Release Notes for Cisco Catalyst Center, Release 3.1.6

Contents

Catalyst Center, Release 3.1.6 3
New software features 4
Changes in behavior 9
Resolved issues 10
Open issues 11
Known issues 12
Compatibility 14
Scalability 15
Supported hardware 16
Related resources 17
Legal information 17

© 2025 Cisco and/or its affiliates. All rights reserved.

Catalyst Center, Release 3.1.6

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 3.1.6.

Note: The latest release, the Catalyst Center 3.1.6-75524.200 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
2026-08-12	Updated supported firmware details.	Supported firmware
	Added CSCwv91096.	Open issues
2026-08-04	Added behavior change information for automatic detection of new APs through the switch port in the **AP Refresh** workflow.	Changes in behavior
2026-07-28	Removed the beta note and added device guidelines and limitations for security service insertion.	Catalyst Center, Known issues
2026-07-06	Added support for Catalyst Center on Amazon Web Services (AWS) deployments.	Supported virtual appliances
2026-06-30	Noted general availability of the 3.1.6-75524.200 SMU.	Package versions in Catalyst Center 3.16
2026-05-18	Added information about the AI Assistant for Catalyst Center.	Catalyst Center
2026-04-17	Added information about the 3.1.6-75524.200 SMU, including package versions and resolved bugs.	Package versions in Catalyst Center 3.16, Resolved issues
2026-04-01	Updated supported firmware details.	Supported firmware
2026-03-25	Added limitations for using IPv6 mode.	Known issues
2026-03-16	Added support for Catalyst Center on Microsoft Azure deployments.	Support virtual appliances
2026-03-05	Added information about the 3.1.6-75405.100 SMU, including package versions and resolved bugs.	Package versions in Catalyst Center 3.16, Resolved issues
2026-02-24	Added a limitation about the required Catalyst Center user role permissions for applying device credentials to sites.	Known issues
2026-01-27	Updated supported firmware and added information about upgrade guidelines and cross-version backup and restore.	Supported firmware, Known issues
2025-12-18	Initial release	–

© 2025 Cisco and/or its affiliates. All rights reserved.

New software features

Package versions in Catalyst Center 3.1.6

To download Catalyst Center software, go to https://software.cisco.com/download/home/286316341/type.

Table 2. Package versions in Catalyst Center 3.1.6

Package name	Release 3.1.6-75524.200	Release 3.1.6-75405.100	Release 3.1.6
Release build version			
Release version	3.1.6-75524.200	3.1.6-75405.100	3.1.6-75205
System updates			
System	3.1.290	3.1.286	3.1.283
System Commons	2.734.65659	2.734.65525	2.734.65386
System Addons	0.10.526	0.10.510	0.10.506
Package updates			
Access Control Application	2.734.65659	2.734.65525	2.734.65386
AI Assistant	2.734.122207	–	–
AI Endpoint Analytics	3.160.202	3.160.26	3.160.26
AI Network Analytics	4.0.38	4.0.38	4.0.35
API Catalog	6.8.519	6.8.518	6.8.515
Application and Service Remediation	3.16.44	3.16.28	3.16.23
Application Hosting	2.4.226031812	2.4.225112005	2.4.225112005
Application Visibility and Policy	2.734.117701	2.734.117614	2.734.117614
Assurance	3.160.204	3.160.194	3.160.192
Assurance – Sensor	3.160.159	3.160.159	3.160.159
Automation – Intelligent Capture	2.734.65659	2.734.65525	2.734.65386
Automation – Sensor	2.734.65659	2.734.65525	2.734.65386
Cisco Identity Services Engine Bridge	3.160.203	3.160.38	3.160.38
Cloud Connectivity	6.10.509	6.10.507	6.10.505

© 2025 Cisco and/or its affiliates. All rights reserved.

Package name	Release 3.1.6-75524.200	Release 3.1.6-75405.100	Release 3.1.6
Cloud Connectivity Communication	7.0.503	7.0.503	7.0.503
Cloud Connectivity Sense	7.0.505	7.0.505	7.0.505
Core Platform	0.10.562	0.10.553	0.10.549
Disaster Recovery	2.734.365017 **Note**: This package is available only for the on-premises hardware appliance, not for the virtual appliance.	2.734.365017 **Note**: This package is available only for the on-premises hardware appliance, not for the virtual appliance.	2.734.365017 **Note**: This package is available only for the on-premises hardware appliance, not for the virtual appliance.
DxHub Cloud Connectivity	6.10.518	6.10.516	6.10.516
Gateway Service	0.10.510	0.10.510	0.10.509
Global Search	6.9.4	6.9.4	6.9.4
Group Based Policy Analytics	3.160.114	3.160.114	3.160.114
Identity and Access Management	5.4.523	5.4.516	5.4.510
Identity and Access Management User Interface	5.4.506	5.4.506	5.4.504
Multiple Instance Enablement	2.734.65659	2.734.65525	2.734.65386
Network Controller Platform	2.734.65659	2.734.65525	2.734.65386
Network Data Platform Base Analytics	3.160.10130	3.160.10130	3.160.10127
Network Data Platform Caching Infra	6.6.503	6.6.503	6.6.503
Network Data Platform Core	6.6.507	6.6.504	6.6.504
Network Data Platform Data Ingestion	6.6.505	6.6.505	6.6.505
Network Data Platform Management User Interface	6.6.101	6.6.101	6.6.101
Network Data Platform Pipeline	6.6.505	6.6.505	6.6.505

© 2025 Cisco and/or its affiliates. All rights reserved.

Package name	Release 3.1.6-75524.200	Release 3.1.6-75405.100	Release 3.1.6
Network Data Platform Storage Management	6.6.509	6.6.503	6.6.503
Platform	6.9.527	6.9.523	6.9.517
Platform Refresh	1.5.82	1.4.505	1.4.40
RCA Collector	0.5.502	0.5.502	0.5.7
Rogue and aWIPS	3.1.411	3.1.411	3.1.411
SD Access	2.734.65658	2.734.65525	2.734.65386
Shared Managed Services	0.10.517	0.10.514	0.10.512
Stealthwatch Security Analytics	2.734.1095099	2.734.1095099	2.734.1095099
Support Services	2.734.885152	2.734.885129	2.734.885129
System Management Operations	1.6.523	1.6.517	1.6.511
Telemetry	4.7.504	4.7.502	4.7.502
User Interface Platform	3.5.509	3.5.507	3.5.507
Wide Area Bonjour	2.734.755017	2.734.755017	2.734.755017

Disaster Recovery witness

The Disaster Recovery witness is available as a separate OVA file for Catalyst Center. Its version number is 2.1.734.370011.

Catalyst Center

Table 3. New and changed features in Catalyst Center 3.1.6

Product impact	Feature	Description
Ease of use	AI Assistant	The AI Assistant is a conversational AI interface designed to help optimize network management and promote troubleshooting. Through AI-powered responses, recommendations, and insights, the AI Assistant helps streamline network operations. With its troubleshooting capabilities, the AI Assistant helps assist you with identifying and resolving network issues and contributes to minimal downtime and enhanced performance. For details about the AI Assistant, refer to Cisco Catalyst Center AI Assistant.
Base functionality	Security service insertion for SD-Access	Catalyst Center supports security service insertion to enhance security for SD-Access fabric networks by steering the traffic through firewalls based on predefined policies.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	SNMPv3 authentication support for SHA256	Catalyst Center now supports SHA256 as an SNMPv3 authentication type. The use of SHA256 provides a stronger authentication mechanism compared to older algorithms, enhancing the security of SNMP communication with Catalyst Center.
	Support for campus networks	The Campus Network feature in Catalyst Center enables you to manage devices across multiple sites using networks and device groups. You can compare device configurations and learn or create group profiles within your network. **Note:** This feature is in beta.
	Traffic steering policy configuration	Catalyst Center supports the configuration of traffic steering policies to redirect the required traffic to the firewall. You can use the traffic steering policies for security service insertion.
	Support for cross-version backup and restore	Catalyst Center supports cross-version backup and restore. You can create a backup of Catalyst Center 3.1.3 or Catalyst Center 3.1.5 and restore it to Catalyst Center 3.1.6.

Cisco Catalyst Assurance

Table 4. New and changed features in Cisco Catalyst Assurance 3.1.6

Product impact	Feature	Description
Ease of use	View details of all rogue APs on a floor	You can view the precise location of all rogue APs and their threat levels on a floor map.

Catalyst Center platform

Table 5. New and changed features in Catalyst Center platform 3.1.6

Product impact	Feature	Description
Base functionality	API Operations	The 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 Event	The Catalyst Center platform supports a new Assurance event called NETWORK-FABRIC_WIRED-1-338, which triggers when firewall connectivity goes down from a fabric edge node for a specific VRF and firewall IP. This firewall IP reachability issue monitors the availability of a route from edge nodes to the firewall in fabric sites with service insertion enabled. One issue is generated for each unique edge node, firewall IP, and VRF combination.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Ease of use	Client Report	The Catalyst Center platform supports a new Client report template called Client Roam Events. Use this template to generate a report on devices that frequently (within 10 minutes) switch between adjacent access points (APs) despite being stationary. For more information, refer to “New and changed information” in the Cisco Catalyst Center Platform User Guide.

Catalyst Center Automation

Table 6. New and changed features in Catalyst Center Automation 3.1.6

Product impact	Feature	Description
Base functionality	AP Locally Significant Certificate (LSC) renewal for wireless devices	Catalyst Center enables you to create AP LSC renewal profiles and renew the AP LSCs for wireless devices before its expiry. **Note:** The device must be running Cisco IOS XE Release 17.1.7.1 or later. In the **Provision** > **Inventory** window, the **Certificate Expiration** and **Certificate Type** columns are added to the **Devices** table for easier access to certificate information.
	Enhancements to 802.11be profiles	For Cisco IOS XE Release 17.18.1, the 802.11be profiles have these enhancements: • Mark as default toggle button to set an 802.11be profile as the default profile. • Support for Multi-Link Operation (MLO) groups to use multiple frequency bands at the same time. In the **Design** > **Network Settings** > **802.11be Profiles** window, the table has these enhancements: • A new Type column indicates whether the 802.11be profile is set as the default profile. • A new info icon next to the Wireless Network Profile column displays information about the network profiles and SSIDs associated with an 802.11be profile.
	Enhancements to Per-Device Configurations for Cisco Catalyst 9800 Series Wireless Controllers	The Per-Device Configuration feature on Catalyst Center now supports these configurations and parameters for a Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS XE Release 17.18.1 or later: • Enhancements to 802.11be configurations • Wi-Fi 7 per-band status in WLAN profiles • WLAN scheduler in policy profiles • LSC provision • AP upgrade configurations
	Support for Cisco Wireless 9171I Series Access Points	Catalyst Center supports the Cisco Wireless 9171I Series Access Points for Wi-Fi 7 configuration with Cisco IOS XE Release 17.18 or later. This AP supports dual-band (XOR) capability allowing slot 1 to operate in either 5-GHz or 6-GHz radio modes. **Note:** When configuring this AP using the **Configure Access Points** workflow, you can't configure the radio parameters for slot 1 in the **Configure 5 GHz Radio Parameters** or **Configure 6 GHz Radio Parameters** windows. Instead, use the **Configure Dual-Band (XOR) Radio Parameters** window to manage these settings.

Cisco Software-Defined Access

Table 7. New and changed features in Cisco Software-Defined Access 3.1.6

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Base functionality	Support for Cisco C9350 Series Smart Switches as fabric edge device	Catalyst Center supports the deployment of Cisco C9350 Series Smart Switches as fabric edge devices. These switches support wireless traffic from connected APs. You can add these switches to your network as new devices. **Note:** Cisco C9350 Series Smart Switches do not support the embedded wireless controller role. Automated replacement of an existing deployed device with a Cisco C9350 is not supported.

Changes in behavior

Table 8. Changes in behavior in Catalyst Center 3.1.6

Change	Description
Automatic detection of APs through the switch port during the **AP Refresh** workflow	In the **Assign New APs to Old APs** window of the **AP Refresh** workflow, automatic detection of new APs through the switch port is enabled by default. If necessary, you can disable automatic detection of new APs using the toggle button.
Catalyst Center integration with CMX 11.0 and TLS 1.3	Starting with CMX 11.0, TLS 1.2 is no longer supported by default; only TLS 1.3 is supported. Catalyst Center 3.1.6 supports FIPS 140-3, TLS 1.3, and the corresponding cipher suites required by CMX 11.0. If you enable Common Criteria and lock the TLS version to TLS 1.2, integration with CMX 11.0 or later may fail. Older CMX versions, such as 10.6.x, support TLS 1.2 and do not present integration issues. From CMX 11.1.0 and later, new configuration options are available to re-enable TLS 1.2 support. For details, refer to the Cisco CMX 11.1 Release Notes and the Cisco CMX 11.1 Command Reference.
Minimum periodic resync interval increases to 6 hours	The minimum periodic resync interval (both per device and global) has been increased from 25 minutes to 6 hours to improve performance and optimize resource allocation. • Any device with a resync interval of less than 6 hours will automatically have its interval increased to the new minimum of 6 hours. • Devices already configured with a resync interval of 6 hours or longer will remain unchanged. • If the global resync interval is set to less than 6 hours, it will be increased to 6 hours. If the global resync interval is already 6 hours or more, it will remain unchanged.
Mobility configuration option removed from Per-Device Configuration for a Cisco Catalyst 9800 Series Wireless Controller	In the left pane of the device details window for a Cisco Catalyst 9800 Series Wireless Controller with Per-Device Configuration enabled, the **Mobility** option under **Global Wireless Configurations** and these tabs are removed: • Global Configuration • Peer Configuration
OFDMA uplink, OFDMA downlink, MU-MIMO uplink, and MU-MIMO downlink configuration changes for 802.11be settings	Starting with Cisco IOS XE Release 17.18.2, the **OFDMA Uplink**, **OFDMA Downlink**, **MU-MIMO Uplink**, and **MU-MIMO Downlink** parameters are deprecated and ignored in these 802.11be configurations: • 802.11be profiles for the 2.4-GHz and 5-GHz bands • 802.11BE PARAMETERS section in RF profiles for the 6-GHz band To configure these settings: • For the 2.4-GHz and 5-GHz bands: use the 802.11ax Configuration tab in the Advanced SSID Configuration feature template. • For the 6-GHz band: use the 802.11AX PARAMETERS section in the RF profiles.

© 2025 Cisco and/or its affiliates. All rights reserved.

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.

Catalyst Center 3.1.6-75524.200

Note: To obtain the SMU, go to the **Software Management** window in the Catalyst Center GUI and install 3.1.6-75524.200. If you don't see it, scroll down and click " Looking for other releases? Click here.

You can upgrade to 3.1.6-75524.200 from these releases: 3.1.6-75405.100, 3.1.6-75205, 3.1.5-75246, 3.1.3-75720, 3.1.3-75710.

Table 9. Resolved issues for Catalyst Center 3.1.6-75524.200 SMU

Bug ID	Description
CSCwe59641	Installing or upgrading an app on a wireless access-point may fail with an error stating that the device is incompatible, and detailed reason " Unknown reason for incompatibility" .
CSCwr55193	SD-Access: IP pool is not appearing in Anycast Gateway dropdown and cannot be released.
CSCwr55208	Provisioning is blocked due to gateway loss in LAN-type pools.
CSCwr72679	Critical alerts are raised for postgres consumption.
CSCws06332	SD-Access: Fabric Zones have different Anycast gateway MAC address from the devices at fabric site.
CSCws12735	Catalyst Center upgrade failed as it timed out during the migrator execution.
CSCws19489	Catalyst AI Assistant responds to a prompt with error message.
CSCws21411	In Catalyst Center 2.3.7.10, LAN automation for IE9320 switches fails due to NETCONF connection error.
CSCws41518	RMA: Retry after device reload step failure, fails with NCRM11001 error.
CSCws49143	Update telemetry settings is not pushing FQDN when certificate is FQDN only.
CSCws74602	On Fresh installation or upgrade to Catalyst Center 3.1.3, 3.1.5, or 3.1.6 running a device resync or inventory collection may fail for affected devices.
CSCws96963	SD-Access: Exception when creating a new Anycast gateway to the fabric site and fabric zone.
CSCwt04418	Catalyst Center sends Email notifications with outdated event time.
CSCwt16680	Configuration preview deploy fails with NCSP11208 error when deploy is attempted more than 7 days after preview creation.
CSCwt23772	Software image management: Readiness Service Entitlement checks failed due to licensing service failure.
CSCwt25250	Attempting to add a new CCO and Smart Account fails with the message: Error - unable to complete registration. Please retry later.
CSCwt25604	Reduce Cisco ISE updates due to intermittent presence anomalies data.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt36165	Assurance down after 3.1.6 platform migration due to missing Indices.
CSCwt48612	Not able to run the SLUP reporting and entitlement refresh.
CSCwt54456	Long path upgrade migration to ESXi VA postgres ownership issue.
CSCwt66399	Idle Catalyst Center session causes 401 unauthorized errors for AI API Calls and Breaks System Status Retrieval
CSCwt71142	Unable to delete Catalyst Center f.3.7.x migrated Full backup.

Catalyst Center 3.1.6-75405.100

Note: To obtain the SMU, go to the **Software Management** window in the Catalyst Center GUI and install 3.1.6-75405.100. If you don't see it, scroll down and click " Looking for other releases? Click here."

You can upgrade to 3.1.6-75405.100 from these releases: 3.1.6-75205, 3.1.5-75246, 3.1.3-75720, 3.1.3-75710.

Table 10. Resolved issues for Catalyst Center 3.1.6-75405.100 SMU

Bug ID	Description
CSCwr74432	Catalyst Center Network Device Health ignores the health score settings.
CSCws13007	Although proxy is configured with username and password, Smart Account and Virtual Account details aren't available, and software image download fails.
CSCws36968	You cannot deploy or discard a pending task after performing a backup and restore when upgrading from 2.3.7.10 to 3.1.6. The system returns this error: " NCSS10156: Unable to get the scheduled activity details."
CSCws52679	The Catalyst Center License Manager displays a hierarchy of unsupported routing licenses for the Catalyst 8200 series, as reported by Cisco Smart Software Manager (CSSM).
CSCws83113	The configuration was removed from fabric devices due to an empty device information field in the API payload.

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

Table 11. Open issues for Catalyst Center 3.1.6

Bug ID	Description
CSCwr86684	If the configuration **ip ssh server algorithm hostkey ecdsa-sha2-nistp256** is used without the configuration **crypto key generate ec keysize 256 label ecdsa-key**, the device accepts the hostkey ecdsa-sha2-nistp256 configuration but doesn’t serve the ECDSA algorithm as configured.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCws74602	On fresh installation or upgrade, running a device resync or inventory collection, there may be a failure for affected devices. In the GUI, the device manageability status shows “Internal Error.” Hovering over the icon displays: " Internal Error: NCIM12024: All information from the device could not be collected successfully or the inventory collection for this device has not yet started. It may be a temporary problem that will be resolved automatically. Resync the device, if that does not resolve the problem, please contact Cisco TAC.” Workaround: Modify the SNMP community or user to use a unique ACL for each. Alternatively, change ACL from standard to named.
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 12. Guidelines and limitations for Catalyst Center 3.1.6

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 a 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.

© 2025 Cisco and/or its affiliates. All rights reserved.

Feature	Description
Stealthwatch Security Analytics	If you are upgrading from Release 2.3.7.x to 3.1.x, you must have **Write** permissions for **Stealthwatch** to provision Stealthwatch Security Analytics on a device. With only **Read** permissions, you can't edit or provision the configurations. Update the permissions before or after the upgrade to enable editing and provisioning the configurations.
Upgrade	Catalyst Center supports direct upgrades from Catalyst Center 3.1.3 or Catalyst Center 3.1.5 to Catalyst Center 3.1.6. For more information, refer to the Cisco Catalyst Center Upgrade Guide.
Limitations	
AP Locally Significant Certificate (LSC) renewal for wireless devices	When you renew the AP LSC certificate in the Catalyst Center inventory, the AP certificate status shows as **Started** on the **Renew Access Point Certificate** window even after successful certificate renewal. This issue is a display issue only and the AP certificates are renewed correctly. To verify successful renewal, check the certificate expiry time, which reflects the updated value.
FIPS mode	The Catalyst Center 3.1.6-75524.200 SMU is not FIPS compliant.
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, SD Access, Cisco AI Endpoint Analytics, Cisco ISE, and Support Services packages are disabled and cannot be downloaded or installed. Before upgrading, remove those packages from the IPv6 deployment, because those packages don't support IPv6. • Communication through Cisco ISE pxGrid is disabled because Cisco ISE pxGrid doesn't support IPv6. • LAN automation is not supported. • Adding devices to a site is supported, but provisioning is not supported. • ITSM integration is not supported. • Network profiles for wireless devices are not supported. • Stealthwatch Security Analytics is not supported. • Disaster Recovery is not supported. • Catalyst Center does not support integration with Cisco ISE when it's also configured for IPv6. It only supports the use of Cisco ISE as an AAA server.
Per-Device Configurations	• When a wireless controller that is managed through Per-Device Configurations is upgraded to Cisco IOS XE Release 17.18.x from 17.15.x, the self-signed trustpoint name is not displayed in the Per-Device Configuration window while configuring HTTPS, web authentication, EAP profile, and management trustpoints with day-n changes. When this issue occurs, configure the trustpoint directly on the Cisco Catalyst 9800 Series Wireless Controller using CLI or Web UI. • When a wireless controller is configured to use an LSC as its management trustpoint, only APs with valid LSCs can join. New APs, especially the APs onboarded through Plug and Play (PnP), present a Manufacturer Installed Certificate (MIC) during their initial join attempt. The wireless controller rejects these APs, so root certificate updates cannot occur. To ensure successful onboarding, configure the AP certificate policy on the Cisco Catalyst 9800 Series Wireless Controller Web UI to temporarily allow MIC-based APs to join. After onboarding, update the AP certificate policy to use an LSC. For more information, refer to the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.
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

© 2025 Cisco and/or its affiliates. All rights reserved.

Feature	Description
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 WiFi" chapter of the Cisco Identity Services Engine Administrator Guide.
Upgrade	In-Service Software Upgrade (ISSU) is not supported in Cisco SD-Access deployments, with this exception: Catalyst IE3200, IE3300, and IE3400 switches are classified as low-flash memory devices. Although Catalyst Center typically recommends using install mode for SWIM upgrades, this method may fail on Catalyst IE switches when upgrading from Cisco IOS XE Release 17.x to 17.12.x. Therefore, for SWIM upgrades in install mode, we recommend upgrading the switch to Release 17.15.x or later. If you are using bundle mode, you can upgrade the switch to Release 17.12.x.
Upgrade	ISSU is not supported on the Cisco C9610 Smart Switch when upgrading from Cisco IOS XE Release 17.18.1 to 17.18.2. Although Catalyst Center typically recommends using install mode for SWIM upgrades, SWIM will continue to function, but ISSU will not work due to compatibility limitations specific to Cisco C9610 Smart Switches when upgrading from 17.18.1 to 17.18.2.

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.

© 2025 Cisco and/or its affiliates. All rights reserved.

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 13. WCAG 2.1 standard for the AA conformance level and limitations

WCAG success criterion	Support	Limitations
1.2.4: Captions (Live)	Not Supported	–
1.2.5: Audio Description (Prerecorded)	Not Supported	–
1.3.4: Orientation	Not Supported	–
1.3.5: Identify Input Purpose	Supported	–
1.4.3: Contrast (Minimum)	Supported	–
1.4.4: Resize Text	Supported	–
1.4.5: Images of Text	Supported	–
1.4.10: Reflow	Supported	–
1.4.11: Non -Text Contrast	Supported	–
1.4.12: Text Spacing	Supported	–
1.4.13: Content on Hover or Focus	Supported	–
2.4.5: Multiple Ways	Supported	–
2.4.6: Headings and Labels	Supported	–
2.4.11: Focus Appearance (Minimum)	Supported	–
2.5.7: Dragging Movements	Partially Supported	Dashboard partially supports drag and drop due to third-party library limitations.
2.5.8: Target Size (Minimum)	Supported	–
3.1.2: Language of Parts	Supported	–
3.2.3: Consistent Navigation	Supported	–
3.2.4: Consistent Identification	Supported	–
3.3.3: Error Suggestion	Supported	–
3.3.4: Error Prevention (Legal, Financial, Data)	Not Supported	–

© 2025 Cisco and/or its affiliates. All rights reserved.

WCAG success criterion	Support	Limitations
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 3.1.6 is supported for deployment as a virtual appliance (VA) only on Amazon Web Services (AWS) or Microsoft Azure in the cloud, or on VMware ESXi for on-premises environments. Neither Catalyst Center nor Cisco TAC can provide support for any issues, bugs, or unexpected behavior that occur in environments that use other hypervisors.

Supported firmware

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

Catalyst Center 3.1.6 has been validated only against these firmware versions:

© 2025 Cisco and/or its affiliates. All rights reserved.

- 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, the “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.

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