Release Notes for Cisco DNA Center, Release 2.3.3.0

First Published: 2022-04-26

Release Notes for Cisco DNA Center, Release 2.3.3.0

Cisco DNA Center 2.3.3.0 is available in a phased rollout. Until the software becomes generally available, contact your Cisco sales representative to request this release. Upon completion of the phased rollout, Cisco DNA Center will be made generally available to all customers.

This document describes the features, limitations, and bugs for Cisco DNA Center, Release 2.3.3.0.

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

Upgrade to the Latest Cisco DNA Center Release

For information about upgrading your current release of Cisco DNA Center, see the *Cisco DNA Center Upgrade Guide*.

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

Package Versions in Cisco DNA Center, Release 2.3.3.0

The following table shows the updated packages and the versions in Cisco DNA Center, Release 2.3.3.0.

Package Name	Release 2.3.3.0
Release Build Version	
Release Version	2.3.3.0.70399
System Updates	
System	1.7.620
System Commons	2.1.510.60908
Package Updates	
Access Control Application	2.1.510.60908
AI Endpoint Analytics	1.7.626
AI Network Analytics	2.9.18.376
Application Hosting	1.9.02204011423

Package Name	Release 2.3.3.0
Application Policy	2.1.510.117310
Application Registry	2.1.510.117310
Application Visibility Service	2.1.510.117310
Assurance - Base	2.3.3.307
Assurance - Sensor	2.3.3.289
Automation - Base	2.1.510.60889
Automation - Intelligent Capture	2.1.510.60908
Automation - Sensor	2.1.510.60908
Cisco DNA Center Global Search	1.8.1.8
Cisco DNA Center Platform	1.8.1.96
Cisco DNA Center UI	1.7.1.289
Cisco Identity Services Engine Bridge	2.1.510.408
Cisco Umbrella	2.1.510.590230
Cloud Connectivity - Contextual Content	2.4.1.308
Cloud Connectivity - Data Hub	1.8.25
Cloud Connectivity - Tethering	2.30.1.66
Cloud Device Provisioning Application	2.1.510.60908
Command Runner	2.1.510.60908
Device Onboarding	2.1.510.60908
Disaster Recovery	2.1.510.36055
Group-Based Policy Analytics	2.3.3.29
Image Management	2.1.510.60908
Machine Reasoning	2.1.510.210344
NCP - Base	2.1.510.60908
NCP - Services	2.1.510.60908
Network Controller Platform	2.1.510.60908
Network Data Platform - Base Analytics	1.8.229
Network Data Platform - Core	1.8.256

Package Name	Release 2.3.3.0
Network Data Platform - Manager	1.8.189
Network Experience Platform - Core	2.1.510.60908
Path Trace	2.1.510.60908
RBAC Extensions	2.1.510.1900009
Rogue and aWIPS	2.5.0.20
SD-Access	2.1.510.60908
Stealthwatch Security Analytics	2.1.510.1090258
Support Services	2.1.510.880029
Wide Area Bonjour	2.4.510.75231

New and Changed Information

New and Changed Features in Cisco DNA Center

Table 1: New and Changed Features for Cisco DNA Center, Release 2.3.3

Feature	Description
Cisco DNA Center Insights	You can subscribe to *Cisco DNA Center Insights*, which contains product announcements, network highlights, information about your network performance, and more. The *Cisco DNA Center Insights* publication is sent in PDF format to the email address that you specify.
Cisco Device Hardware, Software, and Module End of Life (EoX) Status	Cisco DNA Center shows alerts for the devices that are scanned for EoX alerts. The **EoX Status** column in the Inventory table shows the number of EoX alerts.
Credential Status	The **Credential Status** column in the Inventory table shows the device credential status for devices that are configured. Click **See Details** to view the details about the credentials.
View All Discoveries	The new Discoveries table in Cisco DNA Center shows details of all discovery jobs and provides options to rediscover and delete discovery jobs.
Manage System Beacon	You can highlight switches in the Cisco DNA Center inventory by using a system beacon. System beacon supports the following devices: • Cisco Catalyst 3850 Series Ethernet Stackable Switches • Cisco Catalyst 9200 Series Switches • Cisco Catalyst 9300 Series Switches
Integrate Cisco AI Endpoint Analytics with Talos Intelligence	Talos Intelligence is a comprehensive threat-detection network. Talos detects and correlates threats in real time. By integrating Cisco AI Endpoint Analytics with Talos, you can flag endpoints in your network that are connecting to malicious IP addresses.

Feature	Description
Assign Device Roles and Tags to Software Images	You can assign device roles and tags to a software image to indicate that the software image is marked as golden. When both device tags and device roles are assigned to a software image, the device tags take precedence.
Sync Updates for Software Images	You can synchronize the information of software images from cisco.com for all managed devices in Cisco DNA Center.
FIPS 140-2 Support	Software images are compliant with the Federal Information Processing Standard (FIPS). If FIPS mode is enabled in Cisco DNA Center, you cannot import images from a URL. Import images from your computer or cisco.com.
	FIPS mode is supported only in a new installation of Cisco DNA Center. If you are upgrading from an earlier release, FIPS mode is not supported. **Note** FIPS mode is not supported for the Cisco Wide Area Bonjour application. In a FIPS deployment, you cannot install the Cisco Wide Area Bonjour application from the Cisco DNA Center GUI or CLI.
	FIPS mode has the following impact on the export and import of map archives. If FIPS mode is *enabled*: • Exported map archives are unencrypted. • Only unencrypted map archives may be imported. If FIPS mode is *disabled*: • Exported map archives are encrypted. • Both encrypted and unencrypted map archives may be imported.
FIPS Support for Endpoint Analytics	When FIPS mode is enabled in Cisco DNA Center, some of the functions related to Endpoint Analytics are *unavailable* in the Cisco DNA Center GUI.
View Image Update Workflow	You can view the progress of software image update tasks. Cisco DNA Center shows the status of each task that is associated with the Distribution and Activation operations and the amount of time taken to complete each operation.
Control Endpoint Spoofing	The Control Endpoint Spoofing feature provides granular policy control by providing network information other than just the MAC address of an endpoint.

Feature	Description

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

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

Manage Your Inventory	In the **Inventory** window, if you choose the **Default** view from the **Focus** drop-down list, the **Inventory** table displays only the **Device Name**, **IP Address**, **Device Family**, and **MAC Address** of listed devices.
NAS ID Configuration	You can configure network access server identifiers (NAS IDs) for SSIDs for enterprise and guest wireless networks.
Central Web Authentication Using Third-Party AAA Server for Guest Wireless Networks	You can now configure Central Web Authentication (CWA) using a third-party AAA server while creating SSIDs for guest wireless networks.

Feature	Description
Schedule Group-Based Access Control Policy Updates	You can save policy changes immediately or schedule an update at a specific time. You can view the status of the scheduled tasks in **Activities** > **Tasks**. If the **Cisco DNA Center Automation Events for ITSM (ServiceNow)** bundle is enabled, the **Save Now** option is disabled, and only the **Schedule Later** option is enabled for Group-Based Access Control policy changes. The scheduled task must be approved in IT Service Management (ITSM) before the scheduled time.
QoS Settings for Wireless Networks	You can choose one of the following QoS settings for the primary traffic while creating SSIDs for enterprise and guest wireless networks: • **VoIP (Platinum)** • **Video (Gold)** • **Best Effort (Silver)** • **Non-real Time (Bronze)**
Return Material Authorization (RMA) Support for New Devices	RMA Workflow support is extended for the following: • Cisco Catalyst 4500e, Catalyst 6500, Catalyst 6800 and Catalyst 9000 series modular switches. • Supervisors of modular switches with single and dual engines. • Extended node that is part of STP ring/daisy chain. • Daisy chain and ring of Industrial Ethernet (IE) switches. • Devices that have an external SCEP broker PKI certificate.
RMA Support	Zero-touch onboarding of replacement device via PnP is supported for fabric and LAN automation devices.
AP Refresh Across Cisco Wireless Controllers	You can perform an AP refresh when the old AP and new AP are connected to different Cisco Wireless Controllers. You can perform the AP refresh even if the old AP is not provisioned.
Design the Network Hierarchy	You can now search the network hierarchy by **Site Name** and **Site Type** filter criteria.
URL-Based Access Control List	You can create IP-based and URL-based post authentication access control lists (ACLs) for your network.
Custom Template for Day 0 Onboarding Without Site Selection	If you have not assigned the device to a site, you must choose a template to claim the device.
Application Hosting Enhancements	You can validate the HTTPS credentials provided for the device in the device readiness check.
Schedule Recurring Events for APs	You can schedule recurring events for AP and radio parameters in the AP configuration workflow.

Feature	Description
AP Configuration Workflow Enhancements	You can configure an AP even if it is not assigned to any site. You can configure the following AP parameters: • AP height • LED brightness level You can configure the following radio parameters: • CleanAir or spectrum intelligence settings • Antenna settings
Generate Compliance Audit Report	You can get a consolidated compliance report that shows compliance status of devices on your network.
Create Port Group	You can group device ports based on an attribute or rule.
Troubleshoot Unmonitored Devices	Using the MRE workflow, you can troubleshoot unmonitored devices or the devices that do not show Assurance data.
Troubleshoot Wireless Client Issues	Using the MRE workflow, you can troubleshoot wireless client issues.
Custom Policy Tags	You can configure policy tags for Cisco Catalyst 9800 Series Wireless Controllers using the advanced settings while creating network profiles for wireless.
AP Zones	You can add AP zones to a network profile for wireless. You can use AP zones to associate different SSIDs and RF profiles for a set of APs on the same site.

New and Changed Features in Cisco DNA Assurance

Table 2: New and Changed Features for Cisco DNA Assurance, Release 2.3.3

Feature	Description
Cisco AI Network Analytics: 6-GHz Radios Support	Cisco AI Network Analytics supports 6-GHz radio frequency for the following functionality: • Network Heatmaps • AP Performance Advisories • Trend Deviations (Insights) • AP RF Statistics • AP Spectrum Analysis
New AP Radio Down Issue	A new Radio Down issue is added to the Access Point issues. The issue is triggered when a radio goes down. Supported radio frequencies are 2 GHz, 5 GHz, and 6 GHz.
AP Mesh: Information Added to **Device 360** Window	In the **Device 360** window, you can view mesh AP information in the Mesh tab.

Feature	Description
New AP Radio Traffic Utilization Chart	In the **AP 360** window, under **Detail Information** in the **RF** tab, you can view a new chart called **Traffic Utilization**. This chart includes receive (Rx) and transmit (Tx) traffic utilization information. In addition, Rx and Tx traffic utilization information has been added to the **Channel Utilization** chart.
Additional AP Radio Channel Utilization Metrics Added to the **AP Radio Comparison View**	In the **Device 360** window, you can compare AP radios by the following additional KPIs: • Traffic Utilization • Tx Traffic Utilization • Rx Traffic Utilization
Path Trace Enhancements	Path trace results include the average processing delay of ACLs, tunneling, and queues, and the reason for a packet drop decision.
Cisco SD-Access: Transits and Peer Networks	You can monitor the health of the Transits and Peer Networks in the SD-Access Health dashboard.
Cisco AI Network Analytics: Roaming KPIs in Network Heatmaps	The **Network Heatmaps** window supports the following roaming KPIs: • **Successful inbound roaming events** • **Successful outbound roaming events** • **Total inbound roaming events**
Cisco AI Network Analytics: Peer Comparison KPIs	The **Peer Comparison** window supports the following KPIs: • **Onboarding Error Source**: Compares Onboarding Error Source in your network to your peers • **Roaming Error Source**: Compares Roaming Error Source in your network to your peers
Intel Analytics Support	In the **Client 360** window, under **Detail Information**, the **Intel Connectivity Analytics** tab is newly added. This tab is only available for devices supported by Intel wireless adapters.
Client Dashboard Enhancements	In the Assurance **Client** dashboard, the **Client Devices** dashlet includes **Tracked Client**, which allows you to track clients and notify them when they are detected in the network.
Cisco SD-Access: LISP and Pub/Sub Session	SD-Access Health supports **LISP** and **Pub/Sub** session monitoring in the fabric sites. These KPIs are part of Fabric Site, SD-Access Transit, Transit Control Plane, and Device health calculations.

New and Changed Features in Cisco DNA Automation

Feature	Description
Configure System Settings	In this release, Cisco DNA Center supports the following enhancements in the **System Configuration**: • The **Proxy Config** and **Proxy Certificate** are combined under the **Proxy** window. • In the **Proxy** window, you can configure the proxy configuration in the **Outgoing Proxy** tab. • In the **Proxy** window, you can configure the proxy certificate in the **Incoming Proxy** tab. Cisco DNA Center also allows you to retain or delete the licensed smart account users and their associated historical data.
Certificate Signing Request (CSR) Enhancement	You can do the following in the **Certificate Signing** window: • Copy the CSR properties in plain text. • Copy Base64 and paste to MS CA. • Download Base64.
Manage Licenses	You can view the historical trends for all purchased and consumed license consumptions in CSSM on a daily, weekly, and monthly basis. CSSM stores the historical information up to one year.
Support for Dual-Band (XOR) Radio Parameters	You can configure dual-band (XOR) radio parameters on the following APs from Cisco DNA Center: • Cisco Aironet 2800 Series Access Points • Cisco Aironet 3800 Series Access Points • Cisco Aironet 4800 Series Access Points • Cisco Catalyst 9100 Access Points
Support for 300 APs per FlexConnect Site Tag	You can create and provision 300 APs per FlexConnect site tag on the Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches release 17.8 or later.
Support for Cisco OEAP Configuration on Existing Infrastructure	You can configure Cisco Office Extend Access Point (OEAP) settings along with AP authorization lists on the existing infrastructure.
Learning of Mesh Configurations from Cisco Wireless Controller with Pre-existing Infrastructure	Using the **Learn Device Configuration** workflow, you can learn mesh configurations from Cisco Wireless Controllers with pre-existing infrastructure and map them back to the Cisco DNA Center wireless design.
Configure AAA VLAN Name Override for FlexConnect Deployments on Cisco AireOS Controller	For the AAA VLAN override settings, you can configure VLAN ID and VLAN name mapping for a specific FlexConnect profile on the **Design** > **Network Settings** > **Wireless** window.

Feature	Description
Learning of AAA VLAN Override from Cisco AireOS Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller with Pre-existing Infrastructure	Using the **Learn Device Configuration** workflow, you can learn about VLAN configurations from Cisco AireOS Wireless Controllers and Cisco Catalyst 9800 Series Wireless Controllers with pre-existing infrastructure.
Support for 6-GHz Radio Parameters on APs	Using the **Configure Access Points** workflow, you can configure 6-GHz radio parameters on APs.

New and Changed Features in Cisco Software-Defined Access

Table 3: New and Changed Software Features in Cisco Software-Defined Access

Feature	Description
Border Node Preference Option in Fabric Site	Cisco DNA Center now provides you with an option to select a border node for your network traffic. If you have more than one border node in your fabric site, you can set a priority value of each border node. Traffic is routed through the border node that has the highest priority. Priority values range from 1– 9 (1 is the highest priority and 9 is the lowest). By default (if you do not set the priority value), the border node is assigned a priority value of 10. If you do not set border node priority value, traffic is load balanced across the border nodes. The priority value set for a border node is applicable to all the virtual networks that are handed off from that border node. Border priority is supported for both unicast and multicast traffic. If an SD-Access Transit interconnects the fabric sites, an external border node with the highest priority is chosen to send traffic to external networks. Border node priority is supported on both LISP/BGP-based and LISP Pub/Sub-based fabric sites.
Create a Layer 2 Virtual Network	You can now create a Layer 2 virtual network without associating a Layer 3 virtual network. Traffic within the same VLAN is handled by the Layer 2 virtual network. Cisco DNA Center GUI provides an option to hand off only a Layer 2 virtual network. This release of Cisco DNA Center supports the creation of Layer 2 virtual network only in an SD-Access wired deployment.

Feature	Description
TCP MSS Adjustment	To help transmit the endpoints data over lower MTU limits, Cisco SD-Access Automation configures the Transmission Control Protocol (TCP) Maximum Segment Size (MSS) to 1250. All the overlay IP interfaces, including the edge nodes, Layer 3 border nodes, and Layer 2 border nodes, are configured with a TCP adjust MSS value of 1250. This is supported for TCP over IPv4 and IPv6. **Note** This feature is not supported on the Cisco Nexus 7700 Switch operating in Fabric. If you have to upgrade to this release from an earlier Cisco DNA Center release, a migration banner provides you the option to enable the automation of wired TCP adjust MSS settings.
Advertise LAN Automation Summary Route to BGP	In this release of Cisco DNA Center, if you choose to, LAN Automation advertises the summary route for the IP pool into BGP on the primary and peer devices. A new entry in the **LAN Automation Status** > **Summary** window of the Cisco DNA Center GUI displays whether the route advertisement is enabled.
View REP Ring Status	The Cisco DNA Center GUI now has a "View" option to check the status of a REP ring. This option displays the status of the devices in the REP ring and also warns if it detects a segment failure. For information on how to check the REP ring status, see "View REP Ring Status" in the Cisco DNA Center User Guide.
Cisco Industrial Ethernet (IE) Switches with Cisco DNA Essentials License Configured as Extended Node	Cisco Catalyst IE3200, IE3300, IE3400, IE3400H, and IE9300 series switches, and the IE4000, IE4010, and IE5000 series switches, with Cisco DNA Essentials license, are onboarded as SD-Access extended node. When you connect any of these factory-default switches with Cisco DNA Essentials license to an edge node, SD-Access automation configures the switch as an extended node. If you upgrade the license level of the switch to Cisco DNA Advantage, the Cisco DNA Center GUI gives you an option to convert the switch to a policy extended node. See “Upgrade an Extended Node to Policy Extended Node” in the Cisco DNA Center User Guide. Consider the following license combinations on the IE devices: • A device with Network Essentials and a Cisco DNA Essentials license is configured as an extended node. • An IE3400, IE3400H, and IE9300 device with Network Advantage and a Cisco DNA Advantage license is configured as a policy extended node. • A device with Network Advantage and a Cisco DNA Essentials license is configured as an extended node.

Feature	Description
Cisco Catalyst 9000 Series Switches with Cisco DNA Essentials License Configured as an Extended Node	Cisco DNA Center can now onboard a Cisco Catalyst 9000 Series switch with a Cisco DNA Essentials license as an SD-Access Extended Node. A factory-default Cisco Catalyst 9200, 9200CX, 9200L, 9300, 9300L, 9400, 9500, and 9500H series switch that operates Cisco IOS XE 17.8.1 (or later releases) with a Cisco DNA Essentials license is configured as an Extended Node if it is connected to a fabric edge node. If you upgrade the license level to Cisco DNA Advantage, the Cisco DNA Center GUI gives you an option to configure the device as a Policy Extended Node. See “Upgrade an Extended Node to Policy Extended Node” in the Cisco DNA Center User Guide. Consider the following license combinations on the Cisco Catalyst 9000 series devices: • A device with Network Essentials and a Cisco DNA Essentials license is configured as an extended node. • A device with Network Advantage and a Cisco DNA Advantage license is configured as a policy extended node. • A device with Network Advantage and a Cisco DNA Essentials license is configured as an extended node.
Overlapping IP Pools Across Virtual Networks	Cisco DNA Center allows you to choose overlapping IP pools across virtual networks for a fabric site. **Note** Cisco DNA Center doesn't support overlapping IP pools for different sites.
Cisco SD-Access User Interface Enhancements	• The **Create Fabric Site** workflow has been enhanced to include options to configure Wired Endpoint Data Collection and authentication template settings. • The options in the **Port Assignment** tab for a fabric site have been enhanced. • The options to choose an authentication template for a fabric site are now available in the **Authentication Template** tab. • The **Create Port Channel** workflow has been enhanced. • The options to configure the anycast gateway settings are now available in the **Anycast Gateway** tab. • The **Create Layer 2 Virtual Network** and **Create Layer 3 Virtual Networks** have been enhanced.
Cisco SD-Access and Cisco ACI Integration	In this release, Cisco DNA Center adds support for integration of Cisco SD-Access and Cisco ACI. This integration securely connects the campus network with the data center network to provide end-to-end visibility and policy integration. This integration is under limited availability. For more information, see Cisco SD-Access and Cisco ACI Integration.

Feature	Description
Cisco SD-Access and ITSM Integration	In this release, Cisco DNA Center enables you to control and manage the operations of Cisco SD-Access application through ITSM (ServiceNow). Cisco SD-Access and ITSM integration primarily monitors and manages the role assignment for a device in a fabric, thus ensuring that a wrong device is not added to or removed from the fabric. The following Cisco SD-Access workflows are managed through ServiceNow: • Addition of a new device to a fabric site • Deletion of a device from a fabric site To configure Cisco SD-Access integration with ITSM, see the Cisco DNA Center ITSM Integration Guide, Release 2.3.3.
SD-Access-as-code	This release introduces APIs that help in developing customized workflows for fabric operations. Such workflows reduce the overall time to create, change and delete fabric sites and deliver consistent outcomes for each fabric configuration step. SD-Access-as-code enhances the fabric operations, including the essential Day-0 and Day-N tasks in creating a fabric site and enabling multicast within a site.

Table 4: New Hardware Features in Cisco Software-Defined Access

Device Role	Product Family	Part Number	Description
Edge Node Extended Node Policy Extended Node	Cisco Catalyst Industrial Ethernet 9300 Rugged Series switches (IE9300)	IE-9310-26S2C IE-9320-26S2C	You can provision an IE9300 device as an edge node. When configured as an edge node, IE9300 can scale up to 32 virtual networks. You can configure an IE9300 device as an extended node or a policy extended node by connecting it to an edge node. When connected to an edge node, an IE9300 device is assigned a role based on its license level. If the device is at the Cisco DNA Essentials license level, it is onboarded as an extended node. If the device is at the Cisco DNA Advantage license level, it is onboarded as a policy extended node.
Extended Node	Cisco Catalyst Industrial Ethernet 3200 Rugged Series switches (IE3200)	IE-3200-8T2S-E IE-3200-8P2S-E	IE3200 is onboarded as an extended node when it is in factory-default state and connected to an edge node.
Edge Node Extended Node Policy Extended Node Supplicant-Based Extended Node	Cisco Catalyst 9200 Series switches	9200CX-8P-2X2G	You can provision the Cisco Catalyst 9200 Series switch as an edge node. It is onboarded as an extended node when it is in factory-default state and connected to an edge node.

Device Role	Product Family	Part Number	Description
Border Node Control Plane Node Edge Node Supplicant-Based Extended Node	Cisco Catalyst 9300 Series switches	C9300LM-48UX-4Y C9300LM-48U-4Y C9300LM-48T-4Y C9300LM-24U-4Y	You can provision the Cisco Catalyst 9300 Series switch as a border node, control plane node, and edge node. It is onboarded as an extended node when it is in factory-default state and connected to an edge node.

New and Changed Features in Interactive Help

Table 5: New and Changed Features in Interactive Help, Release 2.3.3

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

Deprecated Features

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

Cisco DNA Center Compatibility Matrix

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

Cisco SD-Access Compatibility Matrix

For information about Cisco SD-Access hardware and software support for Cisco DNA Center, see the *Cisco Software-Defined Access Compatibility Matrix*. This information is helpful for deploying Cisco SD-Access.

Compatible Browsers

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

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

We recommend that the client systems you use to log in to Cisco DNA Center be equipped with 64-bit operating systems and browsers.

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

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) for appliance model DN1-HW-APL
- Cisco IMC Version 4.1(1h) for appliance model DN2-HW-APL
- Cisco IMC Version 4.1(1h) for appliance model DN2-HW-APL-L
- Cisco IMC Version 4.1(1h) for appliance model DN2-HW-APL-XL

Cisco DNA Center Scale

For Cisco DNA Center scale numbers, see the *Cisco DNA Center Data Sheet*.

IP Address and FQDN Firewall Requirements

To determine the IP addresses and fully qualified domain names (FQDNs) that must be made accessible to Cisco DNA Center through any 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 data collection, contact your Cisco account representative and the Cisco TAC.

Supported Hardware Appliances

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

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

Installing Cisco DNA Center

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

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

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

Cisco DNA Center Platform Support

For information about the Cisco DNA Center platform, including information about new features, installation, upgrade, and open and resolved bugs, see the *Cisco DNA Center Platform Release Notes*.

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.

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

Plug and Play Considerations

Plug and Play Support

General Feature Support

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

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

Secure Unique Device Identifier Support

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

- Cisco routers:
  - Cisco Catalyst IR 1800 Series with software release Cisco IOS XE 17.5.1 and later
  - Cisco ISR 1100 Series with software release Cisco IOS XE 16.6.2
  - Cisco ISR 4000 Series with software release Cisco IOS XE 3.16.1 or later, except for the ISR 4221, which requires release Cisco IOS XE 16.4.1 or later
  - Cisco ASR 1000 Series (except for the ASR 1002-x) with software release Cisco IOS XE 16.6.1
- Cisco switches:
  - Cisco Catalyst 3850 Series with software release Cisco IOS XE 3.6.3E or Cisco IOS XE 16.1.2E or later
  - Cisco Catalyst 3650 Series and 4500 Series with Supervisor 7-E/8-E, with software release 3.6.3E, Cisco IOS XE 3.7.3E, or Cisco IOS XE 16.1.2E or later
  - Cisco Catalyst 4500 Series with Supervisor 8L-E with software release Cisco IOS XE 3.8.1E or later
  - Cisco Catalyst 4500 Series with Supervisor 9-E with software release Cisco IOS XE 3.10.0E or later
  - Cisco Catalyst 9300 Series with software release Cisco IOS XE 16.6.1 or later
  - Cisco Catalyst 9400 Series with software release Cisco IOS XE 16.6.1 or later
  - Cisco Catalyst 9500 Series with software release Cisco IOS XE 16.6.1 or later
  - Cisco Catalyst IE3300 Series with software release Cisco IOS XE 16.10.1e or later
  - Cisco Catalyst IE3400 Series with software release Cisco IOS XE 16.11.1a or later

- NFVIS platforms:
  - Cisco ENCS 5400 Series with software release 3.7.1 or later
  - Cisco ENCS 5104 with software release 3.7.1 or later

Note Devices that support SUDI have two serial numbers: the chassis serial number and the SUDI serial number (called the License SN on the device label). You must enter the SUDI serial number in the **Serial Number** field when adding a device that uses SUDI authentication. The following device models have a SUDI serial number that is different from the chassis serial number:

- Cisco routers: Cisco ISR 43xx, Cisco ISR 44xx, Cisco ASR1001-X/HX, and Cisco ASR1002-HX
- Cisco switches: Cisco Catalyst 4500 Series with Supervisor 8-E/8L-E/9-E, and Catalyst 9400 Series

Management Interface VRF Support

Plug and Play operates over the device management interface on the following platforms:

- Cisco routers:
  - Cisco ASR 1000 Series with software release Cisco IOS XE 16.3.2 or later
  - Cisco ISR 4000 Series with software release Cisco IOS XE 16.3.2 or later
- Cisco switches:
  - Cisco Catalyst 3650 Series and 3850 Series with software release Cisco IOS XE 16.6.1 or later
  - Cisco Catalyst 9300 Series with software release Cisco IOS XE 16.6.1 or later
  - Cisco Catalyst 9400 Series with software release Cisco IOS XE 16.6.1 or later
  - Cisco Catalyst 9500 Series with software release Cisco IOS XE 16.6.1 or later

4G Interface Support

Plug and Play operates over a 4G network interface module on the following Cisco routers:

- Cisco 1100 Series ISR with software release Cisco IOS XE 16.6.2 or later
- Cisco Catalyst IR 1800 Series

Configure Server Identity

To ensure successful Cisco DNA Center discovery by Cisco devices, the server SSL certificate offered by Cisco DNA Center during the SSL handshake must contain an appropriate Subject Alternate Name (SAN) value so that the Cisco Plug and Play IOS Agent can verify the server identity. This may require the administrator to upload a new server SSL certificate, which has the appropriate SAN values, to Cisco DNA Center. You can generate 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, in case discovery methods vary. For example, you can include both the Cisco DNA Center FQDN and IP address (or NAT IP address) in the SAN field. If you do include both, set the FQDN as the first SAN value followed by the IP address.

If the SAN field in the Cisco DNA Center certificate does not contain the appropriate value, the device cannot successfully complete the Plug and Play process.

Note The Cisco Plug and Play IOS Agent checks only the certificate SAN field for the server identity. It does not check the common name (CN) field.

Bugs

Open Bugs

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

Bug Identifier	Headline
CSCvz83872	For wireless endpoints connected as guest hosts via bridged VM, guest host IPs are not updated and guest hosts don't show as two separate endpoints with IP addresses.
CSCwa00990	For Wide Area Bonjour, restoring a NIC-bonded cluster link in three-node HA sometimes causes Service Discovery Gateway (SDG) agents to remain in inactive status. In an operational three-node cluster running the Cisco Wide Area Bonjour application, when the cluster becomes operational with only two nodes after a node is lost from the cluster or a previously lost third node becomes operational due to manual administrative actions or network malfunction, the following issue may be seen sometimes for the Wide Area Bonjour service: The status of some SDG agents in the **Monitor** > **SDG Agent** window may remain inactive, even if they were active before the incident. This issue is also reflected in Wide Area Bonjour SDG dashlet, where the state of the affected SDG agents is **Reachable**, but **Down**. Wide Area Bonjour shows the status of the services learned from these affected SDG agents as **inactive** and doesn't process queries from these SDG agents. Running the **show mdns controller summary** command on any affected SDG agent switch shows the connection state as negotiating (although a ping to the controller IP from the interface is successful). This issue doesn’t affect the operation of any other service on Cisco DNA Center.
CSCwa19612	In the Web UI, there is no option to enable FIPS.
CSCwa36712	For extended nodes, a resync after reload returns a NETCONF connection failure error.
CSCwb19961	AP zone configuration and custom policy tag configuration on the APs are lost when AI-enhanced RRM is enabled on buildings from Cisco DNA Center. APs get configured with the Cisco DNA Center auto-generated policy tags.
CSCwb36994	Unable to delete any pool from an anchored virtual network that was created on an earlier release and then upgraded to Cisco DNA Center 2.2.3.4.
CSCwb54150	When you choose **System** > **Settings** > **System Certificates** > **Replace Certificates** > **Generate New CSR**, the following error message might appear, and the Common Name and SAN IP/DNS fields don't automatically populate in the CSR form: `Unable to populate FQDN related fields.`

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

Bug Identifier	Headline
CSCwb64910	L2VN border config removes cts enforcements for other VLANs. The above condition is triggered when a user has existing gateways present in fabric and adds one of the below: • L2VN (L2 only without IP pool but associated to a L3VN (affected device: EdgeNode) • New flow L2vn without L3VN (affected device: EdgeNode) • L2 handoff on border (affected device: BorderNode on which L2 handoff is performed)

Resolved Bugs

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

Bug Identifier	Headline
CSCvx52786	Cisco DNA Center may not display an IP address pool or subnet when a user tries to create a segment, citing the errors, "NCIP10071: pool name can contain only alphanumeric characters, underscores and hyphens," and "NCIP10288: There was a failure in the ipam-service."
CSCvz14636	When Cisco DNA Center attempts to configure Application Visibility and Control (AVC) to an eight-member stack of Catalyst 9k switches, the process may fail, citing the error, "NBAR Error: Can not enable Protocol-discovery - platform interface limit reached. AVC needs to restrict pushing NBAR configuration to only access switch port.
CSCvz65062	Cisco DNA Center Inventory reports an internal error for Cisco Catalyst 9300 switches.
CSCvz70561	While adding additional edge switches to an existing fabric, Cisco DNA Center may alter the AAA configuration of an existing Cisco Wireless Controller from TACACS to RADIUS.
CSCvz87778	LAN Automation fails with "Error while reserving link subnet:... " when there are 31+ dummy pools.
CSCvz98644	All wireless controllers are implicitly configured when IP pools are assigned or removed from fabric WLANs on the Host Onboarding window.
CSCvz98664	Adding and removing a fabric edge provisions wireless controllers randomly with different configurations.
CSCvz99700	Unable to delete a segment from host onboarding.
CSCwa01888	IP pools are not displayed in the host onboarding under a virtual network.
CSCwa10370	Cisco ISE node PSN if added as AAA server in Cisco DNA Center cannot be removed even if no WLAN is using the node as AAA.
CSCwa14705	Inconsistent results are shown for the site health API.
CSCwa16652	Manually generated reports in Cisco DNA Center results in blank pages.
CSCwa18877	Cisco DNA Center: Ekahau File import fails with the API error, "The specified group ID is null or empty."
CSCwa21212	Unable to start LAN automation due to "NCND00050: An internal error occurred while processing the request".

Bug Identifier	Headline
CSCwa21575	Supplicant-based extended node fails to onboard via Plug and Play when using the Cisco DNA Center-based onboarding flow. This behavior is seen when referencing the default ACL == AEN_MAB_ACL for use during onboarding.
CSCwa21979	Device Discovery task gets stuck in RUNNING for a long time, clogging up the inventory service, which in turn disrupts loading of global credentials.
CSCwa23879	When configuring integration of Cisco ISE with Cisco DNA Center, RADIUS is enabled by default, and the pxGrid connection to Cisco ISE is enabled. TACACS+ is not enabled by default. If you choose to enable TACACS+ and to also disable RADIUS, you must manually disable the pxGrid connection. Otherwise, the Cisco DNA Center System 360 windows shows the pxGrid state as Unavailable.
CSCwa26591	Supplicant-based extended nodes toggle between inbuilt templates, resulting in error disabled.
CSCwa29973	CTS credentials of the device are not in sync with the Cisco ISE NAD entry.
CSCwa37388	Assurance Dashboard: Rogue on Wire reports with rogue clients with broadcast addresses (all F's) should be ignored while calculating rogue on wire.
CSCwa41677	AP provisioning fails when AAA VLANs are defined and AP reprovisioning is attempted.
CSCwa43532	User intent validation failure when provisioning wireless controller.
CSCwa44338	Cisco DNA Center 2.2.2.8 displays 10+ Gbs interfaces with an interface speed of Catalyst Devices as 4,294,967,295. The interfaces on the device themselves display the correct speed. This is due to a limitation with the SNMP OID being used. Cisco DNA Center is using the ifSpeed OID (1.3.6.1.2.1.2.2.1.5). This OID has a limitation: If the bandwidth of the interface is greater than the maximum value reportable by this object, this object should report its maximum value (4,294,967,295) and ifHighSpeed must be used to report the interface's speed.
CSCwa45898	NAC is not enabled via advanced SSID Model config when pushing to two Cisco Wireless Controllers at the same time.
CSCwa46093	Cisco DNA Center may fail to create a trust-point when the system certificate contains ".local" or ".com.corp" in the common name.
CSCwa51827	LISP key banner push fails for wireless devices in Cisco DNA Center 2.2.2.x.
CSCwa52917	A null pointer exception occurs while you try to access Show Task from the Image Repository window.
CSCwa68838	The spf-service-manager-service does not start after an upgrade to Cisco DNA Center 2.1.2.7.
CSCwa73823	Assurance Client Health window does not load when Client Data Rate dashlets are deleted.
CSCwa77904	Cisco DNA Center provisioning fails with "NCSP10246 Internal error while attempting to transform".
CSCwa87716	Template content only returns a specific value instead of the entire content.
CSCwa88686	Download of latest KGV files fails due to a certificate change on tools.cisco.com.
CSCwa90595	A Cisco Wireless Controller provisioning failure occurs due to an invalid $apMac configuration element.

Bug Identifier	Headline
CSCwb06814	System Health displays stale pxGrid information after updating the FQDN information.
CSCwb08617	Wireless controller provisioning failed with error "NCSP10250: Error During persistence (modify) of CFS & SerializedSnapshot (name: x.x.x type: DeviceInfo qualifier: null)".
CSCwb15711	Fabric edge provisioning fails if you use a single-digit VLAN ID with sgt during pool addition in a virtual network.
CSCwb15727	During an attempt to activate the Cisco DNA Center Disaster Recovery system after registration, the DR activation workflow never completes. On the Main cluster, the "Configure active" flow completes properly, and the Main site moves to a "Waiting Standby Configuration" state. But on the "Configure standby" flow, the Configure replication step doesn't complete, leaving the Recovery site in the "Configuring Standby" state indefinitely.

Limitations and Restrictions

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 UI 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.

Cloud Connectivity via SSL Intercept Limitation

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

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

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

Backup and Restore Limitations

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

- After performing a restore operation, update your integration of Cisco ISE with Cisco DNA Center. After a restore operation, Cisco ISE and Cisco DNA Center might not be in sync. To update your Cisco ISE integration with Cisco DNA Center, choose **System Settings** > **Settings** > **Authentication and Policy Servers**. Choose **Edit** for the server. Enter your Cisco ISE password to update.
- After performing a restore operation, the configuration of devices in the network might not be in sync with the restored database. In such a scenario, you should manually revert the CLI commands that are pushed for authentication, authorization, and accounting (AAA) and configuration on the network devices. Refer to the individual network device documentation for information about the CLI commands to enter.
- Reenter the device credentials in the restored database. If you updated the site-level credentials before the database restore, and the backup that is being restored does not have the credential change information, all the devices go to partial collection after the restore. You must then manually update the device credentials on the devices for synchronization with Cisco DNA Center, or perform a rediscovery of those devices to learn the device credentials.
- Perform AAA provisioning only after adjusting network device differential changes to the restored database. Otherwise, device lockouts might occur.
- You can back up and restore Automation data only or both Automation and Assurance data. But you cannot use the GUI or the CLI to back up or restore only Assurance data.

Cisco ISE Integration Limitations

- ECDSA keys are not supported as either SSH keys for Cisco ISE SSH access or in certificates in Cisco DNA Center and Cisco ISE.
- Full certificate chains must be uploaded to Cisco DNA Center while replacing an existing certificate. If a Cisco DNA Center certificate is issued by a subCA of a rootCA, the certificate chain uploaded to Cisco DNA Center while replacing the Cisco DNA Center certificate must contain all three certificates.
- Self-signed certificates applied on Cisco DNA Center must have the Basic Constraints extension with cA:TRUE (RFC5280 section-4.2.19).
- The IP address or FQDN of both Cisco ISE and Cisco DNA Center must be present in either the **Subject Name** field or the **Subject Alt Name** field of the corresponding certificates.
- If a certificate is replaced or renewed in either Cisco ISE or Cisco DNA Center, trust must be re-established.
- The Cisco DNA Center and Cisco ISE IP or FQDN must be present in the proxy exceptions list if there is a web proxy between Cisco DNA Center and Cisco ISE.
- Cisco DNA Center and Cisco ISE nodes cannot be behind a NAT device.
- Cisco DNA Center and Cisco ISE cannot integrate if the ISE Admin and ISE pxGrid certificates are issued by different enterprise certificate authorities.

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

License Limitations

- The Cisco DNA Center License Manager supports Smart Licensing only for wireless controller models that run Cisco IOS XE. License Manager does not support Smart License registration of the Cisco 5500 Series AireOS Wireless Controller when the connection mode is smart-proxy.
- 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

Device Onboarding Limitations

For IE-3200-8P2S-E/A, IE-3200-8T2S-E/A, IE-3300-8P2S-E/A, and IE-3300-8T2S-E/A devices that operate 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.

Fabric Limitations

- IP address pools that are reserved at the area level are shown as inherited at the building level on the **Design** > **Network Settings** > **IP Address Pools** window; however, these IP address pools are not listed on the **Host Onboarding** window if the fabric site is defined at the building level. If the fabric site is defined at the building level, you must reserve the IP address pools at the building level. If the fabric site is defined at the area level, you must reserve the IP address pools at the area level.

  To work around this issue, release and reserve the IP address pool at the same level (area or building) as the fabric site, or reconfigure the fabric site at the same level as the reserved IP address pool.
- Cisco DNA Center does not support multicast across multiple fabric sites that are connected by an SD-Access transit network.

Existing Feature-Related Limitations

- Cisco DNA Center cannot learn device credentials.
- You must enter the preshared key (PSK) or shared secret for the AAA server as a part of the import flow.
- Cisco DNA Center does not learn the details about DNS, WebAuth redirect URL, and syslog.
- Cisco DNA Center can learn the device configuration only one time per controller.
- Cisco DNA Center can learn only one wireless controller at a time.
- For site profile creation, only the AP groups with AP and SSID entries are considered.
- Automatic site assignment is not possible.
- SSIDs with an unsupported security type and radio policy are discarded.

- For authentication and accounting servers, if the RADIUS server is present in the device, it is given first preference. If the RADIUS server is not present, the TACACS server is considered for design.
- The Cisco ISE server (AAA) configuration is not learned through existing device provisioning.
- The authentication and accounting servers must have the same IP addresses for them to be learned through existing device provisioning.
- When an SSID is associated with different interfaces in different AP groups, during provisioning, the newly created AP group with the SSID is associated with the same interface.
- A wireless conflict is based only on the SSID name and does not consider other attributes.

Wireless 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, `Policy Deployment failed` is displayed.

AP Limitations

- AP as a sensor is not supported in this release of Cisco DNA Center.
- Configuring APs in FlexConnect mode before provisioning the locally switched WLANs bypasses the AP provisioning error. Otherwise, the AP provisioning fails when the locally switched WLANs are provisioned on the wireless controller or APs through Cisco DNA Center.

  After the provisioning failure, the AP rejoins the wireless controller. You can reprovision the AP for a successful provisioning.
- Provisioning of 100 APs takes longer in this release as compared to 3 minutes in earlier releases. The amount of time varies depending on the "wr mem" time of the Cisco Catalyst 9800 Series Controller, which includes Cisco Catalyst 9800-40 Wireless Controller, Cisco Catalyst 9800-80 Wireless Controller, and Cisco Catalyst 9800-CL Cloud Wireless Controller devices.

Inter-Release Controller Mobility (IRCM) Limitation

The interface or VLAN configuration is not differentiated between foreign and anchor controllers. The VLAN or interface that is provided in Cisco DNA Center is configured on both foreign and anchor controllers.

IP Device Tracking on Trunk Port Limitation

Rogue-on-wire detection is impacted; Cisco DNA Center does not show all clients connected to a switch via an access point in bridge mode. The trunk port is used to exchange all VLAN information. When you enable IP device tracking on the trunk port, clients connected on the neighbor switch are also shown. Cisco DNA Center does not collect client data if the connected interface is a trunk port and the neighbor is a switch. As a best practice, disable the IP device tracking on the trunk port. The rogue on wire is not detected if the IP device tracking is enabled on the trunk port. See Disabling IP Device Tracking for more information.

IP Address Manager Limitations

- You might see the following error when editing an existing IPAM integration or when adding a new IPAM manager.

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

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

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

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

  To correct this error for a self-signed certificate:

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

     ```
     openssl s_client -showcerts -connect Infoblox-FQDN:443
     ```

     ```
     openssl s_client -showcerts -connect Bluecat-FQDN:443
     ```

  2. From the output, use the content from ---BEGIN CERTIFICATE--- to ---END CERTIFICATE--- to create a new .pem file.
  3. Go to **System** > **Settings** > **Trust & Privacy** > **Trustpool**, click **Import**, and upload the certificate (.pem file).
  4. Go to **System** > **Settings** > **External Services** > **IP Address Manager** and configure the external IPAM server. (If the IPAM server is already configured, skip this step.)

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

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

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

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

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

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

  To correct this, log in to the external IPAM server (such as BlueCat). Confirm that the parent pool CIDR exists in the external IPAM server, and remove all the child pools that are configured under that parent pool. Then, return to the Cisco DNA Center GUI and reconfigure the IPAM server under **System** > **Settings** > **External Services** > **IP Address Manager**.

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

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

```
OU=Engineering,
O=Infoblox, L=Sunnyvale, ST=California, C=US) |
```

To correct this, log in to the external IPAM server (such as Infoblox) and regenerate your external IPAM certificate with the common name (CN) value as the valid hostname or IP address. In the preceding example, the CN value is www.infoblox.com, which is not the valid hostname or IP address of the external IPAM.

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

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

Encryption Limitation with SNMPv3

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

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

IPv6 Limitations

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

- Access Control Application, Group-Based Policy Analytics, 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.

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 times out.

- Data aggregation occurs at hourly offsets from UTC in Cisco Group-Based Policy Analytics. However, some time zones are at a 30 or 45 minute offset from UTC. If the Cisco DNA Center server is located in a time zone with a 30 minute or 45 minute offset from UTC and the client is located in a time zone with an hourly offset from UTC, or vice versa, the time ranges for data aggregation in Cisco Group-Based Policy Analytics are incorrect for the client.

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

Application Telemetry Limitation

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

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

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

The following syntax is invalid:

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

Get Assistance from the Cisco TAC

Use this link to open a TAC case. Choose the following when opening a TAC case:

- **Technology**: Cisco DNA - Software-Defined Access
- **Subtechnology**: Cisco DNA Center Appliance (SD-Access)
- **Problem Code**: Install, uninstall, or upgrade

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.

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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

For This Type of Information...	See This Document...
Use of the Cisco DNA Assurance GUI.	Cisco DNA Assurance User Guide
Use of the Cisco DNA Center platform GUI and its applications.	Cisco DNA Center Platform User Guide
Cisco DNA Center platform release information, including new features, deployment, and bugs.	Cisco DNA Center Platform Release Notes
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 Management functionality as a dashboard within Cisco DNA Assurance in the Cisco DNA Center GUI.	Cisco DNA Center Rogue Management Application Quick Start Guide