Release Notes for Cisco Catalyst Center, Release 3.1.3

Contents

Catalyst Center, Release 3.1.3 3
New software features 4
Changes in behavior 11
Resolved issues 11
Open issues 11
Known issues 12
Compatibility 15
Scalability 15
Supported hardware 17
Related resources 18
Legal information 18

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

Catalyst Center, Release 3.1.3

Cisco Catalyst Center is a powerful and 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 3.1.3.

Note: Catalyst Center 3.1.3 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
2026-09-28	Added out-of-band AP replacement guidelines.	Known issues
2026-08-12	Updated supported firmware details.	Supported firmware
	Added CSCwv91096.	Open issues
2026-04-01	Revised the supported firmware details.	Supported firmware
2026-02-24	Added a limitation about the required Catalyst Center user role permissions for applying device credentials to sites.	Known issues
2026-01-29	Updated the Cisco Connected Mobile Experiences support information.	Support for Cisco Connected Mobile Experiences
2026-01-05	Added a wireless limitation about the use of existing Cisco ISE portals for guest SSIDs.	Known issues
2025-12-10	Added information about support for 9800-CL on Azure.	Catalyst Center Automation
2025-12-08	Added new feature content for ECDSA-based private keys support.	Catalyst Center platform
2025-10-21	Revised supported firmware details.	Supported firmware
2025-10-17	Added Authentication templates with optional voice VLAN configuration.	Cisco Software-Defined Access
2025-10-10	Added information about new user email address handling changes.	Changes in behavior
2025-10-10	Added an upgrade limitation about Software Image Management (SWIM) upgrades for Catalyst IE3200, IE3300, and IE3400 switches.	Known issues
2025-10-06	Added information about IPv6 limitations.	Known issues
2025-09-30	Added information about the option to edit policy profile name in SSIDs and wireless network profiles.	Changes in behavior
2025-09-15	Added information about new features for Stealthwatch Security Analytics service on Cisco Catalyst.	Stealthwatch Security Analytics service on Catalyst Center

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

Date	Change	Location
2025-09-11	Noted that Disaster Recovery is supported for only on-premises hardware appliances.	New software features
2025-08-28	Noted that for virtual appliance deployments, neither Catalyst Center nor Cisco TAC can provide support for any issues, bugs, or unexpected behavior that occur in environments that use unsupported hypervisors.	Supported virtual appliance
2025-08-21	Noted that when SFTP mode is disabled, Catalyst Center still returns ssh-rsa over port 22. However, there is no risk to Catalyst Center, as it does not support key-based client authentication.	Known issues
2025-08-11	Added information about API rate limit limitations for Catalyst Center on ESXi.	Known issues
2025-08-08	Added guidelines about permission requirements for provisioning Stealthwatch Security Analytics on a device after an upgrade.	Known issues
2025-07-18	Added information about Catalyst Center on ESXi limitations.	Known issues
2025-06-30	Added information about the enhancements to the synchronization process for wireless controller configuration changes	Catalyst Center Automation
2025-06-16	Initial release	–

New software features

Package versions in Catalyst Center 3.1.3

Table 2. Package versions in Catalyst Center 3.1.3

Package name	Release 3.1.3
Release build version	
Release version	3.1.3-75710
System updates	
System	3.1.59
System Commons	2.730.65945
System Addons	0.10.35
Package updates	
Access Control Application	2.730.65945
AI Endpoint Analytics	1.11.1529
AI Network Analytics	4.0.30
Application and Service Remediation	3.0.20
Application Hosting	2.3.125041411

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

Package name	Release 3.1.3
Application Visibility and Policy	2.730.117956
Assurance	3.130.480
Assurance – Sensor	3.130.416
Automation - Intelligent Capture	2.730.65945
Automation – Sensor	2.730.65945
Catalyst Center API Catalog	6.8.80-3
Catalyst Center Gateway Service	0.10.8
Cisco Catalyst Center Global Search	6.9.3
Cisco Catalyst Center Platform	6.9.39-3
Cisco Catalyst Center UI	3.5.138-3
Cisco Identity Services Engine Bridge	3.130.14
Cloud Connectivity	6.10.8
Cloud Connectivity - Contextual Content	7.0.7
Cloud Connectivity – Digestor	7.0.4
Core Platform	0.10.162-3
Disaster Recovery	2.730.365227 **Note**: This package is available only for the on-premises hardware appliance, not for the virtual appliance.
DxHub Cloud Connectivity	6.10.21
Group Based Policy Analytics	3.130.15
Identity and Access Management	5.4.36-3
Identity and Access Management - UI	5.4.23-1
Multiple Cisco Catalyst Center	2.730.65945
Network Controller Platform	2.730.65945
Network Data Platform - Base Analytics	3.130.150390
Network Data Platform - Caching Infra	6.6.9
Network Data Platform – Core	6.6.118

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

Package name	Release 3.1.3
Network Data Platform - Ingestion Infra	6.6.10
Network Data Platform - Manager	6.6.100
Network Data Platform - Pipeline Infra	6.6.119
Network Data Platform - Storage Management	6.6.38
Platform Refresh	1.2.90
RCA-Scripts Package	0.5.6
Rogue and aWIPS	3.1.57
SD Access	2.730.65945
SEA App	2.730.685124
Shared Managed Services	0.10.14
Stealthwatch Security Analytics	2.730.1095371
Support Services	2.730.885298
System Management Operations	1.6.38
Telemetry	4.7.15-2
Wide Area Bonjour	2.730.755051

Disaster Recovery witness

The Disaster Recovery witness is available as a separate OVA file for Catalyst Center. Its version number is 2.1.730.370045.

Catalyst Center

Table 3. New and changed features in Catalyst Center 3.1.3

Product impact	Feature	Description
Base functionality	Configure Parallel Redundancy Protocol	This workflow helps you set up and manage Parallel Redundancy Protocol (PRP) channels, which are used to ensure high availability and zero packet loss in critical network systems.
	Energy Management	Catalyst Center's Energy Management offers insights into energy consumption patterns. This enables more strategic energy usage, significantly reduces operational costs, and reduces carbon footprint, that contributes to environmental sustainability.
	Role-based access control enhancements for wireless devices	Catalyst Center supports site-based, role-based access control (SRBAC), which limits a user's scope of access to certain network sites. You must ensure you have access to the sites and devices while using the wireless provisioning workflows.

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

Product impact	Feature	Description
	Security and industrial configurations	You can view and edit these device configurations in Catalyst Center inventory: • Security: Supported for Cisco Catalyst 9000 Series Switches and Cisco Catalyst IE switches. • Industrial configurations: Supported for Cisco Catalyst IE switches only.
	Support for site-based, role-based access control	You can create access groups that limits access to certain network sites. Access group is a combination of the role and site. The behavior of Catalyst Center features depends on the user role and site specified in the access group.
	Validation enhancements for assigning sites between different parent sites	In network hierarchy, you can move a site under a different parent site only when the new parent site shares the same network settings as the current parent site. The new parent site must have the same network profile as the site.
	VLAN support for trunk ports	Catalyst Center supports the configuration of the allowed and native VLAN values for each trunk port.
Ease of use	Enhancements to discovery dashboard	The discovery dashboard now has the option to monitor and manage all the scheduled network operations.
	Enhancements to software image repository	The software image repository is now enhanced with more options to check the status of the image updates, schedule the image update at a specific date and time, and download readiness report for the updates.

Cisco Catalyst Assurance

Table 4. New and changed features in Cisco Catalyst Assurance 3.1.3

Product impact	Feature	Description
Base functionality	AFC support for 6-GHz radio frequency in AP 360	In the **AP 360** window, under the **Detail Information > RF tab**, **Radio 2** (6-GHz band) includes support for **Automated Frequency Coordination (AFC)**. This feature helps to reduce interference between APs and other devices operating on 6-GHz radio frequency, and enables the use of Standard Power AP operations.
	Site-based, role-based access control for Assurance dashboards	Assurance supports site-based, role-based access control (SRBAC), which limits a user's scope of access to certain network sites. Based on the scope or site-based assignment, the user can access and view the Network dashboard, Client dashboard, Issues dashboard, Application health dashboard, Network services dashboard, AI-enhanced RRM dashboard, devices, and clients. Only new users assigned with site- and role-based access control have restricted access to their respective scope-based dashboards and widgets and can view only the limited number of devices, clients, network topology, global issues, and health score settings.

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

Product impact	Feature	Description
Ease of use	Enhanced visibility into Cisco ISE authentication failures for wired and wireless clients	Instead of logging in to the Cisco ISE GUI to view Cisco ISE authentication failure details for wired and wireless clients, you can now view the Cisco ISE authentication failure details in Assurance on the • **Assurance > Health** dashboard under the **Client** tab, • **Client 360** window, • **Assurance > Issues and Events** dashboard under the Events tab, and • **Assurance > Health** dashboard under the **Network Services > AAA** tab.
	Contextual RCA for support bundle	You can initiate a contextual root cause analysis (RCA) directly from the **Activity Logs** and also download the logs for provisioning failures.
	Enhancement to ThousandEyes Enterprise Agent	You can install and manage ThousandEyes Enterprise Agents from the **Health > Application** dashboard.

Catalyst Center platform

Table 5. New and changed features in Catalyst Center platform 3.1.3

Product impact	Feature	Description
Software reliability	Support for ECDSA-based private keys	Catalyst Center adds support for certificates that use the Elliptic Curve Digital Signature Algorithm (ECDSA). This update improves how digital signatures are generated, making them more efficient and secure than those from older public-key algorithms like RSA. ECDSA offers similar security levels but uses much shorter key lengths. This means it requires less computing power and processes information faster. As a result, ECDSA is ideal for systems with limited resources and for today's advanced cryptographic needs. Note that Catalyst Center continues to support RSA-based certificates.
Base functionality	API Operations	Catalyst Center platform supports new API operations. For more information, see “New and changed information” in the Cisco Catalyst Center Platform User Guide. For detailed information about the API operations, see the Cisco Catalyst Center APIs on Cisco DevNet.
	Network Devices Report	This Catalyst Center platform release supports a new Energy Management report template. Using this report template, you can retrieve a consolidated Energy Management report showing energy consumption, cost, carbon emission, and carbon intensity data of your network devices, providing complete visibility. For more information, see “Run a Network Devices Report” in the Cisco Catalyst Center Platform User Guide.

Catalyst Center Automation

Table 6. New and changed features in Catalyst Center Automation 3.1.3

Product impact	Feature	Description
Base functionality	Support for 9800-CL on Azure	Catalyst Center supports Cisco Catalyst 9800-CL Wireless Controllers that are hosted in the Microsoft Azure environment.

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

Product impact	Feature	Description
	Access point (AP) priming for Cisco Catalyst 9800 Series Wireless Controller	AP priming for Cisco Catalyst 9800 Series Wireless Controller enables users to preconfigure an AP to join a specific wireless controller. This allows the AP to automatically join its preferred wireless controller upon bootup.
	Cloning the profiles across multiple wireless controllers	Catalyst Center supports cloning the existing profiles created for wireless controllers. This allows users to reuse the configurations across multiple controllers, reducing the time taken to manually recreate the settings.
	Support for new APs for Wi-Fi 7 configuration	Catalyst Center supports these APs for Cisco IOS XE Release 17.17.1 or later: • Cisco Catalyst 9172H Series Access Points • Cisco Catalyst 9172I Series Access Points
	Support for new country codes	Catalyst Center supports new country codes for the Cisco Wireless Controllers and APs running Cisco IOS XE Release 17.17.1 or later. The radios within the APs are assigned to a specific regulatory domain at the factory. A 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, see https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html.
	Support for XOR on Cisco Catalyst 9176D1 Series APs and Cisco Catalyst 9176I Series APs	Catalyst Center supports dual-band (XOR) between 2.4-GHz and 5-GHz radio modes on slot 0 for these APs when they're running Cisco IOS XE Release 17.17.1 or later: • Cisco Catalyst 9176D1 Series Access Points • Cisco Catalyst 9176I Series Access Points **Note**: If the APs are running Cisco IOS XE Release 17.15.2, slot 0 supports only the 2.4 GHz band.
Ease of use	Enhancements to AFC integration with Standard Power Mode	Catalyst Center supports configuring AP Geolocation Parameters through the AP configuration workflow. You can view and edit geo-location parameters for eligible access points, which are utilized for Automated Frequency Coordination (AFC).
	Enhancements to Per-Device Configuration on Cisco Catalyst 9800 Series Wireless Controller	The Per-Device Configuration feature on Catalyst Center is enhanced to customize more features and parameters for a Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS XE Release 17.12 or later.
	Enhancements to the AP configuration workflow	The Configure Access Points workflow includes these AP configurations to support the Per-Device Configuration feature: • VLAN tag • DNS configuration • LAN port parameters • BSS color configuration

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

Product impact	Feature	Description
	Enhancements to the synchronization process for wireless controller configuration changes	The synchronization process triggered by a wireless controller configuration change event is optimized to improve performance: • In earlier releases, a wireless controller configuration change caused Catalyst Center to resynchronize the wireless controller and its associated APs. This synchronization included updating AP details such as their configuration, operational status, and other related data. • Starting with this release, a wireless controller configuration change now triggers only the synchronization of the wireless controller. During this synchronization, the configuration and status of APs that are associated with the wireless controller are not updated.

Cisco Software-Defined Access

Table 7. New and changed features in Cisco Software-Defined Access 3.1.3

Product impact	Feature	Description
Base functionality	Custom role for Cisco SD-Access fabric	Catalyst Center supports the creation of custom roles with the **SD-Access** capability that allows users to create and manage Cisco SD-Access fabric.
Ease of use	Enhancements to Layer 2 virtual network configurations in Cisco SD-Access fabric	Layer 2 virtual network supports configuration of these attributes: • **Resource Guard**: Option to block or unblock the SSDP traffic in the Cisco SD-Access fabric. • **Flood Access Tunnel**: Enable or disable flood access tunnel for a Layer 2 virtual network. • **Flooding Address Assignment**: Option to choose between a shared or custom flooding address and configure the custom flooding address.
	Enhancements to site hierarchy changes in Cisco SD-Access fabric	You can move a site under a new site if it is within the fabric. Movement of fabric sites to a new fabric or a site outside the fabric is not allowed.
	Mapping transits to sites in Cisco SD-Access fabric network	Associating a transit (SDA transit and IP transit) to a geographical site such as an area, building, or floor allows site users to efficiently manage the transits.
	Authentication templates with optional voice VLAN configuration	In SD-Access versions earlier than 3.1.3, fabric site interface templates were configured by default with a voice VLAN ID of 2046. This default setting was necessary because IOS XE requires a statically preconfigured voice VLAN for dynamic voice VLAN ID assignment. However, this static configuration can cause some endpoints to learn about voice VLAN 2046 through CDP or LLDP. As a result, these endpoints may send traffic to VLAN 2046, potentially leading to unintended traffic patterns or even traffic loss. Some users may want to prevent the assignment of voice VLAN ID 2046 on fabric site edge node and extended node ports. With this new feature, you can now disable the default voice VLAN 2046 during fabric site creation or at day *n* using an authentication template in the SD-Access UI. If you need a voice VLAN on specific edge node or extended node ports, you can configure it manually through the SD-Access port configuration UI. **Note**: Critical voice VLAN functionality is not supported for any authentication template where voice VLAN 2046 has been disabled.

Stealthwatch Security Analytics service

Table 8. New and changed features in Stealthwatch Security Analytics service on Catalyst Center 3.1.3

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

Product impact	Feature	Description
Base functionality	Custom role for Stealthwatch	Catalyst Center allows you to create a custom role and choose the required permission for **Stealthwatch** to manage Stealthwatch Security Analytics.
	Support for Visibility and Control of Configurations	The Visibility and Control of Configurations feature is now supported for Stealthwatch Security Analytics. 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.

Changes in behavior

Table 9. Changes in behavior in Catalyst Center 3.1.3

Change	Description
Editable policy profile name in SSIDs and wireless network profiles	In earlier releases, the policy profile name that was automatically generated from the WLAN profile name in SSID creation workflows and wireless network profiles was not editable. Starting in this release, you can edit the policy profile name in SSID creation workflows and wireless network profiles using the **Copy to Policy Profile Name** check box. You can also configure site-level overrides for policy profile name in SSIDs.
In the current release, when you create a new user, the email address of the new user must be unique, regardless of case. For example, john.doe@example.com, JOHN.DOE@example.com, and John.Doe@Example.com are all considered the same and cannot be used for multiple users.	Earlier Catalyst Center releases did not enforce a uniqueness check for case. Therefore, if you migrate existing Catalyst Center users from an earlier release to the current release, migrated users with the same email address (but different case) will be retained as separate users.

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.

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

Known issues

Table 10. Guidelines and limitations for Catalyst Center 3.1.3

Feature	Description
Guidelines	
APs	Starting with this release, 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 onboarding	For IE-3200-8P2S-E/A, IE-3200-8T2S-E/A, IE-3300-8P2S-E/A, and IE-3300-8T2S-E/A devices with Cisco IOS XE 17.8.1 or later, to avoid an increase in memory consumption: • Ensure that the device is in install boot mode before upgrading it to Catalyst Center. • Use the **no netconf-yang** command to disable NETCONF.
ssh-rsa as a host key algorithm	Even when SFTP mode is disabled, Catalyst Center still returns ssh-rsa over port 22. However, there is no risk to Catalyst Center, as it does not support key-based client authentication. Any risk from ssh-rsa's use of SHA-1 affects clients verifying the server, not the server itself. ssh-rsa is one of the public key algorithms specified in RFC 4253 for use in SSH for server host key authentication and user authentication. It indicates the use of the RSA algorithm for digital signatures. For ssh-rsa signatures, the RFC mandates the use of the SHA-1 hash algorithm for signing and verifying, as per the Digital Signature Standard (DSS) [FIPS-186-2]. With server authentication, the burden of risk associated with using the SHA-1 hashing employed by ssh-rsa falls on the client and not the server, because the client tries to establish the legitimacy of the server, which could be any host, not just Catalyst Center. With key-based client authentication, the burden of risk associated with using the SHA-1 hashing employed by ssh-rsa falls on the server and not the client, because the server tries to establish the identity of the client. Because Catalyst Center doesn't support key-based authentication, Catalyst Center is not subject to any risk with client authentication.
Stealthwatch Security Analytics	If you are upgrading from an earlier release to 3.1.3, 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.

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

Limitations	
APs	In the **Inventory** window, if you add a wireless controller with associated Wi-Fi 7 APs that don't meet license requirements, Catalyst Center displays a dialog box with details of these APs. If these APs become unreachable later, Catalyst Center continues to list them in the dialog box.
Application telemetry	With Catalyst Center, application telemetry is not supported for Cisco Catalyst 9500 Series switches.
Catalyst Center on ESXi	• Catalyst Center 3.1.3 on ESXi supports all the features that Catalyst Center 2.3.7.x on ESXi supports except for these features: ◦ Wireless: Cisco Umbrella ◦ System Workflows: These backup and restore methods are not supported: ◦ Backup and restore using the VMware vSphere Client snapshot function. ◦ Backup and restore from the Catalyst Center hardware appliance to the Catalyst Center virtual appliance on ESXi. ◦ System Performance APIs: These APIs are not supported: ◦ /dna/intent/api/v1/diagnostics/system/performance ◦ /dna/intent/api/v1/diagnostics/system/performance/history • The API rate limit policies that are documented in the official API documentation aren't enforced. As a result, you might exceed the recommended API request limits without being automatically throttled or blocked by the system with an error response 429. While exceeding the API rate limits is not recommended, it is unlikely to cause immediate service disruption or security vulnerabilities. However, excessive API usage could lead to: ◦ Performance degradation: High API request volumes could impact the overall performance of the Catalyst Center platform, potentially causing slower response times or temporary unavailability. ◦ Resource contention: Increased API activity could consume additional system resources, affecting other platform functions or user experiences. ◦ Unexpected behavior: In some cases, exceeding the API rate limits could trigger unexpected platform behavior or errors. We recommend that you adhere to the documented API rate limit policies to ensure optimal platform performance and stability. • For Group-Based Policy Analytics, the summary for the 24-hour and 12-hour Sankey charts isn't available in Catalyst Center on ESXi. • The three-node HA is not supported for Catalyst Center running on ESXi. For information about the VMware vSphere implementation and requirements for creating and using a vSphere HA cluster, see the VMware vSphere product documentation. • Catalyst Center on ESXi does not support these VMware vSphere features: ◦ Fault tolerance ◦ Suspending and resuming VMs ◦ Cloning VMs ◦ Snapshot (as backup) • To configure the Management interface and the Enterprise interface, manually create a virtual machine using the VMware vSphere UI and then configure both interfaces using either the Maglev Configuration wizard or the Install Configuration wizard. For more information, see " Deploy a Virtual Appliance" in the Cisco Catalyst Center on ESXi Deployment Guide.
Cisco AireOS Wireless Controller	When you onboard a FIPS-enabled Cisco AireOS Wireless Controller to Catalyst Center, the device compliance checks may fail due to a mismatch in the NA server CA certificate. To resolve this issue, complete these steps: **Step 1.**From the Catalyst Center UI, download the NA server CA certificate. Use this URL to automatically download the certificate file: *http://<Catalyst Center IP address>/ca/pem* **Note**: Use the HTTP method to download the CA certificate file. **Step 2.**Download this certificate file to Cisco AireOS Wireless Controller.

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

	• From the Cisco AireOS Wireless Controller main menu, choose **Commands > Download File**. • Choose the file type **NA-Serv-CA-Certificate**. • Choose the required transfer mode. • Enter valid data for the required configurations and click **Download**.
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	If you choose to run Catalyst Center in 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 a AAA server.
Required Catalyst Center user role permissions for applying device credentials to sites	You must have the required user role permissions to use the **Apply** action on **Network Settings** page under the **Device Credentials** tab. The permissions have changed in this release. The required permissions are the • Network Management > Network-wide Settings permission with write access, and • Network Provision > Device Provision permission with write access. Custom roles created with the Network Design > Advanced Network Settings permission with write access and the Network Provision > Provision permission with read or deny access in Catalyst Center Release 2.3.7.x and earlier will not have access to the **Apply** action after upgrading to this release. Ensure that you update the user role permissions to the required permission for this release, so you can apply device credentials to sites successfully.
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, see "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.
Zero-touch onboarding	In Catalyst Center 3.1.3 and earlier, zero-touch onboarding is not supported for intermediate node replacements. To replace an intermediate node, first add the new device via inventory/discovery, then complete the process using the Catalyst Center device replacement workflow.

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

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, see the Cisco Catalyst Center Compatibility Matrix.

Cisco SD-Access compatibility matrix

For information about Cisco SD-Access hardware and software support for Catalyst Center, see the Cisco Software-Defined Access Compatibility Matrix. This information is helpful for deploying Cisco SD-Access.

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.

Supported upgrade paths

For information about upgrading your current release of Catalyst Center, see 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, see "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, see the Cisco Catalyst Center Data Sheet.

Support for Cisco Connected Mobile Experiences

Catalyst Center supports Cisco Connected Mobile Experiences (CMX) Release 10.6.3 or later. Earlier versions of Cisco CMX are not supported.

Caution:

- While configuring the CMX settings, do not include the # symbol in the CMX admin password. The CMX integration fails if you include the # symbol in the CMX admin password.
- Catalyst Center validates the CMX TLS/SSL certificates. The Catalyst Center GUI provides an option to review and import CMX certificates to establish trust for new and existing CMX integrations. To avoid interruption of service between Catalyst Center and CMX, configure the CMX SSL/TLS certificates and import the CMX certificate to Catalyst Center Trusted Certificates before upgrading to Catalyst Center 3.1.3. After the upgrade, you can validate the CMX connection status under **System > Settings > Cisco Spaces/CMX Servers**. Self-signed server certificates that aren't signed by a certificate authority (CA) aren't trusted.

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

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	–
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	–

© 2025 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	–

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, see the Statement of Volatility for Cisco UCS Hardware.

Supported virtual appliance

Catalyst Center 3.1.3 is supported for deployment as a virtual appliance (VA) 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 3.1.3 has been validated only against these firmware:

- 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

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

Update the Cisco IMC firmware

To update your Cisco IMC firmware, first see 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, see 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. See “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

See Cisco Catalyst Center Documentation for additional documents 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.

© 2025 Cisco Systems, Inc. All rights reserved