# Release Notes for Cisco DNA Center, Release 1.3.3.x

**First Published:** 2020-01-17

**Last Modified:** 2021-01-14

## Release Notes for Cisco DNA Center, Release 1.3.3.x

This document describes the features, limitations, and bugs for Cisco DNA Center, Release 1.3.3.x. Cisco DNA Center gets smarter, using machine reasoning to automatically check for inconsistencies in switch configuration and in security patches. This release also lets your Samsung smartphones tell you how to improve Wi-Fi connectivity.

### Change History

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

***Table 1: Document Change History***

| Date | Change | Location |
|---|---|---|
| 2021-01-14 | Updated the Network Controller Platform package for 1.3.3.9. | New and Changed Information, on page 4 |
| | Added a resolved bug in Cisco DNA Center 1.3.3.9: CSCvw76745. This bug is resolved in 1.3.3.9 only when you update the Network Controller Package version to the version listed in New and Changed Information, on page 4. | Resolved Bugs, on page 23 |
| 2020-12-22 | Added a fabric limitation: multicast is not supported across fabric sites that are connected with SDA transit network. | Limitations and Restrictions, on page 34 |
| 2020-12-01 | Added the list of packages in Cisco DNA Center 1.3.3.9. | New and Changed Information, on page 4 |
| | Added the Resolved Bugs table for 1.3.3.9. | Resolved Bugs, on page 23 |
| 2020-11-05 | Added the link to download Cisco DNA Center software: https://software.cisco.com/download/home/286316341/type. | New and Changed Information, on page 4 |
| 2020-10-20 | Added the list of packages in Cisco DNA Center 1.3.3.8. | New and Changed Information, on page 4 |
| | Added the Resolved Bugs table for 1.3.3.8. | Resolved Bugs, on page 23 |
| 2020-08-26 | Added a resolved bug in Cisco DNA Center 1.3.3.0: CSCvr72551. | Resolved Bugs, on page 23 |

| Date | Change | Location |
|---|---|---|
| 2020-08-20 | Added a resolved bug in Cisco DNA Center 1.3.3.7: CSCvu23957. | Resolved Bugs, on page 23 |
| 2020-08-10 | Added the list of packages in Cisco DNA Center 1.3.3.7. | New and Changed Information, on page 4 |
| | Added the Resolved Bugs table for 1.3.3.7. | Resolved Bugs, on page 23 |
| | Added an open bug: CSCvu12292. | Open Bugs—Non-High Availability, on page 20 |
| 2020-08-05 | Added CSCvr54376 to the 1.3.3.0 Resolved Bugs table. | Resolved Bugs, on page 23 |
| 2020-07-16 | Added the list of packages in Cisco DNA Center 1.3.3.6. | New and Changed Information, on page 4 |
| | Added the Resolved Bugs table for 1.3.3.6. | Resolved Bugs, on page 23 |
| | Added open bugs: CSCvu29282, CSCvu42019, and CSCvu77846. | Open Bugs—Non-High Availability, on page 20<br>Open Bugs—High Availability, on page 22 |
| 2020-06-15 | Added an open bug: CSCvq86168. | Open Bugs—Non-High Availability, on page 20 |
| | Noted that application hosting is not supported on stacked switches. | Limitations and Restrictions, on page 34 |
| 2020-06-08 | Added an open bug: CSCvu48710. | Open Bugs—Non-High Availability, on page 20 |
| 2020-06-03 | Added the list of packages in Cisco DNA Center 1.3.3.5. | New and Changed Information, on page 4 |
| | Added the Resolved Bugs table for 1.3.3.5. | Resolved Bugs, on page 23 |
| | Added open bugs: CSCvu28044, CSCvu15218. | Open Bugs—Non-High Availability, on page 20<br>Open Bugs—High Availability, on page 22 |
| 2020-04-20 | Added the list of packages in Cisco DNA Center 1.3.3.4. | New and Changed Information, on page 4 |
| | Added the Resolved Bugs table for 1.3.3.4. | Resolved Bugs, on page 23 |
| | Added open bugs: CSCvs72105, CSCvt85320, CSCvt87610, CSCvt89349. | Open Bugs—Non-High Availability, on page 20<br>Open Bugs—High Availability, on page 22 |

| Date | Change | Location |
|---|---|---|
| 2020-03-30 | Updated the following package versions:<br>• Automation - Base<br>• Cisco DNA Center UI<br>• Cisco SD-Access<br>• Machine Reasoning<br>• Network Controller Platform | New and Changed Information, on page 4 |
| | When you update the Cisco DNA Center UI package version to 1.4.1.105, the **About** dialog box in the GUI shows the Cisco DNA Center version as **1.3.3.3(1)**. | — |
| | Added resolved bugs in Cisco DNA Center 1.3.3.3: CSCvt23943, CSCvt65855.<br>**Note** CSCvt23943 and CSCvt65855 are resolved in 1.3.3.3 only when you update the following packages to the versions listed in New and Changed Information, on page 4:<br>• Automation - Base<br>• Cisco DNA Center UI<br>• Cisco SD-Access<br>• Machine Reasoning<br>• Network Controller Platform | Resolved Bugs, on page 23 |
| 2020-03-13 | Added the list of packages in Cisco DNA Center 1.3.3.3. | New and Changed Information, on page 4 |
| | Added the Resolved Bugs table for 1.3.3.3. | Resolved Bugs, on page 23 |
| | Added an open bug: CSCvt10826. | Open Bugs—Non-High Availability, on page 20 |
| 2020-02-04 | Added the list of packages in Cisco DNA Center 1.3.3.1. | New and Changed Information, on page 4 |
| | Added the Resolved Bugs table for 1.3.3.1. | Resolved Bugs, on page 23 |
| | Added an open bug: CSCvs87002. | Open Bugs—Non-High Availability, on page 20 |
| 2020-01-17 | 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.

# New and Changed Information

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

***Table 2: Updated Packages and Versions in Cisco DNA Center Release 1.3.3.x***

| Package Name | Release 1.3.3.9 | Release 1.3.3.8 | Release 1.3.3.7 | Release 1.3.3.6 | Release 1.3.3.5 | Release 1.3.3.4 | Release 1.3.3.3(1) | Release 1.3 |
|---|---|---|---|---|---|---|---|---|
| **System Updates** | | | | | | | | |
| System | 1.3.0.167 | 1.3.0.159 | 1.3.0.147 | 1.3.0.142 | 1.3.0.142 | 1.3.0.135 | 1.3.0.122 | 1.3.0.115 |
| **Package Updates** | | | | | | | | |
| Access Control Application | 2.1.119.62020 | 2.1.118.62055 | 2.1.117.62009 | 2.1.116.62020 | 2.1.114.62044 | 2.1.113.62059 | 2.1.112.62025 | 2.1.109.624 |
| AI Network Analytics | 2.1.26.0 | 2.1.24.0 | 2.1.19.0 | 2.1.19.0 | 2.1.18.0 | 2.1.14.0 | 2.1.13.0 | 2.1.7.0 |
| Application Hosting | 1.1.0.200914 | 1.1.0.200914 | 1.1.0.191121 | 1.1.0.191121 | 1.1.0.191121 | 1.1.0.191121 | 1.1.0.191121 | 1.1.0.19112 |
| Application Policy | 2.1.118.170001 | 2.1.111.170010 | 2.1.111.170006 | 2.1.111.170006 | 2.1.111.170002 | 2.1.111.170000 | 2.1.111.170000 | 2.1.109.170 |
| Assurance - Base | 1.4.2.477 | 1.4.2.453 | 1.4.2.396 | 1.4.2.373 | 1.4.2.373 | 1.4.2.338 | 1.4.2.300 | 1.4.2.263 |
| Assurance - Sensor | 1.4.2.447 | 1.4.2.447 | 1.4.2.392 | 1.4.2.369 | 1.4.2.369 | 1.4.2.332 | 1.4.2.298 | 1.4.2.262 |
| Automation - Base | 2.1.119.62020 | 2.1.118.62055 | 2.1.117.62009 | 2.1.116.62020 | 2.1.114.62044 | 2.1.113.62059 | 2.1.112.62059 (Updated on 2020-03-30. The originally released package version was 2.1.112.62025.) | 2.1.109.624 |
| Automation - Intelligent Capture | 2.1.119.62020 | 2.1.118.62055 | 2.1.117.62009 | 2.1.116.62020 | 2.1.114.62044 | 2.1.113.62059 | 2.1.112.62025 | 2.1.109.624 |
| Automation - Sensor | 2.1.119.62020 | 2.1.118.62055 | 2.1.117.62009 | 2.1.116.62020 | 2.1.114.62044 | 2.1.113.62059 | 2.1.112.62025 | 2.1.109.624 |

| Package Name | Release 1.3.3.9 | Release 1.3.3.8 | Release 1.3.3.7 | Release 1.3.3.6 | Release 1.3.3.5 | Release 1.3.3.4 | Release 1.3.3.3(1) | Release |
|---|---|---|---|---|---|---|---|---|
| Cisco DNA Center Global Search | 1.0.0.72 | 1.0.0.72 | 1.0.0.72 | 1.0.0.72 | 1.0.0.68 | 1.0.0.68 | 1.0.0.47 | 1.0.0.47 |
| Cisco DNA Center Platform | 1.2.1.603 | 1.2.1.603 | 1.2.1.603 | 1.2.1.580 | 1.2.1.523 | 1.2.1.489 | 1.2.1.392 | 1.2.1.35 |
| Cisco DNA Center UI | 1.4.1.140 | 1.4.1.133 | 1.4.1.120 | 1.4.1.116 | 1.4.1.115 | 1.4.1.111 | 1.4.1.105<br>(Updated on 2020-03-30. The originally released package version was 1.4.1.100.) | 1.4.1.50 |
| Cisco SD-Access | 2.1.119.62020 | 2.1.118.62055 | 2.1.117.62009 | 2.1.116.62020 | 2.1.114.62044 | 2.1.113.62059 | 2.1.112.62059<br>(Updated on 2020-03-30. The originally released package version was 2.1.112.62025.) | 2.1.111. |
| Command Runner | 2.1.119.62020 | 2.1.118.62055 | 2.1.117.62009 | 2.1.116.62020 | 2.1.114.62044 | 2.1.113.62059 | 2.1.112.62025 | 2.1.109. |
| Device Onboarding | 2.1.119.62020 | 2.1.118.62055 | 2.1.117.62009 | 2.1.116.62020 | 2.1.114.62044 | 2.1.113.62059 | 2.1.112.62025 | 2.1.109. |
| Image Management | 2.1.119.62020 | 2.1.118.62055 | 2.1.117.62009 | 2.1.116.62020 | 2.1.114.62044 | 2.1.113.62059 | 2.1.112.62025 | 2.1.109. |
| Machine Reasoning | 2.1.119.210019 | 2.1.115.210016 | 2.1.115.210011 | 2.1.114.210004 | 2.1.114.210002 | 2.1.113.210008 | 2.1.112.210003<br>(Updated on 2020-03-30. The originally released package version was 2.1.111.212006.) | 2.1.111. |
| NCP - Base | 2.1.119.62020 | 2.1.118.62055 | 2.1.117.62009 | 2.1.116.62020 | 2.1.114.62044 | 2.1.113.62059 | 2.1.112.62025 | 2.1.109. |
| NCP - Services | 2.1.119.62020 | 2.1.118.62055 | 2.1.117.62009 | 2.1.116.62020 | 2.1.114.62044 | 2.1.113.62059 | 2.1.112.62025 | 2.1.109. |

| Package Name | Release 1.3.3.9 | Release 1.3.3.8 | Release 1.3.3.7 | Release 1.3.3.6 | Release 1.3.3.5 | Release 1.3.3.4 | Release 1.3.3.3(1) | Release 1.3 |
|---|---|---|---|---|---|---|---|---|
| Network Controller Platform | 2.1.119.62203 (Updated on 2021-01-14. The originally released package version was 2.1.119.62020.) | 2.1.118.62055 | 2.1.117.62009 | 2.1.116.62020 | 2.1.114.62044 | 2.1.113.62059 | 2.1.112.62059 (Updated on 2020-03-30. The originally released package version was 2.1.112.62025.) | 2.1.111.620 |
| Network Data Platform - Base Analytics | 1.4.1.175 | 1.4.1.173 | 1.4.1.164 | 1.4.1.164 | 1.4.1.162 | 1.4.1.156 | 1.4.1.152 | 1.4.1.150 |
| Network Data Platform - Core | 1.4.1.428 | 1.4.1.427 | 1.4.1.420 | 1.4.1.416 | 1.4.1.416 | 1.4.1.412 | 1.4.1.399 | 1.4.1.397 |
| Network Data Platform - Manager | 1.4.1.152 | 1.4.1.152 | 1.4.1.145 | 1.4.1.145 | 1.4.1.145 | 1.4.1.141 | 1.4.1.137 | 1.4.1.135 |
| Path Trace | 2.1.119.62020 | 2.1.118.62055 | 2.1.117.62009 | 2.1.116.62020 | 2.1.114.62044 | 2.1.113.62059 | 2.1.112.62025 | 2.1.109.624 |
| Rogue Management | 1.4.1.41 | 1.4.1.41 | 1.4.1.41 | 1.4.1.41 | 1.4.1.41 | 1.4.1.41 | 1.4.1.41 | 1.4.1.39 |
| Stealthwatch Security Analytics | 2.1.119.1090015 | 2.1.118.1090006 | 2.1.113.1090011 | 2.1.113.1090011 | 2.1.113.1090011 | 2.1.113.1090008 | 2.1.112.1090001 | 2.1.109.1090 |
| Wide Area Bonjour | 2.4.1.10016 | 2.4.1.10016 | 2.4.1.10016 | 2.4.1.10016 | 2.4.1.10016 | 2.4.1.10004 | 2.4.1.10004 | 2.4.1.10004 |

### New and Changed Features

The following table summarizes the new and changed features in Release 1.3.3.9.

*Table 3: New and Changed Features in Cisco DNA Center 1.3.3.9*

| Feature | Description |
|---|---|
| SSH connections to Cisco DNA Center | SSH connections to Cisco DNA Center adhere to the following security measures:<br>• SSH login attempt timeouts (LoginGraceTime): Any incomplete or broken SSH login attempts to Cisco DNA Center time out after 60 seconds. For example, when a client attempts to log in, Cisco DNA Center waits for 60 seconds for the client to enter the correct password.<br>• SSH login attempt retries (MaxAuthTries): Cisco DNA Center allows a client (a network device or a shell user) a maximum of three unsuccessful SSH login attempts before timing out and closing the SSH connection.<br>• SSH timeout limit (ClientAliveInterval*ClientAliveCountMax): SSH connections to Cisco DNA Center time out after 5 minutes of inactivity.<br>• SSH banner customization: Cisco DNA Center provides an option to customize the default SSH login banner or message of the day (MOTD) banner. For more information, see "Set Up a Login Message" in the Cisco DNA Center Administrator Guide. |

The following tables summarize the new and changed features in Release 1.3.3.0. For more information about these features, see the Cisco DNA Center End-User Guides and Cisco DNA Center Maintain and Operate Guides.

*Table 4: New and Changed Features in Cisco DNA Center 1.3.3.0*

| Feature | Description |
|---|---|
| **About** window lists appliance serial numbers | The **About** window lists the appliance serial numbers in addition to the system and application package versions. |
| Reserve IP pools | During single-stack (IPv4 only) and dual-stack (IPv4 and IPv6) pool reservation, the **Global Pool** drop-down list is enhanced to show all available global pools instead of the first 500 global pools. |
| Account lockout | **System Settings** > **Settings** > **Account Lockout** lets you configure the account lockout policy to manage user login attempts, the account lockout period, and login retries. |
| Password expiry | **System Settings** > **Settings** > **Password Expiry** lets you configure a password expiration policy to manage the password expiration frequency, the number of days that users are notified before their password expires, and the grace period. |

| Feature | Description |
|---|---|
| Global search enhancement | Global search functionality is enhanced to find items in the following categories anywhere in Cisco DNA Center:<br>• Authentication template<br>• Devices<br>• Fabric<br>• Network profiles<br>• Network settings<br>  • Device credentials<br>  • IP address pools<br>  • Service provider profiles<br>• Policy<br>• Traffic copy<br>• Transits |
| Service Explorer enhancement | On the **System 360** tab, in the **Cluster Tools** area, click **Service Explorer**.<br>The node clusters and the associated services are displayed in a tree-like structure in a new browser window. |

***Table 5: New and Changed Features in Cisco DNA Automation***

| Feature | Description |
|---|---|
| SSID provisioning for Meraki devices | Cisco DNA Center provides SSID provisioning support for Cisco Meraki devices managed by a Meraki dashboard. |
| New device support for Application Policy | The Cisco DNA Center Application Policy extends support for Duplo (IW6300 Series) devices. |
| Switchport screen enhancements for Cisco ISR 4000 | Provisioning for routing is enhanced with the switchport integration configuration and support is available for Cisco 4000 Series ISRs. |
| Advanced configuration mode for NFVIS | The NFVIS network profile configuration is enhanced to view flexible topologies, remove default network connections, and add connections between any VNF to the default network connection. |
| Provisioning/topology integration enhancements | The **Provision** window is enhanced with the option to launch the topology map view of the discovered devices from inventory. |
| Inventory | The **Stack** tab now appears only for switch stack devices and the primary stack. |
| Cisco StackWise Virtual link (SVL) support | Added support for Cisco StackWise Virtual, which is supported on Cisco Catalyst 9500 Series Switches. |

| Feature | Description |
| --- | --- |
| Support for new APs | This release introduces support for the following APs:<br>• Cisco Catalyst IW6300 Heavy Duty Series Access Points: The Cisco Catalyst IW6300 Heavy Duty Series Access Points increase plant productivity and worker safety measures. These are mesh APs that have a Class I Division 2 enclosure and simplified management, which can lead to increased cost savings. These APs are designed to bring resilient Wi-Fi mesh that is scalable and secure to hazardous environments.<br>• Cisco Industrial Wireless 3700 Series Access Points: The Cisco Industrial Wireless 3700 Series Access Points offer industrial-grade environmental qualifications while providing higher speeds for video and other bandwidth-intensive applications. These APs extend support to a new generation of Wi-Fi clients, such as smart phones, tablets, and high-performance laptops that have integrated 802.11ac support.<br>The Cisco Industrial Wireless 3700 Series Access Points offer a scalable and secure mesh architecture for high-performance Wi-Fi services, and can also serve as an advanced static or mobile Workgroup Bridge (WGB).<br>• Cisco 6300 Series Embedded Services Access Points: Cisco 6300 Series Embedded Services Access Points are supported with dual band 802.11a/g/n/ac, wave 2 access point, external antenna, voltage specification of 44 VDC to 57 VDC, power over Ethernet, and universal power over Ethernet. |
| Hypervisor support for Cisco Catalyst 9800-CL Cloud Wireless Controller | A virtual form factor of Cisco Catalyst 9800-CL Cloud Wireless Controller for private cloud now supports Hyper-V along with the existing hypervisors such as ESXi, KVM, and Cisco ENCS. |
| Support for Cisco Embedded Wireless Controller on Catalyst Access Points | This release supports the Day 0 workflow for Cisco Embedded Wireless Controller on Catalyst Access Points.<br>The Cisco Embedded Wireless Controller on Catalyst Access Points is available in multiple form factors:<br>• Cisco Embedded Wireless Controller on Catalyst 9115AX APs<br>• Cisco Embedded Wireless Controller on Catalyst 9117AX APs<br>• Cisco Embedded Wireless Controller on Catalyst 9120AX Access Points<br>• Cisco Embedded Wireless Controller on Catalyst 9130AX APs |

*Table 6: New and Changed Features in Cisco DNA Security Integration*

| Feature | Description |
|---|---|
| Supported features for Cisco ASA 5500-X Series Firewalls | Cisco DNA Center provides the following features support for Cisco ASA 5500-X Series Firewalls:<br>• Inventory<br>• Topology<br>• Software Image Management<br>• Templates for onboarding and customization of firewalls<br>Base automation supports Cisco ASA 5500-X Series Firewall in single context mode only. |
| Rogue Management application | The Rogue Management application is an optional package that you can install on Cisco DNA Center. Operating within Cisco DNA Center, the Rogue Management application helps you monitor threats from unauthorized access points. You can access the Rogue Management functionality as a dashboard within Cisco DNA Assurance in the Cisco DNA Center user interface.<br>The Rogue Management application supports Cisco Catalyst 9800 Series Wireless Controllers in this release, along with the existing support for Cisco AireOS Controllers.<br>After installing the Rogue Management package, you must enable the Rogue Management application by choosing **Enable** from the **Rogue** drop-down list on the **Rogue Management** window in Cisco DNA Center. This enables rogue detection on the Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller. |

*Table 7: New and Changed Features in Cisco DNA Assurance*

| Feature | Description |
|---|---|
| Health score settings for network devices | Added a new **Assurance** > **Manage** > **Health Score Settings** window.<br>Use this window to configure the health score settings for network devices. You can customize the health score calculation for network devices by changing the KPI thresholds and specifying the KPIs that are included for the calculation. |
| Trigger conditions for issues involving wireless clients with excessive onboarding times | Added trigger conditions for issues involving wireless clients with excessive onboarding times. You can specify the allowable time for the following phases during onboarding:<br>• AAA authentication<br>• Obtaining an IP address<br>To configure the trigger conditions, go to the **Assurance** > **Manage** > **Issue Settings** window. |

| Feature | Description |
| --- | --- |
| Wireless sensors dashboard changes | Updated the wireless sensors dashboard for the following changes:<br>• Changed the timeline to display colored-coded blocks that represent the percentage of overall sensor test failures for a specific time window.<br>• Added the **Overall Summary** dashlet, which provides an overall view of all the sensors in your network and their status.<br>This dashlet also provides the total number of tests performed by all sensors and a breakdown of the test results for test categories. Each test category provides additional details about its test results.<br>• Changed the **Test Results** dashlet to provide the **Heatmap View** and the **Card View**.<br>The **Heatmap View** displays the top five rankings for statistical categories. This view also displays a heatmap representation of the sensor test result failures.<br>The **Card View** displays the test result data in a card format for high-level monitoring and comparison.<br>To access the wireless sensors dashboard, go to the **Assurance** > **Dashboards** > **Wireless Sensors** window. |
| Sensor 360 window | Added a new window that provides a 360° view of a specific wireless sensor. With this window, you can view a sensor's test results, performance trends, and neighboring APs.<br>You can also view and download a sensor's event logs. |
| Sensor test templates | Added a new method to create and run sensor-driven tests.<br>With templates, you can reuse sensor-driven tests for quick deployment to multiple locations in the network.<br>To access the test templates, go to the **Assurance** > **Manage** > **Sensors** > **Test Templates** window. |
| Sensor legacy tests | Renamed the **Test Suites** method to **Legacy Tests**.<br>To access the legacy tests, go to the **Assurance** > **Manage** > **Sensors** > **Legacy Tests** window. |
| Persistent wireless backhaul connections on sensor devices | Added support for persistent wireless backhaul connections on sensor devices, which means that the wireless connection is "always on" regardless of wireless testing activities. |
| Intelligent Capture enhancements | The menu option **Manage** > **Intelligent Capture Settings** > **Client** changed to **Manage** > **Intelligent Capture Settings** > **Client Schedule Capture**.<br>You can view the history of Client Data Packet Capture sessions.<br>If no APs are enabled, you can use the **Configure AP Enablement** area to start enabling the APs. You can disable AP statistics capture on all APs.<br>The Spectrum Analysis charts are enhanced to provide more granular data. |
| Cisco StackWise Virtual link (SVL) support | Added support for Cisco StackWise Virtual, which is supported on the Cisco Catalyst 9500 Series Switches. |

| Feature | Description |
|---|---|
| Wired client syslogs and events displayed in Event Viewer | Cisco ISE server events, switch system-level syslogs, switch port or interface-specific events, and client-specific events are now displayed in the Event Viewer. |
| Issue enhancements | You can resolve or ignore a bulk of issues at a time.<br>The system automatically resolves issues if the issue condition no longer exists. This feature is supported for the following issues: Interface is down, wireless controller/switch/router is unreachable, and AP is down. |
| Executive Summary reports | You can now schedule Executive Summary Reports to capture detailed data about network devices and clients, which you can use to analyze network performance. |
| Samsung device support | Added support for Samsung devices. For Samsung devices, the **Detail Information** > **Device Info** tab displays additional information, such as build number, origin, country code, device type (mobile, tablet, and so on), and host operating system. |
| AI Network Analytics configuration workflow | Simplified the workflow for configuring AI Network Analytics. |

***Table 8: New and Changed Features in Cisco Software-Defined Access***

| Feature | Description |
|---|---|
| Extended node enhancements:<br>• Policy Extended Nodes: authentication support on extended nodes<br>• Multicast on extended nodes | • Cisco Industrial Ethernet 3400 and 3400H series switches running Cisco IOS XE 17.1.1s or later are policy extended nodes.<br>802.1x and MAB authentication is enabled on a policy extended node to communicate with Cisco ISE in order to download the VLAN and scalable group tag (SGT) attributes for the endpoints.<br>The link between the edge node and policy extended node is configured with inline tagging to propagate the SGT.<br>A policy extended node performs SGACL enforcement.<br>• Extended node devices can now handle multicast traffic. Multicast receivers are configured on the extended node devices. |
| Authentication template enhancements | • Hitless authentication: You can now switch directly between authentication modes (Open, Low Impact, Closed) without removing the device from the fabric<br>• Site-specific authentication: You can configure authentication settings specifically for a site and can also change the authentication settings at a global level. This can be helpful in a multisite environment where a site has specific requirements for authentication settings. |
| Multicast enhancements: support for custom source-specific multicast (SSM) | This release introduces a workflow-based configuration for multicast traffic. You can specify multiple custom SSM IP ranges for every virtual network. You can also configure a rendezvous point (RP) outside the fabric. |

| Feature | Description |
|---|---|
| Layer 2 intersite | This feature allows connectivity of endpoints from one fabric site to another, in the Layer 2 domain. Layer 2 intersite communication is achieved by extending the same subnet across multiple fabric sites. This extends Layer 2 across the fabric sites connected over a Layer 2 segment. |
| StackWise Virtual link (SVL) support at border, edge, and Fabric in a Box | Cisco Catalyst 9500 Series Switches, when configured as StackWise Virtual, can be added to the fabric as an edge, border, border with colocated control plane, or a Fabric in a Box device.<br>• Only wired clients are supported on the edge nodes that are connected in SVL.<br>• SVL configuration on the device should be done manually before adding the device to the Inventory. |

***Table 9: New Hardware in Cisco Software-Defined Access***

| Device Role | Product Family | Part Number | Description |
|---|---|---|---|
| Fabric edge, border, control plane node, and Fabric in a Box, with embedded wireless | Cisco Catalyst 9300 Series Switches | C9300L-24UX-4X<br>C9300L-24UX-2Q<br>C9300L-48UX-4X<br>C9300L-48UX-2Q<br>C9300L-48PF-4G<br>C9300L-48PF-4X | Cisco Catalyst 9300 Series Switches are available with 24 and 48 ports and support multi-Gigabit port and universal power supply over Ethernet. |
| Access points | Cisco Catalyst IW6300 Heavy Duty Series Access Points | IW-6300H-DC-x-K9 | Cisco Catalyst IW6300 Heavy Duty Series access points are supported with dual-band 802.11a/g/n/ac, wave 2 access point, external antenna, voltage specification of 44 VDC to 57 VDC, power over Ethernet, and universal power over Ethernet. |
| | | IW-6300H-DCW-x-K9 | Cisco Catalyst IW6300 Heavy Duty Series access points are supported with dual-band 802.11a/g/n/ac, wave 2 access point, external antenna, voltage specification of 10.8 VDC to 36 VDC, power over Ethernet, and universal power over Ethernet. |
| | | IW-6300H-AC-x-K9 | Cisco Catalyst IW6300 Heavy Duty Series access points are supported with dual-band 802.11a/g/n/ac, wave 2 access point, external antenna, voltage specification of 110 VAC to 220 VAC, power over Ethernet, and universal power over Ethernet. |

| Device Role | Product Family | Part Number | Description |
|---|---|---|---|
| Access points | Cisco 6300 Series Embedded Services Access Points | ESW-6300-CON-x-K9 | Cisco 6300 Series Embedded Services access points are supported with dual-band 802.11a/g/n/ac, wave 2 access point, external antenna, voltage specification of 44 VDC to 57 VDC, power over Ethernet, and universal power over Ethernet. |
| Access points | Cisco Industrial Wireless 3702 Access Points | IW3702-2E-x-K9, IW3702-4E-x-K9 | Cisco Industrial Wireless 3702 access points support 802.11ac wave 1 technology with 4x4 MIMO, three spatial streams, IP67 rated, ruggedized, and certified for onboard rail and outdoor use cases. |
| Policy extended node | Cisco Catalyst IE3400 Heavy Duty Series (IE3400H) | IE-3400H-8FT-E<br>IE-3400H-16FT-E<br>IE-3400H-24FT-E | Cisco IE3400H Series switches are available with 8, 16, or 24 Fast Ethernet (D-coded) M12 interfaces. |
| Policy extended node | Cisco Catalyst IE3400 Heavy Duty Series (IE3400H) | IE-3400H-8T-E<br>IE-3400H-16T-E<br>IE-3400H-24T-E | Cisco IE3400H Series switches are available with 8, 16, or 24 Gigabit Ethernet (X-coded) M12 interfaces. |

***Table 10: New and Changed Features in Cisco DNA Center Platform***

| Feature | Description |
|---|---|
| Enhanced data synchronization between Cisco DNA Center and a Configuration Management Database (CMDB) | You can now map inventory and SWIM fields from Cisco DNA Center to the ServiceNow CMDB for synchronization. These fields can be mapped as attributes, reference fields, configuration items (CIs), or CI classes. |
| New software image management (SWIM) closed loop automation between Cisco DNA Center and an ITSM | This release supports closed loop automation for SWIM between Cisco DNA Center and ServiceNow. For supported ServiceNow releases, a ServiceNow admin can review, approve, and close Cisco DNA Center SWIM change requests (CRs) in ServiceNow. |
| New Assurance-to-ITSM enhancements | You can now view ServiceNow ticket data associated with an Assurance issue in the Cisco DNA Center GUI. |

## 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.

## Cisco DNA Center Compatibility Matrix

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

## Compatible Browsers

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

- Google Chrome: Version 73.0 or later
- Mozilla Firefox: Version 65.0 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.

## Cisco DNA Center Scale

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

## IP Address and FQDN Firewall Requirements

To determine the IP addresses and fully qualified domain names (FQDNs) that must be made accessible to Cisco DNA Center through any existing network firewall, see "Required Internet URLs and FQDNs" in the Cisco DNA Center Installation Guide.

## 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) for appliance model DN1-HW-APL
- Cisco IMC Version 3.1(2c) for appliance model DN2-HW-APL
- Cisco IMC Version 3.1(3a) for appliance model DN2-HW-APL-L
- Cisco IMC Version 4.0(1a) for appliance model DN2-HW-APL-XL

The preceding versions are the minimum firmware versions. While some later versions are also supported, Cisco DNA Center is not compatible with all later versions. Do not update later than Cisco IMC 4.0(4b), unless you update to 4.0(4k) or later.

## Installing Cisco DNA Center

You can 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** The following applications are not installed on Cisco DNA Center by default. If you need any of these applications, you must manually download and install the packages separately.

- Application Hosting
- Application Policy
- Assurance - Sensor
- Automation - Sensor
- Cisco DNA Center platform
- Cisco SD-Access
- Cisco Wide Area Bonjour Application
- Intelligent Capture

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

## Cisco DNA Center Platform Support

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

## Support for Cisco Connected Mobile Experiences

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

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

## Plug and Play Considerations

### Plug and Play Support

#### General Feature Support

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

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

the switch is booted in install mode. (Image install and upgrade is not supported for switches booted in bundle mode.)

### Secure Unique Device Identifier Support

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

- Cisco routers:
  - Cisco ISR 1100 Series with software release 16.6.2
  - Cisco ISR 4000 Series with software release 3.16.1 or later, except for the ISR 4221, which requires release 16.4.1 or later
  - Cisco ASR 1000 Series (except for the ASR 1002-x) with software release 16.6.1
- Cisco switches:
  - Cisco Catalyst 3850 Series with software release 3.6.3E or 16.1.2E or later
  - Cisco Catalyst 3650 Series and 4500 Series with Supervisor 7-E/8-E, with software release 3.6.3E, 3.7.3E, or 16.1.2E or later
  - Cisco Catalyst 4500 Series with Supervisor 8L-E with software release 3.8.1E or later
  - Cisco Catalyst 4500 Series with Supervisor 9-E with software release 3.10.0E or later
  - Cisco Catalyst 9300 Series with software release 16.6.1 or later
  - Cisco Catalyst 9400 Series with software release 16.6.1 or later
  - Cisco Catalyst 9500 Series with software release 16.6.1 or later
  - Cisco Catalyst IE3300 Series with software release 16.10.1e or later
  - Cisco Catalyst IE3400 Series with software release 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 16.3.2 or later
  - Cisco ISR 4000 Series with software release 16.3.2 or later
- Cisco switches:
  - Cisco Catalyst 3650 Series and 3850 Series with software release 16.6.1 or later
  - Cisco Catalyst 9300 Series with software release 16.6.1 or later
  - Cisco Catalyst 9400 Series with software release 16.6.1 or later
  - Cisco Catalyst 9500 Series with software release 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 16.6.2 or later

## 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

## Use the Bug Search Tool

Use the Bug Search tool to search for a specific bug or to search for all bugs in this release.

### Procedure

**Step 1** Enter the following URL in your browser:

https://tools.cisco.com/bugsearch

**Step 2** In the **Log In** window, enter your registered cisco.com username and password and click **Log In**.

The **Bug Search** window opens.

**Note** If you do not have a cisco.com username and password, register at https://idreg.cloudapps.cisco.com/idreg/guestRegistration.do.

**Step 3** To search for a specific bug, enter the bug ID in the **Search For** field and press **Return**.

**Step 4** To search for bugs in the current release:

a) In the **Search For** field, enter **Cisco DNA Center** and press **Return**. (Leave the other fields empty.)

b) When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by modified date, status, severity, and so on.

To export the results to a spreadsheet, click the **Export Results to Excel** link.

## Open Bugs—Non-High Availability

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

***Table 11: Open Bugs—Non-HA***

| Bug Identifier | Headline |
|---|---|
| CSCvo44394 | When you try to add Cisco ISE 2.4 to Cisco DNA Center 1.3, the following certificate error is generated:<br>`"Error establishing trust with ISE: Expected phrase [Enter URI for uploading ISE certificate chain:] wasn't received from ise"`<br>To work around this problem, configure the network MTU size to 9100 between Cisco ISE and Cisco DNA Center. |
| CSCvo60306 | Device activation fails when the image is not the minimum supported image version. |
| CSCvp15026 | Devices remain in Partial Collection Failure state after an incomplete provision and resynch.<br>This problem occurs only when there is an incomplete manual clearing of CLI commands on a device. When a device goes through the full removal flow, subsequent synchronizations work correctly.<br>Related bug: CSCvj15139. |
| CSCvp25402 | After you delete a wireless controller with 4000 APs from Cisco DNA Center, it takes 25 minutes or longer for the wireless controller to be removed from the inventory. |
| CSCvp48020 | The IR829 does not display the correct Gigabit interface in the WAN interface drop-down list. |
| CSCvp48160 | Software image management: Cisco Catalyst 6000 image activation fails while upgrading the image version 152-2.SY to 152-2.SY*. |
| CSCvp49120 | A Cisco Catalyst 6000 ISSU upgrade from SY2 to SY3 fails when the device has `snmp-server enable traps vstack` in the running configuration. |
| CSCvp83057 | During migration from Cisco DNA Center 1.2 or earlier to Cisco DNA Center 1.3 or later, the incorrect CLI **use-petr** (which is pushed to SD-Access Anywhere borders) is not automatically removed from the network. |
| CSCvp95386 | After upgrading the embedded wireless software on Cisco Catalyst 9000 devices from 16.10.1.e to 16.11.1s, the AP country code configuration is lost. |
| CSCvp96088 | An image change on the wireless controller causes the AP Intelligent Capture 360 page to lose all data. |
| CSCvq13219 | Copying the golden tag for a base image does not copy the wireless package. |
| CSCvq34252 | During Return Material Authorization (RMA), the AVC configuration is not replaced completely; match commands are missing for class-map. |
| CSCvq53490 | After migrating policy data to Cisco ISE, some policies are not migrated from Cisco DNA Center to Cisco ISE. |
| CSCvq53511 | No loop is detected if MSTP is enabled on the device. |
| CSCvq55154 | Cisco Catalyst 9800 Series Wireless Controller: NETCONF discovery fails after performing a write erase on the device. |

| Bug Identifier | Headline |
|---|---|
| CSCvq55394 | If STP is not enabled on devices, loops are not detected, and MRE does not conclude. |
| CSCvq61710 | Cisco DNA Center: For Cisco Nexus 7000 Release 8.2(4) devices, the kick start image should also show under latest/suggested. |
| CSCvq63486 | Rogues coming from a Cisco Catalyst 9800 Series Wireless Controller show empty data for SNR values in the Cisco DNA Center Rogue page. |
| CSCvq66963 | ENCS/NFVIS devices with NFVIS version 3.12.1 are not managed and show partial collection failure in Cisco DNA Center. |
| CSCvq70912 | Cannot onboard 8.8.261 wireless sensors after upgrading to Cisco DNA Center. |
| CSCvq86168 | Application installation fails with an error message that the device does not support third-party applications, even though the device (such as a Cisco Catalyst 9300) has a Cisco USB connected in the back panel. |
| CSCvq95775 | The catalog server tries to pull the packages even if there is a failure due to capability level after Cisco DNA Center is powered on. |
| CSCvr13910 | If you use a default policy with the "Deny IP" SGACL and the policy is pushed to the switch, all control packets are denied and the switch loses connectivity to the network. |
| CSCvr59764 | Day-N templates are not pushed to the second device in multisite router provisioning. |
| CSCvr72364 | In the Routers tab, the device count shows incorrect values in the **Marked for Replacement** window. |
| CSCvr87910 | Cannot enable wireless on ECA due to the error "NCWL 10033 wrong address (Country) set." |
| CSCvr98946 | Inventory: Device config clean fails. |
| CSCvs08584 | VRF and Layer 3 routing are not supported on the Cisco Catalyst 9800 Series Wireless Controller.<br>The Catalyst 9800 Series Wireless Controller goes into unmonitored state when the management VRF is configured, and that interface is discovered by or added to the Cisco DNA Center inventory.<br>To work around this issue, use a non-VRF interface to add the Catalyst 9800 Series Wireless Controller. |
| CSCvs47608 | An AP claim through PnP hangs in onboarding state.<br>Related bug: CSCvt01785. |
| CSCvs57800 | The initial installation of Cisco DNA Center fails if localhost resolves to any IP address other than 127.0.0.1. |
| CSCvs72105 | Cisco DNA Assurance: A wireless controller fails to download a certificate from Cisco DNA Center due to an invalid URL error. |
| CSCvs87002 | After you add a new Cisco Catalyst 9800 Series Wireless Controller, if the first-time NETCONF discovery fails, the wireless controller finds the AP and clients join correctly, but Assurance contains no data. |
| CSCvs87674 | In the Discovery window, the eye icon is reversed for hidden and unhidden passwords. (That is, when the password is hidden, the unhidden eye icon is shown, and vice versa.) |
| CSCvs87703 | In the Inventory window, the count of devices per site or per floor is missing. |

| Bug Identifier | Headline |
|---|---|
| CSCvt10826 | Unable to delete a device because an inventory synch proceeds while an ongoing configuration cleanup is taking place. |
| CSCvt33310 | By default, Cisco DNA Center configures a Cisco Catalyst 9800 Series Wireless Controller with the management VRF and IP address of the management interface for connections back to Cisco DNA Center for Assurance information gathering. However, if both the management VRF and the IP address are configured, the connection may fail.<br>From Cisco DNA Center, if the VRF is configured and the device is added to Cisco DNA Center, the Assurance TLS connection is not established and the device goes into unmonitored state. |
| CSCvt85320 | Under **Design** > **Network Hierarchy**, a device that is assigned to a floor through PnP does not appear on the floor map.<br>To work around this problem, unclaim the device in inventory, reclaim the device, and then assign it to the desired site or floor. |
| CSCvt89349 | Cannot edit an existing enterprise SSID or add a new enterprise SSID. |
| CSCvu12292 | For a TCAM issue, the window takes longer than 30 minutes to reflect in Cisco DNA Center. |
| CSCvu42019 | Client-based custom groups create more callback execution and therefore a lag in 100,000 wired clients. |
| CSCvu48710 | Under **Tools** > **License Manager** > **All Licenses** > **Action** > **Enable License Reservation**, Cisco DNA Center reserves the correct number of licenses for a StackWise virtual switch. However, when reviewing the stack, only the stack member that is in active mode has activated the license. Any stack member that is in standby mode shows the reservation status as "RESERVATION IN PROGRESS."<br>To work around this problem, activate the licenses manually. |
| CSCvv88788 | Cisco DNA Center installation fails due to initrd corruption. The CIMC console displays a kernel panic error. There is a large time drift from the NTP server.<br>To work around this problem, copy the initrd from flash to disk, correct the NTP server configuration, and ensure the correct time synch. |
| CSCvw56838 | If you remove a provisioned device from the inventory and from the Plug and Play window, after about 1 minute the device returns to the Plug and Play window and displays the status "Error." This problem occurs because a device that has a PnP profile continues to try to reach Cisco DNA Center.<br>To work around this problem, remove the PnP profile from the managed device. |

## Open Bugs—High Availability

The following table lists the open high availability (HA) bugs in Cisco DNA Center for this release.

*Table 12: Open Bugs—HA*

| Bug Identifier | Headline |
|---|---|
| CSCvn32215 | In a three-node cluster, if you bring down the node while LAN automation is in progress, the LAN automation status shows as complete, yet without success.<br>This problem occurs if you perform a network-orchestration service restart or a full node restart while LAN automation is in progress.<br>The network orchestration service doesn't resume the ongoing LAN automation session. It marks LAN automation as complete and releases all IP addresses allocated from IPAM. Users are expected to perform a configuration cleanup on the seed device, write-erase/reload discovered devices, and start a new LAN automation session. |
| CSCvr98946 | Inventory: Device configuration clean operation fails on an HA cluster. |
| CSCvt87610 | The Cisco Catalyst 9800 Series Wireless Controller telemetry connection remains in the Connecting state, and no Assurance data corresponding to the Catalyst 9800 Series Wireless Controller is displayed in Cisco DNA Center. Alternatively, Assurance data for an Catalyst 9800 Series Wireless Controller goes missing, then recovers by itself, depending on whether the node running the collector-iosxe-db service and the primary node (the one that holds the virtual IP) are the same.<br>This problem occurs in a three-node upgraded cluster only if the collector-iosxe-db service is not running in the node that holds the virtual IP. |
| CSCvu15218 | Upgrade from Cisco DNA Center 1.3.1.6 to 1.3.3.5 is failing at 41% due to rabbitmq-3 instances in crashloop. |
| CSCvu29282 | In a three-node cluster, a new member ID is created after the system upgrade is completed from Cisco DNA Center 1.3.3.4 to 2.1.1. |

## Resolved Bugs

The following table lists the resolved bugs in Cisco DNA Center, Release 1.3.3.9.

*Table 13: Resolved Bugs in Cisco DNA Center, Release 1.3.3.9*

| Bug Identifier | Headline |
|---|---|
| CSCvu25442 | The sdn-network-infra-iwan certificate is expired on the device. |
| CSCvu89185 | SSID is being broadcasted in a site even after disassociating the respective wireless profile. |
| CSCvv04838 | PnP fails with "NCOB02051: Failed to parse cli output for show mod" for a switch stack. |
| CSCvv08806 | Extended nodes must be configured on distinct edge ports. |
| CSCvv39538 | Image Repository displays "Failed to load data" after adding a Meraki dashboard to Cisco DNA Center. |
| CSCvv60854 | A Cisco Catalyst 9800 Series Wireless Controller in high availability fails inventory collection. |
| CSCvv67156 | Cisco DNA Center can't start LAN automation if the primary seed device is deleted before stopping a previous LAN automation session. This causes subsequent LAN automation sessions to fail. |

| Bug Identifier | Headline |
|---|---|
| CSCvv70086 | Cisco DNA Center pushes conflicting configurations to the extended node interfaces during PnP. |
| CSCvv81654 | C9500-16X borders fail inventory collection after upgrading to Cisco DNA Center 1.3.3.7. |
| CSCvv84323 | Wireless controller provisioning fails due to a guest SSID that was created during the Cisco DNA Center 1.2.x time frame. |
| CSCvv91822 | The IPDT configuration is rejected on a Bluetooth interface during provisioning. |
| CSCvv94215 | Cisco DNA Center cannot start LAN automation due to a discovered site deleted from the system. |
| CSCvv95170 | Device-tracking configuration push fails when the Cisco Catalyst 9407 device role is changed to ACCESS. |
| CSCvw00591 | Cisco DNA Center doesn't remove a stale VLAN configuration. |
| CSCvw03683 | Cisco DNA Center can't start new LAN automation sessions, citing the error "NCND05022: New LAN Automation cannot start as previous session is still in-progress." |
| CSCvw08311 | Cisco DNA Center's Assurance data may be incomplete, or incoherent, and gaps may appear in the charts on the Application Health and Application 360 pages when unsupported DSCP values are in NetFlow records received by the managed devices. |
| CSCvw08944 | Many devices display "Managed (Internal Error)" after an upgrade to Cisco DNA Center. |
| CSCvw09106 | An external webauth SSID is configured with "central-webauth" enabled. |
| CSCvw14715 | Cisco DNA Center doesn't push the default-site-tag-fabric configuration to the Cisco Catalyst 9800 Series Wireless Controller after an upgrade. |
| CSCvw42212 | LAN automation doesn't work due to an IPAM IP address allocation issue.<br>Related bug ID: CSCvv73881. |
| CSCvw76745 | Attempts to provision a Cisco Catalyst 9800 wireless LAN controller may fail with a null pointer exception in Cisco DNA Center's network-programmer log. This problem occurs on Cisco DNA Center 1.3.3.9 when the wireless LAN controller has a guest SSID.<br>This bug is resolved in 1.3.3.9 only when you update the Network Controller Platform (network-visibility) package to version 2.1.119.62203. |

The following table lists the resolved bugs in Cisco DNA Center, Release 1.3.3.8.

***Table 14: Resolved Bugs in Cisco DNA Center, Release 1.3.3.8***

| Bug Identifier | Headline |
|---|---|
| CSCvj21529 | When a guest virtual network managed by Cisco DNA Center has a different DNS server than the global DNS server, the webauth ACL applied needs to contain that DNS server's IP address. |
| CSCvj70154 | Cisco DNA Center should not push the "default-information originate" configuration for a nonborder device as a seed. |
| CSCvj87768 | Cisco DNA Center's documentation is missing details about how to enable TLS version 1 for older Cisco Catalyst devices to be able to use software image management functions. |

| Bug Identifier | Headline |
|---|---|
| CSCvk17285 | Cisco DNA Center 1.2.x has some issues configuring the wireless controller for Assurance. |
| CSCvk20682 | Cisco DNA Center's provisioning Status shows "Failed" with the error message "Authentication Failure while connecting to device x.x.x.x using protocol ssh2," but the configuration gets pushed to the device. |
| CSCvk53436 | Cannot upgrade fusion packages after initiating an upgrade. |
| CSCvn02210 | Cisco DNA Center may have managed switch stacks go into "Partial Collection Failure Unknown" status, with logs indicating problems with an xmp-im-security-module. |
| CSCvn95906 | A Cisco DNA Center 1.2.6 to 1.2.8 upgrade fails on a three-node cluster with missing deployment for the inventory-manager service. |
| CSCvo11462 | The Assurance Device 360 page shows gaps in CPU and memory charts. |
| CSCvo21286 | Buttons on sidebar/slideout are not visible with Chrome 72.0.x.x. As a workaround, use Firefox. |
| CSCvp55926 | Device deletion does not work for a Cisco ASR 1002 device. |
| CSCvp97371 | Cannot delete a Cisco Catalyst 9300 edge from the device inventory. |
| CSCvq09405 | Cannot update an IP address pool in a virtual network. |
| CSCvq42780 | An application package upgrade failure occurs. |
| CSCvq43900 | System upgrade fails due to etcd going into error state. |
| CSCvq47566 | Cisco DNA Center's etcd service may exhaust its memory, causing the system to become unstable. |
| 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, it may cause some port security configurations to be removed. |
| CSCvq81851 | A Cisco DNA Center upgrade failure occurs due to tenant data migration. A duplicated entry appears in serialnumberipaddressmapping. |
| CSCvq88023 | Packages upgrade fails after upgrading Maglev to 1.3.0.73. |
| CSCvq97467 | Cisco DNA Center does not display virtual network information after upgrading from 1.2.10.4 to 1.3.0.3. |
| CSCvr02827 | An access tunnel goes down and does not recover after applying a security fix on an AireOS wireless controller. |
| CSCvr42300 | Cisco DNA Center may fail to upgrade the Access Control Application and Cisco SD-Access packages while upgrading to 1.3.1.0. |
| CSCvs51143 | When an edge device that is managed by Cisco DNA Center has a StackWise virtual link (SVL) member down, Cisco DNA Center's GUI and the rest of the network can become out of sync. |
| CSCvs68065 | Cisco DNA Center 1.2.10, 1.2.12, and 1.3.1.4 ISO install fails. |
| CSCvs83964 | Assurance-2 pod restarts continuously because of OutOfMemory in metaspace. |
| CSCvs86290 | An enterprise port failure causes service disruption in a three-node cluster. |

| Bug Identifier | Headline |
|---|---|
| CSCvs87767 | The primary node (seed) configuration is missing from etcd. |
| CSCvt25302 | Cisco DNA Center may not install a new image to a managed device, citing the errors, "NCOB04023: Failed to install image on the device," and "NCOB02002: Command unsuccessful from device: PnP Service Error 1803 Source file not found." This is due to complications of using the device's .bin file out of the .tar file it is compressed into. |
| CSCvt26808 | Cisco DNA Center should mask details about running components such as the versions of the webserver running from command line interactions. |
| CSCvt29159 | Cisco ISE connection failure: Error importing the Cisco ISE certificate chain into the Cisco DNA Center truststore. |
| CSCvt35920 | Cisco DNA Center's etcd service may fail negotiation among nodes, causing the election of a leader node to fail. When etcd has no leader node, other services, including those that provide Cisco DNA Center's UI, may fail. |
| CSCvt41445 | The Group-Based Access Policy page becomes blank after a node powercyle in a three-node setup. |
| CSCvt97301 | Some or all of Assurance's data may be missing, due to the "kube-dns" service restarting. |
| CSCvu09115 | AP provisioning fails with the error "OwningEntityId" details for wireless controller missing in the database. |
| CSCvu15632 | Control plane name in virtual network anchor workflows should be 32 characters or less. |
| CSCvu22453 | Cisco DNA Center's external authentication over TACACS times out after 5 seconds, even if the timeout is a larger value. |
| CSCvu24866 | Member switch request code is not generated for Cisco Catalyst 9000 stacked switches using SLR in Cisco DNA Center. |
| CSCvu38087 | Map file exported from Cisco DNA Center 1.3.3.3 has an exclusion region with duplicate vertices. |
| CSCvu48408 | Wireless controller provisioning fails due to a special character in the site name. |
| CSCvu57991 | Cisco DNA Center may fail to learn the brownfield configuration of a wireless LAN controller, when the wireless has an invalid selection of channel width and DCA channels. |
| CSCvu68204 | Elasticsearch remains in init state after an upgrade from Cisco DNA Center 1.3.3.x. |
| CSCvu71843 | AP deletion causes wireless controller provisioning failure. |
| CSCvu92247 | Maglev system upgrade fails at 60% because of an inability to restart the network. |
| CSCvu93584 | Application Experience is down in Assurance. |
| CSCvu95095 | Application package fails for Cisco DNA Center. |
| CSCvu96315 | Cisco DNA Center's Cloud AI registration may fail, and complain about not having cloud connectivity. |
| CSCvu96801 | Webhooks notifications stop working for pre-existing destinations or new destinations. |

| Bug Identifier | Headline |
|---|---|
| CSCvv06151 | In Cisco DNA Center 1.3.3.5, the INFRA_VN may not be available under L2 Handoff for border configuration, so it cannot be removed. |
| CSCvv22070 | After restoring a backup, provision doesn't work if the inventory sync is disabled. |
| CSCvv25658 | Cisco ISE pxGrid connections are missing after a manual disaster recovery failover. |
| CSCvv64614 | Cisco DNA Center does not push the IP Device Tracking (IPDT) configuration to switchports that are in access mode, in switches whose role is defined as access switches. |

The following table lists the resolved bugs in Cisco DNA Center, Release 1.3.3.7.

***Table 15: Resolved Bugs in Cisco DNA Center, Release 1.3.3.7***

| Bug Identifier | Headline |
|---|---|
| CSCvs76592 | Many device-registration "Sensor-Client-AP" requests lead to slow access of the Cisco DNA Center GUI. |
| CSCvt54476 | Cisco DNA Center fails to delete a device. On the Provision page, when you try delete a device from Inventory, the message "Error while deleting device" is displayed.<br>The following error is recorded in the apic-em-inventory-manager-service log file when this problem occurs:<br>`20-03-19 19:08:40,863 \| ERROR \| impleAsyncTaskExecutor-14 \| \|`<br>`c.c.e.i.impl.InventoryServiceImpl \|`<br>`Error while deleting device x.x.x.x. \|`<br><br>`org.postgresql.util.PSQLException: ERROR: update or delete on table "igmpnrsettings" violates`<br>`foreign key constraint "fk49a8c2318028e9a8" on table "igmpsnoopingsettings"` |
| CSCvt58303 | Cisco DNA Center's GUI loads intermittently when the enterprise and cluster virtual IPs are assigned to two nodes in a three-node cluster. |
| CSCvt59522 | A device that was successfully provisioned by Cisco DNA Center's PnP application may not be added to Inventory when the HTTPS write credentials are missing from the site credential settings. |
| CSCvt76571 | When you navigate to Cisco DNA Assurance's Rogue Management page, the "Please hold on" notification is displayed, and the page does not fully load. |
| CSCvt82136 | On the Device 360 page for an AP, the Intelligent Capture panel shows the warning message "GRPC link is not ready (TRANSIENT FAILURE)." However, contrary to what the message suggests, the condition persists. |
| CSCvt88163 | Cannot remove an ISRV border node from a fabric that was provisioned with an NFV profile. |
| CSCvu03221 | Reprovisioning a wireless controller without a CLI template removes the VLANs from the Flex profile. |
| CSCvu14815 | Cisco DNA Center performs an image upgrade for a Fabric-in-a-Box device even if the wireless package doesn't exist. |
| CSCvu15218 | Upgrade from Cisco DNA Center 1.3.1.6 to 1.3.3.5 fails at 41% due to 2/3 rabbitmq instances in crashloop. |

| Bug Identifier | Headline |
|---|---|
| CSCvu23957 | Cisco DNA Center fails to collect inventory for a device, citing an error that the SNMP walk returned too many rows. |
| CSCvu31870 | Catalyst 9500: Image activation fails with NCSW10249. |
| CSCvu66737 | During inventory collection from a managed device, if connectivity is interrupted or the device fails to respond to feature_config_interface inquiries, any static port configuration may be removed from Cisco DNA Center's GUI, and from the managed device itself. |
| CSCvu73783 | Devices fail inventory collection due to violating the unique constraint "routepolicymapentry_bk". |
| CSCvu77846 | After a Cisco DNA Center upgrade, switch provisioning is blocked if the code is not running 16.12.2 or later. |
| CSCvu98732 | In a large-scale fabric deployment and in some race conditions, the spf-device-manager-service restarts. |

The following table lists the resolved bugs in Cisco DNA Center, Release 1.3.3.6.

***Table 16: Resolved Bugs in Cisco DNA Center, Release 1.3.3.6***

| Bug Identifier | Headline |
|---|---|
| CSCvr49629 | Cannot start LAN automation. The following error occurs:<br>`Error while reserving the SVI space.` |
| CSCvt59517 | Application 360 is missing information for clients connected to a Cisco Catalyst 9000. |
| CSCvu03050 | Reprovisioning a wireless controller fails after site floor deletion. |
| CSCvu15592 | Cisco DNA Center removes a QoS policy after applying it. |
| CSCvu18273 | The devices on a site don't appear on the Assurance Network Health page, even though devices are present. |

The following table lists the resolved bugs in Cisco DNA Center, Release 1.3.3.5.

***Table 17: Resolved Bugs in Cisco DNA Center, Release 1.3.3.5***

| Bug Identifier | Headline |
|---|---|
| CSCvp87542 | A Cisco Catalyst 9800 Series Wireless Controller provisioning failure occurs when a special character is used in a Cisco ISE shared key. |
| CSCvq09974 | In a three-node setup, Influxdb crashes with OOM errors. |
| CSCvs02409 | After a fresh installation of Cisco DNA Center, the root (/) partition of the appliance is 85% or more full. An out-of-disk-space situation causes Kubernetes to be unable to schedule or destroy any pods. |
| CSCvs52947 | GlusterFS does not heal automatically because of stale references. |
| CSCvs55949 | Network validation fails for Cisco DNA Center's 10 Gigabit Ethernet interface. |
| CSCvs59089 | Provisioning switches fails due to an error in retrieval of the Cisco ISE PAN IP addresses. |

| Bug Identifier | Headline |
|---|---|
| CSCvs71990 | Cisco DNA Center three-node cluster: If you select multiple fabric edges to provision, the provisioning is performed one device at a time. |
| CSCvs93317 | An upgrade to Cisco DNA Center 1.3.3 fails because the NFS server configured for Assurance backup is unresponsive. |
| CSCvs93670 | LAN automation doesn't generate an alert if the LAN subnet is exhausted during L3 configuration. |
| CSCvs97183 | Cisco SD-Access: Need to configure the **flood arp-nd** command on L2 flooding IP pools to disable the AR relay. |
| CSCvs99118 | Audit logs: The service request processing fails with the following error:<br>`Previous request with the same intent is either being processed or was already processed.` |
| CSCvt00103 | Cisco DNA Center does not show heatmaps for APs in 2.4 GHz. Heatmaps for the same APs are seen in 5 GHz. |
| CSCvt04397 | When an attempt is made to upgrade Cisco DNA Center while its postgres database is not functioning properly, the SchemaUpdater process times out, but the process is not killed. This causes the upgrade to fail. |
| CSCvt08105 | A change in a building name on **Design** > **Network Hierarchy** > **List View** > **Edit Building** is not immediately reflected on the Assurance Device 360 page. |
| CSCvt18788 | After upgrade, reprovisioning a wireless controller creates a new wireless profile. |
| CSCvt25042 | The Cisco DNA Center GUI goes into maintenance mode intermittently. |
| CSCvt29668 | Cisco DNA Center may fail to collect inventory from a Cisco Catalyst 9800 Series Wireless Controller, citing the dmm_modelclass table not having entries for the tables EwlcTsFlexProfile and EwlcTsFlexProfilePolicyAcl. |
| CSCvt32995 | Disable IPv6 to avoid services binding to an IPv6 address space. |
| CSCvt44539 | Policy: Deploying wired QoS results in FMANRP_QOS-3-HWIDBCHECK: on Fabric border Catalyst 9800 Series Wireless Controller. |
| CSCvt44900 | PnP conflict with LAN automation due to PnP startup-vlan CLI. |
| CSCvt45288 | Not all host groups are retrieved from Stealthwatch when multiple domains are used. |
| CSCvt45686 | AQ reporting for radio 1 has no data, whereas radio 0 shows data. |
| CSCvt46026 | Stealthwatch association shows "Error undefined." |
| CSCvt63046 | Taskmgr-data crashes with an out-of-memory error. |
| CSCvt68900 | The Client 360 page keeps spinning when the username contains special characters. |
| CSCvt76587 | The Inventory page and Provisioning page display no devices. |
| CSCvt81829 | Software Image Management (SWIM) activation script prechecks fail during database communication. |

| Bug Identifier | Headline |
|---|---|
| CSCvt87433 | Cisco DNA Center fails to collect inventory from an ISR 4000 series router, due to a constraint violation error with the configuredActiveModules object. |
| CSCvu03730 | A Cisco Catalyst 9800 Series Wireless Controller is unmonitored in Cisco DNA Center because the "sdn-network-infra-iwan" certificate is not installed. |
| CSCvu21987 | Addition of backup server results in an internal server error. |
| CSCvu28044 | In a scaled fabric setup, when you retry a failed operation, the spf-service-manager-service restarts with out-of-memory errors. |

The following table lists the resolved bugs in Cisco DNA Center, Release 1.3.3.4.

***Table 18: Resolved Bugs in Cisco DNA Center, Release 1.3.3.4***

| Bug Identifier | Headline |
|---|---|
| CSCvq40879 | Unable to restore a backup from Cisco DNA Center 1.3.0.2. |
| CSCvr12994 | Cisco DNA Center: Stored cross-site scripting vulnerability. |
| CSCvr93473 | High CPU load and more than 3000 Docker containers in init state. |
| CSCvr95235 | Telemetry agent ends up constantly in CrashLoopBackOff error state on both active and standby clusters. |
| CSCvs18203 | Cisco DNA Center search service doesn't work if the MongoDB connection is unstable. |
| CSCvs19560 | Mismatch between client data shown in maps and Assurance, and actual client data. |
| CSCvs33846 | Validate before a node joins the cluster. |
| CSCvs42952 | After enabling maximal visibility, the flow monitor configuration is sent to the wrong L3 port. |
| CSCvs48901 | Changing the Cisco ISE VIP leads to a loss of security group tag (SGT) configuration on ports. |
| CSCvs78950 | The Cisco Catalyst 9800 Series Wireless Controller telemetry connection remains in the Connecting state, and no Assurance data corresponding to the Catalyst 9800 Series Wireless Controller is displayed in Cisco DNA Center. |
| CSCvs85704 | Cisco DNA Center fails to decrypt passwords after restoring from a backup. |
| CSCvs86018 | An AP provisioning failure occurs due to missing "OwningEntityId" details for the wireless controller. |
| CSCvs88980 | Wireless controller fails inventory collection with the exception "ManagedNetworkElement was altered." |
| CSCvt05278 | Cisco DNA Center upgrade from 1.3.1.4 to 1.3.3.1 fails when the network contains Cisco Nexus 7000 devices. |
| CSCvt06511 | Cisco DNA Center fails to collect inventory data from the Meraki dashboard due to an unknown error. |
| CSCvt07586 | Cisco DNA Center 1.3.0.2 to 1.3.0.6 upgrade triggers a device provision switchport change notification. |
| CSCvt13963 | Fabric provisioning fails after adding vManage to Cisco DNA Center 1.3.3.1. |

| Bug Identifier | Headline |
|---|---|
| CSCvt19768 | During failover, isolate recovery fails because the maintenance service is not available. |
| CSCvt20541 | The configuration object "DNAC_ACL_WEBAUTH_REDIRECT" gets removed and readded to a managed wireless controller when adding or removing a dot1x/PSK SSID. |
| CSCvt34006 | Duplicate migration status causing causes provisioning operations to fail on duplicate key CVLAN_EXAUTH. |
| CSCvt34300 | After migration, adding ext-node shows a banner due to an error. |
| CSCvt39849 | The Client Summary report does not show the entire site hierarchy. |
| CSCvt54592 | Multiple devices fail inventory collection after Cisco DNA Center is upgraded to 1.3.3.1 RADIUS key size. |

The following table lists the resolved bugs in Cisco DNA Center, Release 1.3.3.3.

***Table 19: Resolved Bugs in Cisco DNA Center, Release 1.3.3.3***

| Bug Identifier | Headline |
|---|---|
| CSCvp34431 | Cisco DNA Center 1.3 uses a longer JWT token, which may cause the integration with a wireless LAN controller to fail, causing incoming Assurance data to stop. |
| CSCvq31127 | Backup fails with a "Taskname=BACKUP.fusion:postgres" error. |
| CSCvs22065 | A three-node setup may become unresponsive after over 100 days of service. |
| CSCvs50957 | Device provisioning fails with "Error in authentication profile processing." |
| CSCvs53995 | A seed device fails inventory collection due to a switchport constraint violation exception. |
| CSCvs68068 | Keepalived: VRRP-script node health check false alarm causes VIP jitters. |
| CSCvs69931 | Cisco DNA Center may fail to synchronize inventory from Cisco Catalyst 9300 edge switches after upgrading to Cisco DNA Center 1.3.1.4. This problem is seen only when there are non-Cisco devices connected to the switch, and CDP is enabled. |
| CSCvs84253 | Site comparison: Building drop-down list does not work due to a mismatch in sqlQuery. |
| CSCvt00402 | A Cisco Catalyst 3000 switch with a 1.6-GB flash size cannot perform a software image upgrade between 16.12.x images. |

| Bug Identifier | Headline |
|---|---|
| CSCvt23943 | An SPF deduplication error occurs during the SDA migration workflow.<br>This bug is resolved in 1.3.3.3 only when you update the following packages to the versions listed in New and Changed Information, on page 4:<br>• Automation - Base<br>• Cisco DNA Center UI<br>• Cisco SD-Access<br>• Machine Reasoning<br>• Network Controller Platform |
| CSCvt65855 | While restoring a backup of a Cisco DNA Center installation that had been upgraded to 1.3.3.3 to a new installation from an ISO image of 1.3.3.3, the restore operation fails due to the Machine Reasoning Engine package version. The following error message is generated:<br>`{'version': '1.0', 'error': {'message': 'Exception while performing preRestore: Following model plugins deployed in backup are from a higher version than current deployment: [semantic-reasoner-event-model-plugin:7.6.111.62002, cnsr-model-plugin:7.6.111.62002, common-view-model-plugin:7.6.111.62002]', 'datasource': 'postgres', 'status': 'error', 'appstack': 'fusion', 'lastUpdateTime': 0}`<br>This bug is resolved in 1.3.3.3 only when you update the following packages to the versions listed in New and Changed Information, on page 4:<br>• Automation - Base<br>• Cisco DNA Center UI<br>• Cisco SD-Access<br>• Machine Reasoning<br>• Network Controller Platform |

The following table lists the resolved bugs in Cisco DNA Center, Release 1.3.3.1.

***Table 20: Resolved Bugs in Cisco DNA Center, Release 1.3.3.1***

| Bug Identifier | Headline |
|---|---|
| CSCvs66857 | After upgrading from Cisco DNA Center 1.3.1.4 to 1.3.3.0, if you try to create a new SGT with multiple virtual networks (VNs) on the **Policy** page, the following error message is generated:<br>`errorKey:NCSP10000 errorCode:InternalError failureReason:Unable to find cfs VirtualNetworkContext` |

| Bug Identifier | Headline |
|---|---|
| CSCvs74635 | Wireless connectivity problems might occur after upgrading to Cisco DNA Center 1.3.0.6. If the IP pool association from the AAA override for the client is not defined as part of Cisco DNA Center, host onboarding could result in connectivity problems. This is because with Cisco DNA Center 1.3.0.6, all IP pools that are not associated with a fabric SSID are deleted from the wireless controller during reprovisioning. |

The following table lists the resolved bugs in Cisco DNA Center, Release 1.3.3.0.

***Table 21: Resolved Bugs in Cisco DNA Center, Release 1.3.3.0***

| Bug Identifier | Headline |
|---|---|
| CSCvq40037 | LAN automation PnP: An image upgrade fails for a Cisco Catalyst 9500 device. |
| CSCvq65765 | After upgrading to Cisco DNA Center and enabling the Autoconf feature, macro configurations are not removed from extended nodes. |
| CSCvq65784 | When IPv4 multicasting is enabled on an edge device, Cisco DNA Center does not push the **ip igmp explicit-tracking** command to the Layer 2 handoff VLAN on the corresponding border device. |
| CSCvq85254 | The AP Intelligent Capture page has no data after a device image is changed and reloaded. |
| CSCvq92221 | Devices do not appear in the "Monitored" section in Assurance because one device remains in Partial Collection Failure state. |
| CSCvq94904 | The Overall Health map shows incorrect information. |
| CSCvr02321 | The SMU API count result shows 2, but the GUI displays 1 for a Cisco ISR 4331 router. |
| CSCvr04915 | Provisioning is blocked on a new controller in a fabric-provisioned site. |
| CSCvr10816 | For some devices, provisioning fails at the Activate VNFs stage with the following error:<br>`The device to be provisioned does not exist` |
| CSCvr13984 | Cisco DNA Center does not manage an IE 5000 after a reload with 1-G SFPs inserted in 10-G uplink ports. |
| CSCvs52742 | Cannot access files with 110,000 directories created by cfg-archiver; backup times out. |
| CSCvr54376 | A vulnerability in Cisco DNA Center software could allow an unauthenticated remote attacker access to sensitive information on an affected system.<br>The vulnerability is due to improper handling of authentication tokens by the affected software. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker access to sensitive device information, which includes configuration files.<br>Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.<br>This advisory is available at the following link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dna-info-disc-3bz8BCgR |

| Bug Identifier | Headline |
|---|---|
| CSCvr72551 | Multiple vulnerabilities in the web-based management interface of Cisco DNA Center software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device.<br><br>The vulnerabilities exist because the web-based management interface on an affected device does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.<br><br>There are no workarounds that address these vulnerabilities.<br><br>This advisory is available at the following link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-mlt-xss-zUzbcdEV |

# 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 the required 2.6 patch 1 or 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 or 2.4 patch 7 or later, and retry the Cisco DNA Center upgrade.

### 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 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.

### HA Limitation

In this release, Cisco DNA Center provides HA support only for Automation and Cisco SD-Access. HA for Assurance is not supported.

### 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.
- The Cisco ISE internal certificate authority must issue the pxGrid certificate for Cisco DNA Center.

### 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.
- Cisco DNA Center does not support multicast across multiple fabric sites that are connected by an SDA transit network.

### Brownfield 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 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 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 brownfield provisioning.
- The authentication and accounting servers must have the same IP addresses for them to be learned through brownfield 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.

### Application Hosting Limitation

In this release of Cisco DNA Center, application hosting is not supported on stacked switches.

### 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 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.

### AAA Provisioning Limitation

Cisco DNA Center does not support provisioning AAA on Cisco Nexus 7000 devices.

### 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>*

## Get Assistance from the Cisco TAC

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

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

## Related Documentation

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

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

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