# Release Notes for Cisco Catalyst Center, Release 3.1.5

# Contents

Catalyst Center, Release 3.1.5 ..... 3
New software features ..... 3
Changes in behavior ..... 7
Resolved issues ..... 8
Open issues ..... 8
Known issues ..... 8
Compatibility ..... 10
Scalability ..... 11
Supported hardware ..... 12
Related resources ..... 13
Legal information ..... 13

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

## Catalyst Center, Release 3.1.5

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 3.1.5.

**Note**: Catalyst Center 3.1.5 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 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 |
| 2026-01-15 | Added CSCws74602 to Open Issues | Open issues |
| 2026-01-05 | Added a wireless limitation about the use of existing Cisco ISE portals for guest SSIDs. | Known issues |
| 2025-12-11 | Added AP guidelines. | Known issues |
| 2025-11-07 | Added Catalyst Center integration with CMX 11.0 and TLS 1.3 details. | Changes in behavior |
| 2025-10-21 | Revised supported firmware details. | Supported firmware |
| 2025-10-10 | Added an upgrade limitation about Software Image Management (SWIM) upgrades for Catalyst IE3200, IE3300, and IE3400 switches. | Known issues |
| 2025-10-01 | Initial release | – |

## New software features

### Package versions in Catalyst Center 3.1.5

**Table 2.** Package versions in Catalyst Center 3.1.5

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

| Package name | Release 3.1.5 |
|---|---|
| **Release build version** | |
| Release version | 3.1.5-75246 |
| **System updates** | |
| System | 3.1.175 |
| System Commons | 2.732.65542 |
| System Addons | 0.10.51 |
| **Package updates** | |
| Access Control Application | 2.732.65542 |
| AI Endpoint Analytics | 1.11.1708 |
| AI Network Analytics | 4.0.34 |
| Application and Service Remediation | 3.15.24 |
| Application Hosting | 2.3.325091505 |
| Application Visibility and Policy | 2.732.117669 |
| Assurance | 3.150.171 |
| Assurance – Sensor | 3.150.151 |
| Automation - Intelligent Capture | 2.732.65542 |
| Automation – Sensor | 2.732.65542 |
| Catalyst Center API Catalog | 6.8.103 |
| Catalyst Center Gateway Service | 0.10.8-3 |
| Cisco Catalyst Center Global Search | 6.9.4 |
| Cisco Catalyst Center Platform | 6.9.54 |
| Cisco Catalyst Center UI | 3.5.147 |
| Cisco Identity Services Engine Bridge | 3.150.3 |
| Cisco Umbrella | 2.732.595019 |
| Cloud Connectivity | 6.10.15 |
| Cloud Connectivity - Contextual Content | 7.0.9 |
| Cloud Connectivity – Digestor | 7.0.5 |

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

| Package name | Release 3.1.5 |
|---|---|
| Core Platform | 0.10.219 |
| Disaster Recovery | 2.732.365035<br>**Note**: This package is available only for the on-premises hardware appliance, not for the virtual appliance. |
| Cloud-Connectivity-Datahub | 6.10.29 |
| Group Based Policy Analytics | 3.150.11 |
| Identity and Access Management | 5.4.57 |
| Identity and Access Management - UI | 5.4.32 |
| Multiple Cisco Catalyst Center | 2.732.65542 |
| Network Controller Platform | 2.732.65542 |
| Network Data Platform - Base Analytics | 3.150.100247 |
| Network Data Platform - Caching Infra | 6.6.12 |
| Network Data Platform – Core | 6.6.131 |
| Network Data Platform - Ingestion Infra | 6.6.16 |
| Network Data Platform - Manager | 6.6.101 |
| Network Data Platform - Pipeline Infra | 6.6.132 |
| Network Data Platform - Storage Management | 6.6.52 |
| RCA-Scripts Package | 0.5.7 |
| Rogue and aWIPS | 3.1.206 |
| SD Access | 2.732.65542 |
| Shared Managed Services | 0.10.21 |
| Stealthwatch Security Analytics | 2.732.1095171 |
| Support Services | 2.732.885199 |
| System Management Operations | 1.6.56 |
| Telemetry | 4.7.20 |
| Wide Area Bonjour | 2.732.755008 |

## Disaster Recovery witness

The Disaster Recovery witness is available as a separate OVA file for Catalyst Center. Its version number is 2.1.732.370017.

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

## Catalyst Center

**Table 3.** New and changed features in Catalyst Center 3.1.5

| Product impact | Feature | Description |
|---|---|---|
| Base functionality | Rule-Based Compliance Policies | Catalyst Center enables you to create custom configuration rules and policies that it periodically evaluates across the network to detect violations. |
| | Overlapping IP address pools | Catalyst Center allows you to enable overlapping for the CIDR subnet of an IP address pool, which provides more flexibility when assigning IP addresses dynamically. |

## Cisco Catalyst Assurance

**Table 4.** New and changed features in Cisco Catalyst Assurance 3.1.5

| Product impact | Feature | Description |
|---|---|---|
| Base functionality | Enhancements to dashboards | Enhanced capability to define the scope and configure specific filters for client and network template dashboards. |

## Catalyst Center platform

**Table 5.** New and changed features in Catalyst Center platform 3.1.5

| Product impact | Feature | Description |
|---|---|---|
| Base functionality | API Operations | Catalyst Center platform supports new API operations.<br>For more information, see “New and changed information” in the Cisco Catalyst Center Platform User Guide.<br>For detailed information about the API operations, see the Cisco Catalyst Center APIs on Cisco DevNet. |

## Catalyst Center Automation

**Table 6.** New and changed features in Catalyst Center Automation 3.1.5

| Product impact | Feature | Description |
|---|---|---|
| Base functionality | Support for OS licenses | Catalyst Center supports OS Essentials and OS Advantage perpetual device licenses for these switches:<br>• Cisco C9610 Series Smart Switches<br>• Cisco C9350 Series Smart Switches<br>Enhancements to the **License Manager** window for OS licenses:<br>• **Overview** tab: displays information about the purchased, used, and available OS licenses.<br>• **Licenses** tab: displays the number of total, expiring, and noncompliant OS licenses.<br>• **Devices** tab: the procedure for change license level is enhanced to support OS license conversion and removal.<br>During the PnP onboarding of these switches, you can now select OS Essentials or OS Advantage stack license level from the **Select a License Level** drop-down list. |

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

| Product impact | Feature | Description |
|---|---|---|
| Ease of use | Enhancements to cloning Per-Device Configurations across multiple wireless controllers | Catalyst Center supports cloning these Per-Device Configuration features from another Cisco Catalyst 9800 Series Wireless Controller:<br>• Flex profiles<br>• RF profiles<br>• Site tags |

## Cisco Software-Defined Access

**Table 7.** New and changed features in Cisco Software-Defined Access 3.1.5

| Product impact | Feature | Description |
|---|---|---|
| Base functionality | Support for IE3500 and IE3500H as fabric edge | Catalyst Center supports Cisco Catalyst IE3500 and 3500H configured as fabric edge nodes in a campus fabric.<br>Campus fabric provides the basic infrastructure for building virtual networks based on policy-based segmentation constructs.<br>Fabric edge devices<br>• provide connectivity to users and devices that connect to the fabric domain<br>• identify and authenticate endpoints<br>• register endpoint ID information in the fabric host-tracking database, and<br>• encapsulate at ingress and unencapsulate at egress to forward traffic to and from endpoints connected to the fabric domain. |

# Changes in behavior

**Table 8.** Changes in behavior in Catalyst Center 3.1.5

| Change | Description |
|---|---|
| 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 3.1.5, which includes FIPS 140-3 support, adds TLS 1.3 and the corresponding cipher suites required by CMX 11.0. If you use TLS 1.2, integration with CMX 11.0 or later may fail.<br>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.<br>For details, see 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.<br>• Any device with a resync interval of less than 6 hours will automatically have its interval increased to the new minimum of 6 hours.<br>• Devices already configured with a resync interval of 6 hours or longer will remain unchanged.<br>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. |

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

| Change | Description |
|---|---|
| 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:<br>• Global Configuration<br>• Peer Configuration |

## 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.

**Table 9.** Open issues in Catalyst Center 3.1.5

| 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<br>“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.<br>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 10.** Guidelines and limitations for Catalyst Center 3.1.5

| Feature | Description |
|---|---|
| **Guidelines** | |

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

| Feature | Description |
|---|---|
| APs | A wireless controller configuration change triggers only a wireless controller synchronization. During this synchronization, Catalyst Center:<br>• collects the wireless controller-related configurations, but<br>• doesn't update the configuration and status of the APs associated with the wireless controller.<br>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:<br>1. On the **Inventory** window, select the wireless controller.<br>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.<br>Use the **AP Refresh** workflow to replace an AP. If you have already replaced an AP outside Catalyst Center, complete these steps:<br>1. Identify the old AP record using its serial number, MAC address, status, and last update time.<br>**Note:** Do not select a record based only on its hostname or search result.<br>2. Delete the old AP record.<br>3. Refresh the inventory or synchronize it for the replacement AP.<br>4. Confirm that only the current AP record remains and that its hostname, serial number, MAC address, and reachability state are correct. |
| 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. |
| **Limitations** | |
| Can't uninstall optional packages | Due to a known software issue (CSCwr13826) in Catalyst Center 3.1.5, Cisco has temporarily disabled the option to uninstall optional application packages. Optional packages can only be uninstalled by Cisco TAC. Open a service request with Cisco TAC for assistance. |
| Group-Based Policy Analytics | For Group-Based Policy Analytics, the summary for the 24-hour and 12-hour Sankey charts isn't available in<br>• Catalyst Center on AWS<br>• Catalyst Center on Azure, and<br>• Catalyst Center on ESXi. |
| Network Reasoner | The Machine Reasoning Engine workflows are not supported on Catalyst 9350 and Catalyst 9610 devices. |
| In-product help | • Online help and Interactive Help are available in light mode only and don't support dark mode.<br>• 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. |

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

| Feature | Description |
| --- | --- |
| IPv6 | If you choose to run Catalyst Center in IPv6 mode:<br>• 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.<br>• Communication through Cisco ISE pxGrid is disabled because Cisco ISE pxGrid doesn't support IPv6.<br>• LAN automation is not supported.<br>• Adding devices to a site is supported, but provisioning is not supported.<br>• ITSM integration is not supported.<br>• Network profiles for wireless devices are not supported.<br>• Stealthwatch Security Analytics is not supported.<br>• Disaster Recovery is not supported.<br>• 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<br>• Network Management > Network-wide Settings permission with write access, and<br>• Network Provision > Device Provision permission with write access.<br>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.<br>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:<br>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. |

# 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.

## Compatible browsers

The Catalyst Center GUI is compatible with the following HTTPS-enabled browsers:

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

- 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, 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 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 | – |

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

| WCAG success criterion | Support | Limitations |
|---|---|---|
| 2.4.5: Multiple Ways | Supported | – |
| 2.4.6: Headings and Labels | Supported | – |
| 2.4.11: Focus Appearance (Minimum) | Supported | – |
| 2.5.7: Dragging Movements | Partially Supported | Dashboard partially supports drag and drop due to third-party library limitations. |
| 2.5.8: Target Size (Minimum) | Supported | – |
| 3.1.2: Language of Parts | Supported | – |
| 3.2.3: Consistent Navigation | Supported | – |
| 3.2.4: Consistent Identification | Supported | – |
| 3.3.3: Error Suggestion | Supported | – |
| 3.3.4: Error Prevention (Legal, Financial, Data) | Not Supported | – |
| 3.1.2: Language of Parts | Supported | – |
| 3.2.3: Consistent Navigation | Supported | – |
| 3.2.4: Consistent Identification | Supported | – |
| 3.3.3: Error Suggestion | Supported | – |
| 3.3.4: Error Prevention (Legal, Financial, Data) | Not Supported | – |

# 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

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

- 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 appliances

Catalyst Center 3.1.5 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 3.1.5 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 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