Release Notes for Cisco DNA Center, Release 2.3.2.x

First Published: 2021-12-15

Last Modified: 2023-11-07

Release Notes for Cisco DNA Center, Release 2.3.2.x

Cisco DNA Center 2.3.2.x is a Commercial Availability release. Contact your Cisco sales representative to request this release.

This document describes the features, limitations, and bugs for Cisco DNA Center, Release 2.3.2.x.

For links to all of the guides in this release, see Cisco DNA Center 2.3.2 Documentation.

Change History

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

Table 1: Document Change History

Date	Change	Location
2023-11-07	Added a limitation about maintenance mode for APs	Limitations and Restrictions, on page 26
2023-02-17	Added a limitation about In-Service Software Upgrade (ISSU).	Limitations and Restrictions, on page 26
2022-05-25	Added the list of packages in Cisco DNA Center 2.3.2.3.	Package Versions in Cisco DNA Center, Release 2.3.2.x, on page 2
	Added the Resolved Bugs table for 2.3.2.3.	Resolved Bugs, on page 21
	Noted that Cisco DNA Center 2.3.2.3 contains fixes for the Spring4Shell vulnerability.	New and Changed Features in Cisco DNA Center, on page 4
	Added the open bugs CSCwa92273 and CSCwa00990.	Open Bugs, on page 20
	Added the new and changed Interactive Help information for 2.3.2.3.	New and Changed Features in Interactive Help, on page 14
	Added the new feature information for the Cisco Wide Area Bonjour application.	New and Changed Features in Cisco DNA Center, on page 4

Date	Change	Location
2022-01-20	Added the list of packages in Cisco DNA Center 2.3.2.1.	Package Versions in Cisco DNA Center, Release 2.3.2.x, on page 2
	Noted that Cisco DNA Center 2.3.2.1 contains fixes for the Apache Log4j vulnerability.	New and Changed Features in Cisco DNA Center, on page 4
2021-12-15	Initial release.	—

Upgrade to the Latest Cisco DNA Center Release

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

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

Package Versions in Cisco DNA Center, Release 2.3.2.x

The following table shows the updated packages and the versions in Cisco DNA Center, Release 2.3.2.x.

Package Name	Release 2.3.2.3	Release 2.3.2.1	Release 2.3.2.0
Release Build Version			
Release Version	2.3.2.3.72213	2.3.2.1-70507	2.3.2.0-70475
System Updates			
System	1.7.609	1.7.534	1.7.523
System Commons	2.1.461.62272	2.1.460.60859	2.1.460.60853
Package Updates			
Access Control Application	2.1.461.62272	2.1.460.60859	2.1.460.60853
AI Endpoint Analytics	1.6.615	1.6.557	1.6.540
AI Network Analytics	2.8.16.459	2.8.15.455	2.8.15.455
Application Hosting	1.8.1.2201310931	1.8.1.2112171046	1.8.0.2110260825
Application Policy	2.1.461.170220	2.1.460.117490	2.1.460.117441
Application Registry	2.1.461.170220	2.1.460.117490	2.1.460.117441
Application Visibility Service	2.1.461.170220	2.1.460.117490	2.1.460.117441
Assurance - Base	2.3.2.351	2.3.2.287	2.3.2.279
Assurance - Sensor	2.3.2.339	2.3.2.286	2.3.2.260

Package Name	Release 2.3.2.3	Release 2.3.2.1	Release 2.3.2.0
Automation - Base	2.1.461.62272	2.1.460.60859	2.1.460.60853
Automation - Intelligent Capture	2.1.461.62272	2.1.460.60859	2.1.460.60853
Automation - Sensor	2.1.461.62272	2.1.460.60859	2.1.460.60853
Cisco DNA Center Global Search	1.7.1.103	1.7.1.102	1.7.1.97
Cisco DNA Center Platform	1.7.1.132	1.7.1.107	1.7.1.106
Cisco DNA Center UI	1.7.0.1036	1.7.0.970	1.7.0.970
Cisco Identity Services Engine Bridge	2.1.461.394	2.1.460.380	2.1.460.380
Cisco Umbrella	2.1.461.592131	2.1.460.590229	2.1.460.590184
Cloud Connectivity - Contextual Content	1.3.1.441	1.3.1.441	1.3.1.441
Cloud Connectivity - Data Hub	1.7.13	1.6.0.380	1.6.0.380
Cloud Connectivity - Tethering	2.30.1.59	2.21.1.3	2.21.1.3
Cloud Device Provisioning Application	2.1.461.62272	2.1.460.60859	2.1.460.60853
Command Runner	2.1.461.62272	2.1.460.60859	2.1.460.60853
Device Onboarding	2.1.461.62272	2.1.460.60859	2.1.460.60853
Disaster Recovery	2.1.461.3620050	2.1.460.36097	2.1.460.36097
Group-Based Policy Analytics	2.3.2.41	2.3.2.40	2.3.2.39
Image Management	2.1.461.62272	2.1.460.60859	2.1.460.60853
Machine Reasoning	2.1.461.212131	2.1.460.210115	2.1.460.210110
NCP - Base	2.1.461.62272	2.1.460.60859	2.1.460.60853
NCP - Services	2.1.461.62272	2.1.460.60859	2.1.460.60853
Network Controller Platform	2.1.461.62272	2.1.460.60859	2.1.460.60853
Network Data Platform - Base Analytics	1.7.189	1.7.188	1.7.185
Network Data Platform - Core	1.7.287	1.7.286	1.7.282
Network Data Platform - Manager	1.7.144	1.7.144	1.7.141
Network Experience Platform - Core	2.1.461.62272	2.1.460.60859	2.1.460.60853
Path Trace	2.1.461.62272	2.1.460.60859	2.1.460.60853
RBAC Extensions	2.1.461.1902002	2.1.460.1900012	2.1.460.1900012
Rogue and aWIPS	2.4.0.34	2.4.0.33	2.4.0.33

Package Name	Release 2.3.2.3	Release 2.3.2.1	Release 2.3.2.0
SD-Access	2.1.461.62272	2.1.460.60859	2.1.460.60853
Stealthwatch Security Analytics	2.1.461.1093118	2.1.460.1092227	2.1.460.1092183
Support Services	2.1.461.880012	2.1.460.880040	2.1.460.880040
Wide Area Bonjour	2.4.461.75209	2.4.368.75006	2.4.364.75035

New and Changed Information

New and Changed Features in Cisco DNA Center

Important Updates in Cisco DNA Center 2.3.2.3

Feature	Description
Fixes for the Spring4Shell Vulnerability	In March 2022, VMware disclosed vulnerabilities in the Spring4Shell Spring Framework. Cisco is committed to transparency and we have published a security advisory to make sure our customers understand the issue and how to address it. Please refer to our advisory for the latest information: Cisco Security Advisory: Vulnerability in Spring Framework Affecting Cisco Products: March 2022 Cisco DNA Center 2.3.2.3 contains fixes for the Spring4Shell vulnerability. This effort is being tracked as CSCwb43650 for the Cisco DNA Center product and contains the following fix: • CVE-2022-22965: Spring Framework RCE via Data Binding on JDK 9+. To help assess, identify, and reduce exposure to vulnerabilities, consider running a trusted vulnerability scanner. For example: • Rapid7 remote check (vulnerability ID spring-cve-2022-22965-remote-http)
Support for Cisco Nexus 9000 Series Switches on the Cisco Wide Area Bonjour Application	Cisco DNA Service for Bonjour supports Cisco Nexus 9000 Series Switches as an SDG agent in multicast mode.

Important Updates in Cisco DNA Center 2.3.2.1

Feature	Description
Fixes for the Apache Log4j Vulnerability	In December 2021, the Apache Software Foundation disclosed vulnerabilities in the open-source Log4j logging library. At this time, almost all affected Cisco products have either been remediated or have a software update scheduled for release. Cisco is committed to transparency and we have published a security advisory to make sure our customers understand the issue and how to address it. Please refer to our advisory for the latest information: Cisco Security Advisory: Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021 Cisco DNA Center 2.3.2.1 contains fixes for the Apache Log4j vulnerability. This effort is being tracked as CSCwa47322 for the Cisco DNA Center product and contains the following fixes: • CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints. • CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack. To help assess, identify, and reduce exposure to vulnerabilities, consider running a trusted vulnerability scanner. For example: • https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance • https://github.com/cisagov/log4j-scanner • https://github.com/CERTCC/CVE-2021-44228_scanner

Table 2: New and Changed Features in Cisco DNA Center 2.3.2.0

Feature	Description
IP Access Control	You can control the access to Cisco DNA Center based on the IP address of the host or network. By default, all IP addresses can access Cisco DNA Center.
License Consumption Report Upload Support for Cisco AireOS Controllers	You can register Cisco DNA Center to a specific smart account and virtual account in Cisco SSM so that Cisco DNA Center uploads the license utilization details on behalf of Cisco AireOS Controllers to Cisco SSM. This feature addresses the limitation that Cisco AireOS Controllers do not recognize Cisco DNA Center licenses and Network licenses and therefore do not send license utilization details directly to Cisco SSM.
Device Certificate Lifecycle Management	You can view and manage the certificates that Cisco DNA Center issues for managed devices to authenticate and identify the devices.
Certificate Signing Request (CSR) Support for Cisco DNA Center	You can create your CSR, and then submit it to your provider to generate your certificate.

Feature	Description
Recognize Existing Licensing Configuration in Customer's Environment with Satellite Server	Cisco DNA Center discovers the registration state of devices after a connection mode change. You can reregister the devices with the updated SSM.
License Manager GUI Enhancements	The **License Manager** window has the following changes: • The **All Licenses** tab is split into two tabs, **Licenses** and **Devices**. • The **SLP Compliance** tab is changed to the **Sync Status** tab.
Create Custom Prompts	Cisco DNA Center lets you create custom prompts for the username and password. You can configure the devices in your network to use custom prompts and collect information about the devices.
Configure Device Configuration Backup Settings	Cisco DNA Center lets you configure your device configuration backup settings. You can choose the day and time and the total number of config drifts that can be saved per device.
Configure External Server for Archiving Device Configuration	Cisco DNA Center lets you configure an external SFTP server for archiving the running configuration of devices.
Label Configuration Drift	You can label the configuration drift of device. The labeled configuration drift is saved and can be used for future reference.
Support for Restricted Shell	For added security, Cisco DNA Center supports restricted shell. If your network uses any CLI-based scripts or troubleshooting commands, you have the option of disabling the restricted shell in the current Cisco DNA Center release. For more information, see "Disable Restricted Shell" in the *Cisco DNA Center 2.3.2 Administrator Guide*.
3D Wireless Maps Enhancements	Enhancements to 3D wireless maps include: • Search and locator capability. • Enhanced Drop a Pin functionality that includes highlighting active arrows for ease of selection and movement. • Measurements move to stay in your field of view when resizing or changing the map display. • Ability to display multiple floors and their APs and define whether to include the APs in the heat map computation.
Network Profiles for Assurance	You can configure issue settings in an Assurance network profile and apply the profile to a site or group of sites independently from the global issues settings. You can enable or disable an issue, and you can change its priority.
Install Hosted Application on Switches Workflow Enhancements	You can view the configuration template before deploying an application on switches.
Device Pack Support for Legacy Devices	You can display the device pack support for legacy devices. In the **Provision** > **Network Devices** > **Inventory** window, the **Support Type** for legacy devices is shown as **Limited**.

Feature	Description
Display Information About Your Inventory	You can display the following inventory details in the **Inventory** > **Provision** table: • **AP Ethernet Mac Address**: The Ethernet MAC address of an AP. • **AP CDP Neighbors**: Switch and port connected to an access point. This information is displayed even if the connected access switch is not managed by Cisco DNA Center.
View Flow Count Details and Policy Enforcement Statistics	You can view additional details about scalable groups: • You can view the number of flows detected for a particular service, port, and protocol combination for a selected time period. The **Flow Count** column in the **View Contract** window displays this information. You can click the flow count link to view the flow details for each endpoint. To launch the **View Contract** window, from the **Explore Scalable Groups** window, click **View Contract**. • You can view a time-series graph of permit and deny counts for any source and destination group pair. In the **Explore Scalable Groups** window, click the **View Policy Enforcement Stats** option. You can use the **All Packets** drop-down list to select only the permitted or dropped packets.
Schedule Maintenance for Devices	You can place devices into maintenance mode in Cisco DNA Center. If a device is in maintenance mode, Cisco DNA Center does not process any telemetry data associated with the device. By placing faulty devices into maintenance mode, you can avoid receiving unnecessary alerts from these devices.
Learn Device Configuration from Brownfield Devices (Beta Feature)	Cisco DNA Center can learn configurations from devices, such as Cisco Wireless Controllers, in an existing deployment and save the configurations at the global level.
Application Visibility	Cisco DNA Center support is extended for the following enhancements in **Application Visibility**: • Embedded Wireless Controller (EWC) switches can now also be used as a wireless controller in fabric mode. • Your device must be wireless enabled to enable CBAR in wireless mode. • EWC devices are enabled with CBAR in wireless mode. • For EWC devices with a border role, CBAR is enabled only in wireless mode. • EWC devices with the access switch role support wired and wireless mode. • CBAR enabled for flex and fabric SSID types on wireless controller is supported on OS version 17.7.1 or later. • Cisco Embedded Wireless Controller on Catalyst 9000 series switches are supported with **Fabric** modes. • When you enable CBAR for a device, the **Enable CBAR** slide-in pane lets you select the SSIDs types. Available SSID types are **Local**, **Flex**, and **Fabric**. • In the **CBAR Readiness Status** column, an info icon next to the **Ready** status shows the respective device is wireless enabled.

Feature	Description
Enable Application Telemetry for Wireless Controllers.	When you enable Application Telemetry for a new or existing device, you can select the SSID type. Available SSID types are **Local** and **Flex/Fabric**. You can also select **Guest SSID**.
System Analyzer Tool	Using the System Analyzer tool, you can retrieve log files to help you troubleshoot system issues. To help you troubleshoot Cisco SD-Access or software image management (SWIM) issues, you can also retrieve log files that are specific to those components.
Disk Utilization Event Notifications	You can now subscribe to and receive notifications that are sent whenever disk utilization by the nodes in your system reaches a level that can impact network operations.
Software Management Window	The look and feel of the **Software Updates** window that was provided in earlier Cisco DNA Center releases has been updated. In this release, you can initiate system and application updates from the new **Software Management** window (menu icon > **System** > **Software Management**).
Configure ThousandEyes Integration	You can configure an external ThousandEyes APIs agent to enable ThousandEyes Integration using the authentication token. After integration, Cisco DNA Center provides ThousandEyes agent test data in the Application Health dashboard.
Two-Site Failure Response Updates	Cisco DNA Center's response to failures involving at least two of a disaster recovery system's sites has been enhanced.
NTP Server Authentication	When configuring your Cisco DNA Center appliance using the Advanced Install Configuration wizard, you can now enable the authentication of your NTP server before it is synchronized with Cisco DNA Center.

New and Changed Features in Cisco DNA Assurance

Feature	Description
Wireless Controller Event Viewer	Event Viewer has been updated to include events logged by Cisco AireOS and Cisco IOS wireless controllers.
Wireless Controller 360 KPIs	Cisco DNA Assurance now provides temperature and interface information on the Device 360 window for wireless controllers.
Custom Issue Settings (Network Profiles for Assurance)	You can create custom issue settings for a specific site or group of sites. These settings are called *network profiles* for Assurance and can be managed from both Assurance and Cisco DNA Center. By creating a network profile for Assurance, you can control which issue settings are monitored, and you can change the issue priority.
Maintenance Mode	While a network device is in maintenance mode, Cisco DNA Center does not gather health data, collect interface statistics, trigger issues, or include the device in calculating health scores. Devices that are under maintenance are displayed in the **Under Maintenance** banner below the timeline slider in the Application 360 window.

Feature	Description
Enhanced RRM Dashboard	With this release, Cisco AI Network Analytics uses artificial intelligence to define the behavior of a radio frequency (RF) network within a building enabled with enhanced Radio Resource Management (RRM).
Export Assurance Windows	With this release, you can export the following Assurance Health windows to PDF format: • Overall Dashboard • Network Dashboard • Client Dashboard • WiFi- 6 Dashboard • PoE Dashboard
Webex Client 360	In the Webex Client 360, the client meetings table is enhanced with the following columns to indicate the overall health for each meeting: • Application: Shows the health scores and KPIs reported by Webex Control Hub. • Network: Shows the health scores and KPIs reported by Cisco DNA Center through NetFlow exported from the managed network devices.
Floor Filters	In the Assurance Network Heatmap window, you can filter heatmap data for specific floors from the **Building** drop-down list in the site hierarchy.
Wi-Fi 6E	With this release, Wi-Fi 6E support is added to the Wi-Fi 6 dashboard. • Insight for Wi-Fi 6E. • Added **Wi-Fi 6E** and **Wi-Fi 6** in the **Status** drop-down for the Client Distribution by Capability and Network Readiness dashlets. • Added **Wi-Fi 6E Traffic** for the Wireless Airtime Efficiency and Wireless Latency dashlets.
NetFlow Visibility	In the Application Health dashboard, the summary dashlet displays the total number of packets and the exporters in the **NETFLOW** area.
Application Health Dashboard Enhancement	With this release, the Application Health dashboard includes ThousandEyes Integration with enterprise agent tests. The dashboard is populated with agent tests only when NetFlow is received for at least one device on the site.
Cisco AI Network Analytics - Radio Insights Based on Client Experience	Cisco AI Network Analytics uses machine learning algorithms to identify wireless access points with a potentially poor client experience. APs are continually analyzed over long periods and those suspected of providing a suboptimal client experience are grouped by underlying root cause and suggested improvements.

New and Changed Features in Cisco DNA Automation

Feature	Description
Remote Teleworker Site	You can use Cisco DNA Center to configure remote teleworker sites. Remote teleworker sites provide a more secure connection, proper application prioritization, and a simple installation and onboarding experience for remote workers.
Network Bug Identifier Tool	The Network Bug Identifier Tool GUI has been enhanced due to integration improvements between the Network Bug Identifier Tool and the Cisco CX Cloud. The GUI no longer shows the number of affected routers, switches, and hubs in the summary pane at the top of the results window. Instead, the GUI shows the scan mode, either **Essential** using the Cisco Machine Reasoning Engine (MRE) or **CX Cloud**. The results table also shows the scan status for each device. For the Network Bug Identifier Tool and bugs supported through the Cisco CX Cloud, the supported families are switches and hubs, routers.
Download Error Report	In the **Tasks** window, **Download Error Report** link is added in the slide-in pane of a failed task that allows you to download the contextual troubleshooting information of a particular task.
Default Home Page	The default home page includes the following enhancements: • **Remote Support Authorization**: You can grant remote access to a Cisco specialist to access Cisco DNA Center and troubleshoot your network. • **Keyboard Shortcuts**: You can view keyboard shortcut names, shortcut keys, and shortcut key combinations for shortcut groups.
Remote Support Authorization Dashboard	You can create, cancel, and view past remote support authorizations along with total, scheduled, and completed remote support authorizations. **Note** In this release, the Cisco DNA Center remote support authorization is supported with only LM Console version 0.40.5.
Create Remote Support Authorization	With this release, Cisco DNA Center allows you to create remote support authorization to grant remote access to a Cisco specialist for troubleshooting the network.
View Security Advisories	• Cisco DNA Center support is extended for **SCAN CRITERIA** in the security advisory dashboard. You can view the **Software Version**, **Custom** scan, and **Advanced** scan. • With this release, in the security advisory window, a new **Try Cisco CX Cloud Success Track** link allows you to enable the Cisco CX Cloud service and rescan the network to identify security advisories based on automated config scans. For the security advisories enhanced through the Cisco CX Cloud, the following families, software, and versions are supported: • Supported families: Switches and hubs, routers, wireless controllers. • Supported software: Cisco IOS, IOS-XE. • Supported versions: For Cisco IOS, 15.2(2)E3 and later. For Cisco IOS-XE, 3.6.5E and later, 16.3.1 and later, 3.7.0 and later, 17.1.1 and later.

Feature	Description
Machine Reasoning Knowledge Base	Machine reasoning knowledge base support is extended for the Cisco CX Cloud service for network bug identifier and security advisory.
Manage Your Inventory	While assigning a device to a site, **Generate Configuration Preview** allows you to preview the configuration.
Configure Telemetry	When you update a device configuration using telemetry, **Generate Configuration Preview** allows you to preview the configuration.
Configure Network Settings	Cisco DNA Center support is extended for AI Radio Frequency (RF) profiles, which allows you to define the behavior of an RF network within a building enabled with enhanced Radio Resource Management (RRM).
Support for New Model Config Designs	• **Model config design for Advanced SSID**: Use the advanced Service Set Identifier (SSID) model config to configure the advanced SSID parameters on devices. • **Model Config Design for Event Driven RRM**: The event-driven RRM model config feature configures event driven RRM parameters for 2.4 GHz, 5 GHz, and 6 GHz radios. **Note** 6 GHz radio band is not supported on Cisco AireOS Wireless Controller. Cisco Catalyst 9800 Series Wireless Controller version 17.6 and later releases support 2.4 GHz and 5 GHz radio bands. • **Model config design for RRM general parameters**: The RRM general configuration model config feature configures the RRM general parameters for 2.4 GHz, 5 GHz, and 6 GHz radios. **Note** 6 GHz radio band is not supported on Cisco AireOS Wireless Controller. Cisco Catalyst 9800 Series Wireless Controller version 17.6 and later releases support 6 GHz radio band.
AP Reboot for Troubleshooting	Using the AP Reboot feature, you can reboot one or more APs for troubleshooting and maintenance using the Cisco DNA Center GUI.
Support for AP LED Flash Status	You can locate APs on the physical site by enabling LED Flash Status for APs using the Cisco DNA Center GUI.
Custom Redirect ACL for Enterprise SSID	Using the Pre-Authentication ACL feature, you can create a pre-authentication ACL for web authentication to allow certain types of traffic before authentication is complete. This ACL is referenced in the access-accept of Cisco Identity Services Engine (ISE) and defines what traffic to be permitted and what traffic to be denied by the ACL. After ACLs are configured on the wireless controller, they can be applied to the management interface, the AP-manager interface, any of the dynamic interfaces, or a WLAN to control data traffic to and from wireless clients or to the controller central processing unit (CPU) to control all traffic destined for the CPU. You can configure both IPv4 and IPv6 ACLs.

Feature	Description
URL Filtering	Using URL filtering, you can add specific URLs to the allowed list for web authentication of captive portals and walled gardens. Authentication is not required to access the allowed list of URLs. When you try to access sites that are not in the allowed list, you are redirected to the login page.
Posture Assessment	Posture is a service in Cisco ISE that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies. This allows you to control clients to access protected areas of a network.
Create an Event Notification	You can use the Cisco DNA Center event notification to associate multiple channels inside one notification. The notification delivers the details of selected events that occur at multiple points.
Artificial Intelligence (AI) Radio Frequency (RF) Profile	You can create, edit, delete, configure, assign, and unassign an AI RF profile. An AI RF profile allows you to define the behavior of an RF network within a building that is enabled with enhanced Radio Resource Management (RRM). You can also upgrade a basic RF profile to an AI RF profile.

New and Changed Features in Cisco Software-Defined Access

Feature	Description
Support for Supplicant-Based Extended Nodes	You can onboard supplicant-based extended nodes by configuring an authenticator port on the fabric edge with a Closed Authentication Template. Only specific platforms support supplicant-based extended node onboarding. Supplicant-based extended nodes are extended node devices that receive an 802.1X supplicant configuration and are onboarded into the SD-Access network only after a complete authentication and authorization. The authenticator port on the edge node must be configured with a Closed Authentication Template. Supplicant-based extended node onboarding is a one-touch process. After the network administrator claims the supplicant device through the Cisco DNA Center Plug and Play menu options, the supplicant device is onboarded into the network. Cisco Catalyst 9200 Series, 9300 Series, 9400 Series, 9500 Series, and 9500H Series switches that run on Cisco IOS XE 17.7.1 or later release can be configured as a supplicant-based extended node. Cisco Catalyst 9300 Series, 9400 Series, 9500 Series, and 9500H Series switches that run on Cisco IOS XE 17.7.1 or later release can be configured as an edge node.
DHCP Snooping on Extended Nodes	DHCP Snooping is now provisioned on the Cisco Catalyst 9000 Series switches that are configured as extended nodes. Extended node devices share the device sensor configuration data of the endpoints with the Cisco Identity Services Engine (ISE). Cisco ISE uses this data to profile the endpoints.

Feature	Description
Bridge-Mode Virtual Machine in a Fabric-Enabled Wireless Network	The virtual machines that run inside a host computer must be identifiable. To profile the virtual machines, create the virtual machines in a bridge mode. In the bridge mode, each virtual machine is assigned an IP address and all the virtual machines are connected by a bridge. Each virtual machine is individually authenticated and authorized into the Cisco SD-Access network. This release of Cisco DNA Center supports onboarding of wireless bridge-mode virtual machines. You can configure a Wireless IP address pool with **Bridge Mode VM** enabled to authenticate and profile wireless bridge-mode virtual machines. For more information, see the *Cisco DNA Center User Guide*.
Support for FQDN-Based Certificate in LAN Automation and Plug and Play Workflows	LAN Automation workflows now support the onboarding of factory default devices with a fully qualified domain name (FQDN)-based certificate.
IS-IS Configuration Through LAN Automation	LAN Automation now configures devices to operate at IS-IS Level 2, instead of operating at both Level 1 and Level 2.
REP Ring Topology Support for Extended Nodes and Policy Extended Nodes	When extended nodes are connected to a fabric network, they onboard as a Spanning Tree Protocol (STP) ring, by default. In Cisco DNA Center 2.3.2 and later releases, you can configure the extended nodes and policy extended nodes in a Resilient Ethernet Protocol (REP) ring. Multiple rings within a given ring and a ring of rings aren't supported. However, a fabric edge node can support multiple independent rings. REP rings can only start and end on the same fabric edge node. REP rings starting and ending on extended nodes aren't supported. A REP ring or a daisy chain can't be a mix of extended nodes and policy extended nodes. A REP ring or a daisy chain must consist entirely of either extended nodes or policy extended nodes. The following devices can be configured in a REP ring: • Extended Node Devices: Cisco Industrial Ethernet (IE) 4000 Series switches, IE4010 Series switches, and IE5000 Series switches that run on Cisco IOS 15.2(7)E3 or later releases. Cisco Catalyst IE3300 Rugged Series switches that run on Cisco IOS XE 17.3.3 and later releases. • Policy Extended Node Devices: Cisco Catalyst IE3400 Rugged Series switches and IE3400 Heavy Duty Series switches that run on Cisco IOS XE 17.3.3 and later releases.

Feature	Description
Application Hosting support for ThousandEyes in a Cisco SD-Access network	Cisco DNA Center Application Hosting Service already supports ThousandEyes Enterprise Agent on nonfabric devices. Cisco DNA Center Release 2.3.2.0 introduces the support for ThousandEyes Enterprise Agent on the devices in your fabric network too. In the **App Hosting for Switches** workflow, select a fabric device and select the VLAN to map with the ThousandEyes Enterprise Agent network interface. For more information on installing an application and its maintenance, see "Application Hosting" in the *Cisco DNA Center User Guide*. Cisco Catalyst 9300 Series switches, Cisco Catalyst 9300L Series switches and Cisco Catalyst 9400 Series switches that run Cisco IOS XE 17.3.1 and later releases support the hosting of ThousandEyes Enterprise Agent application in a fabric network.

New and Changed Features in Interactive Help

Table 3: New and Changed Features in Interactive Help, Release 2.3.2.3

Feature	Description
Additional Interactive Help Walkthroughs	Added the following walkthroughs: • Edit a Fabric Zone • Add Layer 3 Virtual Network to Fabric Site • Add Layer 3 Virtual Network to Fabric Zone • Add Anycast Gateway to Fabric Zone • Add Layer 2 Virtual Network to Fabric Zone • Edit Layer 2 Virtual Network Properties • Edit Anycast Gateway Properties
Deprecated Walkthroughs	The following walkthrough is deprecated: Create a Fabric

Table 4: New and Changed Features in Interactive Help, Release 2.3.2

Feature	Description
Additional Interactive Help Walkthroughs	Added the following walkthroughs: • Add Walls and Shelving Units to a Floor • Position APs on a Floor
Additional Resources Pages	Added the following resources: • Cisco DNA Center Product Page • Log Advisor

Deprecated Features

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

Cisco DNA Center Compatibility Matrix

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

Cisco SD-Access Compatibility Matrix

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

Compatible Browsers

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

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

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

Note For an upgrade to Cisco DNA Center 2.3.2, 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 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(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 an existing network firewall, see "Required Internet URLs and Fully Qualified Domain Names" in the "Plan the Deployment" chapter of the *Cisco DNA Center Installation Guide*.

About Telemetry Collection

Telemetry data is collected by default in Cisco DNA Center, but you can opt out of some data collection. The data collection is designed to help the development of product features and address any operational issues, providing greater value and return on investment (ROI). Cisco collects the following categories of data: Cisco.com ID, System, Feature Usage, Network Device Inventory, and License Entitlement. See the *Cisco DNA Center Data Sheet* for a more expansive list of data that we collect. To opt out of some of 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 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.

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

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.

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
CSCvz84414	In a Cisco DNA Center system where file system utilization exceeds 60%, if you upgrade to Cisco DNA Center 2.3.2, you can see the warning or critical notifications for file system utilization only on the **System** > **System Health** window; you are not notified via email. If you subscribe to the event after the upgrade, only events that occur after the subscription generate email notifications.
CSCvz88977	In the Wide Area Bonjour Dashboard, you cannot select the year and date in the **Average Service Query Statistics** area.
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.
CSCwa09236	Devices health information is missing in multiple Assurance dashboards for few devices randomly.
CSCwa11477	The **Assurance** > **AI Network Analytics** > **Enhanced RRM** window shows some inconsistencies in the X-axis values for the Trend charts. Some dates and timestamps are missing from the X axis on the graphs.
CSCwa15687	In Cisco DNA Center 2.3.2, there is a new "Software Management" feature for upgrading. If you use a Firefox browser for the Cisco DNA Center upgrade, there are some problems with maintenance mode updates and exiting the original browser connection. When you use a Chrome browser for the upgrade, the problems are not seen. **Note** For an upgrade to Cisco DNA Center 2.3.2, we recommend that you use Chrome, not Firefox.

Bug Identifier	Headline
CSCwa16013	On the **Policy** > **AI Endpoint Analytics** > **Endpoint Inventory** window, filtering is slightly delayed when the table contains large amounts of data. For example, if you have more than 5000 values for endpoint type or hardware manufacturer, filtering may take approximately 20 seconds or more.
CSCwa16886	The Cisco DNA Center GUI allows the same minimum and maximum power level value in a radio frequency profile. The expected behavior is that the minimum and maximum power levels must be different.
CSCwa29973	CTS credentials of the device are not in sync with the ISE NAD entry.
CSCwa35027	Deleting faulty device from inventory failed in RMA flow.
CSCwa40072	Assurance data of wired clients is inconsistent in a disaster recovery setup after failover.
CSCwa44702	For Wide Area Bonjour, inactive services are not flushed after the inactive timer expires.
CSCwa44851	NetFlow are not processed by Cisco DNA Center. NetFlow information doesn't appear in the **Assurance** > **Application** window.
CSCwa44855	After an upgrade, some devices under the **Tools** > **License Manager** > **Devices** tab are tagged incorrectly with "Needs Registration."
CSCwa45180	During HA, the pipeline-taskmgr-assurance service goes into a crash loop.
CSCwa45925	On the Device 360 window, CPU and Memory values do not populate for Cisco Catalyst 9300 switches.
CSCwa51111	During HA, the pipeline-task mgr-assurance service keeps restarting.
CSCwa53762	In the Learn Device Configuration workflow, if a non-flex SSID is learned, the site tag has "default-flex-profile" as the flex profile name. Under **Design** > **Network Profiles** > **Wireless**, the same non-flex site tag is mapped with "default-flex-profile" as the profile name. This behavior is inline with the device configuration.
CSCwa92273	The dnacp-formatter-service is not starting after upgrading from Cisco DNA Center 2.1.2.6 to 2.2.2.8.

CSCwb14795	While deploying Cisco DNA Center 2.3.2.3, packages do not download correctly.
	To work around this problem, do the following:
	1. Pull the packages.
	2. Enter the following command to verify that the relevant packages are in Ready state:
	`maglev catalog package display -V`
	3. Deploy the packages and then enter the following command to check the progress:
	`maglev package status`

Resolved Bugs

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.2.3.

Table 5: Resolved Bugs in Cisco DNA Center, Release 2.3.2.3

Bug Identifier	Headline
CSCvw64912	Cisco DNA Center may fail to provision a Cisco Catalyst 9800 Series Wireless Controller, citing the following error: `ERROR: duplicate key value violates unique constraint "wirelessgrouping_bk".`
CSCvz98664	Adding and removing a fabric edge provisions wireless controllers randomly with different configurations.
CSCwa16652	Many manually generated reports in Cisco DNA Center result in blank pages.
CSCwa18877	Ekahau file import fails with the following API error: `The specified group ID is null or empty.`
CSCwa21212	Unable to start LAN automation due to the following error: `NCND00050: An internal error occurred while processing the request.`
CSCwa26591	SBEN nodes toggle between inbuilt templates, resulting in error disabled.
CSCwa27606	Cisco DNA Center 2.2.3.3: PnP fails to claim a device.
CSCwa40727	Fabric deploy sends an incorrect RADIUS authentication server command, and provisioning fails for an AireOS wireless controller.
CSCwa43532	A user intent validation failure occurs when provisioning a wireless controller.
CSCwa51430	Assurance shows an end host MAC in an old user's client 360 window.
CSCwa51827	Banner push for LISP key change fails in Cisco DNA Center 2.2.2.x if there are wireless devices.
CSCwa52917	A null pointer exception occurs while accessing Show Task from the **Image Repository** window.
CSCwa67154	The new Cisco DNA Center Platform UI API docs are missing the API URL.
CSCwa72663	The banner must be updated with a warning that wireless controller provisioning must succeed before attempting a LISP key change.
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.
CSCwb17117	After a DR Pause + Backup and Restore + DR Rejoin workflow, the Config Preview workflow for provisioning fails. Also, device reprovisioning fails for all devices with the following error: `Provisioning failed due to error in retrieval of the ISE PAN IP addresses.`

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.2.0.

Table 6: Resolved Bugs in Cisco DNA Center, Release 2.3.2.0

Bug Identifier	Headline
CSCvq54768	Cisco DNA Center silently pushes Identity-Based Networking Services (IBNS) 2.0 "new-style" commands to any switch that is provisioned. If there is no Cisco ISE integration to replace these commands, the port security configurations might be removed.
CSCvw68074	Containers from one Cisco DNA Center node may become stuck in the state "ContainerCreating, failing to pull image" due to issues with GlusterFS mounting on one node, and replication across all nodes.
CSCvw80355	AAA/Cisco ISE inheritance settings do not display correctly between Global and sites in certain flows.
CSCvx10782	A package upgrade fails because the table "lispmssiteeidprefix" violates a foreign key constraint.
CSCvx41364	The large MongoDB database size causes a MongoDB clustering failure.
CSCvx52786	Creating a segment with non-alphanumeric characters in the VLAN name fails with a provisioning error.
CSCvx56010	Virtual routing and forwarding (VRF)-specific name servers are removed by Cisco DNA Center.
CSCvx74221	Provisioning fails when adding a AAA server using a port number greater than 32767 to Cisco DNA Center.
CSCvx76405	During an upgrade of Cisco DNA Center application packages, the upgrade may appear to be stuck for hours at 20% with no obvious movement forward. The migration logs show a deadlock on the Postgres executionevent table. This issue stems from a large database table upon which database update queries pile up, causing a deadlock.
CSCvx79755	Interface information takes a long time to populate after LAN automation.
CSCvx93717	Client Detail, Client Session, and AP Radio reports fail.
CSCvy05782	In stacked devices, the TrustSec ID and password are set to primary/active serial numbers only.
CSCvy06455	Cisco DNA Center may fail to provision a Nexus 7710 if there is an octothorp "#" character in the device login banner.
CSCvy10747	Messages in the "dna.lan.common.service" queue block subsequent LAN automation.
CSCvy12915	When importing an .esx file from an Ekahau project, the azimuth is always off by 90 degrees.
CSCvy17114	SNMP traps are not configured after a device is deleted and readded.
CSCvy18066	Templates created and exported from Cisco DNA Center 2.1.2.6 may not be able to be imported into Cisco DNA Center 2.1.2.5.
CSCvy24764	Offline APs are shown as active on a heatmap.
CSCvy26789	When attempting to set up the integration between Cisco DNA Center and Cisco DNA Spaces, the integration may fail with the error message, "Unable to export hierarchy to the CMX DNA Spaces for one or more domains."
CSCvy27260	Cisco DNA Center may fail to synchronize a Cisco Catalyst 9000 series switch that is configured with an access-list associated to the netconfig-yang configuration.

Bug Identifier	Headline
CSCvy37982	Cisco DNA Center may push a different Anycast Gateway MAC address to some fabric edge nodes, which causes multiple edge nodes to register a single wired client with the MSMR and control plane, even though the wired client is connected to a single edge node and is not roaming.
CSCvy43861	The config archive tries to capture data from unreachable devices.
CSCvy48594	The Assurance event notifications device parameter returns the device UUID, not the device IP address.
CSCvy53714	Wireless controller provisioning fails on IRCM version validation.
CSCvy56987	An upgrade to Cisco DNA Center 2.1.2.x fails with the PSQLException error, "ERROR: could not create unique index mdfproductfamily_pkey."
CSCvy60496	Cisco DNA Center may fail to provision a device, citing the error, "Unable to push CLI 'timeout 0' to device x.x.x.x."
CSCvy63436	Updating many devices frequently may cause Cisco DNA Center's scheduler service to restart.
CSCvy63818	Cisco DNA Center fails to generate a PKCS12 certificate due to the error, "Failed to find internal Trustpoint."
CSCvy65690	Reserved child pools for L3 handoff are not released after a failed fabric provision.
CSCvy66833	Cisco DNA Center cannot assign some Meraki APs to a site.
CSCvy72489	An error occurs while using the Cisco DNA Center BAPI connector on ServiceNow.
CSCvy73302	Cisco DNA Center may not generate a heatmap for the 2.4-GHz band of Cisco Catalyst 9120 APs, even though it is generated for the 5-GHz band as expected.
CSCvy80252	Cisco ISE integration fails with the error, "FQDN x doesn't match the common name contained in the system certificate."
CSCvy86724	The Inventory service may crash if the managed devices send a high volume of syslogs to Cisco DNA Center.
CSCvy88667	After upgrading to Cisco DNA Center 2.1.2.7, inventory collection from an existing Catalyst 9500 switch fails, citing the exception, "ERROR: update or delete on table 'protocolendpoint' violates foreign key constraint 'fkad4b72e9a8fce39d' on table 'vxlannvesettings'."
CSCvy89652	Cisco DNA Center fails to display an ROI report.
CSCvy91546	Provisioning fails after segment deletion and site rename while a device is offline.
CSCvy93346	Cisco DNA Center may be unable to remove a managed device from a fabric-in-a-box installation, citing the following error in the network programmer service's logs: `ERROR: update or delete on table "lisprtrlocatorset" violates foreign key constraint "fk9d5ac9b056ea3464" on table "lisprtrlocatorsetentry".`
CSCvy94846	An appliance mismatch occurs between the main (DN2-HW-APL-XL) and the recovery (DN2-HW-APL-XL-U) appliance.
CSCvy94920	After setting TLS v1.2 as the minimum supported version, some ports still show TLS v1.1.

Bug Identifier	Headline
CSCvy97313	A device fails inventory collection due to missing database entries after an image upgrade.
CSCvy98355	LAN automation may not configure the L3 link between the peer seed and the PnP agent.
CSCvz07929	NetFlow table updates are too aggressive for large-scale deployments.
CSCvz10208	Cisco DNA Center may create a duplicate site tag with the default-flex-profile linked to it when an existing wireless LAN controller is reprovisioned.
CSCvz11253	A system upgrade fails from Cisco DNA Center 2.2.2.x to Cisco DNA Center 2.2.3.x.
CSCvz14636	When Cisco DNA Center attempts to configure Application Visibility and Control (AVC) to an eight-member stack of Catalyst 9000 switches, the process may fail with the error, "NBAR Error: Cannot enable Protocol-discovery - platform interface limit reached."
CSCvz18219	Cisco DNA Center may fail to provision a wireless LAN controller that had previously been removed from a fabric and inventory, citing a null pointer exception during the updateApN1HAConfig process.
CSCvz18421	The NAC RADIUS configuration on the WLAN profile is lost when the wireless controller reloads.
CSCvz24855	Fabric provisioning fails when a border device is removed.
CSCvz27424	When Cisco DNA Center provisions a managed wireless controller, the affected wireless SSID may go down because the required interface description on the SSID's switched virtual interface (SVI) is overwritten with null.
CSCvz33630	Clear Port Config succeeds from the GUI, but the config is still present on the device.
CSCvz36352	LAN automation doesn't release the DHCP subnet while LAN Auto start fails.
CSCvz43500	WLANs on a foreign wireless controller get disabled on provisioning of the anchor wireless controller.
CSCvz48575	An upgrade to Cisco DNA Center removes the TACACS key to network devices from Cisco ISE.
CSCvz51081	Cisco DNA Center may become unresponsive in two to four weeks after being rebooted. When this happens, there is no GUI access, no SSH access, or response from the Cisco IMC's KVM console.
CSCvz55757	The wrong L2 instance is pushed to the anchoring site if a different VLAN name is used.
CSCvz56988	SSA to address route lookup gaps for interface selection.
CSCvz59187	Create or update floormaps API documentation does not include the payload request schema.
CSCvz61107	Cannot edit email parameters after the first entry in destinations in Cisco DNA Center 2.2.2.x.
CSCvz65929	Cisco DNA Center may fail to configure native Any-Source Multicast (ASM), citing the error, "Unable to push CLI 'ip pim lisp transport multicast' to device xx.xx.xx.xx using protocol ssh2".
CSCvz70561	While adding additional edge switches to an existing fabric, Cisco DNA Center may alter the AAA configuration of an existing wireless LAN controller from TACACS to RADIUS.
CSCvz72857	Image import fails with the error, "File exists in Softwareimageinfo but unable to add to File Service."

Bug Identifier	Headline
CSCvz87778	LAN automation fails with "Error while reserving link subnet:..." when there are more than 31 dummy pools.
CSCvz88461	When the maps API calls Assurance APIs, the sensor API fails.
CSCvz89312	An interface (like GigabitEthernet0/0/0, 0/0/1) selected from the drop-down list reverts to GigabitEthernet0.
CSCvz94163	Deployment of the security fix fabric banner removes RADIUS PAC from extended nodes.
CSCvz98644	All wireless controllers are implicitly configured when IP pools are assigned or removed from fabric WLANs on the Host Onboarding window.
CSCvz99700	Cannot delete a segment from host onboarding.
CSCwa01977	LAN automation must align to the *Cisco DNA Center Security Best Practices Guide*.
CSCwa10370	A Cisco ISE node PSN that is added as a AAA server in Cisco DNA Center cannot be removed, even if no WLAN is using the node as AAA.
CSCwa21575	A supplicant-based extended node fails to onboard via Plug and Play using a Cisco DNA Center-provisioned ACL.
CSCwa21789	EVENT_BASED_WIRED_WIRELESS_SYNC causes an internal error for the protocol endpoint.
CSCwa21979	Device discovery tasks remain stuck in RUNNING state for a long time, clogging up the inventory service, which in turn prevents global credentials from being displayed. Because the global credentials don't load, new discovery tasks cannot start. The inventory service logs contain the following error logs: `ERROR | covery-Pingsweep-Thread-0 | | com.cisco.nm.discovery | ERROR: [Failed to process status of ping request]. | mid=10001, MSGNAME=ERROR, ch=com.cisco.nm.discovery, sev=error`

Limitations and Restrictions

Upgrade Limitation

- If you are upgrading to Cisco DNA Center and all of 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 related to the upgrade failure.

  To work around this problem, upgrade Cisco ISE to 2.6 patch 1, 2.4 patch 7, or later, and retry the Cisco DNA Center upgrade.

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

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 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.
- Re-enter the device credentials in the restored database. If you updated the site-level credentials before the database restore, and the backup that is being restored does not have the credential change information, all the devices go to partial collection after the restore. You must then manually update the device credentials on the devices for synchronization with Cisco DNA Center, or perform a rediscovery of those devices to learn the device credentials.
- Perform AAA provisioning only after adjusting network device differential changes to the restored database. Otherwise, device lockouts might occur.
- You can back up and restore Automation data only or both Automation and Assurance data. But you cannot use the GUI or the CLI to back up or restore only Assurance data.

Cisco ISE Integration 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 Limitation

The Cisco DNA Center License Manager supports Smart Licensing only for wireless LAN controller models that run Cisco IOS XE. License Manager does not support wireless LAN controller models that run Cisco AireOS.

Fabric Limitations

- Cisco DNA Center supports up to a maximum of 1.2 million interfaces on fabric devices. Fabric interfaces include physical and virtual interfaces like switched virtual interfaces, loopback interfaces, and so on.

  Physical ports cannot exceed 480,000 ports on a 112-core appliance.

- IP address pools 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.
- When a wireless controller is in maintenance mode, all the associated APs are automatically placed in maintenance mode. However, you can't place the APs in maintenance mode individually if the associated wireless controller is not in maintenance mode.

Inter-Release Controller Mobility (IRCM) Limitation

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

IP Device Tracking on Trunk Port Limitation

Rogue-on-wire detection is impacted; Cisco DNA Center does not show all 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 is met:

  - No values are configured in the 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, 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 will 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 - 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 scalable group to another, Cisco Group-Based Policy Analytics is unaware of this change until the next hour.
- You cannot sort the Scalable 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
```

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 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 ITSM integration and Cisco DNA Center ITSM 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*

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021–2023 Cisco Systems, Inc. All rights reserved.