



# Release Notes for Cisco DNA Center, Release 2.3.5.x

**First Published:** 2022-12-21

**Last Modified:** 2024-05-28

## Release Notes for Cisco DNA Center, Release 2.3.5.x

The latest release, Cisco DNA Center 2.3.5.6, is available in a phased rollout. Until the software becomes generally available, contact your Cisco sales representative to request this release. Upon completion of the phased rollout, Cisco DNA Center will be made generally available to all customers.

This document describes the features, limitations, and bugs for Cisco DNA Center, Release 2.3.5.x.

For links to all of the guides in this release, see [Cisco DNA Center 2.3.5 Documentation](#).

### Change History

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

Date	Change	Location
2024-05-28	Added the open bug <a href="#">CSCwk04523</a> .	<a href="#">Open Bugs</a> , on page 30
2024-05-13	Added the list of packages in 2.3.5.6.	<a href="#">Package Versions in Cisco DNA Center, Release 2.3.5.x</a> , on page 3
	Added the Resolved Bugs table for 2.3.5.6.	<a href="#">Resolved Bugs</a> , on page 34
	Added the open bugs for 2.3.5.6.	<a href="#">Open Bugs</a> , on page 30
	Updated the supported Cisco Integrated Management Controller (Cisco IMC) versions.	<a href="#">Supported Firmware</a> , on page 26
	Noted that in 2.3.5.6, you cannot integrate your Network Analysis Module (NAM) or vNAM server with Cisco DNA Center.	<a href="#">Deprecated Features</a> , on page 25
	Added information in 2.3.5.6 about AI-enhanced RRM guidelines for scale provisioning.	<a href="#">Limitations and Restrictions</a> , on page 60
2024-03-07	Added information in 2.3.5.4 about enhancements to FlexConnect settings modifications for existing SSIDs.	<a href="#">New and Changed Features in Cisco DNA Center</a> , on page 6

Date	Change	Location
2023-12-11	Cisco DNA Center 2.3.5.5 contains fixes for the critical issues listed in the <a href="#">Resolved Bugs, on page 34</a> list.  We recommend that customers on all earlier Cisco DNA Center releases, including the 2.3.5.x releases, upgrade to Cisco DNA Center 2.3.5.5.	<a href="#">Resolved Bugs, on page 34</a>
	Added the list of packages in 2.3.5.5.	<a href="#">Package Versions in Cisco DNA Center, Release 2.3.5.x, on page 3</a>
2023-10-20	Added a limitation about the site hierarchy for a Rogue and aWIPS report.	<a href="#">Limitations and Restrictions, on page 60</a>
2023-10-19	Added the Resolved Bugs table for the 2.3.5.4-70852-HF3 hot fix.	<a href="#">Resolved Bugs, on page 34</a>
	Added the list of packages in 2.3.5.4-70852-HF3.	<a href="#">Package Versions in Cisco DNA Center, Release 2.3.5.x, on page 3</a>
2023-10-12	Added the Resolved Bugs table for the 2.3.5.3-70194-HF5 hot fix.	<a href="#">Resolved Bugs, on page 34</a>
	Added the list of packages in 2.3.5.3-70194-HF5.	<a href="#">Package Versions in Cisco DNA Center, Release 2.3.5.x, on page 3</a>
2023-10-03	Added <a href="#">CSCwe98803</a> , which is resolved in 2.3.5.4.	<a href="#">Resolved Bugs, on page 34</a>
2023-09-27	Updated the list of packages in 2.3.5.3.	<a href="#">Package Versions in Cisco DNA Center, Release 2.3.5.x, on page 3</a>
2023-09-14	Added support for Cisco DNA Center on AWS, which enables you to deploy Cisco DNA Center as a virtual appliance on Amazon Web Services (AWS).	<a href="#">Supported Virtual Appliance, on page 27</a>
2023-08-24	Added the list of packages in 2.3.5.4.	<a href="#">Package Versions in Cisco DNA Center, Release 2.3.5.x, on page 3</a>
	Added the Resolved Bugs table for 2.3.5.4.	<a href="#">Resolved Bugs, on page 34</a>
	Added the open bugs for 2.3.5.4.	<a href="#">Open Bugs, on page 30</a>
2023-08-18	Added a limitation about custom applications.	<a href="#">Limitations and Restrictions, on page 60</a>
2023-07-17	Previously, the <i>Cisco DNA Center Release Notes</i> and the <i>Cisco DNA Center Platform Release Notes</i> 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.	<a href="#">Limitations and Restrictions, on page 60</a>
2023-06-07	Noted that if you run Cisco DNA Center in IPv6 mode, LAN automation is not supported.	<a href="#">Limitations and Restrictions, on page 60</a>

Date	Change	Location
2023-05-19	Added information about using the Validation Tool to run preupgrade checks.	<a href="#">Upgrade to the Latest Cisco DNA Center Release, on page 3</a>
2023-05-08	Added the list of packages in 2.3.5.3.	<a href="#">Package Versions in Cisco DNA Center, Release 2.3.5.x, on page 3</a>
	Added the Resolved Bugs table for 2.3.5.3.	<a href="#">Resolved Bugs, on page 34</a>
	Added the list of new walkthroughs for 2.3.5.3.	<a href="#">New and Changed Features in Interactive Help, on page 21</a>
	Explained the licensing changes in 2.3.5.3.	<a href="#">Licensing Changes, on page 22</a>
	Added a limitation about In-Service Software Upgrade (ISSU).	<a href="#">Limitations and Restrictions, on page 60</a>
2022-12-21	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 2.3.5.x

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

Package Name	Release 2.3.5.6	Release 2.3.5.5	Release 2.3.5.4		Release 2.3.5.3		Release 2.3.5.0
<b>Release Build Version</b>							
Release Version	2.3.5.6.70143	2.3.5.5.70026	2.3.5.4-70852-HF3	2.3.5.4.70852	2.3.5.3-70194-HF5	2.3.5.3.70194	2.3.5.0.70586
<b>System Updates</b>							
System	1.7.1127	1.7.1013	1.7.1013		1.7.905		1.7.832
System Commons	2.1.617.60344	2.1.616.60023	2.1.614.61521		2.1.613.61093		2.1.610.60911
<b>Package Updates</b>							
Access Control Application	2.1.617.60344	2.1.616.60023	2.1.614.61521		2.1.613.61093		2.1.610.60911
AI Endpoint Analytics	1.9.859	1.9.823	1.9.805		1.9.704		1.9.613
AI Network Analytics	2.11.31.410	2.11.27.394	2.11.27.394		2.11.24.376		2.11.19.356

Package Name	Release 2.3.5.6	Release 2.3.5.5	Release 2.3.5.4	Release 2.3.5.3	Release 2.3.5.0
Application Hosting	2.1.02402211124	2.1.02307250922	2.1.02307250922	2.1.02304051333	2.1.02212150608
Application Policy	2.1.617.117247	2.1.616.117003	2.1.614.117979	2.1.613.170209	2.1.610.117535
Application Registry	2.1.617.117247	2.1.616.117003	2.1.614.117979	2.1.613.170209	2.1.610.117535
Application Visibility Service	2.1.617.117247	2.1.616.117003	2.1.614.117979	2.1.613.170209	2.1.610.117535
Assurance - Base	2.3.5.551	2.3.5.475	2.3.5.475	2.3.5.329	2.3.5.271
Assurance - Sensor	2.3.5.536	2.3.5.408	2.3.5.408	2.3.5.312	2.3.5.269
Automation - Base	2.1.617.60344	2.1.616.60023	2.1.614.61521	2.1.613.61121	2.1.610.60911
Automation - Intelligent Capture	2.1.617.60344	2.1.616.60023	2.1.614.61521	2.1.613.61093	2.1.610.60911
Automation - Sensor	2.1.617.60344	2.1.616.60023	2.1.614.61521	2.1.613.61093	2.1.610.60911
Cisco DNA Center Global Search	1.10.1.11	1.10.1.11	1.10.1.11	1.10.1.11	1.10.1.11
Cisco DNA Center Platform	1.10.1.230	1.10.1.188	1.10.1.188	1.10.1.143	1.10.1.103
Cisco DNA Center UI	1.7.3.299	1.7.3.292	1.7.3.292	1.7.3.277	1.7.3.236
Cisco Identity Services Engine Bridge	2.1.617.510	2.1.614.510	2.1.614.510	2.1.610.476	2.1.610.476
Cisco Umbrella	2.1.617.590153	2.1.614.590510	2.1.614.590510	2.1.613.590114	2.1.610.590253
Cloud Connectivity - Contextual Content	2.6.1.350	2.6.1.350	2.6.1.350	2.6.1.350	2.6.1.350
Cloud Connectivity - Data Hub	1.10.48	1.10.48	1.10.48	1.10.47	1.10.40
Cloud Connectivity - Tethering	2.31.1.55	2.31.1.55	2.31.1.55	2.31.1.53	2.31.1.43
Cloud Device Provisioning Application	2.1.617.60344	2.1.616.60023	2.1.614.61521	2.1.613.61093	2.1.610.60911

Package Name	Release 2.3.5.6	Release 2.3.5.5	Release 2.3.5.4	Release 2.3.5.3		Release 2.3.5.0
Command Runner	2.1.617.60344	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
Device Onboarding	2.1.617.60344	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
Disaster Recovery	2.1.617.360015	2.1.614.360049	2.1.614.360049	2.1.613.360017		2.1.610.360079
Disaster Recovery—Witness Site	2.1.617.370008	2.1.614.370026	2.1.614.370026	2.1.613.370006		2.1.610.370032
Group-Based Policy Analytics	2.3.5.32	2.3.5.30	2.3.5.30	2.3.5.27		2.3.5.27
Image Management	2.1.617.60344	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
Machine Reasoning	2.1.617.210108	2.1.616.210007	2.1.614.210567	2.1.613.210134		2.1.610.210377
NCP - Base	2.1.617.60344	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
NCP - Services	2.1.617.60344	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
Network Controller Platform	2.1.617.60344	2.1.616.60023	2.1.614.61521	2.1.613.61121	2.1.613.61093	2.1.610.60911
Network Data Platform - Base Analytics	2.3.5.306	2.3.5.97	2.3.5.97	2.3.5.44		2.3.5.32
Network Data Platform - Core	1.9.1116	1.9.1078	1.9.1078	1.9.1039		1.9.1011
Network Data Platform - Manager	1.9.1013	1.9.1013	1.9.1013	1.9.1013		1.9.1010
Network Experience Platform - Core	2.1.617.60344	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
Path Trace	2.1.617.60344	2.1.616.60023	2.1.614.61521	2.1.613.61093		2.1.610.60911
RBAC Extensions	2.1.617.1900001	2.1.614.1900017	2.1.614.1900017	2.1.613.1900011		2.1.613.1900008
Rogue and aWIPS	2.7.0.52	2.7.0.46	2.7.0.46	2.7.0.41		2.7.0.36
SD-Access	2.1.617.60344	2.1.616.60023	2.1.614.61521	2.1.613.61121	2.1.613.61093	2.1.610.60911
Stealthwatch Security Analytics	2.1.617.1090150	2.1.616.1090003	2.1.614.1090427	2.1.613.1090136		2.1.610.1090258

Package Name	Release 2.3.5.6	Release 2.3.5.5	Release 2.3.5.4	Release 2.3.5.3	Release 2.3.5.0
Support Services	2.1.614.880027	2.1.614.880027	2.1.614.880027	2.1.613.880003	2.1.610.880024
System Remediation	1.0.102	1.0.51	1.0.2	1.0.2	—
Wide Area Bonjour	2.4.615.75154	2.4.614.75573	2.4.614.75573	2.4.610.75310	2.4.610.75310

## New and Changed Information

### New and Changed Features in Cisco DNA Center

*Table 1: New and Changed Features for Cisco DNA Center, Release 2.3.5.6*

Feature	Description
Enhancements to AP Provisioning for N+1 High Availability	If you are using N+1 High Availability (HA) and modify any nonflex SSIDs that are already provisioned on the primary and secondary controllers to flex SSIDs (or conversely), ensure that the states of WLANs are consistent across both the primary and secondary controllers on the corresponding site.
Enhancements to Channel Width Selection for APs in Dual Radio Mode	In earlier releases, if the dual radio mode was enabled on an AP, its slot 2 couldn't be in the <b>Client-Serving</b> or <b>Monitor</b> radio role with the 160 MHz channel width.  Effective with this release, if the dual radio mode is enabled on an AP, its slot 2 can't be in the <b>Client-Serving</b> radio role with the 160 MHz channel width.
Enhancements to the Configure AI RF Profile Workflow	In earlier releases, in the <b>Configure AI RF Profile</b> workflow, when you select a site, Cisco DNA Center selected all the existing sites that are managed by the same wireless controller as the impacted locations. This selection included the sites where AI-Enhanced RRM was already enabled.  Effective with this release, when you select a site, Cisco DNA Center doesn't select the existing AI-Enhanced RRM-enabled sites as impacted locations to avoid unnecessary reprovisioning of these sites.  <b>Note</b> To modify any settings for the existing AI-Enhanced RRM-enabled sites, you must select the corresponding sites during the workflow.
Enhancements to VLAN Creation for FlexConnect SSIDs	For the FlexConnect SSIDs, VLANs are not automatically created on the Cisco Catalyst 9800 Series Wireless Controller during provisioning. Instead, the interface and VLANs that are mapped to the wireless network profile are created on the Flex profile during AP provisioning.

Table 2: New and Changed Features for Cisco DNA Center, Release 2.3.5.5

Feature	Description
Recommended Release	<p>Cisco DNA Center 2.3.5.5 contains fixes for critical issues.</p> <p>We recommend that customers on all earlier Cisco DNA Center releases, including the 2.3.5.x releases, upgrade to Cisco DNA Center 2.3.5.5.</p>
Enhancements to Default AP Profiles During Upgrade	<p>In earlier releases, the default AP profile was pushed to the wireless controller during upgrade.</p> <p>When you upgrade to this release from an earlier version, by default, Cisco DNA Center doesn't push the default AP profile to the wireless controller. To update the default AP profile on the wireless controller, you must explicitly save it on the <b>Design &gt; Network Settings &gt; Wireless &gt; AP Profiles</b> window. After you save the default AP profile, if there is a difference between the current wireless controller configuration and the AP profile configuration saved on Cisco DNA Center, the default AP profile is pushed to the wireless controller during subsequent reprovisioning.</p>

Table 3: New and Changed Features for Cisco DNA Center, Release 2.3.5.4

Feature	Description
Ability to Assign Ports for Uplink Ports	<p>Effective with this release, you can assign ports for the uplink ports. Choose <b>Provision &gt; Fabric Sites</b> and click the fabric site. Under <b>Host Onboarding &gt; Port Assignment</b>, assign ports for the uplink ports. In earlier releases, you could assign ports for the uplink ports only for extended node devices.</p>
AP Location Configuration for PnP Onboarding	<p>Effective with this release, you can configure the site assigned during the PnP claim as the AP location for PnP onboarding.</p> <p>In the <b>System &gt; Settings &gt; Device Settings &gt; PnP AP Location</b> window:</p> <ul style="list-style-type: none"> <li>• If you check the <b>Configure AP Location</b> check box, Cisco DNA Center configures the assigned site as the AP location for PnP onboarding.</li> <li>• If you uncheck the <b>Configure AP Location</b> check box, Cisco DNA Center doesn't configure the AP location during PnP onboarding and you can use the <b>Configure Access Points</b> workflow to configure the AP location.</li> </ul> <p>This check box is unchecked by default.</p> <p><b>Note</b> These settings aren't applicable for the AP provisioning or other day-<i>n</i> operations.</p>
Enhancements to Access Control Lists for Central Web Authentication SSIDs of Guest Wireless Network	<p>Effective with this release, Cisco DNA Center-generated preauthentication Access Control Lists (ACL) are created only for the configured AAA or PSN servers for Central Web Authentication (CWA) SSIDs of guest wireless networks.</p>
Enhancements to Admin Status of Radio Bands in RF Profiles for Cisco AireOS Wireless Controllers	<p>Effective with this release, for Cisco AireOS Wireless Controllers, if you disable the Admin status of a band in the RF profile and reprovision the wireless controller or AP, Cisco DNA Center creates the RF profile for the corresponding band and maps it to the AP group (instead of configuring it as <b>None</b>) and disables the Admin status of all radios of the corresponding band on the APs.</p>

Feature	Description
Enhancements to FlexConnect Settings Modifications for Existing SSIDs	<p>If you modify any nonflex SSIDs that are already provisioned on a wireless controller to flex SSIDs (or conversely), you must reprovision the wireless controller to ensure that the expected intent is configured on the wireless controller.</p> <p>If you modify the VLAN ID value in the <b>Local to VLAN ID</b> field of an existing SSID and reprovision the AP without reprovisioning the wireless controller, the latest value of the VLAN ID is updated in the flex profile used by the AP.</p> <p><b>Note</b> If the same flex profile is used by other APs, these APs will also have the updated local VLAN ID.</p>
Enhancements to RF Profile Updates for Cisco AireOS Wireless Controllers	<p>In earlier releases, for Cisco AireOS Wireless Controllers, if you modify any configuration in an RF profile that is already provisioned on a wireless controller, Cisco DNA Center resets the corresponding radio.</p> <p>Effective with this release, for Cisco AireOS Wireless Controllers, if you modify the DCA channels or data rates for an RF profile that is already provisioned on a wireless controller, Cisco DNA Center resets the corresponding radio.</p>
Support for Manual Data Refresh to Track the Replacement Status in the AP Refresh Workflow	<p>In the <b>Access Point Refresh</b> workflow, to view the latest AP replacement status, you can use the <b>Refresh Data</b> option.</p> <p><b>Note</b> Effective with this release, Cisco DNA Center doesn't refresh the data automatically.</p>
Support for Static IP Address for Wireless Management Interface During Provisioning of Cisco Catalyst 9800 Series Wireless Controller	<p>Effective with this release, you must configure a static IP address for the wireless management interface on the Cisco Catalyst 9800 Series Wireless Controller to prevent provisioning failure.</p>

Table 4: New and Changed Features for Cisco DNA Center, Release 2.3.5.3

Feature	Description
Dynamic Channel Assignment (DCA) Validation	<p>DCA channel support is based on the regulatory domain of the device. During AP provisioning with an RF profile selected, out of all the DCA channels configured on the RF profile only the supported channels as per the country code are considered and the unsupported channels are ignored. You can view the list of unsupported channels in the AP preprovision summary window.</p>
Enhancements to Accounting Server Configuration	<p>Effective with this release, you must configure an accounting server for an SSID to push the accounting configuration for the SSID.</p>
Enhancements to AP Configuration Workflow	<p>The <b>Configure Access Points</b> workflow has the following enhancements:</p> <ul style="list-style-type: none"> <li>• The <b>Antenna Name</b> parameter has been replaced with the <b>Antenna Gain</b> parameter. The antenna name selected in this workflow isn't reflected in wireless maps.</li> <li>• The <b>AP Height</b>, <b>Azimuth</b>, and <b>Elevation</b> parameters have been removed. You can configure these parameters in the <b>Design &gt; Network Hierarchy</b> window.</li> <li>• You can select a maximum of 2000 sites in the <b>Select Access Points</b> window.</li> </ul>



Feature	Description
Enhancements to AP Location Configuration	During AP provisioning and AP Plug and Play (PnP) onboarding, Cisco DNA Center doesn't configure the assigned site as the AP location. You can configure the AP location using the <b>Configure Access Points</b> workflow.
Enhancements to Application Hosting on APs	When the <b>App Hosting Status</b> of an AP is <b>Ready</b> , to configure the updates on the AP, you can use the <b>Resync</b> option.
Enhancements to Authentication using AAA Server for Wireless Networks	Effective with this release, you must configure an AAA server for an SSID to push the authentication configuration for the SSID. If an AAA server is not configured for the SSID, Cisco DNA Center pushes the <b>aaa authentication dot1x default local</b> command to the wireless controller and the default method list that points to local authentication is mapped to the SSID.
Enhancements to Editing RF Profiles	<p>Effective with this release, when you update an RF profile that is already provisioned on a wireless controller and AP, you must reprovision either the wireless controller or AP. Wireless controller reprovisioning also pushes the RF profiles updates to the devices and AP reprovisioning is not necessary.</p> <p>If you don't need the RF profile updates during the wireless controller reprovisioning, you can check the <b>Skip AP Provision</b> check box.</p>
Enhancements to RF Profiles	<p>Effective with this release, for Cisco Catalyst 9800 Series Wireless Controllers, disabling a radio band on the RF profile doesn't disable the Admin status of the respective radios on all APs that use the RF profile. Instead, Cisco DNA Center disables the Admin status of the corresponding RF profile.</p> <p><b>Note</b> When the Admin status of a radio band on the RF profile is in disabled state and you upgrade to Release 2.3.5.3 from Release 2.3.3.6 or earlier, if you reprovision the wireless controller or AP:</p> <ul style="list-style-type: none"> <li>• Cisco DNA Center creates the RF profile for the corresponding radio band with Admin status as disabled.</li> <li>• Cisco DNA Center updates the RF profile mapping in the RF tag on the device from <b>Global Config</b> to the newly created RF profile.</li> </ul>
Enhancements to Site Tags, Policy Tags, and AP Zone Provisioning	<p>Site tags, policy tags, and AP zone provisioning have the following enhancements:</p> <ul style="list-style-type: none"> <li>• If an AP zone is already provisioned on an AP and you update the AP zone configuration, you must reprovision the wireless controller. Reprovisioning the AP is not necessary.</li> <li>• Newly added custom site tag and policy tag configurations are applied only when you provision the APs. Provisioning the wireless controller alone doesn't configure the new custom tags on the APs. If there are any updates to the tags after the first provisioning, you must reprovision the wireless controller or APs.</li> </ul>

Table 5: New and Changed Features for Cisco DNA Center, Release 2.3.5.0

Feature	Description
Advanced WLAN Parameters Configuration Support for Enterprise and Guest Wireless Networks	You can configure the following advanced WLAN parameters while creating SSIDs for enterprise and guest wireless networks: <ul style="list-style-type: none"> <li>• <b>AAA Override</b></li> <li>• <b>Configure MPSK</b></li> <li>• <b>Protected Management Frame (802.11w)</b></li> <li>• <b>Coverage Hole Detection</b></li> </ul>
Basic RF Profile and AI RF Profile Enhancements	You can configure the following settings for basic radio frequency (RF) profiles: <ul style="list-style-type: none"> <li>• Coverage hole detection</li> <li>• Flexible Radio Assignment (FRA)</li> <li>• 802.11ax</li> </ul> You can configure the following settings for AI RF profiles: <ul style="list-style-type: none"> <li>• Coverage hole detection</li> <li>• 802.11ax</li> </ul>
Cisco DNA Center Journey Map	The Cisco DNA Center journey map shows various capabilities provided by Cisco DNA Center and its usage.
Client Rate Limit Configuration Support for Enterprise and Guest Wireless Networks	You can configure the client rate limit on Cisco IOS XE devices while creating SSIDs for enterprise and guest wireless networks.
Compliance Support Extended for Cisco Umbrella	You can check compliance for switches or Cisco Embedded Wireless Controllers configured with Cisco Umbrella. You can view any violations under <b>Workflow</b> in the <b>Compliance Summary</b> window.
Compliance Support Extended for Network Settings	You can check compliance for device network settings. You can view any violations under <b>Network settings</b> in the <b>Compliance Summary</b> window.
Detect Conflicts in a CLI Template	You can detect potential design conflicts and run-time conflicts in the CLI templates for switching, SD-Access, and fabric.
Enhancements to Default Configuration of Fast Transition Over Distributed Systems for SSIDs	Effective with this release, fast transition over a distributed system ( <b>Over the DS</b> check box) is disabled by default for SSIDs for guest and enterprise wireless networks.
Exclude Interfaces in Application Visibility Service Enablement	You can exclude or include interfaces in the Application Visibility service enablement.
Fix Compliance Violations	Cisco DNA Center provides you with an automated fix for device compliance violations that are identified during a compliance run.

Feature	Description
HTTPS Protocol Support for Software Image Management	HTTPS protocol support is extended for software image management on Cisco Embedded Wireless Controllers.
PSC Enforcement Support for RF Profiles	You can enable Preferred Scanning Channel (PSC) enforcement for the 6-GHz radio type for basic RF profiles and AI RF profiles.
Resilient Ethernet Protocol (REP) Ring Device Support (Nonfabric)	REP Ring support for nonfabric devices is extended for S5800.
Support for AP Authorization Configuration	You can configure a list of authorized APs. You can configure local and AAA authorization for APs using their MAC address, serial number, or both.
Support for AP Power Profiles	You can create AP power profiles for Cisco Wireless Controllers running Cisco IOS XE Release 17.10.1 and later. You can assign the AP power profile to APs by associating it with an AP profile. You can define multiple rules for the AP power profile and specify the sequences of the rules.
Support for Custom AP Profiles	<p>AP profiles consolidate the AP authentication settings, aWIPS, rogue management, and mesh settings. AP profiles allow you to manage and provision APs.</p> <p>Cisco DNA Center provides a default AP profile for Cisco IOS XE devices and Cisco AireOS devices. You can create custom AP profiles for Cisco IOS XE devices and Cisco AireOS devices.</p> <p><b>Note</b> If there are any out-of-band custom AP profiles that are created directly on the wireless controller and used with Cisco DNA Center running earlier than Release 2.3.5, ensure that you create a custom AP profile on Cisco DNA Center with same name and map it to the custom site tag to retain the configuration.</p>
Support for Reuse of AP Groups and Flex Groups Within an Area	While creating a network profile for wireless, you can use the same AP group and flex group across sites (buildings or floors) within an area.
Template Hub	<p>You can filter CLI templates based on Project Name, Template Language, Device Family, Device Series, Commit State, and Provision Status from <b>Tools &gt; Template Hub</b>.</p> <p>You can attach the CLI template to network profiles in the <b>Template Hub</b> window. You can also create a new network profile.</p>

## New and Changed Features in Cisco DNA Assurance

Feature	Description
AI-Enhanced RRM Enhancements - FRA Support	<p>Cisco DNA Center displays the <b>FRA Changes</b> dashlet in the <b>AI-Enhanced RRM</b> dashboard. This new dashlet displays the total number of Flexible Radio Assignment (FRA)-capable and FRA-enabled radios for the following modes:</p> <ul style="list-style-type: none"> <li>• 2.4-GHz radio</li> <li>• 5-GHz radio</li> <li>• Monitor</li> </ul>

Feature	Description
Automatic Issue Resolution	With this release, the system automatically resolves the following issue types: <ul style="list-style-type: none"> <li>• Stack Port Link has failed</li> <li>• Stack Member Removal</li> </ul>
Cisco SD-Access Assurance - Fabric KPI Enhancements	With this release, the following Fabric Site KPIs are included: <ul style="list-style-type: none"> <li>• <b>CTS Environment Data Download</b></li> <li>• <b>BGP Session from Border to Peer Node for INFRA VN</b></li> <li>• <b>BGP Session from Border to Control Plane</b></li> </ul>
Cisco SD-Access Assurance - Transits KPI Enhancements	With this release, the following Transits KPIs are included: <ul style="list-style-type: none"> <li>• <b>BGP Session from Border to Transit Control Plane</b></li> </ul>
Cisco SD-Access Assurance - VN Services KPI Enhancements	With this release, the following VN Services KPIs are included: <ul style="list-style-type: none"> <li>• <b>BGP Session from Border to Peer Node</b></li> <li>• <b>Remote Internet Availability</b></li> </ul>
Client-360 Dashboard Enhancements	In the <b>Summary</b> dashboard on the Client-360 window, you can view a list of onboarding, roaming, and connectivity issues for a particular client. You can click the hyperlinked issues to view details about the issue the client experienced at a specific location.
DHCP Dashboard Enhancement	You can view a breakdown of DHCP failures, such as DHCP decline and DHCP Negative Acknowledgment (NACK). These failures are also displayed in the Event Viewer in the <b>Client-360</b> window.
DNS Dashboard	You can view and monitor all the DNS server transactions reported by wireless controllers in your network. <b>Note</b> If your network contains existing devices with application telemetry enabled, you must disable and then re-enable application telemetry before you can see any data in the DNS dashboard.
Enhanced Site Analytics	The KPIs on the Site Analytics Health Dashboard window are subdivided into more granular data points. Onboarding now shows both onboarding attempts and onboarding duration. Roaming shows both roaming attempts and roaming duration.
Flex/Fabric mode support for Application Experience	From this release, Application Experience supports Flex/Fabric mode on Cisco 9800 Series Wireless Controllers.
Issue Notes	You can add a comment, such as the TAC case number or other information, to an issue.
Issue Resolution	You can view whether an issue is resolved automatically or manually. In the <b>Issue Settings &gt; Global Profile</b> window, the <b>Issue Resolution</b> column displays either <b>Auto</b> for issues that are resolved by the system or <b>Manual</b> for issues that you must resolve.

Feature	Description
PSC Enforcement Insights for 6-GHz Radio Band	Cisco DNA Center displays the Preferred Scanning Channel (PSC) enforcement configuration recommendations for the 6-GHz radio band in the <b>Insights</b> dashlet of the <b>AI-Enhanced RRM</b> dashboard.
Support for ThousandEyes Integration	With this release, the following types of ThousandEyes agent tests are supported: <ul style="list-style-type: none"> <li>• Network agent-to-agent test: Collects network data, including jitter, packet loss, and latency.</li> <li>• Voice RTP test: Collects Mean Opinion Score (MOS), packet loss, latency, and Packet Delay Variation (PDV).</li> </ul>
User-Defined Issue Settings	You can create new issues based on the syslog details.

## New and Changed Features in Cisco DNA Center Platform

Feature	Description
<b>New API Changes</b>	
Wireless API	<p>Starting in 2.3.5.3, the Cisco DNA Center platform no longer supports <code>configureApHeight</code>, <code>apHeight</code>, <code>configureElevAngleDegree</code>, <code>antennaElevAngleDegree</code>, <code>antennaElevAngleSign</code>, <code>configureAntennaDegree</code>, and <code>antennaDegree</code> parameters in the following wireless API:</p> <p>POST&lt;cluster-ip&gt;/dna/intent/api/v1/wireless/accesspoint-configuration</p> <p><b>Note</b> When you configure <code>antennaName</code>, the Cisco DNA Center platform configures only the antenna gain using this attribute. The Cisco DNA Center platform doesn't configure the antenna pattern using this attribute.</p> <p>In response, the GET&lt;cluster-ip&gt;/dna/intent/api/v1/wireless/accesspoint-configuration API returns default values for the following attributes:</p> <ul style="list-style-type: none"> <li>• <code>antennaElevAngle</code>: The API returns the value 0 for this attribute.</li> <li>• <code>antennaPatternName</code>: The API returns the value <code>null</code> for this attribute.</li> <li>• <code>apHeight</code>: The API returns the value 0 for this attribute.</li> <li>• <code>antennaAngle</code>: The API returns the value 0 for this attribute.</li> </ul> <p>To access the new <b>Wireless API</b>, click the menu icon and choose <b>Platform &gt; Developer Toolkit &gt; APIs</b>.</p> <p>Expand the <b>Connectivity</b> drop-down list and choose <b>Wireless</b>.</p>
<b>New API Features</b>	

Feature	Description
Devices APIs	<p>The Cisco DNA Center platform supports the following <b>Devices</b> APIs for rogue additional details:</p> <ul style="list-style-type: none"> <li>• POST&lt;cluster-ip&gt;/dna/intent/api/v1/security/rogue/additional/details/count Rogue Additional Detail Count.</li> <li>• POST&lt;cluster-ip&gt;/dna/intent/api/v1/security/rogue/additional/details Rogue Additional Details.</li> </ul> <p>To access the new Devices API, click the menu icon and choose <b>Platform &gt; Developer Toolkit &gt; APIs</b>.</p> <p>Expand the <b>Know your Network</b> drop-down list and choose <b>Devices</b>.</p>
Discovery API	<p>The Cisco DNA Center platform supports the following <b>Discovery</b> APIs for rogue additional details:</p> <ul style="list-style-type: none"> <li>• DELETE&lt;cluster-ip&gt;/dna/intent/api/v2/global-credential/{id} Delete Global Credential V2.</li> <li>• GET&lt;cluster-ip&gt;/dna/intent/api/v2/global-credential Get All Global Credentials V2.</li> <li>• POST&lt;cluster-ip&gt;/dna/intent/api/v2/global-credential Create Global Credentials V2.</li> <li>• PUT&lt;cluster-ip&gt;/dna/intent/api/v2/global-credential Update Global Credentials V2.</li> </ul> <p>To access the new <b>Discovery</b> API, click the menu icon and choose <b>Platform &gt; Developer Toolkit &gt; APIs</b>.</p> <p>Expand the <b>Operational Tasks</b> drop-down list and choose <b>Discovery</b>.</p>
End of Life (EoX) APIs	<p>The Cisco DNA Center platform supports the following <b>End of Life (EoX)</b> APIs:</p> <ul style="list-style-type: none"> <li>• GET &lt;cluster-ip&gt;/dna/intent/api/v1/eox-status/device Get EoX Status For All Devices.</li> <li>• GET &lt;cluster-ip&gt;/dna/intent/api/v1/eox-status/device/{deviceId} Get EoX Details Per Device.</li> <li>• GET &lt;cluster-ip&gt;/dna/intent/api/v1/eox-status/summary Get EoX Summary.</li> </ul> <p>To access the new <b>Platform</b> API, click the menu icon and choose <b>Platform &gt; Developer Toolkit &gt; APIs</b>.</p> <p>Expand the <b>Know your Network</b> drop-down list and choose <b>EoX</b>.</p>

Feature	Description
LAN Automation API	<p>The Cisco DNA Center platform supports the following <b>LAN Automation</b> APIs:</p> <ul style="list-style-type: none"><li>• GET &lt;cluster-ip&gt;/dna/intent/api/v1/lan-automation/log/\${id}/\${serialNumber} LAN automation logs for individual devices.</li><li>• GET &lt;cluster-ip&gt;/dna/intent/api/v1/lan-automation/sessions LAN automation active sessions.</li></ul> <p>To access the new <b>LAN Automation</b> API, click the menu icon and choose <b>Platform &gt; Developer Toolkit &gt; APIs</b>.</p> <p>Expand the Site Management drop-down list and choose LAN Automation.</p>

Feature	Description
Policy APIs	<p>The Cisco DNA Center platform supports the following <b>Policy</b> APIs:</p> <ul style="list-style-type: none"> <li>• PUT &lt;cluster-ip&gt;/dna/intent/api/v1/endpoint-analytics/endpoints/\${epId}/anc-policy Apply ANC policy.</li> <li>• PUT &lt;cluster-ip&gt;/dna/intent/api/v1/endpoint-analytics/endpoints/\${epId} Update a registered endpoint.</li> <li>• GET &lt;cluster-ip&gt;/dna/intent/api/v1/endpoint-analytics/endpoints/count Get the count of endpoints.</li> <li>• GET &lt;cluster-ip&gt;/dna/intent/api/v1/endpoint-analytics/tasks/\${taskId} Get task details.</li> <li>• GET &lt;cluster-ip&gt;/dna/intent/api/v1/endpoint-analytics/dictionaries Get AI endpoint analytics attribute dictionaries.</li> <li>• GET &lt;cluster-ip&gt;/dna/intent/api/v1/endpoint-analytics/endpoints/\${epId} Get endpoint details.</li> <li>• GET &lt;cluster-ip&gt;/dna/intent/api/v1/endpoint-analytics/endpoints Query the endpoints.</li> <li>• GET &lt;cluster-ip&gt;/dna/intent/api/v1/endpoint-analytics/anc-policies Get ANC policies.</li> <li>• POST &lt;cluster-ip&gt;/dna/intent/api/v1/endpoint-analytics/endpoints Register an endpoint.</li> <li>• POST &lt;cluster-ip&gt;/dna/intent/api/v1/endpoint-analytics/cmdb/endpoints Process CMDB endpoints.</li> <li>• DELETE &lt;cluster-ip&gt;/dna/intent/api/v1/endpoint-analytics/endpoints/\${epId} Delete an endpoint.</li> <li>• DELETE &lt;cluster-ip&gt;/dna/intent/api/v1/endpoint-analytics/endpoints/\${epId}/anc-policy Revoke ANC policy.</li> </ul> <p>To access the new <b>Policy</b> API, click the menu icon and choose <b>Platform &gt; Developer Toolkit &gt; APIs</b>.</p> <p>From the left hierarchy tree, choose <b>Policy</b>.</p>



Feature	Description
System Settings API	<p>The Cisco DNA Center platform supports the following <b>System Settings</b> APIs:</p> <ul style="list-style-type: none"> <li>• GET &lt;cluster-ip&gt;/dna/intent/api/v1/authentication-policy-servers</li> </ul> <p>Get authentication and policy servers.</p> <p>To access the new <b>System Settings</b> API, click the menu icon and choose <b>Platform &gt; Developer Toolkit &gt; APIs</b>.</p> <p>In the <b>Developer Toolkit</b> window, expand <b>System Settings</b>.</p>
<b>New ITSM Integration Features</b>	
Endpoint Attribute Retrieval with ITSM (ServiceNow) Bundle	<p>This Cisco DNA Center platform release supports <b>Synchronization Options</b> in the <b>Configure Endpoint Attribute Retrieval with ITSM (ServiceNow)</b> window to define the incremental sync of endpoints. For more information, see the <a href="#">Cisco DNA Center ITSM Integration Guide</a>.</p>
<b>New Reports</b>	

Feature	Description
Rogue Additional Details Report	

Feature	Description
	<p>This release supports a new <b>Rogue Additional Details</b> report that provides additional information of the rogue threats with details at the BSSID level.</p> <ul style="list-style-type: none"> <li>• The <b>Rogue Additional Details</b> report is generated on the following criteria: <ul style="list-style-type: none"> <li>• MAC Address</li> <li>• Last Updated</li> <li>• First Time Seen</li> <li>• Detecting AP Name</li> <li>• Radio Type</li> <li>• Controller IP Address</li> <li>• SSID</li> <li>• Channel Number</li> <li>• Containment</li> <li>• Encryption</li> <li>• Switch IP Address</li> <li>• Switch Name</li> <li>• Port Description</li> <li>• Location</li> <li>• Threat Level</li> <li>• Threat Type</li> <li>• Start Time</li> <li>• End Time</li> </ul> </li> <li>• Supported report file formats include <b>CSV</b>, <b>TDE</b>, and <b>JSON</b>.</li> <li>• In the <b>Setup Report Scope</b> window, the <b>Rogue Additional Details</b> report provides port details based on the following scope: <ul style="list-style-type: none"> <li>• Location</li> <li>• Threat Level</li> <li>• Threat Type</li> </ul> </li> <li>• In the <b>Schedule Report</b> window, available time range options are <b>Last 3 Hours</b>, <b>Last 7 Days</b>, and <b>Custom</b>.</li> </ul> <p><b>Note</b> Use the <b>Custom</b> option to customize the date and time interval, as well as the time zone (GMT) for the time range.</p>

Feature	Description
	<p>To access the <b>Rogue Additional Details</b> report, click the menu icon and choose <b>Report &gt; Reports Templates &gt; Rogue and aWIPS</b>.</p> <p>In the <b>Report</b> window, choose <b>Rogue Additional Details</b>.</p> <p>For more information about <b>Rogue Additional Details</b>, see <b>Run a Rogue and aWIPS Report</b> in the <a href="#">Cisco DNA Center Platform User Guide</a>.</p>

## New and Changed Features in Cisco DNA Automation

Feature	Description
Activate or Deactivate AppX MS-Teams	You can now activate or deactivate AppX MS-Teams from your Cisco DNA Center integration.

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

**Table 6: New and Changed Features in Cisco Software-Defined Access, Release 2.3.5.3**

Feature	Description
Intrasubnet Routing	<p>SD-Access forwarding behavior is optimized to route the intrasubnet traffic based on the destination IP address, instead of the destination MAC address. Intrasubnet routing is deployed for an IP pool or an anycast gateway by disabling the Layer 2 Virtual Network.</p> <p>This release of Cisco DNA Center supports intrasubnet routing for IPv4 address pool. Dual-stack IP pool and IPv6 traffic are not supported in the intrasubnet routing segment. Intrasubnet routing and Layer 2 flooding cannot coexist for the same IP pool.</p>

**Table 7: New and Changed Features in Cisco Software-Defined Access, Release 2.3.5.0**

Feature	Description
<p>LAN Automation Enhancements: New GUI Multiple LAN Automation Sessions</p>	<p>A new user interface window for LAN Automation supports both Day 0 and Day N operations, such as:</p> <ul style="list-style-type: none"> <li>• Start and stop LAN Automation session</li> <li>• Add and delete a Layer 3 interface link</li> <li>• View the newly discovered devices</li> <li>• View the provisioned devices</li> <li>• Check the history of LAN Automation sessions</li> <li>• View the session logs, logs for newly discovered devices, and so on</li> </ul> <p>You can run multiple (a maximum of five) LAN Automation sessions simultaneously, across sites. However, you can enable only one LAN Automation session per site.</p>

Feature	Description
Multicast Enhancements	<p>Multicast capabilities have been enhanced to support the following through Cisco DNA Center:</p> <ul style="list-style-type: none"> <li>• ASM and SSM multicast can be configured concurrently in an SD-Access Virtual Network.</li> <li>• ASM multicast supports dual stack pools (IPv4 and IPv6 pools).</li> <li>• ASM multicast supports multiple external rendezvous points.</li> <li>• SSM multicast supports addition and deletion of IP address ranges.</li> </ul>
Support for Multiple IP Addresses for a Wired MAC Address	Cisco SD-Access fabric supports wired endpoints with multiple IP addresses. You can associate multiple IPv4 addresses with a single MAC address.
Support for Native Multicast over SD-Access Transit	<p>You can configure SD-Access Native Multicast on a network that has multiple fabric sites that are connected to an SD-Access transit. Cisco DNA Center provides an option to enable multicast on the border nodes and on the SD-Access transit.</p> <p>This feature is supported only on the fabric sites that have a LISP Pub/Sub control plane node.</p> <p><b>Note</b> To enable native multicast over SD-Access transit, ensure that the border node devices operate Cisco IOS XE Release 17.10 or later.</p>
Support Power Profiles Across APs in a Fabric	Cisco SD-Access supports creation of AP power profiles for Cisco Wireless Controllers running Cisco IOS XE Release 17.10.1 and later. You can assign an AP power profile to an AP and define multiple rules for the AP power profiles.
Support for Wireless IP Address Pools from Layer 2 Segments for Fabric Sites	<p>Cisco DNA Center allows you to choose the wireless IP address pools that are configured for Layer 2 segments while configuring wireless SSIDs for fabric sites.</p> <p><b>Note</b> This functionality can only be enabled from the new SD-Access user interface workflow.</p>

## New and Changed Features in Interactive Help

Feature	Description
<b>New in 2.3.5.3</b>	
New Walkthroughs	<ul style="list-style-type: none"> <li>• Configure Site Analytics Settings</li> <li>• View Site Analytics</li> </ul>
<b>New in 2.3.5.0</b>	

Feature	Description
New Walkthroughs	<ul style="list-style-type: none"> <li>• Add a Building</li> <li>• Add a Floor Without a Map</li> <li>• Add Align Points on a Floor</li> <li>• Add an Area</li> <li>• Add an Exclusion Region to a Floor</li> <li>• Configure Native Multicast over SD-Access Transit</li> <li>• Position Sensors on a Floor</li> <li>• View Your Journey Maps</li> </ul>

### Licensing Changes

After upgrading from Cisco DNA Center 2.3.5.0 to 2.3.5.3, you might see that your physical license is out of compliance:

Settings / Cisco Accounts

## Smart Licensing

✔
Cisco DNA Center registration completed successfully.
✕

Smart Licensing is a cloud-based, software license management solution that allows you to manage and track the status of your license and software usage.

On Registering this Cisco DNA Center Product Instance, it will be able to communicate with Cisco Smart Software Manager.

Cisco Smart Software Manager offers an integrated view of the licenses you have purchased and what has been deployed in your network.

Smart Account

Smart Account Domain

Virtual Account

Product Instance Name

Registration Status	✔ Registered (October 27, 2020) ⓘ
License Authorization Status	✖ Out of compliance (October 16, 2020) ⓘ

To remain in compliance with the Cisco commercial agreements, ensure that your license is compliant by completing the following steps.

## Procedure

- Step 1** In Cisco Smart Software Manager (Cisco SSM), in the **Inventory** tab, confirm that you already have an appropriate license, and move it to the appropriate virtual account.
- Step 2** If you don't find a license in Cisco SSM, you must add the Cisco DNA Center PID to the inventory as explained below and in the [Cisco DNA Center appliance license self-serve](#) guide.
- a) In Cisco SSM, choose **Inventory > Product Instances**. Choose the product instance with type **DNASW** and then choose **Actions > Add to Inventory**.

Virtual Account: Major Minor Hide Alerts

General Licenses **Product Instances** Event Log

Authorize License-Enforced Features... Search by Name, Product Type

Name	Product Type	Last Contact	Alerts	Actions
a2ba9d8e23811ea98887e7204243eab	DNASW	2020-Aug-19 16:28:41		Actions
a5d89b00eb311ebaecb3e23711fae27	DNASW	2020-Oct-15 06:59:56		Actions
b8284d0add2b11eaaaf92aafd474254a	DNASW	2020-Aug-19 01:18:25		Actions
c462d092ebb111eaa8352eff0a3d2e60	DNASW	2020-Oct-27 15:26:52		Actions
c911c38dccb11eaa63fe2c016accdd5	DNASW	2020-Aug-17 23:23:08		Actions

Transfer...  
Remove...  
**Add to Inventory...**

- b) Choose the appliance license based on the hardware appliance model. If you are registering a regular Cisco DNA Center appliance, enter **1** for **DNAC Gen2 Appliance - Regular (44 Core)**.

Licenses Available to Add

License	Expires	Available	Add to Inventory
DNAC Gen2 Appliance - Regular (44 Core) Cisco DNAC Gen2 Regular (44 Core) Appliance License	-never-	1	<input style="width: 50px;" type="text" value="1"/>
DNAC Gen2 Appliance - XL (112 Core) Cisco DNAC Gen2 XL (112 Core) Appliance License	-never-	1	<input style="width: 50px;" type="text"/>
DNAC Gen2 Appliance - Large (56 Core) Cisco DNAC Gen2 Large (56 Core) Appliance License	-never-	1	<input style="width: 50px;" type="text"/>

Cancel **Next**

- c) Click **Next** and review the added license.
- d) Click **Add to Inventory** to add the appliance license to the inventory.

**Note** If you added the wrong appliance license or quantity, contact your Cisco account representative.

- e) In Cisco SSM, choose **Inventory > Licenses** and confirm whether the Cisco DNA Center appliance self-service license has been deposited.

Virtual Account: 1 Major 4 Minor Hide Alerts

General **Licenses** Product Instances Event Log

Available Actions Manage License Tags License Reservation...  Show License Transactions Search by License

By Name | By Tag

Advanced Search

License	Billing	Purchased	In Use	Substitution	Balance	Alerts	Actions
C9500 Network Advantage	Prepaid	25	0	-	+ 25		Actions
C9500 Network Essentials	Prepaid	25	0	-	+ 25		Actions
DNAC Gen2 Appliance - XL (112 Core)	Prepaid	1	0	-	+ 1		Actions
DNAC Gen2 Appliance - Large (56 Core)	Prepaid	1	0	-	+ 1		Actions
DNAC Gen2 Appliance - Regular (44 Core)	Prepaid	1	1	-	0		Actions

**Step 3** In Cisco DNA Center, click the menu icon and choose **System > Settings > Cisco Accounts > Smart Licensing**. Click the three vertical dots on the right side of the **Register** button and choose **Renew Authorization Now**. The authorization status changes to **Authorized**.

Settings / Cisco Accounts

## Smart Licensing

Smart Licensing is a cloud-based, software license management solution that allows you to manage and track the status of your license and software usage.

On Registering this Cisco DNA Center Product Instance, it will be able to communicate with Cisco Smart Software Manager.

Cisco Smart Software Manager offers an integrated view of the licenses you have purchased and what has been deployed in your network.

Smart Account

Smart Account Domain

Virtual Account

Product Instance Name Cisco DNA Center

Registration Status ✔ Registered (April 7, 2023) ⓘ

Renew Authorization Now...

Renew Registration Now...

Reregister

Deregister

✔ Authorized (April 14, 2023) ⓘ

Not Allowed

Direct

Register ⋮



- Step 4** If **Add to Inventory** is unavailable in Cisco SSM, the PID might have been added already to a different virtual account. Note that any request for additional licenses that aren't consistent with your appliance type will result in out of compliance with the Cisco commercial agreements.

## Telemetry Subscription Changes

When you upgrade to Release 2.3.5.4 from an earlier release, a banner message with information about the telemetry subscription changes is displayed on the **Provision > Inventory** window.

These changes are also displayed as telemetry subscription compliance violations under **Network Settings** on the **Compliance Summary** window.

To address the changes, do one of the following:

- In the banner message on the **Provision > Inventory** window, click **Apply Fix** to apply the changes to the applicable devices.
- On the **Compliance Summary** window, click **Network Settings** and perform the necessary compliance remediation to address the compliance violations.

## Deprecated Features

### Network Analysis Module

Starting in 2.3.5.6, you cannot integrate your Network Analysis Module (NAM) or vNAM server with Cisco DNA Center. Intelligent Capture no longer integrates with NAM or vNAM.

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

## Supported Firmware

Cisco Integrated Management Controller (Cisco IMC) versions are independent from Cisco DNA Center releases. Cisco DNA Center 2.3.5.0, 2.3.5.3, and 2.3.5.4 have 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, DN2-HW-APL-L, DN2-HW-APL-XL

Cisco DNA Center 2.3.5.5 and later has been validated only against the following firmware:

- Cisco IMC Version 4.1(2m) for appliance model DN1-HW-APL
- Cisco IMC Version 4.3(2.240009) for appliance model DN2-HW-APL, DN2-HW-APL-L, 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 or 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

## Supported Virtual Appliance

Cisco announces support for Cisco DNA Center 2.3.5 and 2.3.5.3 on Amazon Web Services (AWS) as a new form factor that supports Cisco DNA Center in a virtual environment. The virtual appliance (VA) form factor helps customers rapidly deploy and operate Cisco DNA Center.

You can deploy and manage Cisco DNA Center on AWS manually or use a Cisco product called Cisco DNA Center Virtual Appliance (VA) Launchpad (as a local installation or through the Cisco-hosted server).

For more information about Cisco DNA Center 2.3.5 and 2.3.5.3 on AWS, see the [Documentation for Cisco DNA Center 2.3.5 on AWS](#).

## 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, Release 2.3.5.x.

Bug Identifier	Headline
<a href="#">CSCwc46954</a>	<p>After a failed AP provisioning during a configuration push, remediation tries to push the same configurations again, instead of trying to remediate based on the last successful operation.</p> <p>This problem occurs when a failed AP provisioning is followed by a compliance remediation (fix all).</p> <p>This behavior is expected. Remediation picks up the last snapshot, whether or not the snapshot succeeded. If provisioning fails after the validation step (after CFS persistence), a new snapshot is attempted. If provisioning fails before or during the validation step (when the snapshot does not persist), the old snapshot remediation is attempted.</p>
<a href="#">CSCwc46985</a>	<p>Compliance doesn't detect any device-level IPDT configuration violations for devices that are running legacy Cisco IOS (earlier than 16.11). Cisco DNA Center doesn't learn IPDT from devices that are running older software versions.</p> <p>For example, the following legacy CLI example shows a device-level IPDT configuration. For these legacy CLI commands, if there is any mismatch between the configuration on Cisco DNA Center and the configuration on the device, the configuration violation isn't captured as part of the Compliance report.</p> <pre> ip device tracking ip device tracking probe auto-source override ip device tracking probe delay 60 Interface Level Ipdt Configuration, interface GigabitEthernet1/0/2 ip device tracking maximum 10 </pre>
<a href="#">CSCwc71086</a>	The provisioning status shows "\"out of sync\"", even though provisioning succeeded.
<a href="#">CSCwd04527</a>	When Cisco DNA Center provisions a Cisco Catalyst 9800 Series Wireless Controller, the Pre-Auth ACL is created and applied. This can cause issues on wireless controllers that do not use the Pre-Auth ACL and can result in an outage, if the Pre-Auth ACL is not noticed immediately.
<a href="#">CSCwd19997</a>	After removing all IP pools from a virtual network that is associated with a fabric site, Pub/Sub or Default Route sessions from that virtual network are not removed for devices in that fabric site for the virtual network.
<a href="#">CSCwd24425</a>	After an upgrade or a fresh installation of Cisco DNA Center, certificates are missing from the trustpool.
<a href="#">CSCwd31475</a>	<p>After integrating Cisco ISE with Cisco DNA Center, the RAPI AAA API payload shows the role as <b>secondary</b>.</p> <p>This problem occurs when Cisco ISE integration is done after Cisco DNA Center is integrated with one or more AAA servers.</p>
<a href="#">CSCwd31523</a>	Flex WLAN provisioning fails on Azure-hosted Cisco Catalyst 9800 Series Wireless Controller-CL, wireless controller for cloud.
<a href="#">CSCwd41946</a>	Upgrade for fabric: After intra upgrade, the SSIDs are disabled on the Cisco Wireless Controller device.
<a href="#">CSCwd44924</a>	The Cisco DNA Center platform fails to generate an email or webhook for subscribed events or issues. When you publish a subscribed issue, the Cisco DNA Center fails to send e-mails or webhooks.
<a href="#">CSCwd46971</a>	A virtual interface is shown as a physical interface in the API for the Cisco AireOS Wireless Controller.
<a href="#">CSCwd47013</a>	The RabbitMQ virtual host (vhost) goes down due to data corruption. Although RabbitMQ has logic to check and restart the RabbitMQ vhost, the vhost does not restart due to data corruption.

Bug Identifier	Headline
<a href="#">CSCwd49581</a>	Retrieving AP-managed locations takes approximately 12 seconds.
<a href="#">CSCwd50715</a>	An incorrect rate limit is shown for sda/hostonboarding/ssid-ippool.
<a href="#">CSCwd51885</a>	Configuration preview is not generated after moving an AP to another floor.
<a href="#">CSCwd53644</a>	The generated AP report contains entries for APs that are no longer active.
<a href="#">CSCwd58147</a>	During upgrade, Cisco Wireless Controller provisioning fails with the following error: device lock required in RFS flow Error,message-null
<a href="#">CSCwd61298</a>	Cisco DNA Center does not update 802.11r changes of a deployed SSID for the Cisco Catalyst 9800 Series Wireless Controller.
<a href="#">CSCwd67815</a>	The End of Life (EoX) report is not available in PDF format.
<a href="#">CSCwd69321</a>	The Cisco DNA Center platform fails to create the <b>Security Advisory Report</b> with the following error message: Formatting failed - Message: Unable to find specified template or user doesn't have permissions to read it: null, Cause: null. Report is not generated.
<a href="#">CSCwd79259</a>	The Cisco Catalyst 9800 Series Wireless Controller telemetry connection gets stuck after a disaster recovery failover.
<a href="#">CSCwd79769</a>	Cisco DNA Center fails to create or update notifications for PagerDuty when you select the following events: <ul style="list-style-type: none"> <li>• Fabric Devices Connectivity - AAA Server</li> <li>• Fabric Devices Connectivity - Port Channel Down</li> <li>• Fabric Devices Connectivity - Multicast RP</li> <li>• Switch Power Failure</li> <li>• AP disconnected from WLC</li> </ul>
<a href="#">CSCwd80676</a>	The Application Recognition service restarts due to a Java Out of Memory (OOM) error.
<a href="#">CSCwd83339</a>	One or more devices already have VLAN(s) with name(s) and show the following error: overlapping_sub2-VN2
<a href="#">CSCwd90050</a>	After an upgrade to Cisco DNA Center 2.3.5, the DNS dashboard remains empty when application telemetry is enabled or provisioned.
<a href="#">CSCwd93216</a>	Reprovisioning a wireless controller by adding several managed AP locations fails.
<a href="#">CSCwe45252</a>	If some Assurance events are configured for notification, SNMP is shown as a channel for notification. However, Assurance events do not support SNMP, and the SNMP notification does not work.
<a href="#">CSCwe59920</a>	After a credential change, the device config (Syslog/SNMP) gets repushed with the same configuration.
<a href="#">CSCwe70104</a>	When using an external API, the wireless provisioning response is different from the expected response.



Bug Identifier	Headline
<a href="#">CSCwe70250</a>	CMDB bundle is not working.
<a href="#">CSCwf02397</a>	When you configure a Basic ITSM CMDB instance, the configuration fails and displays the following error message:  Source Identifier List not found in ITSM.
<a href="#">CSCwf04644</a>	You cannot cancel a scheduled task to update devices using the Cisco DNA Center GUI.
<a href="#">CSCwf12027</a>	In Cisco DNA Center, email Event notifications that are site specific are not working properly.
<a href="#">CSCwf45735</a>	Cisco DNA Center may crash with no or few Docker images left.
<a href="#">CSCwf48529</a>	Compliance Remediation workflow for Cisco Catalyst 9300 device fails with the following error:  NCSP11205: Compliance remediation failed. Additional info for support:  taskId: '25598512-0699-4dc2-857b-db851bda4313'
<a href="#">CSCwf57427</a>	Rolling AP upgrade doesn't work if the image distribution to the wireless controller is done out of band.
<a href="#">CSCwf59765</a>	Cisco DNA Center-generated pre-auth ACLs have only AAA/ISE servers mapped to a specific SSID. Cisco DNA Center ignores all other AAA servers that are added. Because this change brings the ACE's changes to the ACL rule that's already created, Cisco DNA Center repushes the complete ACL to the device. There are no WLAN flaps, but there is a change in the ACL definition.
<a href="#">CSCwf73998</a>	After powering down a node in a Cisco DNA Center High Availability environment, the node's CLI inaccurately displays some services in the <code>Running</code> state.
<a href="#">CSCwh00975</a>	All MAC address formats should be supported while adding external wireless controller to anchor group.
<a href="#">CSCwh13346</a>	The AP name cannot be changed due to empty BLE Radios.
<a href="#">CSCwh15394</a>	Enabling fabric wireless fails with the following error message:  NCSO10011: Error in generating CFS.
<a href="#">CSCwh28311</a>	Disaster Recovery - Rejoin fails after upgrading from Cisco DNA Center 2.3.5.3 to 2.3.5.4.
<a href="#">CSCwh29152</a>	When you edit a personal SSID with a new passphrase and reprovision the Cisco AireOS Wireless Controller, the updated passphrase doesn't get pushed to the wireless controller. Configuration preview doesn't show the CLI pushing the updated passphrase.
<a href="#">CSCwh31187</a>	Fabric edge provisioning fails. Unable to push the device-tracking policy IPDT_POLICY.
<a href="#">CSCwh31664</a>	After a second Cisco Software-Defined AVC (SD-AVC) restart, the Endpoint Analytics (EA) configuration and SD-AVC cloud connectivity configuration might be lost.
<a href="#">CSCwi38752</a>	After an upgrade to Cisco DNA Center 2.3.5.5, if one of the nodes in a three-node HA setup goes down, Assurance health displays "No Health" for policy extended node (PEN) and extended node devices.
<a href="#">CSCwi71546</a>	When you upgrade to Cisco DNA Center 2.3.5.3 or later, Cisco DNA Center doesn't support the out-of-band configuration for the migrated anchor group. The migrated anchor group is formed with a priority of tertiary.

Bug Identifier	Headline
<a href="#">CSCwj04713</a>	In border priority update workflow, fabric provisioning fails with the following error: NCSFP01009: Error occurred while processing the 'modify' request.
<a href="#">CSCwj83979</a>	In Reader node, the security groups are not synced and show a "sync not started" warning message on pre-existing security groups. Bulk download API fails because Cisco ISE is in an unstable state. Cisco ISE status changes from In-Active to Active multiple times.
<a href="#">CSCwj96129</a>	When you restore a backup, the operation hangs at 80% for more than 2 hours.
<a href="#">CSCwk04523</a>	After a fresh air gap ISO installation and running the script to set the cisco.com credentials and accept the device license agreement, the credentials and license agreement aren't set on the GUI. A manual restart of the license-management service is required to enable the cisco.com credentials and license agreement.
<a href="#">CSCwk15350</a>	Cisco DNA Center does not learn TrustSec entities like security groups, SGACLs, or TrustSec policies created, updated, or deleted on Cisco ISE.

## Resolved Bugs

### Cisco DNA Center 2.3.5.6

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.5.6.

Bug Identifier	Headline
<a href="#">CSCvz62216</a>	All WLANs are disabled while enabling application telemetry for Cisco AireOS Wireless Controllers.
<a href="#">CSCwd16465</a>	Cisco DNA Center's Kube-scheduler and Kube-controller services may restart themselves every 10 minutes. This has been observed under SnP load (inventory + UI work-flows) with sustained Disk IO loads.

Bug Identifier	Headline
CSCwd42565	<p>The telemetry update task deploys the following configuration to the wireless controller for each profile policy that is applicable for Cisco Application Visibility and Control (AVC):</p> <pre> ipv4 flow monitor avc_ipv4_assurance input ipv4 flow monitor avc_ipv4_assurance_rtp input   ipv4 flow monitor avc_ipv4_assurance output ipv4 flow monitor avc_ipv4_assurance_rtp output   ipv6 flow monitor avc_ipv6_assurance input ipv6 flow monitor avc_ipv6_assurance_rtp input   ipv6 flow monitor avc_ipv6_assurance output ipv6 flow monitor avc_ipv6_assurance_rtp output </pre> <p>This appears to be the maximum number of flow monitors that is supported on an SSID for Cisco Catalyst 9800 Series Wireless Controllers, which returns an error if the limit is passed. Therefore, if the wireless controller already had another flow monitor configured on a policy profile, the provision fails at the deployment stage when the wireless controller throws the error:</p> <pre> % node-1:dbm:wireless:At most 2 IPv4 input flow monitor(s) can be configured per policy profile </pre> <p>The provision task fails and the policy profile is in disabled state, resulting in a wireless outage on the SSID.</p> <p>To work around this problem, do the following:</p> <ul style="list-style-type: none"> <li>• Remove all custom flow monitor configurations.</li> <li>• Resync the device and rerun the telemetry provision.</li> </ul>
CSCwd71623	Large amount of aWIPS events causing event notification database growth.
CSCwe28861	Cisco DNA Center experiences pipelineruntime-taskmgr-base restarts due to OOM condition.
CSCwe37981	<p>When maglev system and ndp elastic search is running on an appliance, and maglev-system/elasticsearch is restarted, restart count of both maglev-system/elasticsearch and ndp/elasticsearch is increased.</p> <p>To work around this problem, do a hard restart of elasticsearch-0 and elasticsearch-2 for ndp or whichever restarted to bring the number of restarts back to 0.</p>
CSCwe87244	<p>On Cisco DNA Center, we may get an error when trying to perform actions like assigning a device to a site, provisioning a device, adding a device tag to a device.</p> <p>This issue is seen if the IP address that Cisco DNA Center is using to manage the network device is present more than once on the device. We may have the IP address present on the device in two separate VRFs. Cisco DNA Center is not VRF aware and sees these two entries as separate devices. Cisco DNA Center adds both the entries to its database. The duplicate entries are causing this behavior.</p>
CSCwe92274	<p>In Cisco DNA Center, fabric provisioning may fail with the following error message:</p> <pre> Error in generating CFS due to internal error. CFS Generation Failed for task id &lt;task_id&gt; </pre> <p>The SPF service logs show the following error message:</p> <pre> NCSO20933: Provisioning failed due to Loopback0 interface not found in database for device &lt;switch_hostname&gt;. Re-sync the device and then retry the operation. </pre>
CSCwf09766	AP Usage PDF report looks broken when KPIs are more.

Bug Identifier	Headline
<a href="#">CSCwf30218</a>	API_ENDPOINT_CREATE workflow takes longer time to complete.
<a href="#">CSCwf45145</a>	In Cisco DNA Center the composite template simulation doesn't show any CLI preview even for the individual templates. The CLI preview is shown if the simulation is run on the templates individually. This behavior was observed for all the device families that is, routers, switches and Cisco Catalyst 9800 Series Wireless Controller.
<a href="#">CSCwf54593</a>	Incorrect country codes are pushed to the wireless controllers for some countries. To work around this problem, user can provide latitude/longitude of the location or use pin option in the map to get the correct country code.
<a href="#">CSCwf58957</a>	Cisco DNA Center 2.3.5.3 Rejoin task passed - dB replication happens when DR setup is ready for Manual failover.
<a href="#">CSCwf62913</a>	Cisco DNA Center 2.3.5.3: After system upgrade all Postgres services are in CrashLoopBackOff with no Master.
<a href="#">CSCwf66065</a>	When the SSID filter is changed on the Assurance application dashboard, the dashlets are not updated with the new filter values.
<a href="#">CSCwf68082</a>	In Cisco DNA Center 2.3.5.3 deployed on a single-node cluster, sites filtering is not working properly, after selecting a site/building and then expanding that site/building.
<a href="#">CSCwf70144</a>	Triggering a deregister for disaster recovery from the Active site shows successful. But when we navigate to the Standby/Passive site, it is still in Passive Mode, and it has no options to deregister from disaster recovery.
<a href="#">CSCwf70826</a>	When the payload goes beyond a specific size, its gets exception on the backend and task is stuck in progress states and sends continuous GET requests.
<a href="#">CSCwf73197</a>	HA cluster: Hook execution skipped on two-nodes and proceeds with system update.
<a href="#">CSCwf77077</a>	Cisco DNA Center inventory should handle special characters at the end of device hostname. To work around this issue, remove the special characters from the device's prompt.
<a href="#">CSCwf77542</a>	In Cisco DNA Center 2.3.5.4, get device enrichment details API call returns with the following error: <pre>The client made a request for a resource that does not exist, for get all devices APIwhile enriching device information.</pre>
<a href="#">CSCwf87650</a>	Cisco DNA Center may delete a Plug and Play (PnP) acquired device from the inventory, but the device is not deleted from PnP.
<a href="#">CSCwf88099</a>	Upgrade from Cisco DNA Center 2.2.3.6 to 2.3.3.7 fails due to cloud-connectivity-data-hub API failure.
<a href="#">CSCwf90780</a>	After protocol pack version update to 65.0, some of the endpoints were reprofiled. Two such new profiles were Evoko and Crestron devices. In the tab that shows review changes on the UI of EA inventory, these devices show up intermittently. Also, the number of endpoints that were affected by the change show empty list.

Bug Identifier	Headline
<a href="#">CSCwf94495</a>	<p>Attempting to remove an edge node from Cisco DNA Center's fabric window may fail with the following error:</p> <pre>NCSO20125:Cannot delete device from the Fabric Site/Zone since device has port assignments.Please remove port assignments from the device prior to deleting the device from the Fabric Site/Zone.</pre>
<a href="#">CSCwf99188</a>	<p>In Cisco DNA Center 2.3.5.3 deployed in a 3-node cluster, unable to create IP address pool with the same name that was previously used at global site and then deleted. While attempting to do so got the following error:</p> <pre>NCIP10245: A group named xxxxx already exists.</pre> <p>These IP address pools couldn't be seen in the GUI, but they can be seen in the database.</p>
<a href="#">CSCwh10806</a>	<p>Cisco DNA Center maps may fail to display a heatmap or the APs, if they were added to inventory without their <code>ifType</code> attribute being polled and recorded accurately.</p>
<a href="#">CSCwh13831</a>	<p>Cisco DNA Center may fail to delete a device from inventory citing a constraint violation against the <code>ntpserverassociation</code> table.</p>
<a href="#">CSCwh17180</a>	<p>Cisco DNA Center 2.3.3.5: Application package fails to install with TACACS numerical username.</p>
<a href="#">CSCwh18053</a>	<p>Pipeline Timeseries-Analytics state may stuck in CANCELLED and restart doesn't recover the pipeline.</p>
<a href="#">CSCwh23337</a>	<p>Cisco DNA Center may fail to collect inventory from a Cisco Catalyst 9600 stacked Switches with the following error:</p> <pre>NCIM12004: Serial number conflict detected for the IP address.</pre> <p>This was observed in Cisco DNA Center 2.3.3.6 while managing devices with SNMPv3.</p> <p>To work around the problem, update the device with SNMPv2 credentials and then change back to SNMPv3.</p>
<a href="#">CSCwh28002</a>	<p>In Cisco DNA Center 2.3.3.7, the reports were successfully generated in Cisco DNA Center, but the generated reports were not sent to the webhook server.</p> <p>To work around the problem, do the following:</p> <ul style="list-style-type: none"> <li>• Make sure that the root CA cert and the intermediate cert, if any, are imported into the Cisco DNA Center's trustpool on the GUI.</li> <li>• Run the following command from Cisco DNA Center CLI: <pre>magctl service restart -d daas-runtime</pre> </li> <li>• After the pod is up and running, generate the report and Cisco DNA Center should send it to the webhook server successfully.</li> </ul>
<a href="#">CSCwh29098</a>	<p>Wireless controller provisioning failed with CFS persistence error when trying to delete RLAN configured custom PT .</p>

Bug Identifier	Headline
<a href="#">CSCwh29173</a>	<p>In Cisco DNA Center 2.3.5.3, while adding or editing an SP profile on <b>Policy &gt; Application QoS &gt; Edit (Sites &gt; Devices &gt; WAN)</b> window, and using a tunnel interface with the DMVPN hub role, the configuration save button may become grayed out due to a red test indicating <code>At least one Branch BW is needed</code>. On adding a branch BW entry, the <b>Save</b> button is not enabled.</p> <p>To work around this problem, do the following:</p> <ul style="list-style-type: none"> <li>• On addition of the branch BW or multiple branch BWs select the blue circle with the " ^ " symbol to submit the entry or entries for branch BW.</li> <li>• Toggle to the DMVPN branch role and then back to the DMVPN hub role.</li> </ul> <p>You must now see that each entry will show as added and the <b>Save</b> button is enabled.</p>
<a href="#">CSCwh33036</a>	Cisco DNA Center inventory reports should handle the 0.0.0.0 IP address.
<a href="#">CSCwh41189</a>	After upgrade to Cisco DNA Center 2.3.5.3, two anchor Cisco Catalyst 9800 Series Wireless Controller and two foreign Cisco Catalyst 9800 Series Wireless Controller were provisioned, it was found that one of the foreign Cisco Catalyst 9800 Series Wireless Controllers was deployed with a wrong <b>Mobility &gt; Configure &gt; Wireless Mobility Group Member</b> . On the <b>Network Profile</b> and <b>Network Design</b> windows, there are two automatically generated anchor groups.
<a href="#">CSCwh41361</a>	Cisco DNA Center's inventory service may degrade into an out of memory condition, when there is a huge number of records in the BaseRadio table (these represent stale radios when the corresponding AP is still associated with a wireless controller) almost 9,000 in number.
<a href="#">CSCwh42571</a>	Standby activate fails due to Postgres replication failure.
<a href="#">CSCwh45346</a>	CMDB sync fails with "Schedule to Publish Inventory Details - ServiceNow Connector timing out".
<a href="#">CSCwh45985</a>	Guest anchor SSID cannot have same WLAN profile name at multiple network profiles after upgrade.
<a href="#">CSCwh46746</a>	<p>Cisco DNA Center 112 core, three-node cluster on Cisco DNA Center 2.3.3 HF1 load was provisioned with two Cisco Catalyst 9800 Series Wireless Controllers with Cisco Aironet 1700 Series Access Points per wireless controller. The cluster was migrated from Cisco DNA Center 2.3.3 HF1 to Cisco DNA Center 2.3.5.4.</p> <p>After the cluster was up we reprovisioned the N wireless controllers, compliance is displaying error with the following system error:</p> <pre>Error in executeIntentReportGenerator, errorMsg : java.lang.NegativeArraySizeException: -202096447</pre>
<a href="#">CSCwh48892</a>	Device stuck in syncing state for days.
<a href="#">CSCwh51345</a>	SSH Access to node is lost when enterprise interface flaps.
<a href="#">CSCwh55601</a>	Scalability: CBAR disabled and device counts are all 0 in DPI Enablement page.
<a href="#">CSCwh56816</a>	Remediating the compliance mismatch shown, post disable/enabling WLAN's admin status manually on an Cisco AireOS Wireless Controller, is not resolving the admins status on the WLAN.
<a href="#">CSCwh57011</a>	Upgrade fails from DR_UNPASSIVATE_CLUSTER with a hook execution error.

Bug Identifier	Headline
<a href="#">CSCwh57622</a>	In Cisco DNA Center, trying to configure an IP transit L3 handoff using IPv6 addresses may result in the input field reporting "IP already part with a user pool," even though no IPv6 pools are using the same subnet.
<a href="#">CSCwh58173</a>	<p>When you go to a floor map, the map starts polling Assurance for AP and client data to display on the floor map. This data is polled every minute in the backend to support the GUI "Auto-Refresh 1 Minute" option, though it is not dependent on the view option being set. If no data is requested for the map after 5 minutes, they are stopped. If an AP is deleted from Inventory Assurance while the Assurance polling jobs are still running, the polling thread was unexpectedly being stuck open indefinitely. Over time, if the system has active map users and is seeing a high rate of AP deletion / replacement, it can cause dozens or even hundreds of runaway background threads polling Assurance for AP and client data, which eventually can cause Assurance and/or QueryEngine services to crash.</p> <p>To work around this problem, restart the dna-maps-service.</p>
<a href="#">CSCwh58183</a>	When you update the protocol pack to version 67 in Cisco DNA Center, the update fails.
<a href="#">CSCwh63708</a>	After upgrading Cisco DNA Center from 2.3.3.6 to 2.3.5.3, a user may be unable to access the GUI citing the error "{"message": "Unauthorized"}".
<a href="#">CSCwh64123</a>	An Cisco ASR 1000 Series device added to inventory may take long time to sync. While processing the device's inventory sync status may change from syncing to yet to sync and then back to syncing.
<a href="#">CSCwh70281</a>	After upgrading to Cisco DNA Center 2.3.5.4, REDIS cluster_size mismatch is observed.
<a href="#">CSCwh72329</a>	Cisco Catalyst 8000 routers that have been provisioned in Cisco DNA Center with a routing network profile (required for templates) do not show up as valid SDA transit devices in the <b>Create Transit</b> workflow.
<a href="#">CSCwh73187</a>	After Cisco DNA Center connectivity to Cisco ISE is lost and restored, the locations of some network devices changed on Cisco ISE during DR failover.
<a href="#">CSCwh76304</a>	The <b>Distribution</b> step of <b>Image Distribution</b> workflow running for more than 10 hours was aborted as expected. However, the next step <b>Post Distribution Operation</b> of the workflow which is expected to release pertinent resources held by the distribution step was never run and hence the resources (essentially swim-service worker threads) were stuck, unable to process the new/pending image distribution requests.
<a href="#">CSCwh79081</a>	If the wired client's MAC address is present in two or more devices MAC address table, in Client 360 a wired client shows connection to the port channel interface of a device that has the wired client in the mac address table, but is not physically connected.
<a href="#">CSCwh79706</a>	Hosts discovered with VLAN ID set to <code>undefined</code> leads to no assurance data.
<a href="#">CSCwh84666</a>	<p>Assigning border/CP role to the device fails due to configuration push failure. The logs indicate the issue is due to incorrect LISP instance-id value associated with a particular VN.</p> <p>To work around the problem, delete the VN, recreate it and confirm it has a valid 4XXXX instance-id assigned to it.</p>
<a href="#">CSCwh85599</a>	<p>LAN automation reconfigures loopback 0 of primary/secondary seed.</p> <p>To work around the problem, update the new IP address of seed device in <b>Inventory &gt; Edit Device &gt; Management IP</b>.</p>

Bug Identifier	Headline
<a href="#">CSCwh91278</a>	Cisco DNA Center 2.3.5.4: Device deletion failed due to constraint violation acldcondition.
<a href="#">CSCwh91534</a>	Unable to generate inventory report with ~100 device "BAPI Execution Failed".
<a href="#">CSCwh92936</a>	Cisco DNA Center successfully imports the floor map from the PDF file, but then it shows them as blank. This issue was found while importing the floor map to Cisco DNA Center from the PDF file that was compressed using the JBIG2 compression algorithm.
<a href="#">CSCwh96306</a>	Cisco DNA Center appliance issue, you can create reports, task successfully ends but report just contains the headers with no more information, devices are manageable and reachable.  To work around the problem, clear cache, try different browsers, restart daas-runtime services.
<a href="#">CSCwi00888</a>	If a composite template has a regular template with implicit variable, during the provisioning of the composite template to two or more switches Cisco DNA Center pushes same configs to all switches.
<a href="#">CSCwi08641</a>	NCSP11033: Error occurred while processing the 'modify' request.
<a href="#">CSCwi09672</a>	When Assurance reports were generated from the report template, there was a mismatch in results that were obtained from two templates, that is, client detail gives onboarding details whereas long-term client details will not give onboarding details for the same set of devices instead it is blank.
<a href="#">CSCwi10037</a>	AI-Enhanced RRM provisioning tasks (assign/unassign) are marked failed although provisioning of APs continue longer.
<a href="#">CSCwi12046</a>	Docker/registry is holding up 1.2T in all three nodes leading to service crash.
<a href="#">CSCwi13390</a>	In Cisco DNA Center 2.3.5.3, the network profile has <code>wireless.wlanSchedulerName</code> empty attributes. After upgrade to Cisco DNA Center 2.3.5.4, <code>wireless.wlanSchedulerName</code> doesn't have an empty attribute; the attributes are present only when you configure <code>wlanScheduler</code> .  This mismatch causes a unique WLAN definition, and during the foreign provision, the anchor IP is removed from the policy profile, which causes an outage in guest anchor.  To work around this problem, do the following:  <ol style="list-style-type: none"> <li>1. Open the guest anchor associated network profile.</li> <li>2. Enable and disable the WLAN schedule.</li> <li>3. Save the network profile.</li> </ol> This resets the <code>wireless.wlanSchedulerName</code> . To enable WLAN scheduling, create a dummy scheduler name.
<a href="#">CSCwi28529</a>	Upgrade to Cisco DNA Center 2.3.5.4 failing at 55%.
<a href="#">CSCwi34328</a>	During enablement of wireless on border switch as primary wireless controller, if you already have the other border provisioned as the secondary wireless controller, you may get the following error:  <pre>NCSP11001: User intent validation failed while processing the 'modify' request. Additional info for support: taskId: 'a7bc6711-d1fd-492c-8508-a7da92adab43'</pre>
<a href="#">CSCwi37131</a>	Kubelet.conf client certificate fails to renew while upgrading from Cisco DNA Center 2.3.5.3.
<a href="#">CSCwi44844</a>	LISP fabric authentication key update from banner push fails for wireless controller.



Bug Identifier	Headline
<a href="#">CSCwi79754</a>	<p>WLC or AP Provision failure with below error reason:</p> <pre>"2023-08-23 21:48:07,452   ERROR   lateDeployerTaskAdapter-3     c.c.e.d.s.p.u.DevicePersistenceUtil   NCWL13000: An internal error occurred during processing of the requested 'provision' operation . If problem persists , please contact Cisco TAC   java.lang.IllegalStateException: Duplicate key 50037819-efe3-45e7-a985-b24db5aaa9f5 (attempted merging values UnmanagedDeviceConfigStatus"</pre>
<a href="#">CSCwi83290</a>	Devices shown as "Managed with Internal Errors and Partial Collection Failures" in inventory. Inventory service logs indicate error message pertaining to data collection/persistence of SpanSessionSettings model.
<a href="#">CSCwi90342</a>	Post upgrade config drift page not loading as valid file object got removed.

### Cisco DNA Center 2.3.5.5

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.5.5.

Bug Identifier	Headline
<a href="#">CSCwe15923</a>	<p>The internally autogenerated etcd certificate is not activated after renewal. When accessing the Cisco DNA Center CLI, the following errors may be present:</p> <pre>WARNING:urllib3.connectionpool:Retrying(Retry(total=0, connect=None, read=None, redirect=None, status=None)) after connection broken by 'SSLError(SSLError(1, u'[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:727)'),)': /v2/keys/maglev/config/node-169.254.64.1?sorted=true&amp;recursive=true  ERROR:etcd.client:Request to server https://169.254.64.1:4001failed: MaxRetryError(u"HTTPSConnectionPool(host=u'169.254.64.1', port=4001): Max retries exceeded with url: /v2/keys/maglev/config/node-169.254.64.1?sorted=true&amp;recursive=true (Caused by SSLError(SSLError(1, u'[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:727)'),))",)</pre> <p>For more information, see <a href="#">Field Notice FN74065</a>.</p>
<a href="#">CSCwh08460</a>	<p>Cisco DNA Center may fail to import an Ekahau project, citing the following error:</p> <pre>Archive is invalid. Failed to initiate archive import due to unacceptable archive: Unsupported mime type: application/esx</pre> <p>In the payload of the API call, initiate-async, the following content-type in the header is present:</p> <pre>WebKitFormBoundaryFe9lBzA5DgmlccSK Content-Disposition: form-data; name="archive"; filename="multi-bld.esx" Content-Type: application/esx In Windows 11 or 10, there is an .esx registry in HKEY_CLASSES_ROOT\MIME\Database\Content Type</pre>
<a href="#">CSCwh10626</a>	Cisco DNA Center may mark a configuration archive task as a success even though no data is transferred to the external configuration archive server. This issue happens when the archive is configured to be raw or sanitized, and this issue is specific to the disaster recovery use case.
<a href="#">CSCwh26820</a>	In Cisco DNA Center 2.3.5.3, the eaworker pod may degrade into a reboot loop. The logs note that the Java virtual machine is running out of memory.

Bug Identifier	Headline
<a href="#">CSCwh85079</a>	After upgrading from Cisco DNA Center 2.3.3.7 to Cisco DNA Center 2.3.5.4 -70852, nonguest (enterprise) SSIDs require AAA details when the level of security is set to personal. This issue is not consistent with all enterprise SSIDs, and new SSIDs don't exhibit this behavior.
<a href="#">CSCwh90168</a>	<p>Features in Cisco DNA Center stop working due to APIs failing with kong errors. Features like AP and floor map associations and GUI reporting services are down. The command <code>magctl service status cassandra-0</code> shows that cassandra-0 is in crashloopback or OOMKilled state:</p> <pre> Name:          cassandra-0 Namespace:    maglev-system Node:         xxxx Start Time:   xxxx Labels:       addon=true               adjustReplicationDuringNodeScale=async               controller-revision-hash=cassandra-7f86d68787               nodeScale=3               serviceName=cassandra               statefulset.kubernetes.io/pod-name=cassandra-0               version=1.7.38 Annotations:  kubernetes.io/psp: ai-network-analytics-psp Status:       Running IP:          xxxx IPs:   IP:        xxxx Controlled By:  StatefulSet/cassandra Containers:   cassandra:     ...     State:          Running       Started:      xxxx     Last State:    Terminated       Reason:       OOMKilled       Message:      xxxx   ERROR   Cassandra node is not running.      Exit Code:     137       Started:     xxxx       Finished:    xxxx     Ready:         False     Restart Count: 3 </pre>
<a href="#">CSCwh98689</a>	Enterprise SSID provisioning might fail because Cisco DNA Center validates nonanchored SSIDs when provisioning an anchor wireless controller. Cisco DNA Center should only validate anchored SSIDs when provisioning an anchor wireless controller and should ignore enterprise SSIDs.
<a href="#">CSCwi28259</a>	After upgrading to Cisco DNA Center 2.3.5.4, the out-of-band mobility anchor configuration is removed from the controller without selecting the force push template option.
<a href="#">CSCwi28419</a>	After upgrading from Cisco DNA Center 2.3.3.7 to Cisco DNA Center 2.3.5.4, the Cisco DNA Center intent overwrites the CLI template for the default-ap-join profile, which was initially set up to allow SSH access to APs. Cisco DNA Center automatically generates a default AP profile using device default values, which disables SSH access. Therefore, any postupgrade provisioning overwrites the value configured by the CLI template (if CLI templates are not force-pushed during reprovision), causing a change from enabled to disabled SSH access.

### Cisco DNA Center 2.3.5.4-70852-HF3 Hot Fix

The following table lists the resolved bugs in the Cisco DNA Center 2.3.5.4-70852-HF3 hot fix.



- Note**
- To obtain the hot fix, go to the **Software Management** window in the Cisco DNA Center GUI and install the 2.3.5.4-70852-HF3 hot fix. If you don't see it, scroll down and click "Looking for other releases? **Click here.**"
  - The 2.3.5.4-70852-HF3 hot fix is visible only if you have 2.3.5.4 installed.

Bug Identifier	Headline
<a href="#">CSCwe15923</a>	<p>Under some conditions, a newly installed, autogenerated etcd certificate in Cisco DNA Center does not get activated. When the etcd certificate does not get activated, the system might become unresponsive and inaccessible through the GUI, ultimately discarding network telemetry and losing the management capability of Cisco DNA Center.</p> <p>CSCwe15923 is resolved in 2.3.5.4. If you upgraded from 2.3.5.3 to 2.3.5.4 before 2023-10-12, install the 2.3.5.4.70852-HF3 hot fix atop 2.3.5.4.</p>
<a href="#">CSCwh81546</a>	<p>An internally autogenerated etcd certificate is not activated after upgrade. This problem occurs in the following scenario:</p> <ol style="list-style-type: none"> <li>1. Cisco DNA Center is freshly installed using 2.3.5.3, or is upgraded to 2.3.5.3.</li> <li>2. The etcd certificate renews, but is not activated (etcd keeps using the old certificate).</li> <li>3. Cisco DNA Center is upgraded to 2.3.5.4.</li> <li>4. After the upgrade, the old certificate is still used. The system is expected to experience an outage when the certificate expires.</li> </ol>

### Cisco DNA Center 2.3.5.4

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.5.4.

Bug Identifier	Headline
<a href="#">CSCvz61877</a>	Neighbor topology map for AP may show link status is down when it is up.
<a href="#">CSCwb88254</a>	pxGrid REST API access from Cisco DNA Center fails with the following certificate validation error: certificate signed by unknown authority
<a href="#">CSCwc08277</a>	You can't see devices intermittently on the Fabric window. The topology-service's memory utilization is high and it may crash due to running out of memory. Many links in the database have more than 2 link termination points. Malformed links are being formed in the database. The links were learned via LLDP and the device name being reported by CDP vs LLDP was different.
<a href="#">CSCwc39642</a>	Event Notification using Webex, REST, and email stops working after upgrade.
<a href="#">CSCwc45545</a>	User 360 Appendix Business irrelevant and default tabs are missing.

Bug Identifier	Headline
<a href="#">CSCwc61920</a>	Browserbot fails to install on TE update from version 3.0 to 4.1 via the Cisco DNA Center GUI.
<a href="#">CSCwd15864</a>	The API call fails at the NSA web application Assurance back-end service.
<a href="#">CSCwd34162</a>	Cannot apply CLI credentials for the Global site.
<a href="#">CSCwd45971</a>	An SGT created in Cisco DNA Center does not synchronize with Cisco ISE and hangs at the message "Sync not started."
<a href="#">CSCwd50441</a>	Templates that failed in previous provisioning attempts are pushed through during port assignment on the <b>Host Onboarding</b> window.
<a href="#">CSCwd58899</a>	Cisco DNA Center does not show the latest ThousandEyes Enterprise application version (4.3.0) for upgrade.
<a href="#">CSCwd64902</a>	Net configuration error scenarios are lost in the NP error response and flex RLAN provisioning fails.
<a href="#">CSCwd69187</a>	An application package fails to install for a user with only numerals in the username.
<a href="#">CSCwd77779</a>	Editing an authentication template does not update CLIs on the device.
<a href="#">CSCwd93614</a>	After adding FIAB to a fabric, no other config-preview operation succeeds due to an internal error.
<a href="#">CSCwe03653</a>	Adding an IP address in the IP Access Control list to the allowed list stops provisioning Cisco ISE settings to the switch.
<a href="#">CSCwe07052</a>	Too many "RS request content-type header is out-dated" errors are sent after Cisco ISE integrates with Cisco DNA Center successfully.
<a href="#">CSCwe09844</a>	On the <b>Application 360</b> window, only 25 applications are displayed.
<a href="#">CSCwe12283</a>	LAN automation or other provisioning operations may fail and report existing operations as in progress.
<a href="#">CSCwe14566</a>	Port assignment to an IE-3200 extended node fails due to the <b>access-session inherit disable autoconf</b> command.
<a href="#">CSCwe16678</a>	Postgres-0 is running as the primary, but has a DIMM issue. Postgres-1 then attempts to become the primary, but that change fails with an error.
<a href="#">CSCwe21735</a>	Multiple postgres instances indicate themselves as primary following a power outage.
<a href="#">CSCwe25338</a>	After learning of a Catalyst 9800 Series Wireless Controller configuration and provisioning it with the learned Network Profile with Advanced SSID Model Configs, the provisioning may fail.
<a href="#">CSCwe26616</a>	The Catalyst 9410R switch and related hypervisor families don't show the correct number of devices under the family in the Cisco DNA Center Image Repository, showing duplicates for each family.
<a href="#">CSCwe27459</a>	A banner shows an incorrect AI Endpoint Analytics warning alert for Cisco ISE integration.
<a href="#">CSCwe28947</a>	When LAN is automating, plug and play fails on the IPAM server with a client exception in the ipam-service.
<a href="#">CSCwe30879</a>	After an upgrade to Cisco DNA Center 2.3.3.5, one of the Kubernetes service objects, "collector-netflow-ext," is missing, resulting in Assurance data loss for the NetFlow service.

Bug Identifier	Headline
<a href="#">CSCwe31676</a>	Disaster Recovery in a Cisco DNA Center three-node cluster may fail to isolate when two of the three nodes in the cluster are brought down and back up.
<a href="#">CSCwe32559</a>	The Cisco DNA Center VLAN report returns 0 or one site VLAN records. The RestApiSourceExecutor return count is inaccurate.
<a href="#">CSCwe39302</a>	When onboarding new devices via LAN automation, Cisco DNA Center fails to automatically create Network Access Device (NAD) entries in Cisco ISE.
<a href="#">CSCwe39807</a>	An incorrect AP port for switch in Device 360 also affects wireless maps.
<a href="#">CSCwe42089</a>	An external server is successfully set up for Config Archive in Cisco DNA Center, but only a directory is made. There are no config files placed in the directory.
<a href="#">CSCwe46169</a>	The addition of a new IP pool under Guest VN fails with an exception.
<a href="#">CSCwe47530</a>	Postgres goes into a crashloop and restarts continuously. The postgres logs show a syntax error with the configuration file.
<a href="#">CSCwe48765</a>	The Cisco DNA Advantage-level license with the name "C9300X Low-density DNA Advantage Fiber Agg/Core in SMI" for C9300X switches is not detected as a Cisco DNA Advantage-level license when syncing with Cisco SSM, resulting in the level license count showing less than it is.
<a href="#">CSCwe52889</a>	The <b>Inventory</b> window shows "No devices available" and "An unknown error occurred," even though all pods are healthy and running.
<a href="#">CSCwe54540</a>	The reachability polling schedule from the database is removed if the refresh message is not processed so Cisco DNA Center will not poll for the reachability status of devices in the inventory.
<a href="#">CSCwe55226</a>	After upgrading from Cisco DNA Center 2.2.3.6 to 2.3.5.3, Network Settings compliance fails at IPDT after migration.
<a href="#">CSCwe56718</a>	When a customer uses the GET Issues API, they may receive a 500 error response and there are only outputs from the Issues API if a device ID is specified.
<a href="#">CSCwe60241</a>	Cisco DNA Center SWIM's image update readiness check and file transfer check may fail with the error "HTTPS is not reachable" when Cisco DNA Center has a fully qualified domain name (FQDN) in its CA certificate, instead of an IP address.
<a href="#">CSCwe65663</a>	Software image information for some of the devices is missing in Software Images Inventory window. This problem occurs because the model type for Meraki APs is missing in the network element table of the inventory database. As a result, the swim-service fails to build the device image information cache.
<a href="#">CSCwe66587</a>	When setting the scale for a floor, you can enter the required values, but nothing happens when you click OK. The following error is displayed:  <code>Uncaught TypeError: Cannot read properties of null (reading 'style')</code>
<a href="#">CSCwe66786</a>	With network profiles, under Advanced settings, adding or deleting an AP group results in a blank GUI window.

Bug Identifier	Headline
<a href="#">CSCwe68219</a>	Cisco DNA Center application upgrade may fail due to a schema update failure for the SD-access service. The following error is returned:  ERROR: column "networkdeviceid" contains null values
<a href="#">CSCwe71699</a>	When upgrading Cisco DNA Center, the upgrade may stall or fail at roughly 56% or phase 6 of installing host components. The maglev-node-updater logs show that the task that is stalling or failing is updating the Docker images.
<a href="#">CSCwe74038</a>	A configuration mismatch may occur if a fabric in a box device is failing provisioning but the wired fabric operation on the <b>Host Onboarding</b> window is performed. The mismatched items may include IP address pool addition to a VN, VN creation, and IP address pool modification under a VN.
<a href="#">CSCwe82555</a>	An incorrect number of devices may be exported from the Cisco DNA Center License Manager GUI. An export as PDF or CSV doesn't export correctly.
<a href="#">CSCwe83522</a>	Device migration for IBNS2.0 fails if NWS only has AAA Network Auth defined.
<a href="#">CSCwe88997</a>	With APIs, the L2only segment onboarding doesn't work. The "ippoolname" should be optional.
<a href="#">CSCwe89409</a>	Distribution of image 17.6.4 fails due to the following error:  NCSW10090: Failed to distribute image.
<a href="#">CSCwe90447</a>	A get device info from the Cisco SD-Access fabric does not return wireless controller device details from the fabric.
<a href="#">CSCwe92124</a>	Cannot sync with the primary after one Cisco DNA Center node link comes up.
<a href="#">CSCwe95262</a>	Cisco DNA Center may fail to provision a Catalyst 9800 wireless LAN controller.
<a href="#">CSCwe95707</a>	Cisco DNA Center may not distribute a ROMMON update to a managed ISR 4300 router.
<a href="#">CSCwe96016</a>	IPDT compliance remediation does not work on the port where the intent is changed.
<a href="#">CSCwe98036</a>	A provisioning error occurs while processing the request.
<a href="#">CSCwe98737</a>	A "Resource not found" error occurs when using the Provision Template workflow.
<a href="#">CSCwe98803</a>	<p>A vulnerability in Cisco DNA Center could allow an unauthenticated, remote attacker to read and modify data in a repository that belongs to an internal service on an affected device.</p> <p>This vulnerability is due to insufficient access control enforcement on API requests. An attacker could exploit this vulnerability by sending a crafted API request to an affected device. A successful exploit could allow the attacker to read and modify data that is handled by an internal service on the affected device.</p> <p>Cisco has released software updates that address this vulnerability. There are workarounds that address this vulnerability.</p> <p>This advisory is available at the following link: <a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-ins-acc-con-nHAVDRBZ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-ins-acc-con-nHAVDRBZ</a></p>

Bug Identifier	Headline
<a href="#">CSCwe98851</a>	APs or planned APs aren't shown on the floor map on load. The API call fails with a 500 internal server error. Attempts to assign a planned AP from a real AP in the global inventory may fail, with the task result marked with an internal failure.
<a href="#">CSCwf00700</a>	The up-to-date flow collectors are not used to provision the device. In the logs, the SMC API returns 403 (unauthorized).
<a href="#">CSCwf01879</a>	In Cisco DNA Center, upgrading to version 2.3.3.6 allows you to modify the email destination only once.
<a href="#">CSCwf03814</a>	After a Cisco DNA Center power cycle or power outage, the network devices can't update the device-side certificates.
<a href="#">CSCwf03999</a>	The Configure Access Points workflow may fail to configure the AP or radio-related parameters in certain scenarios.
<a href="#">CSCwf07455</a>	The Client Detail report expires every few months and there is no way to regenerate the same report.
<a href="#">CSCwf12835</a>	The current mechanism of authorizing the AP to join the controller is via <i>local authorization</i> . (Local authorization makes use of the AP MAC address or serial number from the controller database.) If you want to switch from local to AAA only or AAA+local, the config diff to configure this setting is not generated in Cisco DNA Center 2.3.5.x.
<a href="#">CSCwf14502</a>	AAA configurations are removed from Cisco Catalyst 9800 Series Wireless Controllers when you create an AP authorization first and then you create a WLAN with the same AAA IP.
<a href="#">CSCwf16116</a>	In a three-node cluster of Cisco DNA Center appliances, when one of the nodes is powered down and then powered back up, the services remain down. The expected behavior is that services rebalance within 15 to 30 minutes.
<a href="#">CSCwf18318</a>	The Task view shows that the provisioning completed successfully, but the new switch may not show up on the <b>Topology</b> window, where it can be changed to a fabric role.
<a href="#">CSCwf20392</a>	The AP Claim workflow may leave APs configured with default site tags and location parameters.
<a href="#">CSCwf23391</a>	In Cisco DNA Center, you subscribe to the event "no Activity on Radio," but this event is disabled on the <b>Issue Settings</b> window. Even though the event "no Activity on Radio" is disabled, it's seen on Issues & Events.
<a href="#">CSCwf23486</a>	When there are only two nodes, the Liveness probe fails on the primary node.
<a href="#">CSCwf25968</a>	Due to the default selection of Cisco DNA Center as a NetFlow server on the <b>Network Settings</b> window, the telemetry push task may fail while deploying network settings due to the unsupported configuration of NetFlow on IE 3000 series switches.

Bug Identifier	Headline
<a href="#">CSCwf26589</a>	<p>In Cisco DNA Center, when more than one device is selected for provisioning and the selection includes a Catalyst 9500 model, the "Advanced Configuration" step does not correctly show the templates for all devices, meaning not all devices or templates are displayed. For example, if only Catalyst 9300 devices are selected, the issue is not seen; the issue only occurs when the selection includes a Catalyst 9500.</p> <p><b>Note</b> The CSV format of the import/export template variables in the provisioning workflow has been fixed as part of this defect. Therefore, exported CSV files from 2.3.5.3 aren't acceptable and generate an invalid CSV file error when you try to import template variables based on the old CSV. You must export the latest CSV from 2.3.5.4 and use that as the basis for importing the template variables for both regular and composite templates.</p> <p>Related bug ID: <a href="#">CSCwf15199</a>.</p>
<a href="#">CSCwf29125</a>	Cisco DNA Center's config-archive-service may decline into an out of memory condition and restart repeatedly.
<a href="#">CSCwf31240</a>	Postgres fails due to a multiple primary issue.
<a href="#">CSCwf31445</a>	Cisco DNA Center may not create a second policy profile when a different VLAN group is created for the same WLAN in a second network profile, resulting in a partial configuration being pushed to a managed wireless controller.
<a href="#">CSCwf31965</a>	The wireless controller provisioning workflow may return an error in the Model Config tab of the <b>Provisioning</b> window.
<a href="#">CSCwf32124</a>	MAB clients using Open authentication are not reauthenticated when the switch reloads, or when they lose connection with the AAA server and that connectivity comes back.
<a href="#">CSCwf34712</a>	Cisco DNA Center is detected to be running weak ciphers.
<a href="#">CSCwf36885</a>	After an upgrade to Cisco DNA Center 2.3.3.6, the device inventory collection status may change to "internal error."
<a href="#">CSCwf37179</a>	Deploying a template with the "bound to source" variable doesn't work because the value is not saved correctly. The template simulation works correctly; however, generating a config preview or trying to provision a device with the variable fails.
<a href="#">CSCwf38305</a>	IP phones are misclassified and shown as rogue APs. IP phones are shown as a host on the switch, causing Cisco DNA Center to classify IP phones incorrectly. The same host MAC address is displayed for every High Rogue Threat alert.
<a href="#">CSCwf39426</a>	AP and planned APs overlay on the map.
<a href="#">CSCwf39469</a>	Provisioning may fail when trying to create a new port-channel or add a link to an existing port-channel in an SDA fabric device from Cisco DNA Center's <b>Host Onboarding</b> window.
<a href="#">CSCwf40854</a>	<p>Cisco DNA Center may fail to provision a Catalyst 9800 wireless controller. The following error is returned:</p> <pre>NCSF11108 CFS persistence failed deleted object would be re-saved by cascade.</pre>
<a href="#">CSCwf41422</a>	Cisco DNA Center's inventory service may restart frequently when several thousand discovery requests are queued up by an API call.



Bug Identifier	Headline
<a href="#">CSCwf43384</a>	A system compliance request causes Orchestration-engine-service in java.lang.StackOverflowError.
<a href="#">CSCwf44636</a>	The AP Refresh workflow doesn't work after upgrading from Cisco DNA Center 2.3.5.3 to 2.3.5.4.
<a href="#">CSCwf45474</a>	After a pause and unregister, Cisco DNA Center's disaster recovery virtual IP address is still available in the last known active cluster.
<a href="#">CSCwf45734</a>	The disaster recovery hangs in an ambiguous state where a user-actionable option is available.
<a href="#">CSCwf45762</a>	Cisco DNA Center disables the radios to make changes to any custom RF profile. This includes any out-of-band changes detected. On subsequent wireless controller provisioning, the 2.4-GHz band is disabled.
<a href="#">CSCwf47012</a>	When provisioning or updating telemetry to a Catalyst 2960C switch using Cisco DNA Center, an error is generated, even though NetFlow is not supported on the device.
<a href="#">CSCwf47760</a>	An open violation for the DNS server is not generated under Network Settings Compliance.
<a href="#">CSCwf48385</a>	Cisco DNA Center may show inaccurate information about the node state on the System Health window, citing the error, "The CIMC appliance is currently IP unreachable" when everything is functional.
<a href="#">CSCwf48403</a>	A Cisco DNA Center user wants to enable IP overlap on an SSID and defines this in the model config editor for flex configuration. While trying to provision the wireless controller, at Step 3 of the provision task where there is an option to choose a model config, a "constraint validation failure" error occurs for the applied model config. When the view option is clicked, the IP overlap toggle is displayed. When toggled once and saved, the error about the constraint validation failure disappears. When the provision is attempted after that, provisioning the model config fails, but the other items being provisioned succeed.
<a href="#">CSCwf48701</a>	An upgrade fails with the following exception: "Exception postgres FATAL: role "replicausser" does not exist." Some services restart constantly.
<a href="#">CSCwf53661</a>	An error is returned when a VLAN with 4 digits is configured with 64 VLANs in a single VLAN group.
<a href="#">CSCwf57289</a>	Cisco DNA Center may stop working completely when there are no Docker images left. The /data disk fills up due to rapid core or heap dumps generation by one or more applications. If one or more applications suffer crashes, they generate large-sized code crash reports that can fill up the disk partition where Docker images are cached. Due to a Kubernetes self-recovery mechanism that triggers garbage collection of Docker images to bring down the free disk space to above 15%, the deleted Docker images result in a Cisco DNA Center crash.
<a href="#">CSCwf62146</a>	RabbitMQ does not recover correctly after a node is powered on during three-node HA testing. Multiple services in a three-node cluster of Cisco DNA Center appliances may restart continuously.
<a href="#">CSCwf62922</a>	The Disaster Recovery GUI shows site Down and Up activities continuously. The disaster-recovery-service in the CLI shows multiple restarts. The haproxy container in disaster-recovery-service goes into a crashloop state. The haproxy logs show "SSL client certificate not trusted" error messages.
<a href="#">CSCwf63492</a>	Assurance data may continue to grow to the point where Elasticsearch hits red status. The purge job may become unable to connect to Elasticsearch to remove information because the connection to Identity Manager is refused.

Bug Identifier	Headline
<a href="#">CSCwf71659</a>	LAN automation may fail for a Catalyst 9407R Sup1XL with a 40G port running IOS-XE 17.3.4. The 40G port connected to the seed device may go into an Inactive state when stopping LAN automation, causing a loss of connectivity.
<a href="#">CSCwf73241</a>	Migration fails for file-service Objects in Mongoloid, wiping out maps after failover.
<a href="#">CSCwf74542</a>	Cisco DNA Center's aca-controller-service may degrade into a CrashLoopBackOff state after a node reboot.
<a href="#">CSCwf78576</a>	While deploying multicast on a VRF(X), the "LISP mobility" configuration under the interface VLAN and the "dynamic-eid" configuration under the router LISP are removed for multiple VLANs on another VRF(Y), which causes a major network outage.
<a href="#">CSCwf86819</a>	Cisco DNA Center 2.3.5.3 reports SPF-service-down and can't retrieve compliance-related device data.
<a href="#">CSCwh01986</a>	Cisco DNA Center may fail to provision a Catalyst 9800 wireless LAN controller. The following error is returned:  update or delete on table "sitetaginfo" violates foreign key constraint "fka8f74ee1e2aa2c55" on table "wirelessgrouping".
<a href="#">CSCwh16262</a>	AP PnP onboarding fails when using SNMPv3 + AES 256 on the embedded wireless controller.
<a href="#">CSCwh26174</a>	ThousandEyes agents are not shown in Assurance.

### Cisco DNA Center 2.3.5.3-70194-HF5 Hot Fix

The following table lists the resolved bugs in the Cisco DNA Center 2.3.5.3-70194-HF5 hot fix.



#### Note

- To obtain the hot fix, go to the **Software Management** window in the Cisco DNA Center GUI and install the 2.3.5.3-70194-HF5 hot fix. If you don't see it, scroll down and click "Looking for other releases? **Click here.**"
- The 2.3.5.3-70194-HF5 hot fix is visible only if you have 2.3.5.0 or 2.3.5.3 installed, not 2.3.5.4.

Bug Identifier	Headline
<a href="#">CSCwe15923</a>	Under some conditions, a newly installed, autogenerated etcd certificate in Cisco DNA Center does not get activated. When the etcd certificate does not get activated, the system might become unresponsive and inaccessible through the GUI, ultimately discarding network telemetry and losing the management capability of Cisco DNA Center.  CSCwe15923 is resolved in 2.3.5.4. For 2.3.5.3, this bug is resolved with the 2.3.5.3-70194-HF5 hot fix. If you upgraded from 2.3.5.3 to 2.3.5.4 before 2023-10-12, install the 2.3.5.4.70852-HF3 hot fix atop 2.3.5.4.

Bug Identifier	Headline
<a href="#">CSCwe72149</a>	<p>Cisco DNA Center blocks the ability for valid IP transit handoffs to be configured for any site, signaling the following error message:</p> <pre>Error: BGP AS Number must be between 1 and 65535.</pre> <p>This problem occurs with 2.3.3.7 or 2.3.5.3 if you are using a four-byte autonomous system number (ASN) and only under certain scenarios, as described below.</p> <p>Steps to reproduce:</p> <p>This problem occurs if you are on 2.3.3.7 or 2.3.5.3 and you attempt to create a new fabric border with an ASN that is greater than 65535. The following error message is logged:</p> <pre>Error: BGP AS Number must be between 1 and 65535.</pre> <p>This problem also occurs if:</p> <ol style="list-style-type: none"> <li>1. You are running a release other than 2.3.3.7 or 2.3.5.3, and the local ASN on the existing fabric border is greater than 65535 (for example, 500000).</li> <li>2. Upgrade to 2.3.3.7 or 2.3.5.3.</li> <li>3. Attempt to perform operations on a fabric border that contains the higher ASN. At this point, the following error message is logged:</li> </ol> <pre>Error: BGP AS Number must be between 1 and 65535.</pre>
<a href="#">CSCwf38534</a>	<p>Wireless controllers managed by Cisco DNA Center go into syncing state. This problem occurs when the wireless controller sends when large amounts of ciscoConfigManEvent traps to Cisco DNA Center. Cisco DNA Center should ignore configuration change traps (ciscoConfigManEvent) for processing.</p>
<a href="#">CSCwf56827</a>	<p>An SNMP trap is pushed with an incorrect group authentication mode, even when a read view is defined.</p>
<a href="#">CSCwf59179</a>	<p>Floor maps go missing and must be reuploaded. This problem occurs when floor map images are uploaded manually via the Cisco DNA Center GUI, but can also happen in certain cases after an Ekahau project, Cisco Prime Infrastructure map archive import, or Prime Infrastructure Data Migration Tool (PDMT) provides the floor images.</p> <p>Related bug ID: <a href="#">CSCwf70671</a>.</p>
<a href="#">CSCwf61895</a>	<p>When a wireless controller has a 9124AXE AP in bridge mode associated to it, provisioning that wireless controller may fail with the following error:</p> <pre>NCWL 12001: Channel or Power Assignment is not configured as custom for 5GHz Radio on the AP.</pre>
<a href="#">CSCwf63148</a>	<p>The LAN automation process may hang at the "Starting Seed Device Configuration" phase for Disaster Recovery 1+1+1 and a three-node cluster.</p>
<a href="#">CSCwh13140</a>	<p>Provisioning a 9124AX AP in mesh root AP mode fails with the following error:</p> <pre>Configuration on the device failed. Error: Unable to push to device WLC_IP using protocol ssh2 the CLI do ap name AP_NAME controller primary WLC_NAME WLC_IP. Device Response: % Error: no ap_name exists.</pre>

### Cisco DNA Center 2.3.5.3

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.5.3.

Bug Identifier	Headline
<a href="#">CSCvy30961</a>	Cisco DNA Center's <b>Smart Licensing</b> window does not load as expected and displays the following error:  Error in loading data. Please see log for more info.
<a href="#">CSCvz59447</a>	Cisco DNA Center fails to provision a managed device if the loopback0 interface IP address is not available.
<a href="#">CSCwb02969</a>	In a three-node setup, after provisioning a Cisco Catalyst 9500 Series Switch stack and completing the fabric configuration, the switch stack status changes to "Managed Internal error."
<a href="#">CSCwb99632</a>	SWIM report generation fails when the run time exceeds the defined maximum running time for the worker pod (16 hours).
<a href="#">CSCwc05125</a>	Cisco DNA Center wireless controller compliance fails with a mismatch in the WLAN policy profile name.
<a href="#">CSCwc39603</a>	When you configure a new event notification in Cisco DNA Center, the <b>Try It</b> option for the subscribed event returns the following error:  FAILURE - 'Endpoint Connection Timed Out.'
<a href="#">CSCwc79851</a>	In a single-node setup, while trying to deploy ThousandEyes 4.3.0 on switches (25 switches per pane), the following error was displayed:  Device Not Ready  To work around this problem, either change the pagination to 10 switches per pane, or filter the switches on which you want to install ThousandEyes.
<a href="#">CSCwd00896</a>	AP group-related configurations are not pushed in an implicit provisioning, which causes a wireless outage while resetting AAA inheritance.  To work around this problem, review the configuration before deploying it on the device.
<a href="#">CSCwd09391</a>	Cisco DNA Center orchestrated app hosting is disabled on the AP when the primary wireless controller is changed.
<a href="#">CSCwd13881</a>	For single node, Cisco DNA Center shows the slot 2 radio on 2800 Series APs.
<a href="#">CSCwd24258</a>	In a three-node setup, the provisioning task fails with the following error:  NCS010011: Error in generating CFS due to internal error
<a href="#">CSCwd25750</a>	Under scale, the kafka pod cannot handle data and slows down with gaps in the Assurance Health trend chart.
<a href="#">CSCwd26099</a>	While trying to create one IP network group, the GUI spins for longer than 5 minutes.
<a href="#">CSCwd27458</a>	Cisco Wireless Controller provisioning fails when the AAA Radius Attributes Configuration model config is attached to a network profile.

Bug Identifier	Headline
<a href="#">CSCwd28811</a>	While provisioning a Cisco Wireless Controller with an open SSID or an SSID without assigning AAA servers, Cisco DNA Center pushes a default accounting list.  To work around this problem, remove the default accounting list configuration manually, until next Cisco DNA Center provisioning.
<a href="#">CSCwd31345</a>	If external webauth SSIDs configured from Cisco DNA Center resolve to the same DNS servers, but in a different order, Cisco DNA Center pushes the flexconnect ACL on every wireless controller provisioning.
<a href="#">CSCwd33248</a>	The fabric wireless SSID window takes longer than 30 seconds to load.
<a href="#">CSCwd36272</a>	When an AP is provisioned with a new AP zone, all SSIDs go down after AP reprovisioning.
<a href="#">CSCwd36581</a>	AP outband config and provisioning from Cisco DNA Center policy tags are different.
<a href="#">CSCwd36789</a>	Provisioning failure occurs on N+1 with custom site tag or policy tag addition.
<a href="#">CSCwd37176</a>	When you try to delete a virtual network policy, the following error is displayed:  NCSP11001: User intent validation failed while processing the 'terminate' request.
<a href="#">CSCwd37272</a>	Cisco Catalyst 9800 Series Wireless Controller provisioning fails with the following error:  \$RadioType_config" is an invalid value.
<a href="#">CSCwd37292</a>	A wireless pool is deleted from the virtual network, despite being mapped to the fabric SSID.
<a href="#">CSCwd37822</a>	Cisco SD-Access: First-time reprovisioning of a Cisco Catalyst 9800 Series Wireless Controller causes WLAN SSIDs to flap in Cisco DNA Center. This problem occurs when the Cisco Catalyst 9800 Series Wireless Controller is upgraded to Cisco IOS XE 17.7.0 or later.
<a href="#">CSCwd37961</a>	After AP zone, policy tag, or site tag removal, the following error is displayed:  NCSP11108 Error occurred while processing.
<a href="#">CSCwd38259</a>	Cisco Wireless Controller or AP provisioning fails with an NCSP11001 error when changing between custom and Cisco DNA Center autogenerated site tags in a network profile.
<a href="#">CSCwd38863</a>	Cisco Adaptive Wireless Intrusion Prevention Service (aWIPS) is removed from the default AP profile during Cisco Catalyst 9800 Series Wireless Controller provisioning, even when aWIPS is enabled in the wireless network settings.
<a href="#">CSCwe39568</a>	A continuous java.lang.OutOfMemory error occurs when adding 20 pools or 10 VNs.
<a href="#">CSCwd40022</a>	A policy tag is not activated on the WLAN during an AP zone change from Cisco DNA Center AP provisioning.
<a href="#">CSCwd40306</a>	Cisco DNA Center is sending the SNMP trap payload field <code>snmpTrapAddress</code> with the external SNMP collector IP.
<a href="#">CSCwd40954</a>	When selecting sites under <b>Policy &gt; IP Based Policy</b> , it takes approximately 20 seconds to list the sites.
<a href="#">CSCwd42794</a>	Cisco Catalyst 9800 Series Wireless Controller provisioning fails after upgrading to Cisco DNA Center.
<a href="#">CSCwd43192</a>	Anchor wireless controller provisioning fails with the following error:  NullPointerException

Bug Identifier	Headline
<a href="#">CSCwd44800</a>	Removal of the anchor controller results in policy tag removal and outage.
<a href="#">CSCwd46164</a>	After upgrading a Cisco Catalyst 3850 Switch stack of two switches (from INSTALL mode), only one member comes up after reboot (in BUNDLE mode). The Cisco DNA Center audit logs show that incorrect commands were pushed for INSTALL mode upgrade, causing this issue.
<a href="#">CSCwd46246</a>	Template Hub Plug and Play Day-0 and Day- <i>n</i> templates associated with onboarding fail to attach to a profile.
<a href="#">CSCwd46870</a>	While configuring mobility, the screen takes approximately 25 seconds to load.
<a href="#">CSCwd47011</a>	<p>In Cisco DNA Center, a network profile is configured with custom site tags, policy tags, or flex profiles for the managed site of the Polaris Catalyst 9800 Series Wireless Controller. The Polaris Catalyst 9800 Series Wireless Controller is provisioned with the network profile-managed sites and the custom tags generated on the device as a placeholder for the AP provision to use the preprovisioned tags. In this scenario, the following cases are seen:</p> <ul style="list-style-type: none"> <li>• No preprovisioned tags, custom tags, flex tags, policy tags, or site tags are configured on the Polaris Catalyst 9800 Series Wireless Controller without an AP being part of that custom tag site.</li> <li>• If there are any preprovisioned tags or custom tags without an AP (configured before upgrade) and upgraded to Cisco DNA Center 2.3.37, wireless controller reprovisioning deletes the orphan custom tags.</li> </ul>
<a href="#">CSCwd47125</a>	Deleting an anchor results in stale mobility configs in N+1, which causes a provisioning failure in N+1.
<a href="#">CSCwd48297</a>	<p>In a network profile, you have flex-enabled and non-flex SSIDs. When you create an AP zone for only non-flex enabled SSIDs, the following validation error occurs:</p> <p>One or more Flex SSIDs need to be part of this zone as the site will be deployed as a flex site</p>
<a href="#">CSCwd48939</a>	<p>When you add a Cisco Wireless Controller through an API call to a fabric site that has a control plane node configured with LISP Pub/Sub, the provisioning fails with the following error:</p> <pre>FailureReason : Conversion of SDA PubSub Control Plane to SDA BGP/LISP Control Plane not supported. To change the Control Plane to SDA BGP/LISP, remove all Control Plane(s), Save and Re-Add Control Plane(s) to fabric site.</pre>
<a href="#">CSCwd49596</a>	Cisco Wireless Controller reprovisioning fails with an internal error.
<a href="#">CSCwd49629</a>	Unable to view error details because the device-config-status API returns a 504 error.
<a href="#">CSCwd50263</a>	Catalyst 9800 Series Wireless Controller provisioning fails with an error.
<a href="#">CSCwd53051</a>	AP zone addition in network profile and Cisco Wireless Controller provisioning results in the policy tag getting updated for the AP.
<a href="#">CSCwd53091</a>	After deleting an AP zone, there is a policy tag mismatch between the N and N+1 controllers.
<a href="#">CSCwd53101</a>	<p>Cisco Wireless Controller provisioning fails with the following error:</p> <pre>NCSP11001: User intent validation failed while processing the 'modify' request. Additional info for support: taskId: 'ae6b113b-d3ce-4cb0-8361-db00fdbe3c60'</pre>

Bug Identifier	Headline
<a href="#">CSCwd53571</a>	Cisco DNA Center fails to reprovision a Cisco Wireless Controller after the AP zones in the network profiles are updated with tags.
<a href="#">CSCwd53607</a>	Deleting a Cisco Catalyst 9800 Series Wireless Controller and adding it again to Cisco DNA Center generates a Flex ACL IPv6/EXT_RE_ACL_IPV6 compliance error for Network Profile after provisioning.
<a href="#">CSCwd54833</a>	AP groups without an associated AP zone are removed from the Cisco AireOS Wireless Controller after provisioning.
<a href="#">CSCwd55727</a>	Wireless provisioning fails during the validation phase.
<a href="#">CSCwd55811</a>	While trying to add a sensor to a floor, the filter option doesn't work in the <b>Network Hierarchy</b> window.
<a href="#">CSCwd56050</a>	The Configuration Archive report does not display in PDF format.
<a href="#">CSCwd56704</a>	Changing a custom policy tag's site results in moving the AP to the default policy tag.
<a href="#">CSCwd57297</a>	Custom site tags are not created, even though a success message is shown.
<a href="#">CSCwd58125</a>	During upgrade, Cisco Catalyst 9800 Series Wireless Controller provisioning fails with the following error:  No device lock required in RFS flow - PMF
<a href="#">CSCwd58701</a>	A disaster recovery failure occurs with the following error:  NCFS10077: Disaster recovery mandatory data missing,namespace=ejbca,filename=<xyz> is not present in mongodb
<a href="#">CSCwd59216</a>	While provisioning a Cisco Catalyst 9800-CL Wireless Controller running on Cisco IOS XE 17.3.5a/17.7.1/17.3.3, provisioning fails with the following error:  NCSP11108: Error occurred while processing the request.
<a href="#">CSCwd59876</a>	When you provision a nonfabric WLAN (locally switched) on a fabric wireless controller, it converts the APs to flex mode, which is not a supported scenario for fabric deployments.
<a href="#">CSCwd62967</a>	Cisco DNA Center Inventory Telemetry: Compute resources run out on the cloud side.
<a href="#">CSCwd63406</a>	Wireless provisioning creates tasks with an incorrect task hierarchy.
<a href="#">CSCwd66051</a>	On a Cisco Catalyst 9800 wireless LAN controller, the output of <code>show telemetry ietf subscription all detail</code> shows many invalid subscriptions with the following error:  Notes: Subscription limit reached.
<a href="#">CSCwd67305</a>	Cisco DNA Center provisioning of AAA to transit control plane fails during the configuration deployment or network intent with the following error:  Unable to push configuration to device x.x.x.x. Device Response - This operation will permanently convert all relevant authentication commands to their CPL control-policy equivalents. As this conversion is irreversible and will disable the conversion CLI 'authentication display [legacy new-style]'

Bug Identifier	Headline
<a href="#">CSCwd68079</a>	<p>In the WLAN advance window, Fast Transition (802.11r) must be enabled at the site level.</p> <p>Fast Transition (802.11r) is not inherited at the site level. It remains grayed out, because of which site override is not possible.</p> <p>Unable to change Fast Transition (802.11r) after the initial configuration at the site level.</p>
<a href="#">CSCwd68327</a>	After a network outage, postgres occasionally goes out of sync and does not recover.
<a href="#">CSCwd75024</a>	Cisco DNA Center fails to enable application telemetry on wireless LAN controllers due to an exception that occurs during device controllability configurations in application telemetry.
<a href="#">CSCwd75501</a>	<p>When you rerun the Security Advisory report, it fails and displays the following error:</p> <pre>BAPI Execution Failed. Response Code = 500, Response Content=null</pre>
<a href="#">CSCwd77279</a>	During power loss of a network device on Cisco DNA Center, the device is not populated as DEVICE_UNREACHABLE until a scheduled or manual resync occurs.
<a href="#">CSCwd79307</a>	<p>While syncing images, the following error occurs:</p> <pre>Getting device mdf data Failed-Invalid Index</pre>
<a href="#">CSCwd79358</a>	When Cisco Catalyst 9000 Switches are integrated in Cisco DNA Center through the Meraki Dashboard, they are displayed as third-party devices. Applications like SWIM and SDA provisioning don't work on those Catalyst 9000 devices. Also, you can't add any new images to the <b>Image Repository</b> window or sync any images with cisco.com until those Catalyst 9000 devices are removed from the inventory.
<a href="#">CSCwd79923</a>	When you choose ALL as the License mode, no devices are listed in the <b>Devices</b> tab.
<a href="#">CSCwd83022</a>	<p>Cisco Wireless Controller provisioning fails with the following error:</p> <pre>Validation failed node-1:dbm:wireless:Same WLAN ID 18 is already present in database</pre> <p>To work around this problem, do the following:</p> <ol style="list-style-type: none"> <li>1. Delete the WLAN from the network profile and save the changes.</li> <li>2. Reprovision the wireless controller.</li> <li>3. Add the WLAN to the network profile.</li> </ol>
<a href="#">CSCwd84123</a>	<p>In Cisco DNA Center, enabling features in fabric IP pools (for example, enabling a wireless pool) results in a provisioning failure on fabric devices with the following error:</p> <pre>Unable to push to device x.x.x.x using protocol ssh2 the CLI router lisp. Device Response - %No policy information.</pre> <p>To work around this problem, enable a new fabric view, revert the changes, and attempt to re-enable the desired feature.</p>
<a href="#">CSCwd84374</a>	<p>After an extended node pool (Anycast Gateway) is defined and subsequently deleted from a fabric site, LAN automation does not proceed beyond the seed configuration stage. This problem is triggered after the extended node pool is deleted from the fabric site, even if no devices have been onboarded previously into Cisco DNA Center.</p> <p>The network orchestration log shows that the extended node onboarding workflow is trying to proceed, even though there is no extended node pool defined. This prevents LAN automation from working.</p>



Bug Identifier	Headline
<a href="#">CSCwd84447</a>	After a primary/standby node restart, a <code>Connection refused</code> error occurs.
<a href="#">CSCwd86638</a>	Addition of a node on Cisco DNA Center 2.3.3.5 fails on an upgraded cluster.
<a href="#">CSCwd86714</a>	After upgrading to Cisco DNA Center 2.3.3.5, the sticky-scheduler service is down.
<a href="#">CSCwd88946</a>	The AI-enhanced RRM site selection operation fails.
<a href="#">CSCwd89482</a>	SWIM internal calls go to proxy, causing issues with image distribution, image update, or Cisco DNA Center CA trustpoint push.  To work around this problem, delete the proxy from settings, restart the SWIM container, and force push the telemetry.
<a href="#">CSCwd90641</a>	In a single-node setup, AP provisioning fails with the following error:  <code>ERROR: duplicate key value violates unique constraint "wirelessgrouping_bk"</code>
<a href="#">CSCwd91440</a>	After upgrading from Cisco DNA Center 2.3.5.0.70583 to 2.3.5.0.70586, the Cisco Catalyst 9800 Series Wireless Controller provisioning fails with an <code>NCSP11108</code> error.
<a href="#">CSCwd92838</a>	A new device that is in reachable and managed state does not show the golden image in the inventory window, even when the golden image is assigned to that new device.
<a href="#">CSCwd93194</a>	The Cisco DNA Center GUI login hangs and maglev commands fail to run due to the following error:  <code>API rate limit exceeded</code>
<a href="#">CSCwd93259</a>	After upgrade, the devices in the License Manager show the "Needs re-registration" tag, even though the connection mode hasn't changed.
<a href="#">CSCwe04247</a>	An error occurs while applying a critical fix for the Closed Authentication mode template update.
<a href="#">CSCwe05972</a>	Duplicate validation must be checked for the complete source and destination, which includes source port and destination port, and so on. Currently, a check is added only for IP addresses. Using Cisco DNA Center's pre-auth ACL list, the user cannot have a TCP ACL with the same IP address on a different port.
<a href="#">CSCwe06738</a>	While upgrading from Cisco DNA Center 2.3.4 to 2.3.5, downloading fails with the following error:Exception in package:  <code>Exception in package: automation-core, kind: ServiceBundleGroup, name: apicem-basics - Shell command timed out after &lt;n&gt; seconds of inactivity: /srv/maglev/replicated_storage//fusion/plugin_type_catalog/model/7.1.610.60911/install UPGRADE</code>
<a href="#">CSCwe10186</a>	When bulk sites are selected to create fabric zones, the wrong fabric zone is assigned for multicast pools. This causes the multicast IP lookup to fail, and provisioning fails for that device.  To work around this problem, select one site at a time to create fabric zones.
<a href="#">CSCwe10342</a>	Cisco DNA Center's SPF services crash while previewing the configuration of a wireless LAN controller provisioning. The SPF service crash occurs with an <code>OutOfMemoryError</code> during wireless controller provisioning with 3250 sites.
<a href="#">CSCwe11463</a>	After disaster recovery failover, image distribution for devices hangs at 10% for several hours with a "Distributing Image with null Protocol Running" state.

Bug Identifier	Headline
<a href="#">CSCwe15942</a>	Upon clicking an image family name on the <b>Image Repository</b> window, it redirects to <b>Design &gt; Image Repository &gt; Image Family</b> . The image family name is displayed as the title, but no image is displayed under the <b>Image Repository</b> window.
<a href="#">CSCwe17325</a>	For a Cisco Catalyst 3850 Switch with 16.12.x, the base image gets deleted before the SMU is copied to the switch.
<a href="#">CSCwe19750</a>	Provisioning a Cisco Catalyst 9800 Series Wireless Controller with an AI RF profile pushing 6 GHz with non-Europe-compliant channels fails with the following error:  Unable to push configuration to device X.X.X.X. Device Response Validation failed node-2:dbm:wireless:Configured countries do not support the channel 101
<a href="#">CSCwe28523</a>	In a Cisco DNA Center setup using disaster recovery, the MongoDB replication fails with a conflict error.  When this problem occurs, the log from the dr-mongodb-replicator service displays a message similar to the following example:  [23:22:44 UTC 2023/02/05] [EROR] (mongoshake/executor.(*BulkWriter).doUpdate:349) detail error info with index[0] msg[Updating the path 'lastProbeCollectionTimeStamp' would create a conflict at 'lastProbeCollectionTimeStamp'] dup[false]
<a href="#">CSCwe31951</a>	In a three-node setup, full backup fails for NDP Elasticsearch with the following error:  "no_such_file_exception"
<a href="#">CSCwe32845</a>	In a three-node cluster, after upgrading from Cisco DNA Center 2.3.3.6 to 2.3.3.7, a large number of unbound queues are seen in RabbitMQ.
<a href="#">CSCwe33933</a>	Deploying changes to fabric, provisioning of fabric devices from inventory, and device compliance checks fail with the following error:  NCSO10001: CFS validation failed due to internal error
<a href="#">CSCwe35389</a>	Cisco DNA Center's release download hangs on the main system package while calculating requirements.
<a href="#">CSCwe36863</a>	With a backward compatibility check, the BAPI response does not generate a BAPI error with the invalid interface name in the POST call of the wireless profile.
<a href="#">CSCwe39334</a>	Fabric provisioning fails with an error stating that a pool has intra-subnet routing enabled.  To work around this problem, delete and recreate the offending pool.
<a href="#">CSCwe39344</a>	When you configure a new event notification in Cisco DNA Center, the <b>Try It</b> option for the subscribed event returns the following error:  Endpoint Connection Timed Out
<a href="#">CSCwe39650</a>	The template does not configure the correct name when used with a bind to source with the wireless network profile.
<a href="#">CSCwe39718</a>	After you attach a template to a profile, the count is not shown in the <b>Template Hub</b> window.
<a href="#">CSCwe41944</a>	Unsupported images are listed under the Cisco Catalyst 9200 Series Switches, which causes devices to go into ROMMON mode.

Bug Identifier	Headline
<a href="#">CSCwe42201</a>	After upgrading Cisco DNA Center from 2.3.3.5 to 2.3.3.6, the appliance goes into a constant reboot loop.
<a href="#">CSCwe44726</a>	PnP onboarding fails for certain switches with the following error: AP PNP Claim failed. Invalid RF-Profile: null
<a href="#">CSCwe47539</a>	Cisco DNA Center application upgrade fails with an exception in the group-based-policy-analytics package.
<a href="#">CSCwf12001</a>	Cisco DNA Center upgrade from 2.3.3.7 to 2.3.5.3: AP authorization is enabled for a normal (regular) AP.

### Cisco DNA Center 2.3.5.0

The following table lists the resolved bugs in Cisco DNA Center, Release 2.3.5.0.

Bug Identifier	Headline
<a href="#">CSCwa22823</a>	AireOS wireless controller provisioning fails during the deployment stage in Network Programmer.
<a href="#">CSCwa77904</a>	Cisco Wireless Controller provisioning fails with the following error: NCSP10246: Internal error while attempting to transform the object for further processing.
<a href="#">CSCwb28540</a>	A tag mismatch is seen between the primary and secondary controller.
<a href="#">CSCwb51750</a>	User intent validation of Cisco Catalyst 9800 Series Wireless Controller fails with a change in the network profile.
<a href="#">CSCwb85233</a>	A third-party device is reported as Catalyst 9800 Series Wireless Controller for Cloud.
<a href="#">CSCwc02517</a>	Cisco DNA Center selects a switching profile for a wireless controller if the same sites are assigned to switching and wireless.
<a href="#">CSCwc12746</a>	AP provisioning fails with the following error: Cannot delete AP mac from the custom APG on the N+1 HA device.
<a href="#">CSCwc18664</a>	External AAA with RADIUS and TACACS is not displayed under the WLAN AAA section.
<a href="#">CSCwc39642</a>	Cisco DNA Center 2.3.3.x event notifications using Webex, REST, and email stop working after an upgrade.
<a href="#">CSCwc42824</a>	AP provisioning fails because Cisco DNA Center pushes duplicate commands in sequential order.
<a href="#">CSCwc62887</a>	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.
<a href="#">CSCwc76362</a>	Devices show an internal error due to the following exception: Exception while persisting: java.lang.NullPointerException.
<a href="#">CSCwc93896</a>	AP and wireless controller provisioning fails due to the following error: NCSP10001: User intent validation failed.

Bug Identifier	Headline
<a href="#">CSCwc94852</a>	Cannot provision or delete the wireless controller due to the following error: NCSFP11108 CFS persistence failed.
<a href="#">CSCwc96069</a>	The Cisco DNA Center platform license reports fail with the following error message: Sorry, data aggregation failed - missing cache of invalid parameters. Please try later or create new report.
<a href="#">CSCwc98950</a>	Cannot export the hierarchy to the CMX for one or more domains.
<a href="#">CSCwc99150</a>	Wireless controller provisioning fails after changing the VLAN for the SSID under network profile.
<a href="#">CSCwd08429</a>	Cannot assign SGT to Policy Extended Node port assignment.
<a href="#">CSCwd08474</a>	Reprovisioning BAPI fails with the following error: Interface Input Error: Duplicate IP found.
<a href="#">CSCwd18464</a>	Cisco DNA Center incorrectly shows C1000-8P-2G-L as supported.
<a href="#">CSCwd22124</a>	Cisco DNA Center takes too long to identify an AP IP address.
<a href="#">CSCwd26583</a>	Cisco DNA Center keeps repushing the TACACAS configuration on every wireless controller provisioning.
<a href="#">CSCwd30229</a>	The add and update APs return a success response for Execution ID, but the SSID and segment mapping are not updated in the fabric.
<a href="#">CSCwd30455</a>	HTML code is displayed in the task name of image distribution.
<a href="#">CSCwd34162</a>	Cannot apply CLI credentials at a site.
<a href="#">CSCwd34763</a>	Cisco DNA Center may configure AP tags with default values, rather than the site tags configured in the network profile.
<a href="#">CSCwd46904</a>	A device upgrade from 16.x to 17.x fails during activation through three-step activation.
<a href="#">CSCwd59885</a>	After upgrading to Cisco DNA Center 2.3.5, the Command Runner task gets stuck on the ECA device.

## 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.

### AI-Enhanced RRM Guidelines

In earlier releases, Cisco DNA Center marked the AI-Enhanced RRM tasks as failed if the AP provisioning didn't complete within 3 hours. During scale provisioning for a large number of APs, provisioning can take a longer time. Even if the tasks were marked as failed after 3 hours, the AP provisioning continued in Cisco DNA Center.

Effective with Release 2.3.5.6, the timeout value for AI-Enhanced RRM tasks is increased to 24 hours to accommodate the scale provisioning scenarios for large number of APs.

### 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.

### 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 supports only native multicast across multiple fabric sites that are connected by an SD-Access transit. Head-end replication is not supported over SD-Access transit.
- Multicast routing over LISP/BGP SD-Access Transit is not supported.

### Cisco DNA Center on AWS Limitations

- Cisco DNA Center on AWS supports only the r5a.8xlarge instance size. Any changes to this configuration aren't supported.
- Cisco DNA Center on AWS doesn't support the Federal Information Processing Standards (FIPS).
- Cisco DNA Center on AWS doesn't support IPv6.
- Cisco DNA Center on AWS doesn't support disaster recovery. Therefore, we recommend that you don't install the optional Cisco DNA Center Disaster Recovery (DR) package.

### 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.
- Starting in Cisco DNA Center 2.3.5.4, when you export the Inventory, the export file includes up to 10,000 devices total, including APs. Credential information is excluded from the export file.

In earlier releases, the export file didn't have the 10,000-device limit and APs were excluded.

- 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 Limitations

- With IPDT on trunk ports, rogue-on-wire detection is impacted. Cisco DNA Center does not show all the clients connected to a switch through an access point in bridge mode. The trunk port is used to exchange all the VLAN information. When you enable IP device tracking on the trunk port, clients connected on the neighbor switch are also shown. Cisco DNA Center does not collect client data if the connected interface is a trunk port and the neighbor is a switch. As a best practice, disable the IP device tracking on the trunk port. Rogue-on-wire is not detected if IP device tracking is enabled on the trunk port. See [Disabling IP Device Tracking](#) for more information.
- When you add a line card to a chassis, or remove a line card from a chassis, the changes take several minutes to update on Cisco DNA Center. Any IPDT configurations are pushed to the device automatically for newly added interfaces.
- When you add a device to a stack pool, or remove a device from a stack pool, the changes take several minutes to update on Cisco DNA Center. Any IPDT configurations are pushed to the device automatically for newly added interfaces.

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



### Encryption Limitation with SNMPv3

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

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

### IPv6 Limitations

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

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

- 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.
- To generate a Rogue and aWIPS report, you must choose a site hierarchy that contains a maximum of 254 floors. If you choose a site hierarchy that contains 255 floors or more, the Rogue and aWIPS report fails to generate.

### 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.

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

---

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

© 2022–2024 Cisco Systems, Inc. All rights reserved.