Release Notes for Cisco Catalyst Center, Release 3.3.2

Contents

Catalyst Center, Release 3.3.2 3
New software features 3
Resolved issues 7
Open issues 7
Known issues 7
Compatibility 8
Scalability 8
Supported hardware 10
Related resources 11
Legal information 11

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

Catalyst Center, Release 3.3.2

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 3.3.2.

Note: Catalyst Center 3.3.2 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
2026-10-27	Initial release	_

New software features

Package versions in Catalyst Center 3.3.2

Table 2. Package versions in Catalyst Center 3.3.2

Package name	Release 3.3.2
Release build version	
Release version	3.3.2-75136
System updates	
System	3.12.9
System Commons	2.747.65279
System Addons	0.12.110
System hooks	3.31.19
System post hooks	3.31.14
Package updates	
Access Control Application	2.747.65279
AI Assistant	2.747.122116
AI Endpoint Analytics	3.320.24
AI Network Analytics	4.1.23
Application and Service Remediation	3.32.15

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

Package name	Release 3.3.2
Application Hosting	3.3.526101614
Application Visibility and Policy	2.747.117636
API Catalog	6.10.211
Assurance	3.320.222
Assurance – Sensor	3.320.198
Automation – Intelligent Capture	2.747.65279
Automation – Sensor	2.747.65279
Cisco Identity Services Engine Bridge	3.320.11
Cloud Connectivity	6.12.55
Cloud Connectivity Communication	7.2.4
Cloud Connectivity Sense	7.2.6
Core Platform	0.12.244
Disaster Recovery	2.747.365004
DxHub Cloud Connectivity	6.12.56
Gateway Service	0.12.41
Global Search	6.11.1
Group Based Policy Analytics	3.320.10
Identity and Access Management	5.6.67
Identity and Access Management User Interface	5.6.33
Industrial App Orchestrator	2.747.685058
Multiple Instance Enablement	2.747.65279
Network Controller Platform	2.747.65279
Network Data Platform Base Analytics	3.320.100205

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

Package name	Release 3.3.2
Network Data Platform Caching Infra	6.8.31
Network Data Platform Core	6.8.45
Network Data Platform Data Ingestion	6.8.34
Network Data Platform Management User Interface	6.8.30
Network Data Platform Pipeline	6.8.51
Network Data Platform Storage Management	6.8.68
Platform	6.11.85
Platform Refresh	1.6.6
RCA Collector	0.6.6
Rogue and aWIPS	3.3.205
SD Access	2.747.65279
Shared Managed Services	0.12.59
Stealthwatch Security Analytics	2.747.1095122
Support Services	2.747.885137
System Management Operations	1.8.68
Telemetry	4.9.15
User Interface Platform	3.9.33
Wide Area Bonjour	2.747.755020

Disaster Recovery witness

You can deploy the Disaster Recovery witness, version 2.1.747.370000, as a separate OVA file or a QCOW2 image on KVM.

Cisco Catalyst Assurance

Table 3. New and changed features in Cisco Catalyst Assurance 3.3.2

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

Product impact	Feature	Description
Base functionality	Support for monitoring the health of fabric sites with shared wireless controllers	Assurance now monitors LISP session connectivity between control plane nodes and wireless controllers that are shared across multiple fabric sites. The **Control Plane 360** and **Fabric Site 360** windows display wireless controller connectivity health information. This enhancement isolates connectivity failures to the affected control plane node and fabric site. The new LISP Session Status KPI from control plane to wireless controller is monitored from the control plane node. Wireless controllers no longer contribute to fabric site health. To eliminate redundant or outdated health information, these KPIs are removed from **Wireless Controller 360** window: • **Fabric Site Connectivity** > **Control Plane Reachability** • **Fabric Control Plane** > **LISP Session Status** These KPIs are replaced by the LISP Session Status KPI from the control plane to wireless controller. The **Wireless Controller 360** session chart provides a non-health-impacting view of all source control plane nodes and fabric sites connected to the wireless controller. This chart is included only for observability and does not display information about health impact on the wireless controller. **Note:** After an upgrade, Assurance monitors LISP Session Status from control plane nodes. Historical LISP session data collected from wireless controllers before the upgrade remains available in the **Wireless Controller 360** health timeline for the configured historical period. This historical data is not displayed in session charts or transferred to the new KPI. Use **Control Plane 360** or **Fabric Site 360** to monitor current LISP session health. Existing connectivity issues generated by the previous monitoring model are automatically resolved and remain available under **Resolved Issues**.

Catalyst Center platform

Table 4. New and changed features in Catalyst Center platform 3.3.2

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 3.3.2

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

Product impact	Feature	Description
Base functionality	Shared wireless controller for multiple fabric sites	Catalyst Center now supports sharing a Cisco Catalyst 9800 Series Wireless Controller across multiple SD-Access fabric sites. **Note:** This feature is in beta. A wireless controller can be shared across a maximum of 16 fabric sites. You can select eligible remote fabric sites, validate network profile compatibility, resolve configuration conflicts, and prepare site-specific wireless intent before deployment.

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 3.3.2

Feature	Description
Guidelines	
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.
Limitations	
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.

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

Feature	Description
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

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

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

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	–
3.3.3: Error Suggestion	Supported	–
3.3.4: Error Prevention (Legal, Financial, Data)	Not Supported	–

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

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 3.3.2 is supported for deployment as a virtual appliance (VA) on these platforms:

- VMware ESXi for on-premises environments
- KVM (Ubuntu Native - Desktop and Server)

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 3.3.2 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
- Cisco IMC Version 6.0.(2.260143) for appliance model DN4-HW-APL, DN4-HW-APL-L, DN4-HW-APL-XL

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

Update the Cisco IMC firmware

To update your Cisco IMC firmware, first refer to the release notes for the corresponding release of Catalyst Center that you are installing. In the release notes, refer to “Supported firmware” section shows the Cisco IMC firmware version for your Catalyst Center release.

Then, 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