Release Notes for Cisco Catalyst Center, Release 3.2.3

Contents

Catalyst Center, Release 3.2.3

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 3.2.3.

Note: Catalyst Center 3.2.3 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
2026-07-06	Initial release	_

New software features

Package versions in Catalyst Center 3.2.3

Table 2. Package versions in Catalyst Center 3.2.3

Package name	Release 3.2.3
Release build version	
Release version	3.2.3.75345
System updates	
System	3.5.7
System Commons	2.740.65645
System Addons	0.11.91
Package updates	
Access Control Application	2.740.65645
AI Applications	2.740.122142
AI Endpoint Analytics	3.230.2
AI Network Analytics	4.1.19
Application and Service Remediation	3.23.14
Application Hosting	3.2.326060811

Package name	Release 3.2.3
Application Visibility and Policy	2.740.117666
Assurance	3.230.257
Assurance – Sensor	3.230.226
Automation – Intelligent Capture	2.740.65645
Automation – Sensor	2.740.65645
Catalyst Center API Catalog	6.9.133
Catalyst Center Gateway Service	0.11.35
Cisco Catalyst Center Global Search	6.10.0
Cisco Catalyst Center Platform	6.10.87
Cisco Catalyst Center UI	3.8.26
Cisco Identity Services Engine Bridge	3.230.4
Cloud Connectivity	6.11.28
Cloud Connectivity – Contextual Content	7.1.10
Cloud Connectivity – Digestor	7.1.7
Core Platform	0.11.410
Disaster Recovery	2.740.365056
DxHub Cloud Connectivity	6.11.41
Group Based Policy Analytics	3.230.2
Identity and Access Management	5.5.59
Identity and Access Management - UI	5.5.26
Multiple Cisco Catalyst Center	2.740.65645

Package name	Release 3.2.3
Network Controller Platform	2.740.65645
Network Data Platform - Base Analytics	3.230.100213
Network Data Platform - Caching Infra	6.7.18
Network Data Platform - Core	6.7.49
Network Data Platform - Ingestion Infra	6.7.32
Network Data Platform - Manager	6.7.106
Network Data Platform - Pipeline Infra	6.7.72
Network Data Platform - Storage Management	6.7.97
Platform Refresh	1.5.82
RCA-Scripts Package	0.6.6
Rogue and aWIPS	3.2.203
SD Access	2.740.65645
Shared Managed Services	0.11.59
Stealthwatch Security Analytics	2.740.1095182
Support Services	2.740.885191
System Management Operations	1.7.38
Telemetry	4.8.22
Wide Area Bonjour	2.740.755017

Disaster Recovery witness

The Disaster Recovery witness is available as a separate OVA file for Catalyst Center. Its version number is 2.1.740.370008.

Catalyst Center

Table 3. New and changed features in Catalyst Center 3.2.3

Product impact	Feature	Description
Base functionality	Support for Cisco Catalyst 9200 and 9200CX Compact Series Switches for security service insertion	Security service insertion for SD-Access supports these devices: • Cisco Catalyst 9200 Series switches • Cisco Catalyst 9200CX Compact Series switches

Catalyst Center platform

Table 4. New and changed features in Catalyst Center platform 3.2.3

Product impact	Feature	Description
Base functionality	API Operations	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.

Cisco Software-Defined Access

Table 5. New and changed features in Cisco Software-Defined Access 3.2.3

Product impact	Feature	Description
Base functionality	Support for silent host detection in Cisco SD-Access fabric network	Catalyst Center supports the configuration of silent host discovery in anycast gateways. Silent host discovery enables the detection of silent hosts, thereby enhancing endpoint reachability.
	Support for OSPF routing protocol in the LAN automation workflow	Catalyst Center supports OSPF routing for provisioning a LAN underlay.

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

Known issues

Table 6. Guidelines and limitations for Catalyst Center 3.2.3

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 full synchronization, complete these steps: **Step 1.** On the Inventory window, select the wireless controller. **Step 2.** Choose **Actions > Inventory > Resync Device**.
IPv6 support for wireless networks	For dual-stack and IPv6 deployments, Catalyst Center sets IPv6 as the preferred mode in the AP join profile when you provision a wireless controller that supports IPv6.
Per-Device Configurations for Cisco Catalyst 9800 Series Wireless Controllers	In IPv6 deployments, Per-Device Configuration continues to support IPv4 configurations. Supported options are aligned with the configurations available in the Cisco Catalyst 9800 Series Wireless Controller web UI in any Catalyst Center deployment mode.
Limitations	
Can't reuse the hard disk drive (HDD) from a failed appliance on new hardware	Don't reuse the HDD from a failed Catalyst Center appliance in a replacement or new Catalyst Center appliance. This is because Catalyst Center links each appliance's identity to its motherboard serial number and stores this identity information on the hard drive during installation. If you move the HDD to a different appliance, the identity information doesn't match, which can cause problems. For this reason, reusing HDDs from failed appliances is not supported.
Connecting IPv4 and IPv6 fabric sites with SDA transit	You can connect an existing IPv4 fabric site to a new IPv6 fabric site using SDA transit, as long as you use a dual border on the IPv6 site. Any limitations of the IPv6 site also affect the traffic between the two sites. For example, native multicast is not supported on the IPv6 site, so this feature doesn’t work across the connection.
Device replacement, device refresh	Catalyst Center supports device replacement or device refresh for devices with IPv6 addresses only if they are running IOS XE version 17.6.1 or later. Device replacement or device refresh is not supported for Catalyst 3650 or Catalyst 3850 Series Switches when they use IPv6 addresses.
Different VLAN information is shown under Provision > Inventory > Configuration > Layer 2 > VLAN versus Provision > Inventory > Details > Interfaces > VLANs.	VLAN information differs depending on the navigation path. Under **Provision > Inventory > Configuration > Layer 2 > VLAN**, this logic applies: • Only manually configured VLANs are displayed. Default VLANs (1 and 1002–1005) are excluded. • For devices running versions earlier than 17.15.x, VLANs don’t appear if the VTP mode is set to Server.

Feature	Description
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.
IPv6 mode	• Access Control Application, Group-Based Policy Analytics, Cisco AI Endpoint Analytics, and Support Services packages are disabled and cannot be downloaded or installed. Before upgrading, remove these packages from the IPv6 deployment because they do not support IPv6. • Adding devices to a site is supported, but provisioning is not supported. • For existing deployments, migration from IPv4 to an IPv6 or dual-stack environment is not supported. • These features are not supported: ◦ ITSM integration ◦ Network profiles for wireless devices ◦ Disaster Recovery ◦ High Availability ◦ Wide Area Bonjour ◦ Security service insertion
REP ring device replacement limitations for nonfabric deployments	When replacing a faulty device within a REP Ring, after the PnP claim is completed, initiate the Return Material Authorization (RMA) workflow by selecting the new device in the **Provision** > **Plug and Play** window. **Note:** Do not initiate the RMA workflow for the new device in the **Inventory** window after claiming and onboarding it. During the RMA workflow: • REP rediscovery is not triggered for the replacement device. • REP configurations from the faulty device are automatically copied to the new device. If the REP ring is in a faulty state, do not initiate dynamic addition or deletion of nodes in the REP ring.
Required Catalyst Center user role permission for applying device credentials to sites	You must have the required user role permission to use the **Apply** action on **Network Settings** page under the **Device Credentials** tab. The permission has changed in this release. The required permission is the Network Provision > Device Provision permission with write access. Custom roles created with these permissions in these releases will not have access to the **Apply** action after upgrading to this release: • If you created custom roles in Catalyst Center Release 3.1.x: ◦ Network Management > Network-wide Settings permission with write access ◦ Network Provision > Device Provision permission with read or deny access • If you created custom roles in Catalyst Center Release 2.3.7.x and earlier: ◦ Network Design > Advanced Network Settings permission with write access ◦ Network Provision > Provision permission with read or deny access Ensure that you update the user role permissions to the required permission for this release, so you can apply device credentials to sites successfully.
SSIDs for a guest wireless network	Catalyst Center supports creation of new Cisco ISE portals while creating SSIDs for a guest wireless network. However, you cannot use existing Cisco ISE portals during the SSID creation. For more information about using existing Cisco ISE portals, refer to " Create a Self-Registered Guest Portal" in the " Guest and Secure Wi-Fi" chapter of the Cisco Identity Services Engine Administrator Guide.

Feature	Description
ThousandEyes integration isn't preserved after backup and restore	If you integrate ThousandEyes into Catalyst Center and then back up and restore Catalyst Center, you must redo the ThousandEyes integration.
ThousandEyes integration isn't preserved after Disaster Recovery failover	If you integrate ThousandEyes into Catalyst Center and run a Disaster Recovery failover process, you must redo the ThousandEyes integration.

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, refer to the Cisco Catalyst Center Compatibility Matrix.

Cisco SD-Access compatibility matrix

For information about Cisco SD-Access hardware and software support for Catalyst Center, refer to 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, refer to 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, refer to " 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, refer to 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 7. 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	–
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	–

WCAG success criterion	Support	Limitations
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, refer to the Statement of Volatility for Cisco UCS Hardware.

Supported virtual appliances

Catalyst Center 3.2.3 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

Cisco Integrated Management Controller (Cisco IMC) versions are independent from Catalyst Center releases.

Catalyst Center 3.2.3 has been validated only against these firmware versions:

- Cisco IMC Version 4.3(2.260007) for appliance model DN2-HW-APL, DN2-HW-APL-L, DN2-HW-APL-XL
- Cisco IMC Version 4.3(6.260017) for appliance model DN3-HW-APL, DN3-HW-APL-L, DN3-HW-APL-XL

Update the Cisco IMC firmware

Refer to 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. Refer to “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

Refer to Cisco Catalyst Center User Content for additional content relating to Catalyst Center.

Legal information