Release Notes for Cisco Catalyst Center, Release 3.3.1

Contents

Catalyst Center, Release 3.3.1 3
New software features 3
Changes in behavior 12
Resolved issues 13
Open issues 13
Compatibility 14
Scalability 15
Supported hardware 16
Related resources 17
Legal information 17

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

Catalyst Center, Release 3.3.1

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 3.3.1.

Note: Catalyst Center 3.3.1 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
2026-10-07	Updated supported firmware details	Supported firmware
2026-09-29	Added out-of-band AP replacement guidelines	Known issues
2026-09-09	Initial release	_

New software features

Package versions in Catalyst Center 3.3.1

Table 2. Package versions in Catalyst Center 3.3.1

Package name	Release 3.3.1
Release build version	
Release version	3.3.1-75640
System updates	
System	3.10.102
System Commons	2.746.65616
System Addons	0.12.81
System hooks	3.31.19
System post hooks	3.31.14
Package updates	
Access Control Application	2.746.65635
AI Assistant	2.746.122150
AI Endpoint Analytics	3.310.14
AI Network Analytics	4.1.23

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

Package name	Release 3.3.1
Application and Service Remediation	3.31.44
Application Hosting	3.3.326080521
Application Visibility and Policy	2.746.117745
API Catalog	6.10.76
Assurance	3.310.295
Assurance – Sensor	3.310.259
Automation – Intelligent Capture	2.746.65635
Automation – Sensor	2.746.65635
Cisco Identity Services Engine Bridge	3.310.17
Cloud Connectivity	6.12.24
Cloud Connectivity Communication	7.2.4
Cloud Connectivity Sense	7.2.6
Core Platform	0.12.178
Disaster Recovery	2.746.365077 **Note**: This package is available only for the on-premises hardware appliance, not for the virtual appliance.
DxHub Cloud Connectivity	6.12.27
Gateway Service	0.12.13
Global Search	6.11.1
Group Based Policy Analytics	3.310.15
Identity and Access Management	5.6.35
Identity and Access Management User Interface	5.6.20
Industrial App Orchestrator	2.746.685150
Multiple Instance Enablement	2.746.65635

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

Package name	Release 3.3.1
Network Controller Platform	2.746.65635
Network Data Platform Base Analytics	3.310.100217
Network Data Platform Caching Infra	6.8.13
Network Data Platform Core	6.8.22
Network Data Platform Data Ingestion	6.8.8
Network Data Platform Management User Interface	6.8.3
Network Data Platform Pipeline	6.8.21
Network Data Platform Storage Management	6.8.38
Platform	6.11.51
Platform Refresh	1.5.105
RCA Collector	0.6.6
Rogue and aWIPS	3.3.13
SD Access	2.746.65635
Shared Managed Services	0.12.32
Stealthwatch Security Analytics	2.746.1095216
Support Services	2.746.885262
System Management Operations	1.8.41
Telemetry	4.9.15
User Interface Platform	3.9.31
Wide Area Bonjour	2.746.755075

Disaster Recovery witness

You can deploy the Disaster Recovery witness, version 2.1.746.370009, as a separate OVA file or a QCOW2 image on KVM.

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

Catalyst Center

Table 3. New and changed features in Catalyst Center 3.3.1

Product impact	Feature	Description
Base functionality	Decouple templates configuration from network profile	If you want to configure one or a few devices with specific configurations that do not apply to the rest of the devices at the same site, you can provision the CLI template without associating it with a network profile. The compliance check is skipped if you provision the template without associating it with a network profile.
	Enhancements to application hosting	Catalyst Center supports multi-architecture app packages across CPU architectures such as x86_64 and aarch64.
	Enhancements to delete a REP ring	If any device in the REP ring is unreachable, you cannot delete the ring. Use Catalyst Center to rediscover the REP ring so you can remove unreachable devices and then delete the ring.
	Enhancements to MRP monitoring	When the link between two devices goes down in an MRP ring, Catalyst Center indicates the affected MRP Ring node.
	Enhancements to REP ring configuration	You can configure REP ring with MACsec encryption.
	Enhancements to the scheduling experience in the Visibility and Control of Configurations workflow	Catalyst Center streamlines the scheduling experience in the Visibility and Control of Configurations workflow: • Configure scheduling and preview from one page. • Enable configuration preview using the **Preview** check box. • Schedule the deployment to run **Now** or **Later**, regardless of the Visibility and Control of Configurations settings.
	Increased support for network profiles	Catalyst Center now supports up to 250 switching, routing, and wireless network profiles.
	Integrated Cisco Technical Assistance Center (TAC) capabilities	Catalyst Center 3.3.1 integrates TAC capabilities directly into the user interface. To access these support capabilities: 1. In the Catalyst Center UI, choose **Help > Cisco Support Assistant**. 2. Sign in using your Cisco.com account credentials. After you're logged in, you can perform these tasks directly within the interface: • Open a new support case or view a list of your existing cases. • Record your screen to capture technical issues for troubleshooting. • Upload your screen recordings directly to new or existing support cases.
	More users can import and export wireless maps	In earlier Catalyst Center releases, only Super-Admin users could import and export wireless maps from the Network Hierarchy view. In this release, any user with a site-based custom role can import or export wireless maps from the Network Hierarchy view. The user must have this permission group: • **Wireless Maps > Read** (for map Export) • **Wireless Maps > Write** (for map Import)

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

Product impact	Feature	Description
	More users can import and export sites	In earlier Catalyst Center releases, only Super-Admin users could import and export sites from the Site Hierarchy view. In this release, any user with a site-based custom role can import or export sites from the Site Hierarchy view. The user must have this permission group: • **Network Management > Hierarchy > Read** (for site Export) • **Network Management > Hierarchy > Write** (for site Import)
	Live Protect	Live Protect validates security shields that protect Cisco products without requiring device reloads or service interruptions. You can deploy security shields in two modes: • Monitoring mode: Provides visibility into potential exploit attempts without enforcement, allowing you to assess threats before taking action. • Enforce (Protecting) mode: Actively applies mitigation policies to reduce exposure to known vulnerabilities. Live Protect allows you to monitor, enforce, disable, and retire the security shields, enabling a smooth transition to remediation. This capability helps businesses maintain continuous operations while managing risks until the software upgrades or patches are deployed.
	Return Material Authorization (RMA) device support	Catalyst Center provides RMA support for Cisco IE3500 and IE3100 Rugged Series switches.
	Scheduler support for fabric SSIDs	In earlier Catalyst Center releases, you could use an SSID scheduler only with nonfabric SSIDs to enable or disable a WLAN based on the selected time zone. Starting in Catalyst Center 3.3.1, this scheduler support also applies to fabric SSIDs.
	Support for automatic service insertion site updates for edge node and border node addition and deletion in fabric sites	Catalyst Center now automatically updates a service insertion site when an edge node or border node is added to or deleted from the corresponding fabric site.
	Support for MACsec encryption in AP profile for Cisco IOS XE devices	Catalyst Center supports MACsec encryption and automatic MACsec configuration in AP profiles for Cisco IOS XE devices. The **MACsec Encrypted** toggle button is applicable for: • Cisco Catalyst 9000 Series Switches running Cisco IOS XE Release 26.1.1 or later. • Wireless controllers running Cisco IOS XE Release 26.1.1 or later. **Note:** Catalyst Center does not support MACsec encryption for fabric sites that contain a Cisco Catalyst 9350 Series Smart Switch. The **Auto-Secure MACsec** toggle button is supported on applicable Wi-Fi 7 APs and Cisco Catalyst 9350 Series Smart Switches running Cisco IOS XE Release 26.2.1 or later. **Note:** This configuration is supported only in nonfabric deployments on Cisco Catalyst 9350 Series Smart Switches. It is not supported in fabric deployments.

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

Product impact	Feature	Description
	Support for security service insertion for SD-Access over HTTPS	Security service insertion for SD-Access is enhanced to support Cisco TrustSec (CTS) policy and data download over HTTPS: • To enable service insertion on a fabric site, you must enable CTS policy and data download over HTTPS for the site. • To disable CTS policy and data download over HTTPS for a site configured as a service insertion site, you must delete the security service insertion configuration. The **Provision** > **Security Service Insertion** window has these enhancements to indicate if CTS policy and data download over HTTPS is enabled for the site: • Day zero: The **TrustSec HTTPS Download** column has been added to the **Site readiness** dialog box. • Day *n*: The **TrustSec HTTPS Download** column has been added to the **Service insertion sites** area in the **Service insertion sites** tab. **Note:** If you upgrade to this release from an earlier release, CTS policy and data download over HTTPS is disabled by default. You must enable CTS policy and data download over HTTPS on the service insertion site after you upgrade to ensure ongoing security service insertion operations on day *n*.
	Support for Cisco TrustSec (CTS) data download over HTTPS	Catalyst Center allows using HTTPS for CTS policy and data download. You can enable or disable this option in Catalyst Center while configuring the ISE servers under **Design** > **Network Settings** > **Servers**.
	Ultra Reliable Wireless Backhaul (URWB) network profile support for wireless controller	You can create a Ultra Reliable Wireless Backhaul (URWB) network profile for a wireless controller and provision it.

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

Product impact	Feature	Description
Licensing	Unified licensing support for Cisco Catalyst 9000 Series switches	Catalyst Center supports unified (device) licensing visibility and reporting for Cisco Catalyst 9000 Series switches, aligning them with the existing unified licensing experience supported by Cisco C9350 Series Smart Switches and Cisco C9610 Series Smart Switches. For a Cisco Catalyst 9000 Series switch to begin consuming a unified device license (OS Essentials/OS Advantage), the switch must be upgraded to a unified licensing-compatible image, and its boot mode must be updated using device CLI commands. Refer to the relevant device guides for the required steps. In Catalyst Center 3.3.1, after a device's boot mode is changed, Catalyst Center detects the updated device license consumption during the device's next inventory sync. Catalyst Center then automatically triggers a Smart License Compliance workflow to report the updated license usage to Cisco Smart Software Manager (SSM). For the automatic Smart License Compliance workflow to run, verify that the devices meet these criteria in the Catalyst Center UI at **Tools > License Manager > Reporting**: • Ready for Smart License Compliance • Preregistered to a Smart Account and Virtual Account • In Managed state under Provision > Inventory Exceptions apply. If the configured policy indicates that a scheduled Smart License Compliance workflow is already upcoming for the Smart Account associated with the device, the automatic Smart License Compliance workflow skips the associated devices. Troubleshooting: If the Resource Utilization Measurement (RUM) sync status shows that the "Boot Mode Update" Smart License Compliance workflow failed for a device, ensure that the preceding criteria are met. Then, trigger an ad hoc Smart License Compliance workflow from the Reporting tab.

Cisco Catalyst Assurance

Table 4. New and changed features in Cisco Catalyst Assurance 3.3.1

Product impact	Feature	Description
Base functionality	Rogue update frequency	Catalyst Center monitors the incoming rogue message count from the devices. When the count exceeds the defined threshold, the dashboard displays an error banner.
	Support for monitoring the health of steering policies	Catalyst Center supports monitoring and troubleshooting the health of service insertion sites and traffic steering policies in the Assurance dashboard.
	Support for monitoring the health of URWB networks	Catalyst Center supports the monitoring and troubleshooting the health of Ultra-Reliable Wireless Backhaul (URWB) networks. The URWB Health dashboard provides visibility into URWB network status, link performance, RF quality metrics, and throughput statistics for Catalyst 9100 Series Access Points operating in URWB mode.
	AI PCAP Analysis for wireless controllers	Catalyst Center supports AI PCAP analysis which simplifies wireless troubleshooting by using machine learning to analyze packet captures for client onboarding failures.

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

Catalyst Center platform

Table 5. New and changed features in Catalyst Center platform 3.3.1

Product impact	Feature	Description
Base functionality	API Operations	Catalyst Center platform supports new API operations. For more information, refer to "New and changed information" in the Cisco Catalyst Center Platform User Guide. For detailed information about the API operations, refer to the Cisco Catalyst Center APIs on Cisco DevNet.
	Assurance Events	Catalyst Center platform supports these new Assurance events: • NETWORK-DEVICES-4-401: This event triggers when the URWB AP Node is experiencing Packet Error Rate (PER) that is exceeding the defined URWB Critical PER threshold. • NETWORK-DEVICES-4-402: This event triggers when the URWB AP Node is experiencing MCS Index that is lower than the defined URWB Critical MCS Index threshold. • NETWORK-DEVICES-4-403: This event triggers when the URWB Link is experiencing Link Error Rate (LER) that is exceeding the defined URWB Critical LER threshold. • NETWORK-DEVICES-4-404: This event triggers when the URWB Link is experiencing RSSI that is lower than the defined URWB Link RSSI threshold. • NETWORK-DEVICES-2-900: This event triggers when there is a Traffic Steering Policy configuration failure. • NETWORK-FABRIC_WIRED-1-339: This event triggers when Fabric Control Plane Node loses connectivity to one or more Wireless Controllers. • NETWORK-DEVICES-2-157: This event triggers when the standby unit in Catalyst 9800 HA SSO pair is down, indicating redundancy failure.
	Rogue Events	Catalyst Center platform now provides email support to these existing Rogue events: • NETWORK-THREATS-ROGUE-01 • NETWORK-THREATS-AWIPS-01 We recommend that you use webhooks instead of email notifications when you anticipate a high volume of alerts due to scaling.
Ease of use	Flexible Report	Catalyst Center platform supports a new entity under Flexible reports called Network Interface. Use the new Network Interface entity to generate Trend, TopN, Summary, and Distribution reports. This update integrates enhanced KPIs and advanced filtering to optimize data retrieval and provide granular visibility into network performance and health.

Catalyst Center Automation

Table 6. New and changed features in Catalyst Center Automation 3.3.1

Product impact	Feature	Description
Base functionality	Enhancements to Per-Device Configurations for Cisco Catalyst 9800 Series Wireless Controllers	Per-Device Configurations for Cisco Catalyst 9800 Series Wireless Controllers are enhanced to support new and updated configurations for Cisco IOS XE Release 26.2.1.

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

Product impact	Feature	Description
	Enhancements to the wireless controller provisioning workflow in campus networks	Catalyst Center supports these enhancements for provisioning wireless controllers in a campus network: • Associate configuration profiles to multiple wireless controllers • Create new configuration profile for wireless controllers. • Support for additional configurations for wireless controller configuration profile. • Configure and review device overrides for wireless controller configuration profiles.
	Enhancements to per-device configurations for Cisco Catalyst Switches in Catalyst Center	Catalyst Center supports these enhancements for per-device configurations of Cisco Catalyst Switches: • Configuration of QoS, BFD, OSPF, and AAA attributes in the per-device configurations. • View and edit of per-device configurations for fabric devices.
	Enhancements to port configuration profiles for Cisco Catalyst Switches in campus networks workflow	The configuration profiles for Cisco Catalyst Switches are enhanced to support additional profiles for port configurations.
	Enhancements to the switching provisioning workflow in campus networks	Catalyst Center supports these features for provisioning switching devices in a campus network. • Configuration of Industrial configuration profile. • Configuration of device-level overrides for configuration profile attributes.
	Configuration profile limits for switching device groups in campus networks	Catalyst Center imposes these limits for switching device groups in a campus network: • A device group can have at most 20 port configuration profiles. • A device group can have at most 20 port channel profiles.
	Regulatory activation for wireless controllers	Catalyst Center supports regulatory activation for Cisco Catalyst 9800 Series Wireless Controllers and Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches in nonfabric deployment. When the APs associated with a wireless controller are unable to obtain a country code through standard geolocation or proximity methods, the AP radios are not operational. Catalyst Center can use the regulatory activation file obtained from the Meraki dashboard to resolve the country code on these APs.
	Support for Cisco Wireless 9177D, 9177E, and 9177I Series Access Points	Catalyst Center supports the Cisco Wireless 9177D, 9177E, and 9177I Series Access Points. You can configure these APs with Wi-Fi 7 for Cisco IOS XE Release 26.2.1 or later, enable bridge and mesh roles, and use dual-band (XOR) capability to operate slot 2 in either 5-GHz or 6-GHz radio mode. **Note:** When configuring these APs using the **Configure Access Points** workflow, you cannot set radio parameters for slot 2 in the **Configure 6 GHz Radio Parameters** window. Use the **Configure Dual-Band (XOR) Radio Parameters** window to manage these settings.
Usability	Enhancements to the AP configuration workflow	The **Configure Access Points** workflow is enhanced for improved usability.

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

Product impact	Feature	Description
	Enhancements to the wireless SSID creation workflow for enterprise and guest wireless networks	The **Associate SSID to Wireless Network Profile** window in the wireless SSID creation workflow has been enhanced.

Cisco Software-Defined Access

Table 7. New and changed features in Cisco Software-Defined Access 3.3.1

Product impact	Feature	Description
Base functionality	Support for MACsec encryption for fabric APs	For the INFRA_VN virtual network, Catalyst Center supports MACsec encryption of AP uplink traffic for supported APs during anycast gateway configuration. Catalyst Center supports MACsec configuration on switches in the fabric edge role for these platforms: Cisco Catalyst 9300, 9500, and 9500H Series Switches. **Note:** If a fabric site contains a Cisco Catalyst 9350 Series Smart Switch, you cannot enable MACsec for that fabric site.

Interactive help

Table 8. New and changed features in interactive help 3.3.1

Product impact	Feature	Description
Ease of use	New walkthroughs	• Create a Traffic Steering Contract • Create a Traffic Steering Policy • Enable a Service Insertion Site for SD-Access

Changes in behavior

Table 9. Changes in behavior in Catalyst Center 3.3.1

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

Change	Description
Enhancements to 5-GHz DBS channel width in RF profiles	Starting with Catalyst Center 3.3.1, for wireless controllers that are running Cisco IOS XE Release 26.2.1 or later, 5-GHz Dynamic Bandwidth Selection (DBS) channel width is configured in RF profiles using minimum and maximum values. • New 5-GHz basic and AI RF profiles use the default 40 MHz for both minimum and maximum values. • New 6-GHz basic and AI RF profiles use the default 80 MHz for both minimum and maximum values. During upgrade: • Existing 5-GHz basic RF profiles are migrated to 40 MHz minimum and maximum values. • Existing 5-GHz AI RF profiles are migrated to the 20 MHz minimum value while retaining the configured maximum value. • Existing 6-GHz RF profiles retain their current values. After upgrade, if RF profile DBS minimum and maximum values differ between the wireless controller and Catalyst Center, compliance mismatches occur. If a mismatch occurs, compare the configured DBS minimum and maximum values on both sides, update the Catalyst Center RF profile if needed, and reprovision the wireless controller to synchronize the configuration.
Support for Tableau Hyper format for reports	Catalyst Center is updating its supported file formats for reports. Earlier Catalyst Center releases supported the Tableau Data Extract (TDE) format; however, due to Tableau's decision to discontinue TDE, Catalyst Center has transitioned to the Hyper format. Starting with Catalyst Center 3.3.1, the TDE format is no longer supported. Catalyst Center supports the Tableau Hyper format for report exports.

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

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

Known issues

Table 10. Guidelines and limitations for Catalyst Center 3.3.1

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.
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

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

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 11. 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	–

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

WCAG success criterion	Support	Limitations
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)
  - 56-core appliance: DN3-HW-APL-L (Cisco UCS C220 M6)
  - 80-core appliance: DN3-HW-APL-XL (Cisco UCS C240 M6)

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

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 3.3.1 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 3.3.1 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

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