Release Notes for Cisco Catalyst Center, Release 3.2.2

Contents

Catalyst Center, Release 3.2.2 3
New software features 3
Changes in behavior 14
Resolved issues 15
Open issues 15
Known issues 15
Compatibility 18
Scalability 19
Supported hardware 20
Related resources 21
Legal information 21

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

Catalyst Center, Release 3.2.2

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 3.2.2.

Note: Catalyst Center 3.2.2 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
2026-10-28	Added information about edge device support for Cisco C9350 Series Smart Switches.	Cisco Software-Defined Access
2026-10-22	Updated the feature information about RMA support for wireless controllers.	Catalyst Center Automation
2026-09-28	Added out-of-band AP replacement guidelines.	Known 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
2026-06-30	Updated limitations about the IPv6 mode.	Known issues
2026-05-05	Initial release.	–

New software features

Package versions in Catalyst Center 3.2.2

Table 2. Package versions in Catalyst Center 3.2.2

Package name	Release 3.2.2
Release build version	
Release version	3.2.2-75131
System updates	
System	3.3.72
System Commons	2.739.65146
System Addons	0.11.78

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

Package name	Release 3.2.2
Package updates	
Access Control Application	2.739.65146
AI Applications	2.738.122309
AI Endpoint Analytics	3.220.5
AI Network Analytics	4.1.12
Application and Service Remediation	3.22.14
Application Hosting	3.0.226031211
Application Visibility and Policy	2.739.117537
Assurance	3.220.126
Assurance – Sensor	3.220.114
Automation – Intelligent Capture	3.220.114
Automation – Sensor	2.739.65146
Catalyst Center API Catalog	6.9.122
Catalyst Center Gateway Service	0.11.33
Cisco Catalyst Center Global Search	6.10.0
Cisco Catalyst Center Platform	6.10.82
Cisco Catalyst Center UI	3.8.23
Cisco Identity Services Engine Bridge	3.220.9
Cloud Connectivity	6.11.25
Cloud Connectivity – Contextual Content	7.1.10
Cloud Connectivity – Digestor	7.1.7
Core Platform	0.11.399

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

Package name	Release 3.2.2
Disaster Recovery	2.739.365018 **Note**: This package is available only for the on-premises hardware appliance, not for the virtual appliance.
DxHub Cloud Connectivity	6.11.39
Group Based Policy Analytics	3.220.9
Identity and Access Management	5.5.56
Identity and Access Management - UI	5.5.25
Multiple Cisco Catalyst Center	2.739.65146
Network Controller Platform	2.739.65146
Network Data Platform - Base Analytics	3.220.100013
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	6.7.93
Platform Refresh	1.5.26
RCA-Scripts Package	0.6.3
Rogue and aWIPS	3.2.33
SD Access	2.739.65146
Shared Managed Services	0.11.58
Stealthwatch Security Analytics	2.739.1095027
Support Services	2.739.885009

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

Package name	Release 3.2.2
System Management Operations	1.7.33
Telemetry	4.8.20
Wide Area Bonjour	2.739.755005

Disaster Recovery witness

The Disaster Recovery witness is available as a separate OVA file for Catalyst Center. Its version number is 2.1.739.370002.

Catalyst Center

Table 3. New and changed features in Catalyst Center 3.2.2

Product impact	Feature	Description
Base functionality	AP zone support for plug and play	You can apply AP zone configurations to the APs claimed from the plug and play process.
	Deploy Cyber Vision Center from Catalyst Center	Catalyst Center supports integration with Cisco Cyber Vision, which is a network security solution. The browser-based manager is called Cisco Cyber Vision Center. The Cyber Vision Center helps monitor and manage network devices.
	Edit PRP channel	You can modify the **Allowed VLAN** details in the PRP configuration.
	Enhanced Catalyst Center home page	This release introduces an enhanced home page that offers a granular summary view of your network. This data allows you to quickly assess its overall performance, status, and health. The main menu, icons in the top-right portion of the window, and **Interactive Help** work the same as they did on the previous home page.
	Enhanced Catalyst Center first-time setup	After installing and configuring your Catalyst Center appliance, you can complete the first-time setup of Catalyst Center using one of these enhanced setup methods: • Express setup • Standard setup • Expert setup These setup methods offer you flexibility, allowing you to choose how you would like to set up the system and onboard devices.
	Extended Fast Software Upgrade (xFSU) support for Catalyst 9300 Series devices	You can choose to upgrade the device using xFSU to minimize downtime during upgrades.
	IPv6 support for wireless maps	Wireless maps support IPv6 networks. The Cisco Spaces connection endpoint is transitioning to https://ciscospaces.io from https://dnaspaces.io to support IPv6 functionality. **Note:** Before upgrading to this release, update your firewall rules to permit access to https://ciscospaces.io to ensure uninterrupted integration with Cisco Spaces.

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

Product impact	Feature	Description
	MACsec encryption support for onboarding of Supplicant-based extended node	You can onboard a new supplicant-based extended node with MACsec enabled, or you can provide MACsec encryption support to an already onboarded extended node.
	Manage out-of-band RMA device replacement in Catalyst Center	The workflow detects the serial number conflict and prompts user for confirmation of replacement of out-of-band RMA device.
	Plug and Play (PnP) claim flow and StackWise Virtual Switch (SVL) enhancements	PnP claim flow is enhanced to reduce confusion when managing devices in PnP and inventory. SVL support during PnP onboarding allows users to onboard a pair of connected Catalyst 9500 switches as a single logical device.

Cisco Catalyst Assurance

Table 4. New and changed features in Cisco Catalyst Assurance 3.2.2

Product impact	Feature	Description
Base functionality	AAA Network Services enhancements	You can now view AAA server transaction statistics, latency trends, and client events aggregated for both wireless controllers and switches.
	AI Syslog Summarization and Explanation	AI-driven summarization of syslog messages in the Assurance Event Analytics dashboard transforms raw syslog data into actionable insights, enabling quick identification of trends and facilitating efficient event analysis and management.
	Device and Client Health enhancements	Enhanced health score and issue detection for Wireless LAN Controllers and clients by incorporating critical KPIs such as retries, monitoring WLC HA pair failures and mobility tunnel status, and improving issue triggering to reflect accurate user health scores, including customer-specific escalated use cases.
	Packet capture for wired client devices	You can now initiate a packet capture from Assurance to help troubleshoot a wired client device's connectivity or traffic issues.
	Industrial Ethernet (IE) Switch support	Catalyst Center now supports ThousandEyes agent management for the Cisco Catalyst Industrial Ethernet (IE) 3500 Series and Cisco Catalyst Industrial Ethernet (IE) 9300 Series Switches.

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

Product impact	Feature	Description
	Outdoor area support	Catalyst Center now supports Outdoor Areas as a distinct site type in the Assurance dashboard. You can monitor outdoor access points and view their health status within the site map and hierarchy. If **Try Outdoor Area feature** is enabled in Catalyst Center, you will find the outdoor area selection option in the Site Selector window in these dashlets. • Overview • Threats ◦ Threat table > Detecting AP Site • Rogues on Map • Allowed List ◦ Create Allowed Vendor List • Rules ◦ Create Rogue Rule Profile
	OTA Sniffer capture enhancements	Enhancements to the OTA packet capture providing greater flexibility for troubleshooting complex Wi-Fi 7 and Multi-Link Operation (MLO) environments. These enhancements allow for simultaneous traffic capture across multiple radios and Access Points (APs).
	Track when clients disconnect from the network	You can now track clients when they disconnect from the network and receive disconnect notifications.
	Wi-Fi 7 capability support	Wi-Fi 7 capability support is added to Client 360. Multiple Link Operational (MLO) capable clients can simultaneously connect to different combinations of 2.4-GHz, 5-GHz, or 6-GHz bands.

Catalyst Center platform

Table 5. New and changed features in Catalyst Center platform 3.2.2

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, see the Cisco Catalyst Center APIs on Cisco DevNet.
	BMC Remedy integration	Catalyst Center platform offers integration with a new Information Technology service management (ITSM) system called BMC Remedy through the 'Network Issue Monitor and Enrichment' bundle. This integration currently supports only incident management tasks. For more information, see the “New and changed information” topic in the Cisco Catalyst Center ITSM Integration Guide.

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

Product impact	Feature	Description
Ease of use	Assurance Events	Catalyst Center platform supports these new Network events: • NETWORK-DEVICES-1-220: This event triggers when one or more devices are unreachable from the site. • NETWORK-DEVICES-3-220: This event triggers when there is low transmit power on the transceiver interface. • NETWORK-DEVICES-3-221: This event triggers when there is high transmitting power on the transceiver interface. • NETWORK-DEVICES-3-222: This event triggers when there is low receive power on the transceiver interface. • NETWORK-DEVICES-3-223: This event triggers when there is high receive power on the transceiver interface. • NETWORK-DEVICES-3-224: This event triggers when there is high temperature on the transceiver interface. • NETWORK-DEVICES-3-225: This event triggers when there is low voltage on the transceiver interface. • NETWORK-DEVICES-3-226: This event triggers when there is high voltage on the transceiver interface. • NETWORK-DEVICES-3-322: This event triggers when one or more WLC process(es) experience high CPU utilization. • NETWORK-APPLICATIONS-3-601: This event triggers when business relevant applications experience degraded health score continuously for 30 minutes. • NETWORK-DEVICES-2-600: This event triggers when the device is in insecure mode. Catalyst Center platform supports this event enhancement: NETWORK-DEVICES-3-115: From this release, APs can either be on the floor or in an outdoor area. This event triggers when APs (6 GHz) on a site are experiencing high interference or noise. With this release, the NETWORK-APPLICATIONS-3-600 event is deprecated.
	Flexible Report	Catalyst Center platform supports a new entity under Flexible reports called AP Ethernet Interface. You can now use this entity to generate reports with AP Ethernet statistics. The report supports attributes related to AP Ethernet like TX Errors, RX Errors, TX Utilization, AP Name, AP Mac Address, and so on. The AP Ethernet Interface entity data is available for the previous 30 days. For more information, see the “Generate a flexible report” topic in the Cisco Catalyst Center Platform User Guide.
	Report Generation Duration (Days)	With this release, you can generate some of the Client and Flexible reports for the past 180 days. For more information, see the “Run a client report” and “Generate a flexible report” topics in the Cisco Catalyst Center Platform User Guide.

Catalyst Center Automation

Table 6. New and changed features in Catalyst Center Automation 3.2.2

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

Product impact	Feature	Description
Base functionality	AP accelerometer support	You can now enable the AP accelerometer to display tilt information and monitor AP orientation for supported APs. AP accelerometer is disabled by default. It is available only on Cisco Catalyst 9166D1, 9176I, 9176D1, and 9178I Series APs. The **Provision** > **Inventory** window has these enhancements: • The **Sensor Accelerometer Tilt (Degrees)** column is added to the **Devices** table to display AP tilt information for applicable APs. • The **View Device Details** > **Details** > **Configuration** window displays the **Sensor Accelerometer Tilt (Degrees)** for applicable APs. Click **Show More** to view the x, y, and z coordinates for the AP sensor accelerometer.
	AP label enhancements in 2D wireless maps	You can now display up to four label types for each AP and up to two label types for each planned AP in 2D wireless maps.
	AP zone optimization	Catalyst Center supports AP zone optimization to enhance efficiency in large-scale wireless deployments. After upgrading to Release 3.2.2 from an earlier release, reprovision all Cisco Catalyst 9800 Series Wireless Controllers to enable this optimization. If there are no other intent changes, reprovisioning the wireless controllers does not push new configurations to devices.
	Cisco Catalyst 9800 Series Wireless Controller provisioning optimizations	Catalyst Center includes these performance optimizations for Cisco Catalyst 9800 Series Wireless Controller provisioning: • Intuitive skip AP provisioning: When you reprovision the wireless controller, Catalyst Center detects if there are no changes to the AP-related configurations. It skips configuring AP-related commands if the AP intent configuration does not change. • Selective AP group RFS translate: This feature optimizes reprovisioning for AP-related configurations (such as AP tag mapping, RF tags, and flex or RF profiles). Out-of-band changes to AP-related configurations are not automatically corrected during reprovisioning unless a compliance report explicitly flags them. To correct the AP-related out-of-band configurations to match your network intent, perform a wireless controller resynchronization and compliance run. To disable this feature, contact Cisco Technical Assistance Center (TAC).
	Dynamic AP elevation reporting	For 2D and 3D wireless maps, the **Elevation** field automatically displays the tilt angle for APs with enabled and supported accelerometer hardware.
	Enhancements to the AP configuration workflow	The **Configure Access Points** workflow is enhanced to support the **RAP Downlink Backhaul** check box. After enabling this option, you can select the downlink backhaul radio band for Root Access Points (RAP).
	Enhancements to AP selection during AP configuration	The AP selection in the **Configure Access Points** workflow has these enhancements to support large-scale deployments: • The Select All option is added to allow selection of up to 4000 APs simultaneously. • The Access Points table now allows you to display 200 or 300 rows per page. • Column-level filtering is available for the Access Points table to quickly search and select specific APs. • The table settings slide-in pane is restructured for easier customization.

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

Product impact	Feature	Description
	Enhancements to Per-Device Configurations for Cisco Catalyst 9800 Series Wireless Controllers	Per-Device Configurations for Cisco Catalyst 9800 Series Wireless Controllers have these enhancements: • In the **Configuration** tab of the device details window, menu group names are updated and settings are reorganized. The updated group names are **SSID**, **RF**, **AP**, **Tag Mapping**, **Security**, **Global Wireless**, **Services**, **Layer 2**, **Network Settings**, **Layer 3**, and **Administration**. • Support for CTS over HTTPS and HTTPS policy server configuration. • Support for IPv6 configurations in SXP and SXP peer creation. • Support for MACsec configurations. • Support for new and updated configurations for Cisco IOS XE Release 17.18.2 and Cisco IOS XE Release 26.1.1.
	Enhancements to Per-Device Configurations for wireless controllers running Cisco IOS XE Release 17.18.2	For Per-Device Configurations, Catalyst Center displays warning messages for insecure configuration options that do not meet the current security standards and will be deprecated in Cisco IOS XE Release 17.18.2, such as Lightweight Extensible Authentication Protocol (LEAP).
	Enhancements to per-device configurations for Cisco Catalyst Switches in Catalyst Center inventory	You can view and edit the Layer 3 configurations, network settings, and port configurations on a single device. Additionally, the Layer 2, security, and industrial profiles are updated to include new configurations.
	Enhancements to custom site tags for load-balancing	Catalyst Center allows you to configure a load value for a custom site tag. The valid range for load is 0 to 1000, and it can be set according to the AP density at the site.
	Enhancements in AP refresh and AP configuration workflows	Catalyst Center supports these enhancements in AP workflows: • AP Refresh workflow: AP onboarding through Plug and Play for assurance use case. • Configure APs: Configuration of mesh roles through the AP configuration workflow.
	Enhancements in campus networks provisioning	Campus networks workflow in Catalyst Center now supports provisioning switching device groups using group profiles for Layer 2, Layer 3, security, network settings, industrial, and port profiles.
	Enhancements to Catalyst Center Compliance	You can view and manage the Compliance Dashboard for centralized, enterprise-wide network compliance health monitoring. The dashboard categorizes compliance into Configuration, Hardware/Software, and Vulnerability, and introduces bulk operational capabilities to acknowledge and manage violations across multiple devices simultaneously.
	Out-of-band AP image download	The wireless controller pushes the image to the APs after the image is distributed to it. Catalyst Center allows image download on APs from the wireless controller, over HTTPS. This out-of-band file transfer efficiently upgrades the AP image.

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

Product impact	Feature	Description
	RMA support for wireless controllers	Catalyst Center supports RMA for wireless controllers. The **Replace Device** workflow allows you to replace standalone wireless controllers or both wireless controllers in a High Availability (HA) pair. In SD-Access fabric networks, Catalyst Center supports zero-touch replacement for Cisco Catalyst 9800 Series Wireless Controllers and Catalyst 9800 Embedded Wireless Controller for Cisco Catalyst 9000 Series Switches using this workflow. This workflow is not supported for these devices: • Cisco AireOS Wireless Controllers • Mobility Express devices
	Site-based, role-based access control support	You can create custom roles for site users, enabling precise allocation of read/write access to Field Notices, EoX Status, Security Advisories, Network Bug Identifier, and Network Reasoner.
	Smart Licensing Using Policy reporting through On-Prem CSSM	You can upload resource details to CSSM through On-Prem SSM.
	Support for campus networks provisioning for Cisco Catalyst 9800 Series Wireless Controllers	Campus networks support provisioning multiple Cisco Catalyst 9800 Series Wireless Controllers by learning configurations from an existing Cisco Catalyst 9800 Series Wireless Controller. Catalyst Center can learn the configurations from a wireless controller that is provisioned through Per-Device Configuration, provisioned through intent-based network configuration, or available in the inventory without being provisioned. These configurations are saved as configuration profiles. You can apply the configuration profiles to multiple wireless controllers, ensuring uniform configurations and standardized deployment. **Note:** This feature is in beta and requires feature enablement. To enable the feature, contact Cisco TAC. If this feature is not enabled, the options for wireless controller-related configurations are unavailable or dimmed.
	Support for IPv6 in wireless networks	Catalyst Center supports IPv6 in single-stack and dual-stack deployments for wireless networks. These configurations support IPv6 addresses: • Device inventory • Anchor group • NAT IP address configuration for remote teleworkers • Preauthentication ACLs • ACL association with SSIDs • IP-based access control policies • Mobility groups • Application visibility and application policy • AI-enhanced RRM • Cisco Catalyst 9800 Series Wireless Controller and AP provisioning • Plug and Play (PnP) onboarding for APs and wireless controllers • High availability (HA) in the AP configuration workflow • Per-Device Configurations • AP refresh • RMA for wireless controllers • AAA support

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

Product impact	Feature	Description
	Support for new country codes	Catalyst Center supports new country codes for the Cisco Wireless Controllers and APs running these versions: • Cisco IOS XE Release 17.18.2 or later • Cisco IOS XE Release 26.1.1 or later The radios within the APs are assigned to a specific regulatory domain at the factory, but the country code enables you to specify a particular country of operation within that regulatory domain. For a complete list of country codes supported per product, refer to https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html.
	Support for outdoor areas in Catalyst Center network hierarchy	Catalyst Center supports the **Outdoor Areas** site element in the network hierarchy. Outdoor areas can be added with physical address or latitude and longitude coordinates and can reside under **Global** or under areas or buildings. **Note:** The Outdoor Area feature is in beta. Only wireless access points can be assigned to an outdoor area. Outdoor areas cannot be assigned as physical sites for wireless controllers but they can be selected as managed AP location during wireless controller provisioning.

Cisco Software-Defined Access

Table 7. New and changed features in Cisco Software-Defined Access 3.2.2

Product impact	Feature	Description
Base functionality	Enhanced support for Cisco C9350 Series Smart Switches in fabric network	Cisco C9350 Series Smart Switches is supported in all fabric network roles, such as edge, border, and control plane nodes. **Note:** To deploy Cisco C9350 Series Smart Switches as edge devices, the control plane node must run Cisco IOS XE Release 17.18.x or later.
	Support for Cisco C9610 Series Smart Switches	Catalyst Center supports Cisco C9610 Series Smart Switches in the fabric network. **Note:** Cisco C9610 Series Smart Switches do not support edge and extended node capability.
	Support for dynamic addition of nodes to a REP ring for fabric deployments	You can now dynamically add a node to an existing REP ring for fabric deployments without deleting the REP ring. Nodes must be added one at a time.
	Support for editing the BGP Autonomous System (AS) number	You can now edit the BGP AS number for fabric sites in Catalyst Center. **Note:** Editing the BGP AS Number temporarily disrupts BGP peerings and removes any custom BGP configurations on border nodes and control plane nodes, requiring updates to templates and reconfiguration of custom settings. If you edit the BGP AS number, all virtual networks may lose external connectivity and management access may be disrupted temporarily.
	Support for MACsec switch-to-host connections	Catalyst Center supports MACsec switch-to-host connections for Cisco Catalyst 9000 Series switches. Use the Catalyst Center CLI templates to manually configure MACsec switch-to-host connections for edge devices running Cisco IOS XE Release 26.1.1 or later.

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

Product impact	Feature	Description
	Support for post-authentication ACL configuration for fabric SSIDs	Catalyst Center supports post-authentication Access Control List (ACL) configuration for fabric SSIDs in the **Create IP & URL-Based Access Control Policy** workflow.
	Support for secondary IP address pools in anycast gateways	Catalyst Center supports the configuration of up to four additional IP address pools in an anycast gateway. You can add or edit these pools while creating the anycast gateway.
	Support for extranet policy without policy-based routing configurations in Cisco SD-Access fabric	Catalyst Center introduces a new CLI configuration for extranet policy operations within the Cisco SD-Access fabric. This feature is supported on border devices running Cisco IOS XE 17.18.1 or later. Additionally, Catalyst Center offers migration support to transition from policy-based routing (PBR) to the new CLI approach.
	Support for IPv6 underlay in Cisco SD-Access fabric	Cisco SD-Access fabric supports IPv6 underlay for single stack and dual stack Catalyst Center deployments.
	Support for IPv6 in LAN automation workflow	LAN automation workflow has been enhanced to support IPv6 for a single stack (IPv6-only) Catalyst Center deployment.
	Support for Visibility and Control of Configurations for policy-extended node upgrades	The Visibility and Control of Configurations feature is now supported for policy-extended node upgrades. With enhanced visibility, you can enforce the previewing of device configurations before deploying them. With enhanced control, you can ensure only authentic and authorized configurations are provisioned onto your network devices through an IT Service Management (ITSM) check.

Stealthwatch Security Analytics service

Table 8. New and changed features in Stealthwatch Security Analytics service on Catalyst Center 3.2.2

Product impact	Feature	Description
Base functionality	IPv6 support	Stealthwatch Security Analytics service supports IPv6 addresses. You can now provision devices to use flow destinations with IPv6 addresses.

Changes in behavior

Table 9. Changes in behavior in Catalyst Center 3.2.2

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

Change	Description
NAT IP address retained when configuration cleanup is performed during wireless controller deletion for the remote teleworker use case	For the remote teleworker use case: • In earlier releases, the NAT IP address was reset to 0.0.0.0 when configuration cleanup was performed during wireless controller deletion. • Starting with this release, the NAT IP address is retained when configuration cleanup is performed during wireless controller deletion. This persistence of NAT IP address ensures continuous network address translation functionality without requiring manual reconfiguration.

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

Bug ID	Description
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.

Known issues

Table 10. Guidelines and limitations for Catalyst Center 3.2.2

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**.

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

Feature	Description
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.
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.

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

Feature	Description
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.
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.

© 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
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:

- 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.

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

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	–
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	–

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

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

Supported virtual appliances

Catalyst Center 3.2.2 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.

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

Supported firmware

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

Catalyst Center 3.2.2 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

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