Release Notes for Cisco DNA Center, Release 2.3.7.0 and 2.3.7.3

First Published: 2023-08-11

Last Modified: 2024-04-04

Release Notes for Cisco DNA Center, Release 2.3.7.0 and 2.3.7.3

Cisco DNA Center 2.3.7.0 and 2.3.7.3 are available in a phased rollout. Until the software becomes generally available, contact your Cisco sales representative to request this release. Upon completion of the phased rollout, Cisco DNA Center will be made generally available to all customers.

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

For links to all the guides in this release, see Cisco DNA Center 2.3.7 Documentation.

Change History

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

Date	Change	Location
2024-04-04	Added information about enhancements to FlexConnect settings modifications for existing SSIDs in 2.3.7.0.	New and Changed Features in Cisco DNA Automation, on page 15
2024-03-27	Added information about email authentication support for primary and secondary SMTP servers. This feature was introduced in 2.3.7.0.	New and Changed Features in Cisco DNA Center Platform, on page 7
2024-03-21	Described the option to provide a customized loopback IP address during LAN automation. This feature was introduced in 2.3.7.0.	New and Changed Features in Cisco DNA Center, on page 4
2023-11-28	Added open bug CSCwi28419.	Open Bugs, on page 35
2023-11-22	Added the list of packages in Cisco DNA Center 2.3.7.3.	Package Versions in Cisco DNA Center, on page 2
	Added the Resolved Bugs table for 2.3.7.3.	Resolved Bugs, on page 37
	Added the Open Bugs for 2.3.7.3.	Open Bugs, on page 35
2023-09-15	Added information about enhancements to the Devices API and the Enrichment Details APIs.	New and Changed Features in Cisco DNA Center Platform, on page 7
2023-08-22	Added a limitation about the Application Policy feature and the Application Visibility feature.	Guidelines and Limitations, on page 27
2023-08-18	Added a limitation about custom applications.	Guidelines and Limitations, on page 27

Date	Change	Location
2023-08-11	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, use the Validation Tool to perform an appliance health and upgrade readiness check for Cisco DNA Center. Choose the **Appliance Infrastructure Status** and **Upgrade Readiness Status** validation sets for running preupgrade checks. For more information, see "Use the Validation Tool" in the "Configure System Settings" chapter of the *Cisco DNA Center Administrator Guide*.

Package Versions in Cisco DNA Center

Package Name	Release 2.3.7.3	Release 2.3.7.0
Release Build Version		
Release Version	2.3.7.3.70332	2.3.7.0.70488
System Updates		
System	1.7.1063	1.7.1011
System Commons	2.1.713.60610	2.1.710.60872
Package Updates		
Access Control Application	2.1.713.60610	2.1.710.60872
AI Endpoint Analytics	1.11.524	1.11.219
AI Network Analytics	3.1.23.315	3.1.20.303
Application Hosting	2.3.12309151849	2.3.12307240540
Application Policy	2.1.713.117299	2.1.710.117317
Application Registry	2.1.713.117299	2.1.710.117317
Application Visibility Service	2.1.713.117299	2.1.710.117317
Assurance - Base	2.3.7.1168	2.3.7.396
Assurance - Sensor	2.3.7.1141	2.3.7.308
Automation - Base	2.1.713.60610	2.1.710.60872
Automation - Intelligent Capture	2.1.713.60610	2.1.710.60872
Automation - Sensor	2.1.713.60610	2.1.710.60872

Package Name	Release 2.3.7.3	Release 2.3.7.0
Cisco DNA Center Docs	2.1.713.60610	2.1.710.60872
Cisco DNA Center Global Search	1.12.1.18	1.12.1.16
Cisco DNA Center Platform	1.12.241.40	1.12.1.230
Cisco DNA Center UI	1.7.5.221	1.7.5.201
Cisco Identity Services Engine Bridge	2.1.713.90102	2.1.710.80882
Cisco Umbrella	2.1.713.590143	2.1.710.590223
Cloud Connectivity - Contextual Content	2.8.1.368	2.8.1.368
Cloud Connectivity - Data Hub	1.12.9	1.12.9
Cloud Connectivity - Tethering	2.33.2.40	2.33.2.34
Cloud Device Provisioning Application	2.1.713.60610	2.1.710.60872
Command Runner	2.1.713.60610	2.1.710.60872
Device Onboarding	2.1.713.60610	2.1.710.60872
Disaster Recovery	2.1.713.360050	2.1.710.360089
Disaster Recovery—Witness Site	2.1.713.370022	2.1.710.370026
Group-Based Policy Analytics	2.3.7.16	2.3.7.10
Image Management	2.1.713.60610	2.1.710.60872
Machine Reasoning	2.1.713.210038	2.1.710.210245
NCP - Base	2.1.713.60610	2.1.710.60872
NCP - Services	2.1.713.60610	2.1.710.60872
Network Controller Platform	2.1.713.60610	2.1.710.60872
Network Data Platform - Base Analytics	2.3.7.10082	2.3.7.137
Network Data Platform - Core	1.9.3085	1.9.3069
Network Data Platform - Manager	1.9.3016	1.9.3016
Network Experience Platform - Core	2.1.713.60610	2.1.710.60872
Path Trace	2.1.713.60610	2.1.710.60872
RBAC Extensions	2.1.713.1900008	2.1.710.1900007
Rogue and aWIPS	2.9.0.26	2.9.0.17
SD-Access	2.1.713.60610	2.1.710.60872

Package Name	Release 2.3.7.3	Release 2.3.7.0
Stealthwatch Security Analytics	2.1.713.1090146	2.1.710.1090230
Support Services	2.1.713.880009	2.1.710.880043
System Remediation	1.1.0	—
Wide Area Bonjour	2.4.713.75128	2.4.710.75209

New and Changed Information

New and Changed Features in Cisco DNA Center

Table 1: New and Changed Features in Cisco DNA Center 2.3.7.3

Feature	Description
2D and 3D Wireless Heatmap Performance Enhancement	Using Cisco DNA Assurance, Cisco DNA Center delivers a performance enhancement for 2D and 3D wireless heatmaps. Cisco DNA Center displays AP and heatmap data within seconds.
Cisco Connected Mobile Experiences (CMX) Integration Enhancements	Cisco DNA Center performs validation of CMX TLS/SSL certificates. The enhanced GUI provides an option to review and import CMX certificates to establish trust for new and existing CMX integrations. To avoid interruption of service between Cisco DNA Center and CMX, configure the CMX SSL/TLS certificates and import the CMX certificate to Cisco DNA Center Trusted Certificates before installing the Cisco DNA Center 2.3.7.3 upgrade. After the upgrade, you can validate the CMX connection status under **System** > **Settings** > **Cisco Spaces/CMX Servers**.
Configuration Drift of a Device	You can view the timestamp of the last configuration that was archived for the network devices and the timestamp of the config-drift verification that was performed on the device.
Control of Configurations Support in SWIM Upgrade Workflow	With the delivery of the enhanced control of configuration changes, you can send planned software image upgrades to ITSM for approval before deploying them.
Deletion of a Stack Member from a Switch Stack	You can delete a stack member from a switch stack by using the **Delete Member** option in the PnP dashboard.
Enhancements to VLAN Creation for FlexConnect SSIDs	Effective with this release, for the FlexConnect SSIDs, VLANs are not automatically created on the Cisco Catalyst 9800 Series Wireless Controller during provisioning. Instead, the interface and VLANs that are mapped to the wireless network profile are created on the Flex profile during AP provisioning.
Floor Import History of 2D Wireless Heatmaps	You can view the floor import history of 2D wireless heatmaps, including the logs of successfully and unsuccessfully imported APs, planned APs, and overlay objects.

Table 2: New and Changed Features in Cisco DNA Center 2.3.7.0

Feature	Description
AP Join Profile Rogue Parameters Support	Cisco DNA Center supports the following rogue parameters: • Rogue detection minimum Received Signal Strength Indicator (RSSI) • Rogue detection transient interval • Rogue detection report interval • Protected Management Frame (PMF) denial
AP Location Configuration for PnP Onboarding	You can configure the site assigned during the PnP claim as the AP location for PnP onboarding.
AP Preimage Download Progress	You can view details about an AP's preimage download task for all the APs associated with the device.
Application Quality of Service (QoS) Support	Cisco DNA Center allows you to enable Application QoS policy by default on wired devices onboarded through Plug and Play or through site assignment, if you deploy QoS policy on the site to which the device is provisioned.
Application Visibility and Controller-Based Application Recognition (CBAR) Enablement on Devices	Cisco DNA Center allows you to enable Application Visibility and CBAR by default on wired discovered devices and devices onboarded through Plug and Play or through site assignment.
C9800 Day 0 Onboarding Template Support	Cisco DNA Center PnP supports an onboarding template for wireless devices.
Configurable Limit on Importing Walls from CAD Files	When importing a CAD file to use as a floor map, you can set a limit to the number of walls that are imported. Setting this limit helps to minimize the time it takes to generate a 3D heatmap.
Deletion of Nodes from REP Ring for Nonfabric Deployments	Cisco DNA Center supports dynamic deletion of nodes from a REP ring for nonfabric deployments.
Enhanced 2D Wireless Heatmap Generation	The 3D-computed heatmap generator, which is enabled by default, supports both 2D and 3D heatmap generation. Although you can disable the 3D-computed heatmap generator and use the original heatmap generator, we recommend that you use the 3D-computed heatmap generator. It can generate heatmaps substantially faster than the original heatmap generator, and you can set a limit to the number of walls that are included in a heatmap computation, which also enhances processing speed.
Enhanced Experience Enabling CX License Trials for the Security Advisories, Field Notices, and Network Bug Identifier Features	The process for enabling the Security Advisories, Field Notices, and Network Bug Identifier feature trials has been enhanced. To begin any of these feature trials, you must accept the trial terms and conditions. However, you only have to accept them once for any of the trials. Afterward, you can simply start the other feature trials.
Inventory Resync Insights	You can view the last sync start time and the reason for the last sync in your inventory.

Feature	Description
Option to Provide a Customized Loopback IP Address During LAN Automation	Under **Provision** > **LAN Automation**, when you provision LAN automation, in the **HOSTNAME MAPPING** section **>** **Discovered Devices Hostname Prefix** field, you can upload a CSV file that contains a serial number and hostname for each device. Optionally, it can also have a customized loopback IP address for each device. The ability to upload a customized loopback IP address is new in this release.
Software Image Management (SWIM) Extended Support for a Two-Way Compatibility Matrix Comparison	Cisco DNA Center SWIM performs a two-way compatibility matrix file comparison to improve In-Service Software Upgrade (ISSU) compatibility decision-making. Cisco DNA Center is able to autodownload the compatibility matrix files of ISSU-supported devices' running images and golden tagged images available in cisco.com.
Support for Operational and Planned APs in 2D Heatmaps	You can display a coverage heatmap in 2D that shows both operational and planned APs. This option is only available when the 3D-computed heatmap generator is enabled, which is the default configuration. If you disable the 3D-computed heatmap generator, the 2D heatmap reverts to the original heatmap generator and only displays operational APs or planned APs in a heatmap, not both simultaneously.
Tooltip for the Resolved IP Address	You can view the resolved IP address of a device in the **IP Address** column.
User Interface Updated for **Design** > **Network Settings** > **Network** Window	**Network Settings** > **Network** window is updated to provide better user experience.
View Cisco DNA Center in Light or Dark Appearance	You can view Cisco DNA Center in light (default) or dark appearance. On the **My Profile and Settings** > **Display Settings** window, you can apply light or dark appearance.
Visibility and Control for Compliance Remediation	While fixing compliance violations, you can send planned network configurations to IT Service Management (ITSM) for approval before deploying them.
Visibility and Control of Configurations	With the delivery of the enhanced control, you can send planned network configurations to ITSM for approval before deploying them. Control ensures that only authentic and authorized configurations are provisioned onto your network devices, which further secures your devices.

New and Changed Features in Cisco DNA Assurance

Table 3: New and Changed Features for Assurance, Release 2.3.7.3

Feature	Description
Cross-Launch from Assurance Device 360 to Device Inventory	You can cross-launch from the **Device 360** window to the **Device Inventory** window to view the device details.

Table 4: New and Changed Features for Assurance, Release 2.3.7.0

Feature	Description
Event Analytics - Preview Dashboard	You can view analytics and insights data for syslog messages and different types of network events. You can identify trends and correlate events across different data sources from the **Event Analytics - Preview** dashboard in the **Issues and Events** window. The dashboard displays heatmaps with counts of syslog messages and reachability transitions from wired and wireless devices.
Refresh Issues	The following issues are refreshed at the time of purge. Refresh time is 28 days. For each issue, the timestamp is updated so that the issue exists until the next purge cycle. • AP Disconnect • Switch Unreachable • Router Unreachable • WLC Unreachable • AP(s) disconnect from WLC on Switch
RF Insights - Tx Drops Chart	The Tx Drops per Client KPI is available for clients connected with Cisco Catalyst 9800 Series Wireless Controller starting from Release 17.12. The **RF** tab in the **Device 360** dashboard displays the **Top Clients with Tx Drops per SSID** chart with the top 5 clients with packet drop count per selected SSID for the selected radios. The **Connected** tab in the **Client 360** dashboard displays the **Tx Drops** chart, which shows the percentage of packet drops.
Third-Party Device Support for Wired Assurance	Third-party devices are supported for Wired Assurance. You can monitor and troubleshoot third-party devices from the **Network** and **Device 360** Assurance health dashboard. By default, third-party devices are mapped under the **Core** device family category. You can view issues generated by third-party devices in the **Issue Settings** dashboard.

New and Changed Features in Cisco DNA Center Platform

Table 5: New and Changed Features in Cisco DNA Center Platform, Release 2.3.7.3

Feature	Description
New APIs	
Sites API	Cisco DNA Center platform supports the following Sites API: • GET <cluster-ip>/dna/intent/api/v1/site-member/${id}/member Get devices that are assigned to a site. To access the new Sites APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Sites**.

Feature	Description
API Enhancements	

Feature	Description
taskId Datatype	In the response schema, the taskId parameter now supports the `string` datatype for the following APIs: • Update SNMPv3 credentials • Delete Device by Id • Sync Devices • Update SNMP read community • Add Device • Delete discovery by Id • Create HTTP write credentials • Start discovery • Create SNMP write community • Update global credentials • Create SNMP read community • Update HTTP read credential • Create CLI credentials • Updates an existing discovery by specified Id • Create SNMPv3 credentials • Create/Update SNMP properties • Update Device Details • Update HTTP write credentials • Update Device role • Create HTTP read credentials • Delete discovery by specified range • Update Netconf credentials • Export Device list • Run read-only commands on devices to get their real-time configuration • Delete all discovery • Delete global credentials by Id • Update CLI credentials • Update SNMP write community • Create Netconf credentials

Feature	Description
Devices API	In the Add Device API, the type request parameter now includes the `FIREPOWER MANAGEMENT CENTER` and `THIRD PARTY DEVICE` device types.
Deprecated APIs	
Network Management APIs	The following Network Management APIs are deprecated: • POST <cluster-ip>/dna/intent/api/v1/device-credential Create Device Credentials. • DELETE <cluster-ip>/dna/intent/api/v1/device-credential/${id} Delete Device Credential. • PUT <cluster-ip>/dna/intent/api/v1/device-credential Update Device Credentials. • GET <cluster-ip>/dna/intent/api/v1/device-credential Get Device Credential Details.

Table 6: New and Changed Features in Cisco DNA Center Platform, Release 2.3.7.0

Feature	Description
New APIs	
Devices API	Cisco DNA Center platform supports the following Devices API: POST <cluster-ip>/dna/intent/api/v2/networkDevices/${deviceId}/interfaces/query Get Device Interface Stats Info. The new API allows 500 requests per minute. 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**.
Sites APIs	Cisco DNA Center platform supports the following Sites APIs: • GET <cluster-ip>/dna/intent/api/v2/site Get Site V2. • GET <cluster-ip>/dna/intent/api/v2/site/count Get Site Count V2. To access the new Sites APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Sites**.

Feature	Description
Compliance APIs	Cisco DNA Center platform supports the following Compliance APIs: • GET <cluster-ip>/dna/intent/api/v1/network-device-config/task Get config task details. • POST <cluster-ip>/dna/intent/api/v1/network-device-config/write-memory Commit device configuration. To access the new Compliance APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Compliance**.
Configuration Archive API	Cisco DNA Center platform supports the following Configuration Archive API: GET <cluster-ip>/dna/intent/api/v1/network-device-config Get configuration archive details. To access the new Configuration Archive API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Configuration Archive**.
System Settings APIs	Cisco DNA Center platform supports the following System Settings APIs: • DELETE <cluster-ip>/dna/intent/api/v1/authentication-policy-servers/${id} Delete Authentication and Policy Server Access Configuration. • POST <cluster-ip>/dna/intent/api/v1/authentication-policy-servers Add Authentication and Policy Server Access Configuration. • GET <cluster-ip>/dna/intent/api/v1/ise-integration-status Cisco ISE Server Integration Status. • PUT <cluster-ip>/dna/intent/api/v1/integrate-ise/${id} Accept Cisco ISE Server Certificate for Cisco ISE Server Integration. • PUT <cluster-ip>/dna/intent/api/v1/authentication-policy-servers/${id} Edit Authentication and Policy Server Access Configuration. To access the new System Settings APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs** > **System Settings**.

Feature	Description
User and Roles APIs	Cisco DNA Center platform supports the following User and Roles APIs: • PUT <cluster-ip>/dna/system/api/v1/role Update role API. • DELETE <cluster-ip>/dna/system/api/v1/user/${userId} Delete user API. • POST <cluster-ip>/dna/system/api/v1/role Add role API. • DELETE <cluster-ip>/dna/system/api/v1/role/${roleId} Delete role API. To access the new User and Roles APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Cisco DNA Center System** drop-down list and choose **User and Roles**.
LAN Automation APIs	Cisco DNA Center platform supports the following LAN Automation APIs: • PUT <cluster-ip>/dna/intent/api/v1/lan-automation/${id} LAN Automation Stop and Update Devices. • PUT <cluster-ip>/dna/intent/api/v1/lan-automation/updateDevice LAN Automation Device Update. To access the new LAN Automation APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **LAN Automation**.
API Enhancements	
Event Management APIs	The Create Webhook Destination, Get Webhook Destination and Update Webhook Destination APIs now include the isProxyRoute attribute.

Feature	Description
Devices APIs	Cisco DNA Center platform supports the following Devices API enhancements: • Get Device list: Added the pendingSyncRequestsCount, pendingSyncRequestsCount, reasonsForDeviceResync, reasonsForPendingSyncRequests, dnsResolvedManagementAddress and lastDeviceResyncStartTime response fields. • Get the Details of Physical Components of the Given Device: Includes the new manufacturer attribute in the response schema. • Get Device Count API: Added managementIpAddress, macAddress, hostname and locationName query parameters. • Get Chassis Details for Device: The response parameters assemblyNumber, assemblyRevision are now optional. • Returns Device Interface VLANs: The mask response parameter is now an optional field. • Get Modules and Get Module Info by Id: The assemblyNumber, assemblyRevision, moduleIndex and operationalStateCode response parameters are now optional. • Get Device Values that match fully or partially an Attribute: The following sample response schema is now included. `{ "response": [ "string" ], "version": "string" }`
Compliance APIs	Multiple value support is added to the complianceStatus and complianceType attributes in the Get Compliance Detail Count and Get Compliance Detail intent APIs.
Enrichment Details APIs	For improved useability, the rate limit in the following APIs increased to 100 requests per minute: • Get Client Enrichment Details • Get Device Enrichment Details • Get Issue Enrichment Details • Get User Enrichment Details
Sites API	Get devices that are assigned to a site. Updated URL: PUT <cluster-ip>/dna/intent/api/v1/site-member/${id}/member
Deprecated APIs	

Feature	Description
Device Onboarding (PnP) APIs	The following Device Onboarding (PnP) APIs are deprecated: • GET <cluster-ip>/dna/intent/api/v1/onboarding/pnp-device/sacct/${domain}/vacct/${name}/sync-result Get Sync Result for Virtual Account. • POST <cluster-ip>/dna/intent/api/v1/onboarding/pnp-device/vacct-sync Sync Virtual Account Devices. • POST <cluster-ip>/dna/intent/api/v1/onboarding/pnp-device/unclaim Unclaim Device.
New Events	
Assurance Events	Cisco DNA Center platform supports the following new Assurance events: • High input/output utilization on Third Party Device WAN interfaces: The event is generated when there is high input or output utilization on WAN interfaces. • Fabric LISP session status on Control Plane node: The event is generated when the LISP session status from Control Plane to fabric node is down. • Fabric LISP PubSub session status is down: The event is generated when the LISP PubSub session status between border node and control or transit control plane node is down. One event is generated for each pair of border and control plane. • Fabric Border node internet is unavailable: Internet Availability monitors the default route on external borders and registers that with the control plane node within a LISP or PUBSUB site. One event is generated for each pair of border and control plane. • Fabric BGP session status is down with Peer Device: The event is generated when the BGP session is down on border node with IP Transit peer. One issue is generated for each pair of border and control plane. • Fabric Border node remote internet is unavailable: Remote Internet Availability monitors whether remote fabric sites can provide backup internet through SDA-Transit connected Borders within a LISP or PUBSUB site. One event is generated for each pair of border and control plane.
Event Enhancements	
Assurance Events	New supported connector types SNMP and NO_ENDPOINT are added to the existing Assurance events. For information about events and setting up a notification for an event, see the "Developer Toolkit GUI" chapter of the *Cisco DNA Center Platform User Guide*.
New Reports	
AI Endpoint Analytics	The **AI Endpoint Analytics** report type includes the locked Endpoint Profiling report. **Note** To unlock the report, you must install the **Cisco AI Endpoints Analytics** package from **System** > **Software Management** > **AI Endpoint Analytics**.

Feature	Description
Long Term	The **Long Term** report type includes the following types of locked reports: • AP Performance Report • Long Term AP Detail • Long Term AP Radio • Long Term AP Usage and Client Breakdown • Long Term Client Detail • Long term Client Session • Long Term Network Device **Note** To unlock the **Long Term** reports, you must enable AI Network Analytics. For more information about enabling AI Network Analytics, see the "Configure Cisco AI Network Analytics" topic in the *Cisco DNA Center Administrator Guide*.
Report Enhancements	
Flexible Reports	Cisco DNA Center platform supports the following Flexible report enhancements: • The following new options are added under **Entities**: • SWIM: Supports the **Summary** report type. • POE • A new operator-based selection criteria is included for field filters. For more information, see the "Generate a Flexible Report" topic in the "Reports" chapter of the *Cisco DNA Center Platform User Guide*.
Other Enhancements	
Email Authentication Support	This Cisco DNA Center platform release supports email authentication for primary and secondary SMTP servers while configuring an email destination to receive notifications. For more information, see the "Configure an Email Destination" topic in the "Configurations" chapter of the *Cisco DNA Center Platform User Guide*.

New and Changed Features in Cisco DNA Automation

Table 7: New and Changed Features in Cisco DNA Automation, Release 2.3.7.3

Feature	Description
Custom Policy Tag Reuse	You can reuse custom policy tags across sites (areas, buildings, and floors).

Feature	Description
Enhancements to VLAN Creation for FlexConnect SSIDs	Effective with this release, for the FlexConnect SSIDs, VLANs are not automatically created on the Cisco Catalyst 9800 Series Wireless Controllers during provisioning. Instead, the interface and VLANs that are mapped to the wireless network profile are created on the Flex profile during AP provisioning.
Global Search Support for Wireless Menu and Settings	Cisco DNA Center supports the global Search function for the wireless parameters in network settings, model configuration designs, and workflows.

Table 8: New and Changed Features in Cisco DNA Automation, Release 2.3.7.0

Feature	Description
AP Location Configuration for PnP Onboarding	You can configure the site assigned during the PnP claim as the AP location for PnP onboarding. In the **System** > **Settings** > **Device Settings** > **PnP AP Location** window: • If you check the **Configure AP Location** check box, Cisco DNA Center configures the assigned site as the AP location for PnP onboarding. • If you uncheck the **Configure AP Location** check box, Cisco DNA Center doesn't configure the AP location during PnP onboarding and you can use the **Configure Access Points** workflow to configure the AP location. This check box is unchecked by default. **Note** These settings aren't applicable for the AP provisioning or other day-*n* operations.
Detect Conflicts in a CLI Template for Wireless	Cisco DNA Center supports detection of potential design conflicts and run-time conflicts in the CLI templates for wireless. **Note** Cisco DNA Center doesn't support run-time conflict detection for Cisco Catalyst 9800 Series Wireless Controllers.
Enhancement in Handling Cisco Wireless Controller Configurations	During the reprovisioning of a Cisco Wireless Controller, Cisco DNA Center ensures not to overwrite configurations that are not part of the intent.
Enhancements to Access Control Lists for Central Web Authentication SSIDs of Guest Wireless Network	Effective with this release, Cisco DNA Center-generated preauthentication Access Control Lists (ACL) are created only for the configured AAA or PSN servers for Central Web Authentication (CWA) SSIDs of guest wireless networks.
Enhancements to Admin Status of Radio Bands in RF Profiles for Cisco AireOS Wireless Controller	Effective with this release, for Cisco AireOS Wireless Controllers, if you disable the Admin status of a band in the RF profile and reprovision the wireless controller or AP, Cisco DNA Center creates the RF profile for the corresponding band and maps it to the AP group (instead of configuring it as **None**) and disables the Admin status of all radios of the corresponding band on the APs.

Feature	Description
Enhancements to FlexConnect Settings Modifications for Existing SSIDs	If you modify any nonflex SSIDs that are already provisioned on a wireless controller to flex SSIDs (or conversely), you must reprovision the wireless controller to ensure that the expected intent is configured on the wireless controller. If you modify the VLAN ID value in the **Local to VLAN ID** field of an existing SSID and reprovision the AP without reprovisioning the wireless controller, the latest value of the VLAN ID is updated in the flex profile used by the AP. **Note** If the same flex profile is used by other APs, these APs will also have the updated local VLAN ID.
Enhancements to Associating Templates for Wireless Network Profiles	You can associate onboarding and day-*n* templates to a network profile for wireless. The onboarding templates are used while onboarding wireless devices using Plug and Play (PnP).
Enhancements to Channel Width Selection for APs in Dual Radio Mode	In earlier releases, if the dual radio mode was enabled on an AP, its slot 2 couldn't be in the **Client-Serving** or **Monitor** radio role with the 160 MHz channel width. Effective with this release, if the dual radio mode is enabled on an AP, its slot 2 can't be in the **Client-Serving** radio role with the 160 MHz channel width.
Enhancements to RF Profile Updates for Cisco AireOS Wireless Controllers	Effective with this release, for Cisco AireOS Wireless Controllers, if you modify the DCA channels or data rates for an RF profile that is already provisioned on a wireless controller, Cisco DNA Center resets the corresponding radio.
Enhancements to SSID Workflow, Preauthentication ACLs, IP-Based Access Contract, and RX SOP Threshold in RF Profiles	Cisco DNA Center supports authentication key management settings, ingress and egress QoS settings, and wireless encryption settings in the SSID creation workflow for enterprise and guest networks. **Note** When you upgrade to Release 2.3.7 from an earlier release: • For WPA3-Enterprise SSIDs, Cisco DNA Center enables the Dot1x-SHA256 authentication key management settings for the SSIDs. • For WPA2-WPA3-Enterprise SSIDs, Cisco DNA Center enables both Dot1x and Dot1x-SHA256 authentication key management settings for the SSIDs. This configuration might change the intended configuration for the Cisco AireOS Wireless Controllers and wireless controllers running Cisco IOS XE Release 17.6 or earlier. You can update the **Auth Key Management** settings for the SSIDs before reprovisioning the wireless controllers. Cisco DNA Center supports additional protocols in the preauthentication access control lists and IP-based access control contracts. Cisco DNA Center supports custom Receiver Start of Packet Detection (RX SOP) threshold values for each band for basic and AI RF profiles using the **RX-SOP Threshold (dBm) Custom Value** field.
Support for Additional WLAN Parameters	Cisco DNA Center supports additional WLAN parameters for the advanced SSID model configuration design. The SSID creation workflows for enterprise and guest networks support the selection of an advanced SSID model configuration design.

Feature	Description
Support for Manual Data Refresh to Track the Replacement Status in the AP Refresh Workflow	In the **Access Point Refresh** workflow, to view the latest AP replacement status, you can use the **Refresh Data** option. **Note** Effective with this release, Cisco DNA Center doesn't refresh the data automatically.
Support for New Country Codes	Cisco DNA Center supports new country codes for Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.12 or later. The radios within the APs are assigned to a specific regulatory domain at the factory, but the country code enables you to specify a particular country of operation within that regulatory domain. For a complete list of country codes supported per product, see https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html.
Support for Static IP Address for Wireless Management Interface During Provisioning of Cisco Catalyst 9800 Series Wireless Controller	Effective with this release, you must configure a static IP address for the wireless management interface on the Cisco Catalyst 9800 Series Wireless Controller to prevent provisioning failure.
Visibility and Control of Wireless Device Configurations	Effective with this release, Cisco DNA Center supports enhanced control for wireless device configurations. With enhanced control, you can ensure that only authentic and authorized configurations are provisioned onto your network devices through an IT Service Management (ITSM) check. By default, **Configuration Preview** is enabled and **ITSM Approval** is disabled. You can update these settings on the **System** > **Settings** > **Visibility and Control of Configurations** window. To enable **ITSM Approval**, make sure that **Configuration Preview** and ITSM are enabled. **Note** If there is a conflicting operation when you deploy your planned network configurations, the **Pending Operations** dialog box is displayed. To proceed with the current deployment, you must either wait for the existing, scheduled, or pending-review operations to complete or discard the operations.

New and Changed Features in Cisco Software-Defined Access

Feature	Description
Visibility and Control of Fabric Configurations	With the Control feature, you can send planned fabric configurations to ITSM for approval before deploying them on the fabric devices. All fabric workflows and configurations support the Visibility and Control feature.
New Automation for SD-Access	The enhanced Cisco SD-Access user interface provides a succinct view of the fabric elements and their attributes.

Feature	Description
Preprefix Affinity	Preprefix Affinity enables multihoming of a data center wherein multiple fabric sites that are linked through an SD-Access transit are connected to the same data center. In this setup, each fabric site may choose its own local internal border to reach the data center host. If a fabric site does not have local reachability to the data center, traffic is forwarded through a remote site or load balanced across multiple remote sites, if all site borders have equal priority. This behavior is enabled by default. You can also configure the traffic to be routed to a particular remote site though the data center host is reachable through the local internal border. This is helpful in deployments that require traffic to egress through a particular internal border for more efficient routing. For assistance in enabling this steering of traffic to a particular site, contact Cisco Support.
Support for AS Path Prepend	You can steer the selection of the ingress border in the SD-Access fabric by modifying the AS Path prepends. You can define the number of AS Path prepends to the BGP AS_PATH list.
Support for Wireless Mesh Access Point in an SD-Access Fabric	Starting with Cisco DNA Center Release 2.3.7, you can onboard a wireless Mesh AP in an SD-Access fabric. You can provision a mesh AP either as a Mesh Access Point (MAP) or a Root Access Point (RAP), depending on the network requirement.
Support for Workgroup Bridge	Support for the Workgroup Bridge (WGB) in Cisco SD-Access extends the fabric connectivity to areas where deploying a fabric edge, or an extended node, or a policy extended node is not possible. A WGB associates with the fabric Access Point (AP) on a fabric SSID, and the wired client connects to the Layer 2 switch positioned behind the WGB. In scenarios where a client has to be subjected to 802.1X authentication, configure the WGB to enable port-based authentication. For assistance with the configuration of WGB, contact Cisco Support.

New and Changed Features in Interactive Help

Feature	Description
New in 2.3.7.3	
New Walkthroughs	• Add a Window to My Favorites • Manage My Favorites
New in 2.3.7.0	
New Walkthroughs	• Clone a CLI Template • Create a CLI Template • Export a CLI Template • Import a CLI Template • View Field Notices
Deprecated Walkthrough	Create a Composite Template

New Features in the Previous Release

To learn about the new features in the previous release, Cisco DNA Center 2.3.6, see New and Changed Information. Cisco DNA Center 2.3.6 is a Limited Availability release. The features in 2.3.6 are rolled up to 2.3.7.

Deprecated Features

Cisco DNA Center Traffic Telemetry Appliance

Starting in 2.3.7.3, Cisco DNA Center does not support the following features for the Cisco DNA Center Traffic Telemetry Appliance:

- Plug and Play (PnP)
- Profiles
- Provision

In addition, Cisco DNA Center no longer supports the automated workflow to enable telemetry on switches.

Network Analysis Module

Starting in 2.3.7.3, you cannot integrate your Network Analysis Module (NAM) or vNAM server with Cisco DNA Center. Intelligent Capture no longer integrates with NAM or vNAM.

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 2.3.7, 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(3i) for appliance model DN2-HW-APL
- Cisco IMC Version 4.1(3i) for appliance model DN2-HW-APL-L
- Cisco IMC Version 4.1(3i) for appliance model DN2-HW-APL-XL

Update the Cisco IMC Firmware

To update your Cisco IMC firmware, first see the release notes for the corresponding release of Cisco DNA Center that you are installing. In the release notes, the “Supported Firmware” section shows the Cisco IMC firmware version for your Cisco DNA Center release.

Then, see the *Cisco Host Upgrade Utility User Guide* for instructions on updating the firmware.

In a three-node cluster configuration, we recommend that you shut down all three nodes in the cluster before updating the Cisco IMC firmware. However, you can upgrade the cluster nodes individually if that's what you prefer. See “Typical Cluster Node Operations” in the *Cisco DNA Center High Availability Guide* and follow the steps provided to shut down one or all of the nodes for maintenance.

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*.

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. Cisco collects these 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 or 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

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

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 a 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 are 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

  - Cisco Catalyst IE9300 Series with software release Cisco IOS XE 17.8.1 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.

Support for the Web Content Accessibility Guidelines 2.1 Standard

Cisco DNA Center 2.3.7 supports the Web Content Accessibility Guidelines (WCAG) 2.1 standard for the AA conformance level, with the following limitations:

Table 9: Support for WCAG 2.1 Standard

WCAG Success Criterion	Support	Limitation
1.2.4: Captions (Live)	Not Supported	—
1.2.5: Audio Description (Prerecorded)	Not Supported	—
1.3.4: Orientation	Not Supported	—
1.3.5: Identify Input Purpose	Supported	—
1.4.3: Contrast (Minimum)	Supported	—
1.4.4: Resize Text	Supported	—
1.4.5: Images of Text	Supported	—
1.4.10: Reflow	Supported	—
1.4.11: Non -Text Contrast	Supported	—
1.4.12: Text Spacing	Supported	—
1.4.13: Content on Hover or Focus	Supported	—
2.4.5: Multiple Ways	Supported	—
2.4.6: Headings and Labels	Supported	—
2.4.11: Focus Appearance (Minimum)	Supported	—
2.5.7: Dragging Movements	Partially Supported	Dashboard partially supports drag and drop due to third-party library limitations.
2.5.8: Target Size (Minimum)	Supported	—
3.1.2: Language of Parts	Supported	—
3.2.3: Consistent Navigation	Supported	—
3.2.4: Consistent Identification	Supported	—
3.3.3: Error Suggestion	Supported	—
3.3.4: Error Prevention (Legal, Financial, Data)	Not Supported	—

Exception to Support for Cisco Wide Area Bonjour

The Cisco Wide Area Bonjour application will be maintained in Cisco DNA Center Release 2.3.7. However, the Cisco Wide Area Bonjour application is not supported on the Cisco DNA Center Virtual Appliance.

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.

Note 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**. In the **Actions** column, click **Edit** adjacent to the corresponding 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 enter the CLI commands that are pushed for authentication, authorization, and accounting (AAA) and configuration on the network devices. See the corresponding 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 doesn't 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 only Automation data 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 address 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 be integrated if the ISE Admin and ISE pxGrid certificates are issued by different enterprise certificate authorities.

  Specifically, if the Cisco ISE Admin certificate is issued by *CA server A*, the Cisco ISE pxGrid certificate is issued by *CA server B*, and the pxGrid persona is running on a node other than Cisco ISE PPAN, the pxGrid session from Cisco DNA Center to Cisco ISE doesn't work.

In-Product Help Limitation

The online help and Interactive Help support light mode only. The online help and Interactive Help do not support dark mode.

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

In-Service Software Upgrade (ISSU) is not supported in Cisco SD-Access deployments.

License Limitations

- After changing the enterprise IP address or FQDN, before you attempt a licensing-related task, all services must be up and running.
- The Cisco DNA Center License Manager supports Smart Licensing only for wireless controller models that run Cisco IOS XE. The License Manager doesn't 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 doesn't 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 inherited at the building level under **Design** > **Network Settings** > **IP Address Pools**. 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 supports only native multicast across multiple fabric sites that are connected by an SD-Access transit. Head-end replication is not supported over SD-Access transit.
- Multicast routing over LISP/BGP SD-Access transit is not supported.
- Cisco Catalyst 9000 Series switches support MACsec switch-to-switch connections.

  Note We do not recommend using MACsec between switch-to-host connections in an overlay network.

  For assistance with an existing switch-to-host MACSEC implementation or a design review, contact your Cisco Sales Representative or Channel Partner.
- If you manually remove an SD-Access fabric-related CLI from the switch, Cisco DNA Center does not apply the command during normal device provisioning. You must manually add the command on the fabric node. Alternately, remove the device from the fabric, and then readd the device to the fabric.

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 doesn't learn the details about DNS, WebAuth redirect URL, and syslog.
- Cisco DNA Center can learn device configuration only once 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 doesn't consider other attributes.

High Availability Limitation

Cisco DNA Center doesn't support HA for the Cisco Embedded Wireless Controller on Catalyst Access Points.

Wireless Limitations

- If an AP is migrated after a wireless policy is created, you must manually edit the wireless policy and point the policy to an appropriate AP location before deploying the policy. Otherwise, the `Policy Deployment failed` message is displayed.
- Cisco DNA Center doesn't support the display of Bluetooth Low Energy (BLE) radios in wireless maps.

AP Limitations

- 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 the provisioning failure, the AP rejoins the wireless controller. You can reprovision the AP for a successful provisioning.
- The Cisco Catalyst 9130AXE AP with antenna C-ANT9104 doesn't support the Disable option for Dual Radio mode.
- The Cisco Catalyst 9124AXE AP doesn't support the Auto option for Dual Radio 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 Limitations

- With IPDT on trunk ports, rogue-on-wire detection is impacted. Cisco DNA Center doesn't 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 doesn't 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.

- When you add a line card to a chassis, or remove a line card from a chassis, the changes take several minutes to get updated on Cisco DNA Center. IPDT configurations, if any, are pushed to the device automatically for newly added interfaces.
- When you add a device to a stack pool, or remove a device from a stack pool, the changes take several minutes to get updated on Cisco DNA Center. IPDT configurations, if any, are pushed to the device automatically for newly added interfaces.

  To add or remove a device from the stack, you must use manual CLI configurations.

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 doesn't support IPv6.
- LAN automation is not supported.
- Adding devices to a site is supported, but provisioning is not.
- ITSM integration is not supported.
- Network profiles for wireless devices are not supported.
- Disaster Recovery is not supported.
- Cisco DNA Center does not support integration with Cisco ISE when it’s also configured for IPv6. It only supports the use of Cisco ISE as a AAA server.

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

- With Cisco DNA Center, application telemetry is not supported for Cisco Catalyst 9500 Series Switches.
- 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 the **netflow-source** command 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

- Infoblox limitations:
  - Infoblox doesn't 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.

- You may see the following error when editing an existing IPAM integration or when adding a new IPAM:

  ```
  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 the SAN field of the certificate.
  - If a value is configured, the value and type (IP address or FQDN) must match the configured URL under **System** > **Settings** > **External Services** > **IP Address Manager**.

- 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 may see the following error 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 may 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 may 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 may 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 Limitation

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.

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.

Application Policy and Application Visibility Limitation

When you provision the Application Policy feature or the Application Visibility feature from Cisco DNA Center, changes made outside these features do not reflect automatically in Cisco DNA Center. For the changes to be reflected in Cisco DNA Center, you must reprovision these features.

Third-Party Device Support Limitations

Note the following points regarding Cisco DNA Center's support of third-party devices:

- Third-party devices are defined as non-Cisco devices that support MIB-II (RFC 1213) and can be added to Cisco DNA Center.
- Cisco will not issue any new entitlements for third-party devices.
- Cisco will not update its General Terms for third-party devices.
- Third-party devices added to Cisco DNA Center have limited (visibility-only) functionality and are not supported by the Cisco TAC. If you encounter an issue with a third-party device, you'll need to contact its vendor or whoever you have a support contract with for assistance.

Bugs

Open Bugs

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

Bug Identifier	Headline
CSCwe38665	When there are many managed devices in the inventory, running the Inventory report fails and the following error is displayed: `BAPI Execution Failed.Response Code = 500, Response Content=null`
CSCwe74245	After a disaster recovery failover, CBAR provisioning fails in specific scenarios for Catalyst 9800 controllers, Catalyst 9300 switches, and Catalyst 9400 switches that have wireless enabled on them.
CSCwe85799	Cisco DNA Center three-node cluster: After removing the proxy from the setup, the node shows that connectivity with the host is lost, even though it is reachable.
CSCwf16863	In the Global LLDP configuration, if the hold time and timer values are very large, the database discards the configured values during the device sync.
CSCwf17924	Some service instances are inactive after shutting down a node in a three-node cluster.
CSCwf24189	An exception occurs during device controllability configurations.
CSCwf56037	When two site assignment tasks are created—one to assign a device to a site and the other to remove a device from a site—no conflict notification is displayed on the **Tasks** window.
CSCwf59765	Cisco DNA Center-generated preauthentication ACLs have only AAA/ISE servers mapped to a specific SSID. Cisco DNA Center ignores all other AAA servers that are added. Because this change brings the ACE's changes to the ACL rule that's already created, Cisco DNA Center repushes the complete ACL to the device. There are no WLAN flaps, but there is a change in the ACL definition.
CSCwf81439	If a task is discarded, a mismatch occurs between Cisco DNA Center and the device config for N+1 config.

CSCwf88553	Compliance remediation fails for the CBAR interface. The following error is generated:
	`NCSP11000: Error occurred while processing the 'complianceRemediation' request.`
	`Additional info for support: taskId: '71d06526-a361-471a-b66c-acc267369e6a'.`

Bug Identifier	Headline
CSCwf95418	Cisco DNA Center Basic ITSM CMDB sync might fail with a timeout error on the BAPI Schedule to Publish Inventory Details - ServiceNow Connector. To work around this problem, increase the REST and JSON Catch All Transaction Quota rule on ServiceNow to a higher timeout value, which helps the sync complete successfully.
CSCwh03807	If the CLI **prompt** command that is configured on the device contains special characters, spaces, or tabs, the device doesn't go to Managed state in Cisco DNA Center. Instead, the device remains in Syncing state in Cisco DNA Center.
CSCwh16964	The three-node cluster is stuck at 50% optional package install state.
CSCwh35302	When you assign a device with the intent for Cisco ISE integration to a site, the deployment of the device controllability and telemetry settings fails and the Cisco ISE device integration fails.
CSCwh35343	Request to add multiple wireless IP pool support for fabric SSID.
CSCwh45346	In deployments with large numbers of devices in inventory, the CMDB sync fails. The Schedule to Publish Inventory Details - ServiceNow Connector times out after around three hours.
CSCwh48163	Even after the Wide Area Bonjour application is installed and is operational, often the Tools menu does not show the Wide Area Bonjour application as a navigation option. The dashboard also does not show the Wide Area Bonjour application symbol to navigate to.
CSCwh59381	The NETWORK-NON-FABRIC_WIRELESS-1-150 REST event notification does not return key:value pairs such as tenantId, tags, and tntId.
CSCwh63005	The Cisco DNA Center inventory is not synced with Service Now. The devices count in Service Now is 0.
CSCwh88238	The Get Device Enrichment Details API does not work after upgrading Cisco DNA Center. The following error is generated: `The client made a request for a resource that does not exist, for get all devices API while enriching device information.`
CSCwh91534	Inventory report generation fails after upgrading Cisco DNA Center.
CSCwh94858	The Assurance "sdflow" service restarts unexpectedly.
CSCwh96829	The Cisco DNA Center GUI is not accessible. Most of the services are in "CrashLoopBackOff." Some services are in "CreateContainerConfigError" state.
CSCwi28259	A mobility anchor configuration pushed using the CLI template (and without choosing the force push template option) is removed after an upgrade to Cisco DNA Center 2.3.5.4. This problem occurs when you use a CLI template to configure mobility anchors and then you provision the controller without choosing the force push template option.
CSCwi28419	After upgrading from Cisco DNA Center 2.3.3.7 to Cisco DNA Center 2.3.5.4, the Cisco DNA Center intent overwrites the CLI template for the default-ap-join profile, which was initially set up to allow SSH accessto APs. Cisco DNA Center automatically generates a default APprofile using device default values, which disables SSH access.

Resolved Bugs

Cisco DNA Center 2.3.7.3

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.7.3.

Bug Identifier	Headline
CSCvt57069	Cisco DNA Center custom Portal Builder settings are not saved.
CSCwd04618	Unable to upload an image in the Guest portal via the Edit option.
CSCwd32003	Onboarding new APs reverts all APs to default-ap-profile, causing APs to reload.
CSCwd70903	Report generation fails and displays the following error: `Maximum running time for the worker pod exceeded.`
CSCwe45252	If some Assurance events are configured for notification, SNMP is shown as a channel for notification. However, Assurance events do not support SNMP and the SNMP notification does not work.
CSCwf31064	Cisco DNA Center wireless provisioning fails with an error in SiteTagInfo for the Cisco Catalyst 9800 Series Wireless Controller mesh role.
CSCwf39432	In the schema-updater log under /data/maglev/srv/diagnostics/maglev-system/workflow-worker, a number format exception occurs while running the ProfileAttributeMigrator.
CSCwf71596	In SLAAC mode, the Cisco SD-Access wireless client exhibits delayed association for the IPv6 stack.
CSCwf72802	The mobility tunnel creation peer fails via Cisco DNA Center. The following error is generated: `ERROR: duplicate key value violates unique constraint "mobilitypeerproperty_bk"`
CSCwf73918	After upgrading from Cisco DNA Center 2.3.5.4, the Cisco Catalyst 9800 Series Wireless Controller reprovision config preview fails for "Policyprofilename."
CSCwf83571	Unmarking a device for replacement via the API does not work when "faultyDeviceId" is used.
CSCwf86000	When the AP Refresh workflow card is in pending or in-progress state, it doesn't show any APs.
CSCwf87650	Cisco DNA Center may delete a PnP acquired device from inventory but the device is not deleted from PnP.
CSCwf87650	When you delete a PnP device from inventory, the device is not deleted from PnP.
CSCwf90876	Wireless controller provisioning fails for a few countries when running Cisco IOS-XE 17.9.x.
CSCwf94495	Unable to delete an edge node from the Fabric page.
CSCwh02680	When attempting to do a SWIM upgrade, a critical error is shown at the **Schedule Task** and **Clean Up** page of the workflow. The critical error states `invalid inputs`, but there are no errors on the actual page or anything to suggest what the issue is.
CSCwh07308	When switching from a fabric site to a fabric zone, the fabric site view is displayed instead of displaying the fabric zone view.

Bug Identifier	Headline
CSCwh08579	When viewing a failed port-assignment task, the browser floods with endless API calls, causing the browser to time out.
CSCwh12140	After provisioning a wireless controller, Cisco DNA Center's Compliance Report may show that device as non-compliant for Policy Tag, Site Tag, and AP Tag mappings.
CSCwh13140	A failure occurs when provisioning the Cisco Catalyst 9124AX in mesh root AP mode.
CSCwh17495	The map-server key at the inherited site under the LISP L2 instance does not match the anchored site.
CSCwh28374	An upgrade to Cisco DNA Center 2.3.5.3 fails on CommonSettingsApProfileMigrator for the AireOS AP profile with mesh settings.
CSCwh29152	WLAN Passphrase update on any personal SSID is not getting pushed to the AireOS controller.
CSCwh41361	Cisco DNA Center Inventory may degrade to Out of Memory condition due to a huge number of Base Radio records.
CSCwh49384	Cisco SD-Access: CiscoSensorProvisioning SSID mapped to wrong interface.

Cisco DNA Center 2.3.7.0

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.7.0.

Bug Identifier	Headline
CSCwb93305	The AP refresh workflow fails with the following error: `AP already part of another AP refresh task "null".`
CSCwc39603	When a user configures a new event notification in Cisco DNA Center, the **Try It** option for the subscribed event may return the following error: `FAILURE - Endpoint Connection Timed Out.`
CSCwc93896	AP and wireless controller provisioning fails due to the following error: `NCSP10001: User intent validation failed.`
CSCwd34763	Cisco DNA Center may configure AP tags with default values rather than the site tags configured in the network profile.
CSCwd48297	Cannot create a nonflex AP group if at least one flex SSID has been configured.
CSCwd50441	Failed templates get re-pushed during the port assignment process.
CSCwd53101	Wireless controller provisioning fails with an `NCSP11001` error.
CSCwd64690	The credential validation task skips validation of enabled credentials.
CSCwd64902	Several NETCONF error scenario details are lost in the NP error response (code + parameters).
CSCwd66496	When a new stack member is added to a Cisco Catalyst 9400 Series switch, Cisco DNA Center doesn't automatically push down the "device-tracking attach-policy IPDT_POLICY" configuration on new interfaces.

Bug Identifier	Headline
CSCwd77779	Editing auth template does not update CLIs on device.
CSCwd96245	The license usage details API endpoint returns the following error when using the device_type "ise": `500 Internal error.`
CSCwe10186	The wrong fabric zone is assigned for multicast pools when bulk fabric zones are created.
CSCwe14566	Cisco DNA Center's port assignment to an IE-3200 extended node fails for deployment of network intent "RouterProvisioning Failed."
CSCwe24079	License mode shows "NA" for a device in Cisco DNA Center.
CSCwe26616	The Catalyst 9410R switch and related hypervisor families don't show the correct number of devices under the family within Cisco DNA Center's Image Repository.
CSCwe27459	The banner shows an incorrect AI Endpoint Analytics warning alert for ISE integration.
CSCwe32559	The Cisco DNA Center VLAN report returns zero or one site VLAN record: `RestApiSourceExecutor - Returned Total count 0/4.`
CSCwe37500	vManage integration flaps when inventory service logs return a large XML.
CSCwe38622	Meraki MR52/MR53 cloud-managed APs don't show topology links.
CSCwe39344	While configuring event notifications for the webhook and REST channels, event notification does not work after the first attempt. The following error is generated: `Endpoint Connection Timed Out.`
CSCwe42089	The external config archive in Cisco DNA Center doesn't store files.
CSCwe43814	After upgrading to Cisco DNA Center 2.3.5.3, if you try to reprovision an AP by changing the floor (without a controller provision after upgrade), provisioning might fail.
CSCwe43877	New Policy tags and Site tags are created and mapped to the APs when APs are reprovisioned after a Cisco DNA Center upgrade, without reprovisioning the controller first.
CSCwe46169	Addition of a new IP pool under Guest VN fails with an exception. Cisco SD-Access fabric had a dedicated GUEST border deployment from an older release and is currently on a newer release which does not support GUEST border workflow.
CSCwe52889	The **Inventory** window doesn’t load correctly due to a new line character in the Meraki device's serial number.
CSCwe54433	Unable to save an RF profile in a cluster upgraded from 2.2.2.9 to 2.3.3.6 to 2.3.5.3.
CSCwe59569	Software image base and SMU distribution/activation skips the operation to perform flash cleanup.
CSCwe66749	The Meraki AP model type is not populated in the inventory.
CSCwe74038	Virtual network operation triggered wireless controller provisioning replaces WLANs but does not trigger the AP provisioning flow.
CSCwe82555	All device details are not exported in the csv and pdf file.

Bug Identifier	Headline
CSCwe89409	Image distribution fails for the Cisco 1100 Integrated Services router.
CSCwe92274	Device provisioning may fail due to other fabric devices missing loopback interfaces.
CSCwe95262	Wireless controller provisioning fails with the following error: `"NCSP11108: Error occurred while processing the request."`
CSCwe95541	The software image update gets stuck in In Progress state and does not succeed or fail.
CSCwe98803	A vulnerability in Cisco DNA Center could allow an unauthenticated, remote attacker to read and modify data in a repository that belongs to an internal service on an affected device. This vulnerability is due to insufficient access control enforcement on API requests. An attacker could exploit this vulnerability by sending a crafted API request to an affected device. A successful exploit could allow the attacker to read and modify data that is handled by an internal service on the affected device. Cisco has released software updates that address this vulnerability. There are workarounds that address this vulnerability. This advisory is available at the following link: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-ins-acc-con-nHAVDRBZ
CSCwf20392	PnP: AP claim provisioning should error out and not leave with default site tags.
CSCwf20970	The Cisco DNA Center License Manager may not show the virtual account name.
CSCwf25120	Wireless controller provisioning failure occurs when changing from a Cisco DNA Center-generated site tag to a custom site tag.
CSCwf26803	Cisco DNA Center may not send accurate emails for SYSTEM_PERFORMANCE_FILESYSTEM_UTILIZATION.
CSCwf28011	An NCSW32001 error occurs while trying to copy an image to a device using an external repository.
CSCwf29125	Cisco DNA Center's config-archive-service may decline into an out-of-memory condition and restart repeatedly.
CSCwf31445	The WLAN policy profile is not created when a new VLAN group is used in a network profile.
CSCwf31965	The nonflex WLAN policy profile is not created when an SSID is added under two network profiles using different interfaces.
CSCwf36885	After an upgrade to Cisco DNA Center 2.3.3.6, many devices inventory collection status may change to "internal error."
CSCwf38305	Rogue on the wire alerts show an incorrect connected switch.
CSCwf39680	The Add Fabric Border Device API body note should have a 4-byte ASN range, not a 2-byte ASN range.
CSCwf40854	Wireless controller provisioning may fail with the following error: `NCSP11108 CFS persistence failed.`

Bug Identifier	Headline
CSCwf45762	Cisco DNA Center disables the radios to make changes to any custom RF profile.
CSCwh58183	When you update the protocol pack to version 67 in Cisco DNA Center, the update fails.

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*

For This Type of Information...	See This Document...
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*