSCwc74941, CSCwe27538, CSCwe36755, CSCwe42329, and CSCwe47539.	Open Bugs, on page 35
	Added a limitation about In-Service Software Upgrade (ISSU).	Guidelines and Limitations, on page 59
2022-12-20	Added the list of packages in Cisco DNA Center 2.3.3.6.	Package Versions in Cisco DNA Center, Release 2.3.3.x, on page 3
	Added the Resolved Bugs table for 2.3.3.6.	Resolved Bugs, on page 39
	Added the open bugs CSCwc37682 and CSCwd92491.	Open Bugs, on page 35
2022-11-08	Added CSCvy63072 to the Resolved Bugs table for 2.3.3.0.	Resolved Bugs, on page 39

Date	Change	Location
2022-09-30	Added the list of packages in Cisco DNA Center 2.3.3.5.	Package Versions in Cisco DNA Center, Release 2.3.3.x, on page 3
	Added the Resolved Bugs table for 2.3.3.5.	Resolved Bugs, on page 39
	Added the open bugs CSCwc85038 and CSCwd12685.	Open Bugs, on page 35
2022-08-03	Added the list of packages in Cisco DNA Center 2.3.3.4.	Package Versions in Cisco DNA Center, Release 2.3.3.x, on page 3
	Added the Resolved Bugs table for 2.3.3.4.	Resolved Bugs, on page 39
2022-07-06	Added the list of packages in Cisco DNA Center 2.3.3.3.	Package Versions in Cisco DNA Center, Release 2.3.3.x, on page 3
	Added the Resolved Bugs table for 2.3.3.3.	Resolved Bugs, on page 39
	Added the open bug CSCwc34451.	Open Bugs, on page 35
2022-06-03	Added a link to the new features in Cisco DNA Center 2.3.2, which is a Commercial Availability release. The features in 2.3.2.x are rolled up to 2.3.3.x.	New Features in the Previous Release, on page 30
2022-06-01	Added the list of packages in Cisco DNA Center 2.3.3.1.	Package Versions in Cisco DNA Center, Release 2.3.3.x, on page 3
	Added the Resolved Bugs table for 2.3.3.1.	Resolved Bugs, on page 39
2022-04-26	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*.

Before you upgrade, run the Audit & Upgrade Readiness Analyzer (AURA) precheck. AURA is a command-line tool that performs health, scale, and upgrade readiness checks for Cisco DNA Center and the fabric network. For more information, see Enhanced Visibility into Cisco DNA Center Using AURA.

Package Versions in Cisco DNA Center, Release 2.3.3.x

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

Package Name	Release 2.3.3.7				Release 2.3.3.6	Release 2.3.3.5	Release 2.3.3.4
Release Build Version							
Release Version	2.3.3.7-72328-HF5	2.3.3.7-72328-HF4	2.3.3.7.72328	2.3.3.7.72323	2.3.3.6.70045	2.3.3.5.70134	2.3.3.4.72142
System Updates							
System	1.7.858				1.7.828	1.7.769	1.7.717

Package Name	Release 2.3.3.7				Release 2.3.3.6	Release 2.3.3.5	Release 2.3.3.4	Rel
System Commons	2.1.518.62248	2.1.518.62240	2.1.518.62181	2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231	2.1
Package Updates								
Access Control Application	2.1.518.62248	2.1.518.62240	2.1.518.62181	2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231	2.1
AI Endpoint Analytics	1.7.702				1.7.702	1.7.702	1.7.658	1.7
AI Network Analytics	2.9.28.422				2.9.27.414	2.9.24.406	2.9.21.398	2.9
Application Hosting	1.9.02309170357	1.9.02212150812			1.9.02210071514	1.9.02209020733	1.9.02205130731	1.9
Application Policy	2.1.518.170095	2.1.518.170077			2.1.517.117025	2.1.515.117391	2.1.512.170103	2.1
Application Registry	2.1.518.170095	2.1.518.170077			2.1.517.117025	2.1.515.117391	2.1.512.170103	2.1
Application Visibility Service	2.1.518.170095	2.1.518.170077			2.1.517.117025	2.1.515.117391	2.1.512.170103	2.1
Assurance - Base	2.3.3.591	2.3.3.586	2.3.3.584		2.3.3.529	2.3.3.463	2.3.3.382	2.3
Assurance - Sensor	2.3.3.581				2.3.3.526	2.3.3.375	2.3.3.375	2.3
Automation - Base	2.1.518.62248	2.1.518.62240	2.1.518.62181	2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231	2.1
Automation - Intelligent Capture	2.1.518.62248	2.1.518.62240	2.1.518.62181	2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231	2.1
Automation - Sensor	2.1.518.62248	2.1.518.62240	2.1.518.62181	2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231	2.1
Cisco DNA Center Global Search	1.8.1.10				1.8.1.10	1.8.1.10	1.8.1.10	1.8
Cisco DNA Center Platform	1.8.1.159	1.8.1.158			1.8.1.147	1.8.1.137	1.8.1.120	1.8
Cisco DNA Center UI	1.7.1.349				1.7.1.341	1.7.1.339	1.7.1.326	1.7
Cisco Identity Services Engine Bridge	2.1.518.1015				2.1.517.1015	2.1.515.450	2.1.512.417	2.1
Cisco Umbrella	2.1.518.592104				2.1.517.590035	2.1.515.590102	2.1.514.592341	2.1

Package Name	Release 2.3.3.7				Release 2.3.3.6	Release 2.3.3.5	Release 2.3.3.4
Cloud Connectivity - Contextual Content	2.4.1.338				2.4.1.338	2.4.1.338	2.4.1.322
Cloud Connectivity - Data Hub	1.8.43				1.8.43	1.8.43	1.8.33
Cloud Connectivity - Tethering	2.30.1.72				2.30.1.72	2.30.1.72	2.30.1.71
Cloud Device Provisioning Application	2.1.518.62181			2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231
Command Runner	2.1.518.62181			2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231
Device Onboarding	2.1.518.62248	2.1.518.62240	2.1.518.62181	2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231
Disaster Recovery	2.1.518.360011				2.1.517.360009	2.1.515.360031	2.1.514.360024
Disaster Recovery—Witness Site	2.1.518.370008				2.1.517.37002	2.1.515.37015	2.1.512.370012
Group-Based Policy Analytics	2.3.3.35				2.3.3.35	2.3.3.35	2.3.3.32
Image Management	2.1.518.62248	2.1.518.62240	2.1.518.62181	2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231
Machine Reasoning	2.1.518.212109				2.1.517.210046	2.1.515.210125	2.1.514.212433
NCP - Base	2.1.518.62248	2.1.518.62181		2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231
NCP - Services	2.1.518.62248	2.1.518.62181		2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231
Network Controller Platform	2.1.518.62248	2.1.518.62240	2.1.518.62181	2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231
Network Data Platform - Base Analytics	1.8.503	1.8.339			1.8.339	1.8.239	1.8.239
Network Data Platform - Core	1.8.513	1.8.447			1.8.447	1.8.396	1.8.326

Package Name	Release 2.3.3.7				Release 2.3.3.6	Release 2.3.3.5	Release 2.3.3.4	Rel
Network Data Platform - Manager	1.8.244				1.8.244	1.8.244	1.8.244	1.8
Network Experience Platform - Core	2.1.518.62181			2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231	2.1
Path Trace	2.1.518.62248	2.1.518.62181		2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231	2.1
RBAC Extensions	2.1.518.1920001				2.1.517.1900001	2.1.515.1900002	2.1.512.1920014	2.1
Rogue and aWIPS	2.5.0.28				2.5.0.20	2.5.0.20	2.5.0.20	2.5
SD-Access	2.1.518.62248	2.1.518.62240	2.1.518.62181	2.1.518.62180	2.1.517.60110	2.1.515.60238	2.1.514.62231	2.1
Stealthwatch Security Analytics	2.1.518.1092102				2.1.517.1090044	2.1.515.1090110	2.1.514.1092349	2.1
Support Services	2.1.518.880004				2.1.517.880012	2.1.510.880029	2.1.510.880029	2.1
System Remediation	1.0.2		—		—	—	—	—
Wide Area Bonjour	2.4.514.75204				2.4.514.75204	2.4.511.75063	2.4.511.75063	2.4

New and Changed Information

New and Changed Features in Cisco DNA Center

Table 1: New and Changed Features for Cisco DNA Center, Release 2.3.3.7

Feature	Description
Dynamic Channel Assignment (DCA) Validation	DCA channel support is based on the regulatory domain of the device. During AP provisioning with an RF profile selected, out of all the DCA channels configured on the RF profile only the supported channels as per the country code are considered and the unsupported channels are ignored. You can view the list of unsupported channels in the AP preprovision summary window.
Enhancements to AP Location Configuration	During AP provisioning and AP Plug and Play (PnP) onboarding, Cisco DNA Center doesn't configure the assigned site as the AP location. You can configure the AP location using the **Configure Access Points** workflow.
Enhancements to Authentication using AAA Server for Wireless Networks	Effective with this release, you must configure an AAA server for an SSID to push the authentication configuration for the SSID. If an AAA server is not configured for the SSID, Cisco DNA Center pushes the **aaa authentication dot1x default local** command to the wireless controller and the default method list that points to local authentication is mapped to the SSID.

Feature	Description
Enhancements to Default Configuration of Fast Transition Over Distributed Systems for SSIDs	Effective with this release, fast transition over a distributed system (**Over the DS** check box) is disabled by default for SSIDs for guest and enterprise wireless networks.
Enhancements to Editing RF Profiles	Effective with this release, when you update an RF profile that is already provisioned on a wireless controller and AP, you can reprovision either the wireless controller or AP. Wireless controller reprovisioning also pushes the RF profiles updates to the devices and AP reprovisioning is not necessary. If the you don't need the RF profile updates during the wireless controller reprovisioning, you can check the **Skip AP Provision** check box
Enhancements to RF Profiles	Effective with this release, for Cisco Catalyst 9800 Series Wireless Controllers, disabling a radio band on the RF profile doesn't disable the Admin status of the respective radios on all APs that use the RF profile. Instead, Cisco DNA Center disables the Admin status of the corresponding RF profile. **Note** When the Admin status of a radio band on the RF profile is in disabled state and you upgrade to Release 2.3.3.7, if you reprovision the wireless controller or AP: • Cisco DNA Center creates the RF profile for the corresponding radio band with Admin status as disabled. • Cisco DNA Center updates the RF profile mapping in the RF tag on the device from **Global Config** to the newly created RF profile.
Enhancements to Site Tags, Policy Tags, and AP Zone Provisioning	Site tags, policy tags, and AP zone provisioning have the following enhancements: • If an AP zone is already provisioned on an AP and you update the AP zone configuration, you must reprovision the wireless controller. Reprovisioning the AP is not necessary. • Newly added custom site tag and policy tag configurations are applied only when you provision the APs. Provisioning the wireless controller alone doesn't configure the new custom tags on the APs. If there are any updates to the tags after the first provisioning, you must reprovision the wireless controller or APs.

Table 2: New and Changed Features for Cisco DNA Center, Release 2.3.3.0

Feature	Description

2D Wireless Maps Enhancements	• Interaction between 2D wireless maps and Cisco Spaces or Cisco Connected Mobile Experiences (CMX) has been improved.
	• Other enhancements to 2D wireless maps enable you to:
	  • View switch stacks and see the links between individual switches and their associated APs.
	  • View client information, including a client's link to its associated AP.
	  • View AP radio state, health, name, and mode, in the AP icon.
	  • Turn the grid pattern on or off when creating a floor map using a CAD file.
	  • Configure planned APs with dual radios.
	  • Add alignment points to floors so that they are positioned correctly one on top of the other.
	  • Import an Ekahau site survey file to Cisco DNA Center.
	  • Continue to view the 2D maps toolbar after resizing the screen.

3D Wireless Maps Enhancements	• Interaction between 3D wireless maps and Cisco Spaces or Cisco Connected Mobile Experiences (CMX) has been improved.
	• Other enhancements to 3D wireless maps enable you to:
	  • Perform 3D RF modeling of free space within a building.
	  • Include up to five floors in your 3D heatmap computation.
	  • View signal leakage and signal reflection.
	  • View client information, including a client's link to its associated AP.
	  • Continue to view the 3D maps toolbar after resizing the screen.

AP Configuration Workflow Enhancements	You can configure an AP even if it is not assigned to a site. You can configure the following AP parameters: • AP height • LED brightness level You can configure the following radio parameters: • CleanAir or spectrum intelligence settings • Antenna settings
Application Hosting Enhancements	You can validate the HTTPS credentials provided for the device during the device readiness check.

Feature	Description
AP Provisioning Change for XOR Radio Role	With Cisco DNA Center 2.3.3.0 or later, when you provision any AP that has XOR radio (for example, Cisco 2800, 3800, and so on) with an RF profile that has 2.4 GHz disabled, Cisco DNA Center changes the XOR radio role to 5 GHz manual. **Note** You need to use the AP config workflow for any changes to the XOR radio role.
AP Refresh Across Cisco Wireless Controllers	You can perform an AP refresh when the old AP and new AP are connected to different Cisco Wireless Controllers. You can perform an AP refresh even if the old AP is not provisioned.
AP Zones	You can add AP zones to a network profile for wireless devices. You can use AP zones to associate different SSIDs and RF profiles for a set of APs on the same site.
Assign Device Roles and Tags to Software Images	You can assign device roles and tags to a software image to indicate that the software image is marked as golden. When both the device tags and device roles are assigned to a software image, the device tags take precedence.
Central Web Authentication Using Third-Party AAA Server for Guest Wireless Networks	You can now configure Central Web Authentication (CWA) using a third-party AAA server while creating SSIDs for guest wireless networks.
Cisco Device Hardware, Software, and Module End of Life (EoX) Status	Cisco DNA Center shows alerts for the devices that are scanned for EoX alerts. The **EoX Status** column in the **Inventory** table shows the number of EoX alerts.
Cisco DNA Center Insights	You can subscribe to *Cisco DNA Center Insights*, which contains product announcements, network highlights, information about your network performance, and more. The *Cisco DNA Center Insights* publication is sent in PDF format to the email address that you specify.
Control Endpoint Spoofing	The Control Endpoint Spoofing feature provides granular policy control by providing network information other than just the MAC address of an endpoint.
Create Port Group	You can group device ports based on an attribute or rule.
Credential Status	The **Credential Status** column in the **Inventory** table shows the device credential status for devices that are configured. Click **See Details** to view details about the credentials.
Custom Policy Tags	You can configure policy tags for Cisco Catalyst 9800 Series Wireless Controllers using the advanced settings while creating network profiles for wireless devices.
Custom Template for Day 0 Onboarding Without Site Selection	If you have not assigned the device to a site, you must choose a template to claim the device.
Design the Network Hierarchy	You can now search the network hierarchy using the **Site Name** and **Site Type** filter criteria.

Feature	Description
FIPS 140-2 Support	Software images are compliant with the Federal Information Processing Standard (FIPS). If FIPS mode is enabled in Cisco DNA Center, you cannot import images from a URL. Import images from your computer or cisco.com.
	FIPS mode is supported only in a new installation of Cisco DNA Center. If you are upgrading from an earlier release, FIPS mode is not supported.
	In a FIPS deployment, you cannot enable external authentication.
	FIPS mode is not supported for the Cisco Wide Area Bonjour application. In a FIPS deployment, you cannot install the Cisco Wide Area Bonjour application from the Cisco DNA Center GUI or CLI.
	FIPS mode has the following impact on the export and import of map archives. If FIPS mode is *enabled*: • Exported map archives are unencrypted. • Only unencrypted map archives can be imported. If FIPS mode is *disabled*: • Exported map archives are encrypted. • Both encrypted and unencrypted map archives can be imported.
FIPS Support for Endpoint Analytics	When FIPS mode is enabled in Cisco DNA Center, some of the functions related to Endpoint Analytics are *unavailable* in the Cisco DNA Center GUI.
Generate Compliance Audit Report	You can get a consolidated compliance report that shows the compliance status of the devices in your network.
Integrate Cisco AI Endpoint Analytics with Talos Intelligence	Talos Intelligence is a comprehensive threat-detection network. Talos detects and correlates threats in real time. By integrating Cisco AI Endpoint Analytics with Talos, you can flag endpoints in your network that are connecting to malicious IP addresses.
Manage System Beacon	You can highlight switches in the Cisco DNA Center inventory by using a system beacon. System beacon supports the following devices: • Cisco Catalyst 3850 Series Ethernet Stackable Switches • Cisco Catalyst 9200 Series Switches • Cisco Catalyst 9300 Series Switches
Manage Your Inventory	In the **Inventory** window, if you choose the **Default** view from the **Focus** drop-down list, the **Inventory** table displays only the **Device Name**, **IP Address**, **Device Family**, and **MAC Address** of listed devices.
NAS ID Configuration	You can configure network access server identifiers (NAS IDs) for SSIDs for enterprise and guest wireless networks.

Feature	Description
QoS Settings for Wireless Networks	You can choose one of the following QoS settings for the primary traffic while creating SSIDs for enterprise and guest wireless networks: • **VoIP (Platinum)** • **Video (Gold)** • **Best Effort (Silver)** • **Non-real Time (Bronze)**
Return Material Authorization (RMA) Support for New Devices	RMA Workflow support is extended for the following: • Cisco Catalyst 4500e, Catalyst 6500, Catalyst 6800, and Catalyst 9000 Series modular switches. • Supervisors of modular switches with single and dual engines. • Extended node that is part of the STP ring or daisy chain. • Daisy chain and ring of Industrial Ethernet (IE) switches. • Devices that have an external Simple Certificate Enrollment Protocol (SCEP) broker PKI certificate.
RMA Support	Zero-touch onboarding of replacement device through PnP is supported for fabric and LAN automation devices.
Schedule Group-Based Access Control Policy Updates	You can save policy changes immediately or schedule an update at a specific time. You can view the status of the scheduled tasks in **Activities** > **Tasks**. If the **Cisco DNA Center Automation Events for ITSM (ServiceNow)** bundle is enabled, the **Save Now** option is disabled, and only the **Schedule Later** option is enabled for Group-Based Access Control policy changes. Note that the scheduled task must be approved in IT Service Management (ITSM) before the scheduled time.
Schedule Recurring Events for APs	You can schedule recurring events for AP and radio parameters in the AP configuration workflow.
Sync Updates for Software Images	You can synchronize the information of software images from cisco.com for all the managed devices in Cisco DNA Center.
Troubleshoot Unmonitored Devices	Using the MRE workflow, you can troubleshoot unmonitored devices or the devices that do not show Assurance data.
Troubleshoot Wireless Client Issues	Using the MRE workflow, you can troubleshoot wireless client issues.
URL-Based Access Control List	You can create IP-based and URL-based postauthentication access control lists (ACLs) for your network.
View All Discoveries	The new **Discoveries** table in Cisco DNA Center shows details of all the discovery jobs and provides options to rediscover and delete discovery jobs.

Feature	Description
View Image Update Workflow	You can view the progress of software image update tasks. Cisco DNA Center shows the status of each task that is associated with the Distribution and Activation operations and the amount of time taken to complete each operation.

New and Changed Features in Cisco DNA Assurance

Table 3: New and Changed Features for Assurance, Release 2.3.3.5

Feature	Description
RF Simulator	Using the AI RF Simulator, you can simulate changes to the current RF profile configurations and visualize the projected outcome against the enhanced RRM dashlets on the **Enhanced RRM** dashboard.
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.

Table 4: New and Changed Features for Assurance, Release 2.3.3.0

Feature	Description
Additional AP Radio Channel Utilization Metrics Added to the **AP Radio Comparison View**	In the **Device 360** window, you can compare AP radios by the following additional KPIs: • **Traffic Utilization** • **Tx Traffic Utilization** • **Rx Traffic Utilization**
AP Mesh: Information Added to **Device 360** Window	In the **Device 360** window, you can view mesh AP information in the **Mesh** tab.
Cisco AI Network Analytics: 6-GHz Radio Support	Cisco AI Network Analytics supports 6-GHz RF for the following functionalities: • Network Heatmaps • AP Performance Advisories • Trend Deviations (Insights) • AP RF Statistics • AP Spectrum Analysis
Cisco AI Network Analytics: Peer Comparison KPIs	The **Peer Comparison** supports the following KPIs: • **Onboarding Error Source**: Compares Onboarding Error Source in your network to that of your peers • **Roaming Error Source**: Compares Roaming Error Source in your network to that of your peers

Feature	Description
Cisco AI Network Analytics: Roaming KPIs in Network Heatmaps	The **Network Heatmaps** supports the following roaming KPIs: • **Successful inbound roaming events** • **Successful outbound roaming events** • **Total inbound roaming events**
Cisco SD-Access: LISP and Pub/Sub Session	SD-Access Health supports **LISP** and **Pub/Sub** session monitoring in the fabric sites. These KPIs are part of Fabric Site, SD-Access Transit, Transit Control Plane, and Device health calculations.
Cisco SD-Access: Transits and Peer Networks	You can monitor the health of the Transits and Peer Networks in the SD-Access Health dashboard.
Client Dashboard Enhancements	In the Assurance **Client** dashboard, the **Client Devices** dashlet includes **Tracked Client**, which allows you to track clients and notify them when they are detected in the network.
Device Events	Before this release, events were shown only in the Device window. Now, the **Events** dashboard provides a more contextual view of device events. Instead of having to search for events triggered by devices that are connected to other devices involved in an event, Assurance provides these details for you.
Intel Analytics Support	In the **Client 360** window, under **Detail Information**, the **Intel Connectivity Analytics** tab is newly added. This tab is only available for devices supported by Intel wireless adapters.
New AP Radio Down Issue	A new Radio Down issue is added to the AP issues. The Radio Down issue is triggered when a radio goes down. Supported radio frequencies are 2 GHz, 5 GHz, and 6 GHz.
New AP Radio Traffic Utilization Chart	In the **AP 360** window, under **Detail Information** in the **RF** tab, you can view a new chart called **Traffic Utilization**. This chart includes receive (Rx) and transmit (Tx) traffic utilization information. In addition, Rx and Tx traffic utilization information has been added to the **Channel Utilization** chart.
Path Trace Enhancements	Path trace results include the average processing delay of ACLs, tunneling, and queues, and the reason for a packet drop decision.
Application Health	Starting in 2.3.3.0, in the Assurance **Application Health** dashboard, most of the dashlets display the application health data only for the Business Relevant Applications. Some of the dashlets display the Business Irrelevant and Default applications.

New and Changed Features in Cisco DNA Center Platform

Feature	Description
New API Features	

Feature	Description
Cisco DNA Center System API	The Cisco DNA Center platform supports the following **System** API to authorize one or more devices: • POST <cluster-ip>/dna/intent/api/v1/onboarding/pnp-device/authorize To authorize one or more devices. Cisco DNA Center platform allows you to authorize a device only if the authorization is configured in device settings. To access the new **System** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Cisco DNA Center System** drop-down list.

Feature	Description
Cisco SD-Access API	This Cisco DNA Center platform release supports new options in the **SDA** API to get, add, and delete the list of Cisco SD-Access devices: • GET <cluster-ip>/dna/intent/api/v1/business/sda/virtual-network/summary Get a virtual network summary. • GET <cluster-ip>/dna/intent/api/v1/business/sda/transit-peer-network Get transit peer network information from Cisco SD-Access. • POST <cluster-ip>/dna/intent/api/v1/business/sda/transit-peer-network Add a transit peer network in Cisco SD-Access. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/transit-peer-network Delete a transit peer network from Cisco SD-Access. **Note** • All the Cisco SD-Access platform APIs are **Beta**. • With this release, the following Cisco SD-Access APIs are deprecated from Cisco DNA Center platform: • GET <cluster-ip>/dna/intent/api/v1/business/sda/fabric Get Cisco SD-Access fabric information. • GET <cluster-ip>/dna/intent/api/v1/business/sda/fabric/count Get Cisco SD-Access fabric count. • POST <cluster-ip>/dna/intent/api/v1/business/sda/fabric Add Cisco SD-Access fabric. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/fabric Delete Cisco SD-Access fabric. To access the new **SDA** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Connectivity** drop-down list and choose **SDA**.

Feature	Description
Devices API	The Cisco DNA Center platform **Devices** API support is extended for voice VLAN to perform devices operations: • PUT <cluster-ip>/dna/intent/api/v1/interface/${interfaceUuid Add/Update interface description, VLAN membership, Voice VLAN, and change interface admin status (UP/DOWN) from request body. The Cisco DNA Center platform **Devices** API also supports the following rouge and aWIPS APIs: • GET<cluster-ip>/dna/intent/api/v1/security/threats/type To retrieve all the defined threat types. • GET<cluster-ip>/dna/intent/api/v1/security/threats/rogue/allowed-list To retrieve all the allowed MAC addresses in the system. • DELETE<cluster-ip>/dna/intent/api/v1/security/threats/rogue/allowed-list/${macAddress} To remove the threat MAC address from the allowed list. • GET<cluster-ip>/dna/intent/api/v1/security/threats/level To retrieve all the defined threat levels. • POST<cluster-ip>/dna/intent/api/v1/security/threats/rogue/allowed-list To add the threat MAC address to the allowed list. • GET<cluster-ip>/dna/intent/api/v1/security/threats/rogue/allowed-list/count To retrieve the count of allowed MAC addresses in the system. To access the new **Devices** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Devices**.
New ITSM Integration Features	
Cisco Software-Defined Access Integration with ITSM (ServiceNow)	With this release, the Cisco Software-Defined Access integration with ServiceNow monitors and publishes fabric events that require fabric role updates for security or other operational triggers to an ITSM (ServiceNow) system. It also allows you to trigger or schedule a synchronization between Cisco DNA Center devices and the ServiceNow CMDB system. For more information, see **Configure the Cisco SD-Access Integration with ITSM (ServiceNow)** in the Cisco DNA Center ITSM Integration Guide.
New Reports	

Feature	Description

End-of-Life Data Report	This release supports a new **End of Life (EoX)** report category and **EoX Data** report. The **EoX Data** report provides detailed information about network devices and the end of life alerts that were detected on them from the previous scan.
	• The **EoX Data** report is generated on the following criteria:
	  • Device Name
	  • IP Address
	  • Device Type
	  • Site
	  • EoX Type
	  • EoX Scan Status
	  • End-of-Life Announcement
	  • End-of-Scale
	  • Last Ship
	  • End of SW Maintenance
	  • End of New Service Attachment
	  • End of Vulnerability/Security Support
	  • End of Service Contract Renewal
	  • Last Date of Support
	• The **EoX Data** report file formats include **PDF**, **CSV**, and **TDE**.
	To access the **EoX Data** report, click the menu icon and choose **Report** > **Reports Templates** > **EoX**.
	In the **Report** window, choose **EoX Data**.
	For more information about **EoX Data**, see the *Cisco DNA Center Platform User Guide*.

Feature	Description

License Historical Usage Report	This release supports a new **License Historical Usage** report that provides the detailed information about historical data of license usage.
	• The **License Historical Usage** report is generated on the following criteria:
	  • Licenses
	  • Smart Account
	  • Virtual Account
	  • License Tags
	  • Billing Type
	  • Purchased
	  • In Use
	  • Balance
	  • Entry Date
	• Supported report file format includes CSV.
	• In the **Setup Report Scope** window, the **License Historical Usage** report provides license historical usage details based on the following:
	  • Report Name
	  • Scope (Smart Account User, Smart Account Name, and Frequency)
	• In the **Schedule Report** window, you can define a date range and select a time zone to generate the report.
	  The following **Schedule** options are available:
	  • Run Now
	  • Run Later (One-Time)
	• To access the **License Historical Usage** report, click the menu icon and choose **Reports** > **Report Templates** > **Licensing**.
	  In the **Report** window, choose **License Historical Usage**.
	  For more information about **License Historical Usage**, see the *Cisco DNA Center Platform User Guide*.

Feature	Description
Network Device Compliance Report	

Feature	Description

	This release supports a new **Compliance** report category and **Network Device Compliance** report. The **Network Device Compliance** report provides the compliance status of individual network devices. With this report, you can get complete visibility of your network.
	• The **Network Device Compliance** report is generated on the following criteria:
	  • Device Name
	  • Device Family
	  • Device Type
	  • IP Address
	  • Compliance Status
	  • Software Image Status
	  • Startup vs Running Configuration Status
	  • Critical Security Advisories Status
	  • Network Profile Status
	• Supported report file formats are PDF, CSV, and JSON.
	• The **Network Device Compliance** report allows you to perform the following tasks:
	  • **Compliance Status**: You can audit the mismatch of the device configuration from the intended value, which is shown as Non-Compliant in the report.
	  • **Software Image**: You can audit the mismatch of the device software image from the golden image, which is shown as Non-Compliant in the report.
	  • **Startup Vs Running Configuration**: You can audit the mismatch of the startup configuration from the running configuration of the device, which is shown as Non-Compliant in the report.
	  • **Critical Security Advisories**: If any critical advisory exists for the device, it is marked as Non-Compliant in the report.
	  • **Network Profiles**: You can audit the mismatch of the device configuration from the intent configuration of the profile, which is marked as Non-Compliant in the report.
	To access the **Network Device Compliance** report, click the menu icon and choose **Report** > **Reports Templates** > **Compliance**.
	In the **Report** window, choose **Network Device Compliance**.
	For more information about **Network Device Compliance** report, see the

Feature	Description
	Cisco DNA Center Platform User Guide.

Unique Client and User Summary Report	This release supports a new **Unique Client and User Summary** report that provides detailed information about **Unique Clients**, **Unique Users**, **Unique AP**, **Average Client per AP**, **Breakdown by Protocol**, **Breakdown by Vendor**, **SSID**, and **VLAN**.
	• The **Unique Client and User Summary** report is generated on the following criteria:
	  • Average session per time, client, and users
	  • Average traffic per client, user, and session
	  • Average throughput per client, user, and session
	  • Clients, users, sessions, session time, and traffic per protocol
	  • Top five clients, users, sessions, session time, and traffic per vendor
	  • Top five clients, users, and traffic per VLAN
	• Supported report file formats include PDF.
	• In the **Setup Report Scope** window, the **Unique Client and User Summary** report provides unique client and user summary details based on the following:
	  • Location
	  • Connection type
	  • SSID
	  • Band
	• In the **Schedule Report** window, available time range options are **Last 3 Hours**, **Last 24 Hours** and **Custom**.
	Note Use the **Custom** option to customize the date and time interval up to a maximum range of one day. If you choose a range outside of one day, the range is adjusted to the closest one-day range.
	To access the **Unique Client and User Summary** report, click the menu icon and choose **Report** > **Reports Templates** > **Clients**.
	In the **Report** window, choose **Unique Client and User Summary**.
	For more information about **Unique Client and User Summary**, see the *Cisco DNA Center Platform User Guide*.

Feature	Description

Worst Interferer Report	This release supports a new **Worst Interferers** report that provides detailed information about interferers detected by AP radios.
	Note Worst interferer data is available only from Cisco Embedded Wireless Controllers.
	• The **Worst Interferers** report is generated on the following criteria:
	  • Device name
	  • Severity
	  • Worst server
	  • Interferer ID
	  • RSSI value of interference
	  • Duty cycle
	  • Affected channels
	  • AP name
	  • Slot
	  • Band
	  • Location
	  • First discovered time
	• Supported report file formats include CSV, TDE, and JSON.
	• In the **Setup Report Scope** window, the **AP Name** drop-down list is filtered based on the location you select in the **Location** filter.
	Note From the **AP Name** drop-down list, you can select a maximum of 250 AP names.
	• In the **Schedule Report** window, available time range options are **Last 3 Hours**, **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, **Last 90 Days**, and **Custom**.
	Note Use the **Custom** option to customize the date and time interval, as well as the time zone (GMT) for the time range.
	To access the **Worst Interferers** report, click the menu icon and choose **Report** > **Reports Templates** > **Access Point**.
	In the **Report** window, choose **Worst Interferers**.
	For more information about **Worst Interferers**, see the *Cisco DNA Center Platform User Guide*.

Feature	Description
New Reports Features	
New Reports GUI Features	The Cisco DNA Center platform support is extended for the following enhancements in the **AP Radio** report: • Cisco DNA Center support is extended for sorting and top N filter in existing AP Radio report that allows you to identify and capture the metrics of busiest AP radio. The AP radio report data displays the number of rows equals to the number of radios in an AP. • In the **Setup Report Scope** page, **Sort by** filter supports the following options: • AP Name • Max Radio Utilization • Max Tx Utilization • Max Rx Utilization • Max Client Count • **Select File Type** page, the following new fields are added: • WLC IP Address • Max TX Utilization (%) • Max RX Utilization (%) • Supported report file formats include **CSV**, **TDE**, and **JSON**. For more information about creating reports, see the *Cisco DNA Center Platform User Guide*.

New and Changed Features in Cisco DNA Automation

Feature	Description
Certificate Signing Request (CSR) Enhancement	You can do the following in the **Certificate Signing** window: • Copy the CSR properties in plain text. • Copy Base64 and paste to MS CA. • Download Base64.

Feature	Description
Compliance Audit for Network Devices	You can see if your network device contains a specific configuration. If that configuration is missing, Cisco DNA Center alerts you and then remediates the compliance problem. The workflow is as follows: 1. Under **Tools** > **Template Editor**, create a template that defines the configuration that the network device must have. 2. Under **Design** > **Network Profiles**, associate the template to a network profile. 3. Under **Network Devices** > **Inventory** > **Provision Devices**, provision the network device. 4. Under **Provision** > **Inventory** > **All Devices** > **Compliance** > **Summary**, run a compliance check to compare the network profile with the current running configuration and see the summary. 5. Remedy the compliance problem.
Configure AAA VLAN Name Override for FlexConnect Deployments on Cisco AireOS Controller	For the AAA VLAN override settings, you can configure VLAN ID and VLAN name mapping for a specific FlexConnect profile on the **Design** > **Network Settings** > **Wireless** window.
Configure System Settings	In this release, Cisco DNA Center supports the following enhancements in the **System Configuration**: • The **Proxy Config** and **Proxy Certificate** are combined under the **Proxy** window. • In the **Proxy** window, you can configure the proxy configuration in the **Outgoing Proxy** tab. • In the **Proxy** window, you can configure the proxy certificate in the **Incoming Proxy** tab. Cisco DNA Center also allows you to retain or delete the licensed smart account users and their associated historical data.
Learning of AAA VLAN Override from Cisco AireOS Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller with Pre-existing Infrastructure	Using the **Learn Device Configuration** workflow, you can learn about VLAN configurations from Cisco AireOS Wireless Controllers and Cisco Catalyst 9800 Series Wireless Controllers with pre-existing infrastructure.
Learning of Mesh Configurations from Cisco Wireless Controller with Pre-existing Infrastructure	Using the **Learn Device Configuration** workflow, you can learn mesh configurations from Cisco Wireless Controllers with pre-existing infrastructure and map them back to the Cisco DNA Center wireless design.
Manage Licenses	You can view the historical trends for all purchased and consumed license consumptions in CSSM on a daily, weekly, and monthly basis. CSSM stores the historical information up to one year.
Support for 300 APs per FlexConnect Site Tag	You can create and provision 300 APs per FlexConnect site tag on the Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches release 17.8 or later.

Feature	Description
Support for 6-GHz Radio Parameters on APs	Using the **Configure Access Points** workflow, you can configure 6-GHz radio parameters on APs.
Support for Cisco OEAP Configuration on Existing Infrastructure	You can configure Cisco Office Extend Access Point (OEAP) settings along with AP authorization lists on the existing infrastructure.
Support for Dual-Band (XOR) Radio Parameters	You can configure dual-band (XOR) radio parameters on the following APs from Cisco DNA Center: • Cisco Aironet 2800 Series Access Points • Cisco Aironet 3800 Series Access Points • Cisco Aironet 4800 Series Access Points • Cisco Catalyst 9100 Access Points

New and Changed Features in Cisco Software-Defined Access

Table 5: New and Changed Software Features in Cisco Software-Defined Access, Release 2.3.3.3

Feature	Description
Bridge-Network Virtual Machine Policy Enforcement	In the bridge mode, all virtual machines are connected by a bridge and each virtual machine (VM) is assigned a unique IP address. Every bridge-network virtual machine is individually authenticated and authorized by the Cisco SD-Access network. In addition, this release of Cisco DNA Center supports segmentation, profiling, and Assurance of wireless bridge-network virtual machines. For information on enabling **Bridge Mode VM** for a wireless IP pool, see the *Cisco DNA Center User Guide*. **Note** Support for policy enforcement is only for IPv4 bridge-network virtual machines.
Daisy Chaining Support on the Cisco Catalyst 9000 Series Switches that are configured as Extended Nodes	Cisco Catalyst 9200, 9200CX, 9200L, 9300, 9300L, 9400, 9500, and 9500H Series switches that operate Cisco IOS XE 17.8.1 (or later releases) can be configured in a daisy chain of Extended Nodes, Policy Extended Nodes, and Supplicant-based Extended Nodes. Consider the following when you deploy the Cisco Catalyst 9000 Series switches in a daisy chain topology: • A daisy chain topology can have all devices either as extended nodes or as policy extended nodes or as supplicant-based extended nodes. However, Cisco DNA Center supports one mixed topology, which is, a policy extended node that is connected to an edge node can have multiple supplicant-based extended nodes connected to it in a daisy chain, through its downlink. Apart from this topology, you cannot cascade a mix of extended node, policy extended node, and supplicant-based extended node devices. • A maximum of three devices can be connected in a daisy chain.

Feature	Description
Support for Mixed Type Extended Nodes in a Daisy Chain	You can now connect the Cisco Industrial Ethernet (IE) switches as a mix of extended node and policy extended node in a daisy chain. Consider the following guidelines before connecting the policy extended node-capable IE devices in a daisy chain: • If a device and its onboarding node are at Cisco DNA Essentials license, the device is provisioned as an extended node. • If both the device and its onboarding node are at Cisco DNA Advantage license, the device is provisioned as a policy extended node. • If a device is at Cisco DNA Advantage license but its onboarding node is at Cisco DNA Essentials license, the device is onboarded as an extended node. • If a device is at Cisco DNA Essential license but its onboarding node is at Cisco DNA Advantage license, the device is onboarded as an extended node.

Table 6: New and Changed Software Features in Cisco Software-Defined Access, Release 2.3.3.0

Feature	Description
Advertise LAN Automation Summary Route to BGP	In this release of Cisco DNA Center, if you choose to, LAN Automation can advertise the summary route for the IP pool into BGP on the primary and peer devices. A new entry in the **LAN Automation Status** > **Summary** window of the Cisco DNA Center GUI displays whether the route advertisement is enabled.
Border Node Preference Option in Fabric Site	Cisco DNA Center now provides you with an option to select a border node for your network traffic. If you have more than one border node in your fabric site, you can set a priority value for each border node. Traffic is routed through the border node that has the highest priority. Priority values range from 1 to 10 (1 is the highest priority and 10 is the lowest). By default (if you do not set the priority value), the border node is assigned a priority value of 10. If you do not set border node priority value, traffic is load balanced across the border nodes. The priority value set for a border node is applicable to all the virtual networks that are handed off from that border node. Border priority is supported for both unicast and multicast traffic. If an SD-Access Transit interconnects the fabric sites, an external border node with the highest priority is chosen to send traffic to external networks. Border node priority is supported on both LISP/BGP-based and LISP Pub/Sub-based fabric sites.

Feature	Description
Cisco Catalyst 9000 Series Switches with Cisco DNA Essentials License Configured as an Extended Node	Cisco DNA Center can now onboard a Cisco Catalyst 9000 Series switch with a Cisco DNA Essentials license as an SD-Access Extended Node. A factory-default Cisco Catalyst 9200, 9200CX, 9200L, 9300, 9300L, 9400, 9500, and 9500H Series switch that operates Cisco IOS XE 17.8.1 (or later releases) with a Cisco DNA Essentials license is configured as an extended node if it is connected to a fabric edge node. If you upgrade the license level to Cisco DNA Advantage, the Cisco DNA Center GUI gives you an option to configure the device as a policy extended node. See “Upgrade an Extended Node to Policy Extended Node” in the *Cisco DNA Center User Guide*. Consider the following license combinations on the Cisco Catalyst 9000 series devices: • A device with Network Essentials and a Cisco DNA Essentials license is configured as an extended node. • A device with Network Advantage and a Cisco DNA Advantage license is configured as a policy extended node. • A device with Network Advantage and a Cisco DNA Essentials license is configured as an extended node.
Cisco Industrial Ethernet (IE) Switches with Cisco DNA Essentials License Configured as Extended Node	Cisco Catalyst IE3200, IE3300, IE3400, IE3400H, and IE9300 Series switches, and the IE4000, IE4010, and IE5000 Series switches, with Cisco DNA Essentials license, are onboarded as SD-Access extended node. When you connect any of these factory-default switches with the Cisco DNA Essentials license to an edge node, SD-Access automation configures the switch as an extended node. If you upgrade the license level of a switch to Cisco DNA Advantage, the Cisco DNA Center GUI gives you an option to convert the switch to a policy extended node. See “Upgrade an Extended Node to Policy Extended Node” in the *Cisco DNA Center User Guide*. Consider the following license combinations on the IE devices: • A device with Network Essentials and a Cisco DNA Essentials license is configured as an extended node. • An IE3400, IE3400H, and IE9300 device with Network Advantage and a Cisco DNA Advantage license is configured as a policy extended node. • A device with Network Advantage and a Cisco DNA Essentials license is configured as an extended node.
Cisco SD-Access and Cisco ACI Integration	In this release, Cisco DNA Center adds support for integration of Cisco SD-Access and Cisco ACI. This integration securely connects the campus network with the data center network to provide end-to-end visibility and policy integration. This integration is under limited availability. For more information, see Cisco SD-Access and Cisco ACI Integration.

Feature	Description
Cisco SD-Access and ITSM Integration	In this release, Cisco DNA Center enables you to control and manage the operations of Cisco SD-Access application through ITSM (ServiceNow). Cisco SD-Access and ITSM integration primarily monitors and manages the role assignment for a device in a fabric, thus ensuring that a wrong device is not added to or removed from the fabric. The following Cisco SD-Access workflows are managed through ServiceNow: • Addition of a new device to a fabric site • Deletion of a device from a fabric site To configure Cisco SD-Access integration with ITSM, see the *Cisco DNA Center ITSM Integration Guide, Release 2.3.3*.
Cisco SD-Access User Interface Enhancements	• The **Create Fabric Site** workflow has been enhanced to include options to configure Wired Endpoint Data Collection and authentication template settings. • The options in the **Port Assignment** tab for a fabric site have been enhanced. • The options to choose an authentication template for a fabric site are now available in the **Authentication Template** tab. • The **Create Port Channel** workflow has been enhanced. • The options to configure the anycast gateway settings are now available in the **Anycast Gateway** tab. • The **Create Layer 2 Virtual Network** and **Create Layer 3 Virtual Networks** have been enhanced.
Create a Layer 2 Virtual Network	You can now create a Layer 2 virtual network without associating a Layer 3 virtual network. Traffic within the same VLAN is handled by the Layer 2 virtual network. The Cisco DNA Center GUI provides an option to hand off only a Layer 2 virtual network. This release of Cisco DNA Center supports the creation of Layer 2 virtual network only in an SD-Access wired deployment.
Overlapping IP Pools Across Virtual Networks	Cisco DNA Center allows you to choose overlapping IP pools across virtual networks for a fabric site. **Note** • Cisco DNA Center doesn't support overlapping IP pools for different sites. • Overlapping IP pools are supported only for wired endpoints with IPv4 and IPv6 addresses.
SD-Access-as-code	This release introduces APIs that help in developing customized workflows for fabric operations. Such workflows reduce the overall time to create, change, and delete fabric sites and deliver consistent outcomes for each fabric-configuration step. SD-Access-as-code enhances the fabric operations, including the essential Day-0 and Day-N tasks in creating a fabric site and enabling multicast within a site.

Feature	Description
Streamlined Cisco TrustSec Workflows for Edges and Borders	Effective with this release, CTS role-based enforcement is now the same for SD-Access edge nodes and border nodes. In earlier releases, CTS role-based enforcement is configured globally on SD-Access edge nodes only. In earlier releases, for SD-Access border nodes: • The `cts role-based enforcement` CLI is never configured on the global level. • `cts role-based enforcement vlan-list <list>` is configured when Cisco ISE authentication and Layer 2 handoffs are present. In this release, for SD-Access border nodes: • The `cts role-based enforcement` CLI is configured globally on borders if there is Cisco ISE authentication. • `cts role-based enforcement vlan-list <list>` is configured when Cisco ISE authentication and Layer 2 handoffs are present.
View REP Ring Status	The Cisco DNA Center GUI now has a view option to check the status of a REP ring. This option displays the status of the devices in the REP ring and also warns if it detects a segment failure. For information on how to check the REP ring status, see the "View REP Ring Status" procedure in the *Cisco DNA Center User Guide*.

Table 7: New Hardware Features in Cisco Software-Defined Access, Release 2.3.3.0

Device Role	Product Family	Part Number	Description
Border Node Control Plane Node Edge Node Supplicant-Based Extended Node	Cisco Catalyst 9300 Series switches	C9300LM-48UX-4Y C9300LM-48U-4Y C9300LM-48T-4Y C9300LM-24U-4Y	You can provision the Cisco Catalyst 9300 Series switch as a border node, control plane node, and edge node. It is onboarded as an extended node when it is in factory-default state and connected to an edge node.
Edge Node Extended Node Policy Extended Node	Cisco Catalyst Industrial Ethernet 9300 Rugged Series switches (IE9300)	IE-9310-26S2C IE-9320-26S2C	You can provision an IE9300 device as an edge node. When configured as an edge node, IE9300 can scale up to 32 virtual networks. You can configure an IE9300 device as an extended node or a policy extended node by connecting it to an edge node. When connected to an edge node, an IE9300 device is assigned a role based on its license level. If the device is at the Cisco DNA Essentials license level, it is onboarded as an extended node. If the device is at the Cisco DNA Advantage license level, it is onboarded as a policy extended node.

Device Role	Product Family	Part Number	Description
Edge Node Extended Node Policy Extended Node Supplicant-Based Extended Node	Cisco Catalyst 9200 Series switches	9200CX-8P-2X2G	You can provision the Cisco Catalyst 9200 Series switch as an edge node. It is onboarded as an extended node when it is in factory-default state and connected to an edge node.
Extended Node	Cisco Catalyst Industrial Ethernet 3200 Rugged Series switches (IE3200)	IE-3200-8T2S-E IE-3200-8P2S-E	IE3200 is onboarded as an extended node when it is in factory-default state and connected to an edge node.

New and Changed Features in Interactive Help

Table 8: New and Changed Features in Interactive Help, Release 2.3.3

Feature	Description
New Walkthroughs	Added the following walkthroughs: • Launch Workflows • Configure Edge Node Access Ports • Configure Global Network Servers • Create a Group-Based Access Contract • Create an IP Network Group • Create Enterprise SSID and Associate with a Network Profile • Create Group-Based Access Control Policy • Create IP-Based and URL-Based Access Control Contract • Edit IP-Based and URL-Based Access Control Policy • Gain Insights from a 3D Wireless Map

New Features in the Previous Release

To learn about the new features in the previous release, Cisco DNA Center 2.3.2, see New and Changed Information. Cisco DNA Center 2.3.2 is a Commercial Availability release. The features in 2.3.2.x are rolled up to 2.3.3.x.

Deprecated Features

Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS) provisioning use cases are deprecated. The option to provision an NFV profile has been removed from the Cisco DNA Center GUI. However, image upgrade of NFV is still supported. Also, you can still manage NFVIS devices in Cisco DNA Center by adding them manually or through Plug and Play.

Cisco DNA Center Compatibility Matrix

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

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.

Compatible Browsers

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

- Google Chrome: Version 93 or later.
- Mozilla Firefox: Version 92 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.

Note For an upgrade to Cisco DNA Center 2.3.3, we recommend that you use Chrome, not Firefox.

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 only 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(3d) for appliance model DN2-HW-APL
- Cisco IMC Version 4.1(3d) for appliance model DN2-HW-APL-L
- Cisco IMC Version 4.1(3d) 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, 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 the data collection, contact your Cisco account representative and the Cisco TAC.

Supported Hardware Appliances

Cisco delivers 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 can install Cisco DNA Center as a dedicated physical appliance purchased from Cisco with the Cisco DNA Center ISO image preinstalled. See the *Cisco DNA Center Installation Guide* for information about installation and deployment procedures.

Note Certain applications, such as 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

The following sections provide details of 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 the **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. You can generate a new certificate signing request (CSR) from **System** > **Settings** > **Trust & Privacy** > **System Certificates**. For more information, see "Update the Cisco DNA Center Server Certificate" in the Cisco DNA Center Administrator Guide.

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, if 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 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
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`
CSCwa19612	In the Web UI, there is no option to enable FIPS.
CSCwa36712	For extended nodes, a resync after reload returns a NETCONF connection failure error.
CSCwa77662	In a day-N deployment, a tunnel does not come up in some data center locations. The Cisco Catalyst 9300x supports a unique source and destination over the tunnel. Bringing up multiple tunnels with the same data center is not supported. To work around this problem, bring up only one tunnel per data center.
CSCwb19961	AP zone configuration and custom policy tag configuration on the APs are lost when AI-enhanced RRM is enabled on buildings from Cisco DNA Center. APs get configured with the Cisco DNA Center auto-generated policy tags.
CSCwb35644	When you unsubscribe an event, Cisco DNA Center platform displays the Subscription already exists error.
CSCwb66336	After Cisco DNA Center is deregistered from the cloud, Talos IP Reputation cannot be disabled.

Bug Identifier	Headline

CSCwb85208	A maglev-registry failure occurs due to a TLS issue; unable to load the private key.
	
	The Maglev registry hangs in CrashLoopBackOff state. Because the maglev-registry pod is in a crash loop, other pods don't start, because they can't retrieve their container image. An orange banner appears on the Cisco DNA Center GUI with the message, "Assurance services have been temporarily disrupted. The system is working to restore this functionality."
	
	The following error is generated:
	
	`$ maglev system_updater update_info`
	`DEPRECATION WARNING: 'maglev system_updater update_info' command will be replaced with 'maglev system_update progress' in the future`
	
	`System update status:`
	`  Version successfully installed : 1.6.706`
	`  Version currently processed    : 1.7.620`
	`    Update phase                 : Updating the core services`
	`    Update details             : Installing update package main-system-package:1.7.620. This operation would take a few minutes to complete`
	`    Progress                     : 73%`
	
	`  Updater State:`
	`    Currently processed version  : 1.7.620`
	`    State                        : INSTALLING_UPDATES`
	`    Sub-State                    : INSTALLED_HOST_COMPONENTS`
	`    Details                    : Installing update package main-system-package:1.7.620. This operation would take a few minutes to complete`
	`    Source                       : system-updater-standby`
	`    Abort pending                : Not available`

CSCwc18094	In a non-SDA environment, the CTS authorization list is not configured on the Cisco Catalyst 9800-CL. The **show environment-data command** returns blank output.
CSCwc20229	Applications are unable to receive messages from RabbitMQ. When you log in to the RabbitMQ management GUI and open the respective exchange, queue bindings are shown intermittently; otherwise, the display is empty.
CSCwc23744	Cisco DNA Center inventory reports generated for recurring are assigned with the incorrect time.
CSCwc33564	Cisco DNA Center does not push the audit log because the audit logs subscription shows only syslog servers when using the webhook destination server.
CSCwc34451	The health score for the border router goes down on the Assurance Device 360 window. The border router cannot register an EID to the local map server.
CSCwc37682	Assurance data is missing in the dashboard after a disaster recovery (DR) failover due to stack overflow.
CSCwc57363	In a DR deployment, the IPsec tunnel fails to establish after you upgrade to Cisco DNA Center 2.3.3 from an earlier release like 2.2.2.x or 2.2.3.x. The problem is due to missing kernel modules.
CSCwc58592	After upgrading from Cisco DNA Center 2.2.3.5 to 2.3.3.4, sensor SSID (CiscoSensorProvisioning) provisioning fails with the following error: `NCSP11108: Error occurred while processing the request.` There is no impact to other SSIDs.

Bug Identifier	Headline
CSCwc58712	Upgrading from Cisco DNA Center 2.3.3.3-72139 to 2.3.3.4-72142 fails with the following error: `UPGRADE_ERROR - Exception in package: automation-core, kind: ServiceBundle, name: telemetry-service - could not disable plugin for fusion_telemetry-service_log-control`
CSCwc74941	While using Mozilla Firefox, when user clicks on 'Choose a file', the files with extensions .cer and .pem are grayed out and not allowed for upload, even though it is an acceptable file. format. To workaround this problem, use Google Chrome instead of Mozilla Firefox to upload PKI cert. Another workaround is to drag and drop the file into the upload box instead of browsing via the GUI directly for Firefox.
CSCwc87283	When you generate a security advisory report for global location, Cisco DNA Center generates report with no data.
CSCwd12685	DR failover fails with `Success with Errors`. This intermittent issue can happen during any DR workflow, such as Failover, Rejoin, or Activate.
CSCwd92491	Wired client path trace fails with the error `layer 2 with a vlan,but got multiple vlans.`
CSCwe18591	`dnacaap-jsreport-service` is not supported in the legacy upgrade cluster. However, it is still visible, and an orange banner indicates that the services are disrupted.
CSCwe22715	Destination email top-level domain cannot exceed 6 characters.
CSCwe23363	When you integrate Cisco DNA Center and ServiceNow, the API call to ServiceNow in Integration Slow Summary fails.
CSCwe24274	After upgrading to version 2.3.3.5, event notification emails are not being sent from Cisco DNA Center and the event runtime logs display the following error message: `Failed to deserialize MaglevEvent from queue.`
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.
CSCwe34741	After upgrading from Cisco DNA Center 2.3.3.5 to 2.3.3.7, existing AP site tag failures occur before reprovisioning embedded wireless controllers and APs.
CSCwe36755	After upgrading to Cisco DNA Center 2.3.3.7 in a three-node cluster, collector-snmp goes to crashloop.
CSCwe42201	After upgrading Cisco DNA Center from 2.3.3.5 to 2.3.3.6, the appliance goes into a constant reboot loop. The key_manager.service indicates that TPM is in lockout mode.
CSCwe42329	After upgrading from Cisco DNA Center 2.2.2.9 to 2.3.3.7 on fabric in a box (FIAB) site, empty fabric SAVE pushes a bunch of unwanted CLIs to the box.

Bug Identifier	Headline
CSCwe44241	When you search for client details using the client user name, the result is visible in the log but does not reflect on the User Interface.
CSCwe47539	Application upgrade from Cisco DNA Center 2.2.3 to 2.3.3 fails with the following error: `Exception in package: group-based-policy-analytics.`
CSCwf73998	After powering down a node in a Cisco DNA Center High Availability environment, the node's CLI inaccurately displays some services in the `Running` state.
CSCwh06255	AP name mismatch between the wireless controller and the connected Cisco Catalyst 9300 Series switch.
CSCwh15353	After updating the AAA settings of an AAA server in Cisco DNA Center, the NAD entries update in Cisco ISE for the managed network devices.
CSCwh58183	When you update the protocol pack to version 67 in Cisco DNA Center, the update fails.

Resolved Bugs

Cisco DNA Center 2.3.3.7-72328-HF5 Hot Fix

The following table lists the resolved bugs in the Cisco DNA Center 2.3.3.7-72328-HF5 hot fix.

Note

- To obtain the hot fix, go to the **Software Management** window in the Cisco DNA Center GUI and install the 2.3.3.7-72328-HF5 hot fix. If you don't see it, scroll down and click "Looking for other releases? **Click here**."
- The 2.3.3.7-72328-HF5 hot fix is visible only if you have 2.3.3.7-72328, 2.3.3.7-72328-HF1, 2.3.3.7-72328-HF2, 2.3.3.7-72328-HF3, or 2.3.3.7-72328-HF4 installed.

Bug Identifier	Headline
CSCwb40335	Event notification is not working correctly in the site selection. Related bug: CSCwf28290.
CSCwb80779	The DHCP pool isn't created in the neighboring device after marking it for replacement in the fabric.
CSCwc08277	The topology service crashes due to running out of memory, and there is a delay in loading fabric devices.
CSCwc39603	When configuring a new event notification in Cisco DNA Center, the Try It feature for the subscribed event may return the following error: `FAILURE - 'Endpoint Connection Timed Out.`
CSCwd43073	The Device 360 windows for the wireless controller and APs connected to a site may display blank windows.
CSCwd61675	After successfully completing the Return Material Authorization (RMA) workflow for an extended node—3560CX—the device hostname and device ID do not update in Cisco ISE.

Bug Identifier	Headline
CSCwd93614	After adding a fabric in a box (FIAB) to a fabric, no other configuration preview operation is successful, such as the virtual network operations or removal from the fabric, due to the following error: `com.cisco.apic.controller.spf.api.exception.ServiceProvisioningException: NCSO10011: Error in generating CFS due to internal error. CFS Generation Failed for task id e19729ed-4ba3-4f6e-ab45-c27bd1f13aca.`
CSCwe35483	When attempting to install ThousandEyes Enterprise Agent onto devices using the Enable Apps on Switches workflow, no devices load when you select some sites.
CSCwe38622	On the **Inventory** window, the topology view doesn't display connection links for the Meraki MR52 and MR53 cloud-managed APs due to no response from the Meraki dashboard application programming interface (API) v0.
CSCwe39344	When you configure a webhook destination and REST channel, Cisco DNA Center allows you to configure only one event notification. The following error message displays when you try to create another event notification: `Endpoint Connection Timed Out.`
CSCwe39884	Auto resync may not work for SNMPv3 trap events because of the missing SNMPv3 engine ID; however, manual sync does work.
CSCwe56937	On the **Application Visibility** window, devices aren't displaying for a site and the following error is displayed: `ERROR: value too long for type character varying(255).`
CSCwe65663	Software image data for some Meraki devices is missing in the **Inventory** window where **Focus** is set to **Software Images**.
CSCwe75486	When adding a Layer 2-only pool to the fabric, the following error message may display: `NCSP11108: Error occurred while processing the request.`
CSCwe95262	When provisioning a wireless controller, it may fail with the following error message: `NCSP11108: Error occurred while processing the request.`
CSCwe95541	The Cisco DNA Center SWIM updates may become stuck in the "In Progress" state. The ongoing SWIM upgrade cannot be stopped or retriggered while it's in this state.
CSCwe95707	The distribution of the ROM Monitor (ROMMON) package to an ISR4300 router is not successful even though the GUI displays it as being successful.
CSCwf28123	The PKI configurations triggered during the Kong certificate change and fail.
CSCwf43845	After a template is added to a network profile and a device is provisioned to use the assigned template, Cisco DNA Center reports the device as out of compliance and incorrectly highlights the CLI deviations in red as an open violation.
CSCwf61346	Wireless endpoints in an anchored virtual network don't register to the anchor, multisite remote border, or guest control plane with the AireOS wireless controller, causing client connectivity issues including but not limited to DHCP and ICMP.

Bug Identifier	Headline
CSCwf68953	Cisco DNA Center may incorrectly show disk failure issues on the **System Health** window when there are no issues.
CSCwf72429	Provisioned devices are deleted if you try to delete the same set of devices again.
CSCwh04503	For Cisco DNA Center 2.3.3.7, when two network profiles have multiple VLAN ID mappings on the same VLAN name, Cisco DNA Center displays the following error when provisioning a wireless controller: `NCWL10973: Same VLAN name management cannot be mapped to multiple Local VLAN IDs 1 and 10.`
CSCwh77278	The Enable Application Telemetry feature fails after upgrading to Cisco DNA Center 2.3.3.7-72328-HF4.

Cisco DNA Center 2.3.3.7-72328-HF4 Hot Fix

The following table lists the resolved bugs in the Cisco DNA Center 2.3.3.7-72328-HF4 hot fix.

Note

- To obtain the hot fix, go to the **Software Management** window in the Cisco DNA Center GUI and install the 2.3.3.7-72328-HF4 hot fix. If you don't see it, scroll down and click "Looking for other releases? **Click here**."
- The 2.3.3.7-72328-HF4 hot fix is visible only if you have 2.3.3.x installed.

Bug Identifier	Headline
CSCwb80563	After running the Cisco DNA Center cleanup test, an ECA device cannot be removed from Cisco DNA Center. The following error is displayed: `NCIM90089: Bulk device delete failed for 1 device(s).`
CSCwb88579	The CPU and memory utilization should be inline with Grafana. The System Health Intent API (/diagnostics/system/performance) should show the correct data.
CSCwd77279	During a power down of a network device on Cisco DNA Center, the DEVICE_UNREACHABLE issue is not populated until a resync occurs, either manually or by scheduled interval.
CSCwd94093	If you have locations in United Kingdom islands, such as Isle of Man, Jersey, and Guernsey, and you create a site with that address and try to provision the wireless controller, the following error is displayed: `NCWL1033: managed locations have wrong address (Country) set.`
CSCwe10342	Cisco DNA Center SPF services may crash while previewing the configuration of a wireless controller provisioning.

Bug Identifier	Headline
CSCwe15923	Under some conditions, a newly installed, autogenerated etcd certificate in Cisco DNA Center does not get activated. When the etcd certificate does not get activated, the system might become unresponsive and inaccessible through the GUI, ultimately discarding network telemetry and losing the management capability of Cisco DNA Center. This bug affects all 2.3.3.x releases but is resolved in the 2.3.3.7-72328-HF4 hot fix. For 2.3.3.6 and earlier, we recommend that you upgrade to 2.3.5.4 or 2.3.3.7 to take advantage of the fix.
CSCwe25993	Executive Summary reports fail with the following error: `BAPI Execution Failed.Response Code = 500.`
CSCwe35694	Device provisioning hangs at the **Provision Device** window.
CSCwe39302	When onboarding new devices via LAN automation, Cisco DNA Center fails to automatically create Network Access Device (NAD) entries in Cisco ISE.
CSCwe39334	Fabric provisioning may fail with an error that states that an IP address pool has intrasubnet routing enabled. This problem occurs when onboarding a new switch to an existing fabric, and a Layer 3-only IP address pool was created previously.
CSCwe41944	Unsupported images are listed under the Cisco Catalyst 9200 Series Switches, which causes devices to go into ROMMON mode.
CSCwe46138	In a scale setup with 16 real switches, 3000 Sapro switches, and 10,000 APs, the compliance state hangs in In Progress status. The GUI doesn't let you retrigger the compliance flow.
CSCwe54433	You cannot save an RF profile in a Cisco DNA Center cluster that has been upgraded through a specific path (2.2.2.x > 2.3.3.x > 2.3.3.7 or 2.3.5.3). This problem occurs if an RF band was disabled in an RF profile in 2.2.2.x or earlier, and no operation happened on it in 2.3.3.x. The following error is displayed: `Error Permissible value of RX SOP is HIGH, MEDIUM, LOW and AUTO.`
CSCwe54540	The reachability polling schedule from the database is removed if the refresh message is not processed. As a result, Cisco DNA Center doesn't poll for the reachability status of devices in the inventory.

CSCwe57740	When trying to view the configuration preview in the **Work Items** window, the following message may appear:
	`Your role is not allowed to perform this function.`
	`If you believe this is in error, please contact your System Administrator.`
	Related bug ID: CSCwd75644.

Bug Identifier	Headline
CSCwe72149	Cisco DNA Center blocks the ability for valid IP transit handoffs to be configured for any site, signaling the following error message: `Error: BGP AS Number must be between 1 and 65535.` This problem occurs with 2.3.3.7 or 2.3.5.3 if you are using a four-byte autonomous system number (ASN) and only under certain scenarios, as described below. Steps to reproduce: This problem occurs if you are on 2.3.3.7 or 2.3.5.3 and you attempt to create a new fabric border with an ASN that is greater than 65535. The following error message is logged: `Error: BGP AS Number must be between 1 and 65535.` This problem also occurs if: **1.** You are running a release other than 2.3.3.7 or 2.3.5.3, and the local ASN on the existing fabric border is greater than 65535 (for example, 500000). **2.** Upgrade to 2.3.3.7 or 2.3.5.3. **3.** Attempt to perform operations on a fabric border that contains the higher ASN. At this point, the following error message is logged: `Error: BGP AS Number must be between 1 and 65535.`
CSCwf20392	The AP Claim workflow may leave APs configured with default site tags and location parameters.
CSCwf67040	The GUI must allow you to enable the AP location configuration during the PnP process.
CSCwf71659	LAN automation may fail for a Catalyst 9407R Sup1XL with a 40G port running IOS-XE 17.3.4. The 40G port connected to the seed device may go into an Inactive state when stopping LAN automation, causing a loss of connectivity.
CSCwf74542	Cisco DNA Center's aca-controller-service may degrade into a CrashLoopBackOff state after a node reboot.
CSCwh13321	During the PnP claim process, the AP location is shown as disabled, even though it is already enabled under the **System Settings** window.

Cisco DNA Center 2.3.3.7

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.3.7.

Bug Identifier	Headline
CSCvq31643	Fragmented SNMP Get Bulk response, causing Inventory collection to fail.
CSCvt57069	Cisco DNA Center custom portal builder settings are not saved.
CSCvw86120	The wireless controller drops CoA packets sourced from PAN instead of PSN.

Bug Identifier	Headline

CSCvy30961	The Cisco DNA Center Smart Licensing window may not load as expected. The following error is shown:
	`Error in loading data. Please see log for more info.`
	The Cisco DNA Center License Manager service logs show the following error:
	`requests.exceptions.HTTPError: 500 Server Error: Internal Server Error for url: http://x.x.x.x:8012/registration`

CSCvy82351	Provisioning device fails with the following error: `in SNMP deployconfiguration. Failed due to null.`
CSCwa78657	Device domain name check must be relaxed when comparing hostname with ThousandEyes Enterprise Agent portal.
CSCwb02969	After provisioning a Cisco Catalyst 9500 Series switch stack and fabric configuration, the state changes to "Managed Internal error" state.
CSCwb28540	After a new site is added to the primary controller, and then an AP is provisioned, the AP is down in the primary, and secondary controller provisioning is done. Then AP tags are not pushed to the secondary controller, and a tag mismatch occurs between the primary and secondary controllers. To work around this problem, reprovision the mismatched APs.
CSCwb52645	Unable to subscribe with Syslog to Assurance Event Id NETWORK-DEVICES-2-106.
CSCwb67808	New stack member not getting the closed auth config pushed down to its switchports.
CSCwb78437	When you configure ServiceNow for the first time, Configuring Basic ITSM (ServiceNow) CMDB Synchronization fails to initiate RestClient processing.
CSCwb85233	Third Party Device reported as Cisco Catalyst 9800-CL Wireless Controller for Cloud (C9800-CL-K9).
CSCwb90766	End clients cannot communicate outside, because `'map-cache ::/0 map-request'` is missing under service IPv6.
CSCwb93305	The AP refresh workflow fails with the following error: `AP already part of another AP refresh task "null"`
CSCwc05125	Wireless controller fails compliance with mismatch in "WLAN policy profile name" - PP uniqueness.
CSCwc23153	Provisioning task fails in the Cisco Catalyst 9000 Switch due to Cisco DNA Center trying to provision IOx interface TenGigabitEthernet4/0/48.
CSCwc26098	Unconfigured SSIDs seen in Assurance.
CSCwc28483	Service Entitlement check fails during image upgrade readiness check for devices in Inventory.
CSCwc28605	Telemetry provisioning failure occurs.
CSCwc32766	Layer 2 Handoff-configured VLANs are not persistent in the web interface.

Bug Identifier	Headline
CSCwc39642	Event notifications using Webex, REST, and email stop working after an upgrade. The user receives test email but not event emails. To work around this problem, do the following: **1.** Go to **Settings** > **Destination** where the email and SMTP server are configured. **2.** Take a screen shot of the existing configuration as a backup. **3.** Delete all configurations of the SMTP server, and add the same configurations. **4.** Click **Save**.
CSCwc42824	AP provisioning getting failed as Cisco DNA Center pushing duplicate commands in sequential.
CSCwc43375	The device count is out of sync unless you toggle a role change to rerun the grouping hook.
CSCwc53078	Cisco DNA Center does not archive the device configuration after device provisioning or out-of-band changes. Configuration changes are not captured in the config drift timeline graph, as Cisco DNA Center is not notified about the configuration changes by syslog.

CSCwc53593	Static port assignment from fabric host onboarding page fails with the following error:
	`Provisioning failed due to invalid request. Connected Device Type for an interface cannot be changed.`
	`To change the type, first clear the interface and then try again.`
	To work around this problem, do the following:
	1. If the Cisco DNA Center GUI and the device interface configuration for the port that is modified match, contact Cisco TAC to help identify the ports that are causing this inconsistency.
	2. After the ports are identified, clear the configurations for those ports from host onboarding.
	3. Save the changes and then reattempt port assignment for the original port.

CSCwc55872	Disabling a band on RF profile should disable the admin status on corresponding RF profile on Cisco Catalyst 9800 Series Wireless Controller.

CSCwc59647	In Cisco DNA Center, while creating a new Layer 3 virtual network, the VN comes up with an instance ID that is already in use. When trying to add the VN to the fabric, the following error is shown:
	`VirtualNetwork with same L3 Instance Id cannot be created.`
	`If this is a Multi-Cisco DNA Center environment, then clean up the previously created VirtualNetwork from Reader node.`
	`The VirtualNetwork which failed in getting created is VN_Name-Global/Site with L3 Instance ID XXXX.`

CSCwc64081	Incorrect TLD length check for Cisco ISE FQDN.
CSCwc71806	Mozilla Firefox browser has issues displaying more than six SGTs in Cisco DNA Center GUI when changing views.
CSCwc76512	The GUI does not show the correct status for the OS Update status. As a result, the user cannot upgrade network devices with a Golden Image assigned using the Device-tag.

Bug Identifier	Headline

CSCwc78766	Removing an IP address segment from a site that already has fabric configured causes the fabric site to report the following error:
	`"Failed to add IP Pool to Virtual Network. Invalid IP Pool is assigned to the Virtual Network.`
	`Please assign a valid IP Pool to the Virtual Network."`

CSCwc79851	After installing ThousandEyes on a switch, the following error is seen on the Cisco DNA Center GUI: `"Device Not Ready"`
CSCwc81083	Cannot upload the new KGV file integrity verification.
CSCwc86109	The file system shows 100% utilization. Postgres is over 230 GB in size.
CSCwc91994	AuditResource table in Postgres consuming 37G contributing to database size increase.
CSCwc95578	Scheduled report is not working for Catalyst 9000 Series devices through Cisco DNA Center.
CSCwc96964	Fabric provisioning of Cisco Catalyst 9200CX Series switches fails due to maximum supported VRFs reported as four.
CSCwd00896	AP group-related configurations are not pushed in implicit provisioning, which causes a wireless outage while resetting AAA inheritance. To work around this problem, review the configuration preview before clicking the **Deploy** button.
CSCwd02734	Addition of an IP address pool to a fabric zone fails at validation of device intent and shows the following error: `NCSP11108: Error occurred while processing the request.`
CSCwd04906	An attempt to add a building in country "Democratic Republic of the Congo" fails with error message: `NCGR10081: Invalid country detected for site - Lubumbashi.Please use ISO 3166-1 country string.`
CSCwd08474	Reprovision BAPI fails with the following error: `Interface Input Error: Duplicate IP found.`
CSCwd09391	Cisco DNA Center orchestrated app hosting gets disabled on the AP when the primary wireless controller is changed.
CSCwd13881	Cisco DNA Center shows slot 2 radio on Cisco Aironet 2800 Series Access Points.
CSCwd20910	Wired workstation client connected behind IP Phone shows up as IP_Phone in Client 360 view.
CSCwd24258	In a three-node cluster, device provisioning fails during port assignment in a Cisco SD-Access environment, during inventory provisioning, and when running a compliance check. The following error is shown: `NCS010011: Error in generating CFS due to internal error.`
CSCwd25750	The kafka pod is unable to handle data and slows down with gaps in Assurance.
CSCwd30590	Performing Fabric RMA leads to Task stuck in "In Progress".
CSCwd31345	Flexconnect ACL getting repushed on every wireless controller provisioning with same entries.

Bug Identifier	Headline
CSCwd32998	After fabric port assignment on setups with port channel created on Cisco DNA Center 2.2.2.x or earlier without selecting the connected device type, the host onboarding provisioning fails.
CSCwd33748	Cannot upload a sensor certificate to Cisco DNA Center 2.3.3.4.
CSCwd40306	After configuring an external SNMP collector, Cisco DNA Center sends the SNMP trap payload field and SNMP trap address with the external SNMP collector IP.
CSCwd40518	Cisco AireOS Wireless Controller shows internal error after upgrade and inventory logs refer to PolicyDeviceType.
CSCwd43827	Time range setting is not persistent with refresh.
CSCwd46164	After a SWIM upgrade of a Cisco Catalyst 3850 two-stacked switch from INSTALL mode, only one member switch comes up after reboot in BUNDLE mode. From the Cisco DNA Center audit logs, it was observed that incorrect commands were pushed for INSTALL mode upgrade, causing this issue.
CSCwd46613	Under notifications in **Platform** > **Developer Toolkit** > **Event Notification**, one can see different sites when switching between viewing the notification configuration and the editing of the same configuration.
CSCwd47011	No preprovisioned tags or custom tags (Flex, PolicyTag, or SiteTag) are configured on the wireless LAN controller without an AP being part of that custom tag site. If there are any preprovisioned tags or custom tags without an AP (configured before upgrade) and upgraded to Cisco DNA Center 2.3.3.7, reprovisioning the wireless LAN controller then deletes those orphan custom tags.
CSCwd48213	Cisco AireOS controller HA switch over is not been reported as an issue in Assurance dashboard Device UI.
CSCwd48297	Unable to create a non-flex AP group if at least one flex-SSID is configured.
CSCwd48939	Add wireless controller through API call fails when the control plane in the fabric site is configured with Pub/Sub.
CSCwd49502	Cisco DNA Center doesn't recognize the variable in template and hence disregards the input every alternate attempt of the provisioning of composite template.
CSCwd53101	After upgrade to Cisco DNA Center 2.3.3.5, Cisco Wireless Controller provisioning fails with the following error: `NCSP11001: User intent validation failed while processing the 'modify' request. Additional info for support: taskId: 'ae6b113b-d3ce-4cb0-8361-db00fdbe3c60'.`
CSCwd55811	After removing and re-adding the sensors to Cisco DNA Center through PnP, the Network Hierarchy window does not show the filter option to add sensors on a map floor.
CSCwd59216	Provisioning a Catalyst 9800 controller fails with the following error: `NCSP11108: Error occurred while processing the request DIV:I WirelessGrouping.`
CSCwd59876	Need to disallow user provisioning nonfabric WLAN (locally switched) on fabric wireless controller.

Bug Identifier	Headline
CSCwd60017	Assign device to site for multiple devices/sites takes long time to update inventory page.
CSCwd60859	Cisco DNA Center is sending OOB AAA details during any change in AAA server.
CSCwd62967	Cisco DNA Center sends telemetry data to the cloud for all devices, instead of just the device configured for AI-Enhanced RRM. This problem occurs if the scale of devices on Cisco DNA Center is very large, and the compute resources run out on the cloud side.
CSCwd63406	Wireless provisioning creating tasks with incorrect task hierarchy.
CSCwd63718	When provisioning an OverExtend AP as a remote telework device, Cisco DNA Center is provisioning the AP with the private IP address of the wireless controller instead of NAT IP address of the wireless controller.
CSCwd66051	On a Cisco Catalyst 9800 wireless LAN controller, the CLI command **show telemetry ietf subscription all detail** shows many subscriptions as invalid with the following error: `Notes: Subscription limit reached.` The Cisco Catalyst 9800 Series Wireless Controller has a limit of 100 subscriptions, and Cisco Prime Infrastructure uses 90 of those 100 subscriptions. To work around this problem, remove the Prime Infrastructure subscriptions from the Cisco Catalyst 9800 Series Wireless Controller and repush the telemetry from Cisco DNA Center.
CSCwd66496	Device tracking will not be pushed down to new stack-member/module interfaces.
CSCwd67809	Cisco DNA Center is removing all the VLANs from all the VLAN groups and re-adding it back, which results in WLAN flap.
CSCwd70551	Inventory reports fails with the following error: `Max running Time for worker pod exceeded. Allowed time is 16 hours.`
CSCwd74578	When attempting to learn the config from a Cisco Catalyst 9800 Series Wireless Controller, user may receive the following error: `Exception during learning device null.`

CSCwd75024	Cisco DNA Center fails to enable application telemetry on wireless LAN controllers. The network-design service logs show the following error:
	`ERROR | lemetryConfigDeployment-1 | | c.cisco.dnac.error.log.ErrorLogger | NCND02003: Exception occurred during device controllability configurations in Application Telemetry. Failed due to: Failed to configure Application Telemetry pipeline, please try again later.`
	`java.lang.Exception: Failed to configure Application Telemetry pipeline, please try again later.`

CSCwd79741	Running LAN Automation for an Edge node connected to an Edge node does not reset the seed port.
CSCwd82722	After upgrading Cisco DNA Center and attempting to provision fabric or wireless controller, the operation fails with the following error: `NCSP11108: ERROR: duplicate key value violates unique constraint "wlan_bk".`

Bug Identifier	Headline
CSCwd83022	Wireless controller provisioning failed with dbm:wireless:Same WLAN ID 22 is already present in database.
CSCwd84123	After enabling features in fabric IP pools, provisioning failure occurs on fabric devices with the following error: `Unable to push to device 1.1.1.1 using protocol ssh2 the CLI router lisp. Device Response - %No policy information` To work around this problem, enable the new fabric view, revert the change, and attempt to re-enable the desired feature.
CSCwd85866	Cisco DNA Center fails to add GPS Marker in the floor if units are in meters.
CSCwd86638	Adding a node on Cisco DNA Center 2.3.3.5 fails on an upgraded cluster.
CSCwd86714	After upgrading to Cisco DNA Center 2.3.3.5, the sticky-scheduler service is down on the Web UI.
CSCwd87238	Moving wireless functionality from one device to another requires GUI refresh even after successful provisioning.
CSCwd89482	SWIM internal calls get stuck during distribution or when triggering the image update workflow. The calls get stuck as they reach out to the external proxy configured, which causes a `404 Not found` error.
CSCwd90641	Unable to provision an AP on a single node. The following error is shown: `duplicate key value violates unique constraint "wirelessgrouping_bk"`
CSCwd91148	Cisco DNA Center applies the wrong policy tags to APs on the Catalyst 9800 Series Wireless Controller.
CSCwd91440	Cisco Catalyst 9800 Series Wireless Controller provisioning fails with an NCSP11108 error after intra upgrade.
CSCwd94157	Guest policy update fails with an error from Cisco ISE.
CSCwe00461	Unable to mark a device for replacement in case of Class B or Class A networks.
CSCwe04247	Configuration preview fails for "Closed Authentication Mode Template Update" critical fix on the fabric page.
CSCwe04848	Old SMUs are not cleared when new golden image is selected in "Get software image details" API call.
CSCwe10186	When bulk sites are selected to create fabric zones, the wrong context is set for multiple devices, which causes multicast IP lookup to fail. As a result, provisioning fails for that device. To work around this problem, select one site at a time to create fabric zones.
CSCwe12784	Secondary controller flex profile is not detected for template automation.
CSCwe15942	Upon clicking the image family name in the **Image Repository** window, it is redirecting to **Design** > **Image Repository** > **Image Families**. The image family name is displayed in the title, but no image is displayed under the image family window. It shows "No Image Found."

Bug Identifier	Headline
CSCwe17325	In a Cisco Catalyst 3850 Series Switch running in install mode, the base image gets deleted before the SMU is copied to the switch.

CSCwe19750	Provisioning a wireless controller may fail with the following error:
	`Configuration on the device failed. Error message - Unable to push configuration to device X.X.X.X.`
	`Device Response - Validation failed node-2:dbm:wireless:Configured countries do not support the channel 101.`

CSCwe44726	When you try to onboard a switch to Cisco DNA Center via Plug and Play, onboarding fails with the following error: `AP PNP Claim failed. Invalid RF-Profile: null` **Note** This bug is resolved when you install the latest 2.3.3.7 package version for the Automation – Base package.

Cisco DNA Center 2.3.3.6

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.3.6.

Bug Identifier	Headline
CSCwb57629	When adding a new device through Plug and Play, the process completes, and the State and Onboarding Progress show **Provisioned**. However, the following error message is displayed, and the device is not in the inventory: `NCOB02064: Device not added to Inventory - No CLI credentials provided` To work around this problem, delete and re-enter all the global credentials (not just CLI, but also HTTP, SNMP, and so on). Then, retry the Plug and Play process.
CSCwb78556	Software Image Management - Flash Cleanup causes `NCSW10329: Failed to perform SMU Deactivation error.`
CSCwc12097	1800S sensor may not be onboarded in Cisco DNA Center. During claim process, the following error is displayed: `The current image version (xxx) on the sensor does not allow Day-0 upgrades. Please upgrade via SWIM after successful onboarding.`
CSCwc15295	Cannot delete the device key used in the subscriberparametermapaction table.
CSCwc34749	During the software upgrade, the upgrade phase checks certificate validity. The certificate validity checks need a synchronized time source to configure the NTP server. The code which checks for higher jitter or offset values fails and results in upgrade failure.
CSCwc43113	Due to container subnet overlap with internal pods default route, the communication from a pod to other pods, services or host does not work. This results in a pod continuous restarts.
CSCwc69467	Cisco DNA Center assigning different site tags to APs in the same site.
CSCwc72410	Provisioning a wireless controller may fail with Cisco DNA Center's network-programmer service running out if its allocated Java heap.

Bug Identifier	Headline
CSCwc76362	Devices showing internal error due to `Exception while persisting: java.lang.NullPointerException`.
CSCwc78219	Cisco DNA Center pushes QoS policy for incorrect SSID.
CSCwc85038	If the system update fails at the post hook install phase, and the release upgrade is retried after the failure, the release upgrade proceeds directly to the application packages before installing the post system hooks completely.
CSCwc93896	AP and wireless controller provisioning failing due to `NCSP10001: User intent validation failed`.
CSCwc94852	Cannot provision or delete wireless controller due to `NCSP11108 CFS persistence failed`.
CSCwc98348	CoreDNS fails to resolve reverse lookups.
CSCwc98658	Cisco DNA Center may fail to provision a wireless LAN controller if a compliance operation starts around the same time as the provisioning. This appears to cause the SPF service to exhaust its memory allocation.
CSCwd06658	All the logs are not exporting to the syslog server.
CSCwd07307	The golden image is not properly updated when more than one device type is selected in the same device family.
CSCwd07407	While provisioning or updating telemetry settings on Cisco Catalyst 2960-Plus Series switches, Cisco DNA Center returns an error regarding configuring netflow, when netflow is not supported for the device.
CSCwd08429	In policy extended nodes, the web interface under Fabric > Host Onboarding > Port Assignment has no option to assign SGT value to specific ports.
CSCwd08635	Client global issue trigger does not work as expected in Cisco DNA Center.
CSCwd08919	The wireless client is not deleted, which causes a huge client count stored in ES.
CSCwd08938	Upgrading Cisco DNA Center from version 1.6.718 to 1.7.717 fails. The system shows the following error: `System update failed during INSTALLED_HOST_COMPONENTS. Updating node x.x.x.x failed Retry.`
CSCwd13230	The device list does not match the device count.
CSCwd18464	Cisco DNA Center incorrectly shows C1000-8P-2G-L as supported.
CSCwd28811	While provisioning a wireless controller with an open SSID or an SSID without assigning AAA servers, Cisco DNA Center pushes the default accounting list. To work around this problem, remove the default accounting list configuration manually until the next Cisco DNA Center provisioning.
CSCwd29909	After uploading a wireless floor map to Cisco DNA Center, the map does not populate within CMX. This is due to Cisco DNA Center sending an XML file rather than a JPG to CMX to display.
CSCwd34162	The "Apply CLI credentials for site Global" task fails.
CSCwd34763	Cisco DNA Center configures AP tags with default values, rather than the site tags configured in the Network Profile.

Bug Identifier	Headline
CSCwd35738	Cisco Secure Firewall Management Center (FMC) and Firepower Threat Defense (FTD) devices show an internal error after adding FMC in inventory.
CSCwd36456	Arbitrary file overwrite vulnerability.
CSCwd49171	After upgrading from Cisco DNA Center to 2.3.3.4, the AP count fluctuates in the Assurance dashboard. The kafka service restarts continuously.
CSCwe06947	After a power outage, the DR witness loses the configuration and restarts continuously.

Cisco DNA Center 2.3.3.5

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.3.5.

Bug Identifier	Headline
CSCwb47791	After initiating an image upgrade for the Cisco Catalyst 9300 Series switch, the switch boots with the following error: `Mainboard hardware authentication failed. Abort init ... %PMAN-3-PROCHOLDDOWN: R0/0: The process tamd_proc has been helddown (rc 134).` The Cisco Catalyst 9300 Series switch cannot be recovered.
CSCwb57463	Provisioning single RF profile causes all the access points in the site to disjoin or join.
CSCwb72776	Cisco DNA Center devices fail to sync with the following error: `org.postgresql.util.PSQLException: ERROR: duplicate key value violates unique constraint "icppolicymapaction_bk`
CSCwc10284	Cisco DNA Center deleted some of the switch running image packages during image distribution from Splunk tool.
CSCwc13096	Unable to provision AP, as postgres unable to find large object.
CSCwc18059	Provisioning Cisco Wireless Controller fails due to `StackOverflowError` when having a high number of sites and APs.
CSCwc18906	Mismatch in AAA Key configuration, resulting in provision failure after existing deployment learn and provision.
CSCwc28641	Cisco Catalyst 9300 Series stacked switch re-sync fails with "Internal Error" due to arpDetails_feature failure.
CSCwc43098	Provisioning fails on Cisco Catalyst 9800 Series Wireless Controller due to Mobility configuration.
CSCwc48881	Tri-radio mode gets enabled during AP provisioning on Cisco Wireless Controllers, which have APs that support Tri-radio mode.
CSCwc49833	Disaster Recovery: File service does not delete the purged files from mongo.
CSCwc53951	Some floors in Cisco DNA Center may not display a wireless heatmap, citing a `Matlab connection timeout` error.

Bug Identifier	Headline
CSCwc60578	Prime Data Migration tool with Cisco DNA Center: Maps migration failure for non-system campus with AP mapped to a floor.
CSCwc61000	Disaster Recovery: Re-join operation fails when witness VM tries to reconnect to disaster recovery configuration after software upgrade.
CSCwc62677	Device deletion from Cisco DNA Center's inventory fails, citing a foreign key constraint violation between vrf and ntpserverassociation.
CSCwc66513	Cisco DNA Center may set an L3 VNID to zero for infrastructure segments when a wireless device is provisioned, which results in APs disassociating from the fabric network.
CSCwc69467	Cisco DNA Center 2.3.3.3 assigns different site tags to APs in the same site.
CSCwc73983	The wireless fabric control plane IP address gets removed from the Cisco Wireless Controller following implicit provisioning.
CSCwc78951	Cisco DNA Center's Inventory service is unstable, leading to the inventory web page load slowly, or device synchronizations to take longer time to run.
CSCwc83710	Cisco DNA Center GUI shows error messages when accessing network profile advanced settings and creating custom tags.

Cisco DNA Center 2.3.3.4

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.3.4.

Bug Identifier	Headline
CSCwc17468	On Cisco DNA Center appliances with Disaster Recovery enabled, the Monitoring tab in the Disaster Recovery window displays mostly empty boxes for the Main, Recovery, and Witness sites, without the usual icons and connecting lines. Because of this, the status of the DR sites and connections is not visible by default on this window.
CSCwc47421	After upgrading to Cisco DNA Center 2.3.3.3, provisioning a Cisco Wireless Controller with wireless fabric-enabled APs causes the fabric wireless to go down. This is due to the Cisco Wireless Controller disabling the SSIDs as a fabric-enabled SSID and then disabling the APs for fabric mode. The IP pools associated to the fabric SSIDs are also cleared from host onboarding.

Cisco DNA Center 2.3.3.3

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.3.3.

Bug Identifier	Headline
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.`
CSCvy72489	An error occurs while using the Cisco DNA Center business API connector on ServiceNow.

Bug Identifier	Headline
CSCvz51440	The Switch 360 window shows incorrect interfaces from other devices.
CSCvz86051	Unable to see any devices in the ThousandEyes App Hosting workflow window. The Manage tab shows already-installed devices, but no devices are displayed 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.`
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 is displayed, and no SGTs are shown: `No options are available`
CSCwa59438	The Meraki dashboard and Firepower Management Center (FMC) show an internal error.
CSCwa78331	Multiple devices display an internal error after upgrading Cisco DNA Center to 2.2.3.4.
CSCwa82661	Port assignment in Host Onboarding does not work correctly for Cisco DNA Center 2.2.3.4.
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 Cisco SD-Access deployments to automatically push dot1x security configurations to the ports added to fabric devices.
CSCwa90857	Template provisioning of SNMP commands may fail due to special characters.
CSCwa92594	After a Cisco DNA Center upgrade, the GBP record is missing in the service manager enablement.
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.
CSCwb12871	When importing Ekahau project files, Cisco DNA Center may display the obstacle types and attenuation values differently from what is configured in the Ekahau project.
CSCwb13062	Unable to start LAN automation. The following error is displayed: `Error while reserving subnet: NCIP10288.`
CSCwb18077	Cisco DNA Center reports in PDF format shows the Coordinated Universal Time (UTC) irrespective of selected timezone.
CSCwb22802	Device provisioning on IE3x00 platforms fails with the following error: `Pki Config push failed.`
CSCwb23176	Cisco 1800S sensors become unreachable and fail to auto register with Cisco DNA Center through the PnP flow.

Bug Identifier	Headline
CSCwb27102	BPDU configurations keep pushing to the XTR switches even after the configurations are removed manually.
CSCwb27511	The wirelessgrouping entry can't be deleted, which causes Cisco Wireless Controller provisioning failure.
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.
CSCwb50439	Cisco DNA Center generates false DHCP issues for wireless clients connecting to an anchor cloud SSID.
CSCwb58855	Application Hosting turns the interface value into date format.
CSCwb68947	Unable to delete the multiple devices table snmpgroupversionsettings.
CSCwb71038	Cisco DNA Center may reuse already assigned IP addresses during LAN automation.
CSCwb73178	Disaster recovery failover hangs after you click the Pause button.

Cisco DNA Center 2.3.3.1

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.3.1.

Bug Identifier	Headline
CSCvz83872	For wireless endpoints connected as guest hosts via bridged VM, guest host IPs are not updated and guest hosts don't show as two separate endpoints with IP addresses.
CSCwa00990	For Wide Area Bonjour, restoring a NIC-bonded cluster link in three-node HA sometimes causes Service Discovery Gateway (SDG) agents to remain in inactive status. In an operational three-node cluster running the Cisco Wide Area Bonjour application, when the cluster becomes operational with only two nodes after a node is lost from the cluster or a previously lost third node becomes operational due to manual administrative actions or network malfunction, the following issue may be seen sometimes for the Wide Area Bonjour service: The status of some SDG agents in the **Monitor** > **SDG Agent** window may remain inactive, even if they were active before the incident. This issue is also reflected in Wide Area Bonjour SDG dashlet, where the state of the affected SDG agents is **Reachable**, but **Down**. Wide Area Bonjour shows the status of the services learned from these affected SDG agents as **inactive** and doesn't process queries from these SDG agents. Running the **show mdns controller summary** command on any affected SDG agent switch shows the connection state as negotiating (although a ping to the controller IP from the interface is successful). This issue doesn’t affect the operation of any other service on Cisco DNA Center.

Bug Identifier	Headline
CSCwb36994	Unable to delete any pool from an anchored virtual network that was created on an earlier release and then upgraded to Cisco DNA Center 2.2.3.4.

CSCwb61355	When you try to add an anycast gateway to the inherited site, the following error message is generated:
	`Error: Given Vlan name is already in use by Layer 2 Common Pool.`
	`Cannot use a Vlan Name used by Layer 2 Common Pool on any Fabric Site.`
	`Please choose a different Vlan name.`
	This problem occurs only if the anycast gateway at the parent site is created in Cisco DNA Center 2.2.2 and then the same anycast gateway is added to the inherited site in Cisco DNA Center 2.3.3.
	In Cisco DNA Center 2.2.2, the anycast gateway at the parent site is created with common pool = true. When the same anycast gateway is added to the inherited site in Cisco DNA Center 2.3.3, it is created with common pool = false.
	If the anycast gateway at the parent site is created in Cisco DNA Center 2.3.3, the problem does not occur when adding the anycast gateway to the inherited site.

CSCwb64910	L2VN border config removes cts enforcements for other VLANs. The condition is triggered when you have existing gateways present in the fabric and you then add one of the following: • L2VN (L2 only without IP pool but associated to an L3VN [affected device: EdgeNode]) • New flow L2VN without L3VN (affected device: EdgeNode) • L2 handoff on border (affected device: BorderNode on which L2 handoff is performed)
CSCwb81079	A Cisco DNA Center upgrade from 2.2.3.5 to 2.3.3.0 hangs at 73%.

Cisco DNA Center 2.3.3.0

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.3.0.

Bug Identifier	Headline

CSCvx52786	Cisco DNA Center may not display an IP address pool or subnet when you try to create a segment. The following errors are displayed:
	`NCIP10071: pool name can contain only alphanumeric characters, underscores and hyphens.`
	`NCIP10288: There was a failure in the ipam-service.`

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.

CSCvz14636	When Cisco DNA Center attempts to configure Application Visibility and Control (AVC) to an eight-member stack of Catalyst 9000 switches, the process may fail with the following error:
	`NBAR Error: Cannot enable Protocol-discovery - platform interface limit reached.`
	`AVC needs to restrict pushing NBAR configuration to only access switch port.`

CSCvz65062	Cisco DNA Center Inventory reports an internal error for Cisco Catalyst 9300 switches.

Bug Identifier	Headline
CSCvz70561	While adding additional edge switches to an existing fabric, Cisco DNA Center may alter the AAA configuration of an existing Cisco Wireless Controller from TACACS to RADIUS.
CSCvz87778	LAN automation fails with the following error when there are 31+ dummy pools: `Error while reserving link subnet:...`
CSCvz98644	All wireless controllers are implicitly configured when IP pools are assigned or removed from fabric WLANs on the Host Onboarding window.
CSCvz98664	Adding and removing a fabric edge provisions wireless controllers randomly with different configurations.
CSCvz99700	Unable to delete a segment from host onboarding.
CSCwa01888	IP pools are not displayed in the host onboarding under a virtual network.
CSCwa10370	A Cisco ISE node PSN added as a AAA server in Cisco DNA Center cannot be removed, even if no WLAN is using the node as AAA.
CSCwa14705	Inconsistent results are shown for the site health API.
CSCwa16652	Manually generated reports in Cisco DNA Center result in blank pages.
CSCwa18877	Ekahau file import fails with the following API error: `The specified group ID is null or empty.`
CSCwa21212	Unable to start LAN automation due to the following error: `NCND00050: An internal error occurred while processing the request.`
CSCwa21575	Supplicant-based extended node fails to onboard via Plug and Play when using the Cisco DNA Center-based onboarding flow. This behavior is seen when referencing the default ACL == AEN_MAB_ACL for use during onboarding.
CSCwa21979	Device Discovery task gets stuck in RUNNING for a long time, clogging up the inventory service, which in turn disrupts loading of global credentials.
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.
CSCwa26591	Supplicant-based extended nodes toggle between inbuilt templates, resulting in error disabled.
CSCwa29973	CTS credentials of the device are not in sync with the Cisco ISE NAD entry.
CSCwa37388	Assurance Dashboard: Rogue on Wire reports with rogue clients with broadcast addresses (all F's) should be ignored while calculating rogue on wire.
CSCwa41677	AP provisioning fails when AAA VLANs are defined and AP re-provisioning is attempted.
CSCwa43532	User intent validation failure occurs when provisioning a wireless controller.

Bug Identifier	Headline
CSCwa44338	Cisco DNA Center 2.2.2.8 displays 10+ Gbs interfaces with an interface speed of Catalyst Devices as 4,294,967,295. The interfaces on the device themselves display the correct speed. This is due to a limitation with the SNMP OID being used. Cisco DNA Center is using the ifSpeed OID (1.3.6.1.2.1.2.2.1.5). This OID has a limitation: If the bandwidth of the interface is greater than the maximum value reportable by this object, this object should report its maximum value (4,294,967,295) and ifHighSpeed must be used to report the interface's speed.
CSCwa45898	NAC is not enabled via advanced SSID Model config when pushing to two Cisco Wireless Controllers at the same time.
CSCwa46093	Cisco DNA Center may fail to create a trust-point when the system certificate contains ".local" or ".com.corp" in the common name.
CSCwa51827	The LISP key banner push fails for wireless devices in Cisco DNA Center 2.2.2.x.
CSCwa52917	A null pointer exception occurs while you try to access Show Task from the Image Repository window.
CSCwa68838	The spf-service-manager-service does not start after an upgrade to Cisco DNA Center 2.1.2.7.
CSCwa73823	Assurance Client Health window does not load when Client Data Rate dashlets are deleted.
CSCwa77904	Cisco DNA Center provisioning fails with "NCSP10246 Internal error while attempting to transform".
CSCwa87716	Template content only returns a specific value instead of the entire content.
CSCwa88686	Download of latest KGV files fails due to a certificate change on tools.cisco.com.
CSCwa90595	A Cisco Wireless Controller provisioning failure occurs due to an invalid $apMac configuration element.
CSCwb06814	System Health displays stale pxGrid information after updating the FQDN information.
CSCwb08617	Wireless controller provisioning fails with the following error: `"NCSP10250: Error During persistence (modify) of CFS & SerializedSnapshot (name: x.x.x type: DeviceInfo qualifier: null)"`
CSCwb15711	Fabric edge provisioning fails if you use a single-digit VLAN ID with sgt during pool addition in a virtual network.
CSCwb15727	During an attempt to activate the Cisco DNA Center Disaster Recovery system after registration, the DR activation workflow never completes. On the Main cluster, the "Configure active" flow completes properly, and the Main site moves to a "Waiting Standby Configuration" state. But on the "Configure standby" flow, the Configure replication step doesn't complete, leaving the Recovery site in the "Configuring Standby" state indefinitely.

Guidelines and Limitations

Cloud Connectivity Through SSL Intercept Guidelines

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 cloud endpoint, without any SSL interception device in between.

Cloud connection through an SSL intercept device is not supported and might result in connectivity failures.

Backup and Restore Guidelines

- 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** > **Authentication and Policy Servers**. From the **Actions** column, choose **Edit** corresponding to 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 that are pushed for authentication, authorization, and accounting (AAA) and configuration on the network devices. See 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 Guidelines

- ECDSA keys are not supported as either SSH keys for Cisco ISE SSH access or in the 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.

Device Onboarding Guidelines

For IE-3200-8P2S-E/A, IE-3200-8T2S-E/A, IE-3300-8P2S-E/A, and IE-3300-8T2S-E/A devices with Cisco IOS XE 17.8.1 or later, we recommend that you boot the devices in install mode before onboarding them.

If you upgrade an onboarded IE3200 or IE3300 device to Cisco IOS XE 17.8.1 or later, ensure that the device is in install boot mode before upgrading.

Upgrade Limitation

- If you are upgrading to Cisco DNA Center and all 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 GUI does not indicate that the upgrade failed to start, the logs contain messages that are 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.

License Limitations

- The Cisco DNA Center License Manager supports Smart Licensing only for wireless controller models that run Cisco IOS XE. The License Manager does not support Smart License registration of the Cisco 5500 Series AireOS Wireless Controller when the connection mode is smart proxy.
- The Cisco DNA Center License Manager does not support the following operations under **Actions** > **Manage License Reservation** for Cisco IOS 17.3.2 and later:
  - Enable License Reservation

- Update License Reservation
- Cancel/Return License Reservation
- Factory License Reservation

Fabric Limitations

- IP address pools that are reserved at the area level are shown as Inherited at the building level in the **Design** > **Network Settings** > **IP Address Pools** window. However, these IP address pools are not listed in 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 cannot be 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, the `Policy Deployment failed` message 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, AP provisioning fails when the locally switched WLANs are provisioned on the wireless controller or APs through Cisco DNA Center.

  After 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 Wireless Controller, which includes Cisco Catalyst 9800-40 Wireless Controller, Cisco Catalyst 9800-80 Wireless Controller, and Cisco Catalyst 9800-CL Cloud Wireless Controller devices.
- In Cisco DNA Center 2.3.3.7, when you export the Inventory, the export file excludes APs. In earlier Cisco DNA Center releases, all devices in the Inventory are included in the export file.
- When a wireless controller is in maintenance mode, all the associated APs are automatically placed in maintenance mode. However, you can't place the APs in maintenance mode individually if the associated wireless controller is not in maintenance mode.

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 the clients connected to a switch through an access point in bridge mode. The trunk port is used to exchange all the 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. Rogue-on-wire is not detected if IP device tracking is enabled on the trunk port. See Disabling IP Device Tracking for more information.

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, SD-Access, 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.
- LAN automation is not supported.
- Wireless controller provisioning is not supported.

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 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 to 11:00 p.m. IST, which corresponds to the time range 9:30 to 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 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
```

IP Address Manager Limitations and Workaround

- Infoblox:
  - 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 a value is configured, the value and type (IP address or FQDN) must match the configured URL in the **System** > **Settings** > **External Services** > **IP Address Manager** window.
- 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 message:

  ```
  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 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, do the following:

  1. Log in to the external IPAM server (such as BlueCat).
  2. 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.
  3. 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, do the following:

  1. Log in to the external IPAM server (such as Infoblox).
  2. 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.

3. After you regenerate the certificate with a valid CN value, go to **System** > **Settings** > **Trust & Privacy** > **Trustpool**.
4. Click **Import** and upload the new certificate (.pem file).
5. 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).

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.

Custom Application Limitation

If a custom application is configured as a part of the default bucket, Cisco DNA Center doesn't push the configuration to the managed devices.

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*
Technical references and validated solutions.	*Cisco-Validated Solution Profiles*
Use of the 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 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*