Release Notes for Cisco DNA Center, Release 2.3.6.0

First Published: 2023-04-06

Last Modified: 2023-08-22

About Release Notes for Cisco DNA Center, Release 2.3.6.0

Cisco DNA Center 2.3.6.0 is a Limited Availability release. Contact your Cisco sales representative to request this release.

This document describes the features, limitations, and bugs for Cisco DNA Center, Release 2.3.6.0.

For links to all the guides in this release, see Cisco DNA Center 2.3.6 Documentation.

Change History

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

Table 1: Document Change History

Date	Change	Location
2024-04-08	Indicated that Cisco DNA Center does not support integration with Cisco ISE when both have IPv6 enabled.	Guidelines and Limitations, on page 22
2023-08-22	Added wireless API information for CleanAir configuration.	New and Changed Features in Cisco DNA Center Platform, on page 9
2023-08-18	Added a limitation about custom applications.	Guidelines and Limitations, on page 22
2023-08-07	Previously, the *Cisco DNA Center Release Notes* and the *Cisco DNA Center Platform Release Notes* were separate. Now, they are combined into a single release note; the Cisco DNA Center platform content has been consolidated into this document.	—
2023-07-06	Noted that if you run Cisco DNA Center in IPv6 mode, wireless controller provisioning is not supported.	Guidelines and Limitations, on page 22
2023-06-12	Updated the upgrade limitations.	Guidelines and Limitations, on page 22
2023-06-07	Noted that if you run Cisco DNA Center in IPv6 mode, LAN automation is not supported.	Guidelines and Limitations, on page 22
2023-05-18	Added information about using the Validation Tool to run preupgrade checks.	Upgrade to the Latest Cisco DNA Center Release, on page 2

Date	Change	Location
2023-05-16	Updated the release version for 2.3.6.0 to 2.3.6.0.70351. (The original release version was 2.3.6.0.70349.)	Package Versions in Cisco DNA Center, Release 2.3.6.0, on page 2
	Updated the system version for 2.3.6.0 to 1.7.905. (The original system version was 1.7.899.)	
	Added the resolved bug CSCwe27848, which is resolved when you install the latest 2.3.6.0 release version and system version.	Resolved Bugs, on page 30
	Added the open bugs CSCwf06516 and CSCwf30218.	Open Bugs, on page 29
2023-04-06	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 2.3.6.0

Package Name	Release 2.3.6.0	
Release Build Version		
Release Version	2.3.6.0.70351	2.3.6.0.70349
System Updates		
System	1.7.905	1.7.899
System Commons	2.1.660.60918	
Package Updates		
Access Control Application	2.1.660.60918	
AI Endpoint Analytics	1.10.230	
AI Network Analytics	2.12.11.99	
Application Hosting	2.2.02302081007	
Application Policy	2.1.660.117387	
Application Registry	2.1.660.117387	
Application Visibility Service	2.1.660.117387	

Package Name	Release 2.3.6.0
Assurance - Base	2.3.6.277
Assurance - Sensor	2.3.6.269
Automation - Base	2.1.660.60918
Automation - Intelligent Capture	2.1.660.60918
Automation - Sensor	2.1.660.60918
Cisco DNA Center Global Search	1.11.1.3
Cisco DNA Center Platform	1.11.1.193
Cisco DNA Center UI	1.7.4.162
Cisco Identity Services Engine Bridge	2.1.660.80670
Cisco Umbrella	2.1.660.590363
Cloud Connectivity - Contextual Content	2.7.1.360
Cloud Connectivity - Data Hub	1.11.26
Cloud Connectivity - Tethering	2.32.1.32
Cloud Device Provisioning Application	2.1.660.60918
Command Runner	2.1.660.60918
Device Onboarding	2.1.660.60918
Disaster Recovery	2.1.660.360048
Disaster Recovery—Witness Site	2.1.660.370028
Group-Based Policy Analytics	2.3.6.13
Image Management	2.1.660.60918
Machine Reasoning	2.1.660.211330
NCP - Base	2.1.660.60918
NCP - Services	2.1.660.60918
Network Controller Platform	2.1.660.60918
Network Data Platform - Base Analytics	2.3.5.38
Network Data Platform - Core	1.9.2017
Network Data Platform - Manager	1.9.2028
Network Experience Platform - Core	2.1.660.60918

Package Name	Release 2.3.6.0
Path Trace	2.1.660.60918
RBAC Extensions	2.1.660.1900013
Rogue and aWIPS	2.8.0.22
SD-Access	2.1.660.60918
Stealthwatch Security Analytics	2.1.660.1090356
Support Services	2.1.660.880026
Wide Area Bonjour	2.4.660.75403

New and Changed Information

New and Changed Features in Cisco DNA Center

Feature	Description
Add Third-Party Device to Inventory	You can add a third-party device to your **Inventory** manually.
Automatic NETCONF Enablement Support	NETCONF is automatically configured on port 830 during device onboarding using plug and play. Automatic NETCONF enablement support is available only for Cisco Catalyst 9000 Series Switches running Cisco IOS-XE Version 17.3 or later.
Cisco AI Endpoint Analytics Dashlet on Home Page	The Cisco DNA Center home page has a dashlet that takes you to the AI Endpoint Analytics dashboard (or lets you enable AI Endpoint Analytics if it isn't already installed). The dashlet provides information about the endpoints that are connected to your network, including profiled endpoints, trust score alerts, and AI rules.
Create Network Device Group (NDG) Tag	You can create a new NDG tag and add it to the devices in the **Inventory** window.
Credential Update Restriction for Third-Party Devices	You cannot update the credentials of third-party devices discovered by Cisco DNA Center.
Dynamic Channel Assignment (DCA) Validation	DCA channel support is based on the regulatory domain of a device. During AP provisioning, only the channels that are supported as per the country code are considered, and the unsupported channels are ignored. You can view the list of unsupported channels in the Preprovision Summary window.
Enable AP Impersonation	The wireless network settings dashboard now includes an option to configure an AP impersonation.
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 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.

Feature	Description
Enhancements to AP Selection in the AP Configuration Workflow	The **Configure Access Points** workflow has the following enhancements on the **Select Access Points** window: • You can select a maximum of 2000 sites. • You can choose the necessary APs from the **Assigned APs** and **Unassigned APs** tab. • You can use the search icon to filter the APs listed in the **Access Points** table using quick filters, advanced filters, and recent filters. • You can click the gear icon in the top-right corner of the **Access Points** table to edit or customize the table.
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 CleanAir Pro and CleanAir Spectrum Intelligence Settings During AP Configuration	In the **Configure Access Points** workflow, the CleanAir Pro and CleanAir spectrum intelligence settings are enhanced. You can now enable or disable the radio band-specific CleanAir Pro and CleanAir spectrum intelligence parameter settings for APs in the **Configure AP Parameters** window. **Note** These settings are no longer available in the **Configure 5 GHz Radio Parameters**, **Configure 2.4 GHz Radio Parameters**, **Configure Dual-Band (XOR) Radio Parameters**, and **Configure Tri-Radio Parameters** windows of the AP configuration workflow. To configure these settings, in the **How do you want to configure APs?** window, you must check the **Configure AP Parameters** check box.
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
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.

Feature	Description
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.
Enhancements to the Wireless Network Settings Dashboard	The wireless network settings dashboard is enhanced to display the network settings in a card-based view. You can use the **Search All Settings** option to search for specific settings in the dashboard. You can customize the wireless network settings dashboard to update the priorities of the settings displayed in the dashboard using the **Edit Dashboard** option.
Feature-Based Trials	You can create feature-based trials for security advisories and system bug identifier.
MRE-Based Cisco Wireless Controller HA Health Check and Troubleshooting	You can troubleshoot any high-availability (HA) issues on Cisco Catalyst 9800 Series Wireless Controllers using the Machine Reasoning Engine (MRE) workflow. MRE workflow analyzes the HA health of wireless controllers by processing the relevant command outputs.
Multiple Cisco DNA Center—Limited Availability	Multiple Cisco DNA Center allows you to define a single global set of virtual networks for Software-defined access across multiple Cisco DNA Center clusters integrated with a single Cisco ISE system. This Multiple Cisco DNA Center functionality is a Limited Availability offering. Because there are significant caveats for the Multiple Cisco DNA Center functionality, the Cisco SD-Access Design Council reviews the requests and provides guidance for use of the Multiple Cisco DNA Center to participants in the Limited Availability program. Contact your account team to submit a request to the Cisco SD-Access Design Council to participate in the Limited Availability program. Customers who are using Cisco ISE Version 3.1 or earlier must request and install the Limited Availability package before enabling Multiple Cisco DNA Center. **Note** After this functionality is enabled, it can be disabled only by deleting Cisco ISE. In addition, if this functionality is enabled, because pxGrid is a required component of the solution, pxGrid cannot be disabled subsequently.
My Favorites	For ease of use, you can add any window on Cisco DNA Center to **My Favorites**. **My Favorites** is a list of windows that you have marked as favorites with hyperlinked pathways, to help you navigate to a window quickly and easily.
Resilient Ethernet Protocol (REP) Ring	You can add a device to an existing REP ring for nonfabric deployment.
Rogue General Configuration	You can create a model configuration design for rogue general parameters.

Feature	Description
Show Firepower Threat Defense (FTD) High Availability (HA) Paired Device Details in Inventory	The **Inventory** window shows the available FTD HA pairs with details of active and standby FTDs.
Single Connection Enablement for TACACS	You can configure switches with a single connection between the device and the TACACS server.
Software Image (SWIM) Workflow Upgrade	The **Software Image Update** workflow is enhanced in this release.
Support for Additional Interfaces for Wireless Network Profiles	An additional interface on a Cisco Wireless Controller maps a WLAN to a VLAN or subnet. You can configure additional interfaces for network profiles for wireless.
Support for AP Configuration Using Template in the AP Configuration Workflow	The **Configure Access Points** workflow now includes an option to configure APs using existing templates. You can use the **Create Template for selected Configuration(s)** option in the **Configure AP And Radio Parameters** workflow to create a new template.
Support for Cloning RF Profiles	You can clone the existing basic RF profiles and AI RF profiles.
Support for Editing Channel and Tx Power Settings on Planned APs	In 2D and 3D wireless maps, you can change the channel and Tx power settings for the planned APs.
Support for Individual AP Maintenance Mode	You can schedule maintenance individually for one or more APs when the corresponding Cisco Wireless Controller is not under maintenance mode.
Support for Zero-Wait Dynamic Frequency Selection (DFS) on APs	Zero-wait DFS support is now available on the Cisco Catalyst 9136 Wi-Fi 6E Access Point.
SWIM Flow Restrictions	For third-party devices, you can only perform basic SWIM operations. You cannot perform image update or image management for third-party devices.
Topology Support for Third-Party Devices	Third-party devices monitored by Cisco DNA Center are shown in the **Topology** map with the generic device icon. You can add tags to the third-party devices using the **Topology** map.
View Field Notices	You can view the **Field Notices** and **Potential Field Notices** in your network.
View PSRIT Software Maintenance Update (SMU) details	The Image Update Status workflow is enhanced, you can now view the additional PSRIT SMU related details.
Visibility of Compliance Remediation	To fix compliance violations, you can review the configurations that are deployed on the network device.
Visibility of Template Hub	The commands used in the CLI templates can be reviewed prior to deployment on network devices.
Visibility of Unmanaged Switches	In 2D wireless floor maps, you can view the unmanaged switches that are connected to the managed APs.

Feature	Description
Visibility of Wireless Device Configurations	The Visibility of Wireless Device Configurations feature provides a solution to further secure your planned wireless network configurations before deploying them on your devices. You can enforce previewing the wireless device configurations before deploying them. **Configuration Preview** is enabled by default. You can update this setting on the **System** > **Settings** > **Visibility of Configurations** window. **Note** If there is a conflicting operation when you deploy your planned network configurations, the **Pending Operations** dialog box is displayed. To proceed with the current deployment, you must either wait for the existing, scheduled, or pending-review operations to complete or discard the operations.
Web Content Accessibility Guidelines (WCAG) 2.1 AA Compliance: Keyboard Accessibility Support	You can use the keyboard to access all interactive content in the Cisco DNA Center GUI. Those who cannot use a mouse can access and move between links, buttons, fields, and other controls using the **Tab** key and other keystrokes.

New and Changed Features in Cisco DNA Assurance

Feature	Description
Assurance Device HA Enhancement	With this release, the **Device** tab in the Detailed Information dashlet of the **Device 360** dashboard displays the following **HA Redundancy** state details for wireless controllers: • Local State - READY (ACTIVE) • Peer State - READY (STANDBY HOT)
Automatic Issue Resolution	With this release, the system automatically resolves the following issue types: • Network Device Interface Connectivity - BGP Flap • Interface is Flapping On Network Device
Client 360 Dashboard Enhancements	In the **Summary** dashboard on the **Client 360** window, you can view a list of average latency access categories such as voice, video, background, and the best effort for a particular client. You can click the hyperlinked view details to view more details on client **Average Latency** by **Access Category**.
Custom Profile - User Defined Issue Enhancement	You can edit the **User Defined** issue details of **Custom Profiles** in the **Issues Settings** window.
Endpoint Analytics Assurance Integration	With this release, the **Client Devices** table in the **Assurance Client Health** dashboard shows additional information, such as **Trust Score**, Multi-Factor Classification (MFC) attributes such as **Hardware Manufacturer**, **OS**, **Device Type**, and **Endpoint Type** for the endpoints connected to your network as observed from Cisco AI Endpoint Analytics.
New Fabric Extranet Policy Issue	With this release, the Fabric Extranet Policy Status issue is added to **Core, Distribution, and Access** issues under the **Connectivity** category. The Fabric Extranet Policy Status issue is triggered if the extranet policy state is Down on a control plane at a fabric site. The issue is automatically resolved when the extranet policy status is Up.

Feature	Description
OTA Sniffer Packet Capture	You can run OTA Sniffer packet captures for the Access points using the certain WIFI radio channels.
PoE Dashlet Enhancements	With this release, the **PoE** dashboard is enhanced with the following dashlets: • **AP Power Savings** • **AP Power Save Mode Distribution**
Site Analytics Enhancement	You can view and monitor the Site Analytics KPI data through bubble chart view to identify the impacted sites of your network with the impacted entities such as APs, Clients, and Device Types.
Support for RRM Simulation on **6-GHz** Radio Band	You can now use the RRM simulator for the **6-GHz** radio band.
Support for SSID Monitoring Settings	You can enable or disable (SSID) monitoring for specific SSIDs, without impacting the SSID configuration or wireless connection to these SSIDs. When an SSID isn't monitored, Assurance doesn't collect the client data for the SSID.

New and Changed Features in Cisco DNA Center Platform

Feature	Description
New API Features	

Feature	Description
API Enhancements	The Cisco DNA Center platform supports the following API enhancements: • **SD-Access** APIs: The `InterfaceName` parameter in the **Get Port assignment for user device** API now accepts multiple interface names. • **Devices** APIs: • The **Get Device list** API now includes the `Vendor` attribute as a query(filter) and response parameter. • The `Password` attribute in the **Export Device List** API is now a required field. • **Wireless** APIs: The **Configure Access Points** API, POST <cluster-ip>/dna/intent/api/v1/wireless/accesspoint-configuration API now includes the `isAssignedSiteAsLocation` parameter. The v1 version of the API uses the `configureCleanAirSI` and `cleanAirSI` parameters to push slot-specific CleanAir configuration to the devices. These parameters are applicable for devices running Cisco IOS XE Release 17.8 and earlier. **Note** For multiple devices, if one of the devices is running Cisco IOS XE Release 17.9 or later, an error message is displayed indicating the AP on which CleanAir can't be configured. For a device running Cisco IOS XE Release 17.9 or later, you must use the v2 version of the API. To access the APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**.

Feature	Description
Devices APIs	The Cisco DNA Center platform supports the following new **Devices** APIs: • DELETE <cluster-ip>/dna/intent/api/v1/floors/${floorId}/planned-access-points/${plannedAccessPointUuid} Delete Planned Access Point for Floor. • GET <cluster-ip>/dna/intent/api/v1/floors/${floorId}/planned-access-points Create Planned Access Point for Floor. • PUT <cluster-ip>/dna/intent/api/v1/floors/${floorId}/planned-access-points Update Planned Access Point for Floor. • PUT <cluster-ip>/dna/intent/api/v1/network-device Update Device Details. • PUT <cluster-ip>/dna/intent/api/v1/network-device/${deviceid}/management-address Update Device Management Address. To access the new **Devices** APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know your Network** drop-down list and choose **Devices**.
Event Management APIs	The Cisco DNA Center platform supports the following **Event Management** APIs: • POST <cluster-ip>/dna/intent/api/v1/event/snmp-config Create SNMP Destination. • PUT <cluster-ip>/dna/intent/api/v1/event/snmp-config Update SNMP Destination. To access the new **Event Management** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. In the left hierarchy, choose **Event Management**.

Feature	Description
SDA APIs	The Cisco DNA Center platform supports the following new SDA APIs: • GET <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies/count Get extranet policy count. • POST <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies Add extranet policy. • GET <cluster-ip>/dna/intent//api/v1/sda/extranetPolicies Get extranet policy. • DELETE <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies/${id} Delete extranet policy by ID. • PUT <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies Update extranet policy. To access the new **SDA** APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Connectivity** drop-down list and choose **SDA**.
Sites APIs	The Cisco DNA Center platform supports the following new **Sites** APIs: • DELETE <cluster-ip>/dna/intent/api/v1/maps/import/${importContextUuid} Import Map Archive - Cancel an Import. • GET <cluster-ip>/dna/intent/api/v1/maps/supported-access-points Maps supported Access Points. • GET <cluster-ip>/dna/intent/api/v1/maps/import/${importContextUuid}/status Import Map Archive - Import Status. • POST <cluster-ip>/dna/intent/api/v1/maps/import/${importContextUuid}/perform Import Map Archive - Perform Import. • POST <cluster-ip>/dna/intent/api/v1/maps/import/start Import Map Archive - Start Import. • POST <cluster-ip>/dna/intent/api/v1/maps/export/${siteHierarchyUuid} Export Map Archive. To access the new **Sites** APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know your Network** drop-down list and choose **Sites**.

Feature	Description
Wireless API	The Cisco DNA Center platform supports the following new **Wireless** API: POST <cluster-ip>/dna/intent/api/v2/wireless/accesspoint-configuration Configure access points. The v2 version of the API uses the `configureCleanAirSI24Ghz`, `cleanAirSI24`, `configureCleanAirSI5Ghz`, `cleanAirSI5`, `configureCleanAirSI6Ghz`, and `cleanAirSI6` parameters to push band-specific CleanAir configuration to the devices. These parameters are applicable for devices running Cisco IOS XE Release 17.9 and later. **Note** If you use the v2 version of the API, either slot-specific or band-specific CleanAir configuration is pushed to the devices based on the device version. If you use both v1 and v2 versions of the API, both slot-specific and band-specific CleanAir configuration is pushed to the devices based on the device versions. 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 Events Features	
Assurance Event	This release supports the following new Assurance event: Fabric Extranet policy status: The event is generated when the Fabric Extranet policy status is down. For information about events and setting up a notification for an event, see the *Cisco DNA Center Platform User Guide*.
Compliance Event	This release supports the following new Compliance event: Device config collection event: Cisco DNA Center shows a config drift event across the selected list of devices. For information about events and setting up a notification for an event, see the *Cisco DNA Center Platform User Guide*.
New Reports	

Feature	Description
Flexible Report	This release supports a new **Flexible Report** that allows you to generate customized reports for wired and wireless networks. • In Phase 1, Flexible report supports the following Assurance entities: • Access Point • Clients (Wired and Wireless) • Network Devices • The types of configurations that are supported for each entity are as follows: • Trend • Summary • Top N • Distribution • You can create multiple subreports within each Flexible report. • The supported report file format is **CSV**. • Flexible report allows you to generate or view separate **CSV** files for each subreport, or you may download or view related subreports together as a **ZIP** file. • Each entity has its own associated field sets, aggregations, group-by and sort-by options. • In the **Schedule Report** window, the available schedule options are **Now**, **Later (One Time only)**, and **Recurring**. **Note** Use the **Later (One Time only)** option to customize the date and time interval, and the time zone (GMT) for the time range. Use the **Recurring** option to schedule the days and time along with the time zone (GMT). • To generate a Flexible report, click the menu icon and choose **Report** > **Reports Templates** > **Generate a Flexible Report**. • For more information, see **Generate a Flexible Report** in *Cisco DNA Center Platform User Guide*.
New Reports Features	

Feature	Description
New Reports GUI Features	Cisco DNA Center platform support is extended for enhancements in the following reports: • **Client Summary** report: In this release, the distribution charts (Client Count, Client Traffic, and Client Sessions) are classified and displayed by Protocol and SSID. For example, the **Client Summary** report classified by SSID displays the **Client Count by SSID**, **Client Traffic by SSID**, and **Client Sessions by SSID** charts. • **Client Trend** report: The **Associated Wireless Client Count** and **Authenticated Wireless Client Count** charts are added to the report. **Note** The Associated and Authenticated Wireless charts are available for 30 days. • **Client Details** report: The **Total Session Time (in hours)** field is added to the report. • **AP Radio** report: The **Average RX Utilization (%)** and **Average TX Utilization (%)** fields are added to the report. For more information about creating reports, see the *Cisco DNA Center Platform User Guide*.

New and Changed Features in Cisco DNA Automation

Feature	Description
Configure Visibility	To further secure your devices, you can preview device configurations before deploying them into your network. This feature offers visibility into your devices.

New and Changed Features in Cisco Software-Defined Access

Feature	Description
Customize Loopback Address of Devices in the Underlay	Devices that are onboarded through LAN automation can have a customized loopback IP address. (Earlier, Cisco DNA Center would assign a random IP address as the loopback address of a device.) The LAN automation workflow provides an option to assign a loopback IP address for all the devices in the underlay network. A custom loopback IP address can be provided in the third column of the CSV file for Day 0 operation during the start of LAN automation. The **Stop LAN Automation** process provides you an option to change the loopback IP address. You can also edit the loopback IP address on Day n, through the **Edit Device** option in the **LAN Automation** window.
Customize the TCP MSS Adjustment Value	You can choose a **TCP MSS Adjustment** value for the TCP sessions on the Layer 3 handoff interfaces.

Feature	Description
Integrate Multiple Cisco DNA Center Clusters with a Single Cisco ISE System	You can integrate multiple Cisco DNA Center clusters with a single Cisco ISE system. To facilitate global administration of SD-Access across multiple Cisco DNA Center clusters with a consistent set of virtual networks, the Multiple Cisco DNA Center feature leverages the existing secure connection with Cisco ISE to propagate virtual networks, Security Group Tags (SGTs), access contracts, and Group-Based Access Control (GBAC) Policy from one cluster to another cluster, all integrated with the same Cisco ISE deployment. Cisco ISE takes the information learned from one cluster (the Author node) and propagates it to the other clusters (Reader nodes).
Support for Smaller IP Pools during LAN Automation	LAN automation workflow now accepts /29 and /28 mask for IP pool assignments. Smaller IP pools help in minimizing the unused IP addresses for small branch deployments. From this release, the internal /27 IP pool creation is dissolved, which in turn provides efficient IP pool usage in the IPAM. It minimizes IP address wastage that might occur because of dummy subnet creation from the main IP pool.
Visibility of Cisco SD-Access Fabric Configurations	You can view the configurations before they are deployed on the devices in the fabric network. During the provisioning of an SD-Access fabric, you can generate a preview of the device configurations (CLI commands) and either deploy or discard them.

New and Changed Features in Interactive Help

Feature	Description
Deprecated Walkthroughs	Create an Enterprise SSID and associate with a Network Profile
New Walkthroughs	• Enable Visibility of Configurations • Use the Wireless Network Settings Dashboard

Deprecated Features

In the Cisco Wide Area Bonjour service filter policy configuration XLS template, the **Selective Services (Advanced)** sheet is deprecated. For advanced service routing scenarios where service distribution from Cisco DNA Center must be limited to a specific user endpoint (connected port) or VLAN, you can use location groups.

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 2.3.6, 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*.

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 these categories of data—Cisco.com ID, System, Feature Usage, Network Device Inventory, and License Entitlement. See the *Cisco DNA Center Data Sheet* for a more expansive list of data that we collect. To opt out of some of the data collection, contact your Cisco account representative or Cisco TAC.

Supported Hardware Appliances

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

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

Installing Cisco DNA Center

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

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

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

Support for Cisco Connected Mobile Experiences

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

⚠

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

Plug and Play Considerations

General Feature Support

Plug and Play supports the following features, depending on the Cisco IOS software release on the device:

- AAA device credential support: The AAA credentials are passed to a device securely and the password is not logged. This feature allows provisioning a device with a configuration that contains the **aaa authorization** commands. This feature requires software release Cisco IOS 15.2(6)E1, Cisco IOS 15.6(3)M1, Cisco IOS XE 16.3.2, or Cisco IOS XE 16.4 or later on the device.
- Image install and upgrade for Cisco Catalyst 9200 Series, Catalyst 9300 Series, Catalyst 9400 Series, Catalyst 9500 Series, Catalyst 3650 Series, and Catalyst 3850 Series switches are supported only when the switch is booted in install mode. (Image install and upgrade are not supported for switches booted in bundle mode.)

Secure Unique Device Identifier Support

The Secure Unique Device Identifier (SUDI) feature that allows secure device authentication is available on the following platforms:

- Cisco routers:
  - Cisco Catalyst IR 1800 Series with software release Cisco IOS XE 17.5.1 and later
  - Cisco ISR 1100 Series with software release Cisco IOS XE 16.6.2
  - Cisco ISR 4000 Series with software release Cisco IOS XE 3.16.1 or later, except for the ISR 4221, which requires release Cisco IOS XE 16.4.1 or later
  - Cisco ASR 1000 Series (except for 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.

Guidelines and Limitations

Cloud Connectivity Through SSL Intercept Guidelines

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

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

⚠

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

Backup and Restore Guidelines

- You cannot take a backup of one version of Cisco DNA Center and restore it to another version of Cisco DNA Center. You can only restore a backup to an appliance that is running the same Cisco DNA Center software version, applications, and application versions as the appliance and applications from which the backup was taken.

- After performing a restore operation, update your integration of Cisco ISE with Cisco DNA Center. After a restore operation, Cisco ISE and Cisco DNA Center might not be in sync. To update your Cisco ISE integration with Cisco DNA Center, choose **System** > **Settings** > **Authentication and Policy Servers**. In the **Actions** column, click **Edit** adjacent to the corresponding server. Enter your Cisco ISE password to update.

- After performing a restore operation, the configuration of devices in the network might not be in sync with the restored database. In such a scenario, you should manually enter the CLI commands that are pushed for authentication, authorization, and accounting (AAA) and configuration on the network devices. See the corresponding network device documentation for information about the CLI commands to enter.

- Re-enter the device credentials in the restored database. If you updated the site-level credentials before the database restore, and the backup that is being restored 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 only Automation data or both Automation and Assurance data. But you cannot use the GUI or the CLI to back up or restore only Assurance data.

Cisco ISE Integration Guidelines

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

- Full certificate chains must be uploaded to Cisco DNA Center while replacing an existing certificate. If a Cisco DNA Center certificate is issued by a subCA of a rootCA, the certificate chain uploaded to Cisco DNA Center while replacing the Cisco DNA Center certificate must contain all three certificates.

- Self-signed certificates applied on Cisco DNA Center must have the Basic Constraints extension with cA:TRUE (RFC5280 section-4.2.19).
- The IP address or FQDN of both Cisco ISE and Cisco DNA Center must be present in either the **Subject Name** field or the **Subject Alt Name** field of the corresponding certificates.
- If a certificate is replaced or renewed in either Cisco ISE or Cisco DNA Center, trust must be re-established.
- The Cisco DNA Center and Cisco ISE IP address or FQDN must be present in the proxy exceptions list if there is a web proxy between Cisco DNA Center and Cisco ISE.
- Cisco DNA Center and Cisco ISE nodes cannot be behind a NAT device.
- Cisco DNA Center and Cisco ISE cannot be integrated if the Cisco ISE Admin and Cisco ISE pxGrid certificates are issued by different enterprise certificate authorities.

  Specifically, if the Cisco ISE Admin certificate is issued by *CA server A*, the Cisco ISE pxGrid certificate is issued by *CA server B*, and the pxGrid persona is running on a node other than Cisco ISE PPAN, the pxGrid session from Cisco DNA Center to Cisco ISE 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

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

License Limitations

- After changing the enterprise IP address or FQDN, before you attempt a licensing-related task, all services must be up and running.
- The Cisco DNA Center License Manager supports Smart Licensing only for wireless controller models that run Cisco IOS XE. The License Manager 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 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.

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 device configuration only once per controller.
- Cisco DNA Center can learn only one wireless controller at a time.
- For site profile creation, only the AP groups with AP and SSID entries are considered.
- Automatic site assignment is not possible.
- SSIDs with an unsupported security type and radio policy are discarded.
- For authentication and accounting servers, if the RADIUS server is present in the device, it is given first preference. If the RADIUS server is not present, the TACACS server is considered for design.
- The Cisco ISE server (AAA) configuration cannot be learned through existing device provisioning.
- The authentication and accounting servers must have the same IP addresses for them to be learned through existing device provisioning.
- When an SSID is associated with different interfaces in different AP groups, during provisioning, the newly created AP group with the SSID is associated with the same interface.
- A wireless conflict is based only on the SSID name and does not consider other attributes.

High Availability Limitation

Cisco DNA Center does not support HA for the Cisco Embedded Wireless Controller on Catalyst Access Points.

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, 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.

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.

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

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

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

Encryption Limitation with SNMPv3

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

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

IPv6 Limitations

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

- Access Control Application, Group-Based Policy Analytics, SD Access, and Cisco AI Endpoint Analytics packages are disabled and cannot be downloaded or installed.

- Communication through Cisco ISE pxGrid is disabled because Cisco ISE pxGrid does not support IPv6.

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

Cisco Plug and Play Limitations

- Virtual Switching System (VSS) is not supported.
- The Cisco Plug and Play mobile app is not supported with Plug and Play in Cisco DNA Center.
- The Stack License workflow task is supported for Cisco Catalyst 3650 and 3850 Series switches running Cisco IOS XE 16.7.1 and later.
- The Plug and Play agent on the switch is initiated on VLAN 1 by default. Most deployments recommend that VLAN 1 be disabled. If you do not want to use VLAN 1 when PnP starts, enter the following command on the upstream device:

  ```
  pnp startup-vlan <vlan_number>
  ```

Cisco Group-Based Policy Analytics Limitations

- Cisco Group-Based Policy Analytics supports up to five concurrent requests based on realistic customer data. While it is desirable for GUI operations to respond within 5 seconds or less, for extreme cases based on realistic data, it can take up to 20 seconds. There is no mechanism to prevent more than five simultaneous requests at a time, but if it does happen, it might cause some GUI operations to fail. Operations that take longer than 1 minute, time out.
- Data aggregation occurs at hourly offsets from UTC in Cisco Group-Based Policy Analytics. However, some time zones are at a 30-minute or 45-minute offset from UTC. If the Cisco DNA Center server is located in a time zone with a 30-minute or 45-minute offset from UTC, and the client is located in a time zone with an hourly offset from UTC, or vice versa, the time ranges for data aggregation in Cisco Group-Based Policy Analytics are incorrect for the client.

  For example, assume that the Cisco DNA Center server is located in California PDT (UTC-7), where data aggregations occur at hourly offsets (8:00 a.m., 9:00 a.m., 10:00 a.m., and so on). When a client located in India IST (UTC+5.30) wants to see the data between 10:00 to 11:00 p.m. IST, which corresponds to the time range 9:30 to 10:30 a.m. PDT in California, no aggregations are seen.
- Group changes that occur within an hour are not captured. When an endpoint changes from one security group to another, Cisco Group-Based Policy Analytics is unaware of this change until the next hour.
- You cannot sort the Security Group and Stealthwatch Host Group columns in the **Search Results** window.
- You might see discrepancies in the information related to Network Access Device (including location) between Assurance and Cisco Group-Based Policy Analytics.

Application Telemetry Limitation

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

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

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

The following syntax is invalid:

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

IP Address Manager Limitations

- Infoblox limitations:
  - Infoblox 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 may 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 the 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 may see the following error message:

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

  To correct this error for a self-signed certificate:

  1. Using OpenSSL, enter one of the following commands to download the self-signed certificate, depending on your IPAM type. (You can specify the FQDN [domain name] or IP address in the command.)
     - `openssl s_client -showcerts -connect Infoblox-FQDN:443`
     - `openssl s_client -showcerts -connect Bluecat-FQDN:443`

2. From the output, use the content from ---BEGIN CERTIFICATE--- to ---END CERTIFICATE--- to create a new .pem file.

3. Go to **System** > **Settings** > **Trust & Privacy** > **Trustpool**, click **Import**, and upload the certificate (.pem file).

4. Go to **System** > **Settings** > **External Services** > **IP Address Manager** and configure the external IPAM server. (If the IPAM server is already configured, skip this step.)

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

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

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

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

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

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

To correct this, do the following:

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

2. Confirm that the parent pool CIDR exists in the external IPAM server, and remove all the child pools that are configured under that parent pool.

3. Return to the Cisco DNA Center GUI and reconfigure the IPAM server under **System** > **Settings** > **External Services** > **IP Address Manager**.

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

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

To correct this, do the following:

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

2. Regenerate your external IPAM certificate with the common name (CN) value as the valid hostname or IP address. In the preceding example, the CN value is `www.infoblox.com`, which is not the valid hostname or IP address of the external IPAM.

3. After you regenerate the certificate with a valid CN value, go to **System** > **Settings** > **Trust & Privacy** > **Trustpool**.

4. Click **Import** and upload the new certificate (.pem file).

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

Reports Limitation

Reports with significant data can sometimes fail to generate in the Cisco DNA Center platform. If this occurs, we recommend that you use filters to reduce the report size to prevent such failures.

Custom Application Limitation

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

Bugs

Open Bugs

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

Bug Identifier	Headline
CSCwe22715	The destination email top-level domain cannot exceed 6 characters.
CSCwe32856	In Cisco DNA Center, when you disable a custom attribute (for example, zero-wait DFS or channel width) for an RF profile, that attribute on the RF profile is not disabled on the device unless the parent profile is Custom.
CSCwe39344	When you configure a webhook destination and REST channel, Cisco DNA Center allows you to configure only one event notification. The following error message displays when you try to create another event notification: `Endpoint Connection Timed Out.`
CSCwe44689	Templates get detached from network profiles after upgrading from Cisco DNA Center 2.3.5.3 to 2.3.6.
CSCwe46347	ITSM communication breaks after upgrading from ISO 275 TO 284.
CSCwe47027	Disaster Recovery system: The System Analyzer generates an error when run on the recovery system after a failover.
CSCwe48575	The AP zone banner message regarding wireless controller reprovisioning is not shown in Cisco DNA Center.
CSCwe59920	The Device Controllability configuration is repushed on a credential change with the same configuration.
CSCwe63689	If you enter the CLI username with privilege level 15 and an incorrect ENABLE password, the credential validation shows the CLI credential status as successful (with a green icon), even though the password is incorrect.
CSCwe68032	Due to a wireless management IP issue, the Fabric CP does not get the wireless configuration under LISP.
CSCwe69389	Enabling the NBAR Cloud Connector fails due to an authentication failure.

Bug Identifier	Headline
CSCwe70250	The CMDB bundle is not working.
CSCwe75205	Upgrade fails on a scale cluster while doing an intra-build upgrade from Cisco DNA Center 2.3.6.0-70321 to 2.3.6.0-70326.
CSCwe79044	After creating and deploying a policy under Group-Based Access Control, when you try to edit the policy, the drop-down menu doesn't work. You cannot enable, disable, or monitor the policy.
CSCwf06516	You cannot create a REP ring in Cisco DNA Center if the following configuration is disabled manually: `rep ztp`
CSCwf30218	The "API_ENDPOINT_CREATE" workflow takes a long time to complete.

Resolved Bugs

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

Bug Identifier	Headline
CSCwb23437	The image update status is shown as successful, even though the image update failed on the controller.
CSCwb88301	Creation of SSID without AAA configuration fails if Cisco ISE added in **System Settings** is in Error/Failed state.
CSCwb99632	SWIM report generation fails when the run time exceeds the defined maximum running time for the worker pod (16 hours).
CSCwc05125	Cisco Wireless Controller fails compliance with a mismatch in "WLAN policy profile name" - PP uniqueness.
CSCwc28483	The service entitlement check fails during the image upgrade readiness check for devices in Inventory.
CSCwc39603	When a user configures 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`
CSCwc42824	AP provisioning fails because Cisco DNA Center pushes duplicate commands sequentially.
CSCwc55872	Disabling a band on an RF profile should disable the admin status on the corresponding RF profile on the Cisco Catalyst 9800 Series Wireless Controller.
CSCwc76362	After a sync-with-cleanup API call, devices show the following internal error: `Exception while persisting: java.lang.NullPointerException.`
CSCwc94852	Cannot provision or delete a wireless controller due to the following error: `NCSP11108 CFS persistence failed.`
CSCwd08474	Reprovisioning BAPI fails with the following error: `Interface Input Error: Duplicate IP found.`

Bug Identifier	Headline
CSCwd13881	Cisco DNA Center shows the slot 2 radio on Cisco Aironet 2800 Series APs. On the Network Hierarchy, APs show the slot 2 radio as down. On the Device Detail configuration, APs show slot 2 configuration information. There is no slot 2 configuration on the wireless controllers on the affected APs.
CSCwd21514	During the report generation process, the token of the user who generated the report is stored and displayed to other users, which results in security vulnerabilities.
CSCwd22124	Cisco DNA Center is slow to identify the AP IP address.
CSCwd27862	Using Cisco DNA Center APIs, you cannot retrieve all applicable PIDs for an image.
CSCwd31345	The FlexConnect ACL is repushed on every wireless controller provisioning with the same entries.
CSCwd35888	There is a typo on the MESH Bridge configuration page.
CSCwd37822	First-time reprovision of an embedded wireless controller causes WLAN SSIDs to flap.
CSCwd38863	WIPS is removed from AP profile "default-ap-profile" during Cisco Catalyst 9800 Series Wireless Controller provisioning even when "Enable aWIPS" is checked in wireless network settings.
CSCwd42385	Changes in RF profile should be taken into consideration during wireless controller provisioning.
CSCwd46613	When configuring notifications under **Event Notification**, notification sites in View and Edit are intermittently different.
CSCwd46904	Software image upgrade fails from older versions 16.6.x to 17.x for Cisco Catalyst 9410 devices.
CSCwd66051	Cisco DNA Center shows the IOS telemetry subscription as successful irrespective of device subscription status.
CSCwd65835	Redundant configuration pushed when adding a port after deleting couple of ports.
CSCwd75501	When you rerun the Security Advisory report, it fails and displays the following error: `BAPI Execution Failed.Response Code = 500, Response Content=null`
CSCwe14548	Unable to execute the AP refresh workflow using Role Based Access Control (RBAC).
CSCwe17325	Cisco Catalyst 3850 device running Cisco IOS XE 16.12.x in Install mode - Base image getting deleted before SMU is copied to the switch.
CSCwe25719	After upgrading Cisco DNA Center to 2.3.3.5, policy-tag config breaks in some SSID WLAN profile during the provisioning of modified N+1 wireless controllers.
CSCwe27848	After disaster recovery failover, postgres-0 and postgres-1 run as the primary.
CSCwe33233	AP provisioning and AP refresh workflow fails as Cisco DNA Center trying to enable 6-Ghz radio for Cisco Catalyst 9136 AP.
CSCwe38704	Site information is ignored when performing bulk import of devices to PnP on Cisco DNA Center 2.3.5.

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*

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