# Release Notes for Cisco DNA Center, Release 2.3.4.x

**First Published:** 2022-09-21

**Last Modified:** 2023-11-07

## Release Notes for Cisco DNA Center, Release 2.3.4.x

Cisco DNA Center 2.3.4.x is available in a phased rollout. Contact your Cisco sales representative to request this release.

This document describes the features, limitations, and bugs for Cisco DNA Center, Release 2.3.4.x.

For links to all of the guides in this release, see Cisco DNA Center 2.3.4 Documentation.

### Change History

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

| Date | Change | Location |
|---|---|---|
| 2023-11-07 | Added a limitation about custom applications. | Limitations and Restrictions, on page 31 |
| 2023-08-02 | Previously, the *Cisco DNA Center Release Notes* and the *Cisco DNA Center Platform Release Notes* were separate. Now, they are combined into a single release note; the Cisco DNA Center platform content has been consolidated into this document. | — |
| 2023-07-06 | Noted that if you run Cisco DNA Center in IPv6 mode, wireless controller provisioning is not supported. | Limitations and Restrictions, on page 31 |
| 2023-06-07 | Noted that if you run Cisco DNA Center in IPv6 mode, LAN automation is not supported. | Limitations and Restrictions, on page 31 |
| 2023-05-19 | Added information about using the Validation Tool to run preupgrade checks. | Upgrade to the Latest Cisco DNA Center Release, on page 2 |
| 2023-02-17 | Added a limitation about In-Service Software Upgrade (ISSU). | Limitations and Restrictions, on page 31 |
| 2022-12-14 | Added the list of packages in Cisco DNA Center 2.3.4.3. | Package Versions in Cisco DNA Center, Release 2.3.4.x, on page 2 |
| | Added the Resolved Bugs table for 2.3.4.3. | Resolved Bugs, on page 28 |
| | Added the open bug CSCwd17228. | Open Bugs, on page 27 |
| 2022-09-21 | Initial release. | — |

## Upgrade to the Latest Cisco DNA Center Release

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

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

## Package Versions in Cisco DNA Center, Release 2.3.4.x

| Package Name | Release 2.3.4.3 | Release 2.3.4.0 |
|---|---|---|
| **Release Build Version** | | |
| Release Version | 2.3.4.3.70172 | 2.3.4.0.70523 |
| **System Updates** | | |
| System | 1.7.808 | 1.7.774 |
| System Commons | 2.1.563.60229 | 2.1.560.60835 |
| **Package Updates** | | |
| Access Control Application | 2.1.563.60229 | 2.1.560.60835 |
| AI Endpoint Analytics | 1.8.576 | 1.8.525 |
| AI Network Analytics | 2.10.16.314 | 2.10.10.294 |
| Application Hosting | 2.0.02209080642 | 2.0.02205161126 |
| Application Policy | 2.1.563.170211 | 2.1.560.117594 |
| Application Registry | 2.1.563.170211 | 2.1.560.117594 |
| Application Visibility Service | 2.1.563.170211 | 2.1.560.117594 |
| Assurance - Base | 2.3.4.336 | 2.3.4.277 |
| Assurance - Sensor | 2.3.4.333 | 2.3.4.217 |
| Automation - Base | 2.1.563.60229 | 2.1.560.60835 |
| Automation - Intelligent Capture | 2.1.563.60229 | 2.1.560.60835 |
| Automation - Sensor | 2.1.563.60229 | 2.1.560.60835 |
| Cisco DNA Center Global Search | 1.9.1.6 | 1.9.1.6 |
| Cisco DNA Center Platform | 1.9.1.90 | 1.9.1.78 |
| Cisco DNA Center UI | 1.7.2.312 | 1.7.2.306 |
| Cisco Identity Services Engine Bridge | 2.1.563.1018 | 2.1.560.451 |

| Package Name | Release 2.3.4.3 | Release 2.3.4.0 |
|---|---|---|
| Cisco Umbrella | 2.1.563.590131 | 2.1.560.590253 |
| Cloud Connectivity - Contextual Content | 2.5.1.345 | 2.5.1.345 |
| Cloud Connectivity - Data Hub | 1.9.47 | 1.9.38 |
| Cloud Connectivity - Tethering | 2.30.1.72 | 2.30.1.72 |
| Cloud Device Provisioning Application | 2.1.563.60229 | 2.1.560.60835 |
| Command Runner | 2.1.563.60229 | 2.1.560.60835 |
| Device Onboarding | 2.1.563.60229 | 2.1.560.60835 |
| Disaster Recovery | 2.1.563.360021 | 2.1.560.360043 |
| Disaster Recovery—Witness Site | 2.1.563.370016 | 2.1.560.370025 |
| Group-Based Policy Analytics | 2.3.4.17 | 2.3.4.17 |
| Image Management | 2.1.563.60229 | 2.1.560.60835 |
| Machine Reasoning | 2.1.563.210158 | 2.1.560.210319 |
| NCP - Base | 2.1.563.60229 | 2.1.560.60835 |
| NCP - Services | 2.1.563.60229 | 2.1.560.60835 |
| Network Controller Platform | 2.1.563.60229 | 2.1.560.60835 |
| Network Data Platform - Base Analytics | 1.9.134 | 1.9.96 |
| Network Data Platform - Core | 1.9.212 | 1.9.175 |
| Network Data Platform - Manager | 1.9.59 | 1.9.59 |
| Network Experience Platform - Core | 2.1.563.60229 | 2.1.560.60835 |
| Path Trace | 2.1.563.60229 | 2.1.560.60835 |
| RBAC Extensions | 2.1.563.1900001 | 2.1.560.1900006 |
| Rogue and aWIPS | 2.6.0.37 | 2.6.0.36 |
| SD-Access | 2.1.563.60229 | 2.1.560.60835 |
| Stealthwatch Security Analytics | 2.1.563.1090110 | 2.1.560.1090244 |
| Support Services | 2.1.563.880007 | 2.1.560.880041 |
| Wide Area Bonjour | 2.4.563.75063 | 2.4.560.75194 |

# New and Changed Information

## New and Changed Features in Cisco DNA Center

| Feature | Description |
|---|---|
| Acknowledge Compliance Violations | You can acknowledge less important compliance violations and opt-out the violations from Compliance status calculation. |
| Add Openings (Atriums) in 2D Wireless Maps | You can add openings, also called atriums, to 2D maps. |
| Certificate Revocation Check | You can configure a certificate revocation check. |
| Compliance Support for EoX - End of Life | Compliance support is extended for hardware, software, and module of EoX devices. |
| Configure NBAR Cloud Connector | You can enable a protocol pack auto update. |
| Create Secure Tunnel | You can create an automated, secure IPsec tunnel to a new edge device at a branch location. This provides high-speed, secure, IPsec WAN connectivity to Cloud Security (Umbrella and Zscaler), and Enterprise connections. |
| Default Home Page | The Cisco DNA Center default home page help menu support is extended for Cisco CX Cloud Success Tracks, which allows you to access the Cisco CX cloud success tracks website in a new window. |
| Device Support for Extended Node | Stacked IE9300 switches can be onboarded as Extended Nodes or Policy Extended Nodes through Plug and Play. |
| Disable Applications and Endpoint Visibility | Applications and Endpoint Visibility is enabled by default; you can disable it. |
| Discovery Workflow Enhancements | The following enhancements are available from this release:<br>• In the **Provide Credentials** window, add **HTTP(S) Read** and **HTTP(S) Write** credentials.<br>• In the **Schedule Task** window, click the toggle button to enable or disable **Discover new devices only** option. |
| Fallback Mechanism Support for Remote LAN Ports | Remote LAN ports have a mechanism to fall back from a Dot1x failure to MAC filtering, and from a MAC filtering failure to Dot1x. |
| Initiate EoX Scan | You can initiate an EoX scan from the Inventory window. |
| Inventory User Interface Enhancement | The **Inventory** window user interface is enhanced to provide you the improved filters and layout for better user experience. |
| Mobility Peer Configuration Enhancements | You can add wireless controllers that are not managed by Cisco DNA Center as mobility peers during mobility group configuration. |

| Feature | Description |
|---|---|
| Modeled Access Contract | If you want Cisco DNA Center to generate the valid commands for the underlying Security Group ACLs (SGACLs), enable the **Modeled Access Contract** option while creating an access contract. When this option is enabled, the access contract is based on a model that allows you to create and edit without the need to know the underlying command line syntax.<br>You can disable this option if you want to enter the SGACL command lines directly and store the access contract as text. |
| Port Usage Information | For device ports, you can check the last input received and last output transmitted timestamp in the device **Details** window. |
| Readiness Check for RMA | The RMA flow includes a readiness check to assess the device preparedness for replacement. |
| Resilient Ethernet Protocol (REP) Ring for Nonfabric Devices | You can configure REP Ring for nonfabric devices. |
| Return Material Authorization (RMA) Support | RMA support is extended for the following:<br>• Cisco Switch stacks (hardware stacking): Cisco DNA Center allows you to replace full stack switches.<br>• Supplicant-Based Extended Node (SBEN). |
| RF Profile: 6-GHz Radio Band Support | The 6-GHz radio band is supported on the following RF functionalities:<br>• Basic RF profile<br>• AI Radio Frequency Profile<br>• Configure AI RF Profile workflow |
| Software Image Compliance Support | You can check software image compliance for a Cisco switch stack. |
| Support for CCKM Configuration on SSID | You can enable CCKM as the authentication key management option in Cisco DNA Center. |
| Support for Configuration of Separate Accounting Servers for an SSID | You can configure separate accounting servers that are different from the authentication and authorization server for an SSID. |
| Support for Custom WLAN Profile Configuration | You can configure a custom WLAN profile while creating SSIDs for guest and enterprise wireless networks. |
| Support for External Guest Anchor Cisco Wireless Controller Configurations | You can add external anchor wireless controllers to an anchor group. |
| Support for Multiple Anchor Configurations | You can configure anchor groups with up to three anchor wireless controllers and set the priority for the anchors. You can add an anchor to an SSID and choose the configured anchor group for a network profile for wireless. |

| Feature | Description |
|---|---|
| Support for New APs | Cisco DNA Center supports the following APs:<br>• Cisco Catalyst 9164I Series Access Point<br>• Cisco Catalyst 9166I Series Access Point |
| Support for Other AP Models for Remote Teleworker Configuration | Cisco DNA Center supports the following AP models for the remote teleworker configuration, along with support for the existing Cisco Aironet 1815T (Teleworker) AP:<br>• Cisco Aironet 2800 Series Access Point<br>• Cisco Aironet 3800 Series Access Point<br>• Cisco Catalyst 9100 Series Access Point |
| Support for Scheduling SSID Broadcasting | You can create SSID scheduler to enable or disable WLAN based on time zone. |
| Support for Zero Wait Dynamic Frequency Selection (DFS) on APs | You can configure zero wait DFS as part of custom Radio Frequency (RF) profile configuration for a 5-GHz radio band. Zero wait DFS allows APs with a 5-GHz radio band to switch to a new channel without any waiting time.<br>Zero wait DFS is supported on the following APs with Cisco RF ASIC:<br>• Cisco Catalyst 9120AX Series Access Point<br>• Cisco Catalyst 9124AX Series Access Point<br>• Cisco Catalyst 9130 Wi-Fi 6 Access Point |
| Tri-Radio Configuration Support for APs | You can configure tri-radio parameters for APs that support the tri-radio configurations. |
| Troubleshoot Wireless APs Using the MRE Workflow | Using the MRE workflow, you can troubleshoot wireless AP issues. |
| View Security Advisories | • Cisco DNA Center security advisory support is extended for Cisco AireOS Wireless Controllers running with Cisco IOS software image version 8.5.120.0 or later.<br>• Cisco DNA Center security advisories supports the **FAILED DEVICES** area, which displays information about device scans that are scheduled for a later date and time. |

| Feature | Description |
|---|---|
| View the Remote Support Authorization Dashboard | The **Remote Support Authorization** dashboard supports the following features:<br>• **Manage SSH Credentials**: Allows you to establish the SSH connection to Cisco DNA Center.<br>• **Configure SSH Credential**: Allows a Cisco specialist to access your Cisco DNA Center setup for troubleshooting.<br>• **Access Permission Agreement** window support is extended for the following check boxes:<br>• Access to network devices<br>• Access to Cisco DNA Center setup |
| Wireless Coverage Optimizer | If your wireless coverage isn't meeting its SLA, you can run an optimizer tool. This tool takes your input of the maximum number of APs that you are prepared to move and add and computes a configuration where the wireless coverage is maximized. |
| Wireless Maps GUI Enhancements | Minor enhancements have been implemented to make the GUI more robust and consistent. For example, when you remove an element (a sensor, wall, and so on) from a wireless map, the element is only taken out of the map. It is not deleted from Cisco DNA Center. The terminology in the GUI was changed from **Delete** to **Remove** to more precisely reflect this action. |

## New and Changed Features in Cisco DNA Assurance

| Feature | Description |
|---|---|
| 6-GHz Radio Band Support | The 6-GHz radio band support is added to the **Enhanced RRM** dashboard. |
| Automatic Issue Resolution | With this release, the system automatically resolves issues for the following issue types:<br>• Switch Power Failure<br>• Switch Fan Failure |
| Cisco AI Network Analytics: Network Heatmap Enhancements | With this release, you can generate **Network Heatmaps** for **Switches**. You can filter the heatmap data based on the KPIs and on a specific **Switch Family** for direct comparisons.<br>The following temperature KPIs are supported for switches:<br>• **Temperature: All Sensors**<br>• **Temperature: Core**<br>• **Temperature: Hotspot**<br>• **Temperature: Inlet**<br>• **Temperature: Outlet** |
| Client 360 Enhancements for Fabric | With this release, client device details include fabric attributes such as **Security Group (Tag Value)** and **Bridge-Mode Virtual Machine**. |

| Feature | Description |
|---|---|
| Client Dashboard Enhancements | In the Assurance **Client** dashboard, you can exclude clients for specific Cisco Wireless Controllers using the **Excluded Clients** option in the **Client Devices** dashlet.<br>In the **Client 360** window, you can exclude the device for specific wireless controllers using the hyperlink for the **Excluded** status in the **Device Info** tab under **Client Details**. |
| Endpoint Events | The **Events** dashboard in Assurance provides a more contextual view of endpoint events. Instead of having to search for events triggered by endpoints that are connected to the devices involved in an event, Assurance provides these details for you. |
| MS Teams Application | You can monitor and troubleshoot the health of an **MS Teams** application. |
| New AP-Disconnect Issue | A new global AP disconnect issue is being introduced. AP disconnect issues that happen on the same switch are aggregated and raised as a single issue with a list of affected APs. The new aggregated AP disconnect issue will be logged both on the **Device 360** window and the Global dashboard.<br>The previous AP disconnect issue will still be logged. However, it will only appear on the **Device 360** window, not on the global **Issue** dashboard. |
| New BGP Down Issue | A new BGP Down issue is added to Router, Core, Distribution, and Access issues. The BGP Down issue is triggered when the BGP connectivity is down with its neighbor. You can modify the issue trigger condition to a maximum time duration of 10 minutes. |
| New Charts for Embedded Cisco Wireless Controllers | You can choose to display a number of new charts for embedded wireless controllers in the **Device 360** window. New charts include KPIs, such as Air Quality, Channel Utilization, Total Frame Errors, and so on. |
| New Global Client Counts for Embedded Cisco Wireless Controllers | The **Device 360** window for an embedded wireless controller displays the following new counts in the Client Count chart:<br>**Anchor entries**: Counts for clients who have recently roamed to another wireless controller. The client is no longer connected to the wireless controller that is reporting this data.<br>**Foreign entries**: Counts for clients who recently roamed to the wireless controller. The client connected to thewireless controller that is reporting this data, but may not be currently connected.<br>**Local entries**: Counts for clients that are currently connected to the wireless controller.<br>**Idle State entries**: Counts for clients who are in a temporary idle state. |
| PoE Power Usage Dashlet Enhancements | In the Assurance **PoE** dashboard, the power usage dashlet is enhanced with **Allocation** and **Consumption** views. The latest and trend tabs display the device power consumption and allocation data based on the selected view. |
| RF Charts for APs | You can choose to display RF charts for APs in the **Device 360** window. New charts include KPIs, such as Throughput, Client Count, Channel Utilization, Top SSIDs by Client/Packet Count, and so on. |
| RF Simulator | Using the AI RF Simulator, you can simulate changes to the current RF profile configurations and visualize the projected outcome against the enhanced RRM dashlets on the **Enhanced RRM** dashboard. |
| Site Analytics | You can view KPI statistics for sites that do not meet the configured performance thresholds. |

## New and Changed Features in Cisco DNA Center Platform

| Feature | Description |
|---|---|
| **New API Features** | |
| Cisco DNA Center System Platform API | The Cisco DNA Center platform supports the following **System Platform** APIs:<br>• GET <cluster-ip>/dna/intent/api/v1/dnac-release<br>Get the Cisco DNA Center release summary.<br>• GET <cluster-ip>/dna/intent/api/v1/nodes-config<br>Get the Cisco DNA Center nodes configuration summary.<br>• GET <cluster-ip>/dna/intent/api/v1/dnac-packages<br>Get the Cisco DNA Center packages summary.<br>To access the new **Platform** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**.<br>Expand the **Cisco DNA Center System** drop-down list and choose **Platform**. |
| Cisco DNA Center System User and Roles API | The Cisco DNA Center platform supports the following **System User and Roles** APIs:<br>• POST <cluster-ip>/dna/system/api/v1/user<br>Add a new user for Cisco DNA Center system.<br>• GET <cluster-ip>/dna/system/api/v1/roles<br>Get all roles for the Cisco DNA Center system.<br>• GET <cluster-ip>/dna/system/api/v1/user<br>Get all users for the Cisco DNA Center system.<br>• GET <cluster-ip>/dna/system/api/v1/role/permissions<br>Get permissions for a role from Cisco DNA Center system.<br>• GET <cluster-ip>/dna/system/api/v1/users/external-servers<br>Get external users authentication servers.<br>• PUT <cluster-ip>/dna/system/api/v1/user<br>Update a user for Cisco DNA Center system.<br>To access the new **User and Roles** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**.<br>Expand the **Cisco DNA Center System** drop-down list and choose **User and Roles**. |

| Feature | Description |
|---|---|
| Cisco SD-Access API | This Cisco DNA Center platform release supports new options in the **SDA** API to get, create, and delete the list of Cisco SD-Access devices:<br>• GET <cluster-ip>/dna/intent/api/v1/business/sda/transit-peer-network<br>Get Cisco SD-Access transit network detail.<br>• POST <cluster-ip>/dna/intent/api/v1/business/sda/transit-peer-network<br>Create Cisco SD-Access transit network.<br>• DELETE <cluster-ip>/dna/intent/api/v1/business/sda/transit-peer-network<br>Delete Cisco SD-Access transit network.<br>To access the new **SDA** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**.<br>Expand the **Connectivity** drop-down list and choose **SDA**. |
| Event Management API | The Cisco DNA Center platform supports the following **Event Management** APIs:<br>• GET <cluster-ip>/dna/intent/api/v1/event/webhook<br>Get webhook destination.<br>• GET <cluster-ip>/dna/intent/api/v1/event/syslog-config<br>Get syslog destination.<br>• GET <cluster-ip>/dna/intent/api/v1/event/email-config<br>Get Email destination.<br>• GET <cluster-ip>/dna/intent/api/v1/event/snmp-config<br>Get SNMP destination.<br>To access the new **Event Management** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**.<br>Expand the **Event Management** drop-down list. |
| Issues API | The Cisco DNA Center platform supports the following **Issues** APIs:<br>• POST <cluster-ip>/dna/intent/api/v1/execute-suggested-actions-commands<br>Executes suggested actions command.<br>To access the new **Issues** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**.<br>Expand the **Know Your Network** drop-down list and choose **Issues**. |

| Feature | Description |
|---|---|
| Network Settings API | The Cisco DNA Center platform supports the following **Network Settings** APIs:<br>• GET <cluster-ip>/dna/intent/api/v1/global-credential<br>Get device credential details.<br>• GET <cluster-ip>/dna/intent/api/v2/service-provider<br>Get service provider details.<br>• GET <cluster-ip>/dna/intent/api/v2/network<br>Get SNMP, NTP, Network AAA, Client and Endpoint AAA, and/or DNS center server settings.<br>• POST <cluster-ip>/dna/intent/api/v1/global-credential<br>Create device credentials.<br>• POST <cluster-ip>/dna/intent/api/v2/credential-to-site/${siteId}<br>Assign device credential to site.<br>• POST <cluster-ip>/dna/intent/api/v2/network/${siteId}<br>Create network settings for DHCP, Syslog, SNMP, NTP, Network AAA, Client and Endpoint AAA, and/or DNS center server settings.<br>• POST <cluster-ip>/dna/intent/api/v2/service-provider<br>Create service provider profile (QoS).<br>• PUT <cluster-ip>/dna/intent/api/v2/service-provider<br>Update service provider profile (QoS).<br>• PUT <cluster-ip>/dna/intent/api/v2/service-provider<br>Update network settings for DHCP, Syslog, SNMP, NTP, Network AAA, Client and Endpoint AAA, and/or DNS center server settings.<br>• PUT <cluster-ip>/dna/intent/api/v2/service-provider<br>Update device credentials.<br>• DELETE<cluster-ip>/dna/intent/api/v2/sp-profile/${spProfileName}<br>Delete service provider profile (QoS).<br>• DELETE<cluster-ip>/dna/intent/api/v1/global-credential/${id}<br>Delete device credential.<br>To access the new **Network Settings** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**.<br>Expand the **Site Management** drop-down list and choose **Network Settings**. |

| Feature | Description |
|---|---|
| Wireless APIs | This Cisco DNA Center platform release supports new options in the **Wireless** API for access point configuration and reboot access point.<br>The Cisco DNA Center platform supports the following **Wireless** API for access point configuration:<br>• GET<cluster-ip>/dna/intent/api/v1/wireless/access-point-configuration/task/${taskId}<br>Get Access Point Configuration task result.<br>• GET<cluster-ip>/dna/intent/api/v1/wireless/access-point-configuration<br>Get Access Point Configuration.<br>• POST<cluster-ip>/dna/intent/api/v1/wireless/access-point-configuration<br>Configure Access Points.<br>The Cisco DNA Center platform supports the following **Wireless** API for reboot access point:<br>• GET<cluster-ip>/dna/intent/api/v1/device-reboot/apreboot/status<br>Reboot Access Points.<br>• POST<cluster-ip>/dna/intent/api/v1/device-reboot/apreboot<br>To add the threat MAC address to the allowed list.<br>To access the new **Wireless** API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**.<br>Expand the **Connectivity** drop-down list and choose **Wireless**. |
| **New Reports** | |

| Feature | Description |
|---|---|
| AP RRM Events Report | |

| Feature | Description |
|---|---|
|  | This release supports a new **AP RRM Events** report that provides detailed information about AP RRM events over time grouped by access points.<br>• The **AP RRM Events** report is generated on the following criteria:<br>• Event Time<br>• AP Name<br>• AP MAC Address<br>• AP IP address<br>• Connected WLC Name<br>• Frequency<br>• Event Type<br>• Previous Channels<br>• Current Channels<br>• Previous Power<br>• Current Power<br>• Previous Channel Width<br>• Current Channel Width<br>• Reason<br>• Last Failure Reason<br>• DCA Reason<br>• Site<br>• Location<br>• Band<br>• Start Time<br>• End Time<br>• Timestamp<br>• Supported report file formats include **CSV**, **TDE**, and **JSON**.<br>• In the **Setup Report Scope** window, the **AP RRM Events** report provides port details based on the following scope:<br>• Location<br>• AP Name<br>• Event Type |

| Feature | Description |
|---|---|
| | - Band<br>- In the **Schedule Report** window, available time range options are **Last 3 Hours**, **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, and **Custom**.<br>**Note** Use the **Custom** option to customize the date and time interval, as well as the time zone (GMT) for the time range.<br>To access the **AP RRM Events** report, click the menu icon and choose **Report** > **Reports Templates** > **Access Point**.<br>In the **Report** window, choose **AP RRM Events**.<br>For more information about **AP RRM Events**, see **Run an Access Point Report** in the *Cisco DNA Center Platform User Guide*. |

| **Feature** | **Description** |
|---|---|
| Device CPU and Memory Utilization Report | This release supports a new **Device CPU and Memory Utilization** report that provides detailed information about top N CPU and memory utilization of managed devices.<br>- The **Device CPU and Memory Utilization** report is generated on the following criteria:<br>  - Device name<br>  - Device IP address<br>  - Device family<br>  - Device role<br>  - Device model<br>  - Count of minimum, maximum, and average CPU<br>  - Count of minimum, maximum, and average memory<br>- Supported report file formats include CSV.<br>- In the **Setup Report Scope** window, the **Device CPU and Memory Utilization** report provides top N CPU and memory utilization details based on the following:<br>  - Location<br>  - Device family<br>  - Device role<br>  - Sort by<br>  - Limit (N)<br>- In the **Schedule Report** window, available time range options are **Last 3 Hours**, **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, **Last 90 Days**, and **Custom**.<br>**Note** Use the **Custom** option to customize the date and time interval, as well as the time zone (GMT) for the time range.<br>To access the **Device CPU and Memory Utilization** report, click the menu icon and choose **Report** > **Reports Templates** > **Network Devices**.<br>In the **Report** window, choose **Device CPU and Memory Utilization**.<br>For more information about **Device CPU and Memory Utilization**, see the *Cisco DNA Center Platform User Guide*. |

| Feature | Description |
|---|---|
| Interface Utilization Report | This release supports a new **Interface Utilization** report that provides detailed information about interface utilization metrics.<br>• The **Interface Utilization** report is generated on the following criteria:<br>  • Device name<br>  • IP address<br>  • Device role<br>  • Site<br>  • Interface name<br>  • Count of minimum, maximum, and average Tx<br>  • Output error rate<br>  • Count of minimum, maximum, and average Rx<br>  • Input error rate<br>  • Input discard rate<br>  • Output discard rate<br>• Supported report file formats include CSV.<br>• In the **Setup Report Scope** window, the **Interface Utilization** report provides interface utilization details based on the following:<br>  • Location<br>  • Sort by<br>  • Sort order<br>  • Limit (N)<br>• In the **Schedule Report** window, available time range options are **Last 3 Hours**, **Last 6 Hours**, **Last 9 Hours**, **Last 12 Hours**, **Last 24 Hours**, and **Custom**.<br>**Note** Use the **Custom** option to customize the date and time interval, as well as the time zone (GMT) for the time range.<br>To access the **Interface Utilization** report, click the menu icon and choose **Report** > **Reports Templates** > **Network Devices**.<br>In the **Report** window, choose **Interface Utilization**.<br>For more information about **Interface Utilization**, see the *Cisco DNA Center Platform User Guide*. |

| Feature | Description |
|---|---|
| Port Reclaim View Report | This release supports a new **Port Reclaim View** report that provides detailed information about port level details based on last usage time.<br>• The **Port Reclaim View** report is generated on the following criteria:<br>  • Device Name<br>  • Device Family<br>  • Device Type<br>  • IP address<br>  • Port Name<br>  • Description<br>  • MAC Address<br>  • Admin Status<br>  • Operational Status<br>  • Last Input<br>  • Last Output<br>• Supported report file formats include **CSV**, **TDE**, and **JSON**.<br>• In the **Setup Report Scope** window, the **Port Reclaim View** report provides port details based on the following scope:<br>  • Device Family<br>  • Device Name<br>• In the **Schedule Report** window, the available schedule options are **Run Now**, **Run Later (One-Time)**, and **Run Recurring**.<br>**Note** Use the **Run Later (One-Time)** option to customize the date and time interval, as well as the time zone (GMT) for the time range.<br>Use the **Run Recurring** option to schedule the days and time along with the time zone (GMT).<br>To access the **Port Reclaim View** report, click the menu icon and choose **Report** > **Reports Templates** > **Inventory**.<br>In the **Report** window, choose **Port Reclaim View**.<br>For more information about **Port Reclaim View**, see **Run an Inventory Report** in the *Cisco DNA Center Platform User Guide*. |
| **New Reports Features** | |

| Feature | Description |
|---|---|
| New Reports GUI Features | Cisco DNA Center platform support is extended for the following enhancements in the **Client Detail** report for device classification insights:<br>• In the **Select File Type** window, the **Client Detail** report supports the following device analytic fields for Cisco Catalyst 9800 Series Wireless Controllers :<br>• Device Form<br>• Device Vendor<br>• OS<br>• Firmware Version<br>**Note** The **Client Detail** report displays the device form only if the device analytics are supported by Cisco Catalyst 9800 Series Wireless Controller IOS-XE release version 17.6 or later. Otherwise, the **Device Form** field displays no data for the respective device.<br>For more information, see **Run a Client Report** in the *Cisco DNA Center Platform User Guide*. |

## New and Changed Features in Cisco DNA Automation

| Feature | Description |
|---|---|
| Configure an MS Teams Integration | You can now configure integration with Microsoft Teams. After the integration is enabled, Cisco DNA Center provides call quality metrics information for Application 360 and Client 360 dashboards. |
| Device Certificate | The **Device Certificate** window now contains a **Device Name** column, which lets you filter certificates by device name. |
| Restricted Shell | For added security, access to the root shell is disabled starting in this release of Cisco DNA Center. With restricted shell, users can't access the underlying operating system and file system, which reduces operational risk.<br>Restricted shell is enabled for security purposes. However, if you want to access the root shell temporarily, you must contact the Cisco TAC for assistance. |

## New and Changed Features in Cisco Software-Defined Access

| Feature | Description |
|---|---|
| Border Node Affinity-ID | Cisco DNA Center allows you to configure the border node affinity-ID attribute. Affinity-ID determines the relative geographical location of a border node. You can now choose the preferred border node to route traffic when fabric sites don't have network access using the affinity-ID attribute. |

| Feature | Description |
|---|---|
| Cisco SD-Access Zero-Trust Workplace | Cisco SD-Access provides a zero-trust security solution for your workplace. The Cisco SD-Access zero-trust security solution provides secure access to all users and devices from all locations across your network. The solution lets you automate network access policies using endpoint visibility, trust monitoring, and network segmentation.<br>The Cisco SD-Access **Zero-Trust Overview** dashboard provides an overview of your zero-trust workplace journey. |
| Custom Border Layer 3 Handoff IP Addressing | Earlier releases of Cisco DNA Center automated the IP address allocation for the virtual networks in a Layer 3 Handoff deployment. This release of Cisco DNA Center gives you the option to manually allocate IP Address and subnet mask for each Layer 3 Handoff-enabled virtual network. You can choose to either automate the IP routing between the border node and the peer or manually configure the IP addresses. You cannot do both. |
| Full Flexible NetFlow for Extended Node and Policy Extended Node | You can now enable Application Telemetry on an extended node and policy extended node that is already provisioned. When you enable telemetry, the flow monitor is enabled on all the interfaces of the extended node and policy extended node.<br>For details on enabling telemetry on a device, see the "Configure Telemetry" chapter in the *Cisco DNA Center User Guide*.<br>The following are the extended node or policy extended node devices that support Application Telemetry:<br>• Cisco Industrial Ethernet (IE) 4000 and 5000 Series switches, which run Cisco IOS 15.2(7)E0 or later releases.<br>• Cisco IE 4010 Series switch, which runs Cisco IOS 15.2(7)E2 or later releases.<br>• Cisco Catalyst IE 3300 Series switch, which runs Cisco IOS XE 17.3.1 or later releases.<br>• Cisco Catalyst IE 3400 and IE 3400H Series switches, both configured as extended node or policy extended nodes, and operating Cisco IOS XE 17.3.1 or later releases.<br>• Cisco Catalyst IE 9300 Series switch, which runs Cisco IOS XE 17.8.1 or later releases.<br>• Cisco ESS 3300 Series switch, which runs Cisco IOS XE 17.3.1 or later releases. |
| LAN Automation Task View and Status | This release of Cisco DNA Center enhances the overall LAN Automation experience by providing detailed Status and Log views for each device, including the primary and the peer device.<br>**LAN Automation Status** window provides options to view the device logs and configurations. You can also check whether the configuration was a success or a failure. In the case of a failed configuration, Cisco DNA Center displays actionable error messages to aid further troubleshooting. |
| Layer 3 Virtual Networks, Layer 2 Virtual Networks, Anycast Gateways Workflow Enhancements | The Layer 3 virtual networks, Layer 2 virtual networks, and anycast gateways workflows have been enhanced.<br>You can select and edit up to five Layer 3 virtual networks, Layer 2 virtual networks, and anycast gateways using a single workflow. |

| Feature | Description |
|---|---|
| Remote LAN Support for Fabric Sites | Cisco DNA Center supports remote LAN (RLAN) configuration for fabric sites on Cisco Catalyst 9800 Series Wireless Controllers. You can configure RLAN ports on APs for fabric sites. Cisco Wireless Controller authenticates the wired clients and allows them to connect to the network. You can configure RLAN for fabric sites on wireless controllers that run Cisco IOS XE Release 17.7 or later. |
| Virtual Network Policy to Support Extranet in a Single-Site Fabric and Multisite Fabric with SD-Access Transit | Create a virtual network (VN) policy to allow route leaks between Layer 3 VNs, without using a peer device. Use a VN policy to provide the endpoints (hosts or users) with access to shared services like DHCP, DNS, Internet access, and so on, through Cisco DNA Center automation. The shared services connect to a Provider VN. The endpoints that use the shared services reside in a Subscriber VN. A VN policy establishes communication between the Provider VN and a Subscriber VN, without allowing communication between the Subscriber VNs in the fabric.<br>This release of Cisco SD-Access supports VN Policy only for unicast communication.<br>You can create a VN policy, edit a VN policy, and delete a VN policy in these deployments:<br>• Single-site fabric with IP Transit<br>• Multisite fabric with SD-Access Transit<br>**Note** • VN policy or Extranet is not supported on router platforms.<br>• Multicast leveraging Extranet functionality is not supported. |

## New and Changed Features in Interactive Help

| Feature | Description |
|---|---|
| New Resources | Added the following resources:<br>• Community<br>• Guided Setup |
| New Walkthroughs | Added the following walkthroughs:<br>• Add an Inclusion Region to a Floor<br>• Add Coverage Areas to a Floor<br>• Add GPS Markers to a Floor<br>• Add Markers to a Floor<br>• Add Openings to a Floor<br>• Configure Border Node IP-Based Custom Handoff<br>• Modify an Authentication Template<br>• Run the Wireless Coverage Optimizer |

## 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 2.3.4, we recommend that you use Chrome, not Firefox.

## Supported Firmware

Cisco Integrated Management Controller (Cisco IMC) versions are independent from Cisco DNA Center releases. This release of Cisco DNA Center has been validated only against the following firmware:

- Cisco IMC Version 3.0(3f) and 4.1(2g) for appliance model DN1-HW-APL
- Cisco IMC Version 4.1(3d) for appliance model DN2-HW-APL
- Cisco IMC Version 4.1(3d) for appliance model DN2-HW-APL-L
- Cisco IMC Version 4.1(3d) for appliance model DN2-HW-APL-XL

### Update the Cisco IMC Firmware

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

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

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

## Cisco DNA Center Scale

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

## IP Address and FQDN Firewall Requirements

To determine the IP addresses and fully qualified domain names (FQDNs) that must be made accessible to Cisco DNA Center through an existing network firewall, see "Required Internet URLs and Fully Qualified Domain Names" in the "Plan the Deployment" chapter of the *Cisco DNA Center Installation Guide*.

## About Telemetry Collection

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

## Supported Hardware Appliances

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

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

## Installing Cisco DNA Center

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

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

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

## Support for Cisco Connected Mobile Experiences

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

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

## Plug and Play Considerations

### General Feature Support

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

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

### Secure Unique Device Identifier Support

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

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

  - Cisco Catalyst 9300 Series with software release Cisco IOS XE 16.6.1 or later
  - Cisco Catalyst 9400 Series with software release Cisco IOS XE 16.6.1 or later
  - Cisco Catalyst 9500 Series with software release Cisco IOS XE 16.6.1 or later
  - Cisco Catalyst IE3300 Series with software release Cisco IOS XE 16.10.1e or later
  - Cisco Catalyst IE3400 Series with software release Cisco IOS XE 16.11.1a or later
  - Cisco Catalyst IE9300 Series with software release Cisco IOS XE 17.8.1 or later

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

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

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

### Management Interface VRF Support

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

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

### 4G Interface Support

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

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

# Configure Server Identity

To ensure successful Cisco DNA Center discovery by Cisco devices, the server SSL certificate offered by Cisco DNA Center during the SSL handshake must contain an appropriate Subject Alternate Name (SAN) value so that the Cisco Plug and Play IOS Agent can verify the server identity. This may require the administrator to upload a new server SSL certificate, which has the appropriate SAN values, to Cisco DNA Center. You can generate a new certificate signing request (CSR) from **System** > **Settings** > **Trust & Privacy** > **System Certificates**. For more information, see "Update the Cisco DNA Center Server Certificate" in the Cisco DNA Center Administrator Guide.

The SAN requirement applies to devices running the following Cisco IOS releases:

- Cisco IOS Release 15.2(6)E2 and later
- Cisco IOS Release 15.6(3)M4 and later
- Cisco IOS Release 15.7(3)M2 and later
- Cisco IOS XE Denali 16.3.6 and later
- Cisco IOS XE Everest 16.5.3 and later
- Cisco IOS Everest 16.6.3 and later
- All Cisco IOS releases from 16.7.1 and later

The value of the SAN field in the Cisco DNA Center certificate must be set according to the type of discovery being used by devices, as follows:

- For DHCP option-43 or option-17 discovery using an explicit IPv4 or IPv6 address, set the SAN field to the specific IPv4 or IPv6 address of Cisco DNA Center.
- For DHCP option-43 or option-17 discovery using a hostname, set the SAN field to the Cisco DNA Center hostname.
- For DNS discovery, set the SAN field to the Plug and Play hostname, in the format pnpserver.domain.
- For Cisco Plug and Play Connect cloud portal discovery, set the SAN field to the Cisco DNA Center IP address if the IP address is used in the Plug and Play Connect profile. If the profile uses the Cisco DNA Center hostname, the SAN field must be set to the FQDN of the controller.

If the Cisco DNA Center IP address that is used in the Plug and Play profile is a public IP address that is assigned by a Network Address Translation (NAT) router, this public IP address must be included in the SAN field of the server certificate.

If an HTTP proxy server is used between the devices and Cisco DNA Center, ensure that the proxy certificate has the same SAN fields with the appropriate IP address or hostname.

We recommend that you include multiple SAN values in the certificate, if discovery methods vary. For example, you can include both the Cisco DNA Center FQDN and IP address (or NAT IP address) in the SAN field. If you include both, set the FQDN as the first SAN value, followed by the IP address.

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

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

# Bugs

## Open Bugs

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

| Bug Identifier | Headline |
|---|---|
| CSCwa19027 | Cisco DNA Center pushes the command "automate-tester username dummy ignore-acct-port probe-on" as part of its standard Cisco SD-Access configuration. Cisco DNA Center pushes the "automate-tester" configuration so that the device sends periodic RADIUS requests to the RADIUS server. The server is marked as Up if the device receives a response; the server is marked as Down if the device doesn't receive a response.<br>It doesn't matter whether the user exists in Cisco ISE, because the device merely looks for a response from the RADIUS server, regardless of whether authentication succeeds or fails.<br>If the corresponding Cisco ISE authentication policy uses the "Drop" action instead of the default "Access-Reject" action when the user does not exist, the AAA server might get marked as Dead when Cisco ISE drops the packet (because the dummy user does not exist on Cisco ISE). This in turn could affect CTS operation, and the following log is generated every minute:<br>`%CTS-3-AAA_NO_RADIUS_SERVER: No RADIUS servers available for CTS AAA request for CTS env-data SM` |
| CSCwb28054 | Provisioning a wireless controller with version 17.7 fails with Cisco DNA Center 2.3.4 when using custom RF profiles (includes custom base RF profiles and all AI RF profiles). Provisioning RPC fails for the client-aware-fra parameter configuration. |
| CSCwb85510 | For the SYSTEM-SOFTWARE-UPGRADE event, if you configure the same IP address with multiple DNS names, or if you don't configure the hostname on Cisco DNA Center, the System Upgrade alert uses DNS instead of the source config.<br>To work around this problem, configure only one hostname for your Cisco DNA Center appliance. Also map this hostname with its corresponding DNS server entry. This ensures that the appliance is properly referenced in the **Instance** field of any system event notifications that Cisco DNA Center generates. |
| CSCwc35018 | When client summary reports are executed using Business APIs, Cisco DNA Center platform displays the following error:<br>`BAPI Execution Failed. Response Code = 500, Response Content=null` |
| CSCwc35114 | When you run a report, Cisco DNA Center generates a blank report with the following error:<br>`Duplicate entries found for bapiName Client Data Report` |
| CSCwc37682 | Assurance data does not reflect correctly in the GUI after disaster recovery.<br>The data cob logs reflect broker agent connectivity exceptions from collector SDK, such as "Retrying after 5000 ms," which eventually results in a stack overflow exception. |

| Bug Identifier | Headline |
|---|---|
| CSCwc39022 | The "AP(s) disconnected from WLC on Switch" alarm shows zero APs after adding the switch in Cisco DNA Center. For the AP-Disconnect issue, the Suggested Action is empty.<br>AP-Disconnect issues are grouped by switch and are enabled for automatic resolution. If a switch is added to Cisco DNA Center after the AP-Disconnect issue is triggered, you must resolve the issue manually. Any further issues will support automatic resolution. |
| CSCwc42371 | Sensor Outlook Web Access tests fail with a "Login Fail" error.<br>The sensor Outlook Web Access test fails because most email servers don't allow third-party applications to have direct access with a regular password. For example, Gmail and Yahoo have restrictions on how third-party applications can access the email server. Google, for example, does not support the use of third-party applications or devices that ask you to sign in to your Google account using only your username and password. |
| CSCwc62887 | After you upgrade from Cisco DNA Center 2.2.3 to 2.3.4, the GUI shows the lowest release version as available for download immediately after the system upgrade. This is confusing. |
| CSCwc70685 | The disaster recovery failover workflow takes longer than one hour to complete. |
| CSCwc74941 | If you use Mozilla Firefox to upload a certificate (under **System** > **Settings** > **PKI Certificates**), when you click **Choose a file**, files with the extensions .cer and .pem are grayed out, even though those file formats are supported. Or, you receive an invalid "File type not supported" error.<br>To work around this problem, use Google Chrome instead of Mozilla Firefox to upload the PKI certificate. Alternatively, drag and drop the file into the upload box instead of browsing to the file. |
| CSCwc85038 | The system update fails at post hook install phase, and the release upgrade retries after the failure. The release upgrade directly proceeds to application packages before installing the post system hooks completely. |
| CSCwd17228 | Unbind IP pool with SSID is not provisioned down to device. |
| CSCwd74259 | Unable to load the large fabric site. |

## Resolved Bugs

### Cisco DNA Center 2.3.4.3

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.4.3.

| Bug Identifier | Headline |
|---|---|
| CSCwb57629 | When adding a new device through Plug and Play, the process completes, and the State and Onboarding Progress show **Provisioned**. However, the following error is displayed, and the device is not in the inventory:<br>`NCOB02064: Device not added to Inventory - No CLI credentials provided`<br>To work around this problem, delete and re-enter all the global credentials (not just CLI, but also HTTP, SNMP, and so on). Then, retry the Plug and Play process. |
| CSCwc23153 | Provisioning fails on the Cisco Catalyst 9000 Series switch because Cisco DNA Center tries to provision the IOX interface TenGigabitEthernet4/0/48. |

| Bug Identifier | Headline |
|---|---|
| CSCwc40992 | The fabric instance in the Provision Fabric window can't be accessed. |
| CSCwc48881 | The tri-radio mode gets globally enabled automatically on a wireless controller that has supported APs. |
| CSCwc49833 | Disaster recovery: The file service does not delete the purged files from the mongo database. |
| CSCwc53593 | Static port assignment from the Fabric Host Onboarding window fails with the following error:<br>`Provisioning failed due to invalid request. Connected Device Type for an interface cannot be changed.`<br>`To change the type, first clear the interface and then try again.` |
| CSCwc53951 | Some floors in Cisco DNA Center may not display a wireless heatmap, citing a Matlab connection timeout. |
| CSCwc56341 | The Cisco DNA Center reserve IP pool API does not recognize a second global IP pool. |
| CSCwc59647 | Stale entries for RD remain in the database while readding the VN to the fabric. |
| CSCwc60578 | Maps migration doesn't complete in the Prime Data Migration Tool (PDMT). A Cisco DNA Center prevalidation status REST API error occurs. |
| CSCwc61000 | The disaster recovery rejoin operation fails when the witness VM tries to reconnect to the disaster recovery configuration after a software upgrade. |
| CSCwc62677 | Device deletion from Cisco DNA Center's inventory fails, citing a foreign key constraint violation. |
| CSCwc66513 | Cisco DNA Center may set a Layer 3 VNID to zero for infrastructure segments when a wireless device is provisioned, which results in APs disassociating from the fabric network. |
| CSCwc69467 | Cisco DNA Center 2.3.3.3 assigns different site tags to APs in the same site. |
| CSCwc73983 | The wireless fabric control-plane IP address gets removed from the wireless controller. |
| CSCwc78951 | Cisco DNA Center's inventory service may become unstable. When this problem occurs, the Inventory window loads slowly, and device synchronizations take a long time to run. |
| CSCwc83710 | The Cisco DNA Center GUI displays an error when accessing network profile advanced settings and creating custom tags. |
| CSCwc86109 | The filesystem shows 100% utilization for fusion. The web GUI is intermittent and services don't work correctly. |
| CSCwc94852 | Cannot provision or delete a wireless controller due to the following error:<br>`NCSP11108 CFS persistence failed.` |

| Bug Identifier | Headline |
|---|---|
| CSCwc98658 | Cisco DNA Center may fail to provision a wireless LAN controller if a compliance operation starts around the same time as the provisioning. This appears to cause the SPF service to exhaust its memory allocation. |
| CSCwd02734 | Adding an IP pool to a fabric zone fails with the following error:<br>`NCSP11108: Error occurred while processing the request.` |
| CSCwd07407 | Provisioning or updating telemetry settings on Catalyst 2960-Plus Series version 15.2(7)E6 using Cisco DNA Center generates an error, even though NetFlow is not supported. |

### Cisco DNA Center 2.3.4.0

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.4.0.

| Bug Identifier | Headline |
|---|---|
| CSCwa21212 | Unable to start LAN automation. The following error is displayed:<br>`NCND00050: An internal error occurred while processing the request.` |
| CSCwa29973 | CTS credentials of the device aren't in sync with the Cisco DNA Center NAD entry. |
| CSCwa68838 | The spf-service-manager-service doesn't start after upgrading to Cisco DNA Center 2.1.2.7. |
| CSCwa77904 | Cisco Wireless Controller provisioning fails with the internal error NCSP10246 while attempting to transform the object for further processing. |
| CSCwa90595 | Cisco Wireless Controller provisioning fails due to an invalid $apMac configuration element. |
| CSCwa97774 | Cisco Wireless Controller provisioning fails because the snapshot doesn't exist for the namespace. |
| CSCwb02969 | After provisioning a Cisco Catalyst 9500 Switch stack and pushing the fabric configuration, the status of the switch changes to "Managed Internal error." |
| CSCwb28540 | A tag mismatch occurs between the primary and secondary controllers. |
| CSCwb29770 | In a fabric setup, Cisco 9840 Wireless Controller provisioning fails due to a Dot11 configuration discrepancy. |
| CSCwb40106 | Software image management (SWIM) doesn't show the activation task, even after successful image transfer. |
| CSCwb42071 | Switch provisioning fails because a duplicate key value violates the unique constraint "manageddcs_unique_key." |
| CSCwb47791 | Image repository: The Assign Device Family GUI needs specific PIDs for Cisco Catalyst 9300X models (mdfdata.xml). |
| CSCwb57463 | Provisioning a single RF profile causes all the APs in the site to unjoin and rejoin. |
| CSCwb70550 | After removing duplicate Meraki devices from the Inventory, the Inventory shows the wrong count of unassigned devices. |

| Bug Identifier | Headline |
|---|---|
| CSCwb72776 | Cisco DNA Center devices fail to sync with an "icppolicymapaction_bk constraint" error. |
| CSCwb73232 | The hostname of devices is not shown in the discovery results, even though the SNMP status is shown as Success. |
| CSCwb88023 | Provisioning fails on an invalid LAN port ID: AP3800, port 128. |
| CSCwb96201 | The Application Visibility window loads partially and has two different devices with the same IP address. |
| CSCwc10284 | Cisco DNA Center deletes some of the switch running image packages during SWIM distribution. |
| CSCwc11245 | The Cisco DNA Center inventory service fails after attempting to add more than 500 devices simultaneously through the API. |
| CSCwc13096 | Cannot provision an AP, because postgres cannot find a large object. |
| CSCwc18059 | Provisioning a Cisco Wireless Controller fails with a stack overflow error when there are many sites and APs. |
| CSCwc20229 | Applications are unable to receive messages from RabbitMQ. When you log in to the RabbitMQ management GUI and open the respective exchange, queue bindings are shown intermittently. Otherwise, the display is empty. |
| CSCwc28641 | Cisco Catalyst 9300 stacked switch resync shows "Internal Error" due to an arpDetails_feature failure. |

## Limitations and Restrictions

### Cloud Connectivity Through SSL Intercept Guidelines

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

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

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

### Backup and Restore Guidelines

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

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

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

### Cisco ISE Integration Guidelines

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

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

### Device Onboarding Guidelines

For IE-3200-8P2S-E/A, IE-3200-8T2S-E/A, IE-3300-8P2S-E/A, and IE-3300-8T2S-E/A devices with Cisco IOS XE 17.8.1 or later, we recommend that you boot the devices in install mode before onboarding them.

If you upgrade an onboarded IE3200 or IE3300 device to Cisco IOS XE 17.8.1 or later, ensure that the device is in install boot mode before upgrading.

### Upgrade Limitation

- If you are upgrading to Cisco DNA Center and all the following conditions apply, the upgrade never starts:
  - Cisco ISE is already configured in Cisco DNA Center.
  - The version of Cisco ISE is not 2.6 patch 1, 2.4 patch 7, or later.
  - Cisco DNA Center contains an existing fabric site.
  - The number of DNS servers must not exceed three.

  Although the GUI does not indicate that the upgrade failed to start, the logs contain messages that are related to the upgrade failure.

  To work around this problem, upgrade Cisco ISE to 2.6 patch 1, 2.4 patch 7, or later, and retry the Cisco DNA Center upgrade.
- In-Service Software Upgrade (ISSU) is not supported in Cisco SD-Access deployments.

### License Limitations

- The Cisco DNA Center License Manager supports Smart Licensing only for wireless controller models that run Cisco IOS XE. The License Manager does not support Smart License registration of the Cisco 5500 Series AireOS Wireless Controller when the connection mode is smart proxy.
- The Cisco DNA Center License Manager does not support the following operations under **Actions** > **Manage License Reservation** for Cisco IOS 17.3.2 and later:
  - Enable License Reservation
  - Update License Reservation
  - Cancel/Return License Reservation
  - Factory License Reservation

### Fabric Limitations

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

  To work around this issue, release and reserve the IP address pool at the same level (area or building) as the fabric site, or reconfigure the fabric site at the same level as the reserved IP address pool.
- Cisco DNA Center does not support multicast across multiple fabric sites that are connected by an SD-Access transit network.
- The IP-Directed Broadcast feature is supported over SD-Access transit only for unknown unicast traffic destined to silent hosts (that is, hosts present on the remote SD-Access site but not registered to the control plane). IP-Directed Broadcast over SD-Access transit does not support broadcast packets.

### Existing Feature-Related Limitations

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

### Wireless Policy Limitation

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

### AP Limitations

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

  After the provisioning failure, the AP rejoins the wireless controller. You can reprovision the AP for a successful provisioning.
- The Cisco Catalyst 9130AXE AP with antenna C-ANT9104 does not support the Disable option for Dual Radio mode.
- The Cisco Catalyst 9124AXE AP does not support the Auto option for Dual Radio mode.
- 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 the clients connected to a switch through an access point in bridge mode. The trunk port is used to exchange all the VLAN information. When you enable IP device tracking on the trunk port, clients connected on the neighbor switch are also shown. Cisco DNA Center does not collect client data if the connected interface is a trunk port and the neighbor is a switch. As a best practice, disable the IP device tracking on the trunk port. Rogue-on-wire is not detected if IP device tracking is enabled on the trunk port. See Disabling IP Device Tracking for more information.

### Encryption Limitation with SNMPv3

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

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

### IPv6 Limitations

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

- Access Control Application, Group-Based Policy Analytics, SD-Access, and Cisco AI Endpoint Analytics packages are disabled and cannot be downloaded or installed.
- Communication through Cisco ISE pxGrid is disabled because Cisco ISE pxGrid does not support IPv6.
- LAN automation is not supported.
- Wireless controller provisioning is not supported.

### Cisco Plug and Play Limitations

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

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

### Cisco Group-Based Policy Analytics Limitations

- Cisco Group-Based Policy Analytics supports up to five concurrent requests based on realistic customer data. While it is desirable for GUI operations to respond within 5 seconds or less, for extreme cases based on realistic data, it can take up to 20 seconds. There is no mechanism to prevent more than five simultaneous requests at a time, but if it does happen, it might cause some GUI operations to fail. Operations that take longer than 1 minute time out.

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

  For example, assume that the Cisco DNA Center server is located in California PDT (UTC-7) where data aggregations occur at hourly offsets (8:00 a.m., 9:00 a.m., 10:00 a.m., and so on). When a client located in India IST (UTC+5.30) wants to see the data between 10:00 to 11:00 p.m. IST, which corresponds to the time range 9:30 to 10:30 a.m. PDT in California, no aggregations are seen.

- Group changes that occur within an hour are not captured. When an endpoint changes from one security group to another, Cisco Group-Based Policy Analytics is unaware of this change until the next hour.

- You cannot sort the Security Group and Stealthwatch Host Group columns in the **Search Results** window.

- You might see discrepancies in the information related to Network Access Device (including location) between Assurance and Cisco Group-Based Policy Analytics.

### Application Telemetry Limitation

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

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

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

The following syntax is invalid:

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

### IP Address Manager Limitations and Workaround

- Infoblox limitations:
  - Infoblox does not expose a name attribute; therefore, the comment field in Infoblox is populated by the IP pool name during a sync.
  - For a pool import, the first 50 characters of the comment field are used. If there are spaces in the comments, they are replaced by underscores.
  - If an IP pool name is updated for an imported pool, the comments are overwritten and the new name is reflected.

- BlueCat: There are no limitations identified with BlueCat integration at this time.
- You might see the following error when editing an existing IPAM integration or when adding a new IPAM manager.

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

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

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

- Cisco DNA Center supports integration with an external IPAM server that has trusted certificates. In the Cisco DNA Center GUI, under **System** > **Settings** > **External Services** > **IP Address Manager**, you might see the following message:

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

  To correct this error for a self-signed certificate:

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

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

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

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

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

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

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

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

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

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

  To correct this, do the following:

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

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

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

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

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

To correct this, do the following:

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

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

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

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

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

### Reports Limitation

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

### Custom Application Limitation

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

## Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

### Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

### Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

## Related Documentation

We recommend that you read the following documents relating to Cisco DNA Center.

| For This Type of Information... | See This Document... |
|---|---|
| Release information, including new features, limitations, and open and resolved bugs. | *Cisco DNA Center Release Notes* |
| Installation and configuration of Cisco DNA Center, including postinstallation tasks. | *Cisco DNA Center Installation Guide* |
| Upgrade information for your current release of Cisco DNA Center. | *Cisco DNA Center Upgrade Guide* |
| Use of the Cisco DNA Center GUI and its applications. | *Cisco DNA Center User Guide* |
| Configuration of user accounts, security certificates, authentication and password policies, and backup and restore. | *Cisco DNA Center Administrator Guide* |
| Security features, hardening, and best practices to ensure a secure deployment. | *Cisco DNA Center Security Best Practices Guide* |
| Supported devices, such as routers, switches, wireless APs, and software releases. | *Cisco DNA Center Compatibility Matrix* |
| Hardware and software support for Cisco SD-Access. | *Cisco SD-Access Compatibility Matrix* |
| Technical references and validated solutions. | *Cisco-Validated Solution Profiles* |
| Use of the Assurance GUI. | *Cisco DNA Assurance User Guide* |
| Use of the Cisco DNA Center platform GUI and its applications. | *Cisco DNA Center Platform User Guide* |
| Cisco DNA Center ITSM integration and support. | *Cisco DNA Center ITSM Integration Guide* |
| Use of the Cisco Wide Area Bonjour Application GUI. | *Cisco Wide Area Bonjour Application User Guide* |
| Use of the Stealthwatch Security Analytics Service on Cisco DNA Center. | *Cisco Stealthwatch Analytics Service User Guide* |
| Use of Rogue and aWIPS functionality to monitor threats in Cisco DNA Center. | *Cisco DNA Center Rogue Management and aWIPS Application Quick Start Guide* |