Release Notes for Cisco Catalyst Center, Release 2.3.7.x

First Published: 2023-12-20

Last Modified: 2024-04-15

Release Notes for Cisco Catalyst Center, Release 2.3.7.x

Catalyst Center 2.3.7.x is available in a phased rollout. Until the software becomes generally available, contact your Cisco sales representative to request this release. Upon completion of the phased rollout, Catalyst Center will be made generally available to all customers.

This document describes the features, limitations, and bugs for Catalyst Center, Release 2.3.7.x.

For links to all the guides in this release, see *Cisco Catalyst Center 2.3.7 Documentation.*

Note Cisco DNA Center has been rebranded as Catalyst Center. During the rebranding process, you will see both names used in different collaterals, but both names refer to the same product.

Change History

The following table lists changes to this document since its initial release.

Date	Change	Location
2024-04-15	Updated the list of packages in 2.3.7.5.	Package Versions in Catalyst Center, on page 2
2024-04-08	Added the list of packages in 2.3.7.5.	Package Versions in Catalyst Center, on page 2
	Added the Resolved Bugs table for 2.3.7.5.	Resolved Bugs, on page 41
	Added the open bugs for 2.3.7.5.	Open Bugs, on page 39
	Added information about enhancements to VLAN ID configuration for wireless interfaces in 2.3.7.4.	New and Changed Features in Catalyst Center Automation, on page 23
	Added information about AI-Enhanced RRM guidelines for scale provisioning for 2.3.7.4.	Guidelines and Limitations, on page 30

Date	Change	Location
2024-01-09	Added that Catalyst Center supports CISCOAES192 and CISCOAES256 encryption for SNMPv3 configuration. If you add devices with AES192 or AES256 encryption to Catalyst Center, Assurance data is collected for those devices.	New and Changed Features in Cisco Catalyst Assurance, on page 8
	Added a limitation about provisioning wireless devices that are tagged with the INV_EVENT_SYNC_DISABLED tag.	Guidelines and Limitations, on page 30
2023-12-20	Initial release.	—

Upgrade to the Latest Catalyst Center Release

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*.

Package Versions in Catalyst Center

Package Name	Release 2.3.7.5	Release 2.3.7.4
Release Build Version		
Release Version	2.3.7.5.70434	2.3.7.4.70424
System Updates		
System	1.8.114	1.7.1105
System Commons	2.1.715.60719	2.1.714.60631
Package Updates		
Access Control Application	2.1.715.60719	2.1.714.60631
AI Endpoint Analytics	1.11.938	1.11.726
AI Network Analytics	3.1.39.362	3.1.30.335
Application Hosting	2.3.12402020457	2.3.12311300818
Application Policy	2.1.715.117447	2.1.714.117457
Application Registry	2.1.715.117447	2.1.714.117457
Application Visibility Service	2.1.715.117447	2.1.714.117457

Package Name	Release 2.3.7.5	Release 2.3.7.4
Assurance - Base	2.3.7.5165	2.3.7.4138
Assurance - Sensor	2.3.7.5122	2.3.7.4139
Automation - Base	2.1.715.60719	2.1.714.60631
Automation - Intelligent Capture	2.1.715.60719	2.1.714.60631
Automation - Sensor	2.1.715.60719	2.1.714.60631
Catalyst Center Docs	2.1.715.60719	2.1.714.60631
Catalyst Center Global Search	1.14.1.22	1.13.1.7
Catalyst Center Platform	1.14.160.64	1.13.247.0
Catalyst Center UI	1.7.6.210	1.7.6.128
Cisco Identity Services Engine Bridge	2.1.715.90510	2.1.714.90200
Cisco Umbrella	2.1.715.590202	2.1.714.590189
Cloud Connectivity - Contextual Content	2.10.1.425	2.9.1.424
Cloud Connectivity - Data Hub	1.14.20	1.13.29
Cloud Connectivity - Tethering	2.35.1.17	2.34.1.30
Cloud Device Provisioning Application	2.1.715.60719	2.1.714.60631
Command Runner	2.1.715.60719	2.1.714.60631
Device Onboarding	2.1.715.60719	2.1.714.60631
Disaster Recovery	2.1.715.360110	2.1.714.360086
Disaster Recovery—Witness Site	2.1.715.370026	2.1.714.370028
Group-Based Policy Analytics	2.3.7.43	2.3.7.23
Image Management	2.1.715.60719	2.1.714.60631
Machine Reasoning	2.1.715.210132	2.1.714.210081
NCP - Base	2.1.715.60719	2.1.714.60631
NCP - Services	2.1.715.60719	2.1.714.60631
Network Controller Platform	2.1.715.60719	2.1.714.60631
Network Data Platform - Base Analytics	2.3.7.50173	2.3.7.40097
Network Data Platform - Core	1.9.4202	1.9.4068
Network Data Platform - Manager	1.9.4202	1.9.4006

Package Name	Release 2.3.7.5	Release 2.3.7.4
Network Experience Platform - Core	2.1.715.60719	2.1.714.60631
Path Trace	2.1.715.60719	2.1.714.60631
RBAC Extensions	2.1.715.1900005	2.1.714.1900008
Rogue and aWIPS	2.9.0.404	2.9.0.207
SD-Access	2.1.715.60719	2.1.714.60631
Stealthwatch Security Analytics	2.1.715.1090255	2.1.714.1090194
Support Services	2.1.714.880008	2.1.714.880008
System Remediation	1.3.0	1.2.1
Wide Area Bonjour	2.4.715.75176	2.4.714.75197

New and Changed Information

New and Changed Features in Catalyst Center

Table 1: New and Changed Features in Catalyst Center, Release 2.3.7.5

Feature	Description
Enhancements to Configuring Global Device Credentials	On the **Device Credentials** window, you can now only assign and unassign device credentials to and from sites. On the **Manage Credentials** slide-in pane, you can manage your device credentials using the **Focus** drop-down list. Depending on which focus you choose (**Current site** or **System**), you can perform specific actions.
Enhancements to Device Onboarding and the Discovery Workflow	The **Add Device** option in the Catalyst Center Inventory is enhanced to include options for adding both new and existing devices. The discovery workflow includes enhancements, such as: • The **Provide Credentials** window now includes the option to configure advance settings along with the CLI and SNMP credentials. • The **Schedule Job** window combines site assignment and scheduling of the discovery job.

Feature	Description
Enhancement to Device Resynchronization	Prior to this release, restarting the inventory service would trigger resynchronization for all devices in the inventory. With this release, device resynchronization is triggered after the inventory service restart under the following circumstances only: • After Catalyst Center upgrade. • If the device's synchronization is in terminated or delayed state after the service restart. • If the device's last synchronization time has crossed the configured cutoff time.
Enhancements to Device Upgrade Readiness Check	• Flash Check: Calculates the space required for upgrading to golden image with add-on and performs flash clean up proactively before image distribution. • Weak Crypto Check: Checks whether the device is configured with weak crypto and blocks image upgrade. This readiness check is applicable only for devices with software image version 17.14 and later. • File Transfer Check for FQDN Setup: Checks whether the name server associated with the device is reachable and displays an error message.
Enhancements to Editing LAN Automated Devices	In the **Edit Devices** window, you can now edit the hostname for the devices that are discovered through LAN automation.
Progress Bar Support for Network Devices Provisioning	The **Task Progress** bar on **Activities** > **Tasks** window, displays the progress of the ongoing provisioning task for your network devices.
Support for the Workflow Progression View in Visibility- and Control-Enabled Provisioning Workflows	If a visibility- and control-enabled provisioning workflow supports the workflow progression view, the **Preparing Devices and Configuration Models** window displays the steps the system takes to prepare a listed device.
Support for Third-Generation Catalyst Center Appliances	Catalyst Center now supports the following third-generation appliances, which are based on the Cisco UCS C220 and C240 M6 servers: • 32-core appliance: Cisco part number DN3-HW-APL • 32-core promotional appliance: Cisco part number DN3-HW-APL-U • 56-core appliance: Cisco part number DN3-HW-APL-L • 56-core promotional appliance: Cisco part number DN3-HW-APL-L-U • 80-core appliance: Cisco part number DN3-HW-APL-XL • 80-core promotional appliance: Cisco part number DN3-HW-APL-XL-U For more information, see the *Cisco Catalyst Center Third-Generation Appliance Installation Guide, Release 2.3.7.x*.

Feature	Description
Support for Viewing and Editing Layer 2 Configurations of a Device	You can view and edit the Layer 2 configurations of a device in the Catalyst Center inventory. **Note** This feature is in beta.
Third-Party Devices Support	Catalyst Center allows third-party devices to populate SNMP MIB-II values.
Weak Crypto Check	To ensure a secure network connection Catalyst Center performs weak crypto check to evaluate the device configuration, and blocks the device provisioning/upgrade/site assignment for devices that are configured only with MD5 authentication for SNMP credentials. This is applicable only for devices with software image version or golden tagged image version 17.14.1 and later.
Enhancements to the disaster recovery witness site upgrade process.	Using an SSH client, you can upgrade a disaster recovery system's witness site using the **witness upgrade** command. In the *Cisco Catalyst Center Administrator Guide, Release 2.3.7.x*, see the "Implement Disaster Recovery" chapter's "Upgrade the Current Witness Site" topic.

Table 2: New and Changed Features in Catalyst Center, Release 2.3.7.4

Feature	Description
Name Change to Catalyst Center	As part of our vision to converge our products around an integrated platform, we are changing the name of Cisco DNA Center to Catalyst Center in this release. The capability and functionality of Catalyst Center remains the same as Cisco DNA Center. This name change is part of our simplified branding for the Catalyst Center Stack. Cisco is now connecting the power and flexibility of the Catalyst brand across the entire enterprise networking stack with Catalyst Center (formerly Cisco DNA Center), Catalyst Software and Licensing (formerly Cisco DNA Software and Licensing), Catalyst Wireless, Catalyst Switching, Catalyst Routing, and Catalyst SD-WAN (formerly Cisco SD-WAN or Viptela SD-WAN).
Enhancements to the Catalyst Center Home Page	The Catalyst Center home page displays a new welcome message and displays license and release banner messages relevant to Catalyst Center. The Tools area is removed and is accessible from the menu in the top-left corner.

Feature	Description
Enhancements to the Menus	To streamline workflows and standard nomenclature, we changed several menu option names, moved several submenu options, and added a secondary launch point for Interactive Help. The menu option changes include: • **Design** > **Network Settings** > **Network** is now **Design** > **Network Hierarchy** > **Servers**. • **Design** > **Network Settings** > **SP Profiles** is now **Design** > **Service Provider Profiles**. • **Provision** > **Stealthwatch Security Analytics** is now **Provision** > **Stealthwatch Security**. • **Tools** > **Template Hub** is now **Design** > **CLI Templates**. • **Tools** > **Model Config Editor** is now **Design** > **Feature Templates**. • The **Activities** menu option now lists two submenu options: **Audit Logs** and **Tasks**. • **System** > **System Health** is now **System** > **System 360** > **System Health**. • **System** > **Settings** > **Telemetry Collection** is now **System** > **Settings** > **Product Telemetry**. • The **Help** icon lists the new secondary launch point for **Interactive Help**.
Enhancements to the Configure AI-Enhanced RRM Workflow	You can configure an AI-enabled radio frequency profile without device provisioning.
Device Compliance and Pending Operation Prechecks for a Seamless Deployment	To ensure a seamless deployment, Catalyst Center performs a set of prechecks to ensure that any pending operations that conflict with the current task and any device compliance issues are addressed.
Log Collection for a Device	When a resync is done for a specific device, the debug log is enabled automatically for that device, and XDE and device pack logs are collected.
Software Image Compatibility Check for Fabric Devices	To ensure the network devices (before and after a fabric deployment) are compatible with the recommended or supported software image versions based on the Catalyst Center package version, Catalyst Center performs an Image Compatibility check to evaluate the network devices.
Updating the KGV Bundle	You can request a new KGV download workflow by clearing all the stale and suspended integrity verification (IV) workflows, if there are any.
Usability Enhancements to Previewing Configurations in Visibility- and Control-Enabled Workflows	When previewing configurations in a visibility- and control-enabled workflow, you can display the device configurations in a side-by-side comparison view. **Note** The side-by-side comparison view doesn't support viewing YANG configurations.

Feature	Description
Usability Enhancements to Support Service	Support Service has the following enhancements: • When creating a remote support authorization, you must first accept the **Access Permission Agreement**. • "SR" is replaced with "case number." • The **Past Authorizations** table is searchable and contains a column for the case number.
Visibility and Control of AI RF Profile Configurations	With the Visibility and Control of Configurations feature, you can preview AI RF profile configurations and send those configurations to IT Service Management (ITSM) for approval before deploying them.

New and Changed Features in Cisco Catalyst Assurance

Table 3: New and Changed Features in Cisco Catalyst Assurance, Release 2.3.7.5

Feature	Description
Cisco TrustSec Environment Data Download Status	With this release, the Cisco TrustSec environment data download status issue support is extended to EVPN fabric deployments.
Enhancement to Deploying and Undeploying Sensor-Driven Test Templates	When you deploy or undeploy an IP Service-Level Agreement (SLA) performance test as a part of a sensor-driven test template, Catalyst Center asks if you want to configure the relevant commands on the wireless controllers to enable or disable IP SLA, so the sensors do or do not run the tests against the APs.
Enhancements to Intelligent Capture Settings	In the **Assurance** > **Settings** > **Intelligent Capture Settings**, the enhancements include: • The **Configuration Status** column is added to view the configuration status of the onboarding and full packet capture sessions. You can also view the configuration status of the AP Statistics Capture and Anomaly Capture sessions under the respective tabs. • For AP Statistics Capture and Anomaly Capture, you can now only enable or disable specific APs or all APs managed by a wireless controller. The **None** option to disable these two features on all APs is no longer supported. • To streamline the nomenclature of Intelligent Capture, the tab names on the **Intelligent Capture Settings** are updated, as follows: • **Client Schedule Capture** is now **Onboarding Packet Capture**. • **Client Data Packet Capture** is now **Full Packet Capture**. • **OTA Sniffer Capture** is now **OTA Sniffer**.
Support of Visibility and Control of Wireless Device Configurations for Intelligent Capture	With Intelligent Capture now supporting the Visibility and Control of Configurations feature, you can preview AP and wireless controller configurations and send those configurations to IT Service Management (ITSM) for approval before deploying them.

Feature	Description
Telemetry Status in SD-Access Health Dashboard	In the **Assurance** > **SD-Access** Health dashboard, you can view the **Telemetry Status** of fabric sites, transits, and virtual networks. You can also troubleshoot the root cause and auto recovery for the missing telemetry data for the network devices
Troubleshoot Telemetry Data for Wired Devices Using MRE Checks	Using MRE checks, you can troubleshoot the root cause of missing telemetry data for switches and routers. The MRE check includes: • Check SNMP telemetry subscriptions status • Get NETCONF details MRE availability checks if it's possible to automatically correct and resolve any certificate issues that are causing availability problems for network devices. MRE for Time Drift issue: If an excessive time drift occurs between Catalyst Center and the network device and that time drift is resolved manually by configuring the NTP, during the next synchronization cycle, the excessive time drift issue is resolved automatically.

Table 4: New and Changed Features in Cisco Catalyst Assurance, Release 2.3.7.4

Feature	Description
Assurance EVPN Support	With this release, Assurance supports EVPN fabric deployments. The following issues are newly added: • **VNI(s) Down on Fabric Node**: This issue is triggered when the VNI(s) are down on a fabric node device in an EVPN protocol network. • **Expected Peer not present on Fabric Node**: This issue is triggered when the NVE peer is missing from a fabric node device in an EVPN protocol network. • **BGP Session to Spine Node Down**: This issue is triggered when the BGP session is down between a fabric node and a spine role fabric node in a fabric site. **Note** In this release, the preceding issues are applicable only for EVPN EFT users.
Assurance Issues	With this release, a new **Assurance telemetry status is poor** issue is added to Router, Core, Distribution, and Access issues, Controller, Wired Client, Wireless Client under the System category. This issue is triggered when the telemetry status of the network device or client is poor. The issue is automatically resolved when the telemetry status is good.
SNMPv3 Support for AES192 and AES256 Encryption	With this release, Catalyst Center supports CISCOAES192 and CISCOAES256 encryption for SNMPv3 configuration. If you add devices with AES192 or AES256 encryption to Catalyst Center, Assurance data is collected for those devices.
Support for Visibility and Control of RF Configurations in the AI-Enhanced RRM Control Center	With the Visibility and Control of Configurations feature, you can preview RF configurations and send those configurations to IT Service Management (ITSM) for approval before deploying them. In the AI-Enhanced Radio Resource Management (RRM) Control Center, the AI RF Profile Simulator and Insights support the Visibility and Control of Configurations feature.
Telemetry Status in Assurance Health Dashboards	In the Assurance Network and Client Health dashboards, you can view the **Telemetry Status** of the devices and clients in your network.

New and Changed Features in Catalyst Center Platform

For detailed information about the APIs, see the Cisco Catalyst Center APIs on Cisco DevNet.

Table 5: New and Changed Features in Catalyst Center Platform, Release 2.3.7.5

Feature	Description
New APIs	
LAN Automation APIs	Catalyst Center platform supports the following LAN Automation APIs: • POST <cluster-ip>/dna/intent/api/v2/lan-automation LAN Automation Start V2. • PUT <cluster-ip>/dna/intent/api/v2/lan-automation/${id} LAN Automation Stop and Update Devices V2. To access the new LAN Automation APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **LAN Automation**.
Reports APIs	Catalyst Center platform supports the following Reports APIs: • GET <cluster-ip>/dna/data/api/v1/flexible-report/schedule/${reportId} Get Flexible report schedule by report ID. • GET <cluster-ip>/dna/data/api/v1/flexible-report/report/${reportId}/executions Get Execution ID by report ID. • POST <cluster-ip>/dna/data/api/v1/flexible-report/report/${reportId}/execute Executing the Flexible report. • PUT <cluster-ip>/dna/data/api/v1/flexible-report/schedule/${reportId} Update schedule of Flexible report. • GET <cluster-ip>/dna/data/api/v1/flexible-report/schedules Get all Flexible report schedules. • GET <cluster-ip>/dna/data/api/v1/flexible-report/report/content/${reportId}/${executionId} Download Flexible report. To access the new Reports APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Operational Tasks** drop-down list and choose **Reports**.

Feature	Description
SDA APIs	

Feature	Description
	Catalyst Center platform supports the following SDA APIs: Extranet Policy APIs • GET <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies Get extranet policies. • PUT <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies Update extranet policy. • POST <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies Add extranet policy. • GET <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies/count Get extranet policy count. • DELETE <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies/${id} Delete extranet policy by ID. Port Assignment APIs • POST <cluster-ip>/dna/intent/api/v1/sda/portAssignments Add port assignments. • GET <cluster-ip>/dna/intent/api/v1/sda/portAssignments Get port assignments. • PUT <cluster-ip>/dna/intent/api/v1/sda/portAssignments Update port assignments. • GET <cluster-ip>/dna/intent/api/v1/sda/portAssignments/count Get port assignment count. • DELETE <cluster-ip>/dna/intent/api/v1/sda/portAssignments/${id} Delete port assignment by ID. • DELETE <cluster-ip>/dna/intent/api/v1/sda/portAssignments Delete port assignments. Fabric Site APIs • POST <cluster-ip>/dna/intent/api/v1/sda/fabricSites Add fabric site. • PUT <cluster-ip>/dna/intent/api/v1/sda/fabricSites Update fabric site. • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricSites/${id} Delete fabric site by ID.

Feature	Description
	• GET <cluster-ip>/dna/intent/api/v1/sda/fabricSites Get fabric sites. • GET <cluster-ip>/dna/intent/api/v1/sda/fabricSites/count Get fabric site count. Fabric Zone APIs • POST <cluster-ip>/dna/intent/api/v1/sda/fabricZones Add fabric zone. • PUT <cluster-ip>/dna/intent/api/v1/sda/fabricZones Update fabric zone. • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricZones/${id} Delete fabric zone by ID. • GET <cluster-ip>/dna/intent/api/v1/sda/fabricZones Get fabric zones. • GET <cluster-ip>/dna/intent/api/v1 /sda/fabricZones/count Get fabric zone count. Authentication Profile APIs • PUT <cluster-ip>/dna/intent/api/v1/sda/authenticationProfiles Update authentication profile. • GET <cluster-ip>/dna/intent/api/v1/sda/authenticationProfiles Get authentication profiles. Bulk Device Provisioning APIs

Feature	Description
	• GET <cluster-ip>/dna/intent/api/v1/sda/provisionDevices Get provisioned devices. • POST <cluster-ip>/dna/intent/api/v1/sda/provisionDevices Provision devices. • GET <cluster-ip>/dna/intent/api/v1/sda/provisionDevices/count Get provisioned devices count. • DELETE <cluster-ip>/dna/intent/api/v1/sda/provisionDevices Delete provisioned devices. • PUT <cluster-ip>/dna/intent/api/v1/sda/provisionDevices Reprovision devices. • DELETE <cluster-ip>/dna/intent/api/v1/ sda/provisionDevices/${id} Delete provisioned device by ID. Fabric Device APIs • POST <cluster-ip>/dna/intent/api/v1/sda/fabricDevices Add fabric devices. • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices Get fabric devices. • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/count Get fabric devices count. • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricDevices Delete fabric devices. • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/${id} Delete a fabric device by ID. • PUT <cluster-ip>/dna/intent/api/v1/sda/fabricDevices Update fabric devices. Fabric Device Layer 2 Handoff APIs

Feature	Description
	• POST <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/ layer2Handoffs Add fabric devices Layer 2 handoffs. • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/ layer2Handoffs Get fabric devices Layer 2 handoffs. • GET <cluster-ip>/ dna/intent/api/v1/sda/fabricDevices/layer2Handoffs/count Get fabric devices Layer 2 handoffs count. • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/ layer2Handoffs Delete fabric devices Layer 2 handoffs. • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/ layer2Handoffs/${id} Delete fabric device Layer 2 handoff by ID. Fabric Device IP Transit Layer 3 Handoff APIs • POST <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3Handoffs/ipTransits Add fabric devices Layer 3 handoffs with IP transit. • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3Handoffs/ipTransits Get fabric devices Layer 3 handoffs with IP transit. • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3Handoffs/ipTransits/count Get fabric devices Layer 3 handoffs with IP transit count. • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3Handoffs/ipTransits Delete fabric devices Layer 3 handoffs with IP transit. • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3Handoffs/ipTransits/${id} Delete fabric device Layer 3 handoff with IP transit by ID. • PUT <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3Handoffs/ipTransits Update fabric devices Layer 3 handoffs with IP transit. Fabric Device SDA Transit Layer 3 Handoff APIs

Feature	Description
	• POST <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3Handoffs /sdaTransits Add fabric devices Layer 3 handoffs with SDA transit. • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/ layer3Handoffs/sdaTransits Get fabric devices Layer 3 handoffs with SDA transit. • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/ layer3Handoffs/sdaTransits/count Get fabric devices Layer 3 handoffs with SDA transit count. • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/ layer3Handoffs/sdaTransits Delete fabric devices Layer 3 handoffs with SDA transit. • PUT <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3Handoffs/sdaTransits Update fabric devices Layer 3 handoffs with SDA transit. Anycast Gateways APIs • DELETE <cluster-ip>/dna/intent/api/v1/sda/anycastGateways/${id} Delete anycast gateway by ID. • PUT <cluster-ip>/dna/intent/api/v1/sda/anycastGateways Update anycast gateways. • GET <cluster-ip>/dna/intent/api/v1/sda/anycastGateways Get anycast gateways. • POST <cluster-ip>/dna/intent/api/v1/sda/anycastGateways Add anycast gateways. • GET <cluster-ip>/dna/intent/api/v1/sda/anycastGateways/count Get anycast gateway count. To access the new SDA APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Connectivity** drop-down list and choose **SDA**.
API Enhancements	
LAN Automation APIs	• The LAN Automation Device Update API now includes a new query param HOSTNAME_UPDATE to change the hostname of the device based on the new request body parameter `hostnameUpdateDevices`. • The LAN Automation Status By Id and LAN Automation Status APIs now include three additional optional parameters `discoveryLevel`, `discoveryTimeout`, and `discoveryDevices` which are displayed in the response body when the user starts LAN Automation using the LAN Automation Start V2 API.

Feature	Description

Devices APIs	• In this release, you can provide IPv6 addresses to assign the devices in the Assign Devices to Site API.
	• In the Export Device list API, the `password` parameter is now optional.
	• With this release, Catalyst Center platform supports the following changes in the response parameters of the Get Device Interfaces by specified range, Get Interface info by Id, Get Interface by IP, Get OSPF interfaces, Get ISIS interfaces, Get Interface by interface name, Get all interfaces, and Get Interface by Id APIs:
	  • The `addresses`, `lastOutgoingPacketTime`, `lastIncomingPacketTime`, `mtu`, and `name` response parameters are now included in the above APIs.
	  • The `poweroverethernet`, `networkdevice_id`, `managedNetworkElementUrl`, `managedNetworkElement`, `managedComputeElementUrl`, and `managedComputeElement` response parameters are now removed from the above APIs.

Network Settings API	In this release, a new `groupName` request query parameter is added in the Get Reserve IP Subpool API. The `siteId` parameter is now optional. **Note** When you omit the `siteId` parameter: • You must use the `ignoreInheritedGroups` parameter. • The maximum page size of the response is 1000 entries.
Deprecated APIs	
None	—
API Changes That Break Backward Compatibility	
None	—
New Events	
Assurance Events	Catalyst Center platform supports the following new Assurance events: • NETWORK-SDA-1-322: The event is generated when the Fabric Border loses connectivity with the Multicast RP in the virtual network. Unique issues are generated for each virtual network. • NETWORK-SDA-1-345: The event is generated when the Fabric Border loses connectivity with the Multicast RP in the virtual network. A single issue is generated for each pair of Border and RP.
System Notification Event	Catalyst Center platform supports the following new System Notification event: INTERNET-URL-ACCESS: This notification event is generated when any of the URLs listed in the Installation Guide that Catalyst Center tries to access is not reachable and impacts operations.

Feature	Description
New Reports	

Feature	Description
Audit Log Report	

Feature	Description

	This release supports a new **Audit Log** report type that provides detailed information about audits for a given time frame.
	• You can generate an **Audit Log** report based on the following criteria:
	  • Event Id
	  • Namespace
	  • Name
	  • Description
	  • Type
	  • Category
	  • Domain
	  • Sub Domain
	  • Severity
	  • Timestamp
	  • Details
	  • Note
	  • User
	  • Event Hierarchy
	  • Message
	  • Message Params
	  • Parent InstanceId
	  • Network
	  • Start Time
	  • Child Count
	• Supported report file formats are CSV and JSON.
	• In the **Setup Report Scope** window, you can sort the **Audit Log** report based on the following:
	  • Domain
	  • Category
	  • Time Range
	• In the **Schedule Report** window, you can define a date range and select a time zone to generate the report.
	• To access the **Audit Log** report, click the menu icon and choose **Reports** > **Reports**

Feature	Description
	Templates > **Audit Log**. For more information about the **Audit Log** report, see the *Cisco Catalyst Center Platform User Guide*.

Table 6: New and Changed Features in Catalyst Center Platform, Release 2.3.7.4

Feature	Description
New APIs	
User and Roles APIs	Catalyst Center platform supports the following User and Roles APIs: • POST <cluster-ip>/dna/system/api/v1/users/external-servers/aaa-attribute Add and update AAA Attribute API. • GET <cluster-ip>/dna/system/api/v1/users/external-servers/aaa-attribute Get AAA Attribute API. • DELETE <cluster-ip>/dna/system/api/v1/users/external-servers/aaa-attribute Delete AAA Attribute API. • POST <cluster-ip>/dna/system/api/v1/users/external-authentication Manage External Authentication Setting API. • GET <cluster-ip>/dna/system/api/v1/users/external-authentication Get External Authentication Setting API. To access the new User and Roles APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs** > **User and Roles**.
ITSM Integration API	Catalyst Center platform supports the following ITSM Integration API: GET <cluster-ip>/dna/intent/api/v1/integration-settings/status Fetches the ITSM integration status. To access the new ITSM Integration API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Integrations** drop-down list and choose **ITSM Integration**.
API Enhancements	
Devices API	In the Add User-Defined-Field to device API, the `value` request parameter is now a required attribute.
Discovery APIs	The request parameters of the Create Global Credentials V2 and Update Global Credentials V2 APIs, `httpRead.name` and `httpWrite.name`, are now changed to `httpRead.description` and `httpWrite.description`, respectively.
Deprecated APIs	

Feature	Description
Devices API	The Get Device Config for all devices API is deprecated.
New Events	
Assurance Events	Catalyst Center platform supports the following new Assurance events: • NETWORK-DEVICES-3-801: The event is generated to display the Assurance telemetry status. • NETWORK-APPLICATIONS-3-600: The event is generated when business-relevant applications are experiencing network latencies that are higher than normal.
EVPN Events	Catalyst Center platform supports the following new events for EVPN deployments: • NETWORK-FABRIC_WIRED-1-340: The event is generated when the BGP session is down between the fabric node and the spine role fabric node in the fabric site. • NETWORK-FABRIC_WIRED-1-342: The event is generated when the NVE peer is missing from a fabric node device in an EVPN protocol network. • NETWORK-FABRIC_WIRED-1-343: The event is generated when VNI(s) are down on the fabric node. **Note** In this release, the preceding events are applicable only to EVPN EFT users.
System Notification Events	Catalyst Center platform supports the following new System Notification events: • SYSTEM-APPLICATION-HEALTH-v1: The event is generated when there is any change in the health state of the applications registered for monitoring. • CISCO-TRUSTED-CERTIFICATE-BUNDLE-v1: The notification event is generated when a newer Cisco trusted certificate bundle is available.

New and Changed Features in Catalyst Center Automation

Table 7: New and Changed Features in Catalyst Center Automation, Release 2.3.7.5

Feature	Description
Enhancements in Displaying the MAC Address Details for APs	For APs, the MAC address details are now displayed under the **Base Radio MAC Address** column in the following workflows: • **Access Point Refresh** • **Configure Access Points** • **Configure RLAN** For APs, on the **Provision** > **Inventory** window: • The **MAC Address** column denotes the base radio MAC address. • The **AP Ethernet MAC Address** column is now available to view the Ethernet MAC address. • The device details display both the **Base Radio MAC Address** and **Ethernet MAC Address**.
Enhancements to the AP Refresh Workflow	The **Access Point Refresh** workflow now supports the following: • The Assurance use case where the new AP isn't provisioned after AP refresh and only the old configuration is copied to the new AP. **Note** If the new AP is onboarded through Plug and Play (PnP), the Assurance use case isn't supported. • A toggle button to enable the automatic detection of the new APs using SwitchPort. **Note** If the new AP is onboarded through PnP, automatic detection isn't supported.
Enhancements to Certificate Management UI	System Certificates, Trusted Certificates, and Device Certificates UI are modified to have a uniform layout.
Enhancements to Custom AP Groups and Flex Groups for Cisco AireOS Wireless Controller	Instead of configuring and applying the newly added custom groups to the APs during wireless controller provisioning, Catalyst Center now configures and applies them during AP provisioning. Effective with this release, you can use the same AP groups and flex groups across multiple sites for Cisco AireOS Wireless Controllers. **Note** • You can't use the same AP group on multiple sites with different SSIDs, RF profile, and SSID overrides. • You can't use the same flex group on multiple sites with different native VLAN or AAA override VLAN.

Feature	Description
Support for Displaying IOS CLI in Configuration Preview for Cisco Catalyst 9800 Series Wireless Controller	For Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.13.1 or later, you can generate IOS CLI from YANG configuration in the configuration preview.
Support for Standard Power Service	For APs with the standard power capability, compliance with FCC regulations requires the activation of Automatic Frequency Coordination (AFC). The **Standard Power Service** toggle button in the **Create Wireless Radio Frequency Profile** and **Create AI Radio Frequency Profile** window enables you to activate AFC for the 6-GHz band within an RF profile. **Note** This feature is applicable only for Cisco Catalyst 9800 Series Wireless Controllers. When you provision the corresponding APs, the **Summary** window displays the standard power service configuration details.
Upload Resource Utilization Details to CSSM: Change to Prerequisites	In earlier releases, to upload resource utilization details to CSSM, devices must have NETCONF enabled and devices must be added to the site. Effective with this release, devices don't have to have NETCONF enabled, and devices don't have to be added to the site.

Table 8: New and Changed Features in Catalyst Center Automation, Release 2.3.7.4

Feature	Description
Enhancements to AP Provisioning for N+1 High Availability	Effective with this release, if you are using N+1 High Availability (HA) and modify any nonflex SSIDs that are already provisioned on the primary and secondary controllers to flex SSIDs (or conversely), ensure that the states of WLANs are consistent across both the primary and secondary controllers on the corresponding site.
Enhancements to Custom Flex Profile Creation	A custom flex profile is created during Cisco Wireless Controller provisioning (with model configurations) or during AP provisioning (without model configurations). In both scenarios, the custom profile is configured with settings that are similar to the default flex profile, except for the Catalyst Center intent configurations. Catalyst Center also provides an option to autogenerate a flex profile name.
Enhancements to Default AP Profiles During Upgrade	In earlier releases, the default AP profile was pushed to the wireless controller during upgrade. When you upgrade to this release from an earlier version, by default, Catalyst Center doesn't push the default AP profile to the wireless controller. To update the default AP profile on the wireless controller, you must explicitly save it on the **Design** > **Network Settings** > **Wireless** > **AP Profiles** window. After you save the default AP profile, if there's a difference between the current wireless controller configuration and the AP profile configuration saved on Catalyst Center, the default AP profile is pushed to the wireless controller during subsequent reprovisioning.

Feature	Description
Enhancements to Preauthentication ACLs	Preauthentication Access Control Lists (ACLs) have the following enhancements: • The **Include auto rules** toggle button to enable or disable pushing the Catalyst Center-generated rules to the applicable SSIDs. • For **Walled Garden URLs**, a valid URL must have at least one period. Cisco AireOS Wireless Controllers don't support other special characters. Cisco Catalyst 9800 Series Wireless Controllers support the special characters . * - _.
Enhancements to VLAN ID Configuration for Wireless Interfaces	In earlier releases, the valid range for VLAN ID for wireless interfaces was from 0 through 4094. Effective with this release, the valid range for VLAN ID for wireless interfaces is from 1 through 4094. **Note** • For Cisco AireOS Wireless Controller, the valid range is from 1 through 4094. • For Cisco Catalyst 9800 Series Wireless Controllers, the valid range is from 2 through 4094.

New and Changed Features in Cisco Software-Defined Access

Table 9: New and Changed Features in Cisco Software-Defined Access, Release 2.3.7.5

Feature	Description
Enhancements to Port Configuration Within Fabric Sites	The **Port Assignment** tab for a fabric site now displays the authentication template configured for each port. If you don't configure the authentication template for an individual port, the port inherits these settings from the global authentication template configuration. Inherited settings are displayed with an inherit icon next to the setting.
SD-Access Compatibility Check	A device is added to the SD-Access fabric only if the device runs a software release that is compatible with the Catalyst Center release.
SD-Access Application Health Check	The health of SD-Access application is checked periodically and the status is displayed on the **System Health** page.

Table 10: New and Changed Features in Cisco Software-Defined Access, Release 2.3.7.4

Feature	Description
Enhancements to the Embedded Wireless Controller Image Installation for Switches	Following are the enhancements to the embedded wireless controller image installation process for switches: • The **Activate image on device** option is removed. • During the image import, you can exit the window, and view the progress of the import and schedule the installation later using the **Close** option. • After the image is imported, you can install it immediately or schedule the image installation for a later date or time. • You can check the status of image installation on the **Activities** > **Tasks** window.
Enhancements to Provisioning of Wireless Changes on Fabric Devices	If the wireless capability is enabled for a fabric device in the SD-Access device slide-in pane and there are changes in the wireless settings, you must click **Configure** in the slide-in pane to push the changes to the device. **Note** These enhancements are also applicable for the N+1 configurations.
Reconfiguration of Fabric for IP Address Pool Changes	When you modify the IP address pools that are used in a fabric, you must reconfigure the fabric. **Note** The IP address pool changes are not provisioned automatically.
Unsupported SD-Access Configuration Detection on Fabric Devices	Catalyst Center allows you to detect the unsupported SD-Access configurations on fabric devices using the **SD-Access Unsupported Configuration** compliance check. **Note** This feature is in beta.

New and Changed Features in Interactive Help

Feature	Description
New in 2.3.7.5	
New Walkthroughs	• Configure AI-Enhanced RRM • Create an AI RF Profile • Enable Cisco AI-Enhanced RRM • View AI-Enhanced RRM Dashboard
New in 2.3.7.4	
New Walkthroughs	Enable the Field Notices Trial

Deprecated Features

Starting in 2.3.7.5, Catalyst Center no longer integrates with vManage.

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.

We recommend that the client systems you use to log in to Catalyst Center be equipped with 64-bit operating systems and browsers.

Note For an upgrade to Catalyst Center 2.3.7.x, we recommend that you use Chrome, not Firefox.

Supported Hardware Appliances

Cisco delivers Catalyst Center in the form of a rack-mountable, physical appliance. The following versions of the Catalyst Center appliance are available:

- First generation
  - 44-core appliance: DN1-HW-APL
- 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)
  - 32-core promotional appliance: DN3-HW-APL-U (Cisco UCS C220 M6)
  - 56-core appliance: DN3-HW-APL-L (Cisco UCS C220 M6)
  - 56-core promotional appliance: DN3-HW-APL-L-U (Cisco UCS C220 M6)
  - 80-core appliance: DN3-HW-APL-XL (Cisco UCS C240 M6)
  - 80-core promotional appliance: DN3-HW-APL-XL-U (Cisco UCS C240 M6)

Statement of Volatility

For the statement of volatility for the physical appliances, see the *Statement of Volatility for Cisco USC Hardware*.

Supported Firmware

Cisco Integrated Management Controller (Cisco IMC) versions are independent from Catalyst Center releases. This release of Catalyst Center has been validated only against the following firmware:

- Cisco IMC Version 3.0(3f) and 4.1(2g) for appliance model DN1-HW-APL
- Cisco IMC Version 4.3(2.230270) for appliance model DN2-HW-APL*
- Cisco IMC Version 4.3(2.230270) for appliance model DN3-HW-APL*

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 “Typical 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.

Catalyst Center Scale

For Catalyst Center scale numbers, see the *Cisco Catalyst Center Data Sheet*.

IP Address and FQDN Firewall Requirements

To determine the IP addresses and fully qualified domain names (FQDNs) that must be made accessible to Catalyst Center through an existing network firewall, see "Required Internet URLs and Fully Qualified Domain Names" in the "Plan the Deployment" chapter of the *Cisco Catalyst Center Installation Guide*.

Product Telemetry

Telemetry data is collected by default in Catalyst Center, but you can opt out of some data collection. The data collection is designed to help the development of product features and address any operational issues, providing greater value and return on investment. Cisco collects these categories of data: Cisco.com ID, System, Feature Usage, Network Device Inventory, and License Entitlement. See the *Cisco Catalyst Center Data Sheet* for a more expansive list of data that we collect. To opt out of some of the data collection, contact your Cisco account representative or Cisco TAC.

Installing Catalyst Center

Install Catalyst Center as a dedicated physical appliance purchased from Cisco with the Catalyst Center ISO image preinstalled. See the *Cisco Catalyst Center Installation Guide* for information about installation and deployment procedures.

Note Certain applications, such as Group-Based Policy Analytics, are optional applications that are not installed on Catalyst Center by default. If you need any of the optional applications, you must manually download and install the packages separately.

For more information about downloading and installing a package, see "Manage Applications" in the *Cisco Catalyst Center Administrator Guide*.

Support for Cisco Connected Mobile Experiences

Catalyst Center supports Cisco Connected Mobile Experiences (CMX) Release 10.6.2 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.

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 the following limitations:

WCAG Success Criterion	Support	Limitation
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	—

Guidelines and Limitations

Cloud Connectivity Through SSL Intercept Guidelines

Some Catalyst Center applications, such as the Cisco AI Network Analytics agent on the Catalyst Center appliance, require establishing a secure communication to the cloud with mutual authentication, using X.509 certificates.

In addition to direct connectivity, use of a proxy is also supported, as long as the SSL communication is terminated directly at the agent and cloud endpoint, without any SSL interception device in between.

Note Cloud connection through an SSL intercept device is not supported and might result in connectivity failures.

Backup and Restore Guidelines

- You cannot take a backup of one version of Catalyst Center and restore it to another version of Catalyst Center. You can only restore a backup to an appliance that is running the same Catalyst Center software version, applications, and application versions as the appliance and applications from which the backup was taken.
- After performing a restore operation, update your integration of Cisco ISE with Catalyst Center. After a restore operation, Cisco ISE and Catalyst Center might not be in sync. To update your Cisco ISE integration with Catalyst Center, choose **System** > **Settings** > **Authentication and Policy Servers**. In the **Actions** column, click **Edit** adjacent to the corresponding server. Enter your Cisco ISE password to update.
- After performing a restore operation, the configuration of devices in the network might not be in sync with the restored database. In such a scenario, you should manually enter the CLI commands that are pushed for authentication, authorization, and accounting (AAA) and configuration on the network devices. See the corresponding network device documentation for information about the CLI commands to enter.
- Re-enter the device credentials in the restored database. If you updated the site-level credentials before the database restore, and the backup that is being restored doesn't have the credential change information, all the devices go to partial collection after the restore. You must then manually update the device credentials on the devices for synchronization with Catalyst Center, or perform a rediscovery of those devices to learn the device credentials.
- Perform AAA provisioning only after adjusting network device differential changes to the restored database. Otherwise, device lockouts might occur.
- You can back up and restore only Automation data or both Automation and Assurance data. You cannot use the GUI or the CLI to back up or restore only Assurance data.

AI-Enhanced RRM Guidelines

In earlier releases, Catalyst Center marked the AI-Enhanced RRM tasks as failed if the AP provisioning didn't complete within 3 hours. During scale provisioning for a large number of APs, provisioning can take a longer time. Even if the tasks were marked as failed after 3 hours, the AP provisioning continued in Catalyst Center.

Effective with Release 2.3.7.4, the timeout value for AI-Enhanced RRM tasks is increased to 24 hours to accommodate the scale provisioning scenarios for large number of APs.

Cisco ISE Integration Guidelines

- ECDSA keys are not supported as either SSH keys for Cisco ISE SSH access or in the certificates in Catalyst Center and Cisco ISE.
- Full certificate chains must be uploaded to Catalyst Center while replacing an existing certificate. If a Catalyst Center certificate is issued by a subCA of a rootCA, the certificate chain uploaded to Catalyst Center while replacing the Catalyst Center certificate must contain all three certificates.

- Self-signed certificates applied on Catalyst Center must have the Basic Constraints extension with cA:TRUE (RFC5280 section-4.2.19).
- The IP address or FQDN of both Cisco ISE and Catalyst Center must be present in either the **Subject Name** field or the **Subject Alt Name** field of the corresponding certificates.
- If a certificate is replaced or renewed in either Cisco ISE or Catalyst Center, trust must be re-established.
- The Catalyst Center and Cisco ISE IP address or FQDN must be present in the proxy exceptions list if there is a web proxy between Catalyst Center and Cisco ISE.
- Catalyst Center and Cisco ISE nodes cannot be behind a NAT device.
- Catalyst Center and Cisco ISE cannot be integrated if the ISE Admin and ISE pxGrid certificates are issued by different enterprise certificate authorities.

  Specifically, if the Cisco ISE Admin certificate is issued by *CA server A*, the Cisco ISE pxGrid certificate is issued by *CA server B*, and the pxGrid persona is running on a node other than Cisco ISE PPAN, the pxGrid session from Catalyst Center to Cisco ISE doesn't work.
- If pxGrid policies that restrict access to certain user groups subscribed to topics of Catalyst Center are present, the Catalyst Center client username must be manually readded to the user group whenever Catalyst Center reintegrates with Cisco ISE. This is because the association between the username and the user group is lost during the reintegration workflow on Catalyst Center. Currently, there is no way to associate a pxGrid client to a user group through a REST API call; this must be performed manually from the Cisco ISE GUI.

Device Onboarding Guidelines

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, we recommend that you boot the devices in install mode before onboarding them.

If you upgrade an onboarded IE3200 or IE3300 device to Cisco IOS XE 17.8.1 or later, ensure that the device is in install boot mode before upgrading.

Visibility and Control Guidelines

The Visibility and Control of Configurations feature does not cover out-of-band or event-based changes.

If you generate a configuration preview and then an out-of-band or event-based change occurs (such as a device role change, VIP change, or credential update), the configuration preview is based on the older device configuration.

Upgrade Limitation

In-Service Software Upgrade (ISSU) is not supported in Cisco SD-Access deployments.

In-Product Help Limitations

- The online help and Interactive Help support light mode only. The online help and Interactive Help do not 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.

License Limitations

- After changing the enterprise IP address or FQDN, before you attempt a licensing-related task, all services must be up and running.
- The Catalyst Center License Manager supports Smart Licensing only for wireless controller models that run Cisco IOS XE. The License Manager doesn't support Smart License registration of the Cisco 5500 Series AireOS Wireless Controller when the connection mode is smart proxy.
- The Catalyst Center License Manager doesn't support the following operations under **Actions** > **Manage License Reservation** for Cisco IOS 17.3.2 and later:
  - **Enable License Reservation**
  - **Update License Reservation**
  - **Cancel/Return License Reservation**
  - **Factory License Reservation**

Fabric Limitations

- IP address pools that are reserved at the area level are inherited at the building level under **Design** > **Network Settings** > **IP Address Pools**. However, these IP address pools are not listed in the **Host Onboarding** window if the fabric site is defined at the building level. If the fabric site is defined at the building level, you must reserve the IP address pools at the building level. If the fabric site is defined at the area level, you must reserve the IP address pools at the area level.

  To work around this issue, release and reserve the IP address pool at the same level (area or building) as the fabric site, or reconfigure the fabric site at the same level as the reserved IP address pool.
- Catalyst Center supports only native multicast across multiple fabric sites that are connected by an SD-Access transit. Head-end replication is not supported over SD-Access transit.
- Multicast routing over LISP/BGP SD-Access transit is not supported.
- Cisco Catalyst 9000 Series switches support MACsec switch-to-switch connections.

Note We do not recommend using MACsec between switch-to-host connections in an overlay network.

  For assistance with an existing switch-to-host MACSEC implementation or a design review, contact your Cisco Sales Representative or Channel Partner.
- If you manually remove an SD-Access fabric-related CLI from the switch, Catalyst Center may not apply the command during normal device provisioning. In such cases, you must manually add the command on the fabric node. Alternately, remove the device from the fabric, and then readd the device to the fabric.

Existing Feature-Related Limitations

- Catalyst Center cannot learn device credentials.
- You must enter the preshared key (PSK) or shared secret for the AAA server as a part of the import flow.

- Catalyst Center doesn't learn the details about DNS, WebAuth redirect URL, and syslog.
- Catalyst Center can learn device configuration only once per controller.
- Catalyst Center can learn only one wireless controller at a time.
- For site profile creation, only the AP groups with AP and SSID entries are considered.
- Automatic site assignment is not possible.
- SSIDs with an unsupported security type and radio policy are discarded.
- For authentication and accounting servers, if the RADIUS server is present in the device, it is given first preference. If the RADIUS server is not present, the TACACS server is considered for design.
- The Cisco ISE server (AAA) configuration cannot be learned through existing device provisioning.
- The authentication and accounting servers must have the same IP addresses for them to be learned through existing device provisioning.
- When an SSID is associated with different interfaces in different AP groups, during provisioning, the newly created AP group with the SSID is associated with the same interface.
- A wireless conflict is based only on the SSID name and doesn't consider other attributes.

High Availability Limitation

Catalyst Center doesn't support HA for the Cisco Embedded Wireless Controller on Catalyst Access Points.

Wireless Limitations

- If an AP is migrated after a wireless policy is created, you must manually edit the wireless policy and point the policy to an appropriate AP location before deploying the policy. Otherwise, the `Policy Deployment failed` message is displayed.
- Catalyst Center doesn't support the display of Bluetooth Low Energy (BLE) radios in wireless maps.
- Do not provision wireless devices (APs and wireless controllers) that are tagged with the INV_EVENT_SYNC_DISABLED tag. Because the INV_EVENT_SYNC_DISABLED tag blocks the synchronization operation based on events, provisioning wireless devices that have that tag can lead to inconsistent information in Catalyst Center.

AP Limitations

- Configuring APs in FlexConnect mode before provisioning the locally switched WLANs bypasses the AP provisioning error. Otherwise, AP provisioning fails when the locally switched WLANs are provisioned on the wireless controller or APs through Catalyst Center.

  After the provisioning failure, the AP rejoins the wireless controller. You can reprovision the AP for a successful provisioning.
- The Cisco Catalyst 9130AXE AP with antenna C-ANT9104 doesn't support the Disable option for Dual Radio mode.
- The Cisco Catalyst 9124AXE AP doesn't support the Auto option for Dual Radio mode.

- When only Link Layer Discovery Protocol (LLDP) is enabled between an AP and its directly connected upstream neighbor:
  - The **Tools** > **Topology** window doesn't display the directly connected neighbor link.
  - The **Inventory** table doesn't display the directly connected neighbor details.

Inter-Release Controller Mobility (IRCM) Limitation

The interface or VLAN configuration is not differentiated between foreign and anchor controllers. The VLAN or interface that is provided in Catalyst Center is configured on both foreign and anchor controllers.

IP Device Tracking Limitations

- With IPDT on trunk ports, rogue-on-wire detection is impacted. Catalyst Center doesn't show all the clients connected to a switch through an access point in bridge mode. The trunk port is used to exchange all the VLAN information. When you enable IP device tracking on the trunk port, clients connected on the neighbor switch are also shown. Catalyst Center doesn't collect client data if the connected interface is a trunk port and the neighbor is a switch. As a best practice, disable the IP device tracking on the trunk port. Rogue-on-wire is not detected if IP device tracking is enabled on the trunk port.
- When you add a line card to a chassis, or remove a line card from a chassis, the changes take several minutes to get updated on Catalyst Center. IPDT configurations, if any, are pushed to the device automatically for newly added interfaces.
- When you add a device to a stack pool, or remove a device from a stack pool, the changes take several minutes to get updated on Catalyst Center. IPDT configurations, if any, are pushed to the device automatically for newly added interfaces.

  To add or remove a device from the stack, you must use manual CLI configurations.

IPv6 Limitations

If you choose to run Catalyst Center in IPv6 mode:

- Access Control Application, Group-Based Policy Analytics, SD Access, and Cisco AI Endpoint Analytics packages are disabled and cannot be downloaded or installed.
- 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.

Cisco Plug and Play Limitations

- Virtual Switching System (VSS) is not supported.
- The Cisco Plug and Play mobile app is not supported with Plug and Play in Catalyst Center.
- The Stack License workflow task is supported for Cisco Catalyst 3650 and 3850 Series switches running Cisco IOS XE 16.7.1 and later.
- The Plug and Play agent on the switch is initiated on VLAN 1 by default. Most deployments recommend that VLAN 1 be disabled. If you do not want to use VLAN 1 when PnP starts, enter the following command on the upstream device:

  pnp startup-vlan *<vlan_number>*

Cisco Group-Based Policy Analytics Limitations

- Cisco Group-Based Policy Analytics supports up to five concurrent requests based on realistic customer data. While it is desirable for GUI operations to respond within 5 seconds or less, for extreme cases based on realistic data, it can take up to 20 seconds. There is no mechanism to prevent more than five simultaneous requests at a time, but if it does happen, it might cause some GUI operations to fail. Operations time out after 1 minute.
- Data aggregation occurs at hourly offsets from UTC in Cisco Group-Based Policy Analytics. However, some time zones are at a 30-minute or 45-minute offset from UTC. If the Catalyst Center server is located in a time zone with a 30-minute or 45-minute offset from UTC, and the client is located in a time zone with an hourly offset from UTC, or vice versa, the time ranges for data aggregation in Cisco Group-Based Policy Analytics are incorrect for the client.

  For example, assume that the Catalyst Center server is located in California PDT (UTC-7), where data aggregations occur at hourly offsets (8:00 a.m., 9:00 a.m., 10:00 a.m., and so on). When a client located in India IST (UTC+5.30) wants to see the data between 10:00 to 11:00 p.m. IST, which corresponds to the time range 9:30 to 10:30 a.m. PDT in California, no aggregations are seen.
- Group changes that occur within an hour are not captured. When an endpoint changes from one security group to another, Cisco Group-Based Policy Analytics is unaware of this change until the next hour.
- You cannot sort the Security Group and Stealthwatch Host Group columns in the **Search Results** window.
- You might see discrepancies in the information related to Network Access Device (including location) between Assurance and Cisco Group-Based Policy Analytics.

Application Telemetry Limitation

- With Catalyst Center, application telemetry is not supported for Cisco Catalyst 9500 Series Switches.
- When configuring application telemetry on a device, Catalyst Center might choose the wrong interface as the source for NetFlow data.

  To force Catalyst Center to choose a specific interface, add the **netflow-source** command in the description of the interface. You can use a special character followed by a space after **netflow-source** but not before it. For example, the following syntax is valid:

```
netflow-source
MANAGEMENT netflow-source
MANAGEMENTnetflow-source
netflow-source MANAGEMENT
```

```
netflow-sourceMANAGEMENT
netflow-source & MANAGEMENT
netflow-source |MANAGEMENT
```

The following syntax is invalid:

```
MANAGEMENT | netflow-source
* netflow-source
netflow-source|MANAGEMENT
```

IP Address Manager Limitations

- Infoblox limitations:
  - Infoblox doesn't expose a name attribute; therefore, the comment field in Infoblox is populated by the IP pool name during a sync.
  - For a pool import, the first 50 characters of the comment field are used. If there are spaces in the comments, they are replaced by underscores.
  - If an IP pool name is updated for an imported pool, the comments are overwritten and the new name is reflected.

- You may see the following error when editing an existing IPAM integration or when adding a new IPAM:

  ```
  NCIP10283: The remote server presented a certificate with an incorrect CN of the owner
  ```

  To correct this, regenerate a new certificate for IPAM and verify that any one of the following conditions are met:
  - No values are configured in the SAN field of the certificate.
  - If a value is configured, the value and type (IP address or FQDN) must match the configured URL under **System** > **Settings** > **External Services** > **IP Address Manager**.

- Catalyst Center supports integration with an external IPAM server that has trusted certificates. In the Catalyst Center GUI, under **System** > **Settings** > **External Services** > **IP Address Manager**, you may see the following error message:

  ```
  NCIP10282: Unable to find the valid certification path to the requested target.
  ```

  To correct this error for a self-signed certificate:

  1. Using OpenSSL, enter one of the following commands to download the self-signed certificate, depending on your IPAM type. (You can specify the FQDN [domain name] or IP address in the command.)
     - `openssl s_client -showcerts -connect Infoblox-FQDN:443`
     - `openssl s_client -showcerts -connect Bluecat-FQDN:443`
  2. From the output, use the content from ---BEGIN CERTIFICATE--- to ---END CERTIFICATE--- to create a new .pem file.
  3. Go to **System** > **Settings** > **Trust & Privacy** > **Trustpool**, click **Import**, and upload the certificate (.pem file).
  4. Go to **System** > **Settings** > **External Services** > **IP Address Manager** and configure the external IPAM server. (If the IPAM server is already configured, skip this step.)

To correct this error for a CA-signed certificate, install the root certificate and intermediate certificates of the CA that is installed on the IPAM, into the Catalyst Center trustpool (**System** > **Settings** > **Trust & Privacy** > **Trustpool**).

- You may see the following error if a CA-signed certificate is revoked by the certificate authority:

  ```
  NCIP10286: The remote server presented with a revoked certificate. Please verify the
  certificate.
  ```

  To correct this, obtain a new certificate from the certificate authority and upload it to **System** > **Settings** > **Trust & Privacy** > **Trustpool**.

- You may see the following error after configuring the external IPAM details:

  ```
  IPAM external sync failed:
  NCIP10264: Non Empty parent pool <CIDR> exists in external ipam.
  ```

  To correct this, do the following:

  1. Log in to the external IPAM server (such as BlueCat).
  2. Confirm that the parent pool CIDR exists in the external IPAM server, and remove all the child pools that are configured under that parent pool.
  3. Return to the Catalyst Center GUI and reconfigure the IPAM server under **System** > **Settings** > **External Services** > **IP Address Manager**.

- You may see the following error while using IP Address Manager to configure an external IPAM:

  ```
  NCIP10114: I/O error on GET request for "https://<IP>/wapi/v1.2/":
  Host name '<IP>' does not match the certificate subject provided by the peer
  (CN=www.infoblox.com, OU=Engineering, O=Infoblox, L=Sunnyvale, ST=California, C=US);
  nested exception is javax.net.ssl.SSLPeerUnverifiedException: Host name '<IP>'
  does not match the certificate subject provided by the peer (CN=www.infoblox.com,
  OU=Engineering,
  O=Infoblox, L=Sunnyvale, ST=California, C=US) |
  ```

  To correct this, do the following:

  1. Log in to the external IPAM server (such as Infoblox).
  2. Regenerate your external IPAM certificate with the common name (CN) value as the valid hostname or IP address. In the preceding example, the CN value is `www.infoblox.com`, which is not the valid hostname or IP address of the external IPAM.
  3. After you regenerate the certificate with a valid CN value, go to **System** > **Settings** > **Trust & Privacy** > **Trustpool**.
  4. Click **Import** and upload the new certificate (.pem file).
  5. Go to **System** > **Settings** > **External Services** > **IP Address Manager** and configure the external IPAM server with the server URL as the valid hostname or IP address (as listed as the CN value in the certificate).

Reports Limitation

Reports with significant data can sometimes fail to generate in the Catalyst Center platform. If this occurs, we recommend that you use filters to reduce the report size to prevent such failures.

Custom Application Limitation

If a custom application is configured as a part of the default bucket, Catalyst Center doesn't push the configuration to the managed devices.

Application Policy and Application Visibility Limitation

When you provision the Application Policy feature or the Application Visibility feature from Catalyst Center, changes made outside these features do not reflect automatically in Catalyst Center. For the changes to be reflected in Catalyst Center, you must reprovision these features.

Third-Party Device Support Limitations

Note the following points regarding Catalyst Center's support of third-party devices:

- Third-party devices are defined as non-Cisco devices that support MIB-II (RFC 1213) and can be added to Catalyst Center.
- Cisco will not issue any new entitlements for third-party devices.
- Cisco will not update its General Terms for third-party devices.
- Third-party devices added to Catalyst Center have limited (visibility-only) functionality and are not supported by the Cisco TAC. If you encounter an issue with a third-party device, you'll need to contact its vendor or whoever you have a support contract with for assistance.

Bugs

Open Bugs

The following table lists the open bugs in Catalyst Center for this release.

Bug Identifier	Headline
CSCwh60044	SWIM upgrade fails with the error `NCSW32001`.
CSCwh67057	Unable to switch between tabs from Fabric Infrastructure to L2, L3, Anycast Gateway, and Port Assignment.
CSCwh70738	Wireless controller provisioning fails with the error `NCSP11051` on all fabric and nonfabric wireless controllers.
CSCwh86488	Catalyst Center is unable to verify the Stealthwatch certificate, even though the Stealthwatch certificate and Catalyst Center certificate are signed by the same CA and the root CA certificate is already imported in the trustpool.
CSCwh93547	Catalyst Center and Cisco ISE integration is broken, but OTT wireless controller and NF router provisioning still works.

Bug Identifier	Headline
CSCwh94671	Manual failover to the disaster recovery site fails due to the following BGP VIP advertisement: `"Failed to do a failover. Reason: [{'name': 'Start Bgp Vip Advertisement Task', 'status': ['Failed to start DR VIP advertisement. Reason: 10.14.0.105/32 VIP is not configured on same interface as 10.14.20.106 to advertise, Error while Validating VIP Advertisement payload']}]"`
CSCwi01450	In a disaster recovery environment with multiple Catalyst Center clusters, both the active and passive disaster recovery clusters are shown in Author mode.
CSCwi03241	When you create a Central Web Authentication (CWA) guest SSID or enterprise SSID with posture enabled: • The preauthentication access control list (ACL) returned by Cisco ISE isn't mapped to the WLAN on the wireless controller. • The Layer 3 web policy is set as open on the wireless controller.
CSCwi28581	The network profile contains duplicate templates if multiple device series are added to the template.
CSCwi31665	When IE3x00 (IE3100, 3200, 3300, and 3400) devices are enabled with the PROFINET feature, Catalyst Center fails to recognize the IE3x00 devices as Cisco devices. Instead, Catalyst Center lists them incorrectly as third-party devices in the Inventory window, and the IE3x00 devices cannot be managed by Catalyst Center.
CSCwi37770	Enhance the custom view table settings columns to arrange them alphabetically.
CSCwi44683	Include reachability as a factor for iperf sensor selection.
CSCwi45597	The DHCP address is updated in three out of five segments during Layer 2 handoff.
CSCwi46523	After upgrading to Catalyst Center 2.3.7.4, disaster recovery rejoin fails with the error `SODR10140`.
CSCwi47048	Under **System** > **Settings** > **System Certificates**, the **Disaster Recovery** tab displays a "No expiry date" error.
CSCwi47693	When Cisco ISE is in inactive state during the Catalyst Center upgrade, the eps and eaworker pods crash until Cisco ISE becomes active.
CSCwi47934	Although automatic disaster recovery failover works after shutting down the active cluster, when the shut-down cluster is powered on and becomes standby (passive), the rejoin operation to make it standby (active) fails.
CSCwi51216	Extended node reprovisioning fails with the following error: `NCSO10008: Error in generating RFS due to internal error`
CSCwi53916	When you enter the **magctl sts status redis** command on the host machine, an error is returned.
CSCwi57988	New device onboarding to a nonfabric REP ring fails when image upgrade is part of the Plug and Play (PnP) process.

Bug Identifier	Headline
CSCwi72839	In IPv6-only networks, telemetry doesn't work with FQDN-only certificates. This problem occurs in an IPv6-only network when Catalyst Center pushes its FQDN as a telemetry receiver that can't be resolved by the IOS-XE device. To work around this problem, you must add the IPv6 addresses to the alt_names section.
CSCwj11541	Performance degradation occurs while adding an edge node to the fabric.
CSCwj25876	When creating or editing an AP zone, the SSID selection gets cut off.

CSCwj27165	The wireless controller provisioning workflow generates the following error while loading the Flex configuration model configs:
	`Internal Server Error: An unexpected condition was encountered.`
	`Please try after the system is restored.`

CSCwj33450	Cisco Catalyst 9800 Series Wireless Controller device provisioning fails with the following error: `unable to push configs to the device <device_ip>`
CSCwj40948	Package download hangs while upgrading to Catalyst Center 2.3.7.5.
CSCwj45318	Network Issue Monitor and Enrichment for ITSM (ServiceNow) bundle Help button is not working. Contact Cisco TAC to apply a workaround.
CSCwj48236	After Webhook configuration, Catalyst Center is either not sending the alerts or is sending them incorrectly.
CSCwj49460	After disaster recovery failover, postgres ongoing data replication has stopped.
CSCwj60411	WLAN profile and policy profile is out of synch, causing provisioning failures.

Resolved Bugs

Catalyst Center 2.3.7.5

The following table lists the resolved bugs in Catalyst Center, Release 2.3.7.5.

Bug Identifier	Headline
CSCwd42565	Catalyst Center telemetry provision for AVC on wireless controller SSID disabled on failure
CSCwe68287	Software distribution on Cisco Catalyst 9800 Series Wireless Controller is not recognized if activation is skipped using SMU and APSP.
CSCwf30218	The workflow API_ENDPOINT_CREATE takes a long time to complete.
CSCwf86819	Catalyst Center started reporting SPF-service-down, could not retrieve compliance related device data.
CSCwh19272	Catalyst Center may initiate install commit for ISSU before staggered AP upgrade is completed.
CSCwh22030	Software image shows needs update even after successfully upgrading the software image on the device.
CSCwh23552	Software image activation failed while trying to upgrade the IOS-XE along with sub-package on wireless controller through Catalyst Center.

Bug Identifier	Headline
CSCwh56371	SWIM APSP activation is taking base image name instead of APSP image name.
CSCwh91534	Catalyst Center 2.3.3.7: Unable to generate inventory report with approximately100 device due to "BAPI Execution Failed" error.
CSCwh96306	Catalyst Center is generating reports without complete information.
CSCwi27239	Self-identifying antenna showing as 'Unsupported' in wireless maps.
CSCwi38620	Catalyst Center 2.3.5.4: SWIM task showing In Progress never fails or is completed.
CSCwi76666	The number of managed locations for a site is not changing after successful provisioning.
CSCwi79754	Cisco Catalyst 9800 Series Wireless Controller provisioning fails due to `UnmanagedDCS duplicateKeyException`.
CSCwi85506	Software image management fails for Catalyst 9600 StackWise virtual link due to connection timeout error.
CSCwj08940	Anchor wireless controller provisioning failed with error `NCWL13000`.

Catalyst Center 2.3.7.4

The following table lists the resolved bugs in Catalyst Center, Release 2.3.7.4.

Bug Identifier	Headline
CSCwe74245	After a disaster recovery failover, Controller-Based Application Recognition (CBAR) provisioning fails in specific scenarios for Cisco Catalyst 9800 controllers, Catalyst 9300 switches, and Catalyst 9400 switches that have wireless enabled on them.
CSCwf13940	Inventory Insights shows configuration mismatches for nonexistent uplinks.
CSCwf90631	Image distribution fails for Cisco Catalyst 2960 devices.
CSCwh28002	After successfully generating a report, Catalyst Center doesn't send the report to the configured webhook server.
CSCwh52366	The "Add SSID to IP Pool Mapping" API fails with the following error: `"bapiError": "Failed with error: SyntaxError: Invalid JSON: <json>:1:0 Expected json literal but found eof\n\n^",Expected json literal but found eof`
CSCwi00888	Multiple switch provisioning fails on a template with an implicit variable.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Related Documentation

We recommend that you read the following documents relating to Catalyst Center.

For This Type of Information...	See This Document...
Release information, including new features, limitations, and open and resolved bugs.	*Cisco Catalyst Center Release Notes*
Installation and configuration of Catalyst Center, including postinstallation tasks.	*Cisco Catalyst Center Installation Guide*
Upgrade information for your current release of Catalyst Center.	*Cisco Catalyst Center Upgrade Guide*
Use of the Catalyst Center GUI and its applications.	*Cisco Catalyst Center User Guide*
Configuration of user accounts, security certificates, authentication and password policies, and backup and restore.	*Cisco Catalyst Center Administrator Guide*
Security features, hardening, and best practices to ensure a secure deployment.	*Cisco Catalyst Center Security Best Practices Guide*
Supported devices, such as routers, switches, wireless APs, and software releases.	*Cisco Catalyst Center Compatibility Matrix*
Hardware and software support for Cisco SD-Access.	*Cisco SD-Access Compatibility Matrix*
Technical references and validated solutions.	*Cisco-Validated Solution Profiles*
Use of the Cisco Catalyst Assurance GUI.	*Cisco Catalyst Assurance User Guide*
Use of the Catalyst Center platform GUI and its applications.	*Cisco Catalyst Center Platform User Guide*

For This Type of Information...	See This Document...
Catalyst Center ITSM integration and Catalyst Center ITSM support.	*Cisco Catalyst Center ITSM Integration Guide*
Use of the Cisco Wide Area Bonjour Application GUI.	*Cisco Wide Area Bonjour Application User Guide*
Use of the Stealthwatch Security Analytics Service on Catalyst Center.	*Cisco Stealthwatch Analytics Service User Guide*
Use of Rogue and aWIPS functionality to monitor threats in Catalyst Center.	*Cisco Catalyst Center Rogue Management and aWIPS Application Quick Start Guide*