Release Notes for Cisco Catalyst Center, Release 3.2.3

Contents

Catalyst Center, Release 3.2.3 3
New software features 3
Resolved issues 6
Open issues 7
Known issues 8
Compatibility 10
Scalability 11
Supported hardware 12
Related resources 13
Legal information 13

© 2026 Cisco and/or its affiliates. All rights reserved.

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: The latest release, the Catalyst Center 3.2.3-75346.100 software maintenance update (SMU), is generally available.

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

Date	Change	Location
2026-09-28	Added out-of-band AP replacement guidelines.	Known issues
2026-09-21	Updated the package versions for 3.2.3-75346.100 SMU.	Package versions in Catalyst Center 3.2.3
2026-08-28	Added information about the 3.2.3-75346.100 SMU, including package versions and resolved issues.	Package versions in Catalyst Center 3.2.3
		Resolved issues
2026-08-12	Updated supported firmware details.	Supported firmware
	Added CSCwv91096.	Open issues
2026-07-28	Added device guidelines and limitations for security service insertion.	Known issues
2026-07-20	Added support for Catalyst Center on Ubuntu Kernel-based Virtual Machine (KVM) deployments.	Supported virtual appliances
2026-07-10	Added CSCwv32713 to Open issues.	Open issues
	Updated Release version and Cisco Catalyst Center Platform package version.	Package versions in Catalyst Center 3.2.3
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 3.2.3-75346.100	Release 3.2.3
Release build version		

© 2026 Cisco and/or its affiliates. All rights reserved.

Package name	Release 3.2.3-75346.100	Release 3.2.3
Release version	3.2.3-75346.100	3.2.3.75346
System updates		
System	3.5.9	3.5.7
System Commons	2.740.65729	2.740.65645
System Addons	0.11.96	0.11.91
Package updates		
Access Control Application	2.740.65729	2.740.65645
AI Applications	2.740.122142	2.740.122142
AI Endpoint Analytics	3.230.51	3.230.2
AI Network Analytics	4.1.19	4.1.19
Application and Service Remediation	3.23.15	3.23.14
Application Hosting	3.2.326060811	3.2.326060811
Application Visibility and Policy	2.740.117702	2.740.117666
Assurance	3.230.257	3.230.257
Assurance – Sensor	3.230.226	3.230.226
Automation - Intelligent Capture	2.740.65729	2.740.65645
Automation – Sensor	2.740.65729	2.740.65645
Catalyst Center API Catalog	6.9.133	6.9.133
Catalyst Center Gateway Service	0.11.35	0.11.35
Cisco Catalyst Center Global Search	6.10.0	6.10.0
Cisco Catalyst Center Platform	6.10.88-1	6.10.88-1
Cisco Catalyst Center UI	3.8.26	3.8.26
Cisco Identity Services Engine Bridge	3.230.4	3.230.4
Cloud Connectivity	6.11.28	6.11.28
Cloud Connectivity - Contextual Content	7.1.10	7.1.10
Cloud Connectivity – Digestor	7.1.7	7.1.7
Core Platform	0.11.424	0.11.410

© 2026 Cisco and/or its affiliates. All rights reserved.

Package name	Release 3.2.3-75346.100	Release 3.2.3
Disaster Recovery	2.740.365601	2.740.365056
DxHub Cloud Connectivity	6.11.41	6.11.41
Group Based Policy Analytics	3.230.2	3.230.2
Identity and Access Management	5.5.62	5.5.59
Identity and Access Management - UI	5.5.26	5.5.26
Industrial App Orchestrator	2.740.685155	2.740.685155
Multiple Cisco Catalyst Center	2.740.65729	2.740.65645
Network Controller Platform	2.740.65718	2.740.65645
Network Data Platform - Base Analytics	3.230.100213	3.230.100213
Network Data Platform - Caching Infra	6.7.18	6.7.18
Network Data Platform - Core	6.7.53	6.7.49
Network Data Platform - Ingestion Infra	6.7.32	6.7.32
Network Data Platform - Manager	6.7.106	6.7.106
Network Data Platform - Pipeline Infra	6.7.72	6.7.72
Network Data Platform - Storage Management	6.7.97	6.7.97
Platform Refresh	1.6.56	1.5.82
RCA-Scripts Package	0.6.6	0.6.6
Rogue and aWIPS	3.2.203	3.2.203
SD Access	2.740.65729	2.740.65645
Shared Managed Services	0.11.59	0.11.59
Stealthwatch Security Analytics	2.740.1095182	2.740.1095182
Support Services	2.740.885191	2.740.885191
System Management Operations	1.7.39	1.7.38
Telemetry	4.8.23	4.8.22
Wide Area Bonjour	2.740.755051	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.

© 2026 Cisco and/or its affiliates. All rights reserved.

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.

Bug ID	Description
CSCwu32532	Upgrading Catalyst Center to 3.2.2 is failing with Elasticsearch constantly crashing or restarting. Logs complain about indices from 6.x which cannot be processed/run in 8.x, which is what Elasticsearch is upgrading to.

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwu68404	The API does not appear to support a documented sort/order parameter. Because of this, the paginated response may not have a fixed order. When the same API call is executed multiple times with the same limit and offset values, different site IDs can appear in the returned page.
CSCwu90233	In Cisco Catalyst Center 3.1.6 running on a 3-node DN3 cluster, the Servers page under **Design > Network Settings** is blank or continuously loading and no longer shows Stealthwatch information.
CSCwu99073	Catalyst Center 3.x upgrade aborts when fusion-postgres ServiceInstance update remains in progress.
CSCwv23202	Site based RBAC users don't see the correct number of edge devices under port assignment page, even though the same user can see all edge devices under Fabric Infrastructure page.
CSCwv25463	Switchport data dropped from inventory causing device to go into internal error.
CSCwv45068	Schedule Sync or RUM reporting failed for all the devices within two minutes from the time it is triggered.
CSCwv69460	In Cisco Catalyst Center, after a configuration preview task discard operation fails, the affected preview task may remain on the Tasks page. Retrying the discard operation may continue to fail. The stale preview task can keep the associated device in a pending-task state and may block new provisioning operations for that device.

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

Bug ID	Description
CSCwv32713	The upgrade of the Catalyst Center ESXi virtual appliance from version 3.2.2 to 3.2.3 is failing. The process terminates with the status 'ABORTED' and the error code 'CLOUD-CONNECTIVITY#PACKAGE_FAILED'.
CSCwv91096	DN3 and DN2 appliance: Diag Center rejects supported CIMC firmware 4.3(6.260054) and 4.3(2.260020) even when it is recommended.

© 2026 Cisco and/or its affiliates. All rights reserved.

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: 1. On the Inventory window, select the wireless controller. 2. Choose **Actions > Inventory > Resync Device**.
Out-of-band AP replacement guidelines	If you replace an AP outside Catalyst Center, the original record may remain in the Catalyst Center inventory. If the replacement AP uses the same hostname, but has a different serial number or MAC address, Catalyst Center may add it as a separate record. You may see both records in a global search. Use the **AP Refresh** workflow to replace an AP. If you have already replaced an AP outside Catalyst Center, complete these steps: 1. Identify the old AP record using its serial number, MAC address, status, and last update time. **Note:** Do not select a record based only on its hostname or search result. 2. Delete the old AP record. 3. Refresh the inventory or synchronize it for the replacement AP. 4. Confirm that only the current AP record remains and that its hostname, serial number, MAC address, and reachability state are correct.
Device management for a service insertion site	When you add or remove nodes from a fabric site, use these guidelines: • If you add or remove an edge node, the service insertion site is not updated automatically. To apply the change, delete and then re-enable the service insertion site. • If you add or remove a border node, click the warning message in the **Service insertion sites** window to incorporate the change into the service insertion site. If you added a border node, edit the virtual network to associate the new border node with the service insertion site.
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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Feature	Description
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.
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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Feature	Description
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.
Security service insertion	Catalyst Center does not support security service insertion on these devices in these roles or deployments: • Cisco Catalyst 9500X Series Switches and Catalyst 9600 Series Switches with Supervisor Engine 2 as border nodes • Cisco C9350 Series Smart Switches as edge nodes or in Fabric in a Box deployments • Cisco C9550 and C9610 Series Smart Switches as border nodes or in Fabric in a Box deployments
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.
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:

© 2026 Cisco and/or its affiliates. All rights reserved.

- 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	–

© 2026 Cisco and/or its affiliates. All rights reserved.

WCAG success criterion	Support	Limitations
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	–
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)

© 2026 Cisco and/or its affiliates. All rights reserved.

- 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 and Ubuntu KVM 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(2.260020) for appliance model DN2-HW-APL, DN2-HW-APL-L, DN2-HW-APL-XL
- Cisco IMC Version 4.3(6.260054) 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

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: www.cisco.com/go/trademarks. 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. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2026 Cisco Systems, Inc. All rights reserved