Release Notes for Cisco DNA Center, Release 2.3.5.x

First Published: 2022-12-21

Last Modified: 2024-03-07

Release Notes for Cisco DNA Center, Release 2.3.5.x

This document describes the features, limitations, and bugs for Cisco DNA Center, Release 2.3.5.x.

For links to all of the guides in this release, see Cisco DNA Center 2.3.5 Documentation.

Change History

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

Date	Change	Location
2024-03-07	Added information in 2.3.5.4 about enhancements to AP provisioning with modified local VLAN ID in existing SSIDs.	New and Changed Features in Cisco DNA Center, on page 5
2023-12-11	Cisco DNA Center 2.3.5.5 contains fixes for the critical issues listed in the Resolved Bugs, on page 31 list. We recommend that customers on all earlier Cisco DNA Center releases, including the 2.3.5.x releases, upgrade to Cisco DNA Center 2.3.5.5.	Resolved Bugs, on page 31
	Added the list of packages in 2.3.5.5.	Package Versions in Cisco DNA Center, Release 2.3.5.x, on page 3
2023-10-20	Added a limitation about the site hierarchy for a Rogue and aWIPS report.	Limitations and Restrictions, on page 51
2023-10-19	Added the Resolved Bugs table for the 2.3.5.4-70852-HF3 hot fix.	Resolved Bugs, on page 31
	Added the list of packages in 2.3.5.4-70852-HF3.	Package Versions in Cisco DNA Center, Release 2.3.5.x, on page 3
2023-10-12	Added the Resolved Bugs table for the 2.3.5.3-70194-HF5 hot fix.	Resolved Bugs, on page 31
	Added the list of packages in 2.3.5.3-70194-HF5.	Package Versions in Cisco DNA Center, Release 2.3.5.x, on page 3
2023-10-03	Added CSCwe98803, which is resolved in 2.3.5.4.	Resolved Bugs, on page 31

Date	Change	Location
2023-09-27	Updated the list of packages in 2.3.5.3.	Package Versions in Cisco DNA Center, Release 2.3.5.x, on page 3
2023-09-14	Added support for Cisco DNA Center on AWS, which enables you to deploy Cisco DNA Center as a virtual appliance on Amazon Web Services (AWS).	Supported Virtual Appliance, on page 24
2023-08-24	Added the list of packages in 2.3.5.4.	Package Versions in Cisco DNA Center, Release 2.3.5.x, on page 3
	Added the Resolved Bugs table for 2.3.5.4.	Resolved Bugs, on page 31
	Added the open bugs for 2.3.5.4.	Open Bugs, on page 28
2023-08-18	Added a limitation about custom applications.	Limitations and Restrictions, on page 51
2023-07-17	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.	Limitations and Restrictions, on page 51
2023-06-07	Noted that if you run Cisco DNA Center in IPv6 mode, LAN automation is not supported.	Limitations and Restrictions, on page 51
2023-05-19	Added information about using the Validation Tool to run preupgrade checks.	Upgrade to the Latest Cisco DNA Center Release, on page 2
2023-05-08	Added the list of packages in 2.3.5.3.	Package Versions in Cisco DNA Center, Release 2.3.5.x, on page 3
	Added the Resolved Bugs table for 2.3.5.3.	Resolved Bugs, on page 31
	Added the list of new walkthroughs for 2.3.5.3.	New and Changed Features in Interactive Help, on page 19
	Explained the licensing changes in 2.3.5.3.	Licensing Changes, on page 20
	Added a limitation about In-Service Software Upgrade (ISSU).	Limitations and Restrictions, on page 51
2022-12-21	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, Release 2.3.5.x

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

Package Name	Release 2.3.5.5	Release 2.3.5.4		Release 2.3.5.3		Release 2.3.5.0
Release Build Version						
Release Version	2.3.5.5.70026	2.3.5.4-70852-HF3	2.3.5.4.70852	2.3.5.3-70194-HF5	2.3.5.3.70194	2.3.5.0.70586
System Updates						
System	1.7.1013	1.7.1013		1.7.905		1.7.832
System Commons	2.1.616.60023	2.1.614.61521		2.1.613.61093		2.1.610.60911
Package Updates						
Access Control Application	2.1.616.60023	2.1.614.61521		2.1.613.61093		2.1.610.60911
AI Endpoint Analytics	1.9.823	1.9.805		1.9.704		1.9.613
AI Network Analytics	2.11.27.394	2.11.27.394		2.11.24.376		2.11.19.356
Application Hosting	2.1.02307250922	2.1.02307250922		2.1.02304051333		2.1.02212150608
Application Policy	2.1.616.117003	2.1.614.117979		2.1.613.170209		2.1.610.117535
Application Registry	2.1.616.117003	2.1.614.117979		2.1.613.170209		2.1.610.117535
Application Visibility Service	2.1.616.117003	2.1.614.117979		2.1.613.170209		2.1.610.117535
Assurance - Base	2.3.5.475	2.3.5.475		2.3.5.329		2.3.5.271
Assurance - Sensor	2.3.5.408	2.3.5.408		2.3.5.312		2.3.5.269
Automation - Base	2.1.616.60023	2.1.614.61521		2.1.613.61121	2.1.613.61093	2.1.610.60911
Automation - Intelligent Capture	2.1.616.60023	2.1.614.61521		2.1.613.61093		2.1.610.60911
Automation - Sensor	2.1.616.60023	2.1.614.61521		2.1.613.61093		2.1.610.60911
Cisco DNA Center Global Search	1.10.1.11	1.10.1.11		1.10.1.11		1.10.1.11
Cisco DNA Center Platform	1.10.1.188	1.10.1.188		1.10.1.143		1.10.1.103
Cisco DNA Center UI	1.7.3.292	1.7.3.292		1.7.3.277		1.7.3.236
Cisco Identity Services Engine Bridge	2.1.614.510	2.1.614.510		2.1.610.476		2.1.610.476

Package Name	Release 2.3.5.5	Release 2.3.5.4	Release 2.3.5.3		Release 2.3.5.0
Cisco Umbrella	2.1.614.590510	2.1.614.590510	2.1.613.590114		2.1.610.590253
Cloud Connectivity - Contextual Content	2.6.1.350	2.6.1.350	2.6.1.350		2.6.1.350
Cloud Connectivity - Data Hub	1.10.48	1.10.48	1.10.47		1.10.40
Cloud Connectivity - Tethering	2.31.1.55	2.31.1.55	2.31.1.53		2.31.1.43
Cloud Device Provisioning Application	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
Command Runner	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
Device Onboarding	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
Disaster Recovery	2.1.614.360049	2.1.614.360049	2.1.613.360017		2.1.610.360079
Disaster Recovery—Witness Site	2.1.614.370026	2.1.614.370026	2.1.613.370006		2.1.610.370032
Group-Based Policy Analytics	2.3.5.30	2.3.5.30	2.3.5.27		2.3.5.27
Image Management	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
Machine Reasoning	2.1.616.210007	2.1.614.210567	2.1.613.210134		2.1.610.210377
NCP - Base	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
NCP - Services	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
Network Controller Platform	2.1.616.60023	2.1.614.61521	2.1.613.61121	2.1.613.61093	2.1.610.60911
Network Data Platform - Base Analytics	2.3.5.97	2.3.5.97	2.3.5.44		2.3.5.32
Network Data Platform - Core	1.9.1078	1.9.1078	1.9.1039		1.9.1011
Network Data Platform - Manager	1.9.1013	1.9.1013	1.9.1013		1.9.1010
Network Experience Platform - Core	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
Path Trace	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
RBAC Extensions	2.1.614.1900017	2.1.614.1900017	2.1.613.1900011		2.1.613.1900008
Rogue and aWIPS	2.7.0.46	2.7.0.46	2.7.0.41		2.7.0.36

Package Name	Release 2.3.5.5	Release 2.3.5.4		Release 2.3.5.3		Release 2.3.5.0
SD-Access	2.1.616.60023	2.1.614.61521		2.1.613.61121	2.1.613.61093	2.1.610.60911
Stealthwatch Security Analytics	2.1.616.1090003	2.1.614.1090427		2.1.613.1090136		2.1.610.1090258
Support Services	2.1.614.880027	2.1.614.880027		2.1.613.880003		2.1.610.880024
System Remediation	1.0.51	1.0.2	—	1.0.2	—	—
Wide Area Bonjour	2.4.614.75573	2.4.614.75573		2.4.610.75310		2.4.610.75310

New and Changed Information

New and Changed Features in Cisco DNA Center

Table 1: New and Changed Features for Cisco DNA Center, Release 2.3.5.5

Feature	Description
Recommended Release	Cisco DNA Center 2.3.5.5 contains fixes for critical issues. We recommend that customers on all earlier Cisco DNA Center releases, including the 2.3.5.x releases, upgrade to Cisco DNA Center 2.3.5.5.
Enhancements to Default AP Profiles During Upgrade	In earlier releases, the default AP profile was pushed to the wireless controller during upgrade. When you upgrade to this release from an earlier version, by default, Cisco DNA Center doesn't push the default AP profile to the wireless controller. To update the default AP profile on the wireless controller, you must explicitly save it on the **Design** > **Network Settings** > **Wireless** > **AP Profiles** window. After you save the default AP profile, if there is a difference between the current wireless controller configuration and the AP profile configuration saved on Cisco DNA Center, the default AP profile is pushed to the wireless controller during subsequent reprovisioning.

Table 2: New and Changed Features for Cisco DNA Center, Release 2.3.5.4

Feature	Description
Ability to Assign Ports for Uplink Ports	Effective with this release, you can assign ports for the uplink ports. Choose **Provision** > **Fabric Sites** and click the fabric site. Under **Host Onboarding** > **Port Assignment**, assign ports for the uplink ports. In earlier releases, you could assign ports for the uplink ports only for extended node devices.

Feature	Description
AP Location Configuration for PnP Onboarding	Effective with this release, 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.
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 Controllers	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.
Enhancements to AP Provisioning with Modified Local VLAN ID for Existing SSIDs	In earlier releases, when the VLAN ID value in the **Local to VLAN ID** field of an existing SSID was modified and the AP was reprovisioned without reprovisioning the wireless controller, the site tag for the AP was changed to the default site tag. Effective with this release, when 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 RF Profile Updates for Cisco AireOS Wireless Controllers	In earlier releases, for Cisco AireOS Wireless Controllers, if you modify any configuration in an RF profile that is already provisioned on a wireless controller, Cisco DNA Center resets the corresponding radio. 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.
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.

Feature	Description
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.

Table 3: New and Changed Features for Cisco DNA Center, Release 2.3.5.3

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 Accounting Server Configuration	Effective with this release, you must configure an accounting server for an SSID to push the accounting configuration for the SSID.
Enhancements to AP Configuration Workflow	The **Configure Access Points** workflow has the following enhancements: • The **Antenna Name** parameter has been replaced with the **Antenna Gain** parameter. The antenna name selected in this workflow isn't reflected in wireless maps. • The **AP Height**, **Azimuth**, and **Elevation** parameters have been removed. You can configure these parameters in the **Design** > **Network Hierarchy** window. • You can select a maximum of 2000 sites in the **Select Access Points** 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 Application Hosting on APs	When the **App Hosting Status** of an AP is **Ready**, to configure the updates on the AP, you can use the **Resync** option.
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.
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 must 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 you don't need the RF profile updates during the wireless controller reprovisioning, you can check the **Skip AP Provision** check box.

Feature	Description
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 2.3.5.3 from Release 2.3.3.6 or earlier, 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 4: New and Changed Features for Cisco DNA Center, Release 2.3.5.0

Feature	Description
Advanced WLAN Parameters Configuration Support for Enterprise and Guest Wireless Networks	You can configure the following advanced WLAN parameters while creating SSIDs for enterprise and guest wireless networks: • **AAA Override** • **Configure MPSK** • **Protected Management Frame (802.11w)** • **Coverage Hole Detection**
Basic RF Profile and AI RF Profile Enhancements	You can configure the following settings for basic radio frequency (RF) profiles: • Coverage hole detection • Flexible Radio Assignment (FRA) • 802.11ax You can configure the following settings for AI RF profiles: • Coverage hole detection • 802.11ax

Feature	Description
Cisco DNA Center Journey Map	The Cisco DNA Center journey map shows various capabilities provided by Cisco DNA Center and its usage.
Client Rate Limit Configuration Support for Enterprise and Guest Wireless Networks	You can configure the client rate limit on Cisco IOS XE devices while creating SSIDs for enterprise and guest wireless networks.
Compliance Support Extended for Cisco Umbrella	You can check compliance for switches or Cisco Embedded Wireless Controllers configured with Cisco Umbrella. You can view any violations under **Workflow** in the **Compliance Summary** window.
Compliance Support Extended for Network Settings	You can check compliance for device network settings. You can view any violations under **Network settings** in the **Compliance Summary** window.
Detect Conflicts in a CLI Template	You can detect potential design conflicts and run-time conflicts in the CLI templates for switching, SD-Access, and fabric.
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.
Exclude Interfaces in Application Visibility Service Enablement	You can exclude or include interfaces in the Application Visibility service enablement.
Fix Compliance Violations	Cisco DNA Center provides you with an automated fix for device compliance violations that are identified during a compliance run.
HTTPS Protocol Support for Software Image Management	HTTPS protocol support is extended for software image management on Cisco Embedded Wireless Controllers.
PSC Enforcement Support for RF Profiles	You can enable Preferred Scanning Channel (PSC) enforcement for the 6-GHz radio type for basic RF profiles and AI RF profiles.
Resilient Ethernet Protocol (REP) Ring Device Support (Nonfabric)	REP Ring support for nonfabric devices is extended for S5800.
Support for AP Authorization Configuration	You can configure a list of authorized APs. You can configure local and AAA authorization for APs using their MAC address, serial number, or both.
Support for AP Power Profiles	You can create AP power profiles for Cisco Wireless Controllers running Cisco IOS XE Release 17.10.1 and later. You can assign the AP power profile to APs by associating it with an AP profile. You can define multiple rules for the AP power profile and specify the sequences of the rules.

Feature	Description
Support for Custom AP Profiles	AP profiles consolidate the AP authentication settings, aWIPS, rogue management, and mesh settings. AP profiles allow you to manage and provision APs. Cisco DNA Center provides a default AP profile for Cisco IOS XE devices and Cisco AireOS devices. You can create custom AP profiles for Cisco IOS XE devices and Cisco AireOS devices. **Note** If there are any out-of-band custom AP profiles that are created directly on the wireless controller and used with Cisco DNA Center running earlier than Release 2.3.5, ensure that you create a custom AP profile on Cisco DNA Center with same name and map it to the custom site tag to retain the configuration.
Support for Reuse of AP Groups and Flex Groups Within an Area	While creating a network profile for wireless, you can use the same AP group and flex group across sites (buildings or floors) within an area.
Template Hub	You can filter CLI templates based on Project Name, Template Language, Device Family, Device Series, Commit State, and Provision Status from **Tools** > **Template Hub**. You can attach the CLI template to network profiles in the **Template Hub** window. You can also create a new network profile.

New and Changed Features in Cisco DNA Assurance

Feature	Description
AI-Enhanced RRM Enhancements - FRA Support	Cisco DNA Center displays the **FRA Changes** dashlet in the **AI-Enhanced RRM** dashboard. This new dashlet displays the total number of Flexible Radio Assignment (FRA)-capable and FRA-enabled radios for the following modes: • 2.4-GHz radio • 5-GHz radio • Monitor
Automatic Issue Resolution	With this release, the system automatically resolves the following issue types: • Stack Port Link has failed • Stack Member Removal
Cisco SD-Access Assurance - Fabric KPI Enhancements	With this release, the following Fabric Site KPIs are included: • **CTS Environment Data Download** • **BGP Session from Border to Peer Node for INFRA VN** • **BGP Session from Border to Control Plane**
Cisco SD-Access Assurance - Transits KPI Enhancements	With this release, the following Transits KPIs are included: • **BGP Session from Border to Transit Control Plane**

Feature	Description
Cisco SD-Access Assurance - VN Services KPI Enhancements	With this release, the following VN Services KPIs are included: • **BGP Session from Border to Peer Node** • **Remote Internet Availability**
Client-360 Dashboard Enhancements	In the **Summary** dashboard on the Client-360 window, you can view a list of onboarding, roaming, and connectivity issues for a particular client. You can click the hyperlinked issues to view details about the issue the client experienced at a specific location.
DHCP Dashboard Enhancement	You can view a breakdown of DHCP failures, such as DHCP decline and DHCP Negative Acknowledgment (NACK). These failures are also displayed in the Event Viewer in the **Client-360** window.
DNS Dashboard	You can view and monitor all the DNS server transactions reported by wireless controllers in your network. **Note** If your network contains existing devices with application telemetry enabled, you must disable and then re-enable application telemetry before you can see any data in the DNS dashboard.
Enhanced Site Analytics	The KPIs on the Site Analytics Health Dashboard window are subdivided into more granular data points. Onboarding now shows both onboarding attempts and onboarding duration. Roaming shows both roaming attempts and roaming duration.
Flex/Fabric mode support for Application Experience	From this release, Application Experience supports Flex/Fabric mode on Cisco 9800 Series Wireless Controllers.
Issue Notes	You can add a comment, such as the TAC case number or other information, to an issue.
Issue Resolution	You can view whether an issue is resolved automatically or manually. In the **Issue Settings** > **Global Profile** window, the **Issue Resolution** column displays either **Auto** for issues that are resolved by the system or **Manual** for issues that you must resolve.
PSC Enforcement Insights for 6-GHz Radio Band	Cisco DNA Center displays the Preferred Scanning Channel (PSC) enforcement configuration recommendations for the 6-GHz radio band in the **Insights** dashlet of the **AI-Enhanced RRM** dashboard.
Support for ThousandEyes Integration	With this release, the following types of ThousandEyes agent tests are supported: • Network agent-to-agent test: Collects network data, including jitter, packet loss, and latency. • Voice RTP test: Collects Mean Opinion Score (MOS), packet loss, latency, and Packet Delay Variation (PDV).
User-Defined Issue Settings	You can create new issues based on the syslog details.

New and Changed Features in Cisco DNA Center Platform

Feature	Description
New API Changes	
Wireless API	Starting in 2.3.5.3, the Cisco DNA Center platform no longer supports `configureApHeight`, `apHeight`, `configureElevAngleDegree`, `antennaElevAngleDegree`, `antennaElevAngleSign`, `configureAntennaDegree`, and `antennaDegree` parameters in the following wireless API: POST<cluster-ip>/dna/intent/api/v1/wireless/accesspoint-configuration **Note** When you configure `antennaName`, the Cisco DNA Center platform configures only the antenna gain using this attribute. The Cisco DNA Center platform doesn't configure the antenna pattern using this attribute. In response, the GET<cluster-ip>/dna/intent/api/v1/wireless/accesspoint-configuration API returns default values for the following attributes: • `antennaElevAngle`: The API returns the value `0` for this attribute. • `antennaPatternName`: The API returns the value `null` for this attribute. • `apHeight`: The API returns the value `0` for this attribute. • `antennaAngle`: The API returns the value `0` for this attribute. To access the new **Wireless** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Connectivity** drop-down list and choose **Wireless**.
New API Features	
Devices APIs	The Cisco DNA Center platform supports the following **Devices** APIs for rogue additional details: • POST<cluster-ip>/dna/intent/api/v1/security/rogue/additional/details/count Rogue Additional Detail Count. • POST<cluster-ip>/dna/intent/api/v1/security/rogue/additional/details Rogue Additional Details. 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**.

Feature	Description
Discovery API	The Cisco DNA Center platform supports the following **Discovery** APIs for rogue additional details: • DELETE<cluster-ip>/dna/intent/api/v2/global-credential/${id} Delete Global Credential V2. • GET<cluster-ip>/dna/intent/api/v2/global-credential Get All Global Credentials V2. • POST<cluster-ip>/dna/intent/api/v2/global-credential Create Global Credentials V2. • PUT<cluster-ip>/dna/intent/api/v2/global-credential Update Global Credentials V2. To access the new **Discovery** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Operational Tasks** drop-down list and choose **Discovery**.
End of Life (EoX) APIs	The Cisco DNA Center platform supports the following **End of Life (EoX)** APIs: • GET <cluster-ip>/dna/intent/api/v1/eox-status/device Get EoX Status For All Devices. • GET <cluster-ip>/dna/intent/api/v1/eox-status/device/${deviceId} Get EoX Details Per Device. • GET <cluster-ip>/dna/intent/api/v1/eox-status/summary Get EoX Summary. To access the new **Platform** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know your Network** drop-down list and choose **EoX**.
LAN Automation API	The Cisco DNA Center platform supports the following **LAN Automation** APIs: • GET <cluster-ip>/dna/intent/api/v1/lan-automation/log/${id}/${serialNumber} LAN automation logs for individual devices. • GET <cluster-ip>/dna/intent/api/v1/lan-automation/sessions LAN automation active sessions. To access the new **LAN Automation** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the Site Management drop-down list and choose LAN Automation.

Feature	Description
Policy APIs	The Cisco DNA Center platform supports the following **Policy** APIs: • PUT <cluster-ip>/dna/intent/api/v1/endpoint-analytics/endpoints/${epId}/anc-policy Apply ANC policy. • PUT <cluster-ip>/dna/intent/api/v1/endpoint-analytics/endpoints/${epId} Update a registered endpoint. • GET <cluster-ip>/dna/intent/api/v1/endpoint-analytics/endpoints/count Get the count of endpoints. • GET <cluster-ip>/dna/intent/api/v1/endpoint-analytics/tasks/${taskId} Get task details. • GET <cluster-ip>/dna/intent/api/v1/endpoint-analytics/dictionaries Get AI endpoint analytics attribute dictionaries. • GET <cluster-ip>/dna/intent/api/v1/endpoint-analytics/endpoints/${epId} Get endpoint details. • GET <cluster-ip>/dna/intent/api/v1/endpoint-analytics/endpoints Query the endpoints. • GET <cluster-ip>/dna/intent/api/v1/endpoint-analytics/anc-policies Get ANC policies. • POST <cluster-ip>/dna/intent/api/v1/endpoint-analytics/endpoints Register an endpoint. • POST <cluster-ip>/dna/intent/api/v1/endpoint-analytics/cmdb/endpoints Process CMDB endpoints. • DELETE <cluster-ip>/dna/intent/api/v1/endpoint-analytics/endpoints/${epId} Delete an endpoint. • DELETE <cluster-ip>/dna/intent/api/v1/endpoint-analytics/endpoints/${epId}/anc-policy Revoke ANC policy. To access the new **Policy** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. From the left hierarchy tree, choose **Policy**.

Feature	Description
System Settings API	The Cisco DNA Center platform supports the following **System Settings** APIs: • GET <cluster-ip>/dna/intent/api/v1/authentication-policy-servers Get authentication and policy servers. To access the new **System Settings** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. In the **Developer Toolkit** window, expand **System Settings**.
New ITSM Integration Features	
Endpoint Attribute Retrieval with ITSM (ServiceNow) Bundle	This Cisco DNA Center platform release supports **Synchronization Options** in the **Configure Endpoint Attribute Retrieval with ITSM (ServiceNow)** window to define the incremental sync of endpoints. For more information, see the *Cisco DNA Center ITSM Integration Guide*.
New Reports	

Feature	Description
Rogue Additional Details Report	

Feature	Description

	This release supports a new **Rogue Additional Details** report that provides additional information of the rogue threats with details at the BSSID level.
	• The **Rogue Additional Details** report is generated on the following criteria:
	  • MAC Address
	  • Last Updated
	  • First Time Seen
	  • Detecting AP Name
	  • Radio Type
	  • Controller IP Address
	  • SSID
	  • Channel Number
	  • Containment
	  • Encryption
	  • Switch IP Address
	  • Switch Name
	  • Port Description
	  • Location
	  • Threat Level
	  • Threat Type
	  • Start Time
	  • End Time
	• Supported report file formats include **CSV**, **TDE**, and **JSON**.
	• In the **Setup Report Scope** window, the **Rogue Additional Details** report provides port details based on the following scope:
	  • Location
	  • Threat Level
	  • Threat Type
	• In the **Schedule Report** window, available time range options are **Last 3 Hours**, **Last 7 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.

Feature	Description
	To access the **Rogue Additional Details** report, click the menu icon and choose **Report** > **Reports Templates** > **Rogue and aWIPS**. In the **Report** window, choose **Rogue Additional Details**. For more information about **Rogue Additional Details**, see **Run a Rogue and aWIPS Report** in the *Cisco DNA Center Platform User Guide*.

New and Changed Features in Cisco DNA Automation

Feature	Description
Activate or Deactivate AppX MS-Teams	You can now activate or deactivate AppX MS-Teams from your Cisco DNA Center integration.

New and Changed Features in Cisco Software-Defined Access

Table 5: New and Changed Features in Cisco Software-Defined Access, Release 2.3.5.3

Feature	Description
Intrasubnet Routing	SD-Access forwarding behavior is optimized to route the intrasubnet traffic based on the destination IP address, instead of the destination MAC address. Intrasubnet routing is deployed for an IP pool or an anycast gateway by disabling the Layer 2 Virtual Network. This release of Cisco DNA Center supports intrasubnet routing for IPv4 address pool. Dual-stack IP pool and IPv6 traffic are not supported in the intrasubnet routing segment. Intrasubnet routing and Layer 2 flooding cannot coexist for the same IP pool.

Table 6: New and Changed Features in Cisco Software-Defined Access, Release 2.3.5.0

Feature	Description
LAN Automation Enhancements: New GUI Multiple LAN Automation Sessions	A new user interface window for LAN Automation supports both Day 0 and Day N operations, such as: • Start and stop LAN Automation session • Add and delete a Layer 3 interface link • View the newly discovered devices • View the provisioned devices • Check the history of LAN Automation sessions • View the session logs, logs for newly discovered devices, and so on You can run multiple (a maximum of five) LAN Automation sessions simultaneously, across sites. However, you can enable only one LAN Automation session per site.

Feature	Description
Multicast Enhancements	Multicast capabilities have been enhanced to support the following through Cisco DNA Center: • ASM and SSM multicast can be configured concurrently in an SD-Access Virtual Network. • ASM multicast supports dual stack pools (IPv4 and IPv6 pools). • ASM multicast supports multiple external rendezvous points. • SSM multicast supports addition and deletion of IP address ranges.
Support for Multiple IP Addresses for a Wired MAC Address	Cisco SD-Access fabric supports wired endpoints with multiple IP addresses. You can associate multiple IPv4 addresses with a single MAC address.
Support for Native Multicast over SD-Access Transit	You can configure SD-Access Native Multicast on a network that has multiple fabric sites that are connected to an SD-Access transit. Cisco DNA Center provides an option to enable multicast on the border nodes and on the SD-Access transit. This feature is supported only on the fabric sites that have a LISP Pub/Sub control plane node. **Note** To enable native multicast over SD-Access transit, ensure that the border node devices operate Cisco IOS XE 17.7.1 or later releases.
Support Power Profiles across APs in a Fabric	Cisco SD-Access supports creation of AP power profiles for Cisco Wireless Controllers running Cisco IOS XE 17.10.1 and later release. You can assign an AP power profile to an AP and define multiple rules for the AP power profiles.
Support for Wireless IP Address Pools from Layer 2 Segments for fabric sites	Cisco DNA Center allows you to choose the wireless IP address pools that are configured for Layer 2 segments while configuring wireless SSIDs for fabric sites. **Note** This functionality can only be enabled from new SD-Access user interface workflow.

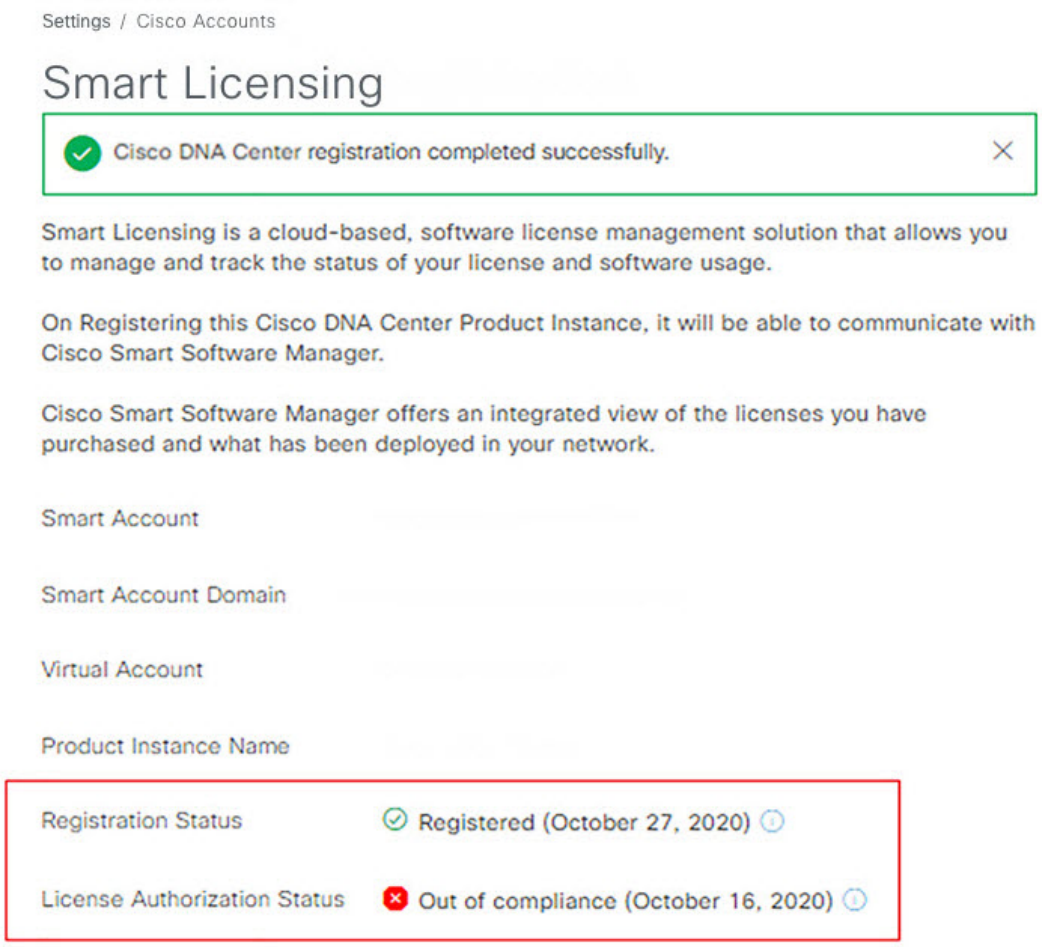
New and Changed Features in Interactive Help

Feature	Description
New in 2.3.5.3	
New Walkthroughs	• Configure Site Analytics Settings • View Site Analytics
New in 2.3.5.0	

Feature	Description
New Walkthroughs	• Add a Building • Add a Floor Without a Map • Add Align Points on a Floor • Add an Area • Add an Exclusion Region to a Floor • Configure Native Multicast over SD-Access Transit • Position Sensors on a Floor • View Your Journey Maps

Licensing Changes

After upgrading from Cisco DNA Center 2.3.5.0 to 2.3.5.3, you might see that your physical license is out of compliance:



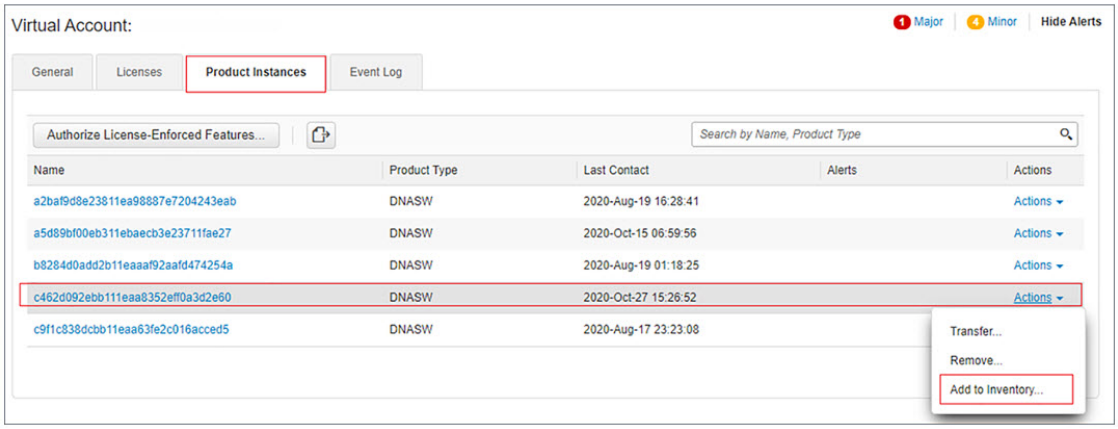
To remain in compliance with the Cisco commercial agreements, ensure that your license is compliant by completing the following steps.

Procedure

Step 1 In Cisco Smart Software Manager (Cisco SSM), in the **Inventory** tab, confirm that you already have an appropriate license, and move it to the appropriate virtual account.

Step 2 If you don't find a license in Cisco SSM, you must add the Cisco DNA Center PID to the inventory as explained below and in the Cisco DNA Center appliance license self-serve guide.

a) In Cisco SSM, choose **Inventory** > **Product Instances**. Choose the product instance with type **DNASW** and then choose **Actions** > **Add to Inventory**.



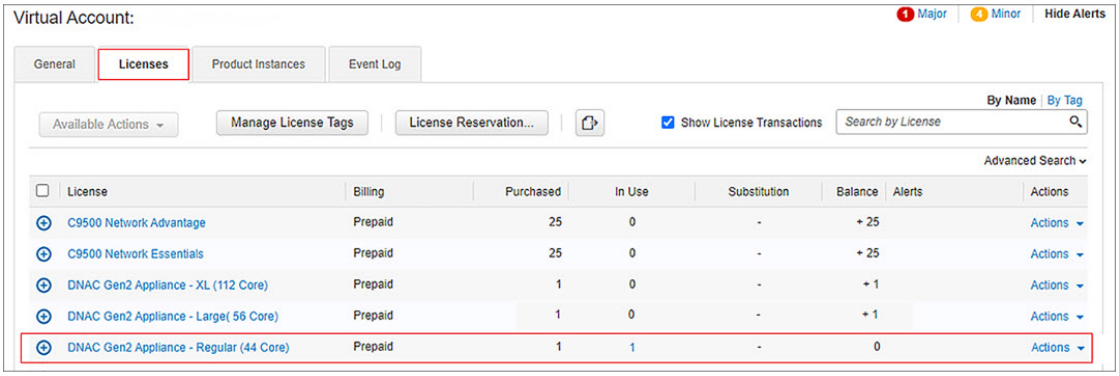
b) Choose the appliance license based on the hardware appliance model. If you are registering a regular Cisco DNA Center appliance, enter `1` for **DNAC Gen2 Appliance - Regular (44 Core)**.

c) Click **Next** and review the added license.

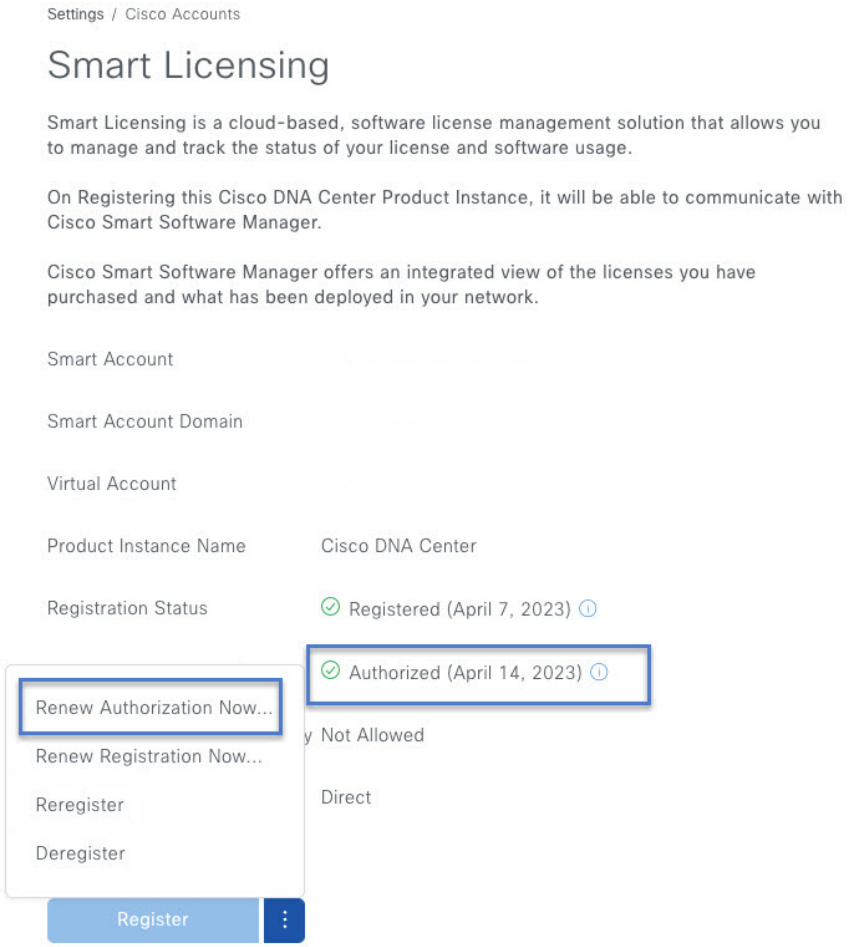
d) Click **Add to Inventory** to add the appliance license to the inventory.

Note If you added the wrong appliance license or quantity, contact your Cisco account representative.

e) In Cisco SSM, choose **Inventory** > **Licenses** and confirm whether the Cisco DNA Center appliance self-service license has been deposited.



Step 3 In Cisco DNA Center, click the menu icon and choose **System** > **Settings** > **Cisco Accounts** > **Smart Licensing**. Click the three vertical dots on the right side of the **Register** button and choose **Renew Authorization Now**. The authorization status changes to **Authorized**.



Step 4 If **Add to Inventory** is unavailable in Cisco SSM, the PID might have been added already to a different virtual account. Note that any request for additional licenses that aren't consistent with your appliance type will result in out of compliance with the Cisco commercial agreements.

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 2.3.5, 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

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*.

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 or 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

Supported Virtual Appliance

Cisco announces support for Cisco DNA Center 2.3.5 and 2.3.5.3 on Amazon Web Services (AWS) as a new form factor that supports Cisco DNA Center in a virtual environment. The virtual appliance (VA) form factor helps customers rapidly deploy and operate Cisco DNA Center.

You can deploy and manage Cisco DNA Center on AWS manually or use a Cisco product called Cisco DNA Center Virtual Appliance (VA) Launchpad (as a local installation or through the Cisco-hosted server).

For more information about Cisco DNA Center 2.3.5 and 2.3.5.3 on AWS, see the *Documentation for Cisco DNA Center 2.3.5 on AWS*.

Installing Cisco DNA Center

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

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

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

Support for Cisco Connected Mobile Experiences

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

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

Plug and Play Considerations

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
  - 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.

Bugs

Open Bugs

The following table lists the open bugs in Cisco DNA Center, Release 2.3.5.x

Bug Identifier	Headline
CSCwc46954	After a failed AP provisioning during a configuration push, remediation tries to push the same configurations again, instead of trying to remediate based on the last successful operation. This problem occurs when a failed AP provisioning is followed by a compliance remediation (fix all). This behavior is expected. Remediation picks up the last snapshot, whether or not the snapshot succeeded. If provisioning fails after the validation step (after CFS persistence), a new snapshot is attempted. If provisioning fails before or during the validation step (when the snapshot does not persist), the old snapshot remediation is attempted.

CSCwc46985	Compliance doesn’t detect any device-level IPDT configuration violations for devices that are running legacy Cisco IOS (earlier than 16.11). Cisco DNA Center doesn’t learn IPDT from devices that are running older software versions.
	For example, the following legacy CLI example shows a device-level IPDT configuration. For these legacy CLI commands, if there is any mismatch between the configuration on Cisco DNA Center and the configuration on the device, the configuration violation isn't captured as part of the Compliance report.
	`ip device tracking`
	`ip device tracking probe auto-source override`
	`ip device tracking probe delay 60`
	`Interface Level Ipdt Configuration,`
	`interface GigabitEthernet1/0/2`
	`ip device tracking maximum 10`

CSCwc71086	The provisioning status shows \"out of sync\", even though provisioning succeeded.

Bug Identifier	Headline
CSCwd04527	When Cisco DNA Center provisions a Cisco Catalyst 9800 Series Wireless Controller, the Pre-Auth ACL is created and applied. This can cause issues on wireless controllers that do not use the Pre-Auth ACL and can result in an outage, if the Pre-Auth ACL is not noticed immediately.
CSCwd19997	After removing all IP pools from a virtual network that is associated with a fabric site, Pub/Sub or Default Route sessions from that virtual network are not removed for devices in that fabric site for the virtual network.
CSCwd24425	After an upgrade or a fresh installation of Cisco DNA Center, certificates are missing from the trustpool.
CSCwd31475	After integrating Cisco ISE with Cisco DNA Center, the RAPI AAA API payload shows the role as **secondary**. This problem occurs when Cisco ISE integration is done after Cisco DNA Center is integrated with one or more AAA servers.
CSCwd31523	Flex WLAN provisioning fails on Azure-hosted Cisco Catalyst 9800 Series Wireless Controller-CL, wireless controller for cloud.
CSCwd41946	Upgrade for fabric: After intra upgrade, the SSIDs are disabled on the Cisco Wireless Controller device.
CSCwd44924	The Cisco DNA Center platform fails to generate an email or webhook for subscribed events or issues. When you publish a subscribed issue, the Cisco DNA Center fails to send e-mails or webhooks.
CSCwd46971	A virtual interface is shown as a physical interface in the API for the Cisco AireOS Wireless Controller.
CSCwd47013	The RabbitMQ virtual host (vhost) goes down due to data corruption. Although RabbitMQ has logic to check and restart the RabbitMQ vhost, the vhost does not restart due to data corruption.
CSCwd49581	Retrieving AP-managed locations takes approximately 12 seconds.
CSCwd50715	An incorrect rate limit is shown for sda/hostonboarding/ssid-ippool.
CSCwd51885	Configuration preview is not generated after moving an AP to another floor.
CSCwd53644	The generated AP report contains entries for APs that are no longer active.
CSCwd58147	During upgrade, Cisco Wireless Controller provisioning fails with the following error: `device lock required in RFS flow Error,message-null`
CSCwd61298	Cisco DNA Center does not update 802.11r changes of a deployed SSID for the Cisco Catalyst 9800 Series Wireless Controller.
CSCwd67815	The End of Life (EoX) report is not available in PDF format.
CSCwd69321	The Cisco DNA Center platform fails to create the **Security Advisory Report** with the following error message: `Formatting failed - Message: Unable to find specified template or user doesn't have permissions to read it: null, Cause: null. Report is not generated.`
CSCwd79259	The Cisco Catalyst 9800 Series Wireless Controller telemetry connection gets stuck after a disaster recovery failover.

Bug Identifier	Headline
CSCwd79769	Cisco DNA Center fails to create or update notifications for PagerDuty when you select the following events: • Fabric Devices Connectivity - AAA Server • Fabric Devices Connectivity - Port Channel Down • Fabric Devices Connectivity - Multicast RP • Switch Power Failure • AP disconnected from WLC
CSCwd80676	The Application Recognition service restarts due to a Java Out of Memory (OOM) error.
CSCwd83339	One or more devices already have VLAN(s) with name(s) and show the following error: `overlapping_sub2-VN2`
CSCwd90050	After an upgrade to Cisco DNA Center 2.3.5, the DNS dashboard remains empty when application telemetry is enabled or provisioned.
CSCwd93216	Reprovisioning a wireless controller by adding several managed AP locations fails.
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.
CSCwe59920	After a credential change, the device config (Syslog/SNMP) gets repushed with the same configuration.
CSCwe70104	When using an external API, the wireless provisioning response is different from the expected response.
CSCwe70250	CMDB bundle is not working.
CSCwf02397	When you configure a Basic ITSM CMDB instance, the configuration fails and displays the following error message: `Source Identifier List not found in ITSM.`
CSCwf04644	You cannot cancel a scheduled task to update devices using the Cisco DNA Center GUI.
CSCwf12027	In Cisco DNA Center, email Event notifications that are site specific are not working properly.
CSCwf45735	Cisco DNA Center may crash with no or few Docker images left.
CSCwf57427	Rolling AP upgrade doesn't work if the image distribution to the wireless controller is done out of band.
CSCwf59765	Cisco DNA Center-generated pre-auth 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.
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.
CSCwh00975	All MAC address formats should be supported while adding external wireless controller to anchor group.

Bug Identifier	Headline
CSCwh13346	The AP name cannot be changed due to empty BLE Radios.
CSCwh15394	Enabling fabric wireless fails with the following error message: `NCSO10011: Error in generating CFS.`
CSCwh28311	Disaster Recovery - Rejoin fails after upgrading from Cisco DNA Center 2.3.5.3 to 2.3.5.4.
CSCwh29152	When you edit a personal SSID with a new passphrase and reprovision the Cisco AireOS Wireless Controller, the updated passphrase doesn't get pushed to the wireless controller. Configuration preview doesn't show the CLI pushing the updated passphrase.
CSCwh31187	Fabric edge provisioning fails. Unable to push the device-tracking policy IPDT_POLICY.
CSCwh31664	After a second Cisco Software-Defined AVC (SD-AVC) restart, the Endpoint Analytics (EA) configuration and SD-AVC cloud connectivity configuration might be lost.
CSCwi38752	After an upgrade to Cisco DNA Center 2.3.5.5, if one of the nodes in a three-node HA setup goes down, Assurance health displays "No Health" for policy extended node (PEN) and extended node devices.
CSCwi71546	When you upgrade to Cisco DNA Center 2.3.5.3 or later, Cisco DNA Center doesn't support the out-of-band configuration for the migrated anchor group. The migrated anchor group is formed with a priority of tertiary.

Resolved Bugs

Cisco DNA Center 2.3.5.5

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.5.5.

Bug Identifier	Headline
CSCwe15923	The internally autogenerated etcd certificate is not activated after renewal. When accessing the Cisco DNA Center CLI, the following errors may be present: `WARNING:urllib3.connectionpool:Retrying(Retry(total=0, connect=None, read=None, redirect=None, status=None)) after connection broken by 'SSLError(SSLError(1, u'[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:727)'),)': /v2/keys/maglev/config/node-169.254.64.1?sorted=true&recursive=true` `ERROR:etcd.client:Request to server https://169.254.64.1:4001failed: MaxRetryError(u"HTTPSConnectionPool(host=u'169.254.64.1', port=4001): Max retries exceeded with url: /v2/keys/maglev/config/node-169.254.64.1?sorted=true&recursive=true (Caused by SSLError(SSLError(1, u'[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:727)'),))",)` For more information, see Field Notice FN74065.

Bug Identifier	Headline

CSCwh08460	Cisco DNA Center may fail to import an Ekahau project, citing the following error:
	`Archive is invalid. Failed to initiate archive import due to unacceptable archive: Unsupported mine type: application/esx`
	In the payload of the API call, initiate-async, the following content-type in the header is present:
	`WebKitFormBoundaryFe9lBzA5DgmlccSK Content-Disposition: form-data; name="archive"; filename="multi-bld.esx" Content-Type: application/esx In Windows 11 or 10, there is an .esx registry in HKEY_CLASSES_ROOT\MIME\Database\Content Type`

CSCwh10626	Cisco DNA Center may mark a configuration archive task as a success even though no data is transferred to the external configuration archive server. This issue happens when the archive is configured to be raw or sanitized, and this issue is specific to the disaster recovery use case.
CSCwh26820	In Cisco DNA Center 2.3.5.3, the eaworker pod may degrade into a reboot loop. The logs note that the Java virtual machine is running out of memory.
CSCwh85079	After upgrading from Cisco DNA Center 2.3.3.7 to Cisco DNA Center 2.3.5.4 -70852, nonguest (enterprise) SSIDs require AAA details when the level of security is set to personal. This issue is not consistent with all enterprise SSIDs, and new SSIDs don't exhibit this behavior.

CSCwh90168	Features in Cisco DNA Center stop working due to APIs failing with kong errors. Features like AP and floor map associations and GUI reporting services are down. The command `magctl service status cassandra-0` shows that cassandra-0 is in crashloopback or OOMKilled state:
	`Name: cassandra-0`
	`Namespace: maglev-system`
	`Node: xxxx`
	`Start Time: xxxx`
	`Labels: addon=true`
	`adjustReplicationDuringNodeScale=async`
	`controller-revision-hash=cassandra-7f86d68787`
	`nodeScale=3`
	`serviceName=cassandra`
	`statefulset.kubernetes.io/pod-name=cassandra-0`
	`version=1.7.38`
	`Annotations: kubernetes.io/psp: ai-network-analytics-psp`
	`Status: Running`
	`IP: xxxx`
	`IPs:`
	`IP: xxxx`
	`Controlled By: StatefulSet/cassandra`
	`Containers:`
	`cassandra:`
	`...`
	`State: Running`
	`Started: xxxx`
	`Last State: Terminated`
	`Reason: OOMKilled`
	`Message: xxxx | ERROR | Cassandra node is not running.`
	`Exit Code: 137`
	`Started: xxxx`
	`Finished: xxxx`
	`Ready: False`
	`Restart Count: 3`

Bug Identifier	Headline
CSCwh98689	Enterprise SSID provisioning might fail because Cisco DNA Center validates nonanchored SSIDs when provisioning an anchor wireless controller. Cisco DNA Center should only validate anchored SSIDs when provisioning an anchor wireless controller and should ignore enterprise SSIDs.
CSCwi28259	After upgrading to Cisco DNA Center 2.3.5.4, the out-of-band mobility anchor configuration is removed from the controller without selecting 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 access to APs. Cisco DNA Center automatically generates a default AP profile using device default values, which disables SSH access. Therefore, any postupgrade provisioning overwrites the value configured by the CLI template (if CLI templates are not force-pushed during reprovision), causing a change from enabled to disabled SSH access.

Cisco DNA Center 2.3.5.4-70852-HF3 Hot Fix

The following table lists the resolved bugs in the Cisco DNA Center 2.3.5.4-70852-HF3 hot fix.

Note

- To obtain the hot fix, go to the **Software Management** window in the Cisco DNA Center GUI and install the 2.3.5.4-70852-HF3 hot fix. If you don't see it, scroll down and click "Looking for other releases? **Click here**."
- The 2.3.5.4-70852-HF3 hot fix is visible only if you have 2.3.5.4 installed.

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. CSCwe15923 is resolved in 2.3.5.4. If you upgraded from 2.3.5.3 to 2.3.5.4 before 2023-10-12, install the 2.3.5.4.70852-HF3 hot fix atop 2.3.5.4.
CSCwh81546	An internally autogenerated etcd certificate is not activated after upgrade. This problem occurs in the following scenario: **1.** Cisco DNA Center is freshly installed using 2.3.5.3, or is upgraded to 2.3.5.3. **2.** The etcd certificate renews, but is not activated (etcd keeps using the old certificate). **3.** Cisco DNA Center is upgraded to 2.3.5.4. **4.** After the upgrade, the old certificate is still used. The system is expected to experience an outage when the certificate expires.

Cisco DNA Center 2.3.5.4

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.5.4.

Bug Identifier	Headline
CSCvz61877	Neighbor topology map for AP may show link status is down when it is up.
CSCwb88254	pxGrid REST API access from Cisco DNA Center fails with the following certificate validation error: `certificate signed by unknown authority`
CSCwc08277	You can't see devices intermittently on the Fabric window. The topology-service's memory utilization is high and it may crash due to running out of memory. Many links in the database have more than 2 link termination points. Malformed links are being formed in the database. The links were learned via LLDP and the device name being reported by CDP vs LLDP was different.
CSCwc39642	Event Notification using Webex, REST, and email stops working after upgrade.
CSCwc45545	User 360 Appendix Business irrelevant and default tabs are missing.
CSCwc61920	Browserbot fails to install on TE update from version 3.0 to 4.1 via the Cisco DNA Center GUI.
CSCwd15864	The API call fails at the NSA web application Assurance back-end service.
CSCwd34162	Cannot apply CLI credentials for the Global site.
CSCwd45971	An SGT created in Cisco DNA Center does not synchronize with Cisco ISE and hangs at the message "Sync not started."
CSCwd50441	Templates that failed in previous provisioning attempts are pushed through during port assignment on the **Host Onboarding** window.
CSCwd58899	Cisco DNA Center does not show the latest ThousandEyes Enterprise application version (4.3.0) for upgrade.
CSCwd64902	Net configuration error scenarios are lost in the NP error response and flex RLAN provisioning fails.
CSCwd69187	An application package fails to install for a user with only numerals in the username.
CSCwd77779	Editing an authentication template does not update CLIs on the device.
CSCwd93614	After adding FIAB to a fabric, no other config-preview operation succeeds due to an internal error.
CSCwe03653	Adding an IP address in the IP Access Control list to the allowed list stops provisioning Cisco ISE settings to the switch.
CSCwe07052	Too many "RS request content-type header is out-dated" errors are sent after Cisco ISE integrates with Cisco DNA Center successfully.
CSCwe09844	On the **Application 360** window, only 25 applications are displayed.
CSCwe12283	LAN automation or other provisioning operations may fail and report existing operations as in progress.
CSCwe14566	Port assignment to an IE-3200 extended node fails due to the **access-session inherit disable autoconf** command.

Bug Identifier	Headline
CSCwe16678	Postgres-0 is running as the primary, but has a DIMM issue. Postgres-1 then attempts to become the primary, but that change fails with an error.
CSCwe21735	Multiple postgres instances indicate themselves as primary following a power outage.
CSCwe25338	After learning of a Catalyst 9800 Series Wireless Controller configuration and provisioning it with the learned Network Profile with Advanced SSID Model Configs, the provisioning may fail.
CSCwe26616	The Catalyst 9410R switch and related hypervisor families don't show the correct number of devices under the family in the Cisco DNA Center Image Repository, showing duplicates for each family.
CSCwe27459	A banner shows an incorrect AI Endpoint Analytics warning alert for Cisco ISE integration.
CSCwe28947	When LAN is automating, plug and play fails on the IPAM server with a client exception in the ipam-service.
CSCwe30879	After an upgrade to Cisco DNA Center 2.3.3.5, one of the Kubernetes service objects, "collector-netflow-ext," is missing, resulting in Assurance data loss for the NetFlow service.
CSCwe31676	Disaster Recovery in a Cisco DNA Center three-node cluster may fail to isolate when two of the three nodes in the cluster are brought down and back up.
CSCwe32559	The Cisco DNA Center VLAN report returns 0 or one site VLAN records. The RestApiSourceExecutor return count is inaccurate.
CSCwe39302	When onboarding new devices via LAN automation, Cisco DNA Center fails to automatically create Network Access Device (NAD) entries in Cisco ISE.
CSCwe39807	An incorrect AP port for switch in Device 360 also affects wireless maps.
CSCwe42089	An external server is successfully set up for Config Archive in Cisco DNA Center, but only a directory is made. There are no config files placed in the directory.
CSCwe46169	The addition of a new IP pool under Guest VN fails with an exception.
CSCwe47530	Postgres goes into a crashloop and restarts continuously. The postgres logs show a syntax error with the configuration file.
CSCwe48765	The Cisco DNA Advantage-level license with the name "C9300X Low-density DNA Advantage Fiber Agg/Core in SMI" for C9300X switches is not detected as a Cisco DNA Advantage-level license when syncing with Cisco SSM, resulting in the level license count showing less than it is.
CSCwe52889	The **Inventory** window shows "No devices available" and "An unknown error occurred," even though all pods are healthy and running.
CSCwe54540	The reachability polling schedule from the database is removed if the refresh message is not processed so Cisco DNA Center will not poll for the reachability status of devices in the inventory.
CSCwe55226	After upgrading from Cisco DNA Center 2.2.3.6 to 2.3.5.3, Network Settings compliance fails at IPDT after migration.
CSCwe56718	When a customer uses the GET Issues API, they may receive a 500 error response and there are only outputs from the Issues API if a device ID is specified.

Bug Identifier	Headline
CSCwe60241	Cisco DNA Center SWIM's image update readiness check and file transfer check may fail with the error "HTTPS is not reachable" when Cisco DNA Center has a fully qualified domain name (FQDN) in its CA certificate, instead of an IP address.
CSCwe65663	Software image information for some of the devices is missing in Software Images Inventory window. This problem occurs because the model type for Meraki APs is missing in the network element table of the inventory database. As a result, the swim-service fails to build the device image information cache.
CSCwe66587	When setting the scale for a floor, you can enter the required values, but nothing happens when you click OK. The following error is displayed: `Uncaught TypeError: Cannot read properties of null (reading 'style')`
CSCwe66786	With network profiles, under Advanced settings, adding or deleting an AP group results in a blank GUI window.
CSCwe68219	Cisco DNA Center application upgrade may fail due to a schema update failure for the SD-access service. The following error is returned: `ERROR: column "networkdeviceid" contains null values`
CSCwe71699	When upgrading Cisco DNA Center, the upgrade may stall or fail at roughly 56% or phase 6 of installing host components. The maglev-node-updater logs show that the task that is stalling or failing is updating the Docker images.
CSCwe74038	A configuration mismatch may occur if a fabric in a box device is failing provisioning but the wired fabric operation on the **Host Onboarding** window is performed. The mismatched items may include IP address pool addition to a VN, VN creation, and IP address pool modification under a VN.
CSCwe82555	An incorrect number of devices may be exported from the Cisco DNA Center License Manager GUI. An export as PDF or CSV doesn't export correctly.
CSCwe83522	Device migration for IBNS2.0 fails if NWS only has AAA Network Auth defined.
CSCwe88997	With APIs, the L2only segment onboarding doesn't work. The "ippoolname" should be optional.
CSCwe89409	Distribution of image 17.6.4 fails due to the following error: `NCSW10090: Failed to distribute image.`
CSCwe90447	A get device info from the Cisco SD-Access fabric does not return wireless controller device details from the fabric.
CSCwe92124	Cannot sync with the primary after one Cisco DNA Center node link comes up.
CSCwe95262	Cisco DNA Center may fail to provision a Catalyst 9800 wireless LAN controller.
CSCwe95707	Cisco DNA Center may not distribute a ROMMON update to a managed ISR 4300 router.
CSCwe96016	IPDT compliance remediation does not work on the port where the intent is changed.
CSCwe98036	A provisioning error occurs while processing the request.
CSCwe98737	A "Resource not found" error occurs when using the Provision Template workflow.

Bug Identifier	Headline
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
CSCwe98851	APs or planned APs aren't shown on the floor map on load. The API call fails with a 500 internal server error. Attempts to assign a planned AP from a real AP in the global inventory may fail, with the task result marked with an internal failure.
CSCwf00700	The up-to-date flow collectors are not used to provision the device. In the logs, the SMC API returns 403 (unauthorized).
CSCwf01879	In Cisco DNA Center, upgrading to version 2.3.3.6 allows you to modify the email destination only once.
CSCwf03814	After a Cisco DNA Center power cycle or power outage, the network devices can't update the device-side certificates.
CSCwf03999	The Configure Access Points workflow may fail to configure the AP or radio-related parameters in certain scenarios.
CSCwf07455	The Client Detail report expires every few months and there is no way to regenerate the same report.
CSCwf12835	The current mechanism of authorizing the AP to join the controller is via *local authorization*. (Local authorization makes use of the AP MAC address or serial number from the controller database.) If you want to switch from local to AAA only or AAA+local, the config diff to configure this setting is not generated in Cisco DNA Center 2.3.5.x.
CSCwf14502	AAA configurations are removed from Cisco Catalyst 9800 Series Wireless Controllers when you create an AP authorization first and then you create a WLAN with the same AAA IP.
CSCwf16116	In a three-node cluster of Cisco DNA Center appliances, when one of the nodes is powered down and then powered back up, the services remain down. The expected behavior is that services rebalance within 15 to 30 minutes.
CSCwf18318	The Task view shows that the provisioning completed successfully, but the new switch may not show up on the **Topology** window, where it can be changed to a fabric role.
CSCwf20392	The AP Claim workflow may leave APs configured with default site tags and location parameters.
CSCwf23391	In Cisco DNA Center, you subscribe to the event "no Activity on Radio," but this event is disabled on the **Issue Settings** window. Even though the event "no Activity on Radio" is disabled, it's seen on Issues & Events.

Bug Identifier	Headline
CSCwf23486	When there are only two nodes, the Liveness probe fails on the primary node.
CSCwf25968	Due to the default selection of Cisco DNA Center as a NetFlow server on the **Network Settings** window, the telemetry push task may fail while deploying network settings due to the unsupported configuration of NetFlow on IE 3000 series switches.
CSCwf26589	In Cisco DNA Center, when more than one device is selected for provisioning and the selection includes a Catalyst 9500 model, the "Advanced Configuration" step does not correctly show the templates for all devices, meaning not all devices or templates are displayed. For example, if only Catalyst 9300 devices are selected, the issue is not seen; the issue only occurs when the selection includes a Catalyst 9500. **Note** The CSV format of the import/export template variables in the provisioning workflow has been fixed as part of this defect. Therefore, exported CSV files from 2.3.5.3 aren't acceptable and generate an invalid CSV file error when you try to import template variables based on the old CSV. You must export the latest CSV from 2.3.5.4 and use that as the basis for importing the template variables for both regular and composite templates. Related bug ID: CSCwf15199.
CSCwf29125	Cisco DNA Center's config-archive-service may decline into an out of memory condition and restart repeatedly.
CSCwf31240	Postgres fails due to a multiple primary issue.
CSCwf31445	Cisco DNA Center may not create a second policy profile when a different VLAN group is created for the same WLAN in a second network profile, resulting in a partial configuration being pushed to a managed wireless controller.
CSCwf31965	The wireless controller provisioning workflow may return an error in the Model Config tab of the **Provisioning** window.
CSCwf32124	MAB clients using Open authentication are not reauthenticated when the switch reloads, or when they lose connection with the AAA server and that connectivity comes back.
CSCwf34712	Cisco DNA Center is detected to be running weak ciphers.
CSCwf36885	After an upgrade to Cisco DNA Center 2.3.3.6, the device inventory collection status may change to "internal error."
CSCwf37179	Deploying a template with the "bound to source" variable doesn't work because the value is not saved correctly. The template simulation works correctly; however, generating a config preview or trying to provision a device with the variable fails.
CSCwf38305	IP phones are misclassified and shown as rogue APs. IP phones are shown as a host on the switch, causing Cisco DNA Center to classify IP phones incorrectly. The same host MAC address is displayed for every High Rogue Threat alert.
CSCwf39426	AP and planned APs overlay on the map.
CSCwf39469	Provisioning may fail when trying to create a new port-channel or add a link to an existing port-channel in an SDA fabric device from Cisco DNA Center's **Host Onboarding** window.

Bug Identifier	Headline
CSCwf40854	Cisco DNA Center may fail to provision a Catalyst 9800 wireless controller. The following error is returned: `NCSP11108 CFS persistence failed deleted object would be re-saved by cascade.`
CSCwf41422	Cisco DNA Center's inventory service may restart frequently when several thousand discovery requests are queued up by an API call.
CSCwf43384	A system compliance request causes Orchestration-engine-service in java.lang.StackOverflowError.
CSCwf44636	The AP Refresh workflow doesn't work after upgrading from Cisco DNA Center 2.3.5.3 to 2.3.5.4.
CSCwf45474	After a pause and unregister, Cisco DNA Center's disaster recovery virtual IP address is still available in the last known active cluster.
CSCwf45734	The disaster recovery hangs in an ambiguous state where a user-actionable option is available.
CSCwf45762	Cisco DNA Center disables the radios to make changes to any custom RF profile. This includes any out-of-band changes detected. On subsequent wireless controller provisioning, the 2.4-GHz band is disabled.
CSCwf47012	When provisioning or updating telemetry to a Catalyst 2960C switch using Cisco DNA Center, an error is generated, even though NetFlow is not supported on the device.
CSCwf47760	An open violation for the DNS server is not generated under Network Settings Compliance.
CSCwf48385	Cisco DNA Center may show inaccurate information about the node state on the System Health window, citing the error, "The CIMC appliance is currently IP unreachable" when everything is functional.
CSCwf48403	A Cisco DNA Center user wants to enable IP overlap on an SSID and defines this in the model config editor for flex configuration. While trying to provision the wireless controller, at Step 3 of the provision task where there is an option to choose a model config, a "constraint validation failure" error occurs for the applied model config. When the view option is clicked, the IP overlap toggle is displayed. When toggled once and saved, the error about the constraint validation failure disappears. When the provision is attempted after that, provisioning the model config fails, but the other items being provisioned succeed.
CSCwf48701	An upgrade fails with the following exception: "Exception postgres FATAL: role "replicauser" does not exist." Some services restart constantly.
CSCwf53661	An error is returned when a VLAN with 4 digits is configured with 64 VLANs in a single VLAN group.
CSCwf57289	Cisco DNA Center may stop working completely when there are no Docker images left. The /data disk fills up due to rapid core or heap dumps generation by one or more applications. If one or more applications suffer crashes, they generate large-sized code crash reports that can fill up the disk partition where Docker images are cached. Due to a Kubernetes self-recovery mechanism that triggers garbage collection of Docker images to bring down the free disk space to above 15%, the deleted Docker images result in a Cisco DNA Center crash.
CSCwf62146	RabbitMQ does not recover correctly after a node is powered on during three-node HA testing. Multiple services in a three-node cluster of Cisco DNA Center appliances may restart continuously.

Bug Identifier	Headline
CSCwf62922	The Disaster Recovery GUI shows site Down and Up activities continuously. The disaster-recovery-service in the CLI shows multiple restarts. The haproxy container in disaster-recovery-service goes into a crashloop state. The haproxy logs show "SSL client certificate not trusted" error messages.
CSCwf63492	Assurance data may continue to grow to the point where Elasticsearch hits red status. The purge job may become unable to connect to Elasticsearch to remove information because the connection to Identity Manager is refused.
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.
CSCwf73241	Migration fails for file-service Objects in Mongoloid, wiping out maps after failover.
CSCwf74542	Cisco DNA Center's aca-controller-service may degrade into a CrashLoopBackOff state after a node reboot.
CSCwf78576	While deploying multicast on a VRF(X), the "LISP mobility" configuration under the interface VLAN and the "dynamic-eid" configuration under the router LISP are removed for multiple VLANs on another VRF(Y), which causes a major network outage.
CSCwf86819	Cisco DNA Center 2.3.5.3 reports SPF-service-down and can't retrieve compliance-related device data.
CSCwh01986	Cisco DNA Center may fail to provision a Catalyst 9800 wireless LAN controller. The following error is returned: `update or delete on table "sitetaginfo" violates foreign key constraint "fka8f74ee1e2aa2c55" on table "wirelessgrouping".`
CSCwh16262	AP PnP onboarding fails when using SNMPv3 + AES 256 on the embedded wireless controller.
CSCwh26174	ThousandEyes agents are not shown in Assurance.

Cisco DNA Center 2.3.5.3-70194-HF5 Hot Fix

The following table lists the resolved bugs in the Cisco DNA Center 2.3.5.3-70194-HF5 hot fix.

Note

- To obtain the hot fix, go to the **Software Management** window in the Cisco DNA Center GUI and install the 2.3.5.3-70194-HF5 hot fix. If you don't see it, scroll down and click "Looking for other releases? **Click here**."
- The 2.3.5.3-70194-HF5 hot fix is visible only if you have 2.3.5.0 or 2.3.5.3 installed, not 2.3.5.4.

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. CSCwe15923 is resolved in 2.3.5.4. For 2.3.5.3, this bug is resolved with the 2.3.5.3-70194-HF5 hot fix. If you upgraded from 2.3.5.3 to 2.3.5.4 before 2023-10-12, install the 2.3.5.4.70852-HF3 hot fix atop 2.3.5.4.
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.`
CSCwf38534	Wireless controllers managed by Cisco DNA Center go into syncing state. This problem occurs when the wireless controller sends when large amounts of ciscoConfigManEvent traps to Cisco DNA Center. Cisco DNA Center should ignore configuration change traps (ciscoConfigManEvent) for processing.
CSCwf56827	An SNMP trap is pushed with an incorrect group authentication mode, even when a read view is defined.
CSCwf59179	Floor maps go missing and must be reuploaded. This problem occurs when floor map images are uploaded manually via the Cisco DNA Center GUI, but can also happen in certain cases after an Ekahau project, Cisco Prime Infrastructure map archive import, or Prime Infrastructure Data Migration Tool (PDMT) provides the floor images. Related bug ID: CSCwf70671.
CSCwf61895	When a wireless controller has a 9124AXE AP in bridge mode associated to it, provisioning that wireless controller may fail with the following error: `NCWL 12001: Channel or Power Assignment is not configured as custom for 5GHz Radio on the AP.`
CSCwf63148	The LAN automation process may hang at the "Starting Seed Device Configuration" phase for Disaster Recovery 1+1+1 and a three-node cluster.

Bug Identifier	Headline

CSCwh13140	Provisioning a 9124AX AP in mesh root AP mode fails with the following error:
	`Configuration on the device failed.`
	`Error: Unable to push to device WLC_IP using protocol ssh2 the CLI do ap name AP_NAME controller primary WLC_NAME WLC_IP.`
	`Device Response: % Error: no ap_name exists.`

Cisco DNA Center 2.3.5.3

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.5.3.

Bug Identifier	Headline
CSCvy30961	Cisco DNA Center's **Smart Licensing** window does not load as expected and displays the following error: `Error in loading data. Please see log for more info.`
CSCvz59447	Cisco DNA Center fails to provision a managed device if the loopback0 interface IP address is not available.
CSCwb02969	In a three-node setup, after provisioning a Cisco Catalyst 9500 Series Switch stack and completing the fabric configuration, the switch stack status changes to "Managed Internal error."
CSCwb99632	SWIM report generation fails when the run time exceeds the defined maximum running time for the worker pod (16 hours).
CSCwc05125	Cisco DNA Center wireless controller compliance fails with a mismatch in the WLAN policy profile name.
CSCwc39603	When you configure a new event notification in Cisco DNA Center, the **Try It** option for the subscribed event returns the following error: `FAILURE - 'Endpoint Connection Timed Out.'`
CSCwc79851	In a single-node setup, while trying to deploy ThousandEyes 4.3.0 on switches (25 switches per pane), the following error was displayed: `Device Not Ready` To work around this problem, either change the pagination to 10 switches per pane, or filter the switches on which you want to install ThousandEyes.
CSCwd00896	AP group-related configurations are not pushed in an implicit provisioning, which causes a wireless outage while resetting AAA inheritance. To work around this problem, review the configuration before deploying it on the device.
CSCwd09391	Cisco DNA Center orchestrated app hosting is disabled on the AP when the primary wireless controller is changed.
CSCwd13881	For single node, Cisco DNA Center shows the slot 2 radio on 2800 Series APs.
CSCwd24258	In a three-node setup, the provisioning task fails with the following error: `NCS010011: Error in generating CFS due to internal error`

Bug Identifier	Headline
CSCwd25750	Under scale, the kafka pod cannot handle data and slows down with gaps in the Assurance Health trend chart.
CSCwd26099	While trying to create one IP network group, the GUI spins for longer than 5 minutes.
CSCwd27458	Cisco Wireless Controller provisioning fails when the AAA Radius Attributes Configuration model config is attached to a network profile.
CSCwd28811	While provisioning a Cisco Wireless Controller with an open SSID or an SSID without assigning AAA servers, Cisco DNA Center pushes a default accounting list. To work around this problem, remove the default accounting list configuration manually, until next Cisco DNA Center provisioning.
CSCwd31345	If external webauth SSIDs configured from Cisco DNA Center resolve to the same DNS servers, but in a different order, Cisco DNA Center pushes the flexconnect ACL on every wireless controller provisioning.
CSCwd33248	The fabric wireless SSID window takes longer than 30 seconds to load.
CSCwd36272	When an AP is provisioned with a new AP zone, all SSIDs go down after AP reprovisioning.
CSCwd36581	AP outband config and provisioning from Cisco DNA Center policy tags are different.
CSCwd36789	Provisioning failure occurs on N+1 with custom site tag or policy tag addition.
CSCwd37176	When you try to delete a virtual network policy, the following error is displayed: `NCSP11001: User intent validation failed while processing the 'terminate' request.`
CSCwd37272	Cisco Catalyst 9800 Series Wireless Controller provisioning fails with the following error: `$RadioType_config" is an invalid value.`
CSCwd37292	A wireless pool is deleted from the virtual network, despite being mapped to the fabric SSID.
CSCwd37822	Cisco SD-Access: First-time reprovisioning of a Cisco Catalyst 9800 Series Wireless Controller causes WLAN SSIDs to flap in Cisco DNA Center. This problem occurs when the Cisco Catalyst 9800 Series Wireless Controller is upgraded to Cisco IOS XE 17.7.0 or later.
CSCwd37961	After AP zone, policy tag, or site tag removal, the following error is displayed: `NCSP11108 Error occurred while processing.`
CSCwd38259	Cisco Wireless Controller or AP provisioning fails with an `NCSP11001` error when changing between custom and Cisco DNA Center autogenerated site tags in a network profile.
CSCwd38863	Cisco Adaptive Wireless Intrusion Prevention Service (aWIPS) is removed from the default AP profile during Cisco Catalyst 9800 Series Wireless Controller provisioning, even when aWIPS is enabled in the wireless network settings.
CSCwe39568	A continuous java.lang.OutOfMemory error occurs when adding 20 pools or 10 VNs.
CSCwd40022	A policy tag is not activated on the WLAN during an AP zone change from Cisco DNA Center AP provisioning.

Bug Identifier	Headline
CSCwd40306	Cisco DNA Center is sending the SNMP trap payload field `snmpTrapAddress` with the external SNMP collector IP.
CSCwd40954	When selecting sites under **Policy** > **IP Based Policy**, it takes approximately 20 seconds to list the sites.
CSCwd42794	Cisco Catalyst 9800 Series Wireless Controller provisioning fails after upgrading to Cisco DNA Center.
CSCwd43192	Anchor wireless controller provisioning fails with the following error: `NullPointerException`
CSCwd44800	Removal of the anchor controller results in policy tag removal and outage.
CSCwd46164	After upgrading a Cisco Catalyst 3850 Switch stack of two switches (from INSTALL mode), only one member comes up after reboot (in BUNDLE mode). The Cisco DNA Center audit logs show that incorrect commands were pushed for INSTALL mode upgrade, causing this issue.
CSCwd46246	Template Hub Plug and Play Day-0 and Day-*n* templates associated with onboarding fail to attach to a profile.
CSCwd46870	While configuring mobility, the screen takes approximately 25 seconds to load.
CSCwd47011	In Cisco DNA Center, a network profile is configured with custom site tags, policy tags, or flex profiles for the managed site of the Polaris Catalyst 9800 Series Wireless Controller. The Polaris Catalyst 9800 Series Wireless Controller is provisioned with the network profile-managed sites and the custom tags generated on the device as a placeholder for the AP provision to use the preprovisioned tags. In this scenario, the following cases are seen: • No preprovisioned tags, custom tags, flex tags, policy tags, or site tags are configured on the Polaris Catalyst 9800 Series Wireless 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 2.3.37, wireless controller reprovisioning deletes the orphan custom tags.
CSCwd47125	Deleting an anchor results in stale mobility configs in N+1, which causes a provisioning failure in N+1.
CSCwd48297	In a network profile, you have flex-enabled and non-flex SSIDs. When you create an AP zone for only non-flex enabled SSIDs, the following validation error occurs: `One or more Flex SSIDs need to be part of this zone as the site will be deployed as a flex site`

CSCwd48939	When you add a Cisco Wireless Controller through an API call to a fabric site that has a control plane node configured with LISP Pub/Sub, the provisioning fails with the following error:
	`FailureReason : Conversion of SDA PubSub Control Plane to SDA BGP/LISP Control Plane not supported.`
	`To change the Control Plane to SDA BGP/LISP, remove all Control Plane(s), Save and Re-Add Control`
	`Plane(s) to fabric site.`

CSCwd49596	Cisco Wireless Controller reprovisioning fails with an internal error.
CSCwd49629	Unable to view error details because the device-config-status API returns a 504 error.

Bug Identifier	Headline
CSCwd50263	Catalyst 9800 Series Wireless Controller provisioning fails with an error.
CSCwd53051	AP zone addition in network profile and Cisco Wireless Controller provisioning results in the policy tag getting updated for the AP.
CSCwd53091	After deleting an AP zone, there is a policy tag mismatch between the N and N+1 controllers.
CSCwd53101	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'`
CSCwd53571	Cisco DNA Center fails to reprovision a Cisco Wireless Controller after the AP zones in the network profiles are updated with tags.
CSCwd53607	Deleting a Cisco Catalyst 9800 Series Wireless Controller and adding it again to Cisco DNA Center generates a Flex ACL IPv6/EXT_RE_ACL_IPV6 compliance error for Network Profile after provisioning.
CSCwd54833	AP groups without an associated AP zone are removed from the Cisco AireOS Wireless Controller after provisioning.
CSCwd55727	Wireless provisioning fails during the validation phase.
CSCwd55811	While trying to add a sensor to a floor, the filter option doesn't work in the **Network Hierarchy** window.
CSCwd56050	The Configuration Archive report does not display in PDF format.
CSCwd56704	Changing a custom policy tag's site results in moving the AP to the default policy tag.
CSCwd57297	Custom site tags are not created, even though a success message is shown.
CSCwd58125	During upgrade, Cisco Catalyst 9800 Series Wireless Controller provisioning fails with the following error: `No device lock required in RFS flow - PMF`
CSCwd58701	A disaster recovery failure occurs with the following error: `NCFS10077: Disaster recovery mandatory data missing,namespace=ejbca,filename=<xyz> is not present in mongodb`
CSCwd59216	While provisioning a Cisco Catalyst 9800-CL Wireless Controller running on Cisco IOS XE 17.3.5a/17.7.1/17.3.3, provisioning fails with the following error: `NCSP11108: Error occurred while processing the request.`
CSCwd59876	When you provision a nonfabric WLAN (locally switched) on a fabric wireless controller, it converts the APs to flex mode, which is not a supported scenario for fabric deployments.
CSCwd62967	Cisco DNA Center Inventory Telemetry: Compute resources run out on the cloud side.
CSCwd63406	Wireless provisioning creates tasks with an incorrect task hierarchy.
CSCwd66051	On a Cisco Catalyst 9800 wireless LAN controller, the output of `show telemetry ietf subscription all detail` shows many invalid subscriptions with the following error: `Notes: Subscription limit reached.`

Bug Identifier	Headline
CSCwd67305	Cisco DNA Center provisioning of AAA to transit control plane fails during the configuration deployment or network intent with the following error: `Unable to push configuration to device x.x.x.x. Device Response - This operation will permanently convert all relevant authentication commands to their CPL control-policy equivalents. As this conversion is irreversible and will disable the conversion CLI 'authentication display [legacy|new-style]'`
CSCwd68079	In the WLAN advance window, Fast Transition (802.11r) must be enabled at the site level. Fast Transition (802.11r) is not inherited at the site level. It remains grayed out, because of which site override is not possible. Unable to change Fast Transition (802.11r) after the initial configuration at the site level.
CSCwd68327	After a network outage, postgres occasionally goes out of sync and does not recover.
CSCwd75024	Cisco DNA Center fails to enable application telemetry on wireless LAN controllers due to an exception that occurs during device controllability configurations in application telemetry.
CSCwd75501	When you rerun the Security Advisory report, it fails and displays the following error: `BAPI Execution Failed. Response Code = 500, Response Content=null`
CSCwd77279	During power loss of a network device on Cisco DNA Center, the device is not populated as DEVICE_UNREACHABLE until a scheduled or manual resync occurs.
CSCwd79307	While syncing images, the following error occurs: `Getting device mdf data Failed-Invalid Index`
CSCwd79358	When Cisco Catalyst 9000 Switches are integrated in Cisco DNA Center through the Meraki Dashboard, they are displayed as third-party devices. Applications like SWIM and SDA provisioning don't work on those Catalyst 9000 devices. Also, you can't add any new images to the **Image Repository** window or sync any images with cisco.com until those Catalyst 9000 devices are removed from the inventory.
CSCwd79923	When you choose ALL as the License mode, no devices are listed in the **Devices** tab.
CSCwd83022	Cisco Wireless Controller provisioning fails with the following error: `Validation failed node-1:dbm:wireless:Same WLAN ID 18 is already present in database` To work around this problem, do the following: **1.** Delete the WLAN from the network profile and save the changes. **2.** Reprovision the wireless controller. **3.** Add the WLAN to the network profile.
CSCwd84123	In Cisco DNA Center, enabling features in fabric IP pools (for example, enabling a wireless pool) results in a provisioning failure on fabric devices with the following error: `Unable to push to device x.x.x.x using protocol ssh2 the CLI router lisp. Device Response - %No policy information.` To work around this problem, enable a new fabric view, revert the changes, and attempt to re-enable the desired feature.

Bug Identifier	Headline
CSCwd84374	After an extended node pool (Anycast Gateway) is defined and subsequently deleted from a fabric site, LAN automation does not proceed beyond the seed configuration stage. This problem is triggered after the extended node pool is deleted from the fabric site, even if no devices have been onboarded previously into Cisco DNA Center. The network orchestration log shows that the extended node onboarding workflow is trying to proceed, even though there is no extended node pool defined. This prevents LAN automation from working.
CSCwd84447	After a primary/standby node restart, a `Connection refused` error occurs.
CSCwd86638	Addition of 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.
CSCwd88946	The AI-enhanced RRM site selection operation fails.
CSCwd89482	SWIM internal calls go to proxy, causing issues with image distribution, image update, or Cisco DNA Center CA trustpoint push. To work around this problem, delete the proxy from settings, restart the SWIM container, and force push the telemetry.
CSCwd90641	In a single-node setup, AP provisioning fails with the following error: `ERROR: duplicate key value violates unique constraint "wirelessgrouping_bk"`
CSCwd91440	After upgrading from Cisco DNA Center 2.3.5.0.70583 to 2.3.5.0.70586, the Cisco Catalyst 9800 Series Wireless Controller provisioning fails with an `NCSP11108` error.
CSCwd92838	A new device that is in reachable and managed state does not show the golden image in the inventory window, even when the golden image is assigned to that new device.
CSCwd93194	The Cisco DNA Center GUI login hangs and maglev commands fail to run due to the following error: `API rate limit exceeded`
CSCwd93259	After upgrade, the devices in the License Manager show the "Needs re-registration" tag, even though the connection mode hasn't changed.
CSCwe04247	An error occurs while applying a critical fix for the Closed Authentication mode template update.
CSCwe05972	Duplicate validation must be checked for the complete source and destination, which includes source port and destination port, and so on. Currently, a check is added only for IP addresses. Using Cisco DNA Center's pre-auth ACL list, the user cannot have a TCP ACL with the same IP address on a different port.
CSCwe06738	While upgrading from Cisco DNA Center 2.3.4 to 2.3.5, downloading fails with the following error:Exception in package: `Exception in package: automation-core, kind: ServiceBundleGroup, name: apicem-basics - Shell command timed out after <n> seconds of inactivity: /srv/maglev/replicated_storage//fusion/plugin_type_catalog/model/7.1.610.60911/install UPGRADE`
CSCwe10186	When bulk sites are selected to create fabric zones, the wrong fabric zone is assigned for multicast pools. This causes the multicast IP lookup to fail, and provisioning fails for that device. To work around this problem, select one site at a time to create fabric zones.

Bug Identifier	Headline
CSCwe10342	Cisco DNA Center's SPF services crash while previewing the configuration of a wireless LAN controller provisioning. The SPF service crash occurs with an OutOfMemoryError during wireless controller provisioning with 3250 sites.
CSCwe11463	After disaster recovery failover, image distribution for devices hangs at 10% for several hours with a "Distributing Image with null Protocol Running" state.
CSCwe15942	Upon clicking an image family name on the **Image Repository** window, it redirects to **Design** > **Image Repository** > **Image Family**. The image family name is displayed as the title, but no image is displayed under the **Image Repository** window.
CSCwe17325	For a Cisco Catalyst 3850 Switch with 16.12.x, the base image gets deleted before the SMU is copied to the switch.
CSCwe19750	Provisioning a Cisco Catalyst 9800 Series Wireless Controller with an AI RF profile pushing 6 GHz with non-Europe-compliant channels fails with the following error: `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`
CSCwe28523	In a Cisco DNA Center setup using disaster recovery, the MongoDB replication fails with a conflict error. When this problem occurs, the log from the dr-mongodb-replicator service displays a message similar to the following example: `[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]`
CSCwe31951	In a three-node setup, full backup fails for NDP Elasticsearch with the following error: `"no_such_file_exception"`
CSCwe32845	In a three-node cluster, after upgrading from Cisco DNA Center 2.3.3.6 to 2.3.3.7, a large number of unbound queues are seen in RabbitMQ.
CSCwe33933	Deploying changes to fabric, provisioning of fabric devices from inventory, and device compliance checks fail with the following error: `NCSO10001: CFS validation failed due to internal error`
CSCwe35389	Cisco DNA Center's release download hangs on the main system package while calculating requirements.
CSCwe36863	With a backward compatibility check, the BAPI response does not generate a BAPI error with the invalid interface name in the POST call of the wireless profile.
CSCwe39334	Fabric provisioning fails with an error stating that a pool has intra-subnet routing enabled. To work around this problem, delete and recreate the offending pool.
CSCwe39344	When you configure a new event notification in Cisco DNA Center, the **Try It** option for the subscribed event returns the following error: `Endpoint Connection Timed Out`

Bug Identifier	Headline
CSCwe39650	The template does not configure the correct name when used with a bind to source with the wireless network profile.
CSCwe39718	After you attach a template to a profile, the count is not shown in the **Template Hub** window.
CSCwe41944	Unsupported images are listed under the Cisco Catalyst 9200 Series Switches, which causes devices to go into ROMMON mode.
CSCwe42201	After upgrading Cisco DNA Center from 2.3.3.5 to 2.3.3.6, the appliance goes into a constant reboot loop.
CSCwe44726	PnP onboarding fails for certain switches with the following error: `AP PNP Claim failed. Invalid RF-Profile: null`
CSCwe47539	Cisco DNA Center application upgrade fails with an exception in the group-based-policy-analytics package.
CSCwf12001	Cisco DNA Center upgrade from 2.3.3.7 to 2.3.5.3: AP authorization is enabled for a normal (regular) AP.

Cisco DNA Center 2.3.5.0

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.5.0.

Bug Identifier	Headline
CSCwa22823	AireOS wireless controller provisioning fails during the deployment stage in Network Programmer.
CSCwa77904	Cisco Wireless Controller provisioning fails with the following error: `NCSP10246: Internal error while attempting to transform the object for further processing.`
CSCwb28540	A tag mismatch is seen between the primary and secondary controller.
CSCwb51750	User intent validation of Cisco Catalyst 9800 Series Wireless Controller fails with a change in the network profile.
CSCwb85233	A third-party device is reported as Catalyst 9800 Series Wireless Controller for Cloud.
CSCwc02517	Cisco DNA Center selects a switching profile for a wireless controller if the same sites are assigned to switching and wireless.
CSCwc12746	AP provisioning fails with the following error: `Cannot delete AP mac from the custom APG on the N+1 HA device.`
CSCwc18664	External AAA with RADIUS and TACACS is not displayed under the WLAN AAA section.
CSCwc39642	Cisco DNA Center 2.3.3.x event notifications using Webex, REST, and email stop working after an upgrade.
CSCwc42824	AP provisioning fails because Cisco DNA Center pushes duplicate commands in sequential order.

Bug Identifier	Headline
CSCwc62887	After you upgrade from Cisco DNA Center 2.2.3 to 2.3.4, the GUI shows the lowest release version as available for download immediately after the system upgrade.
CSCwc76362	Devices show an internal error due to the following exception: `Exception while persisting: java.lang.NullPointerException.`
CSCwc93896	AP and wireless controller provisioning fails due to the following error: `NCSP10001: User intent validation failed.`
CSCwc94852	Cannot provision or delete the wireless controller due to the following error: `NCSP11108 CFS persistence failed.`

CSCwc96069	The Cisco DNA Center platform license reports fail with the following error message:
	`Sorry, data aggregation failed - missing cache of invalid parameters.`
	`Please try later or create new report.`

CSCwc98950	Cannot export the hierarchy to the CMX for one or more domains.
CSCwc99150	Wireless controller provisioning fails after changing the VLAN for the SSID under network profile.
CSCwd08429	Cannot assign SGT to Policy Extended Node port assignment.
CSCwd08474	Reprovisioning BAPI fails with the following error: `Interface Input Error: Duplicate IP found.`
CSCwd18464	Cisco DNA Center incorrectly shows C1000-8P-2G-L as supported.
CSCwd22124	Cisco DNA Center takes too long to identify an AP IP address.
CSCwd26583	Cisco DNA Center keeps repushing the TACACAS configuration on every wireless controller provisioning.
CSCwd30229	The add and update A Pis return a success response for Execution ID, but the SSID and segment mapping are not updated in the fabric.
CSCwd30455	HTML code is displayed in the task name of image distribution.
CSCwd34162	Cannot apply CLI credentials at a site.
CSCwd34763	Cisco DNA Center may configure AP tags with default values, rather than the site tags configured in the network profile.
CSCwd46904	A device upgrade from 16.x to 17.x fails during activation through three-step activation.
CSCwd59885	After upgrading to Cisco DNA Center 2.3.5, the Command Runner task gets stuck on the ECA device.

Limitations and Restrictions

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 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 DNA Center on AWS Limitations

- Cisco DNA Center on AWS supports only the r5a.8xlarge instance size. Any changes to this configuration aren't supported.
- Cisco DNA Center on AWS doesn't support the Federal Information Processing Standards (FIPS).
- Cisco DNA Center on AWS doesn't support IPv6.
- Cisco DNA Center on AWS doesn't support disaster recovery. Therefore, we recommend that you don't install the optional Cisco DNA Center Disaster Recovery (DR) package.

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 Policy Limitation

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

AP Limitations

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

  After the provisioning failure, the AP rejoins the wireless controller. You can reprovision the AP for a successful provisioning.
- The Cisco Catalyst 9130AXE AP with antenna C-ANT9104 does not support the Disable option for Dual Radio mode.
- The Cisco Catalyst 9124AXE AP does not support the Auto option for Dual Radio mode.
- Starting in Cisco DNA Center 2.3.5.4, when you export the Inventory, the export file includes up to 10,000 devices total, including APs. Credential information is excluded from the export file.

  In earlier releases, the export file didn't have the 10,000-device limit and APs were excluded.
- 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 Limitations

- With IPDT on trunk ports, 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.
- When you add a line card to a chassis, or remove a line card from a chassis, the changes take several minutes to update on Cisco DNA Center. Any IPDT configurations 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 update on Cisco DNA Center. Any IPDT configurations are pushed to the device automatically for newly added interfaces.

  To add or remove the 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 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 limitations:
  - Infoblox does not expose a name attribute; therefore, the comment field in Infoblox is populated by the IP pool name during a sync.
  - For a pool import, the first 50 characters of the comment field are used. If there are spaces in the comments, they are replaced by underscores.
  - If an IP pool name is updated for an imported pool, the comments are overwritten and the new name is reflected.
- BlueCat: There are no limitations identified with BlueCat integration at this time.
- You might see the following error when editing an existing IPAM integration or when adding a new IPAM manager.

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

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

  - No values are configured in SAN field of the certificate.

  - If 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*