Release Notes for Cisco Catalyst Center, Release 3.1.6

Contents

Catalyst Center, Release 3.1.6

Cisco Catalyst Center is a comprehensive network management solution with functionality that spans all aspects of modern network management, including design, discovery, policy, provisioning, predictive analytics, intelligent monitoring, visibility, and compliance. Catalyst Center includes built-in automation and simplified workflows to help ensure efficiency and consistency in operations.

This document describes the features, limitations, and bugs for Catalyst Center, Release 3.1.6.

Note: Catalyst Center 3.1.6 is available as a controlled availability release. Contact your Cisco sales representative to request access to this release.

Table 1. Change history to this document since its initial release

Date	Change	Location
2025-12-18	Initial release	_

New software features

Package versions in Catalyst Center 3.1.6

Table 2. Package versions in Catalyst Center 3.1.6

Package name	Release 3.1.6
Release build version	
Release version	3.1.6-75205
System updates	
System	3.1.283
System Commons	2.734.65386
System Addons	0.10.506
Package updates	
Access Control Application	2.734.65386
AI Endpoint Analytics	3.160.26
AI Network Analytics	4.0.35
Application and Service Remediation	3.16.23
Application Hosting	2.4.225112005
Application Visibility and Policy	2.734.117614

Assurance	3.160.192
Assurance – Sensor	3.160.159
Automation – Intelligent Capture	2.734.65386
Automation – Sensor	2.734.65386
Catalyst Center API Catalog	6.8.515
Catalyst Center Gateway Service	0.10.509
Cisco Catalyst Center Global Search	6.9.4
Cisco Catalyst Center Platform	6.9.517
Cisco Catalyst Center UI	3.5.507
Cisco Identity Services Engine Bridge	3.160.38
Cloud Connectivity	6.10.505
Cloud Connectivity – Contextual Content	7.0.505
Cloud Connectivity – Digestor	7.0.503
Core Platform	0.10.549
Disaster Recovery	2.734.365017 **Note**: This package is available only for the on-premises hardware appliance, not for the virtual appliance.
DxHub Cloud Connectivity	6.10.516
Group Based Policy Analytics	3.160.114
Identity and Access Management	5.4.510
Identity and Access Management - UI	5.4.504
Multiple Cisco Catalyst Center	2.734.65386
Network Controller Platform	2.734.65386

Network Data Platform - Base Analytics	3.160.10127
Network Data Platform - Caching Infra	6.6.503
Network Data Platform - Core	6.6.504
Network Data Platform - Ingestion Infra	6.6.505
Network Data Platform - Manager	6.6.101
Network Data Platform - Pipeline Infra	6.6.505
Network Data Platform - Storage Management	6.6.503
Platform Refresh	1.4.40
RCA-Scripts Package	0.5.7
Rogue and aWIPS	3.1.411
SD Access	2.734.65386
Shared Managed Services	0.10.512
Stealthwatch Security Analytics	2.734.1095099
Support Services	2.734.885129
System Management Operations	1.6.511
Telemetry	4.7.502
Wide Area Bonjour	2.734.755017

Disaster Recovery witness

The Disaster Recovery witness is available as a separate OVA file for Catalyst Center. Its version number is 2.1.734.370011.

Catalyst Center

Table 3. New and changed features in Catalyst Center 3.1.6

Product impact	Feature	Description
Base functionality	Security service insertion for SD-Access	Catalyst Center supports security service insertion to enhance security for SD-Access fabric networks by steering the traffic through firewalls based on predefined policies. **Note:** This feature is in beta.

Product impact	Feature	Description
	SNMPv3 authentication support for SHA256	Catalyst Center now supports SHA256 as an SNMPv3 authentication type. The use of SHA256 provides a stronger authentication mechanism compared to older algorithms, enhancing the security of SNMP communication with Catalyst Center.
	Support for campus networks	The Campus Network feature in Catalyst Center enables you to manage devices across multiple sites using networks and device groups. You can compare device configurations and learn or create group profiles within your network. **Note:** This feature is in beta.
	Traffic steering policy configuration	Catalyst Center supports the configuration of traffic steering policies to redirect the required traffic to the firewall. You can use the traffic steering policies for security service insertion. **Note:** This feature is in beta.

Cisco Catalyst Assurance

Table 4. New and changed features in Cisco Catalyst Assurance 3.1.6

Product impact	Feature	Description
Ease of use	View details of all rogue APs on a floor	You can view the precise location of all rogue APs and their threat levels on a floor map.

Catalyst Center platform

Table 5. New and changed features in Catalyst Center platform 3.1.6

Product impact	Feature	Description
Base functionality	API Operations	The Catalyst Center platform supports new API operations. For more information, see “New and changed information” in the Cisco Catalyst Center Platform User Guide. For detailed information about the API operations, see the Cisco Catalyst Center APIs on Cisco DevNet.
	Assurance Event	The Catalyst Center platform supports a new Assurance event called NETWORK-FABRIC_WIRED-1-338, which triggers when firewall connectivity goes down from a fabric edge node for a specific VRF and firewall IP. This firewall IP reachability issue monitors the availability of a route from edge nodes to the firewall in fabric sites with service insertion enabled. One issue is generated for each unique edge node, firewall IP, and VRF combination.
Ease of use	Client Report	The Catalyst Center platform supports a new Client report template called Client Roam Events. Use this template to generate a report on devices that frequently (within 10 minutes) switch between adjacent access points (APs) despite being stationary. For more information, see “New and changed information” in the Cisco Catalyst Center Platform User Guide.

Catalyst Center Automation

Table 6. New and changed features in Catalyst Center Automation 3.1.6

Product impact	Feature	Description
Base functionality	AP Locally Significant Certificate (LSC) renewal for wireless devices	Catalyst Center enables you to create AP LSC renewal profiles and renew the AP LSCs for wireless devices before its expiry. **Note:** The device must be running Cisco IOS XE Release 17.1.7.1 or later. In the **Provision** > **Inventory** window, the **Certificate Expiration** and **Certificate Type** columns are added to the **Devices** table for easier access to certificate information.
	Enhancements to 802.11be profiles	For Cisco IOS XE Release 17.18.1, the 802.11be profiles have these enhancements: • **Mark as default** toggle button to set an 802.11be profile as the default profile. • Support for Multi-Link Operation (MLO) groups to use multiple frequency bands at the same time. In the **Design** > **Network Settings** > **802.11be Profiles** window, the table has these enhancements: • A new **Type** column indicates whether the 802.11be profile is set as the default profile. • A new info icon next to the **Wireless Network Profile** column displays information about the network profiles and SSIDs associated with an 802.11be profile.
	Enhancements to Per-Device Configurations for Cisco Catalyst 9800 Series Wireless Controllers	The Per-Device Configuration feature on Catalyst Center now supports these configurations and parameters for a Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS XE Release 17.18.1 or later: • Enhancements to 802.11be configurations • Wi-Fi 7 per-band status in WLAN profiles • WLAN scheduler in policy profiles • LSC provision • AP upgrade configurations
	Support for Cisco Wireless 9171I Series Access Points	Catalyst Center supports the Cisco Wireless 9171I Series Access Points for Wi-Fi 7 configuration with Cisco IOS XE Release 17.18 or later. This AP supports dual-band (XOR) capability allowing slot 1 to operate in either 5-GHz or 6-GHz radio modes. **Note:** When configuring this AP using the **Configure Access Points** workflow, you can't configure the radio parameters for slot 1 in the **Configure 5 GHz Radio Parameters** or **Configure 6 GHz Radio Parameters** windows. Instead, use the **Configure Dual-Band (XOR) Radio Parameters** window to manage these settings.

Cisco Software-Defined Access

Table 7. New and changed features in Cisco Software-Defined Access 3.1.6

Product impact	Feature	Description
Base functionality	Support for Cisco C9350 Series Smart Switches as fabric edge device	Catalyst Center supports Cisco C9350 Series Smart Switches as edge devices within a fabric network. **Note:** Cisco C9350 Series Smart Switches do not support wireless capability or the configuration of extended nodes.

Changes in behavior

Table 8. Changes in behavior in Catalyst Center 3.1.6

Change	Description
Catalyst Center integration with CMX 11.0 and TLS 1.3	Starting with CMX 11.0, TLS 1.2 is no longer supported by default; only TLS 1.3 is supported. Catalyst Center 3.1.6 supports FIPS 140-3, TLS 1.3, and the corresponding cipher suites required by CMX 11.0. If you enable Common Criteria and lock the TLS version to TLS 1.2, integration with CMX 11.0 or later may fail. Older CMX versions, such as 10.6.x, support TLS 1.2 and do not present integration issues. From CMX 11.1.0 and later, new configuration options are available to re-enable TLS 1.2 support. For details, see the Cisco CMX 11.1 Release Notes and the Cisco CMX 11.1 Command Reference.
Minimum periodic resync interval increases to 6 hours	The minimum periodic resync interval (both per device and global) has been increased from 25 minutes to 6 hours to improve performance and optimize resource allocation. • Any device with a resync interval of less than 6 hours will automatically have its interval increased to the new minimum of 6 hours. • Devices already configured with a resync interval of 6 hours or longer will remain unchanged. • If the global resync interval is set to less than 6 hours, it will be increased to 6 hours. If the global resync interval is already 6 hours or more, it will remain unchanged.
Mobility configuration option removed from Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller	In the left pane of the device details window for a Cisco Catalyst 9800 Series Wireless Controller with Per-Device Configuration enabled, the **Mobility** option under **Global Wireless Configurations** and these tabs are removed: • Global Configuration • Peer Configuration
OFDMA uplink, OFDMA downlink, MU-MIMO uplink, and MU-MIMO downlink configuration changes for 802.11be settings	Starting with Cisco IOS XE Release 17.18.2, the **OFDMA Uplink**, **OFDMA Downlink**, **MU-MIMO Uplink**, and **MU-MIMO Downlink** parameters are deprecated and ignored in these 802.11be configurations: • 802.11be profiles for the 2.4-GHz and 5-GHz bands • **802.11BE PARAMETERS** section in RF profiles for the 6-GHz band To configure these settings: • For the 2.4-GHz and 5-GHz bands: use the **802.11ax Configuration** tab in the **Advanced SSID Configuration** feature template. • For the 6-GHz band: use the **802.11AX PARAMETERS** section in the RF profiles.

Deprecated features

Table 9. Deprecated features in Catalyst Center 3.1.6

Feature	Description
Support for Cisco Umbrella	Catalyst Center deprecates and discontinues support for Umbrella. Data collected for Umbrella will be permanently deleted from Catalyst Center.

Resolved issues

You can use the Cisco Bug Search Tool to search for a specific bug or to search for all resolved bugs in this release.

Open issues

You can use the Cisco Bug Search Tool to search for a specific bug or to search for all open bugs in this release.

To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com

Table 10. Open issues for Catalyst Center 3.1.6

Bug ID	Description
CSCwr86684	If the configuration **ip ssh server algorithm hostkey ecdsa-sha2-nistp256** is used without the configuration **crypto key generate ec keysize 256 label ecdsa-key**, the device accepts the hostkey ecdsa-sha2-nistp256 configuration but doesn't serve the ECDSA algorithm as configured.

Known issues

Table 11. Guidelines and limitations for Catalyst Center 3.1.6

Feature	Description
Guidelines	
APs	A wireless controller configuration change triggers only a wireless controller synchronization. During this synchronization, Catalyst Center: • collects the wireless controller-related configurations, but • doesn't update the configuration and status of the APs associated with the wireless controller. To view updated information for APs associated with the wireless controller (like AP status, new AP discovery, AP configuration, and so on), you must manually perform a full wireless controller synchronization. For a full synchronization, complete these steps: **Step 1.** On the Inventory window, select the wireless controller. **Step 2.** Choose **Actions > Inventory > Resync Device**.
Stealthwatch Security Analytics	If you are upgrading from Release 2.3.7.x to 3.1.x, you must have **Write** permissions for **Stealthwatch** to provision Stealthwatch Security Analytics on a device. With only **Read** permissions, you can't edit or provision the configurations. Update the permissions before or after the upgrade to enable editing and provisioning the configurations.
Limitations	
AP Locally Significant Certificate (LSC) renewal for wireless devices	When you renew the AP LSC certificate in the Catalyst Center inventory, the AP certificate status shows as **Started** on the **Renew Access Point Certificate** window even after successful certificate renewal. This issue is a display issue only and the AP certificates are renewed correctly. To verify successful renewal, check the certificate expiry time, which reflects the updated value.

Feature	Description
Per-Device Configurations	• When a wireless controller that is managed through Per-Device Configurations is upgraded to Cisco IOS XE Release 17.18.x from 17.15.x, the self-signed trustpoint name is not displayed in the Per-Device Configuration window while configuring HTTPS, web authentication, EAP profile, and management trustpoints with day-n changes. When this issue occurs, configure the trustpoint directly on the Cisco Catalyst 9800 Series Wireless Controller using CLI or Web UI. • When a wireless controller is configured to use an LSC as its management trustpoint, only APs with valid LSCs can join. New APs, especially the APs onboarded through Plug and Play (PnP), present a Manufacturer Installed Certificate (MIC) during their initial join attempt. The wireless controller rejects these APs, so root certificate updates cannot occur. To ensure successful onboarding, configure the AP certificate policy on the Cisco Catalyst 9800 Series Wireless Controller Web UI to temporarily allow MIC-based APs to join. After onboarding, update the AP certificate policy to use an LSC. For more information, see Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.
In-product help	• Online help and Interactive Help are available in light mode only and don't support dark mode. • When you place the Interactive Help widget on the top-right, right-center, and bottom-right locations, if you hover your cursor beyond the right edge of the widget, the widget may flicker.
Upgrade	In-Service Software Upgrade (ISSU) is not supported in Cisco SD-Access deployments, with this exception: Catalyst IE3200, IE3300, and IE3400 switches are classified as low-flash memory devices. Although Catalyst Center typically recommends using install mode for SWIM upgrades, this method may fail on Catalyst IE switches when upgrading from Cisco IOS XE Release 17.x to 17.12.x. Therefore, for SWIM upgrades in install mode, we recommend upgrading the switch to Release 17.15.x or later. If you are using bundle mode, you can upgrade the switch to Release 17.12.x.
Upgrade	ISSU is not supported on the Cisco C9610 Smart Switch when upgrading from Cisco IOS XE Release 17.18.1 to 17.18.2. Although Catalyst Center typically recommends using install mode for SWIM upgrades, SWIM will continue to function, but ISSU will not work due to compatibility limitations specific to Cisco C9610 Smart Switches when upgrading from 17.18.1 to 17.18.2.

Compatibility

Catalyst Center compatibility matrix

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

Cisco SD-Access compatibility matrix

For information about Cisco SD-Access hardware and software support for Catalyst Center, see the Cisco Software-Defined Access Compatibility Matrix.

Compatible browsers

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

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

Screen resolution:

- Minimum: 1368 x 768 pixels
- Recommended: 1920 x 1080 pixels

We recommend that the client systems you use to log in to Catalyst Center be equipped with 64-bit operating systems and browsers with internet access to the *.cisco.com domain.

Supported upgrade paths

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

Before you upgrade, use the Validation Tool to perform an appliance health and upgrade readiness check for Catalyst 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 Catalyst Center Administrator Guide.

Scalability

Catalyst Center scale

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

Support for the Web Content Accessibility Guidelines 2.1 standard

Catalyst Center supports the Web Content Accessibility Guidelines (WCAG) 2.1 standard for the AA conformance level, with these limitations:

Table 12. WCAG 2.1 standard for the AA conformance level and limitations

WCAG success criterion	Support	Limitations
1.2.4: Captions (Live)	Not Supported	–
1.2.5: Audio Description (Prerecorded)	Not Supported	–
1.3.4: Orientation	Not Supported	–
1.3.5: Identify Input Purpose	Supported	–
1.4.3: Contrast (Minimum)	Supported	–
1.4.4: Resize Text	Supported	–
1.4.5: Images of Text	Supported	–
1.4.10: Reflow	Supported	–
1.4.11: Non -Text Contrast	Supported	–
1.4.12: Text Spacing	Supported	–
1.4.13: Content on Hover or Focus	Supported	–
2.4.5: Multiple Ways	Supported	–
2.4.6: Headings and Labels	Supported	–
2.4.11: Focus Appearance (Minimum)	Supported	–
2.5.7: Dragging Movements	Partially Supported	Dashboard partially supports drag and drop due to third-party library limitations.
2.5.8: Target Size (Minimum)	Supported	–

WCAG success criterion	Support	Limitations
3.1.2: Language of Parts	Supported	–
3.2.3: Consistent Navigation	Supported	–
3.2.4: Consistent Identification	Supported	–
3.3.3: Error Suggestion	Supported	–
3.3.4: Error Prevention (Legal, Financial, Data)	Not Supported	–
3.1.2: Language of Parts	Supported	–
3.2.3: Consistent Navigation	Supported	–
3.2.4: Consistent Identification	Supported	–
3.3.3: Error Suggestion	Supported	–
3.3.4: Error Prevention (Legal, Financial, Data)	Not Supported	–

Supported hardware

Supported hardware appliances

Cisco delivers Catalyst Center in the form of a rack-mountable, physical appliance. These versions of the Catalyst Center appliance are available:

- Second generation
  - 44-core appliance: DN2-HW-APL (Cisco UCS C220 M5)
  - 44-core promotional appliance: DN2-HW-APL-U (Cisco UCS C220 M5)
  - 56-core appliance: DN2-HW-APL-L (Cisco UCS C220 M5)
  - 56-core promotional appliance: DN2-HW-APL-L-U (Cisco UCS C220 M5)
  - 112-core appliance: DN2-HW-APL-XL (Cisco UCS C480 M5)
  - 112-core promotional appliance: DN2-HW-APL-XL-U (Cisco UCS C480 M5)
- Third generation
  - 32-core appliance: DN3-HW-APL (Cisco UCS C220 M6)
  - 56-core appliance: DN3-HW-APL-L (Cisco UCS C220 M6)
  - 80-core appliance: DN3-HW-APL-XL (Cisco UCS C240 M6)

Statement of volatility

For the statement of volatility for the physical appliances, see the Statement of Volatility for Cisco UCS Hardware.

Supported virtual appliances

Catalyst Center 3.1.6 is supported for deployment as a virtual appliance (VA) only on VMware ESXi for on-premises environments. Neither Catalyst Center nor Cisco TAC can provide support for any issues, bugs, or unexpected behavior that occur in environments that use other hypervisors.

Supported firmware

Catalyst Center 3.1.6 has been validated only against these firmware versions:

- Cisco IMC Version 4.3(2.240077) for appliance model DN2-HW-APL, DN2-HW-APL-L, DN2-HW-APL-XL
- Cisco IMC Version 4.3(5.250030) for appliance model DN3-HW-APL, DN3-HW-APL-L, DN3-HW-APL-XL

Update the Cisco IMC firmware

To update your Cisco IMC firmware, first see the release notes for the corresponding release of Catalyst Center that you are installing. In the release notes, the “Supported firmware” section shows the Cisco IMC firmware version for your Catalyst 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 “Common cluster node operations” in the Cisco Catalyst Center High Availability Guide and follow the steps provided to shut down one or all of the nodes for maintenance.

Related resources

See Cisco Catalyst Center Documentation for additional documents relating to Catalyst Center.

Legal information