

Cisco Catalyst Center Platform User Guide, Release 2.3.7.x

First Published: 2023-12-20

Last Modified: 2026-03-06

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2023–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **New and Changed Information** 1

New and changed information 1

CHAPTER 2 **About Catalyst Center Platform** 99

Catalyst Center platform 99

Intent APIs 100

About events and notifications 100

CHAPTER 3 **Deploy Catalyst Center Platform** 101

Catalyst Center platform deployments 101

Installation of Catalyst Center Platform 101

Configure integration settings 102

API prerequisites 103

Supporting Role-Based Access Control 104

CHAPTER 4 **Platform Overview GUI** 107

Platform overview 107

Navigate through the platform GUI 107

CHAPTER 5 **Platform Manage GUI** 109

About manage 109

About bundles 109

Bundle features 110

Configure bundles: destination to receive events 111

Configure bundles: ServiceNow access settings 114

Configure bundles: CMDB data synchronization for ServiceNow 117

CHAPTER 6 **Configurations** 127

About configurations 127
Configure event settings 127
Configure General Settings: edit an instance 129
Configure General Settings: add an instance 131
Configure a webhook destination 133
Configure an email destination 134
Configure a syslog server destination 135
Configure a trap notification 136

CHAPTER 7 **Reports** 139

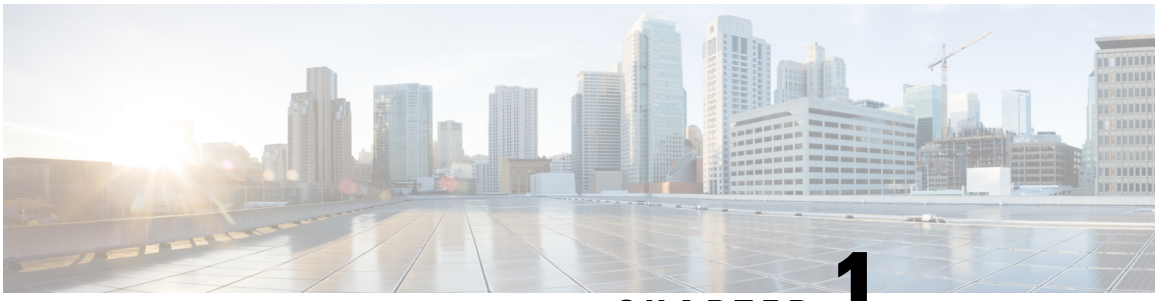
About reports 139
Run your first report 140
Run an access point report 143
Run an audit log report 146
Run a client report 149
Run a compliance report 152
Run a configuration archive report 155
Run an end-of-life report 157
Run an executive summary report 160
Run an inventory report 163
Run a licensing report 166
Run a network devices report 169
Run a rogue and aWIPS report 172
Run an ROI report 175
Run a security advisories report 177
Run a SWIM report 180
Generate a flexible report 183
View generated reports 187

CHAPTER 8 **Developer Toolkit GUI** 191

About developer toolkit 191
Work with APIs 191

Work with integration flows 193
Work with event notifications 195
Work with event notification simulations 198

CHAPTER 9 Runtime Dashboard 201
About Runtime Dashboard 201
Review the event summary 201
Retry an ITSM event 206
Review the API summary 208
Review the CMDB synchronization summary 209
Review the integration flow summary 211



CHAPTER 1

New and Changed Information

• New and changed information, on page 1

New and changed information

Table 1: New and changed features in Catalyst Center platform 2.3.7.10

Feature	Description
New APIs	
None	—
API Enhancements	
Devices APIs	With this release, the reachabilityHealthStatus parameter is included as an optional attribute in the response of the given devices APIs: • Get the device data for the given device id (Uuid). • Gets the list of network devices based on the provided complex filters and aggregation functions. • Gets the network device details based on the provided query parameters.
Network Settings API	With this release, the configureDevice attribute is added as a query parameter in the Sync network devices credential API.
Deprecated APIs	
None	—
API Changes That Break Backward Compatibility	
None	—

Table 2: New and changed features in Catalyst Center platform 2.3.7.9

Feature	Description	Where documented
Inventory Report	This Catalyst Center platform release supports a new **Inventory** report template called **All Data Version 2.0**. This new all data view provides detailed information about network devices, distribution of devices over time, device count by site, device count by device type, device count by software version and device count by fabric role, more efficiently.	For more information, see: • Run an inventory report, on page 163. • **New Report Template** in the Cisco Catalyst Center Release Notes.
New APIs		
Applications APIs	Catalyst Center platform supports the following Applications APIs: • GET <cluster-ip>/dna/data/api/v1/networkApplications Retrieves the list of network applications along with experience and health metrics. • GET <cluster-ip>/dna/data/api/v1/networkApplications/count Retrieves the total count of network applications by applying basic filtering. • POST <cluster-ip>/dna/data/api/v1/networkApplications/trendAnalytics Retrieves the Trend analytics data related to network applications. To access the new Applications APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Applications**.	

Feature	Description	Where documented
Application Policy APIs	Catalyst Center platform supports the following Application Policy APIs: • GET <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices Retrieve the list of network devices with their application visibility status. • GET <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/count Retrieve the count of network devices for the given application visibility status filters. • POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/enableAppTelemetry Enable application telemetry feature on multiple network devices. • POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/disableAppTelemetry Disable application telemetry feature on multiple network devices. • POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/enableCbar Enable CBAR feature on multiple network devices. • POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/disableCbar Disable CBAR feature on multiple network devices. • GET <cluster-ip>/dna/intent/api/v1/qosPolicySetting Retrieves the application QoS policy setting. • PUT <cluster-ip>/dna/intent/api/v1/qosPolicySetting Updates the application QoS policy setting. To access the new Application Policy APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Policy** drop-down list and choose **Application Policy**.	

Feature	Description	Where documented
Cisco Integrated Management Controller (IMC) APIs	Catalyst Center platform supports the following Cisco IMC APIs: • GET <cluster-ip>/dna/system/api/v1/ciscoImcs Retrieves Cisco IMC configurations for Catalyst Center nodes. • POST <cluster-ip>/dna/system/api/v1/ciscoImcs Adds Cisco IMC configuration to a Catalyst Center node. • GET <cluster-ip>/dna/system/api/v1/ciscoImcs/${id} Retrieves the Cisco IMC configuration for a Catalyst Center node. • PUT <cluster-ip>/dna/system/api/v1/ciscoImcs/${id} Updates the Cisco IMC configuration for a Catalyst Center node. • DELETE <cluster-ip>/dna/system/api/v1/ciscoImcs/${id} Deletes the Cisco IMC configurations for a Catalyst Center node. To access the new Cisco IMC APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Appliance** drop-down list and choose **Cisco IMC**.	

Feature	Description	Where documented
Compliance APIs		

Feature	Description	Where documented
	Catalyst Center platform supports the following Compliance APIs: • POST <cluster-ip>/dna/intent/api/v1/networkBugs/trials Creates a trial for bugs detection on network devices. • GET <cluster-ip>/dna/intent/api/v1/networkBugs/trials Get trial details for bugs detection on network devices. • POST <cluster-ip>/dna/intent/api/v1/networkBugs/triggerScan Triggers a bugs scan for the supported network devices. • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices/${networkDeviceId}/bugs/count Get count of bugs affecting the network device. • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices/${networkDeviceId}/bugs Get bugs affecting the network device. • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/bugs/${id} Get network bug by ID. • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/bugs/${id}/networkDevices/count Get count of network bug devices for the bug. • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/bugs/${id}/networkDevices Get network bug devices for the bug. • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/bugs/${id}/networkDevices/${networkDeviceId} Get network bug device for the bug by network device ID. • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices/count Get count of network bug devices. • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices Get network bug devices. • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices/${networkDeviceId} Get network bug device by device ID. • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices/${networkDeviceId}/bugs/count Get count of bugs affecting the network device. • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices/${networkDeviceId}/bugs Get bugs affecting the network device. • GET	

Feature	Description	Where documented
	<cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices/${networkDeviceId}/bugs/${id} Get bug affecting the network device by device ID and bug ID. • GET <cluster-ip>/dna/intent/api/v1/networkBugs/resultsTrend/count Get count of network bugs results trend over time. • GET <cluster-ip>/dna/intent/api/v1/networkBugs/resultsTrend Get network bugs results trend over time. • POST <cluster-ip>/dna/intent/api/v1/fieldNotices/trials Creates a trial for field notices detection on network devices. • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/trials Get trial details for field notices detection on network devices. • POST <cluster-ip>/dna/intent/api/v1/fieldNotices/triggerScan Triggers a field notices scan for the supported network devices. • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices/${networkDeviceId}/notices/count Get count of field notices affecting the network device. • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices/${networkDeviceId}/notices Get field notices affecting the network device. • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/notices/${id} Get field notice affecting the network devices by ID. • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/notices/${id}/networkDevices/count Get count of field notice network devices for the notice. • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/notices/${id}/networkDevices Get field notice network devices for the notice. • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/notices/${id}/networkDevices/${networkDeviceId} Get field notice network device for the notice by network device ID. • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices/count Get count of field notice network devices. • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices Get field notice network devices. • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices/${networkDeviceId} Get field notice network device by device ID.	

Feature	Description	Where documented
	• GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices/${networkDeviceId}/notices/count Get count of field notices affecting the network device. • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices/${networkDeviceId}/notices Get field notices affecting the network device. • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices/${networkDeviceId}/notices/${id} Get field notice affecting the network device by device ID and notice ID. • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/resultsTrend/count Get count of field notices results trend over time. • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/resultsTrend Get field notices results trend over time. • POST <cluster-ip>/dna/intent/api/v1/securityAdvisories/trials Creates a trial for security advisories detection on network devices. • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/trials Get trial details for security advisories detection on network devices. • POST <cluster-ip>/dna/intent/api/v1/securityAdvisories/triggerScan Triggers a security advisories scan for the supported network devices. • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/advisories/count Get count of security advisories affecting the network devices. • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/advisories Get security advisories affecting the network devices. • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/advisories/${id} Get security advisory affecting the network devices by ID. • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/advisories/${id}/networkDevices/count Get count of security advisory network devices for the security advisory. • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/advisories/${id}/networkDevices Get security advisory network devices for the security advisory. • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/advisories/${id}/networkDevices/${networkDeviceId} Get security advisory network device for the security advisory by network device ID. • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/networkDevices/count Get count of security advisory network devices.	

Feature	Description	Where documented
	• GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/networkDevices Get security advisory network devices. • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/networkDevices/${networkDeviceId} Get security advisory network device by network device ID. • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/networkDevices/${networkDeviceId}/advisories/count Get count of security advisories affecting the network device. • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/networkDevices/${networkDeviceId}/advisories Get security advisories affecting the network device. • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/networkDevices/${networkDeviceId}/advisories/${id} Get security advisory affecting the network device by device ID and advisory ID. • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/resultsTrend/count Get count of security advisories results trend over time. • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/resultsTrend Get security advisories results trend over time. To access the new Compliance APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Compliance**.	

Feature	Description	Where documented
Configuration Archive APIs	Catalyst Center platform supports the following Configuration Archive APIs: • GET <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles Get Network Device Configuration File Details. • GET <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/count Count of Network Device Configuration Files. • GET <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/${id} Get Configuration File Details by ID. • POST <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/${id}/downloadMasked Download masked device configuration. • POST <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/${id}/downloadUnmasked Download Unmasked (raw) Device Configuration as ZIP. To access the new Configuration Templates APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Configuration Archive APIs**.	

Feature	Description	Where documented
Configuration Templates APIs		

Feature	Description	Where documented
	Catalyst Center platform supports the following Configuration Templates APIs: • GET <cluster-ip>/dna/intent/api/v1/templates/${templateId}/networkProfilesForSites Retrieve the network profiles attached to a CLI template. • GET <cluster-ip>/dna/intent/api/v1/templates/${templateId}/networkProfilesForSites/count Retrieve count of network profiles attached to a CLI template. • POST <cluster-ip>/dna/intent/api/v1/templates/${templateId}/networkProfilesForSites Attach network profile to a Day-N CLI template. • POST <cluster-ip>/dna/intent/api/v1/templates/${templateId}/networkProfilesForSites/bulk Attach a list of network profiles to a Day-N CLI template. • DELETE <cluster-ip>/dna/intent/api/v1/templates/${templateId}/networkProfilesForSites/bulk Detach a list of network profiles from a Day-N CLI template. • DELETE <cluster-ip>/dna/intent/api/v1/templates/${templateId}/networkProfilesForSites/${profileId} Detach a network profiles from a Day-N CLI template. • GET <cluster-ip>/templates/${templateId}/versions Get Template Versions. • GET <cluster-ip>/dna/intent/api/v1/templates/${templateId}/versions/${versionId} Get Template Version. • GET <cluster-ip>/dna/intent/api/v1/templates/${templateId}/versions/count Get Template Versions Count. • POST <cluster-ip>/dna/intent/api/v1/templates/${templateId}/versions/commit Commit Template For a New Version. • GET <cluster-ip>/dna/intent/api/v1/projects Get Template Projects. • POST <cluster-ip>/dna/intent/api/v1/projects Create Template Project. • PUT <cluster-ip>/dna/intent/api/v1/projects/${projectId} Update Template Project. • GET <cluster-ip>/dna/intent/api/v1/projects/${projectId} Get Template Project. • DELETE <cluster-ip>/dna/intent/api/v1/projects/${projectId} Delete Template Project. • GET <cluster-ip>/dna/intent/api/v1/projects/count	

Feature	Description	Where documented
	Get Template Project Count. To access the new Configuration Templates APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Configuration Templates APIs**.	

Feature	Description	Where documented
Devices APIs		

Feature	Description	Where documented
	Catalyst Center platform supports the following Devices APIs: • POST <cluster-ip>/dna/intent/api/v1/networkDevices/deleteWithoutCleanup Delete a network device without configuration cleanup. • POST <cluster-ip>/dna/intent/api/v1/networkDevices/deleteWithCleanup Delete network device with configuration cleanup. • GET <cluster-ip>/dna/data/api/v1/aaaServices Retrieves the list of AAA Services for given parameters. • GET <cluster-ip>/dna/data/api/v1/aaaServices/count Retrieves the total number of AAA Services for given parameters. • GET <cluster-ip>/dna/data/api/v1/aaaServices/${id} Retrieves the details of a specific AAA Service matching the id of the Service. • POST <cluster-ip>/dna/data/api/v1/aaaServices/query Retrieves the list of AAA Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/aaaServices/query/count Retrieves the total number of AAA Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/aaaServices/summaryAnalytics Get summary analytics data of AAA Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/aaaServices/topNAnalytics Get Top N analytics data of AAA Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/aaaServices/trendAnalytics Get trend analytics data of AAA Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/aaaServices/${id}/trendAnalytics Get trend analytics data for a given AAA Service matching the ID of the Service. • GET <cluster-ip>/dna/data/api/v1/dhcpServices Retrieves the list of DHCP Services for given parameters. • GET <cluster-ip>/dna/data/api/v1/dhcpServices/count Retrieves the total number of DHCP Services for given parameters. • GET <cluster-ip>/dna/data/api/v1/dhcpServices/${id} Retrieves the details of a specific DHCP Service matching the ID of the Service. • POST <cluster-ip>/dna/data/api/v1/dhcpServices/query Retrieves the list of DHCP Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/dhcpServices/query/count	

Feature	Description	Where documented
	Retrieves the total number of DHCP Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/dhcpServices/summaryAnalytics Get summary analytics data of DHCP Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/dhcpServices/topNAnalytics Get Top N analytics data of DHCP Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/dhcpServices/trendAnalytics Get trend analytics data of DHCP Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/dhcpServices/${id}/trendAnalytics Get trend analytics data for a given DHCP Service matching the ID of the Service. • GET <cluster-ip>/dna/data/api/v1/dnsServices Retrieves the list of DNS Services for given parameters. • GET <cluster-ip>/dna/data/api/v1/dnsServices/count Retrieves the total number of DNS Services for given parameters. • GET <cluster-ip>/dna/data/api/v1/dnsServices/${id} Retrieves the details of a specific DNS Service matching the ID of the Service. • POST <cluster-ip>/dna/data/api/v1/dnsServices/query Retrieves the list of DNS Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/dnsServices/query/count Retrieves the total number of DNS Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/dnsServices/summaryAnalytics Get summary analytics data of DNS Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/dnsServices/topNAnalytics Get Top N analytics data of DHCP Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/dnsServices/trendAnalytics Get trend analytics data of DNS Services for given set of complex filters. • POST <cluster-ip>/dna/data/api/v1/dnsServices/${id}/trendAnalytics Get trend analytics data for a given DNS Service matching the ID of the Service. • GET <cluster-ip>/dna/intent/api/v1/networkDeviceMaintenanceSchedules Retrieve scheduled maintenance windows for network devices. • POST <cluster-ip>/dna/intent/api/v1/networkDeviceMaintenanceSchedules Create maintenance schedule for network devices.	

Feature	Description	Where documented
	• GET <cluster-ip>/dna/intent/api/v1/networkDeviceMaintenanceSchedules/count Retrieve the total number of scheduled maintenance windows. • GET <cluster-ip>/dna/intent/api/v1/networkDeviceMaintenanceSchedules/${id} Retrieves the maintenance schedule information. • PUT <cluster-ip>/dna/intent/api/v1/networkDeviceMaintenanceSchedules/${id} Updates the maintenance schedule information. • DELETE <cluster-ip>/dna/intent/api/v1/networkDeviceMaintenanceSchedules/${id} Delete maintenance schedule. • GET <cluster-ip>/dna/intent/api/v1/networkDevices Retrieve network devices. • GET <cluster-ip>/dna/intent/api/v1/networkDevices/${id} Get details of a single network device. • GET <cluster-ip>/dna/intent/api/v1/networkDevices/count Count the number of network devices. • POST <cluster-ip>/dna/intent/api/v1/networkDevices/query Query network devices with filters. • POST <cluster-ip>/dna/intent/api/v1/networkDevices/query/count Count the number of network devices with filters. • POST <cluster-ip>/dna/data/api/v1/networkDevices/topNAnalytics Gets the Top-N analytics data related to network devices. • POST <cluster-ip>/dna/data/api/v1/interfaces/${id}/trendAnalytics The trend analytics data for the interfaces in the specified time range. To access the new Devices APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Devices**.	

Feature	Description	Where documented
Device Replacement APIs	Catalyst Center platform supports the following Device Replacement APIs: • GET <cluster-ip>/dna/intent/api/v1/networkDeviceReplacements/${id} Retrieve the status of device replacement workflow that replaces a faulty device with a replacement device. • GET <cluster-ip>/dna/intent/api/v1/networkDeviceReplacements Retrieve the status of all the device replacement workflows. To access the new Device Replacement APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Device Replacement**.	
Fabric Wireless APIs	Catalyst Center platform supports the following Fabric Wireless APIs: • GET <cluster-ip>/dna/intent/api/v1/sda/fabrics/${fabricId}/switchWirelessSetting Get SDA Wireless details from switches. • PUT <cluster-ip>//dna/intent/api/v1/sda/fabrics/${fabricId}/wirelessMulticast Update SDA Wireless Multicast. • GET <cluster-ip>/dna/intent/api/v1/sda/fabrics/${fabricId}/wirelessMulticast Get SDA Wireless Multicast. • PUT <cluster-ip>/dna/intent/api/v1/sda/fabrics/${fabricId}/switchWirelessSetting Switch Wireless Setting and Rolling AP Upgrade Management. • POST <cluster-ip>//dna/intent/api/v1/sda/fabrics/${fabricId}/switchWirelessSetting/reload Reload Switch for Wireless Controller Cleanup. To access the new Fabric Wireless APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Connectivity** drop-down list and choose **Fabric Wireless**.	
Health and Performance APIs	Catalyst Center platform supports the following Health and Performance APIs: • GET <cluster-ip>/dna/intent/api/v1/diagnosticTasks/${id} Retrieves diagnostic task by ID. • GET <cluster-ip>/dna/intent/api/v1/diagnosticTasks/${id}/detail Retrieves diagnostic task details by ID. To access the new Health and Performance APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **System** drop-down list and choose **Health and Performance**.	

Feature	Description	Where documented
Licenses APIs	Catalyst Center platform supports the following Licenses APIs: • GET <cluster-ip>/dna/intent/api/v1/connectionModeSetting Retrieves CSSM connection mode. • PUT <cluster-ip>/dna/intent/api/v1/connectionModeSetting Update CSSM connection mode. • GET <cluster-ip>/dna/system/api/v1/license/status System licensing status. • POST <cluster-ip>/dna/system/api/v1/license/register Smart licensing registration. • POST <cluster-ip>/dna/system/api/v1/license/renew Smart licensing renew operation. • POST <cluster-ip>/dna/system/api/v1/license/deregister Smart licensing Deregistration. • GET <cluster-ip>/dna/system/api/v1/license/lastOperationStatus System licensing last operation status. To access the new Licenses APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Cisco DNA Center System** drop-down list and choose **Licenses**.	

Feature	Description	Where documented
Network Settings APIs		

Feature	Description	Where documented
	Catalyst Center platform supports the following Network Settings APIs: • GET <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/templates Retrieve CLI templates attached to a network profile. • GET <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/templates/count Retrieve count of CLI templates attached to a network profile. • GET <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools Retrieves global IP address pools. • POST <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools Create a global IP address pool. • GET <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools/${id} Retrieves a global IP address pool. • PUT <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools/${id} Updates a global IP address pool. • DELETE <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools/${id} Deletes a global IP address pool. • GET <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools/${globalIpAddressPoolId}/subpools Retrieves subpools IDs of a global IP address pool. • GET <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools/${globalIpAddressPoolId}/subpools/count Counts subpools of a global IP address pool. • GET <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools/count Counts global IP address pools. • GET <cluster-ip>/dna/intent/api/v1/ipam/siteIpAddressPools Retrieves IP address subpools. • POST <cluster-ip>/dna/intent/api/v1/ipam/siteIpAddressPools Reserve (create) IP address subpools. • GET <cluster-ip>/dna/intent/api/v1/ipam/siteIpAddressPools/${id} Retrieves an IP address subpool. • PUT <cluster-ip>/dna/intent/api/v1/ipam/siteIpAddressPools/{id} Updates an IP address subpool. • DELETE <cluster-ip>/dna/intent/api/v1/ipam/siteIpAddressPools/{id} Releases an IP address subpool.	

Feature	Description	Where documented
	• GET <cluster-ip>/dna/intent/api/v1/ipam/siteIpAddressPools/count Counts IP address subpools. To access the new Network Settings APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Network Settings**.	

Feature	Description	Where documented
SD-Access APIs		

Feature	Description	Where documented
	Catalyst Center platform supports the following SDA APIs: • GET <cluster-ip>/dna/intent/api/v1/sda/pendingFabricEvents Get Pending Fabric Events. • POST <cluster-ip>/dna/intent/api/v1/sda/pendingFabricEvents/apply Apply Pending Fabric Events. • GET <cluster-ip>/dna/data/api/v1/fabricSummary Read Fabric entity summary. • GET <cluster-ip>/dna/data/api/v1/fabricSiteHealthSummaries Read list of Fabric Sites with their health summary. • GET <cluster-ip>/dna/data/api/v1/fabricSiteHealthSummaries/${id} Read Fabric Sites with health summary from ID. • GET <cluster-ip>/dna/data/api/v1/fabricSiteHealthSummaries/${id}/trendAnalytics The Trend analytics data for a fabric site in the specified time range. • GET <cluster-ip> /dna/data/api/v1/fabricSiteHealthSummaries/count Read fabric site count. • GET <cluster-ip> //dna/data/api/v1/virtualNetworkHealthSummaries Read list of Virtual Networks with their health summary. • GET <cluster-ip> /dna/data/api/v1/virtualNetworkHealthSummaries/${id} Read virtual network with its health summary from ID. • GET <cluster-ip> /dna/data/api/v1/virtualNetworkHealthSummaries/count Read Virtual Networks count. • GET <cluster-ip> /dna/data/api/v1/virtualNetworkHealthSummaries/${id}/trendAnalytics The Trend analytics data for a virtual network in the specified time range. • GET <cluster-ip> //dna/data/api/v1/transitNetworkHealthSummaries Read list of Transit Networks with their health summary. • GET <cluster-ip> /dna/data/api/v1/transitNetworkHealthSummaries/${id} Read transit network with its health summary from ID. • GET <cluster-ip> /dna/data/api/v1/transitNetworkHealthSummaries/count Read Transit Networks count. • GET <cluster-ip> /dna/data/api/v1/transitNetworkHealthSummaries/${id}/trendAnalytics The Trend analytics data for a transit network in the specified time range. To access the new SD-Access APIs, click the menu icon and choose **Platform** > **Developer Toolkit** >	

Feature	Description	Where documented
	APIs. Expand the **Connectivity** drop-down list and choose **SDA**.	

Feature	Description	Where documented
Sensor APIs		

Feature	Description	Where documented
	Catalyst Center platform supports the following Sensor APIs: • GET <cluster-ip>/dna/data/api/v1/icap/captureFiles Lists ICAP packet capture files matching specified criteria. • GET <cluster-ip>/dna/data/api/v1/icap/captureFiles/count Retrieves the total number of packet capture files matching specified criteria. • GET <cluster-ip>/dna/data/api/v1/icap/captureFiles/${id} Retrieves details of a specific ICAP packet capture file. • GET <cluster-ip>/dna/data/api/v1/icap/captureFiles/${id}/download Downloads a specific ICAP packet capture file. • GET <cluster-ip>/dna/data/api/v1/icap/spectrumSensorReports Retrieves the spectrum sensor reports sent by WLC for provided AP Mac. • GET <cluster-ip>/dna/data/api/v1/icap/spectrumInterferenceDeviceReports Retrieves the spectrum interference devices reports sent by WLC for provided AP Mac. • POST <cluster-ip>/dna/data/api/v1/icap/clients/${id}/stats Retrieves specific client statistics over specified period of time. • POST <cluster-ip>/dna/data/api/v1/icap/radios/${id}/stats Retrieves specific radio statistics over specified period of time. • POST <cluster-ip>/dna/intent/api/v1/icapSettings/deploy Deploys the given ICAP configuration intent without preview and approve. • POST <cluster-ip>/dna/intent/api/v1/icapSettings/deploy/${id}/deleteDeploy Remove the ICAP configuration on the device without preview. • POST <cluster-ip>/dna/intent/api/v1/icapSettings/configurationModels Creates an ICAP configuration intent for preview-approve. • POST <cluster-ip>/dna/intent/api/v1/icapSettings/configurationModels/${id}/deleteDeploy Creates a ICAP configuration workflow for ICAP intent to remove the ICAP configuration on the device. • GET <cluster-ip>/dna/intent/api/v1/icapSettings/configurationModels/${previewActivityId}/networkDeviceStatusDetails Get ICAP configuration status per network device. • POST <cluster-ip>/dna/intent/api/v1/icapSettings/configurationModels/${previewActivityId}/networkDevices/${networkDeviceId}/config Generates the device's CLIs of the ICAP configuration intent. • GET	

Feature	Description	Where documented
	<cluster-ip>/dna/intent/api/v1/icapSettings/configurationModels/${previewActivityId}/networkDevices/${networkDeviceId}/config Retrieves the device's CLIs of the ICAP intent. • DELETE <cluster-ip>/dna/intent/api/v1/icapSettings/configurationModels/${previewActivityId} Discards the ICAP configuration intent by activity ID. • DELETE <cluster-ip>/dna/intent/api/v1/icapSettings/configurationModels/${previewActivityId}/deploy Deploys the ICAP configuration intent by activity ID. • GET <cluster-ip>/dna/intent/api/v1/icapSettings/deviceDeployments Get device deployment status. • GET <cluster-ip>/dna/intent/api/v1/icapSettings/deviceDeployments/count Get device deployment status count. • GET <cluster-ip>/dna/intent/api/v1/icapSettings Retrieves deployed ICAP configurations while supporting basic filtering. • GET <cluster-ip>/dna/intent/api/v1/icapSettings/count Retrieves the count of deployed ICAP configurations while supporting basic filtering. To access the new Sensor APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Sensors**.	

Feature	Description	Where documented
Site Design APIs	Catalyst Center platform supports the following Site Design APIs: • GET <cluster-ip>/dna/intent/api/v2/floors/${floorId}/accessPointPositions Get Access Points positions. • GET <cluster-ip>/dna/intent/api/v2/floors/${floorId}/accessPointPositions/count Get Access Points positions count. • POST <cluster-ip>/dna/intent/api/v2/floors/${floorId}/accessPointPositions/bulkChange Edit the Access Points Positions. • POST <cluster-ip>/dna/intent/api/v2/floors/${floorId}/plannedAccessPointPositions/bulk Add Planned Access Points Positions. • POST <cluster-ip>/dna/intent/api/v2/floors/${floorId}/plannedAccessPointPositions/bulkChange Edit Planned Access Points Positions. • DELETE <cluster-ip>/dna/intent/api/v2/floors/${floorId}/plannedAccessPointPositions/${id} Delete Planned Access Points Position. • GET <cluster-ip>/dna/intent/api/v2/floors/${floorId}/plannedAccessPointPositions Get Planned Access Points Positions. • GET <cluster-ip>/dna/intent/api/v2/floors/${floorId}/plannedAccessPointPositions/count Get Planned Access Points Positions count. • POST <cluster-ip>/dna/intent/api/v2/floors/${floorId}/plannedAccessPointPositions/assignAccessPointPositions Assign Planned Access Points to operations ones. To access the new Site Design APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Site Design**.	

Feature	Description	Where documented
SWIM APIs	Catalyst Center platform supports the following SWIM APIs: • POST <cluster-ip>/dna/intent/api/v1/images/ccoSync Initiates sync of software images from Cisco.com. • GET <cluster-ip>dna/intent/api/v1/siteWiseImagesSummary Returns the image summary for the given site. • DELETE <cluster-ip>/dna/intent/api/v1/images/${id} Delete image. • POST <cluster-ip>/dna/intent/api/v1/images/${id}/sites/${siteId}/tagGolden Tagging golden image. • POST <cluster-ip>/dna/intent/api/v1/images/${id}/sites/${siteId}/untagGolden Untagging golden image. To access the new SWIM APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Software Image Management (SWIM)**.	
Tag APIs	Catalyst Center platform supports the following Tag APIs: • PUT <cluster-ip>/dna/intent/api/v1/tags/networkDevices/membersAssociations/bulk Update tags associated with the network devices. • PUT <cluster-ip>/dna/intent/api/v1/tags/interfaces/membersAssociations/bulk Update tags associated with the interfaces. To access the new Tag APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Operational Tasks** drop-down list and choose **Tag**.	

Feature	Description	Where documented
Task APIs	Catalyst Center platform supports the following Task APIs: • GET <cluster-ip>/dna/intent/api/v1/activities/${activityId}/triggeredJobs/count Retrieves the count of triggered jobs by activity ID. • GET <cluster-ip>/dna/intent/api/v1/activities Get activities. • GET <cluster-ip>/dna/intent/api/v1/activities/count Retrieves the count of activities. • GET <cluster-ip>/dna/intent/api/v1/activities/${id} Get activity by ID. • GET <cluster-ip>/dna/intent/api/v1/activities/${activityId}/triggeredJobs Get triggered jobs by activity ID. To access the new Task APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Operational Tasks** drop-down list and choose **Task**.	

Feature	Description	Where documented
Wireless APIs		

Feature	Description	Where documented
	Catalyst Center platform supports the following Wireless APIs: • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/anchorGroups Get Anchor Groups. • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/anchorGroups Create anchorGroup. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/anchorGroups/${id} Get AnchorGroup by ID. • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/anchorGroups/${id} Update AnchorGroup. • DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/anchorGroups/${id} Delete anchorGroup by ID. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/anchorGroups/count Get count of anchorGroups. • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/anchorCapableDevices Get Anchor capable devices. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/apAuthorizationLists Get AP Authorization Lists. • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/apAuthorizationLists Create AP Authorization List. • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/apAuthorizationLists/${id} Get AP Authorization List by ID. • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/apAuthorizationLists/${id} Update AP Authorization List. • DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/apAuthorizationLists/${id} Delete AP Authorization List. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/apAuthorizationLists/count Get AP Authorization List Count. • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/${networkDeviceId}/apAuthorizationLists Get AP Authorization List by network device ID. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/powerProfiles Get Power Profiles. • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/powerProfiles	

Feature	Description	Where documented
	Create Power Profile. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/powerProfiles/${id} Get Power Profile by ID. • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/powerProfiles/${id} Update Power Profile by ID. • DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/powerProfiles/${id} Delete Power Profile by ID. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/powerProfiles/count Get Power Profiles Count. • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/meshApNeighbours Get Mesh Ap Neighbours. • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/meshApNeighbours/count Get Mesh Ap Neighbours Count. • POST <cluster-ip>/dna/intent/api/v1/sites/${siteId}/wirelessSettings/ssids/${id}/update Update or override SSID. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/ssids/overrideAtSites Retrieve sites with overridden SSIDs. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles Get AP Profiles. • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles Create AP Profile. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles/${id} Get AP Profile by ID. • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles/${id} Update AP Profile by ID. • DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles/${id} Delete AP Profile by ID. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles/count Get AP Profiles Count. • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/siteTags Retrieve all Site Tags for a Wireless Profile.	

Feature	Description	Where documented
	• POST <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/siteTags/bulk Create multiple Site Tags for a Wireless Profile in bulk. • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/siteTags/${siteTagId} Retrieve a specific Site Tag for a Wireless Profile. • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/siteTags/${siteTagId} Update a specific Site Tag for a Wireless Profile. • DELETE <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/siteTags/${siteTagId} Delete a specific Site Tag from a Wireless Profile. • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/siteTags/count Retrieve the count of Site Tags for a Wireless Profile. • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/policyTags Retrieve all Policy Tags for a Wireless Profile. • POST <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/policyTags/bulk Create multiple Policy Tags for a Wireless Profile in bulk. • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/policyTags/${policyTagId} Retrieve a specific Policy Tag for a Wireless Profile. • PUT <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/policyTags/${policyTagId} Update a specific Policy Tag for a Wireless Profile. • DELETE <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/policyTags/${policyTagId} Delete a specific Policy Tag from a Wireless Profile. • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/policyTags/count Retrieve the count of Policy Tags for a Wireless Profile. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/${networkDeviceId}/assignAnchorManagedApLocations Assign Anchor Managed AP Locations For WLC. • GET <cluster-ip>/dna/intent/api/v1/wireless/accesspoint-configuration/count Get Access Point Configuration Count. To access the new Wireless APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Connectivity** drop-down list and choose **Wireless**.	
Beta APIs		

Feature	Description	Where documented
Wired APIs		

Feature	Description	Where documented
	With this release, Catalyst Center platform includes the following Campus Automation Beta APIs: • POST <cluster-ip>dna/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/configurationModels Create a configuration model for the intended configs for a wired device. • PUT <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2/${feature} Update configurations for an intended layer 2 feature on a wired device. • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/deployed/layer2/${feature} Get configurations for a deployed layer 2 feature on a wired device. • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/deployed/layer2/${feature}/count Get number of configurations for a deployed layer 2 feature on a device. • POST <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/deploy Deploy the intended configuration features on a wired device. • PUT <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2 Update configurations for intended layer 2 features on a wired device. • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/supported/layer2 Get the supported layer 2 features on a wired device. • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/serviceDeployments Get service deployment status. • POST <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/configurationModels/${previewActivityId}/config Generate the device config for the configuration model. • POST <cluster-ip>/dna/intent/api/v1/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/configurationModels/${previewActivityId}/deploy Deploys the configuration model on the network device. • DELETE <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2/${feature} Delete configurations for an intended layer 2 feature on a wired device. • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2/${feature} Get configurations for an intended layer 2 feature on a wired device.	

Feature	Description	Where documented
	• DELETE <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/configurationModels/${previewActivityId} Delete the configuration model. • POST <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2/${feature} Create configurations for an intended layer 2 feature on a wired device. • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2/${feature}/count Get number of configurations for an intended layer 2 feature on a wired device. • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/configurationModels/${previewActivityId}/config Gets the device config for the configuration model. • POST <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2 Create configurations for intended layer 2 features on a wired device. • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/deviceDeployments Get device deployment status. • GET <cluster-ip>/dna/intent/api/v1/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2 Get configurations for intended layer 2 features on a wired device. To access the Wired APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Connectivity** drop-down list and choose **Wired**.	
API Enhancements		
Compliance API	With this release, the `status` and `remediationSupported` properties are added in the request query parameter of the Compliance Details of Device API, and a new response parameter called `remediationSupported` is introduced.	
Devices APIs	The following Devices APIs now include the new response attributes `physicalPortCount` and `virtualPortCount`: • Get the device data for the given device id (Uuid). • Gets the Network Device details based on the provided query parameters. • Gets the list of Network Devices based on the provided complex filters and aggregation functions.	

<table>
<tr><th>Feature</th><th>Description</th><th>Where documented</th></tr>
<tr><td>SD-Access APIs</td><td colspan="2">• The Delete Port Channel API now includes the <code>PortchannelIds</code> and <code>connectedDeviceType</code> request parameters. The <code>networkDeviceId</code> parameter is now optional.
• With this release, a new request parameter called <code>isGlobalAuthenticationProfile</code> is added to the Get Authentication Profiles API.
• The <code>fabricId</code> request attribute is now optional in the Get Authentication Profiles and Update Authentication Profiles APIs.</td></tr>
<tr><td>Wireless APIs</td><td colspan="2">With this release:
• The <code>anchorGroupName</code>, <code>vlanGroupName</code>, <code>additionalInterfaces</code>, <code>apZones</code>, <code>apZoneName</code>, <code>rfProfileName</code> and <code>ssids</code> attributes are included in the Update Wireless Profile, Create Wireless Profile, Get Wireless Profiles and Get Wireless Profile by ID APIs.
• A new response parameter called <code>provisioningStatus</code> is included in the Get Access Point Configuration API.</td></tr>
<tr><td colspan="3">Deprecated APIs
A Sunset banner indicates that the particular API will be deprecated:
Note
If there is an alternative API, the details are given under the respective deprecated API's Features tab.</td></tr>
<tr><td>Discovery API</td><td colspan="2">With this release, the following Discovery API is marked as Sunset:
POST <cluster-ip>/dna/intent/api/v1/discovery
Delete all discovery.</td></tr>
<tr><td>Event Management APIs</td><td colspan="2">With this release, the following Event Management APIs are marked as Sunset and the corresponding new APIs are supported:</td></tr>
<tr><td></td><td>Deprecated APIs</td><td>New APIs</td></tr>
<tr><td></td><td>POST
<cluster-ip>/dna/intent/api/v1/event/subscription
Create Event Subscriptions.</td><td>POST
<cluster-ip>/dna/intent/api/v1/event/subscription/rest
Create Rest/Webhook Event Subscription.</td></tr>
<tr><td></td><td>PUT
<cluster-ip>/dna/intent/api/v1/event/subscription
Update Event Subscriptions.</td><td>PUT
<cluster-ip>/dna/intent/api/v1/event/subscription/rest
Update Rest/Webhook Event Subscriptions.</td></tr>
<tr><td></td><td>GET
<cluster-ip>/dna/intent/api/v1/event/subscription
Get Event Subscriptions.</td><td>GET
<cluster-ip>/dna/intent/api/v1/event/subscription/rest
Update Rest/Webhook Event Subscriptions.</td></tr>
</table>

Feature	Description	Where documented
Network Settings APIs	With this release, the following Network Settings APIs are deprecated: • POST <cluster-ip>/dna/intent/api/v1/global-pool Create Global Pool. • GET <cluster-ip>/dna/intent/api/v1/global-pool Get Global Pool. • PUT <cluster-ip>/dna/intent/api/v1/global-pool Update Global Pool. • DELETE <cluster-ip>/dna/intent/api/v1/global-pool/${id} Delete Global IP Pool. • POST <cluster-ip>/dna/intent/api/v1/reserve-ip-subpool/${siteId} Reserve IP Subpool. • GET <cluster-ip>/dna/intent/api/v1/reserve-ip-subpool Get Reserve IP Subpool. • PUT <cluster-ip>/dna/intent/api/v1/reserve-ip-subpool/${siteId} Update Reserve IP Subpool. • DELETE <cluster-ip>/dna/intent/api/v1/reserve-ip-subpool/${id} Release Reserve IP Subpool.	

Feature	Description	Where documented
SD-Access APIs		

Feature	Description	Where documented
	With this release, the following SD-Access business APIs are deprecated. Fabric Creation APIs • POST <cluster-ip>/dna/intent/api/v1/business/sda/fabric Add Fabric Site. • GET <cluster-ip>/dna/intent/api/v1/business/sda/fabric Get SDA Fabric Info. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/fabric Delete SDA Fabric. Fabric Site in SDA Fabric APIs • POST <cluster-ip>/dna/intent/api/v1/business/sda/fabric-site Add Site in SDA Fabric. • GET <cluster-ip>/dna/intent/api/v1/business/sda/fabric-site Get Site from SDA Fabric. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/fabric-site Delete Site from SDA Fabric. Fabric Zone in SDA fabric APIs • POST <cluster-ip>/dna/intent/api/v1/business/sda/fabric-zone Add fabric zone in SDA Fabric. • GET <cluster-ip>/dna/intent/api/v1/business/sda/fabric-zone Get fabric zone from SDA Fabric. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/fabric-zone Delete fabric zone from SDA Fabric. Control Plane Device APIs • POST <cluster-ip>/dna/intent/api/v1/business/sda/control-plane-device Add control plane device. • GET <cluster-ip>/dna/intent/api/v1/business/sda/control-plane-device Get control plane device. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/control-plane-device Delete control plane device in SDA Fabric. Edge-Device Role Assignment APIs • POST <cluster-ip>/dna/intent/api/v1/business/sda/edge-device	

Feature	Description	Where documented
	Add edge device. • GET <cluster-ip>/dna/intent/api/v1/business/sda/edge-device Get edge device. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/edge-device Delete edge device. Border Device Role Assignment APIs • POST <cluster-ip>/dna/intent/api/v1/business/sda/border-device Adds border device in SDA Fabric. • GET <cluster-ip>/dna/intent/api/v1/business/sda/border-device Gets border device detail from SDA Fabric. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/border-device Deletes border device from SDA Fabric. Default Authentication Template (Profile) APIs • PUT <cluster-ip>/dna/intent/api/v1/business/sda/authentication-profile Update default authentication profile. • POST <cluster-ip>/dna/intent/api/v1/business/sda/authentication-profile Add default authentication profile. • GET <cluster-ip>/dna/intent/api/v1/business/sda/authentication-profile Get default authentication profile. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/authentication-profile Delete default authentication profile. Virtual Network Creation APIs • POST <cluster-ip>/dna/intent/api/v1/business/sda/virtual-network Add VN in SDA Fabric. • GET <cluster-ip>/dna/intent/api/v1/business/sda/virtual-network Get VN from SDA Fabric. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/virtual-network Delete VN from SDA Fabric. • GET <cluster-ip>/dna/intent/api/v1/business/sda/virtual-network/summary Get Virtual Network Summary. SDA Segment APIs	

Feature	Description	Where documented
	• POST <cluster-ip>/dna/intent/api/v1/business/sda/virtualnetwork/ippool Add IP Pool in SDA Virtual Network. • GET <cluster-ip>/dna/intent/api/v1/business/sda/virtualnetwork/ippool Get IP Pool in SDA Virtual Network. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/virtualnetwork/ippool Delete IP Pool in SDA Virtual Network. Port Assignment for User Devices APIs • POST <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/user-device Add Port assignment for user device. • GET <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/user-device Get Port assignment for user device. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/user-device Delete Port assignment for user device. Port Assignment to Access Points APIs • POST <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/access-point Add Port assignment for access point. • GET <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/access-point Get Port assignment for access point. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/access-point Delete Port assignment for access point. SDA Multicast APIs • POST <cluster-ip>/dna/intent/api/v1/business/sda/multicast Add multicast. • GET <cluster-ip>/dna/intent/api/v1/business/sda/multicast Get multicast. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/multicast Delete multicast. Wired Device Provisioning APIs	

Feature	Description	Where documented
	• POST <cluster-ip>/dna/intent/api/v1/business/sda/provision-device Provision Wired Device. • GET <cluster-ip>/dna/intent/api/v1/business/sda/provision-device Get Provision Wired Device. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/provision-device Delete Provision Wired Device. • PUT <cluster-ip>/dna/intent/api/v1/business/sda/provision-device Re-Provision Wired Device. Virtual Network APIs • POST <cluster-ip>/dna/intent/api/v1/virtual-network Add virtual network with scalable groups. • GET <cluster-ip>/dna/intent/api/v1/virtual-network Get virtual network with scalable groups. • DELETE <cluster-ip>/dna/intent/api/v1/virtual-network Delete virtual network with scalable groups. • PUT <cluster-ip>/dna/intent/api/v1/virtual-network Update virtual network with scalable groups. Transit and Peer Networks APIs • POST <cluster-ip>/dna/intent/api/v1/business/sda/transit-peer-network Add Transit Peer Network. • GET <cluster-ip>/dna/intent/api/v1/business/sda/transit-peer-network Get Transit Peer Network. • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/transit-peer-network Delete Transit Peer Network. Retrieve Device Information from SDA fabric API • GET <cluster-ip>/dna/intent/api/v1/business/sda/device Get device info from SDA Fabric. Get SDA Device Role for a given device API • GET <cluster-ip>/dna/intent/api/v1/business/sda/device/role Get device role in SDA Fabric. Get Number of Fabric - Cyclops API	

Feature	Description	Where documented
	• GET <cluster-ip>/dna/intent/api/v1/business/sda/fabric/count Get SDA Fabric Count.	
Security Advisories APIs	With this release, the following Security Advisories APIs are marked as Sunset: • GET <cluster-ip>/dna/intent/api/v1/security-advisory/advisory/aggregate Get Advisories Summary. • GET <cluster-ip>/dna/intent/api/v1/security-advisory/device/${deviceId} Get Advisory Device Detail. • GET <cluster-ip>/dna/intent/api/v1/security-advisory/advisory Get Advisories List. • GET <cluster-ip>/dna/intent/api/v1/security-advisory/device/${deviceId}/advisory Get Advisories Per Device. • GET <cluster-ip>/dna/intent/api/v1/security-advisory/advisory/${advisoryId}/device Get Devices Per Advisory.	
SWIM APIs	With this release, the following SWIM APIs are marked as Sunset: • GET <cluster-ip>/dna/intent/api/v1/image/importation Get software image details. • GET <cluster-ip>/dna/intent/api/v1/image/importation/device-family-identifiers Get Device Family Identifiers. • POST <cluster-ip>/dna/intent/api/v1/image/importation/golden Tag as Golden Image. • GET <cluster-ip>/dna/intent/api/v1/image/importation/golden/site/${siteId}/family/${deviceFamilyIdentifier}/role/${deviceRole}/image/${imageId}/Swagger doc Get Golden Tag Status of an Image. • DELETE <cluster-ip>/dna/intent/api/v1/image/importation/golden/site/${siteId}/family/${deviceFamilyIdentifier}/role/${deviceRole}/image/${imageId} Remove Golden Tag for image.	
API Changes That Break Backward Compatibility		
None	—	

Table 3: New and changed features in Catalyst Center platform 2.3.7.6

Feature	Description
Name change to Catalyst Center app	The Cisco DNA Center app on the ServiceNow Store is rebranded as Catalyst Center from app version 2.3.1 onwards. The previous versions of the app are still called Cisco DNA Center. You can continue using those versions with the corresponding releases of Catalyst Center.
New APIs	
Cisco Trusted Certificates API	Catalyst Center platform supports the following Import Trusted Certificate API: • POST <cluster-ip>/dna/intent/api/v1/trustedCertificates/import Imports trusted certificate into a truststore. Accepts .pem or .der file as input. To access the new Import Trusted Certificate API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **System** drop-down list and choose **Cisco Trusted Certificates**.

Feature	Description
Clients API	Catalyst Center platform supports the following Clients API: • GET <cluster-ip>/dna/data/api/v1/clients Retrieves the list of clients, while also offering basic filtering and sorting capabilities. • GET <cluster-ip>/dna/data/api/v1/clients/${id} Retrieves specific client information matching the MAC address. • GET <cluster-ip>/dna/data/api/v1/clients/count Retrieves the total count of clients by applying basic filtering. • POST <cluster-ip>/dna/data/api/v1/clients/query Retrieves the list of clients by applying complex filters while also supporting aggregate attributes. • POST <cluster-ip>/dna/data/api/v1/clients/query/count Retrieves the number of clients by applying complex filters. • POST <cluster-ip>/dna/data/api/v1/clients/trendAnalytics Retrieves the Trend analytics data related to clients. • POST <cluster-ip>/dna/data/api/v1/clients/${id}/trendAnalytics Retrieves specific client information over a specified period of time. • POST <cluster-ip>/dna/data/api/v1/clients/summaryAnalytics Retrieves summary analytics data related to clients. • POST <cluster-ip>/dna/data/api/v1/clients/topNAnalytics Retrieves the Top-N analytics data related to clients. To access the new Clients APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Clients**.
Compliance API	Catalyst Center platform supports the following Compliance API: • POST <cluster-ip>/dna/intent/api/v1/compliance/networkDevices/${id}/issues/remediation/provision Compliance Remediation. To access the new Compliance API, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Compliance**.

Feature	Description
Devices APIs	

Feature	Description
	Catalyst Center platform supports the following Devices APIs: • PUT <cluster-ip>/dna/intent/api/v1/networkDevices/resyncIntervalSettings Update global resync interval. • PUT <cluster-ip>/dna/intent/api/v1/networkDevices/${id}/resyncIntervalSettings Update resync interval for the network device. • GET <cluster-ip>/dna/intent/api/v1/networkDevices/${id}/resyncIntervalSettings Get resync interval for the network device. • POST <cluster-ip>/dna/intent/api/v1/networkDevices/resyncIntervalSettings/override Override resync interval. • GET <cluster-ip>/dna/data/api/v1/assuranceEvents Query assurance events. • GET <cluster-ip>/dna/data/api/v1/assuranceEvents/count Count the number of events. • GET <cluster-ip>/dna/data/api/v1/assuranceEvents/${id} Get details of a single assurance event. • GET <cluster-ip>/dna/data/api/v1/assuranceEvents/${id}/childEvents Get list of child events for the given wireless client event. • POST <cluster-ip>/dna/data/api/v1/assuranceEvents/query Query assurance events with filters. • POST <cluster-ip>/dna/data/api/v1/assuranceEvents/query/count Count the number of events with filters. • PUT <cluster-ip>/dna/intent/api/v1/healthScoreDefinitions/${id} Update health score definition for the given ID. • GET <cluster-ip>/dna/intent/api/v1/healthScoreDefinitions Get all health score definitions for given filters. • GET <cluster-ip>/dna/intent/api/v1/healthScoreDefinitions/${id} Get health score definition for the given ID. • GET <cluster-ip>/dna/intent/api/v1/healthScoreDefinitions/count Get the count of health score definitions based on provided filters. • POST <cluster-ip>/dna/intent/api/v1/healthScoreDefinitions/bulkUpdate Update health score definitions.

Feature	Description
	• GET <cluster-ip>/dna/data/api/v1/networkDevices Gets the Network Device details based on the provided query parameters. • GET <cluster-ip>/dna/data/api/v1/networkDevices/{id} Get the device data for the given device ID (Uuid). • GET <cluster-ip>/dna/data/api/v1/networkDevices/count Gets the total Network Device counts based on the provided query parameters. • POST <cluster-ip>/dna/data/api/v1/networkDevices/query Gets the list of Network Devices based on the provided complex filters and aggregation functions. • POST <cluster-ip>/dna/data/api/v1/networkDevices/query/count Gets the total number of Network Devices based on the provided complex filters and aggregation functions. • POST <cluster-ip>/dna/data/api/v1/networkDevices/trendAnalytics Gets the Trend analytics data. • POST <cluster-ip>/dna/data/api/v1/networkDevices/${id}/trendAnalytics The Trend analytics data for the network Device in the specified time range. • POST <cluster-ip>/dna/data/api/v1/networkDevices/summaryAnalytics Gets the summary analytics data related to network devices. • GET <cluster-ip>/dna/data/api/v1/interfaces Gets interfaces along with statistics data from all network devices. • GET <cluster-ip>/dna/data/api/v1/interfaces/${id} Get the interface data for the given interface ID (instance Uuid) along with the statistics data. • GET <cluster-ip>/dna/data/api/v1/interfaces/count Gets the total Network device interface counts in the specified time range. When there is no start and end time specified returns the latest interfaces total count. • POST <cluster-ip>/dna/data/api/v1/interfaces/query Gets the list of interfaces across the Network Devices based on the provided complex filters and aggregation functions. • POST <cluster-ip>/dna/data/api/v1/interfaces/query/count The Total interfaces count across the Network devices. To access the new Devices APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Devices**.

Feature	Description
Fabric Wireless APIs	Catalyst Center platform supports the following Fabric Wireless APIs: • PUT <cluster-ip>/dna/intent/api/v1/sda/fabrics/${fabricId}/vlanToSsids Add, Update or Remove SSID mapping to a VLAN. • GET <cluster-ip>/dna/intent/api/v1/sda/fabrics/vlanToSsids/count Return the count of all the fabric site which has SSID to IP Pool mapping. • GET <cluster-ip>/dna/intent/api/v1/sda/fabrics/vlanToSsids Returns all the Fabric Sites that have VLAN to SSID mapping. • GET <cluster-ip>/dna/intent/api/v1/sda/fabrics/${fabricId}/vlanToSsids/count Returns the count of VLANs mapped to SSIDs in a Fabric Site. • GET <cluster-ip>/dna/intent/api/v1/sda/fabrics/${fabricId}/vlanToSsids Retrieve the VLANs and SSIDs mapped to the VLAN within a Fabric Site. To access the new Fabric Wireless APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Connectivity** drop-down list and choose **Fabric Wireless**.

Feature	Description
Health and Performance APIs	Catalyst Center platform supports the following Health and Performance APIs: • GET <cluster-ip>/dna/intent/api/v1/diagnosticValidationSets Retrieves all the validation sets. • GET <cluster-ip>/dna/intent/api/v1/diagnosticValidationSets/${id} Retrieves validation details for a validation set. • GET <cluster-ip>/dna/intent/api/v1/diagnosticValidationWorkflows/count Retrieves the count of validation workflows. • GET <cluster-ip>/dna/intent/api/v1/diagnosticValidationWorkflows/${id} Retrieves validation workflow details. • GET <cluster-ip>/dna/intent/api/v1/diagnosticValidationWorkflows Retrieves the list of validation workflows. • POST <cluster-ip>/dna/ intent/api/v1/diagnosticValidationWorkflows Submits the workflow for executing validations. • DELETE <cluster-ip>/dna/intent/api/v1/diagnosticValidationWorkflows/${id} Deletes a validation workflow. To access the new Health and Performance APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Cisco DNA Center System** drop-down list and choose **Health and Performance**.

Feature	Description
Issues APIs	

Feature	Description
	Catalyst Center platform supports the following Issues APIs: • GET <cluster-ip>/dna/data/api/v1/assuranceIssues Get the details of issues for given set of filters. • GET <cluster-ip>/dna/data/api/v1/assuranceIssues/${id} Get all the details and suggested actions of an issue for the given issue ID. • GET <cluster-ip>/dna/data/api/v1/assuranceIssues/count Get the total number of issues for given set of filters. • POST <cluster-ip>/dna/data/api/v1/assuranceIssues/query Get the details of issues for given set of filters. • POST <cluster-ip>/dna/data/api/v1/assuranceIssues/query/count Get the total number of issues for given set of filters. • POST <cluster-ip>/dna/data/api/v1/assuranceIssues/topNAnalytics Get Top N analytics data of issues. • POST <cluster-ip>/dna/data/api/v1/assuranceIssues/summaryAnalytics Get summary analytics data of issues. • POST <cluster-ip>/dna/data/api/v1/assuranceIssues/trendAnalytics Get trend analytics data of issues. • POST <cluster-ip>/dna/intent/api/v1/assuranceIssues/resolve Resolve the given lists of issues. • POST <cluster-ip>/dna/intent/api/v1/assuranceIssues/ignore Ignore the given list of issues. • POST <cluster-ip>/dna/intent/api/v1/assuranceIssues/${id}/update Update the given issue by updating selected fields. • GET <cluster-ip>/dna/intent/api/v1/customIssueDefinitions Get all the custom issue definitions based on the given filters. • POST <cluster-ip>/dna/intent/api/v1/customIssueDefinitions Creates a new user-defined issue definition. • GET <cluster-ip>/dna/intent/api/v1/customIssueDefinitions/count Get the total custom issue definitions count based on the provided filters. • GET <cluster-ip>/dna/intent/api/v1/customIssueDefinitions/${id} Get the custom issue definition for the given custom issue definition ID. • PUT <cluster-ip>/dna/intent/api/v1/customIssueDefinitions/${id}

Feature	Description
	Updates an existing custom issue definition based on the provided ID. • DELETE <cluster-ip>/dna/intent/api/v1/customIssueDefinitions/${id} Deletes an existing custom issue definition. • GET <cluster-ip>/dna/intent/api/v1/systemIssueDefinitions Returns all issue trigger definitions for given filters. • GET <cluster-ip>/dna/intent/api/v1/systemIssueDefinitions/${id} Get issue trigger definition for given ID. • GET <cluster-ip>/dna/intent/api/v1/systemIssueDefinitions/count Get the count of system defined issue definitions based on provided filters. • PUT <cluster-ip>/dna/intent/api/v1/systemIssueDefinitions/${id} Issue trigger definition update. To access the new Issues APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Issues**.
Licenses APIs	Catalyst Center platform supports the following Licenses APIs: • PUT <cluster-ip>/dna/intent/api/v1/licenseSetting Update license setting. • GET <cluster-ip>/dna/intent/api/v1/licenseSetting Retrieve license setting. To access the new Licenses APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Cisco DNA Center System** drop-down list and choose **Licenses**.

Feature	Description
Network Settings APIs	

Feature	Description
	Catalyst Center platform supports the following Network Settings APIs: • PUT <cluster-ip>/dna/intent/api/v1/sites/{id}/timeZoneSettings Set time zone for a site. • PUT <cluster-ip>/dna/intent/api/v1/sites/{id}/bannerSettings Set banner settings for a site. • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/telemetrySettings Retrieve Telemetry settings for a site. • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/telemetrySettings Set Telemetry settings for a site. • POST <cluster-ip>/dna/intent/api/v1/telemetrySettings/apply Update a device(s) telemetry settings to conform to the telemetry settings for its site. • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/deviceCredentials Get device credential settings for a site. • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/deviceCredentials/status Get network devices credentials sync status at a given site. • GET <cluster-ip>/dna/intent/api/v1/sites/deviceCredentials/apply Sync network devices credential. • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/deviceCredentials Update device credential settings for a site. • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/aaaSettings Set AAA settings for a site. • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/dnsSettings Set DNS settings for a site. • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/dhcpSettings Set DHCP settings for a site. • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/ntpSettings Set NTP settings for a site. • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/imageDistributionSettings Set image distribution settings for a site. • GET<cluster-ip>/dna/intent/api/v1/sites/${id}/aaaSettings Retrieve AAA settings for a site.

Feature	Description
	• GET <cluster-ip>/dna/intent/api/v1/sites/${id}/dnsSettings Retrieve DNS settings for a site. • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/dhcpSettings Retrieve DHCP settings for a site. • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/ntpSettings Retrieve NTP settings for a site. • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/imageDistributionSettings Retrieve image distribution settings for a site. To access the new Network Settings APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Network Settings**.

Feature	Description
SDA APIs	

Feature	Description
	Catalyst Center platform supports the following SDA APIs: Extranet API • DELETE <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies Delete extranet policies. Multicast APIs • GET <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks Get multicast virtual networks. • GET <cluster-ip>/dna/intent/api/v1/sda/multicast Get multicast. • PUT <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks Update multicast virtual networks. • GET <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks/count Get multicast virtual network count. • DELETE <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks/${id} Delete multicast virtual network by ID. • POST <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks Add multicast virtual networks. • PUT <cluster-ip>/dna/intent/api/v1/sda/multicast Update multicast. Port Channel APIs • POST <cluster-ip>/dna/intent/api/v1/sda/portChannels Add Port Channels. • GET <cluster-ip>/dna/intent/api/v1/sda/portChannels Get Port Channels. • PUT <cluster-ip>/dna/intent/api/v1/sda/portChannels Update Port Channels. • DELETE <cluster-ip>/dna/intent/api/v1/sda/portChannels Delete Port Channels. • DELETE <cluster-ip>/dna/intent/api/v1/sda/portChannels/{id} Delete Port Channels by ID. • GET <cluster-ip>/dna/intent/api/v1/sda/portChannels/count Get Port Channels count.

Feature	Description
	Transit Network APIs • GET <cluster-ip>/dna/intent/api/v1/sda/transitNetworks Get Transit Networks. • POST <cluster-ip>/dna/intent/api/v1/sda/transitNetworks Add Transit Networks. • PUT <cluster-ip>/dna/intent/api/v1/sda/transitNetworks Update Transit Networks. • DELETE <cluster-ip>/dna/intent/api/v1/sda/transitNetworks/${id} Delete transit network by ID. • GET <cluster-ip>/dna/intent/api/v1/sda/transitNetworks/count Get transit networks count. Layer 2 Virtual Network APIs • PUT <cluster-ip>/dna/intent/api/v1/sda/layer2VirtualNetworks Update layer 2 virtual networks. • GET <cluster-ip>/dna/intent/api/v1/sda/layer2VirtualNetworks/count Get layer 2 virtual network count. • DELETE <cluster-ip>/dna/intent/api/v1/sda/layer2VirtualNetworks/${id} Delete layer 2 virtual network by ID. • DELETE <cluster-ip>/dna/intent/api/v1/sda/layer2VirtualNetworks Delete layer 2 virtual networks. • POST <cluster-ip>/dna/intent/api/v1/sda/layer2VirtualNetworks Add layer 2 virtual networks. • GET <cluster-ip>/dna/intent/api/v1/sda/layer2VirtualNetworks Get layer 2 virtual networks. Layer 3 Virtual Network APIs

Feature	Description
	• POST <cluster-ip>/dna/intent/api/v1/sda/layer3VirtualNetworks Add layer 3 virtual networks. • GET <cluster-ip>/dna/intent/api/v1/sda/layer3VirtualNetworks Get layer 3 virtual networks. • PUT <cluster-ip>/dna/intent/api/v1/sda/layer3VirtualNetworks Update layer 3 virtual networks. • DELETE <cluster-ip>/dna/intent/api/v1/sda/layer3VirtualNetworks Delete layer 3 virtual networks. • DELETE <cluster-ip>/dna/intent/api/v1/sda/layer3VirtualNetworks/${id} Delete layer 3 virtual network by ID. • GET <cluster-ip>/dna/intent/api/v1/sda/layer3VirtualNetworks/count Get layer 3 virtual network 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**.

Feature	Description
Site APIs	Catalyst Center platform supports the following Site APIs: • GET <cluster-ip>/dna/data/api/v1/siteHealthSummaries Read list of site health summaries. • GET <cluster-ip>/dna/data/api/v1/siteHealthSummaries/${id} Read site health summary data by site ID. • GET <cluster-ip>/dna/data/api/v1/siteHealthSummaries/count Read site count. • GET <cluster-ip>/dna/data/api/v1/siteHealthSummaries/summaryAnalytics Read an aggregated summary of site health data. • POST <cluster-ip>/dna/data/api/v1/siteHealthSummaries/summaryAnalytics Query an aggregated summary of site health data. • GET <cluster-ip>/dna/data/api/v1/siteHealthSummaries/trendAnalytics Read trend analytics data for a grouping of sites in your network. • GET <cluster-ip>/dna/data/api/v1/siteHealthSummaries/${id}/trendAnalytics Read trend analytics data for a specific site in your network. To access the new Site APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Sites**.

Feature	Description
Site Design APIs	

Feature	Description
	Catalyst Center platform supports the following Site Design APIs: • POST <cluster-ip>/dna/intent/api/v1/areas Creates an area. • GET <cluster-ip>/dna/intent/api/v1/areas/${id} Gets an area. • PUT <cluster-ip>/dna/intent/api/v1/areas/${id} Updates an area. • DELETE <cluster-ip>/dna/intent/api/v1/areas/${id} Deletes an area. • POST <cluster-ip>/dna/intent/api/v2/buildings Creates a building. • GET <cluster-ip>/dna/intent/api/v2/buildings/${id} Gets a building. • PUT <cluster-ip>/dna/intent/api/v2/buildings/${id} Updates a building. • DELETE <cluster-ip>/dna/intent/api/v2/buildings/${id} Deletes a building. • POST <cluster-ip>/dna/intent/api/v2/floors Creates a floor. • GET <cluster-ip>/dna/intent/api/v2/floors/${id} Gets a floor. • PUT <cluster-ip>/dna/intent/api/v2/floors/${id} Updates a floor. • DELETE <cluster-ip>/dna/intent/api/v2/floors/${id} Deletes a floor. • POST <cluster-ip>/dna/intent/api/v2/floors/${id}/uploadImage Uploads floor image. • POST <cluster-ip>/dna/intent/api/v1/sites/bulk Create sites. • GET <cluster-ip>/dna/intent/api/v1/sites Get sites. • GET <cluster-ip>/dna/intent/api/v1/sites/count

Feature	Description
	Get sites count. • POST <cluster-ip>/dna/intent/api/v1/networkDevices/assignToSite/apply Assign network devices to a site. • POST <cluster-ip>/dna/intent/api/v1/networkDevices/unassignFromSite/apply Unassign network devices from sites. • GET <cluster-ip>/dna/intent/api/v1/networkDevices/assignedToSite Get site assigned network devices. • GET <cluster-ip>/dna/intent/api/v1/networkDevices/assignedToSite/count Get site assigned network devices count. • GET <cluster-ip>/dna/intent/api/v1/networkDevices/notAssignedToSite Get site not assigned network devices. • GET <cluster-ip>/dna/intent/api/v1/networkDevices/${id}/assignedToSite Get site assigned network device. • GET <cluster-ip>/dna/intent/api/v1/networkDevices/notAssignedToSite/count Get site not assigned network devices count. • GET <cluster-ip>/dna/intent/api/v1/networkDevices/deviceControllability/settings Get device controllability settings. • PUT <cluster-ip>/dna/intent/api/v1/networkDevices/deviceControllability/settings Update device controllability settings. • GET <cluster-ip>/dna/intent/api/v1/networkProfilesforSites Retrieves the list of network profiles for sites. • GET <cluster-ip>/dna/intent/api/v1/networkProfilesforSites/count Retrieves the count of network profiles for sites. • GET <cluster-ip>/dna/intent/api/v1/networkProfilesforSites/${id} Retrieves a network profiles for sites by ID. • DELETE <cluster-ip>/dna/intent/api/v1/networkProfilesforSites/${id} Delete a network profiles for sites. • GET <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/siteAssignments Retrieves the list of sites that the given network profile for sites is assigned to. • POST <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/siteAssignments Assign a network profile for sites to the given site.

Feature	Description
	• POST <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/siteAssignments/bulk Assign a network profile for sites to a list of sites. • DELETE <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/siteAssignments/bulk Unassigns a network profile for sites from multiple sites. • DELETE <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/siteAssignments/${id} Unassigns a network profile for sites from a site. • GET <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/siteAssignments/count Retrieves the count of sites that the given network profile for sites is assigned to. • GET <cluster-ip>/dna/intent/api/v1/sites/${siteId}/profileAssignments Retrieves the list of network profiles that the given site has been assigned. • GET <cluster-ip>/dna/intent/api/v1/sites/${siteId}/profileAssignments/count Retrieves the count of profiles that the given site has been assigned. To access the new Site Design APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Site Design**.

Feature	Description
SWIM APIs	

Feature	Description
	Catalyst Center platform supports the following SWIM APIs: • GET <cluster-ip>/dna/intent/api/v1/images Returns list of software images. • POST <cluster-ip>/dna/intent/api/v1/images/${id}/download Download the software image. • GET <cluster-ip>/dna/intent/api/v1/productNames Retrieves the list of network device product names. • GET <cluster-ip>/dna/intent/api/v1/productNames/count Count of network product names. • GET <cluster-ip>/dna/intent/api/v1/productNames/${productNameOrdinal} Retrieve network device product name. • GET <cluster-ip>/dna/intent/api/v1/siteWiseProductNames Returns network device product names for a site. • POST <cluster-ip>/dna/intent/api/v1/images/${imageId}/siteWiseProductNames Assign network device product name to the given software image. • GET <cluster-ip>/dna/intent/api/v1/siteWiseProductNames/count Returns the count of network device product names for a site. • DELETE <cluster-ip>/dna/intent/api/v1/images/${imageId}/siteWiseProductNames/${productNameOrdinal} Unassign network device product name from the given software image. • PUT <cluster-ip>/dna/intent/api/v1/images/${imageId}/siteWiseProductNames/${productNameOrdinal} Update the list of sites for the network device product name assigned to the software image. • GET <cluster-ip>/dna/intent/api/v1/images/count Returns count of software images. • GET <cluster-ip>dna/intent/api/v1/images/${id}/addonImages/count Returns count of add-on images. • GET <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings Retrieve image distribution servers. • POST <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings Add image distribution server. • GET <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/${id}

Feature	Description
	Retrieve specific image distribution server. • PUT <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/${id} Update remote image distribution server. • DELETE <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/${id} Remove image distribution server. • GET <cluster-ip>/dna/intent/api/v1/networkDeviceImageUpdates Get network device image updates. • GET <cluster-ip>/dna/intent/api/v1/networkDeviceImageUpdates/count Count of network device image updates. • GET <cluster-ip>/dna/intent/api/v1/images/${imageId}/siteWiseProductNames Retrieves network device product names assigned to a software image • GET <cluster-ip>/dna/intent/api/v1/siteWiseProductNames/count Returns the count of network device product names for a site. To access the new SWIM APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Software Image Management (SWIM)**.

Feature	Description
System Settings APIs	Catalyst Center platform supports the following System Settings APIs: • POST <cluster-ip>/dna/intent/api/v1/ipam/serverSetting Creates configuration details of the external IPAM server. You should only create one external IPAM server; delete any existing external server before creating a new one. • GET <cluster-ip>/dna/intent/api/v1/ipam/serverSetting Retrieves configuration details of the external IPAM server. If an external IPAM server has not been created, this resource will return a `404` response. • PUT <cluster-ip>/dna/intent/api/v1/ipam/serverSetting Updates configuration details of the external IPAM server. • DELETE <cluster-ip>/dna/intent/api/v1/ipam/serverSetting Deletes configuration details of the external IPAM server. • GET <cluster-ip>/dna/intent/api/v1/provisioningSettings Get provisioning settings. • PUT <cluster-ip>/dna/intent/api/v1/provisioningSettings Set provisioning settings. To access the new System Settings APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Scroll down and click **System Settings**.

Feature	Description
Task APIs	Catalyst Center platform supports the following Task APIs: • GET<cluster-ip>/dna/intent/api/v1/tasks Get tasks. • GET<cluster-ip>/dna/intent/api/v1/tasks/count Get tasks count. • GET<cluster-ip>/dna/intent/api/v1/tasks/${id} Get tasks by ID. • GET<cluster-ip>/dna/intent/api/v1/tasks/${id}/detail Get task details by ID. • GET <cluster-ip>/dna/data/api/v1/assuranceTasks/${id} Retrieve a specific assurance task by id. • GET <cluster-ip>/dna/data/api/v1/assuranceTasks/count Retrieve a count of the number of assurance tasks that currently exist. • GET <cluster-ip>/dna/data/api/v1/assuranceTasks Retrieve a list of assurance tasks. To access the new Task APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Operational Tasks** drop-down list and choose **Task**.

Feature	Description
Tag APIs	Catalyst Center platform supports the following Tag APIs: • GET <cluster-ip>/dna/intent/api/v1/tags/networkDevices/membersAssociations Retrieve tags associated with network devices. • GET <cluster-ip>/dna/intent/api/v1/tags/interfaces/membersAssociations/count Retrieve the count of interfaces that are associated with at least one tag. • GET <cluster-ip>/dna/intent/api/v1/tags/networkDevices/membersAssociations/count Retrieve the count of network devices that are associated with at least one tag. • POST <cluster-ip>/dna/intent/api/v1/tags/networkDevices/membersAssociations/query Query the tags associated with network devices. • POST <cluster-ip>/dna/intent/api/v1/tags/interfaces/membersAssociations/query Query the tags associated with interfaces. • GET <cluster-ip>/dna/intent/api/v1/tags/interfaces/membersAssociations Retrieve tags associated with the interfaces. To access the new Tag APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Operation Tasks** drop-down list and choose **Tag**.

Feature	Description
Wireless APIs	

Feature	Description
	With this release, Catalyst Center platform introduces the following new Wireless APIs. **Note** The new Wireless APIs do not support Cisco AireOS Wireless Controller. The support is extended only to the Cisco Catalyst 9800 family of devices. • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/${networkDeviceId}/anchorManagedApLocations Get Anchor Managed AP Locations for specific Wireless Controller. • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/${networkDeviceId}/managedApLocations/count Get Managed AP Locations Count for specific Wireless Controller. • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/${networkDeviceId}/primaryManagedApLocations Get Primary Managed AP Locations for specific Wireless Controller. • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/${networkDeviceId}/secondaryManagedApLocations Get Secondary Managed AP Locations for specific Wireless Controller. • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/wirelessMobilityGroups/count Get MobilityGroups Count. • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/wirelessMobilityGroups Get All MobilityGroups. • POST <cluster-ip>/dna/intent/api/v1/wirelessControllers/wirelessMobilityGroups/mobilityProvision Mobility Provision. • POST <cluster-ip>/dna/intent/api/v1/wirelessControllers/wirelessMobilityGroups/mobilityReset Mobility Reset. • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/${networkDeviceId}/ssidDetails Get SSID Details for specific Wireless Controller. • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/${networkDeviceId}/ssidDetails/count Get SSID Count for specific Wireless Controller. • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/interfaces/${id} Update Interface. • DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/interfaces/${id}

Feature	Description
	Delete Interface. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/interfaces Get Interfaces. • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/interfaces Create Interface. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/interfaces/${id} Get Interface by ID. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/interfaces/count Get Interfaces Count. • POST <cluster-ip>/dna/intent/api/v1/sites/${siteId}/wirelessSettings/ssids Create SSID. • PUT <cluster-ip>/dna/intent/api/v1/sites/${siteId}/wirelessSettings/ssids/${id} Update SSID. • DELETE <cluster-ip>/dna/intent/api/v1/sites/${siteId}/wirelessSettings/ssids/${id} Delete SSID. • GET <cluster-ip>/dna/intent/api/v1/sites/${siteId}/wirelessSettings/ssids Get SSID by Site. • GET <cluster-ip>/dna/intent/api/v1/sites/${siteId}/wirelessSettings/ssids/${id} Get SSID by ID. • GET <cluster-ip>/dna/intent/api/v1/sites/${siteId}/wirelessSettings/ssids/count Get SSID Count by Site. • DELETE <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id} Delete Wireless Profile. • PUT <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id} Update Wireless Profile. • POST <cluster-ip>/dna/intent/api/v1/wirelessProfiles Create Wireless Profile. • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles Get Wireless Profiles. • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id} Get Wireless Profile by ID.

Feature	Description
	• GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/count Get Wireless Profiles Count. • DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/rfProfiles/${id} Delete RF Profile. • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/rfProfiles Create RF Profile. • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/rfProfiles/${id} Update RF Profile. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/rfProfiles Get RF Profiles. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/rfProfiles/${id} Get RF Profile by ID. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/rfProfiles/count Get RF Profiles Count. • POST <cluster-ip>/dna/intent/api/v1/wirelessAccessPoints/factoryResetRequest/provision Factory Reset Access Point(s). • GET <cluster-ip>/dna/intent/api/v1/wirelessAccessPoints/factoryResetRequestStatus Get Access Point(s) Factory Reset status. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/dot11beProfiles Get all 802.11be Profiles. • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/dot11beProfiles/${id} Update 802.11be Profile. • DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/dot11beProfiles/${id} Delete a 802.11be Profile. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/dot11beProfiles/${id} Get 802.11be Profile by ID. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/dot11beProfiles/count Get 802.11be Profiles Count. • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/dot11beProfiles Create a 802.11be Profile.

Feature	Description
	• POST<cluster-ip>/dna/intent/api/v1/wirelessControllers/${deviceId}/assignManagedApLocations Assign Managed AP Locations For WLC. • POST<cluster-ip>/dna/intent/api/v1/wirelessControllers/${deviceId}/provision Wireless Controller Provision. • POST <cluster-ip>/dna/intent/api/v1/wirelessAccessPoints/provision AP Provision. To access the new Wireless APIs, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Connectivity** drop-down list and choose **Wireless**.
API Enhancements	
Device Onboarding (PnP) APIs	With this release: • The sudiSerialNos request parameter is renamed as userSudiSerialNos in the Update Device and Add Device APIs. • The addressIpV6 request parameter is added to the Add Virtual Account and Update PnP Server Profile APIs. This parameter is required when the cluster is configured with IPv6. • The isSudiRequired request parameter is renamed as sudiRequired in the Import Devices in bulk API. • A new optional request parameter called hostname is added to the Claim a Device to a Site API. • A new optional request parameter called authorizationNeeded is added to the Claim Device API.
Devices API	With this release, `syncRequestedByApp` and `lastManagedResyncReasons` response parameters are introduced in the Get Device list API.
Event Management API	The Get EventArtifacts API now includes the optional `deprecationMessage` and `deprecated` response parameters. If the deprecated value is `true`, then the event artifact is deprecated and a deprecation message is displayed.
Fabric Device APIs	With this release: • The request parameter `deviceRoles` accepts the WIRELESS_CONTROLLER_NODE value. • The Fabric Device APIs support is extended to wireless role.
Path Trace API	The egressPhysicalInterface, ingressPhysicalInterface, egressInterface, ingressInterface attributes are now optional attributes in the Retrieves Previous Pathtrace API.

Feature	Description
SDA API	In this release, an optional `isBpduGuardEnabled` request body parameter is added in the Update authentication profile API. The value must not be null when the `authenticationProfileName` parameter is set as Closed Authentication.
Deprecated APIs	
Fabric Wireless APIs	With this release, the following Fabric Wireless APIs are marked as Sunset: • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/wireless-controller Remove WLC from Fabric Domain. • PUT <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/ssid-ippool Update SSID to IP Pool Mapping. • POST <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/ssid-ippool Add SSID to IP Pool Mapping. • GET <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/ssid-ippool Get SSID to IP Pool Mapping. • POST <cluster-ip>/dna/intent/api/v1/business/sda/wireless-controller Add WLC to Fabric Domain.
Network Settings APIs	With this release, the following Network Settings APIs are marked as Sunset: • POST <cluster-ip>/dna/intent/api/v1/network/${siteId} Create Network. • POST <cluster-ip>/dna/intent/api/v2/network/${siteId} Create Network V2. • PUT <cluster-ip>/dna/intent/api/v1/network/${siteId} Update Network. • PUT <cluster-ip>/dna/intent/api/v2/network/${siteId} Update Network V2. • GET <cluster-ip>/dna/intent/api/v1/network Get Network. • GET <cluster-ip>/dna/intent/api/v2/network Get Network V2. • POST <cluster-ip>/dna/intent/api/v1/credential-to-site/${siteId} Assign Device Credential To Site. • POST <cluster-ip>/dna/intent/api/v2/credential-to-site/${siteId} Assign Device Credential To Site V2.

Feature	Description
Site Design APIs	With this release, the following Site Design APIs are marked as Sunset: • POST <cluster-ip>/dna/intent/api/v1/networkprofile/${networkProfileId}/site/${siteId} Associate. • DELETE <cluster-ip>/dna/intent/api/v1/networkprofile/${networkProfileId}/site/${siteId} Disassociate.
Site APIs	With this release, the following Site APIs are marked as Sunset: • GET <cluster-ip>/dna/intent/api/v1/site-member/${id}/member Get devices that are assigned to a site. • POST <cluster-ip>/dna/intent/api/v1/assign-device-to-site/${siteId}/device Assign Devices To Site. • POST <cluster-ip>/dna/intent/api/v1/site Create Site. • DELETE <cluster-ip>/dna/intent/api/v1/site/${siteId} Delete Site. • PUT <cluster-ip>/dna/intent/api/v1/site/${siteId} Update Site. • GET <cluster-ip>/dna/intent/api/v1/site Get Site. • GET <cluster-ip>/dna/intent/api/v2/site Get Site V2. • GET <cluster-ip>/dna/intent/api/v1/site/count Get Site Count. • GET <cluster-ip>/dna/intent/api/v1/membership/${siteId} Get Membership. • GET <cluster-ip>/dna/intent/api/v2/site/count Get Site Count V2.

Feature	Description
Task APIs	With this release, the following Task APIs are marked as Sunset: • GET <cluster-ip>/dna/intent/api/v1/task Get tasks. • GET <cluster-ip>/dna/intent/api/v1/task/${taskId} Get task by ID. • GET <cluster-ip>/dna/intent/api/v1/task/operation/${operationId}/${offset}/${limit} Get task by OperationId. • GET <cluster-ip>/dna/intent/api/v1/task/${taskId}/tree Get task tree. • GET <cluster-ip>/dna/intent/api/v1/task/count Get task count.

Feature	Description
Wireless APIs	

Feature	Description
	With this release, the following Wireless APIs are marked as Sunset: • POST <cluster-ip>/dna/intent/api/v1/wireless/profile Create Wireless Profile. • GET <cluster-ip>/dna/intent/api/v1/wireless/profile Get Wireless Profile. • DELETE <cluster-ip>/dna/intent/api/v1/wireless-profile/${wirelessProfileName} Delete Wireless Profile. • PUT <cluster-ip>/dna/intent/api/v1/wireless/profile Update Wireless Profile. • GET <cluster-ip>/dna/intent/api/v1/wireless/rf-profile Retrieve RF profiles. • DELETE <cluster-ip>/dna/intent/api/v1/wireless/rf-profile/${rfProfileName} Delete RF profiles. • POST <cluster-ip>/dna/intent/api/v1/wireless/rf-profile Create or Update RF profile. • GET <cluster-ip>/dna/intent/api/v1/wireless/dynamic-interface Get dynamic interface. • PUT <cluster-ip>/dna/intent/api/v1/wireless/dynamic-interface Create Update Dynamic interface. • DELETE <cluster-ip>/dna/intent/api/v1/wireless/dynamic-interface Delete dynamic interface. • POST <cluster-ip>/dna/intent/api/v1/enterprise-ssid Create Enterprise SSID. • PUT <cluster-ip>/dna/intent/api/v1/enterprise-ssid Update Enterprise SSID. • Delete <cluster-ip>/dna/intent/api/v1/enterprise-ssid/${ssidName} Delete Enterprise SSID. • GET <cluster-ip>/dna/intent/api/v1/enterprise-ssid Get Enterprise SSID. • DELETE <cluster-ip>/dna/intent/api/v1/business/ssid/${ssidName}/${managedAPLocations} Delete SSID and provision it to devices.

Feature	Description
	• POST <cluster-ip>/dna/intent/api/v1/business/ssid Create and Provision SSID. • GET <cluster-ip>/dna/intent/api/v1/task/count AP Provision. • POST <cluster-ip>/dna/intent/api/v1/wireless/ap-provision Provision update. • POST <cluster-ip>/dna/intent/api/v1/wireless/provision Provision.
API Changes That Break Backward Compatibility	
None	—

Table 4: New and changed features in Catalyst Center platform 2.3.7.5

Feature	Description	Where documented
Audit Log Report	This Catalyst Center platform release supports a new **Audit Log** report.	For more information, see: • Run an audit log report, on page 146. • **New Report** in the Cisco Catalyst Center Release Notes.
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**.	

Feature	Description	Where documented
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	Where documented
SD-Access APIs		

Feature	Description	Where documented
	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	

Feature	Description	Where documented
	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/${id} Delete fabric site by ID. • GET <cluster-ip>/dna/intent/api/v1/sda/fabricSites Get fabric sites. • GET <cluster-ip>/dna/intent/api/v1/sda/fabricSites/count Get fabric site count. Fabric Zone APIs • POST <cluster-ip>/dna/intent/api/v1/sda/fabricZones Add fabric zone. • PUT <cluster-ip>/dna/intent/api/v1/sda/fabricZones Update fabric zone. • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricZones/${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	

Feature	Description	Where documented
	• 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 • 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	

Feature	Description	Where documented
	• 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	Where documented
	• 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	

Feature	Description	Where documented
	• 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	Where documented
	• 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	

Feature	Description	Where documented
	• 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.	

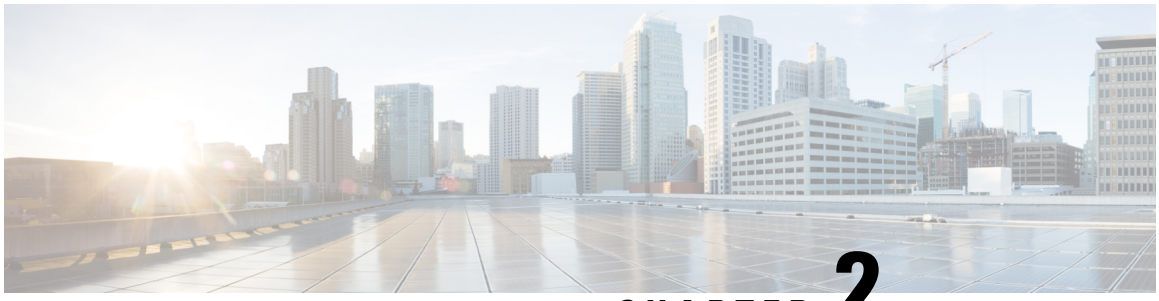
Feature	Description	Where documented

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	—	

Table 5: New and changed features in Catalyst Center platform 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 the Cisco DNA Center platform to Catalyst Center platform in this release. The capability and functionality of Catalyst Center remains the same as Cisco DNA Center.
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	
Devices API	The Get Device Config for all devices API is deprecated.



CHAPTER 2

About Catalyst Center Platform

- Catalyst Center platform, on page 99
- Intent APIs, on page 100
- About events and notifications, on page 100

Catalyst Center platform

Catalyst Center provides an extensible platform that Cisco customers and partners can use to create value-added applications that can be built on top of its native capabilities. You can optimize end-to-end IT processes, reduce the Total Cost of Ownership (TCO), and develop new value networks by leveraging the Catalyst Center platform features to enhance the overall network experience.

- Intent APIs: The Intent APIs are northbound REST APIs that expose specific capabilities of Catalyst Center platform. The Intent APIs provide policy-based abstraction of business intent, allowing you to focus on an outcome to achieve instead of struggling with the mechanisms that implement that outcome. The APIs conform to the REST API architectural style. The APIs are simple, extensible, and secure to use. They support the standard REST methods, which include GET, POST, PUT, and DELETE operations through HTTPS.
- Integration Flows: Integration capabilities are part of westbound interfaces. To meet the need to scale and accelerate operations in modern data centers, IT operators require intelligent, end-to-end work flows built with open APIs. Catalyst Center platform provides mechanisms for integrating Assurance workflows and data with third-party IT Service Management (ITSM) solutions.
- Events and Notifications Services: Supported services are available for Cisco Catalyst Assurance events and Catalyst Center SWIM events to be captured and forwarded to third-party applications.

Note The Catalyst Center platform application is accessible to a user with a SUPER-ADMIN-ROLE. Log in as a user with a SUPER-ADMIN-ROLE to view the Catalyst Center platform and do tasks through its GUI. Additionally, as a user with a SUPER-ADMIN-ROLE, you can create a custom role with read, write, or deny permissions to various platform functionality (APIs, bundles, events, and reports). From the main menu, choose **System** > **Users & Roles** > **Role Based Action Access Control** to access this feature.

Intent APIs

The intent APIs are northbound REST APIs that expose specific capabilities of Catalyst Center platform. The Intent APIs provide policy-based abstraction of business intent, allowing you to focus on achieving the outcome rather than struggling with the mechanisms that implement it.

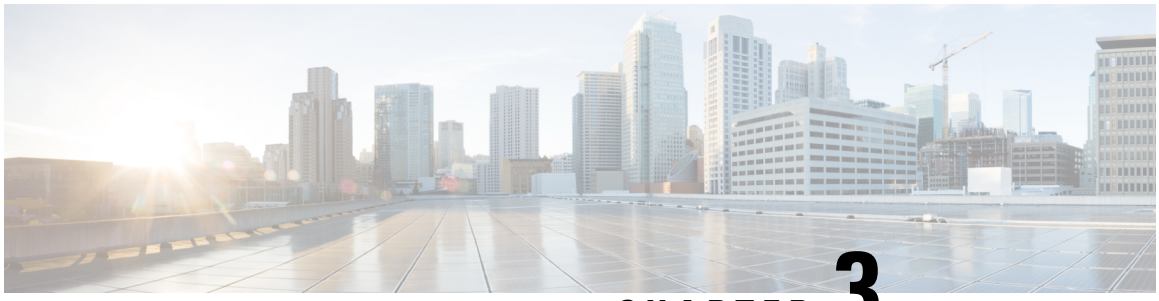
The APIs conform to REST API architectural styles that are simple, extensible, and secure. They support standard REST methods, which include GET, POST, PUT, and DELETE operations through HTTPS. A REST endpoint accepts and returns HTTPS messages containing JavaScript Object Notation (JSON) documents. You can use any programming language to generate the messages and the JSON documents that contain the API methods. These APIs are governed by the Catalyst Center Role Based Access Control (RBAC) rules. As a security measure, users must authenticate successfully before using the API.

The Intent APIs are listed in the API catalog located in the Catalyst Center platform GUI. You can view this catalog by navigating to **Platform** > **Developer Toolkit** > **APIs** . For information about the rate limit of an API, click the **Features** tab in the API details page. The intent APIs have a default API rate limit of 50 requests.

About events and notifications

Catalyst Center platform supports the ability to send custom notifications when specific events are triggered. This is valuable for third-party systems that take business actions based upon event type. For example, when a device in the network is not compliant, a custom application may want to receive notifications and do a software upgrade.

You can view a list of available events for this release. From the main menu, choose **Platform** > **Manage** > **Configurations**. These events can be customized for IT Service Management (ITSM) incidents.



CHAPTER 3

Deploy Catalyst Center Platform

- Catalyst Center platform deployments, on page 101
- Installation of Catalyst Center Platform, on page 101
- Configure integration settings, on page 102
- API prerequisites, on page 103
- Supporting Role-Based Access Control, on page 104

Catalyst Center platform deployments

A Catalyst Center platform deployment is an enterprise network management solution that

- includes installation and integration of multiple platform components,
- supports modular configuration through bundles and API integration, and
- provides centralized management and monitoring for network infrastructure.

Additional reference information:

1. To install the latest version of Catalyst Center, see Installation of Catalyst Center Platform, on page 101.
2. To configure the integration settings, see Configure integration settings, on page 102.

After you deploy the Catalyst Center platform, you must:

- Review the API prerequisites. For information, see API prerequisites, on page 103.
- Review the brief feature descriptions in **Overview** in the GUI to understand the Catalyst Center platform. For information, see Platform overview, on page 107.
- Go to **Bundles** in the GUI. Enable, configure, and activate the bundles needed for your network. For information, see Bundle features, on page 110.

Installation of Catalyst Center Platform

When you install Catalyst Center, you also install the Catalyst Center platform. A separate installation procedure is not required for the Catalyst Center platform.

For information about installing Catalyst Center, see the *Cisco Catalyst Center Installation Guide*.

Additional information:

- The Catalyst Center platform is accessible to a user with a SUPER-ADMIN-ROLE.
- After logging in with a SUPER-ADMIN-ROLE, you can view the Catalyst Center platform and perform actions through its GUI.
- As a user with a SUPER-ADMIN-ROLE, you can create a custom role that grants read, write, or deny permissions for features such as application programming interfaces (APIs), bundles, events, and reports on the platform.
- From the main menu, choose **System** > **Users & Roles** > **Role Based Action Access Control** to access this feature.

Configure integration settings

If firewalls or other rules exist between Catalyst Center and any third-party applications that need to reach Catalyst Center platform, configure **Integration Settings**. This occurs when the IP address of Catalyst Center is mapped internally to another IP address that provides internet or external network access.

Important After you back up and restore Catalyst Center, you must access the **Integration Settings** window and update (if necessary) the **Callback URL Host Name** or **IP Address** using this procedure.

Before you begin

You have deployed Catalyst Center platform as described earlier in the documentation.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **System Configuration** > **Integration Settings**.

Step 2 Enter the **Callback URL Host Name** or **IP Address** that the third-party application needs to connect to when communicating with Catalyst Center platform.

Note
The **Callback URL Host Name** or **IP Address** is the external-facing hostname or IP address that is mapped internally to Catalyst Center. Configure the virtual IP (VIP) address for a setup with three nodes.

Step 3 Click **Apply**.

What to do next

Review the API prerequisites for the Catalyst Center platform to function correctly.

API prerequisites

Meet these Application programming Interface (API) prerequisites to work with the Catalyst Center API and the Catalyst Center platform.

Supported Programming Language

Use a supported programming language and complete the required tasks to run the code previews.

For example, to use Python scripts generated by Catalyst Center platform, you must install the requests library. You can use pip (Pip Installs Packages) to install using a CLI command:

```
pip install requests
```

Code previews for these languages are available in the GUI:

- **Shell**
- **Node - HTTP**
- **Node - Unirest**
- **Node - Request**
- **Python**
- **Ruby**
- **JavaScript**
- **JQuery**
- **PHP**
- **Go**
- **Ansible**

Authentication

The Catalyst Center APIs use token-based authentication. A token remains valid for 60 seconds (1 minute). To access the API, use an authentication script in your supported programming language. For example, run this Python script to log in:

```
def get_token():
    token = requests.post(
       'https://<cluster IP>/api/system/v1/auth/token',
       auth=HTTPBasicAuth(
           username=<username>,
           password=<password>
       ),
   headers={'content-type': 'application/json'},
   verify=False,
    )
    data = token.json()
    return data['Token']
```

Supporting Role-Based Access Control

Catalyst Center platform supports Role-Based Access Control (RBAC), which enables a user with SUPER-ADMIN-ROLE privileges to define custom roles that permit or restrict users access to certain platform features.

Use this procedure to define a custom role and assign someone to that role.

Note If you have a SUPER-ADMIN-ROLE, you can access Catalyst Center platform. You can log in and view the Catalyst Center platform, as well as perform actions through its GUI after logging in as a user with a SUPER-ADMIN-ROLE. The NETWORK-ADMIN-ROLE and the OBSERVER-ROLE have limited capabilities with the Catalyst Center platform. For example, these two roles do not permit the user to do these actions:

- Generate reports
- Subscribe to events
- Configure event settings
- Enable and configure bundles
- Configure users and roles.

For more information, see the "Manage Users" chapter in *Cisco Catalyst Center Administrator Guide*.

Before you begin

You must have SUPER-ADMIN-ROLE privileges to perform this procedure.

Procedure

Step 1 Define a custom role.

a) From the main menu, choose **System** > **Users & Roles** > **Role Based Access Control**.

b) Click **Create a New Role**.

The **Create a User Role** window appears. If you are setting up RBAC for the first time, the system prompts you to assign users after you create the new role.

c) Click **Let's Do it**.

If you want to skip this screen in the future, select the **Don't show this to me again** check box.

The **Create a New Role** window appears.

d) Enter a name for the role and then click **Next**.

The **Define the Access** window appears with a list of options.

e) Click > next to **Platform** to expand it.

These options appear. You can set **Deny** (the default), **Read**, or **Write** permissions for the new role:

- **APIs**: Allows you to view and try out the APIs.
- **Bundles**: Allows you to configure and activate the bundles and IT Service Management (ITSM) integration settings.
- **Events**: Allows you to configure event settings for email, REST API endpoints, and Simple Network Management Protocol (SNMP) traps.
- **Reports**: Allows you to schedule, view, and download reports.

f) Click **Next**.
The **Summary** window appears.

g) Review the summary. If the summary information is correct, click **Create Role**. Otherwise, click **Edit** and make the appropriate changes.

Step 2 Assign a user to the custom role you just created by clicking **Add Users**.

The **User Management** > **Internal Users** window appears, which allows you to assign the custom role to an existing user or a new user.

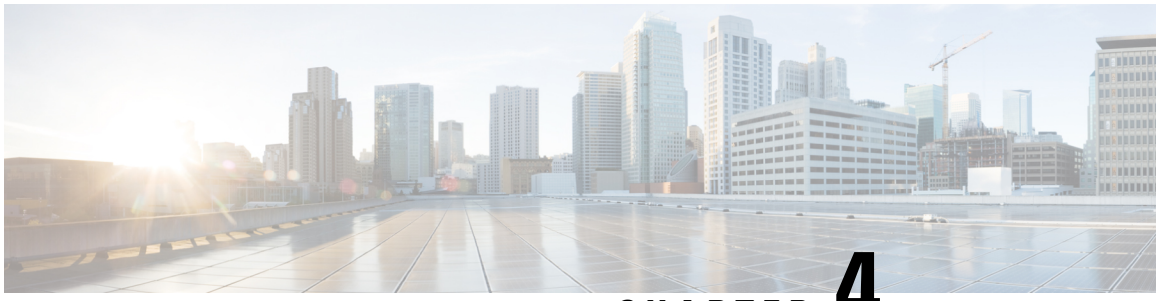
- To assign the custom role to an existing user:
  1. In the **Internal Users** window, click the radio button next to the user to whom you want to assign the custom role, and then click **Edit**.

     The **Update Internal User** slide-in pane appears.
  2. From the **Role List** drop-down list, choose the custom role, and then click **Save**.

- To assign the custom role to a new user:
  1. Click **Add**.

     The **Create Internal User** slide-in pane appears.
  2. Enter the first name, last name, email, and username in the fields provided.
  3. From the **Role List** drop-down list, choose the custom role to assign to the new user.
  4. Enter the password and then confirm it.
  5. Click **Save**.

Step 3 If you were logged in when the administrator changed your access permissions, log out and log back in to activate your new permissions.



CHAPTER 4

Platform Overview GUI

- Platform overview, on page 107
- Navigate through the platform GUI, on page 107

Platform overview

The Platform Overview enables efficient access and configuration of the platform extensibility and monitoring capabilities in a unified location.

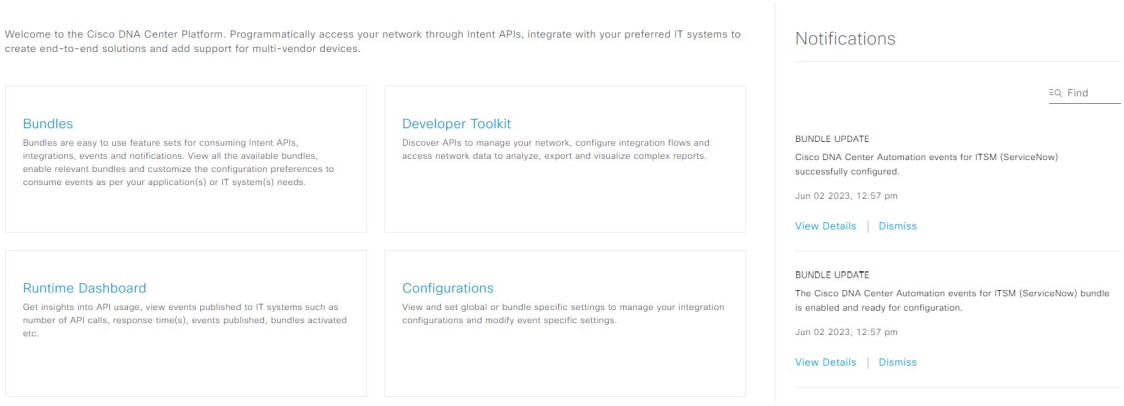
You can access the **Overview** page from the menu by selecting **Platform** and then choosing **Overview**. From this page, you can:

- View summaries and access direct links to important GUI features, including:
  - **Bundles**: Provides access to bundles, which are groupings of APIs, events, integration flows, data services, or applications. The **Bundles** section also includes a link to **Configurations**, where you can configure general, event global settings, or settings for multiple bundles.
  - **Developer Toolkit**: Offers tools (such as APIs and integration flows) for extending platform capabilities or integrating with other applications.
  - **Runtime Dashboard**: Displays collected metrics and summaries for APIs, integration flows, and events.
  - **Configurations**: Allows you to configure event categories, security levels, and types, and to manage instances within bundles.
- Access the **Notifications** slide-in pane to see current notifications about bundle updates and other platform events. Click **View Details** to view detailed data about the bundle under the **Bundles** tab. Click **Dismiss** to dismiss the bundle notification.

Navigate through the platform GUI

Use this procedure to review platform features and functions available through the Catalyst Center GUI. You can access these features and functions in the **Overview** window.

Figure 1: Catalyst Center platform Overview window



Procedure

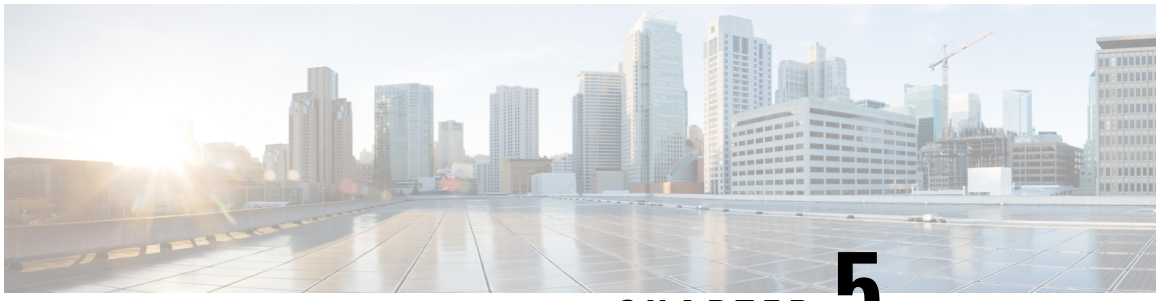
Step 1 From the main menu, choose **Platform** > **Overview**.

Step 2 Review the options available in the **Overview** window.

Step 3 Click the links to access individual Catalyst Center platform features directly.

Step 4 Review bundle update information using the **Notifications** slide-in pane.

Note
The bundle update information provides the current bundle status (enabled, disabled, successfully configured, or ready to be configured).



CHAPTER 5

Platform Manage GUI

- About manage, on page 109
- About bundles, on page 109
- Bundle features, on page 110
- Configure bundles: destination to receive events, on page 111
- Configure bundles: ServiceNow access settings, on page 114
- Configure bundles: CMDB data synchronization for ServiceNow, on page 117

About manage

The Catalyst Center platform **Manage** window provides access to these features:

- **Bundles**: Access to bundles that you can use to integrate Catalyst Center with your own applications or to enhance the performance of Catalyst Center itself. Bundles are comprised of groupings of APIs, events, integration flows, data services, or applications.

Note To view the bundle components, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs** or **Platform** > **Developer Toolkit** > **Integration Flows**.

- **Configurations**: Ability to configure global settings for a single bundle or across multiple bundles for a custom platform experience.

About bundles

Catalyst Center platform provides access to bundles that you can use to integrate Catalyst Center with your own applications or to enhance the performance of Catalyst Center itself.

This Catalyst Center platform information is accessible using the GUI:

- Bundle name, vendor, version, version release date, tags, and description.
- Status of the bundle:

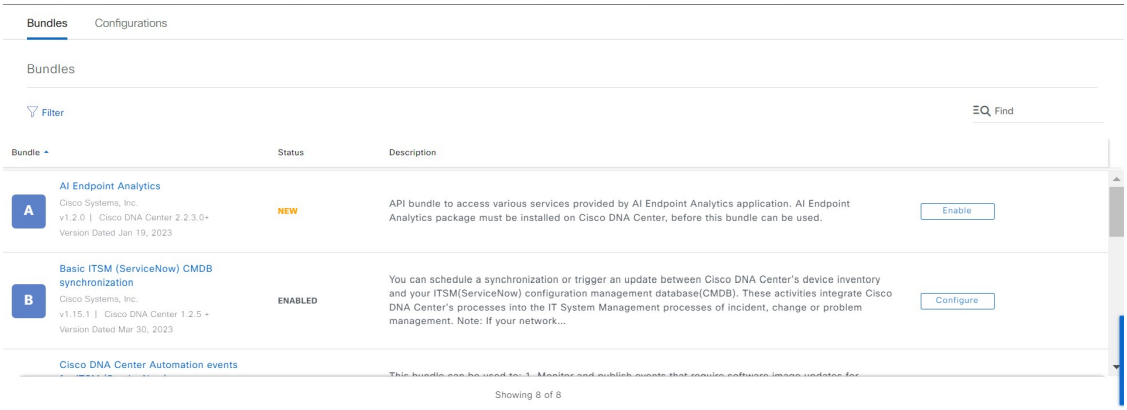
- **NEW**: Bundle that is available through Catalyst Center platform, but has not yet been enabled. Click **Enable** to enable the bundle for configuration and subsequent activation.
- **ENABLED**: Bundle that has been enabled, but not yet configured. Once enabled, the bundle's integration flows and API code can be viewed under the **Contents** tab. Click **Configure** to configure at the bundle level.

  The enablement and configuration of bundles are two separate steps, because a business manager will usually enable a particular bundle as a business decision. The follow-up configuration of the bundle will usually be performed by an IT or network administrator.
- **DISABLED**: The bundle has been stopped from executing any further.
- **ACTIVE**: After either reviewing and/or configuring the bundle (configuring bundle-specific values), you can activate the bundle in your network by clicking **Activate**.
- **UPDATE**: When you upgrade from one version of Catalyst Center platform to a later version of Catalyst Center platform.
- **ERROR**: There is an issue with the bundle and it cannot be activated within your network.

Bundle features

You can review, enable, and configure bundles using the **Bundles** window in the Catalyst Center GUI.

Figure 2: Catalyst Center platform Bundles window



Access the bundles in the GUI to accomplish these tasks:

- Review and try out supported Catalyst Center APIs. For more information, see Work with APIs, on page 191.
- Enable Rogue Management and the Cisco Advanced Wireless Intrusion Prevention System (aWIPS) to detect wired and wireless threats, including rogue access points. For more information, see Work with APIs, on page 191.
- Configure a destination (Event Management or REST API endpoint) to receive events for ServiceNow. For information on using the GUI to configure a destination, see Configure bundles: destination to receive events, on page 111.

- Configure access settings for Catalyst Center to ServiceNow (hostname, username, password, and so on). For information on using the GUI to configure access settings to ServiceNow, see Configure bundles: ServiceNow access settings, on page 114.
- Configure data synchronization between Catalyst Center and ServiceNow (including the option to configure operational and source identifiers). For information on using the GUI to configure data synchronization, see Configure bundles: CMDB data synchronization for ServiceNow, on page 117.

These bundles are available:

- **Basic ITSM (ServiceNow) CMDB synchronization**: Triggers or schedules a synchronization between Catalyst Center devices and your ServiceNow CMDB system. The ServiceNow CMDB provides a single system of record for IT.

Note For an example of an integration flow and ServiceNow, see ServiceNow Integration.

- **REST API**: Contains the REST API supported by Catalyst Center. This API provides a rich set of capabilities to query network knowledge, as well as to initiate network programming.
- **Endpoint Attribute Retrieval with ITSM (ServiceNow)**: Retrieves detailed endpoint information and publishes it once or on a recurring schedule to Catalyst Center. This activity does not modify or delete any CIs on the existing ITSM (ServiceNow) tool.
- **Network Issue Monitor and Enrichment for ITSM (ServiceNow)**: Contains Catalyst Center components that monitor the network for assurance and maintenance issues, and publishes the event details to a ServiceNow system. It also contains APIs to access rich network context data.
- **Rogue and aWIPS**: Contains the REST API supported by Catalyst Center for Rogue Management and aWIPS. This API is used to detect wired and wireless threats, including rogue access points. You must install the **Rogue and aWIPS** package in Catalyst Center to use this bundle and its APIs.
- **Automation events for ITSM (ServiceNow)**: Monitors and publishes events that require software image updates for compliance, security, device provisioning activities, or other operational triggers to a ServiceNow system.
- **Disaster Recovery API**: Contains the REST APIs supported by disaster recovery and provides support to monitor the disaster recovery system.
- **AI Endpoint Analytics**: Lets you access various services provided by the AI endpoint analytics application. You must install the **AI Endpoint Analytics** package in Catalyst Center to use this bundle.

You can adjust the bundles that display in the GUI by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

Configure bundles: destination to receive events

Do this procedure to configure a destination to receive events (network and SWIM) for ServiceNow within a bundle.

You configure a destination to receive events for ServiceNow within these bundles:

- **Network Issue Monitor and Enrichment for ITSM (ServiceNow)**
- **Automation events for ITSM (ServiceNow)**

Before you begin

See the latest *Cisco Catalyst Center ITSM Integration Guide* to understand how this procedure fits within a larger workflow when configuring a Catalyst Center-to-ServiceNow integration.

Procedure

Step 1 From the main menu, choose **Platform** > **Manage** > **Bundles**.

Step 2 Click either the **Network Issue Monitor and Enrichment for ITSM (ServiceNow)** or the **Automation events for ITSM (ServiceNow)** bundle link or icon.

This information is provided:

- **General information**: Vendor, version, platform, tags display under the square icon.

  Note
  Tags indicate what the Catalyst Center component is used for or is affected by the bundle.

- **Information**: Tab that displays general information (purpose of bundle and how bundle works in the network), sample schemas, mapping notes, configuration notes, and other data about the bundle.
- **Contents**: Tab that accesses information about the integration flows within the bundle.
- **Release Notes**: Tab that displays latest release information about the bundle, including its version.

Step 3 Click each of the preceding tabs and review the information about the bundle.

Step 4 Click **Enable** to enable the bundle.

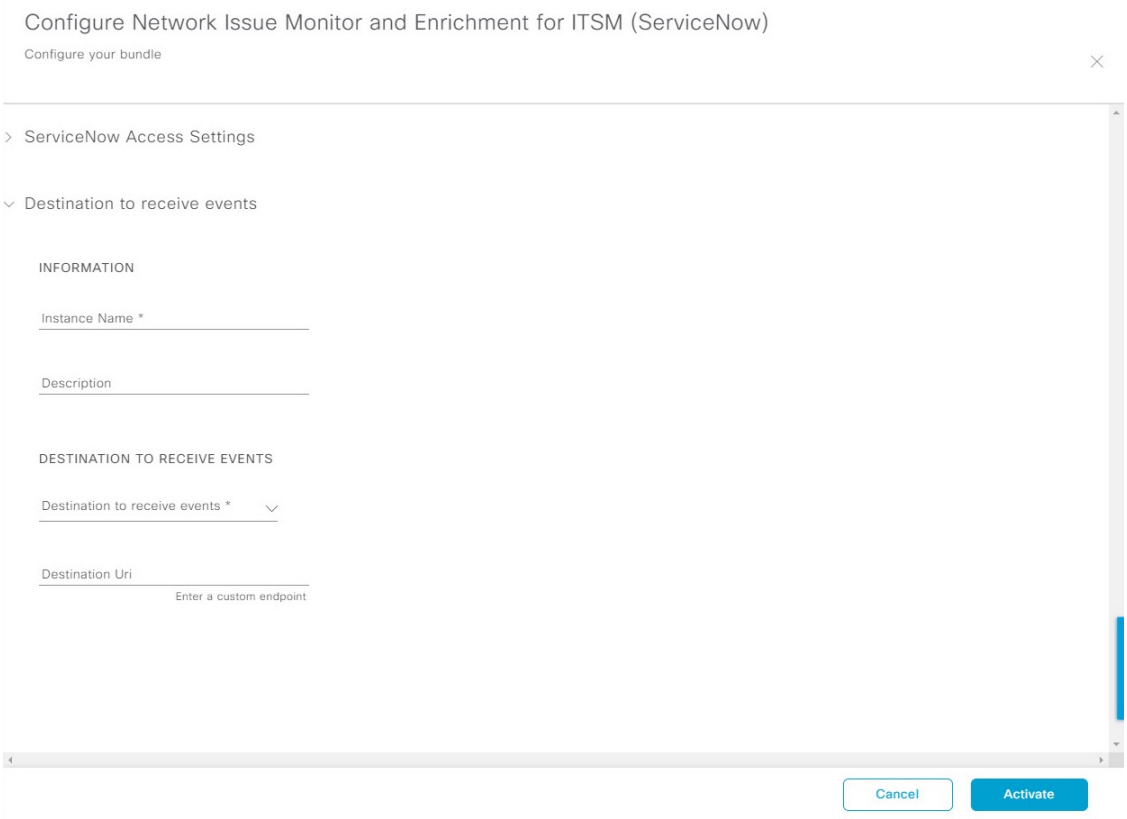
Step 5 In the **Information** field, click **Enable** to confirm enabling the bundle.

Step 6 In the Success message, click **Okay**.

Step 7 Click **Configure** to configure at the bundle level.

Step 8 In the configuration slide-in pane, click **Destination to receive events** to configure a Destination instance.

Figure 3: Example of destination to receive events configuration fields



Note
Use the **Destination to receive events** configuration options for ServiceNow to receive network event and Catalyst Center automation event details in a REST API endpoint and create an incident, problem, or change ticket, based on the configuration chosen by the user in Catalyst Center. For additional information about setting this up with ServiceNow, see the Cisco Catalyst Center ITSM Integration Guide.

Step 9 Click the radio button to configure either an existing Destination instance or configure a new instance.

For configuring an existing Destination instance, choose it from the drop-down list in the window and click **Activate**

Step 10 For configuring a new Destination instance, enter this information:

- **Instance Name**: Name of the instance.
- **Description**: Descriptive text of the instance.
- **Destination to receive events**: Choose one of these options:
  - **Event Management**: When setting up Catalyst Center integration with ServiceNow without using the Cisco Catalyst app, choose the **Event Management** option. The **Event Management** option also requires that you have the Event Management plug-in configured within the ServiceNow instance.
  - **REST API Endpoint**: The **REST API Endpoint** option can be used with the Cisco Catalyst app. Data is sent to a REST API endpoint within the Cisco Catalyst app with the **REST API Endpoint** option.

- **Generic REST Endpoint in ServiceNow**: For the **Generic REST Endpoint in ServiceNow** option, you can send the data to a different staging table in ServiceNow.

For detailed information about integrating Catalyst Center with ServiceNow, see the *Cisco Catalyst Center ITSM Integration Guide*.

- **Destination URI**: Enter a destination Uniform Resource Identifier (URI) for the **Generic REST Endpoint in ServiceNow** option. This field is mandatory for this option.

After entering this information, proceed to the next step.

Step 11 Click **Activate** to save your changes and activate the bundle, or click **Cancel** to cancel the configuration and close the slide-in pane.

Note
By clicking **Activate**, you enable the changes that are made to the bundle and the changes take effect immediately. Additionally, the bundle's status changes from **ENABLED** to **ACTIVE**.

What to do next

To review your configuration, choose **Manage** > **Configurations** > **General Settings** and use the **Filter** or **Find** tools to locate the specific destination instance configured in this procedure.

If necessary, later you can edit, update, or delete the instance in the **General Settings** window. For additional information, see Configure General Settings: edit an instance, on page 129.

Configure bundles: ServiceNow access settings

Do this procedure to configure access settings for ServiceNow within a bundle.

You configure ServiceNow access settings within these bundles:

- **Endpoint Attribute Retrieval with ITSM (ServiceNow)**
- **Network Issue Monitor and Enrichment for ITSM (ServiceNow)**
- **Automation events for ITSM (ServiceNow)**

Before you begin

See the latest *Cisco Catalyst Center ITSM Integration Guide* to understand how this procedure fits within a larger workflow when configuring a Catalyst Center-to-ServiceNow integration.

Procedure

Step 1 From the main menu, choose **Platform** > **Manage** > **Bundles**.

Step 2 Click the **Network Issue Monitor and Enrichment for ITSM (ServiceNow)**, **Automation events for ITSM (ServiceNow)**, or **Endpoint Attribute Retrieval with ITSM (ServiceNow)** bundle link or icon.

Note
For this procedure and as an example, the **Endpoint Attribute Retrieval with ITSM (ServiceNow)** is selected.

This information is provided:

- **General information**: Vendor, version, platform, and tags are displayed under the square icon.

  Note
  Tags indicate what the Catalyst Center component is used for or is affected by the bundle.

- **Information**: Tab that displays general information (purpose of bundle and how bundle works in the network), sample schemas, mapping notes, configuration notes, and other data about the bundle.
- **Contents**: Tab that provides access to information about the integration flows within the bundle.

  Note
  For the **Endpoint Attribute Retrieval with ITSM (ServiceNow)** bundle, access is provided to the **Scheduler for ServiceNow Asset Sync** integration flow.

- **Release Notes**: Tab that displays latest release information about the bundle, including its version.

Step 3 Click each of the preceding tabs and review the information about the bundle.

Step 4 Click **Enable** to activate the link.

Step 5 In the **Information** field, click **Enable** to confirm enabling the bundle.

Step 6 In the success message, click **Okay**.

Step 7 Click the **Contents** tab.

For the **Endpoint Attribute Retrieval with ITSM (ServiceNow)** bundle, a link to the **Scheduler for ServiceNow Asset Sync** integration flow appears. Click the link to do these tasks:

- Review the **Description**, **Tags**, **How to Use this Flow**, and scheduler.
- Click **Run Now** (to run the scheduler now), **Run Later** (to schedule for a later time), or **Recurring** (to set up a recurring schedule).

  For **Run Later**, you must select a date, time, and time zone. For **Recurring**, you must set a repeating interval (daily or weekly), an interval duration (minutes or hours), and a start and end date.

- Click **Schedule** to enable the scheduler.

  Important
  Only configure and enable an integration flow schedule after you have finished configuring the bundle itself as described in these steps. You can configure and enable an integration flow schedule by returning to this view and clicking **Schedule** or by choosing **Platform** > **Developer Toolkit** > **Integration Flows** > **Scheduler for ServiceNow Asset Sync**.

For the other bundles, **Network Issue Monitor and Enrichment for ITSM (ServiceNow)** and **Automation events for ITSM (ServiceNow)**, there is no link to an integration flow. Only information about integration flows is displayed.

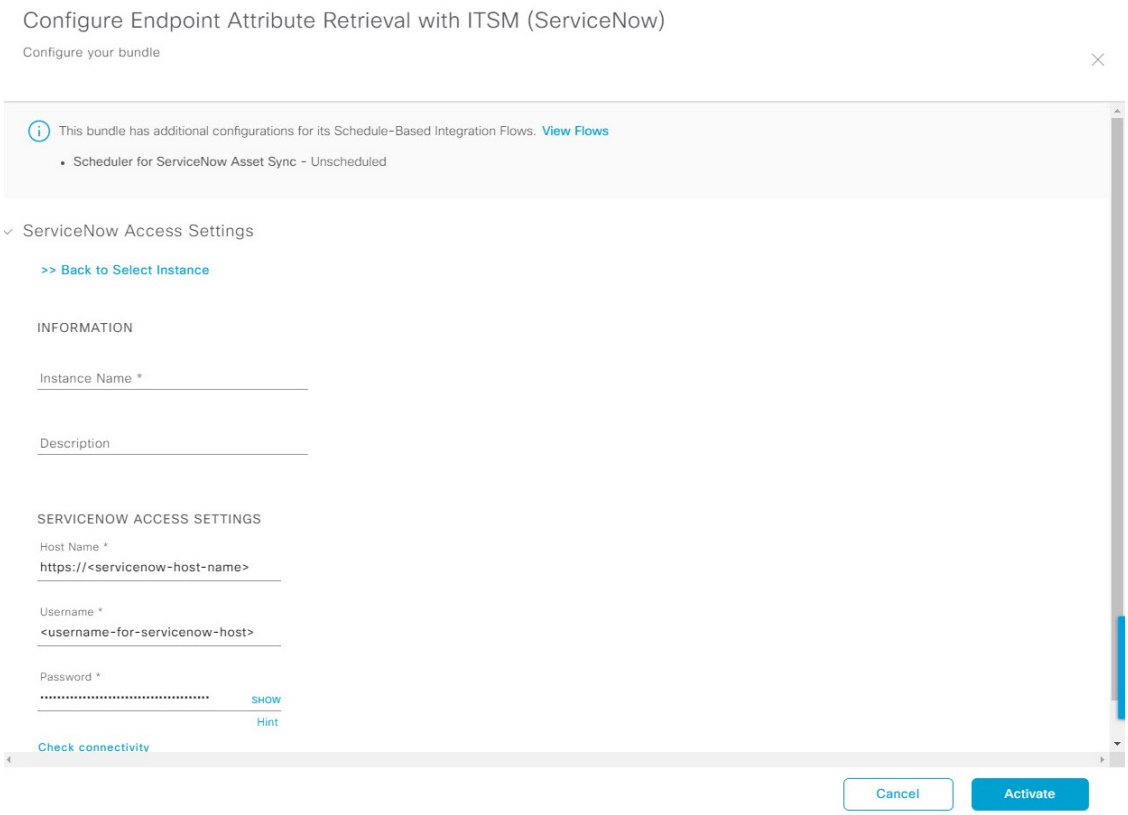
Step 8 Click the **X** icon to close the window and return to the previous bundle window.

Step 9 Click **Configure** to configure at the bundle level.

Step 10 In the configuration slide-in pane, click **ServiceNow Access Settings** to configure a ServiceNow instance.

Step 11 Click the radio button to configure either an existing ServiceNow instance or configure a new instance.

Figure 4: Example of ServiceNow instance configuration fields



To configure an existing ServiceNow instance, choose it from the drop-down list and click **Activate**.

Step 12 To configure a new ServiceNow instance, enter this information:

- **Instance Name**: Name of the instance.
- **Description**: Descriptive text of the instance.
- **Host name**: Hostname for the ServiceNow system.
- **Username**: Username required to access the ServiceNow system.
- **Password**: Password required to access the ServiceNow system.

Step 13 Click **Check Connectivity** to test whether you can connect to the server where the endpoint is located.

After a successful test of connectivity to the server, continue to the next step.

Step 14 Click **Activate** to save your changes and activate the bundle, or click **Cancel** to cancel the configuration and close the slide-in pane.

Note
By clicking **Activate**, you enable the changes that are made to the bundle and the changes take effect immediately. Additionally, the bundle's status changes from **ENABLED** to **ACTIVE**.

What to do next

To review your configuration, choose **Manage** > **Configurations** > **General Settings** and use the **Filter** or **Find** tools to locate the ServiceNow instance configured in this procedure.

If necessary, later you can edit, update, or delete the instance in the **General Settings** window. For additional information, see Configure General Settings: edit an instance, on page 129.

Configure bundles: CMDB data synchronization for ServiceNow

Do this procedure to configure data synchronization between Catalyst Center and ServiceNow (including the option to configure operational and source identifiers) within a bundle.

You configure data synchronization and set the operational limit and identifier for ServiceNow within the **Basic ITSM (ServiceNow) CMDB synchronization** bundle.

Before you begin

See the latest Cisco Catalyst Center ITSM Integration Guide to understand how this procedure fits within a larger workflow when configuring a Catalyst Center-to-ServiceNow integration.

Procedure

Step 1 From the main menu, choose **Platform** > **Manage** > **Bundles**.

Step 2 Click the **Basic ITSM (ServiceNow) CMDB synchronization** bundle link or icon.

This information is provided:

- **General information**: Vendor, version, platform, tags displayed under the square icon.

  Note
  Tags indicate what the Catalyst Center component is used for or is affected by the bundle.

- **Information**: Tab that displays general information (purpose of bundle and how bundle works in the network), sample schemas, mapping notes, configuration notes, and other data about the bundle.
- **Contents**: Tab that accesses the integration flows that make up the bundle, or provides information about the integration flows that make up the bundle.
- **Release Notes**: Tab that displays latest release information about the bundle, including its version.

Step 3 Review the bundle data in the **Information** tab and click the **Contents** tab.

Step 4 Click the **Integration Flows** header.

Review the list of available integration flows (links) under the header. For detailed information about integration flows and their purpose, see Work with integration flows, on page 193.

Step 5 Click **Enable** to activate the links.

Step 6 In the **Information** field, click **Enable** to confirm enabling the bundle.

Step 7 In the success message, click **Okay**.

Step 8 Click the integration flow link to do these tasks:

- Review the **Description**, **Tags**, **How to Use this Flow**, and scheduler.
- Click **Run Now** (to run the scheduler now), **Run Later** (to schedule for a later time), or **Recurring** (to set up a recurring schedule).

  For **Run Later**, you need to select a date, time, and time zone. For **Recurring**, you need to set a repeating interval (daily or weekly), an interval duration (minutes or hours), and a start and end date.
- Click **Schedule** to enable the scheduler.

Important
Only configure and enable an integration flow schedule, after you have finished configuring the bundle itself as described in this procedure. You can configure and enable an integration flow schedule by returning to this view and clicking **Schedule**. Or, click the **View Flows** link in the **Configure Basic ITSM (ServiceNow) CMDB synchronization** slide-in pane (see the next steps). Or, click the menu icon and choose **Platform** > **Developer Toolkit** > **Integration Flows** > **Schedule to Publish Inventory Details-ServiceNow Connector**.

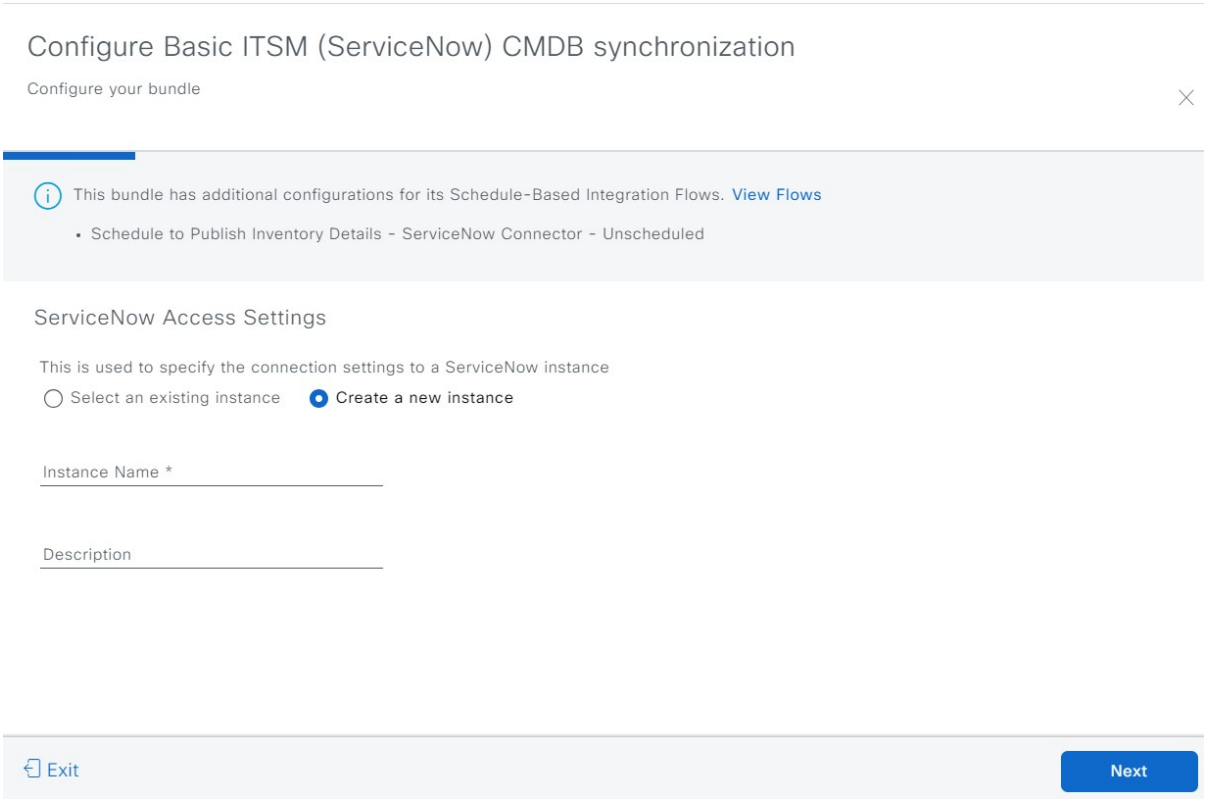
Step 9 Click the **X** icon at the upper right of the window to close it and return to the previous bundle window.

Step 10 Click **Configure** to configure at the bundle level.

A configuration slide-in pane appears. Review the CMDB synchronization information.

Step 11 Click the radio button to configure either existing or new ServiceNow access settings for the CMDB synchronization.

Figure 5: ServiceNow Access Settings



To configure an existing setting, choose it from the drop-down menu in the window and click **Next**.

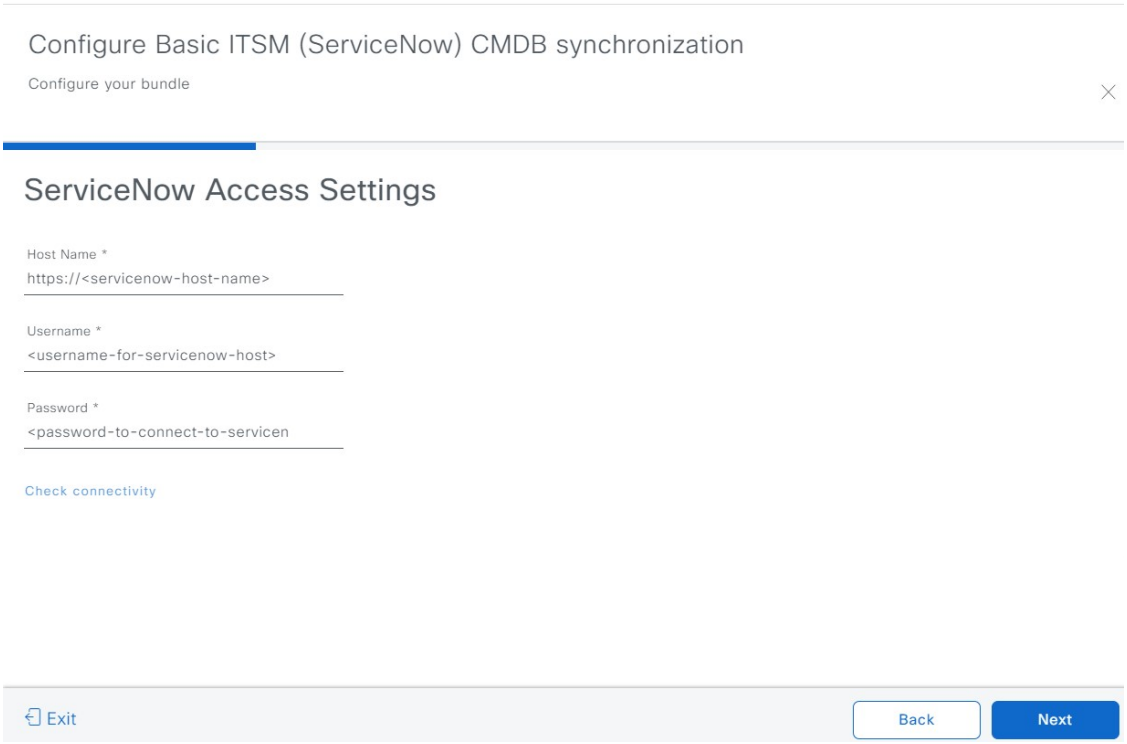
Step 12 To configure a new access setting, enter this instance information:

- **Instance Name**: Name of the instance.
- **Description**: Descriptive text of the instance.

Click **Next**.

Step 13 To configure a new access setting, enter this additional settings information:

Figure 6: ServiceNow Access Settings



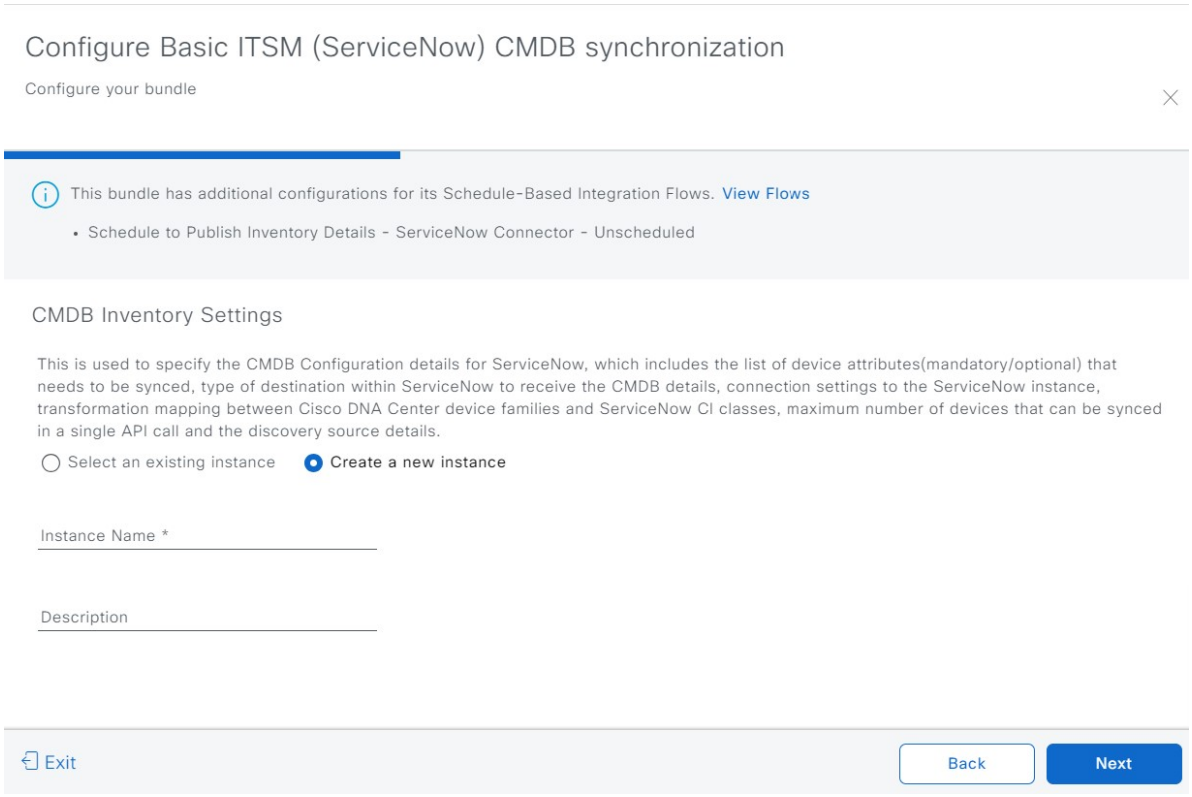
- **Hostname**: Hostname or IP address of the ServiceNow server.
- **Username**: Username for access to the ServiceNow server.
- **Password**: Password for access to the ServiceNow server.

Click **Check Connectivity** to check access to the ServiceNow server.

Click **Next**.

Step 14 Click the radio button to configure either an existing instance or configure a new instance for the CMDB inventory settings.

Figure 7: CMDB Inventory Settings



To configure an existing instance, choose it from the drop-down menu in the window and click **Configure**.

Step 15 To configure a new instance, enter this additional information:

- **Instance Name**: Name of the instance.
- **Description**: Descriptive text of the instance.

Click **Next**.

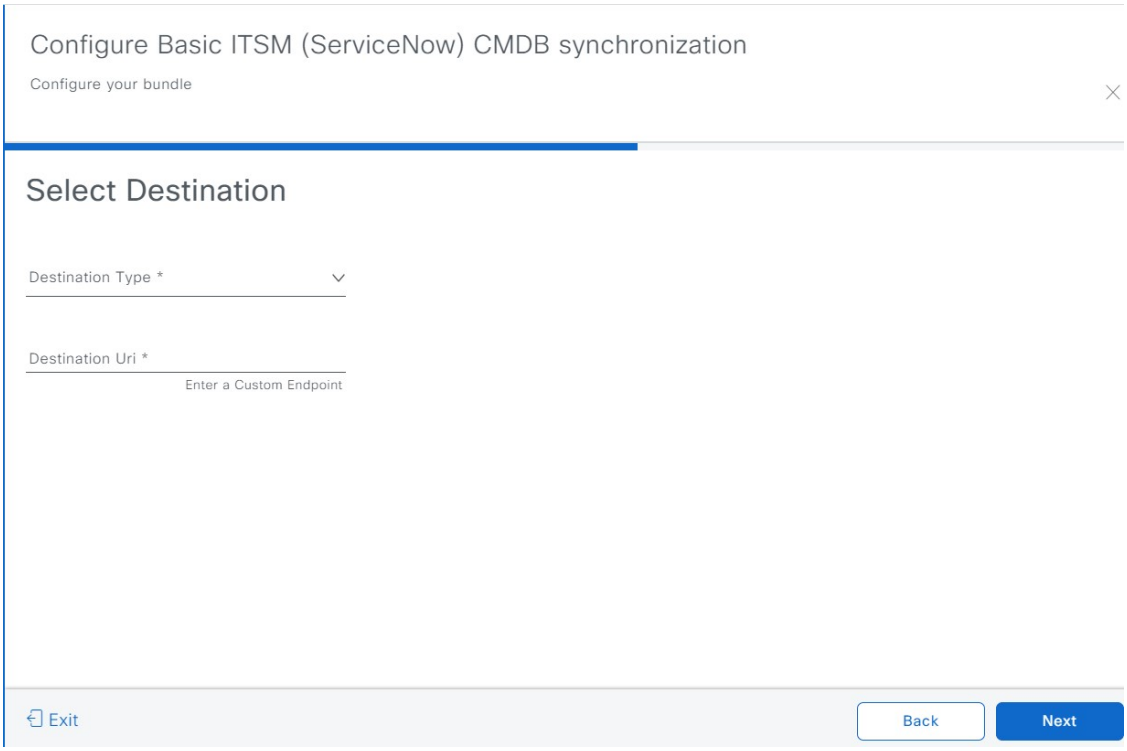
Step 16 In the **Select Destination** window, enter this information:

- **Destination Type**: There are two discovery source options to choose from:
  - **Synchronize device inventory directly with CMDB**
  - **Post device inventory details to a staging table**

  Note
  With a staging table, you can take the values from the table and map it to a ServiceNow CMDB.

- **Destination URI**: Uniform Resource Indicator (URI) of the ServiceNow server (CMDB) or staging table.

Figure 8: Select Destination window



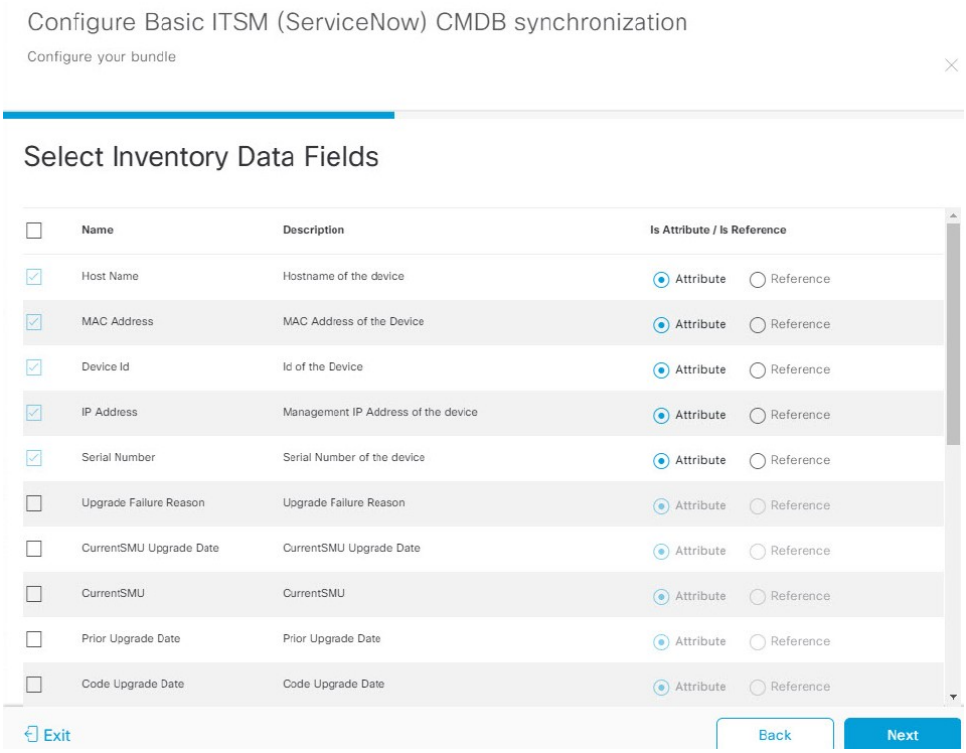
Click **Next**.

Step 17 In the **Select Inventory Data Fields** window, select the inventory data fields to by synchronized.

Note
Inventory data fields are Cisco created data types that can be designated as an attribute or reference to be synchronized into a CMDB or staging table.

Clicking the top check box in the **Select Inventory Data Fields** window will select all of the inventory data fields for synchronization. Click this top check box if you want to sync all of the inventory data fields. Otherwise, review and click a check box at a time to create a smaller subset of inventory data fields for synchronization.

Figure 9: Select Inventory Data Fields window



The **Select Inventory Data Fields** window consists of these columns:

- **Name**: Name of the inventory data field.
- **Description**: Brief description of the inventory data field.
- **Is Attribute/Is Reference**: Whether the inventory data field is an attribute or a reference. A reference data field is used to create a relationship between two tables in a database. An attribute data field is used to add more data to a table in a database.

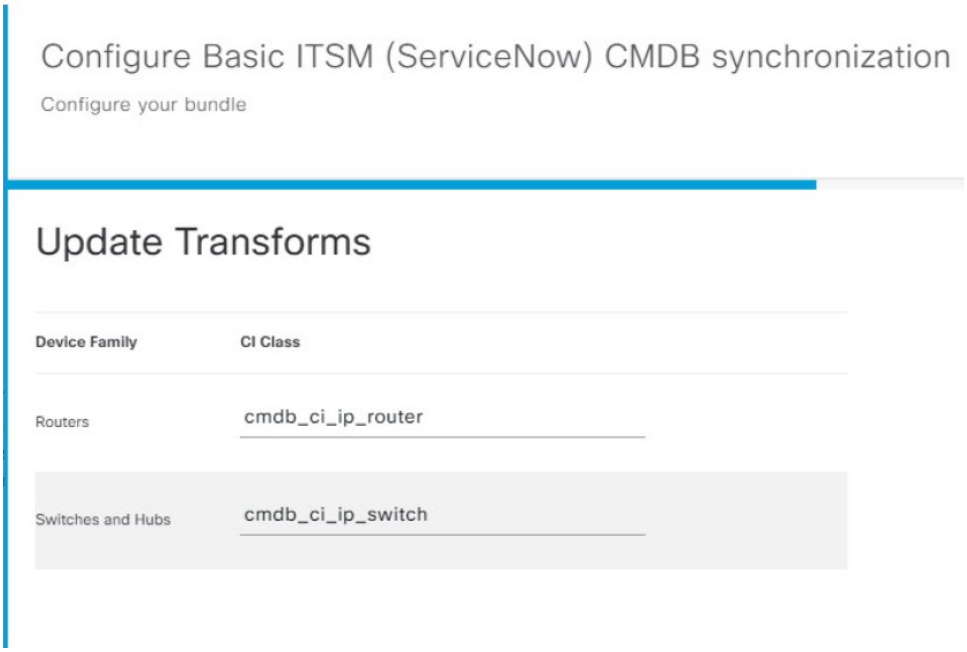
Step 18 For the data fields selected to be synchronized in the preceding step, review their default designation as either an attribute or reference.

To change a data field's default designation, just click the desired data field designation (**Attribute** or **Reference**).

After selecting the data fields to be synchronized and whether the data field is an attribute or reference, click **Next**.

Step 19 In the **Update Transforms** window, either accept or update the ServiceNow transformation mapping between the Catalyst Center device families and the ServiceNow CI classes.

Figure 10: Update Transforms window



Device families are the Catalyst Center device classifications (for example, Unified AP, Routers, Wireless Controller, Switches, and Hubs), where the inventory attributes/references mapping to ServiceNow is already available in the existing Cisco Catalyst application in ServiceNow. The type and number of device families can vary depending upon the different Cisco devices in the user's network.

Note
Catalyst Center platform is able to automatically retrieve all of the device families in the user's Catalyst Center network and display them in this GUI window.

CI classes are the database tables for ServiceNow (for example, cmdb_ci_wap_network, cmdb_ci_ip_router, and cmdb_ci_ip_switchr). The **CI Class** column in the GUI window above is used to map the CI classes to their respective device families.

This table displays the Catalyst Center default CI classes for each device family. The default CI classes can be modified by the user. In case of other device families not listed below, Cisco will not have any default values specified in the **CI Class** column. The ServiceNow application user needs to either manually create the corresponding CI Classes and attributes/references mapping or use a pre-existing CI class a 'parent' CI class.

Table 6: Default device family to CI class mapping list

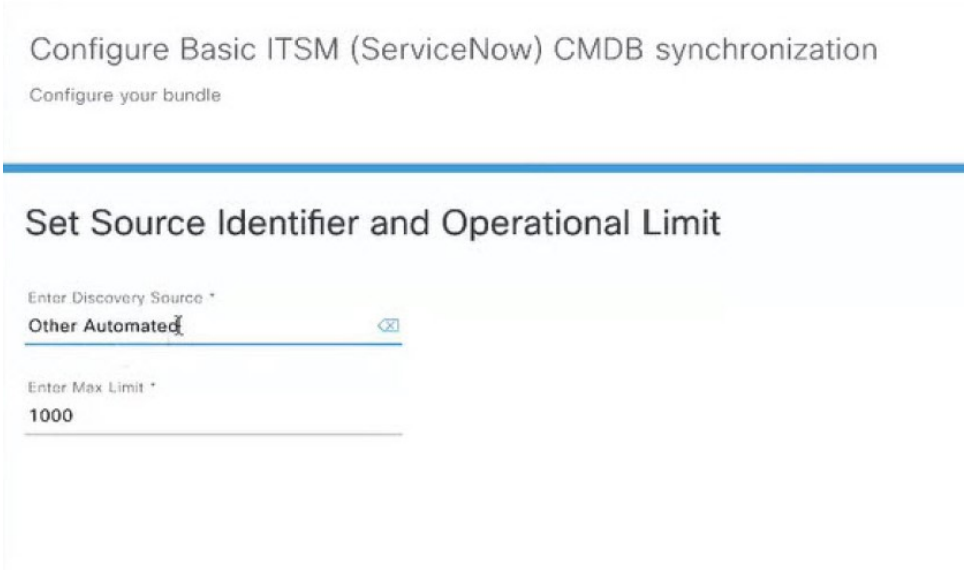
Device family	Corresponding CI class
Unified AP	cmdb_ci_wap_network
Wireless Controller	x_caci_cisco_dna_wireless_lan_controller
Routers	cmdb_ci_ip_router
Switches and Hubs	cmdb_ci_ip_switch
Meraki Access Point	cmdb_ci_wap_network

Device family	Corresponding CI class
Meraki Cameras	cmdb_ci_netgear
Meraki Dashboard	cmdb_ci_netgear
Meraki Security Appliances	cmdb_ci_netgear
Meraki Switches	cmdb_ci_ip_switch

After accepting or updating the information in this window, click **Next**.

Step 20 In the **Set Source Identifier and Operational Limit** window, configure the data source and maximum limit.

Figure 11: Set Source Identifier and Operational Limit window



Configure these values:

- **Enter Discovery Source**: Enter the same value as previously selected or keep the value at its default, **Other Automated**.
  - **Synchronize device inventory directly with CMDB**
  - **Post device inventory details to a staging table**

  Note
  Other Automated is a preconfigured value for the discovery source attribute in an OOB ServiceNow instance. This is the value that indicates the data source from where the ServiceNow CI was discovered. As a default, Cisco uses one of the existing preconfigured values for the integration.

- **Enter the Max Limit**: Maximum number of devices that can be synchronized in an iteration (single API call).

After entering the above information, click **Next**.

Step 21 In the **Summary** window, review the configuration summary.

After reviewing the information, click **Configure**.

For a successful configuration, you receive a **Done! Bundle Configured** message.

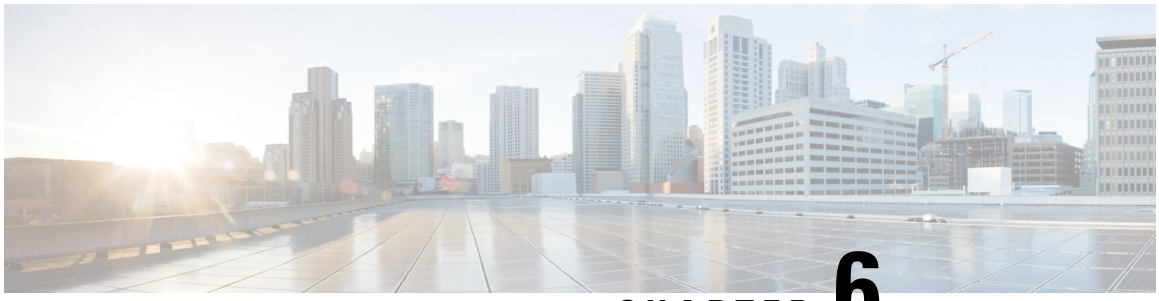
What to do next

Configure the Integration Flow for this bundle (**Schedule to Publish Inventory Details - ServiceNow Connector)**, using one of the preceding methods.

Review your configuration, choose **Manage** > **Configurations** > **General Settings**, and use the **Filter** or **Find** tools to locate the instance configured in this procedure. If necessary, later on you can edit, update, or delete the instance in the **General Settings** window. For additional information, see Configure General Settings: edit an instance, on page 129.

You can test the CMDB synchronization by doing these tasks:

- In the Catalyst Center platform GUI, click the menu icon and choose **Platform** > **Runtime Dashboard** > **Event Summary**. Click **Refresh** to refresh the GUI view. Click the individual events in the window to view the event data and access links to ServiceNow.
- Go to ServiceNow and search for a synchronized device. Check the **Configuration** and **Other Attributes** tabs for the synchronized data in that device's record.



CHAPTER 6

Configurations

- About configurations, on page 127
- Configure event settings, on page 127
- Configure General Settings: edit an instance, on page 129
- Configure General Settings: add an instance, on page 131
- Configure a webhook destination, on page 133
- Configure an email destination, on page 134
- Configure a syslog server destination, on page 135
- Configure a trap notification, on page 136

About configurations

Catalyst Center platform provides you with **Configurations** to configure a customized network experience using these options:

- **Event Settings**: Catalyst Center platform supports specific Cisco Catalyst Assurance events (or incidents) that may occur within your network. This means that Catalyst Center platform can recognize these events and permits you to configure settings that customize the type, category, and severity under which Catalyst Center reports them. Configuring this information in the GUI also permits you to customize the information that Catalyst Center sends to an external system, such as ServiceNow (or perhaps to one or more REST endpoints that you can configure).
- **General Settings**: You can add or edit REST and ITSM endpoint instances within a single or multiple bundles.

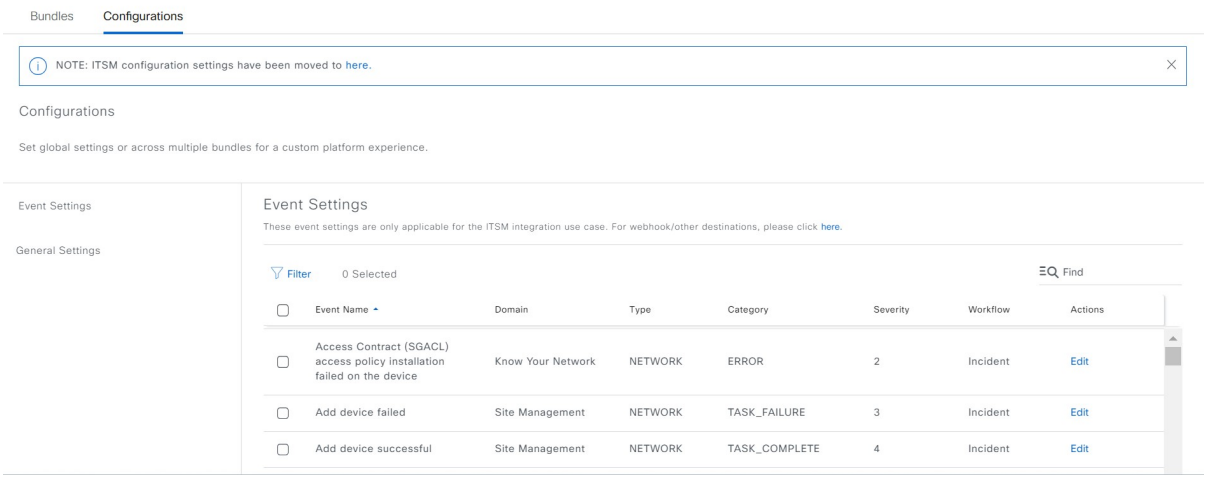
Note You can also configure various types of destinations to deliver the events from the Catalyst Center platform. From the main menu, choose **System** > **Settings** > **External Services** > **Destinations** to access the GUI window to configure a webhook, email, syslog, SNMP trap, or ITSM destination.

Configure event settings

A preset number of issues (or events) that may occur within your network can be found in **Event Settings** in the **Configurations** window. You can configure the type, category, severity, and workflow of these events.

Note The **Event Settings** window functionality is only applicable for an ITSM (ServiceNow) integration and not for generic event notifications. For guidance about how to use this procedure within a larger set of procedures to configure ITSM integration between Catalyst Center and ServiceNow, see the Cisco Catalyst Center ITSM Integration Guide. See the text at the top of this window and click the link (**here**) to access the **Events** window in platform, where you can subscribe to events and receive notifications by email, webhook (REST API), SNMP trap, or syslog server.

Figure 12: Event Settings window



Procedure

Step 1 From the main menu, choose **Platform** > **Manage** > **Configurations** > **Event Settings**.

Step 2 Review the **Event Settings** table that appears.

This **Event Settings** information displays:

- **Event Name**: Name of the Catalyst Center event.
- **Domain**: Domain of the Catalyst Center event.
- **Type**: Network, App, System, Security, or Integrations type of event.
- **Category**: Error, Warn, Info, Alert, Task Progress, Task Complete.
- **Severity**: 1 through 5.

  Note
  Severity 1 is the most important or critical priority and should be assigned as such.

- **Workflow**: Incident, Problem, Event, or RFC.
- **Actions**: Edit.

You can adjust what displays in the table by clicking the **Filter** icon and using the filter, or by typing a keyword in the **Find** field. For example, to display all access point notifications, type 'AP' in the **Find** field. To view all network notifications, type 'Network' in the **Find** field. To view all severity 1 notifications, type '1' in the **Find** field.

You can edit the event, so that its notification is customized to your network standards and conventions.

Step 3 Click **Edit** in the **Actions** column to edit an event.

Choose a setting by clicking on the downward pointing angle and adjust the value. For example, click **Network** and adjust to **App**. This changes the event type from a network type to an application type. Click **Severity** and adjust to **1** from **5**. This raises the severity level from 5 to 1.

Step 4 Click the box next to the event name to enable notifications.

This enables notifications through Catalyst Center when the event occurs in the future.

Step 5 Click **Save** to save your configuration.

What to do next

- From the main menu, choose **Platform** > **Runtime Dashboard**.

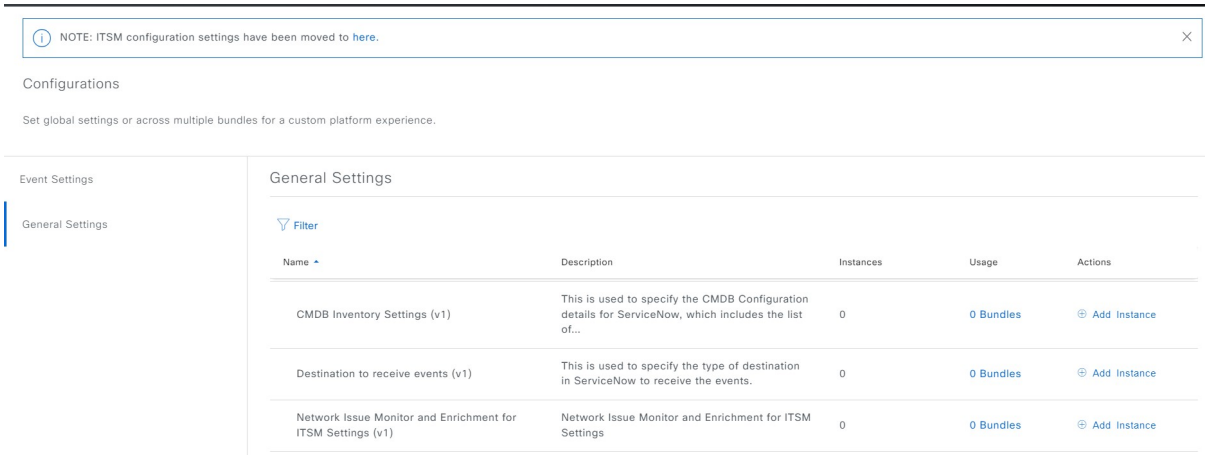
  Notifications for events display in the **Events Summary** field.

- Click **View Details** to view the notifications.

Configure General Settings: edit an instance

You can edit an instance within a single or multiple bundles using **Configurations**.

Figure 13: Catalyst Center platform Configurations window



Before you begin

Enable, configure, and activate the bundles for your network in **Bundles**. For information about **Bundles** see Bundle features, on page 110.

Procedure

Step 1 From the main menu, choose **Platform** > **Manage** > **Configurations** > **General Settings**.

Step 2 Review the **General Settings** table that appears.

This **General Settings** information displays:

- **Name**: Name of the instance and version.
- **Description**: Description of the settings that contain the instances.
- **Instances**: Number of instances currently configured.
- **Usage**: Number of bundles where the instance or instances are used.
- **Actions**: Specific task that you could do for the setting (for example, edit or add an instance for the setting).

You can adjust what displays in the table by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

Step 3 Click the arrow for one of the displayed instances. For example, click the **CMDB Synchronization Settings (v1)** or **Destination to Receive Events (v1)** arrow.

The list of instances for that setting displays.

Step 4 In the **Usage** column, hover your mouse pointer over **Bundles**.

Catalyst Center displays the bundles that use the specified instance.

Step 5 Click the **Edit** icon ('Pad and Pen' icon) in the **Actions** column to edit an existing instance.

Edit the appropriate instance for your requirements in these steps.

Step 6 (Optional) To edit the CMDB synchronization details for a **CMDB Synchronization Settings** instance, choose **Edit** > **Actions** and edit one or more of these instance fields in the slide-in panes that appear:

- **ServiceNow Access Settings**: Select an instance from the drop-down menu.
- **CMDB Inventory Settings**: Enter an **Instance Name** and **Description**.
- **Select Destination**: Enter **Destination Type** and **Destination URI**. Options include **Synchronize device inventory directly with CMDB** or **Post device inventory details to a staging table**.
- **Select Inventory Data Fields**: Select both the Inventory Data Fields to synchronize, as well as whether the data field is an attribute or reference.
- **Update Transforms**: Accept or update the CI class to the device family.
- **Set Source Identifier and Operational Limit**: Configure the discovery source and maximum limit.
- **Summary**: Review the configuration and make any changes before saving.

Step 7 (Optional) To edit a **Destination to receive events** instance, choose **Edit** > **Actions** and edit one or more of these fields in the slide-in pane:

- **Instance Name**: Name of instance.

- **Description**: Description of instance.
- **Destination to Receive Events**: Choose one of these options:
  - **Event Management**: When setting up Catalyst Center integration with ServiceNow without using the Cisco Catalyst app, choose the **Event Management** option. The **Event Management** option also requires that you have the Event Management plugin configured within the ServiceNow instance.
  - **REST API Endpoint**: The **REST API Endpoint** option can be used with the Cisco Catalyst app. Data is sent to a REST API endpoint within the Cisco Catalyst app with the **REST API Endpoint** option.
  - **Generic REST Endpoint in ServiceNow**: For the **Generic REST Endpoint in ServiceNow** option, you can send the data to a different staging table in ServiceNow.
- **Destination URI**: Enter a destination URI for the **Generic REST Endpoint in ServiceNow** option. This field is mandatory for this option.

For detailed information about integrating Catalyst Center with ServiceNow, see the Cisco Catalyst Center ITSM Integration Guide for this release.

Step 8 Click **Update** to save your edits to the instance.

The edits to the instance immediately take effect.

Configure General Settings: add an instance

You can add an instance within a single or multiple bundles using **Configurations**.

Before you begin

Enable, configure, and activate the bundles for your network in **Bundles**. For information about **Bundles** see Bundle features, on page 110.

Procedure

Step 1 From the main menu, choose **Platform** > **Manage** > **Configurations** > **General Settings**.

Step 2 Review the **General Settings** table that appears.

This **General Settings** information displays:

- **Name**: Name of the instance and version.
- **Description**: Description of the settings that contain the instances.
- **Instances**: Number of instances in setting.
- **Usage**: Number of bundles where the instance or instances are used.
- **Actions**: Specific task that you could perform for the setting (for example, edit or add an instance for the setting).

You can adjust what displays in the table by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

Step 3 Click the arrow for one of the displayed instances. For example, click the **CMDB Synchronization Settings (v1)** or **Destination to Receive Events (v1)** arrow.

The list of instances for that setting displays.

Step 4 In the **Usage** column, hover your mouse pointer over **Bundles**.

Catalyst Center displays the bundles that use the specified instance.

Step 5 Click the **Add Instances** link in the **Actions** column to add an instance.

Add the appropriate instance or instances for your requirements in these steps.

Step 6 (Optional) To add a **CMDB Synchronization Settings** instance, click **Add Instance** in the **Actions** column and enter these instance fields in the slide-in panes that appear:

- **ServiceNow Access Settings**: Select an instance from the drop-down menu.
- **CMDB Inventory Settings**: Enter an **Instance Name** and **Description**.
- **Select Destination**: Enter **Destination Type** and **Destination URI**. Options include **Synchronize device inventory directly with CMDB** or **Post device inventory details to a staging table**.
- **Select Inventory Data Fields**: Select both the Inventory Data Fields to synchronize, as well as whether the data field is an attribute or reference.
- **Update Transforms**: Accept or update the CI class to the device family.
- **Set Source Identifier and Operational Limit**: Configure the discovery source and maximum limit.
- **Summary**: Review the configuration and make any changes before saving.

Step 7 (Optional) To add a **Destination to receive events** instance, click **Add Instance** in the **Actions** column and enter these instance fields in the slide-in pane:

- **Instance Name**: Name of instance.
- **Description**: Description of instance.
- **Destination to Receive Events**: Choose one of these otpions:
  - **Event Management**: When setting up Catalyst Center integration with ServiceNow without using the Cisco Catalyst app, choose the **Event Management** option. The **Event Management** option also requires that you have the Event Management plug-in configured within the ServiceNow instance.
  - **REST API Endpoint**: The **REST API Endpoint** option can be used with the Cisco Catalyst app. Data is sent to a REST API endpoint within the Cisco Catalyst app with the **REST API Endpoint** option.
  - **Generic REST Endpoint in ServiceNow**: For the **Generic REST Endpoint in ServiceNow** option, you can send the data to a different staging table in ServiceNow.
- **Destination URI**: Enter a destination URI for the **Generic REST Endpoint in ServiceNow** option. This field is mandatory for this option.

For detailed information about integrating Catalyst Center with ServiceNow, see the *Cisco Catalyst Center ITSM Integration Guide* for this release.

Step 8 Click **Add** to save your instance addition.

The additions to the instance take effect immediately.

Configure a webhook destination

Catalyst Center supports a webhook destination for both events and reports.

To configure a webhook destination for events or reports, do these steps using the Catalyst Center GUI.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **External Services** > **Destination** > **Webhook**.

Step 2 Review the **Webhook** tab.

These fields display:

- **Name**: Name of the webhook.
- **Description**: Description (user provided) of the webhook.
- **URL**: URL of webhook (callback URL).
- **Method**: REST API method of webhook (POST).
- **Edit**: Link that opens field to edit the configured webhook fields. After editing the webhook configuration, click **Update** to save your changes.

For this release, you can configure an IPv6 value for the URL.

Step 3 Click **Add** to configure a webhook.

An **Add Webhook** slide-in pane is displayed.

Step 4 Enter values in the fields in the **Add Webhook** slide-in pane to configure the webhook.

- **Name**: Name of the webhook.
- **Description**: Description of the webhook.
- **URL**: URL address of the webhook (callback URL).

Step 5 Depending upon your webhook configuration, choose whether a trust certificate is associated with the webhook URL.

For the **Trust Certificate** radio button, click **Yes** or **No**.

Step 6 Depending upon your webhook configuration, choose the authentication type associated with your webhook URL.

For the **Authentication** radio button, choose one of these options:

- **Basic**: Authentication where the client sends HTTP requests with an Authorization header that contains the word **Basic**, followed by a space and a base64-encoded string *username:password*. If you select **Basic** in the GUI, the **Header Key** field is automatically populated with the **Authorization** value.

- **Token**: Authentication where users are authenticated using a security token that is provided by the server. If you select **Token**, the **Header Key** field below enters the value **X-Auth-Token**.
- **No Authentication**: No authentication needed.

Step 7 Under **Headers**, enter values for the **Header Name** and **Header Value**.

Click **Add** to add the header name and value.

Note
Depending on the type of authentication you chose, header names and values may be automatically populated.

Step 8 Click **Save** to save your webhook destination configuration.

What to do next

Configure a webhook destination for either an event or a report. For information about the procedures to configure an event or a report using the webhook destination, see Work with event notifications, on page 195 and Run your first report, on page 140.

Configure an email destination

Catalyst Center supports email notification for both events and reports.

Note
- For the emails to have the correct Catalyst Center hyperlink, enter the IP address or hostname of Catalyst Center in the **Integrations Settings** window. To enter this information using the GUI, click the menu icon and choose **System** > **Settings** > **System Configuration** > **Integration Settings**. For more information, see Configure integration settings, on page 102.
- If an email destination is already configured with a username and password, when you navigate to **System** > **Settings** > **External Services** > **Destinations** > **Email**, the password field is blank for security reasons. You can update the password or leave the window without changing the password.

You must have the appropriate permissions to perform the tasks described in this procedure. For information about role-based access control for the Catalyst Center platform, see Supporting Role-Based Access Control, on page 104.

Follow these steps to configure an email destination for events or reports using the Catalyst Center GUI.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **External Services** > **Destinations** > **Email**.

Step 2 Configure the required **Primary SMTP Server** fields:

- **Hostname/IP**: Enter the Hostname or IP address of the primary SMTP server.
- **Type**: Select the protocol type from the drop-down list.

- **Port**: Select the port number of the server form the drop-down list.

  Note
  The default port number is 25.

- **Username**: Enter the username for authenticating the primary SMTP server.
- **Password**: Enter the password for authenticating the primary SMTP server.

Step 3 Configure the optional **Secondary SMTP Server** fields:

- **Hostname/IP**: Enter the Hostname or IP address of the secondary SMTP server.
- **Type**: Select the protocol type from the drop-down list.
- **Port**: Select the port number of the server form the drop-down list.

  Note
  The default port number is 25.

- **Username**: Enter the username for authenticating the secondary SMTP server.
- **Password**: Enter the password for authenticating the secondary SMTP server.

Step 4 Configure the **Senders and Receivers** test email fields:

- **From**: Sender of the test email.
- **To**: Recipient of the test email.
- **Subject**: Enter text (up to a maximum of 200 characters) for a subject line for the test email.

Step 5 To test the email configuration, click **Test**.

After you click **Test**, a test email is sent using the parameters that you configure (for both primary and secondary SMTP server settings with Catalyst Center **SMTP configuration test email** as the subject line). A success (configuration validation) or failure message appears based on the test email connectivity results.

Step 6 To save the configuration, click **Save**.

To cancel the configuration, click **Cancel**.

What to do next

Configure an email destination for either an event or a report. For information, see Work with event notifications, on page 195 and Run your first report, on page 140.

Configure a syslog server destination

Catalyst Center supports a syslog server destination for event notifications.

Follow these steps to configure a syslog server destination for event notifications using the Catalyst Center GUI.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **External Services** > **Destination** > **Syslog**.

Step 2 Review the **Syslog** tab.

These fields appear:

- **Name**: Name of the syslog server.
- **Description**: Description of the syslog server.
- **Hostname/IP**: Hostname or IP address of the syslog server.
- **Port**: Port number of the syslog server.
- **Protocol**: Either TCP or UDP protocol.

Step 3 To configure a syslog server, click the **Addition** icon (+).

Step 4 In the **Name** field, enter a name for the syslog server.

Step 5 In the **Description** field, enter a brief description of the syslog server.

Step 6 In the **Hostname/IP Address** field, enter a hostname or IP address.

Step 7 In the **Port** field, enter a port number.

Step 8 In the **Protocol** field, select a protocol from the drop-down list.

Step 9 (Optional) To test out the configuration, click **Validate**.
After your configuration succeeds, a validation message appears.

Step 10 To save your syslog server destination configuration, click **Save**.

To cancel your configuration, click **Cancel**.

What to do next

Configure a syslog server destination for an event notification. For information, see Work with event notifications, on page 195.

Configure a trap notification

Catalyst Center supports SNMP trap event notifications.

Follow these steps to configure SNMP trap event notifications using the Catalyst Center GUI.

Procedure

Step 1 From the main menu, choose **System** > **Settings** > **External Services** > **Destination** > **SNMP**.

Step 2 Review the **SNMP** window.

Step 3 Click **Add** to configure a trap.

Step 4 Configure these fields:

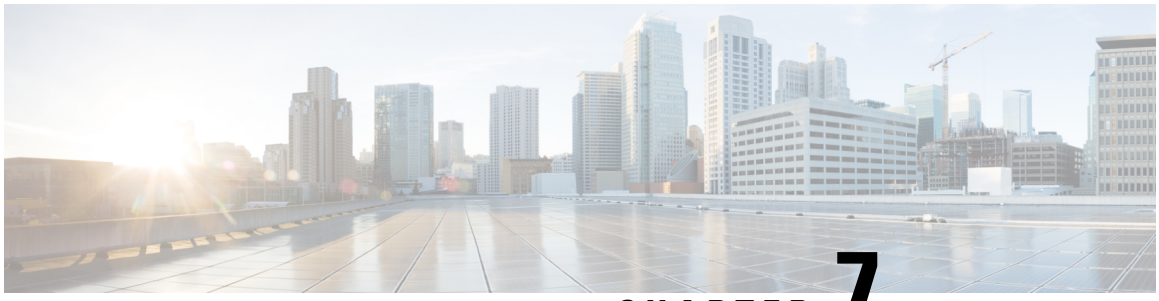
- **Name**: Name of the event.
- **Description**: Word or phrase about the event.
- **Hostname/IP Address**: Enter the hostname or IP address for the SNMP trap receiver (server).

  You can configure an IPv6 value for the **Hostname/IP address**.
- **Port**: Enter the port number for the SNMP trap receiver (server).
- **SNMP Version**: Select the SNMP version from the drop-down list:
  - **SNMP V2C**: For SNMP Version 2C, enter the community string.
  - **SNMP V3**: For SNMP Version 3, enter these additional information:
    - **Username**
    - **Mode**: Select a mode from the drop-down list.
      - For **No Authentication, No Privacy** selection, no further configuration is required.
      - For **Authentication, No Privacy**, configure the Authentication Type (SHA or MD5), Authentication Password, and Confirm Authentication Password.
      - For **Authentication and Privacy**, configure the Authentication Type (SHA or MD5), Authentication Password, Confirm Authentication Password. Additionally, configure the Privacy Type (AES128, DES), Privacy Password, and Confirm Privacy Password.

Step 5 Click **Save**.

What to do next

Access the **Event Notifications** window to select one or more events and subscribe to the configured SNMP trap destination. From the main menu, choose **Platform** > **Developer Toolkit** > **Event Notifications**. Select an event that supports subscription to an SNMP trap destination (SYSTEM type event) and subscribe.



CHAPTER 7

Reports

- About reports, on page 139
- Run your first report, on page 140
- Run an access point report, on page 143
- Run an audit log report, on page 146
- Run a client report, on page 149
- Run a compliance report, on page 152
- Run a configuration archive report, on page 155
- Run an end-of-life report, on page 157
- Run an executive summary report, on page 160
- Run an inventory report, on page 163
- Run a licensing report, on page 166
- Run a network devices report, on page 169
- Run a rogue and aWIPS report, on page 172
- Run an ROI report, on page 175
- Run a security advisories report, on page 177
- Run a SWIM report, on page 180
- Generate a flexible report, on page 183
- View generated reports, on page 187

About reports

Use data from the **Reports** feature to gain insights into your network and its operation. You can customize data and reports using various formats and flexible scheduling options to meet your operational needs.

The **Reports** feature supports these use cases:

- Capacity planning: Understand how your network devices are used in the application.
- Change of pattern: Track changes in usage pattern trends, including clients, devices, bands, or applications on the network.
- Operational reporting: Review reports about network operations, such as upgrade completions or provisioning failures.
- Network health: Use reports to determine the overall health of your network.

Note Each report has a specific maximum row limit. If you try to generate a report that exceeds this limit, you will receive a notification in the GUI and must reduce the report's scope to proceed.

Run your first report

Follow this procedure to begin running specialized data reports about your network.

Before you begin

Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

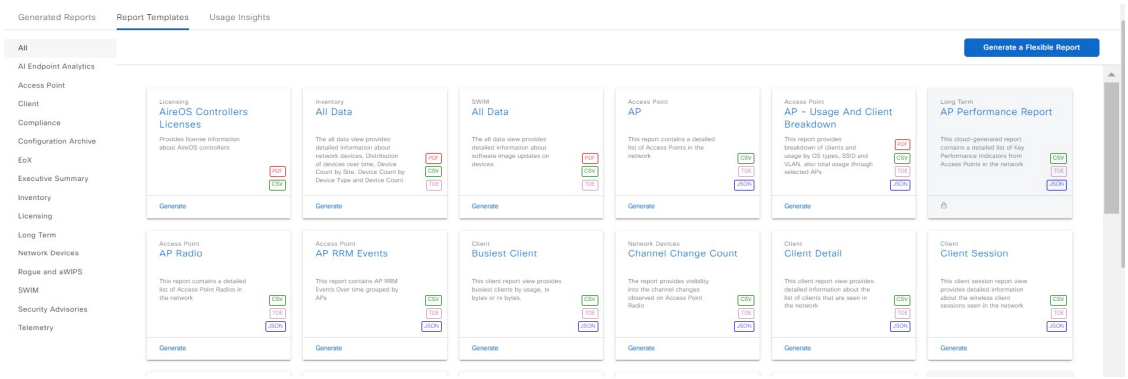
Procedure

Step 1 From the main menu, choose **Reports**.

Step 2 In the **Run Your First Report** window, click **Start**.

The **Report Templates** window displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

Figure 14: Report Templates window



Note
Available options depend on the type of report selected.

Step 3 After clicking a link, review the **Report Templates** window for the selected category.

Each tile represents a template and contains information about the report and links to generate a report. Determine which template you want to use to generate a report. Within each tile are icons that represent the supported file types for the reports (PDF, CSV, TDE, or JSON).

Step 4 In the tile, click the header to view a sample report.

A **Preview** window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report displaying this data:

- Applied filters (data filters that are used in building the report).
- Data metrics and summaries.
- Graphical representation of the data (including line, bar, and pie graphs).
- Tables that assist you in analyzing data.

Note
You can use the sample report to plan how you want your report to look.

Step 5 Click **X** to close the preview.

Step 6 In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window lets you choose a format type for the report, apply data filters for your reports, and set up schedules for the actual report generation.

Step 7 In the **Generate a New Report** window, click **Let's Do It** to get started with the wizard.

Alternatively, click the menu icon and choose **Workflows** > **Generating a New Report** to launch the wizard for generating a new report.

Step 8 In the **Select Report Template** window, select the template for the report.

The **Template** consists of the individual report types within the categories for the release. You can review an autogenerated sample in the same window.

Click **Next**.

Step 9 In the **Setup Report Scope** window, enter a name for the report and select scope.

Enter a report name in the **Report Name** field and click the **Scope** field to display the available filter. Click the filter options that you want for the report.

Note
The **Setup Report Scope** options change depending upon the selected **Template Group**.

Click **Next**.

Step 10 In the **Select File Type** window, select the file type for the report.

Depending on the report that you are creating, these **File Type** options are available:

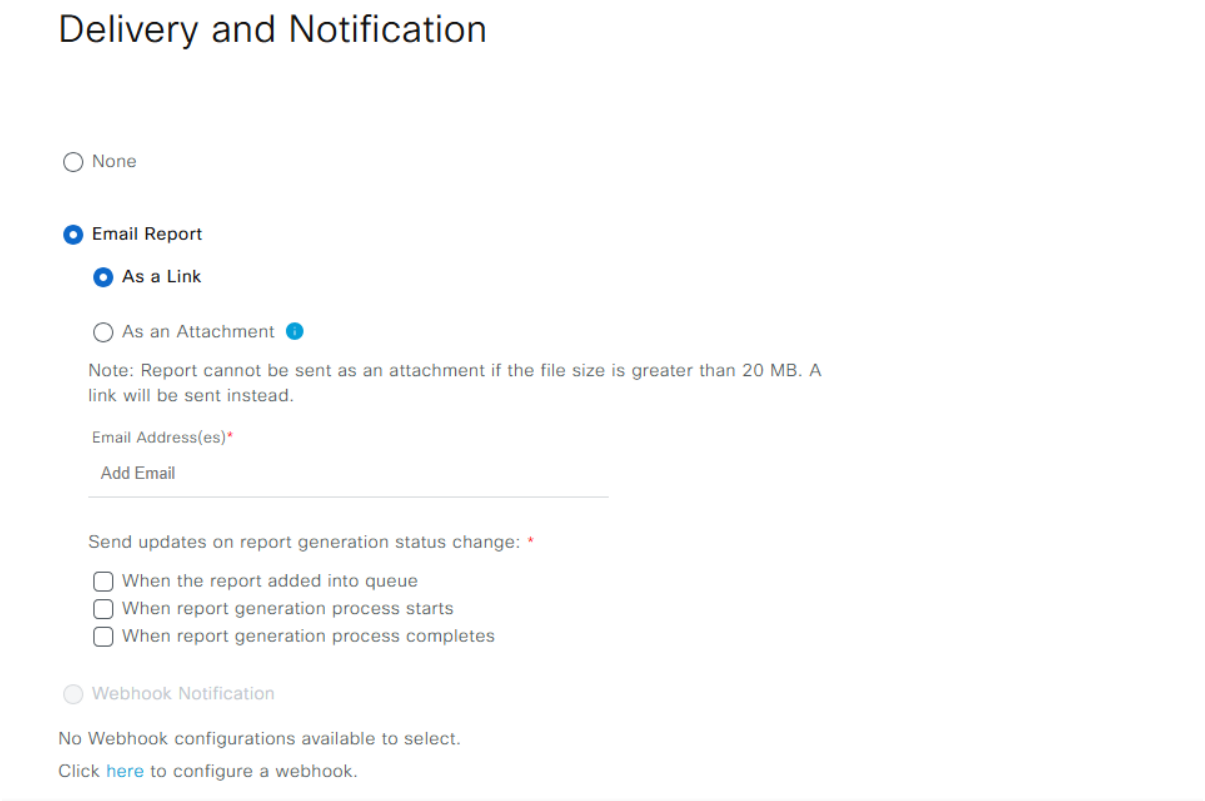
- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, use the **Fields** option to select attributes for the CSV, JSON, and Tableau Data Extract results.

Step 11 In the **Schedule Report** window, select the schedule for the report. Then, click **Next**.

Step 12 In the **Delivery and Notification** window, select the delivery mechanism for the report.

Figure 15: Delivery and Notification window



- **None**: No email or webhook notifications sent.
- **Email Report**: Receive the email report as a link or attachment.

  Note
  If you have not yet configured an SMTP server for the emails, you are prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Choose **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** window under **Reports**. You can view and download the report from this link and location.

    Note
    Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **Attachment**: The Report is attached to the email notification.

    Note
    PDF reports support email notification attachments of up to 20 MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

Catalyst Center sends these email notifications for the report:

- Report is in the queue waiting to be processed.
- Report processing is in progress.
- Report has successfully been compiled and is completed.

To reduce the number of notifications, you can uncheck the preceding check boxes, as needed.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list (**Subscription Profile** field).

  Note
  If you have not yet created a webhook, you are prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

  You will receive the status for the report in the form of webhook notifications like "In Queue", "In Progress", and "Success". You can also view these notifications in the GUI.

Step 13 In the **Summary** window, review the configuration and edit any of the files, if necessary.

Click **Generate Report**.

After report generation, a success window appears.

Step 14 Click the **View all Reports** link.

The **Generated Reports** window shows instance details of the scheduled report.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View generated reports, on page 187.

Run an access point report

Do this procedure to configure **Access Point** (AP) reports for your network.

Before you begin

Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

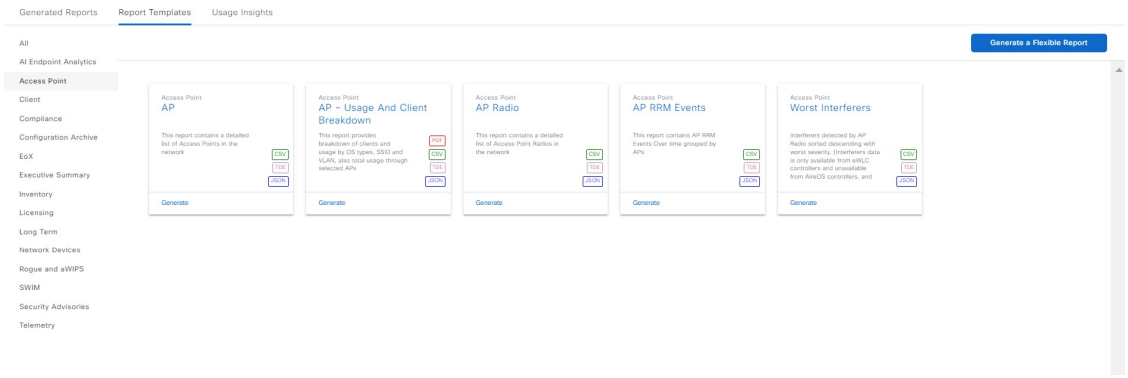
Procedure

Step 1 From the main menu, choose **Reports** > **Report Templates**.

The **Report Templates** window displays the supported reporting categories. A link represents each category. Click a link to view the supported reports for the selected category.

Step 2 After clicking a link, review the **Report Templates** window for the selected category.

Figure 16: AP report



Each template is represented by a tile and contains information about the report and links to generate a report. Determine the template that you want to use to generate a report.

Step 3 In the tile, click the header to view a sample report.

A window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report.

Note
You can use the sample report to plan how you want your report to look.

Step 4 Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window lets you choose a format type for the report, apply data filters for your reports, and set up schedules for the actual report generation.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

To skip this screen in the future, check the **Don't show this to me again** check box.

Step 7 In the **Select Report Template** window, choose the template from **Template** drop-down list.

Note
The **Template** consists of the individual report types within the category for the release.

You can review an auto-generated sample in the same window.

Step 8 Click **Next**.

Step 9 In the **Setup Report Scope** window, name the report, choose the scope and choose the time range.

Enter a report name in the **Report Name** field and click **Scope** to display the available filter. Click the filter options that you want for the report and select the **Time Range**.

Note
The **Setup Report Scope** options change depending on the selected **Template**. The AP reports support up to 90 days of data retention.

Step 10 Click **Next**.

Step 11 In the **Select File Type** window, choose the file type for the report.

Depending on the report that you are creating, these **File Type** options may be available:

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option lets you choose attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Step 12 Click **Next**.

Step 13 In the **Schedule Report** window, choose the schedule for the report. Then, click **Next**.

Step 14 In the **Delivery and Notification** window, choose the delivery mechanism for the report:

- **None**: No email or webhook notifications sent.
- **Email Report**: Email report is sent as a link or attachment.

  Note
  If you have not yet configured an SMTP server for the emails, you are prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Choose **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **As a Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** window under **Reports**. You can view and download the report from this link and location.

    Note
    Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **As an Attachment**: Report is attached to the email notification.

    Note
    PDF reports support email notification attachments of up to 20 MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  Catalyst Center sends these email notifications for the report:

  - Report is in the queue waiting to be processed.
  - Report processing is in progress.
  - Report has successfully been compiled and is completed.

  To reduce the number of notifications, you can uncheck the preceding check boxes, as desired.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Choose a webhook from the drop-down list **(Subscription Profile** field).

  Note

If you have not yet created a webhook, you are prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

Catalyst Center sends these status webhook notifications for the report:

- In Queue
- In Progress
- Success

Step 15 Click **Next**.

Step 16 In the **Summary** window, review the configuration and edit any of the files, if necessary.

Click **Generate Report**.

After the report is generated, a success window appears.

Step 17 Click the **View the Generated Reports** link.

The **Generated Reports** window shows instance details of the report that was scheduled.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View generated reports, on page 187.

Run an audit log report

Follow this procedure to configure **Audit Log** reports for your network.

Before you begin

Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

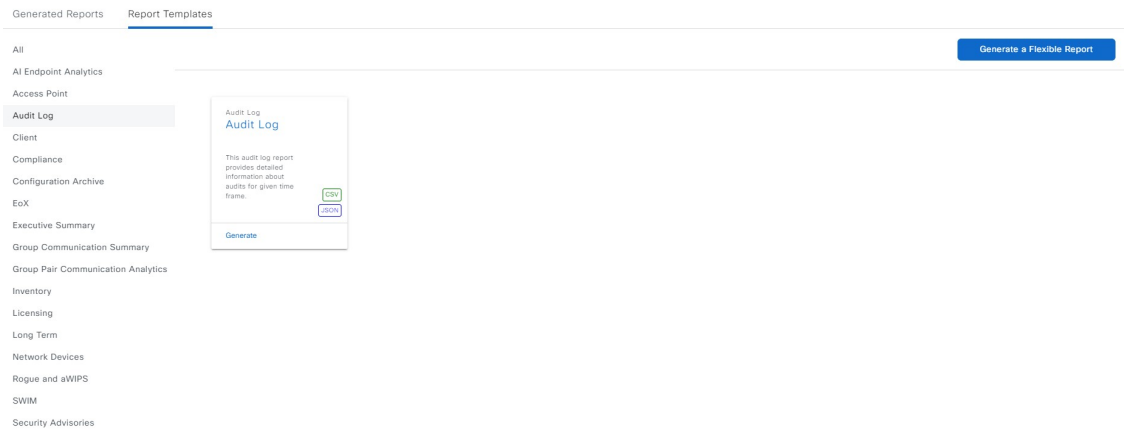
Procedure

Step 1 From the main menu, choose **Reports** > **Report Templates**.

The **Report Templates** window displays the supported reporting categories. A link represents each category. Click a link to view the supported reports for the selected category.

Step 2 After clicking a link, review the **Report Templates** window for the selected category.

Figure 17: Audit Log report



Each template is represented by a tile and contains information about the report and links to generate a report. Determine which template you want to use to generate a report.

Step 3 In the tile, click the header to view a sample report.

A window displays with the sample report. Use the side bar in the window to scroll down and review the entire sample report.

Note
You can use the sample report to plan how you want your report to look.

Step 4 Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

To skip this screen in the future, check the **Don't show this to me again** check box.

Step 7 In the **Select Report Template** window, select the template for the report.

select the **Template** from the drop-down lists.

Note
The **Template** list consists of the individual report types within the categories for the release.

You can review an auto-generated sample in the same window.

Step 8 Click **Next**.

Step 9 In the **Setup Report Scope** window, name the report and select the scope.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report and select the **Time Range**.

Note
The **Setup Report Scope** options change depending on the selected **Template**.

Click **Next**.

Step 10 In the **Select File Type** window, select the file type for the report.

Catalyst Center displays these **File Type** options for the Audit Log report type:

- **CSV**
- **JSON**

For the **CSV** and **JSON** file types, a **Fields** option lets you select attributes for the **CSV** and **JSON** results.

Step 11 Click **Next**.

Step 12 In the **Schedule Report** window, select the schedule for the report. Then, click **Next**.

Step 13 In the **Delivery and Notification** window, select the delivery mechanism for the report:

- **None**: No email or webhook notifications sent.
- **Email Report**: Email report is sent as a link or attachment.

  Note
  If you have not yet configured an SMTP server for the emails, you are prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Choose **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** window under **Reports**. You can view and download the report from this link and location.

    Note
    Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **Attachment**: Report is attached to the email notification.

    Note
    PDF reports support email notification attachments of up to 20 MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  Catalyst Center sends these email notifications for the report:

  - Report is in the queue waiting to be processed.
  - Report processing is in progress.
  - Report has successfully been compiled and is completed.

  To reduce the number of notifications, you can uncheck the preceding check boxes, as needed.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). select a webhook from the drop-down list **(Subscription Profile** field).

  Note
  If you have not yet created a webhook, you are prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

You will receive status webhook notifications for the report. For example, you will receive "In Queue," "In Progress," and "Success" webhook notifications. You will also be able to view these notifications in the GUI.

Step 14 Click **Next**.

Step 15 In the **Summary** window, review the configuration and edit any of the files, if necessary.

Click **Generate Report**.

After the report is generated, a success window displays.

Step 16 Click the **View the Generated Reports** link.

The **Generated Reports** window shows instance details of the report that was scheduled.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View generated reports, on page 187.

Run a client report

Perform this procedure to configure specialized **Client** reports for your network.

Before you begin

Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

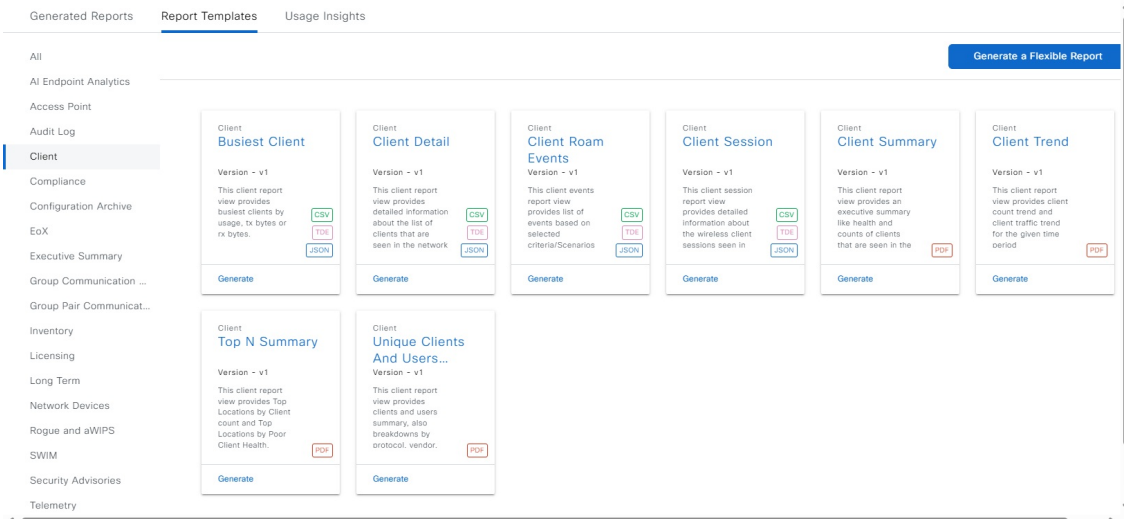
Procedure

Step 1 From the main menu, choose **Reports** > **Report Templates**.

The **Report Templates** window displays the supported reporting categories. A link represents each category. Click a link to view the supported reports for the selected category.

Step 2 After clicking a link, review the **Report Templates** window for the selected category.

Figure 18: Client Report



Each template is represented by a tile and contains information about the report and links to generate a report. Determine which template you want to use to generate a report.

Step 3 In the tile, click the header to view a sample report.

A window displays for the sample report. Use the side bar in the window to scroll down and review the entire sample report. For some of the client reports, this data is presented:

- Applied filters (data filters that were used to build the report).
- Data metrics and summaries.
- Graphical representation of the data (including line, bar, and pie graphs).
- Tables that assist you in analyzing the data.

Note
You can use the sample report to plan how you want your report to look.

Step 4 Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window lets you select a format type for the report, apply data filters for your reports, and set up schedules for the actual report generation.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

To skip this screen in the future, check the **Don't show this to me again** check box.

Step 7 In the **Select Report Template** window, select the template for the report.

Select the **Template** from the drop-down lists.

Note
The **Template** consists of the individual report types within the categories for the release.

You can review an auto-generated sample in the same window.

Step 8 Click **Next**.

Step 9 In the **Setup Report Scope** window, name the report and select the scope.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report and select the **Time Range**.

Note
The **Setup Report Scope** options change depending on the selected **Template**. You can generate the Client Trend, Unique Clients and Users Summary, Client Summary, and Client Detail reports for the past 180 days. Other report types support up to 90 days of data.

Click **Next**.

Step 10 In the **Select File Type** window, select the file type for the report.

Depending on the report that you are creating, these **File Type** options may be available:

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option lets you select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Step 11 Click **Next**.

Step 12 In the **Schedule Report** window, select the schedule for the report. Then, click **Next**.

Step 13 In the **Delivery and Notification** window, select the delivery mechanism for the report:

- **None**: No email or webhook notifications sent.
- **Email Report**: Email report is sent as a link or attachment.

  Note
  If you have not yet configured an SMTP server for the emails, you are prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Choose **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** window under **Reports**. You can view and download the report from this link and location.

    Note
    Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **Attachment**: Report is attached to the email notification.

    Note
    PDF reports support email notification attachments of up to 20 MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

Catalyst Center sends these email notifications for the report:

- Report is in the queue waiting to be processed.
- Report processing is in progress.
- Report has successfully been compiled and is completed.

To reduce the number of notifications, you can uncheck the preceding check boxes, as desired.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list **(Subscription Profile** field).

  Note
  If you have not yet created a webhook, you are prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

  You will receive status webhook notifications for the report. For example, you will receive "In Queue," "In Progress," and "Success" webhook notifications. You will also be able to view these notifications in the GUI.

Step 14 Click **Next**.

Step 15 In the **Summary** window, review the configuration and edit any of the files, if necessary.

Click **Generate Report**.

After the report is generated, a success window displays.

Step 16 Click the **View the Generated Reports** link.

The **Generated Reports** window shows instance details of the report that was scheduled.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View generated reports, on page 187.

Run a compliance report

Catalyst Center allows you to retrieve a consolidated compliance audit report that shows the compliance status of individual network devices. With this report, you can get complete visibility of your network.

This procedure describes how to configure a **Compliance** report for your network.

Procedure

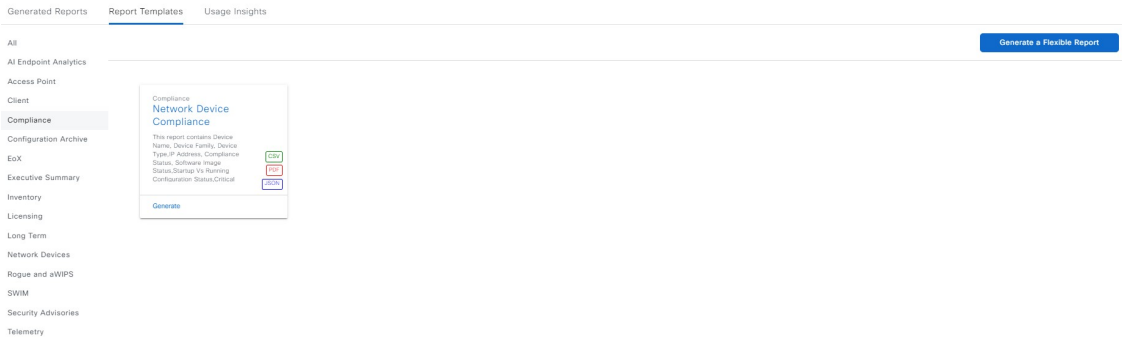
Step 1 From the main menu, choose **Reports** > **Report Templates**.

The **Report Templates** window displays the supported reporting categories.

Step 2 From the left pane, click **Compliance** to display the Compliance templates.

Each template is represented by a tile and contains information about the report and links to generate a report.

Figure 19: Compliance report



Step 3 In the tile, click the header to view a sample report.

A window displays for the sample report. Use the side bar in the window to scroll down and review the entire sample report.

Step 4 Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

To skip this screen in the future, check the **Don't show this to me again** check box.

Step 7 In the **Select Report Template** window, you can change the template from **Template** drop-down list.

Note
You can review an automatically generated sample in the same window.

Step 8 Click **Next**.

The **Setup Report Scope** window appears.

Step 9 In the **Report Name** field, enter a report name.

Step 10 In the **Scope** area, choose the **Compliance Status**, **Compliance Category**, **Device Family** and **Device Type** to include in the report.

Note
The **Setup Report Scope** options change depending on the selected template.

Step 11 Click **Next**.

Step 12 In the **Select File Type** window, select the file type for the report.

Catalyst Center displays these **File Type** options for the Compliance report type:

- **PDF**
- **CSV**
- **JSON**

For the **CSV** and **JSON** file types, a **Fields** option lets you select attributes for the **CSV** and **JSON** results.

Step 13 Click **Next**.

Step 14 When the **Schedule Report** window appears, select the schedule for the report. Then, click **Next**.

Step 15 In the **Delivery and Notification** window, select the delivery mechanism for the report:

- **None**: No email or webhook notifications sent.
- **Email Report**: Email report is sent as a link or attachment.

  If an SMTP server is not configured for emails, Catalyst Center prompts you to configure one. Click the link to configure the email destination in **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **As a Link**: The email notification of a successful compiled report contains a link back to itself and the **Generated Reports** page under **Reports**. You can view and download the report from this link and location.

    Note
    Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you must add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **As an Attachment**: Report is attached to the email notification.

    Note
    PDF reports support email notification attachments of up to 20 MB in size and up to 10 email addresses. To add multiple email addresses, you must add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  Catalyst Center sends these email notifications for the report:

  - Report is in the queue waiting to be processed.
  - Report processing is in progress.
  - Report has successfully been compiled and is completed.

  To reduce the number of notifications, you can uncheck the preceding check boxes, as desired.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL).

  Note
  If a webhook is not created, Catalyst Center prompts you to create one. Click the link to configure a webhook in **Webhook** tab in **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

  Catalyst Center sends you these status webhook notifications for the report:

  - In Queue
  - In Progress
  - Success

  You can view the event notification status in **Platform** > **Runtime Dashboard** > **Event Summary**.

Step 16 Click **Next**.

Step 17 In the **Summary** window, review the configuration and edit any of the files, if necessary.

Step 18 Click **Generate Report**.

After the report is generated, a success window appears.

Step 19 Click the **View the Generated Reports** link.

The **Generated Reports** window displays with instance details of the report that was scheduled.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View Generated Reports.

Run a configuration archive report

Use this procedure to get a consolidated report of configuration changes on your network devices.

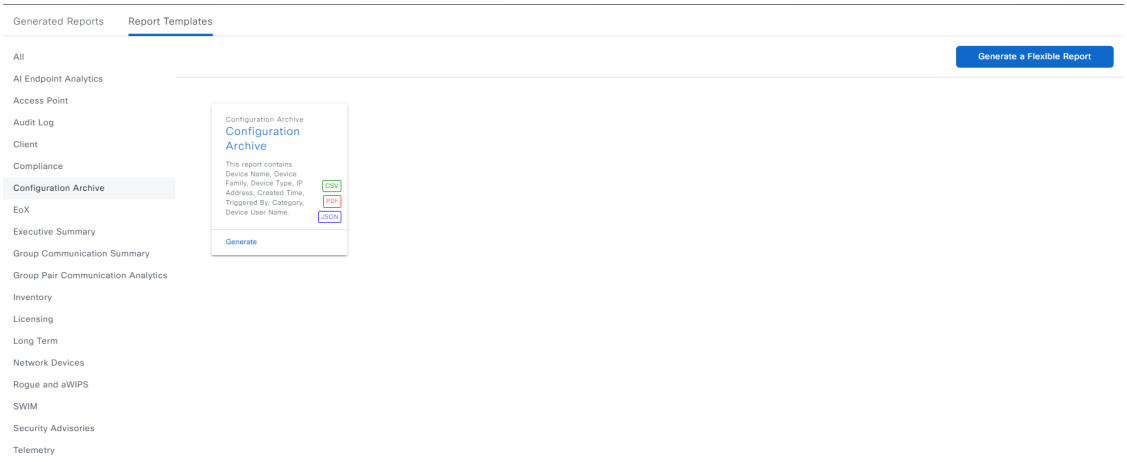
Procedure

Step 1 From the main menu, choose **Reports** > **Report Templates**.

The **Report Templates** window displays the supported reporting categories.

Step 2 From the left pane, click **Configuration Archive** to display the template.

Figure 20: Configuration Archive report



Each template is represented by a tile and contains information about the report and links to generate a report.

Step 3 In the tile, click the header to view a sample report.

A window displays for the sample report. Use the side bar in the window to scroll down and review the entire sample report.

Step 4 Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

To skip this screen in the future, check the **Don't show this to me again** check box.

Step 7 In the **Select Report Template** window, you can change the template from the **Template** drop-down list.

Note
You can review an automatically generated sample in the same window.

Step 8 Click **Next**.

The **Setup Report Scope** window appears.

Step 9 In the **Report Name** field, enter a report name.

Step 10 In the **Scope** area, select **Category** from the drop-down list.

In band refers to configuration changes done by Catalyst Center.

Out Of Band refers to the configuration changes done outside Catalyst Center.

Step 11 Select the **Device Family** and **Device Type** to include in the report.

Note
The **Setup Report Scope** options change depending on the selected template.

Step 12 Click **Next**.

Step 13 In the **Select File Type** window, select the file type for the report.

Catalyst Center displays these **File Type** options for the Configuration Archive report type:

- **PDF**
- **CSV**
- **JSON**

For the **CSV** and **JSON** file types, a **Fields** option lets you select attributes for the **CSV** and **JSON** results.

Step 14 Click **Next**.

Step 15 When the **Schedule Report** window appears, select the schedule for the report. Then, click **Next**.

Step 16 In the **Delivery and Notification** window, select the delivery mechanism for the report:

- **None**: No email or webhook notifications sent.
- **Email Report**: Email report is sent as a link or attachment.

  If an SMTP server is not configured for emails, Catalyst Center prompts you to configure one. Click the link to configure the email destination in **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **As a Link**: The email notification of a successful compiled report contains a link back to itself and the **Generated Reports** page under **Reports**. You can view and download the report from this link and location.

    Note
    Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you must add each email address separately and click **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **As an Attachment**: Report is attached to the email notification.

    Note
    PDF reports support email notification attachments of up to 20 MB in size and up to 10 email addresses. To add multiple email addresses, you must add each email address separately and click **Enter** (on your keyboard)

after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

Catalyst Center sends these email notifications for the report:

- Report is in the queue waiting to be processed.
- Report processing is in progress.
- Report has successfully been compiled and is completed.

To reduce the number of notifications, you can uncheck the preceding check boxes, as needed.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL).

  Note
  If a webhook is not created, Catalyst Center prompts you to create one. Click the link to configure a webhook in the **Webhook** tab in **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

  Catalyst Center sends you these status webhook notifications for the report:

  - In Queue
  - In Progress
  - Success

You can view the event notification status in **Platform** > **Runtime Dashboard** > **Event Summary**.

Step 17 Click **Next**.

Step 18 In the **Summary** window, review the configuration and edit any of the files, if necessary.

Step 19 Click **Generate Report**.

After the report is generated, a success window appears.

Step 20 Click the **View the Generated Reports** link.

The **Generated Reports** window displays with instance details of the report that was scheduled.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View Generated Reports.

Run an end-of-life report

This procedure describes how to configure an **End of Life (EoX)** report for your network.

Before you begin

- You must accept the end-user license agreement (EULA) before downloading software or provisioning a device. For more information, see the **Accept the License Agreement** topic in the *Cisco Catalyst Center Administrator Guide*.

- Ensure that the Cisco CX cloud connection is enabled. For more information, see the **Update the Machine Reasoning Knowledge Base** topic in the *Cisco Catalyst Center Administrator Guide*.
- Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

Procedure

Step 1 From the main menu, choose **Reports** > **Report Templates**.

The **Report Templates** window opens and displays the supported reporting categories. A link represents each category.

In the **Report Templates** window, each template is represented by a tile and contains information about the report and links to generate a report. Decide which template you want to use to generate a report.

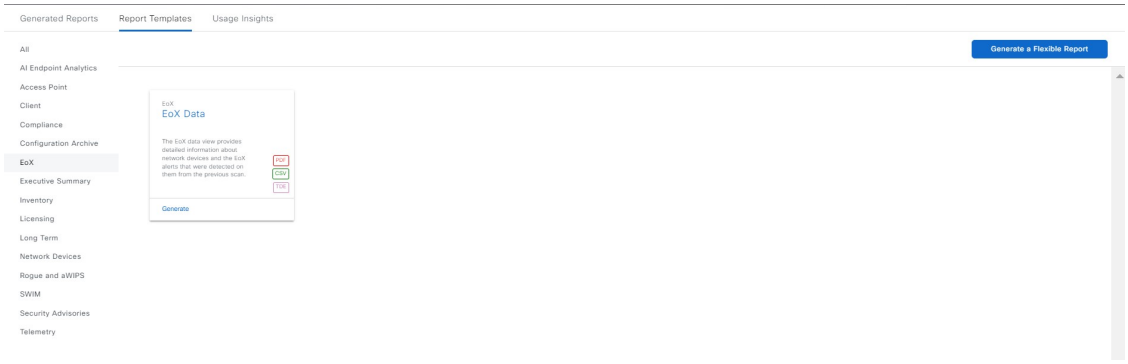
Step 2 In the tile, click the header to view a sample report.

A window displays for the sample report. Use the side bar in the window to scroll down and review the entire sample report.

Step 3 Click **X** to close the preview.

Step 4 In the tile, click the **Generate** link to configure parameters to build a report.

Figure 21: EoX report



Step 5 In the **Generate a New Report** window, click **Let's Do It** to get started.

To skip this screen in the future, check the **Don't show this to me again** check box.

Step 6 In the **Select Report Template** window, select the template from **Template** drop-down list.

Note
The **Template** consists of the individual report types within the categories for the release.

You can review an automatically generated sample in the same window.

Step 7 Click **Next**.

The **Setup Report Scope** window displays.

Step 8 In the **Report Name** field, enter a report name.

Step 9 In the **Scope** area, select the **Device Type** and **Location** to include in the report.

Note
The **Setup Report Scope** options change depending on the selected template.

Step 10 Click **Next**.

Step 11 In the **Select File Type** window, select the file type for the report.

Based on your report, Catalyst Center displays these **File Type** options:

- **PDF**
- **CSV**
- **Tableau Data Extract**

For the **CSV** and **Tableau Data Extract** file types, a **Fields** option lets you select attributes (additional fields) for the **CSV** and **Tableau Data Extract** results.

Step 12 Click **Next**.

In the **Schedule Report** window, select the schedule for the report.

Step 13 Click **Next**.

Step 14 In the **Delivery and Notification** window, select the delivery mechanism for the report:

- **None**: No email or webhook notifications sent.
- **Email Report**: Email report is sent as a link or attachment.

  Follow the prompts to the **Email** tab in the Catalyst Center GUI to configure an SMTP server.

  If an SMTP server is not configured for emails, Catalyst Center prompts you to configure one.

  - **As a Link**: The email notification of a successful compiled report contains a link back to itself and the **Generated Reports** page under **Reports**. You can view and download the report from this link and location.

    Note
    Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you must add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **As an Attachment**: Report is attached to the email notification.

    Note
    PDF reports support email notification attachments of up to 20 MB in size and up to 10 email addresses. To add multiple email addresses, you must add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

Catalyst Center sends these email notifications for the report:

- Report is in the queue waiting to be processed.
- Report processing is in progress.
- Report been has successfully compiled and is completed.

To reduce the number of notifications, you can uncheck the preceding check boxes, as needed.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL).

Note
If a webhook is not created, Catalyst Center prompts you to create one. Follow the prompts to the **Webhook** tab in the Catalyst Center GUI to configure a webhook.

Catalyst Center sends you these status webhook notifications for the report:

- In Queue
- In Progress
- Success

You can view these notifications in the GUI.

Step 15 Click **Next**.

Step 16 In the **Summary** window, review the configuration and edit any of the files, if necessary.

Step 17 Click **Generate Report**.

After the report is generated, a success window appears.

Step 18 Click the **View the Generated Reports** link.

The **Generated Reports** window displays with instance details of the report that was scheduled.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View Generated Reports.

Run an executive summary report

Follow this procedure to configure **Executive Summary** reports for your network.

Before you begin

Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

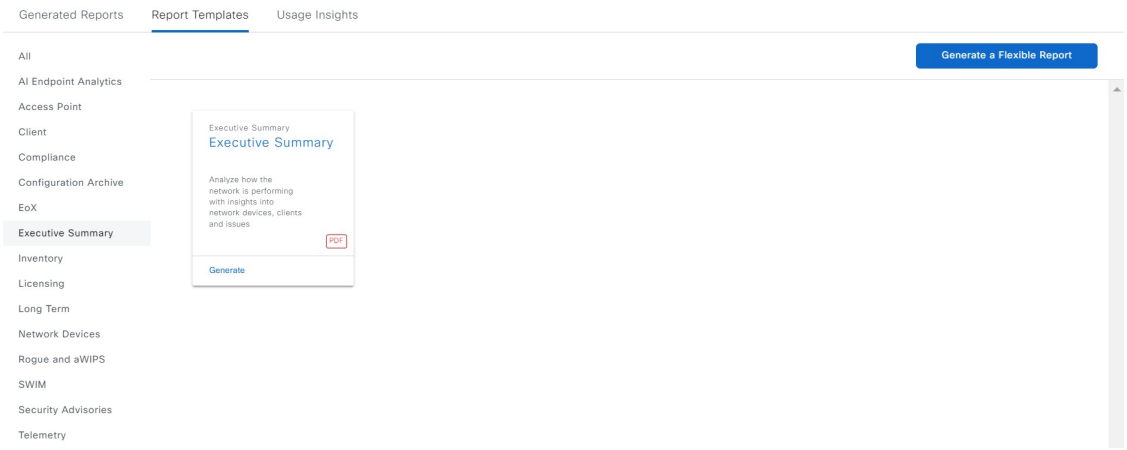
Procedure

Step 1 From the main menu, choose **Reports** > **Report Templates**.

The **Report Templates** window displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

Step 2 After clicking a link, review the **Report Templates** window for that selected category.

Figure 22: Executive Summary report



Each template is represented by a tile and contains information about the report and links to generate a report. Determine which template you want to use to generate a report. Within the tile are icons that represent the supported file types for the reports.

Step 3 In the tile, click the header to view a sample report.

A window displays for the sample report. Use the side bar in the window to scroll down and review the entire sample report. This data is presented:

- Data metrics and summaries.
- Graphical representation of the data (including line, bar, and pie graphs).
- Tables that assist you in analyzing the data.

Note
You can use the sample report to plan how you want your report to look.

Step 4 Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window lets you select a format type for the report, apply data filters for your reports, and set up schedules for the actual report generation.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

Step 7 In the **Select Report Template** window, select the template for the report.

Select the **Template** from the drop-down lists.

Note
The **Template** consists of the individual report types within the categories for the release.

You can review an auto-generated sample in the same window.

Click **Next**.

Step 8 In the **Setup Report Scope** window, name the report and select the scope and the time range.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report and select the **Time Range**.

Note
The **Setup Report Scope** options change depending on the selected **Template**. The Executive Summary reports support up to 90 days of data retention.

Click **Next**.

Step 9 In the **Select File Type** window, select the file type for the report.

Depending on the report that you are creating, these **File Type** options may be available:

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option lets you select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Click **Next**.

Step 10 In the **Schedule Report** window, select the schedule for the report. Then, click **Next**.

Step 11 In the **Delivery and Notification** window, select the delivery mechanism for the report:

- **None**: No email or webhook notifications sent.
- **Email Report**: Email report is sent as a link or attachment.

  Note
  If you have not yet configured an SMTP server for the emails, you are prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Select **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** window under **Reports**. You can view and download the report from this link and location.

    Note
    Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **Attachment**: Report is attached to the email notification.

    Note
    PDF reports support email notification attachments of up to 20 MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  Catalyst Center sends these email notifications for the report:

  - Report is in the queue waiting to be processed.

- Report processing is in progress.
- Report has successfully been compiled and is completed.

To reduce the number of notifications, you can uncheck the preceding check boxes, as needed.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list **(Subscription Profile** field).

  Note
  If you have not yet created a webhook, you are prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

  You will receive status webhook notifications for the report. For example, you will receive "In Queue," "In Progress," and "Success" webhook notifications. You will also be able to view these notifications in the GUI.

Click **Next**.

Step 12 In the **Summary** window, review the configuration and edit any of the files, if necessary.

Click **Generate Report**.

After the report is generated, a success window appears.

Step 13 Click the **View the Generated Reports** link.

The **Generated Reports** window shows instance details of the report that was scheduled.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View generated reports, on page 187.

Run an inventory report

Follow this procedure to configure **Inventory** reports for your network.

Before you begin

Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

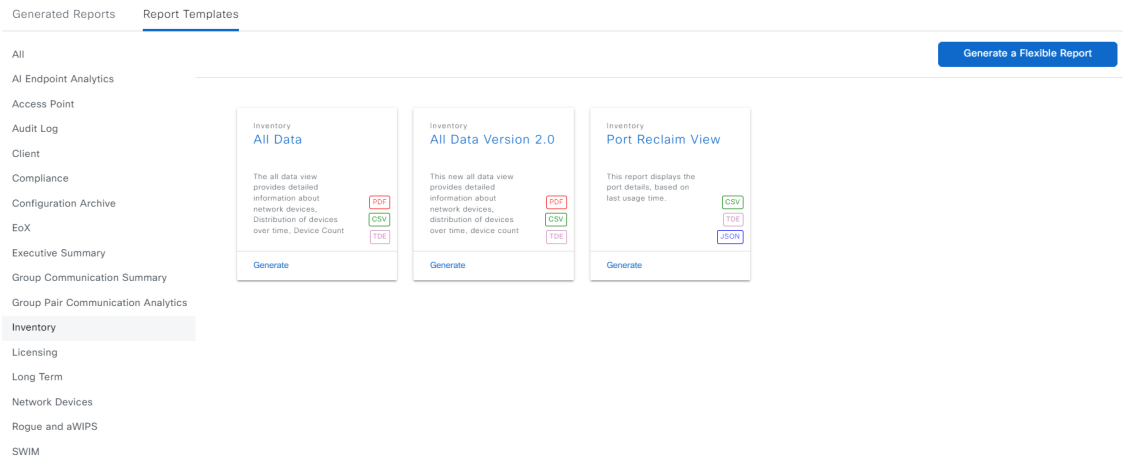
Procedure

Step 1 From the main menu, choose **Reports** > **Report Templates**.

The **Report Templates** window displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

Step 2 After clicking a link, review the **Report Templates** window for that selected category.

Figure 23: Inventory report



Each template is represented by a tile and contains information about the report and links to generate a report. Determine which template you want to use to generate a report. Within the tile are icons that represent the supported file types for the reports.

Step 3 In the tile, click the header to view a sample report.

A window displays with the sample report. Use the side bar in the window to scroll down and review the entire sample report. This data is presented:

- Applied filters (data filters that were used to build the report).
- Data metrics and summaries
- Graphical representation of the data (including line, bar, and pie graphs).
- Tables that assist you in analyzing the data.

Note
You can use the sample report to plan how you want your report to look.

Step 4 Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window lets you select a format type for the report, apply data filters for your reports, and set up schedules for the actual report generation.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

To skip this screen in the future, check the **Don't show this to me again** check box.

Step 7 In the **Select Report Template** window, select the template for the report.

Select the **Template** from the drop-down lists.

Note
The **Template** consists of the individual report types within the categories for the release.

You can review an auto-generated sample in the same window.

Click **Next**.

Step 8 In the **Setup Report Scope** window, name the report and select the scope.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report.

Note
The **Setup Report Scope** options change depending on the selected **Template**.

Click **Next**.

Step 9 In the **Select File Type** window, select the file type for the report.

Step 10 Click **Next**.

Step 11 In the **Schedule Report** window, select the schedule for the report.

Click **Next**.

Step 12 In the **Delivery and Notification** window, select the delivery mechanism for the report:

- **None**: No email or webhook notifications sent.
- **Email Report**: Email report is sent as a link or attachment.

  Note
  If you have not yet configured an SMTP server for the emails, you are prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Choose **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** window under **Reports**. You can view and download the report from this link and location.

    Note
    Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **Attachment**: Report is attached to the email notification.

    Note
    PDF reports support email notification attachments of up to 20 MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  Catalyst Center sends these email notifications for the report:

  - Report is in the queue waiting to be processed.
  - Report processing is in progress.
  - Report has successfully been compiled and is completed.

  To reduce the number of notifications, you can uncheck the preceding check boxes, as desired.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list (**Subscription Profile** field).

Note
If you have not yet created a webhook, you are prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

You will receive status webhook notifications for the report. For example, you will receive "In Queue," "In Progress," and "Success" webhook notifications. You will also be able to view these notifications in the GUI.

Click **Next**.

Step 13 In the **Summary** window, review the configuration and edit any of the files, if necessary.

Click **Generate Report**.

After the report is generated, a success window appears.

Step 14 Click the **View the Generated Reports** link.

The **Generated Reports** window shows instance details of the report that was scheduled.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View generated reports, on page 187.

Run a licensing report

Follow this procedure to configure **Licensing** reports about your network.

Before you begin

Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

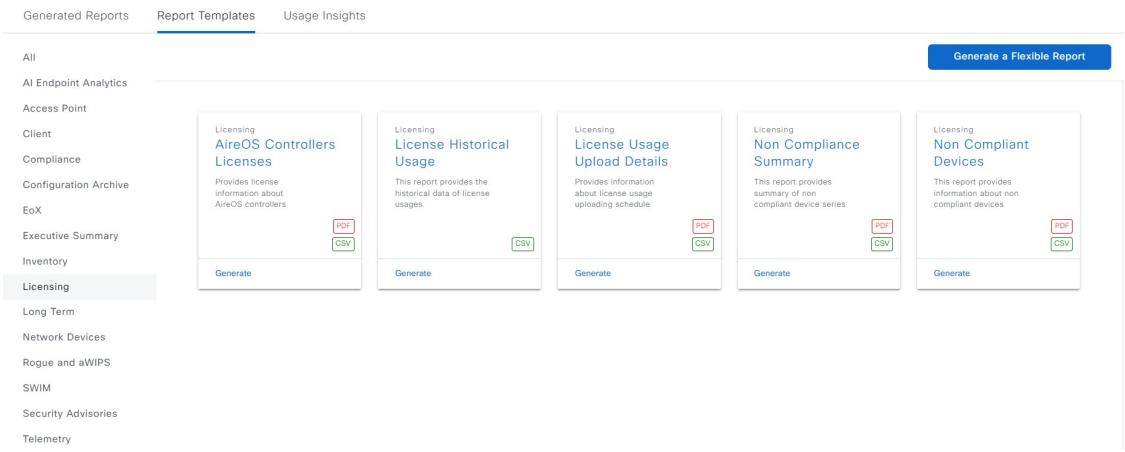
Procedure

Step 1 From the main menu, choose **Reports** > **Report Templates**.

The **Report Templates** window displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

Step 2 After clicking a link, review the **Report Templates** window for that selected category.

Figure 24: Licensing report



Each template is represented by a tile and contains information about the report and links to generate a report. Determine which template you want to use to generate a report. Within the tile are icons that represent the supported file types for the reports.

Step 3 In the tile, click the header to view a sample report.

A window displays for the sample report. Use the side bar in the window to scroll down and review the entire sample report. This data is presented:

- Applied filters (data filters that were used to build the report).
- Data metrics and summaries.
- Tables that assist you in analyzing the data.

Note
You can use the sample report to plan how you want your report to look.

Step 4 Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window lets you select a format type for the report, apply data filters for your reports, and set up schedules for the actual report generation.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

To skip this screen in the future, check the **Don't show this to me again** check box.

Step 7 In the **Select Report Template** window, select the template for the report.

select the **Template** from the drop-down lists.

Note
The **Template** consists of the individual report types within the categories for the release.

You can review an auto-generated sample in the same window.

Click **Next**.

Step 8 In the **Setup Report Scope** window, name the report and select the scope and the time range.

In the **Report Name** field, enter a report name and click inside the **Scope** field to display the available filter. Click the filter options that you want for the report and select the **Time Range**.

Note
The **Setup Report Scope** options change depending on the selected **Template**.

Click **Next**.

Step 9 In the **Select File Type** window, select the file type for the report.

Depending on the report that you are creating, these **File Type** options may be available:

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option lets you select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Click **Next**.

Step 10 In the **Schedule Report** window, select the schedule for the report.

Click **Next**.

Step 11 In the **Delivery and Notification** window, select the delivery mechanism for the report:

- **None**: No email or webhook notifications sent.
- **Email Report**: Email report is sent as a link or attachment.

  Note
  If you have not configured an SMTP server for the emails, you are prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Choose **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **Link**: The email notification of a successfully compiled report has a link to the report and to the **Generated Reports** window under **Reports**. You can view and download the report from this location.

    Note
    Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **Attachment**: Report is attached to the email notification.

    Note
    PDF reports support email notification attachments of up to 20 MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

Catalyst Center sends these email notifications for the report:

- Report is in the queue waiting to be processed.
- Report processing is in progress.
- Report has successfully been compiled and is completed.

To reduce the number of notifications, you can uncheck the preceding check boxes, as desired.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list **(Subscription Profile** field).

  Note
  If you have not yet created a webhook, you are prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

  You receive status webhook notifications for the report, for example, **In Queue**, **In Progress**, and **Success**. You are also able to view these notifications in the GUI.

Click **Next**.

Step 12 In the **Summary** window, review the configuration and edit the files, if necessary.

Click **Generate Report**.

After the report is generated, a success window appears.

Step 13 Click the **View the Generated Reports** link.

The **Generated Reports** window shows instance details of the report that was scheduled.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View generated reports, on page 187.

Run a network devices report

Follow this procedure to configure **Network Devices** reports for your network.

Before you begin

Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

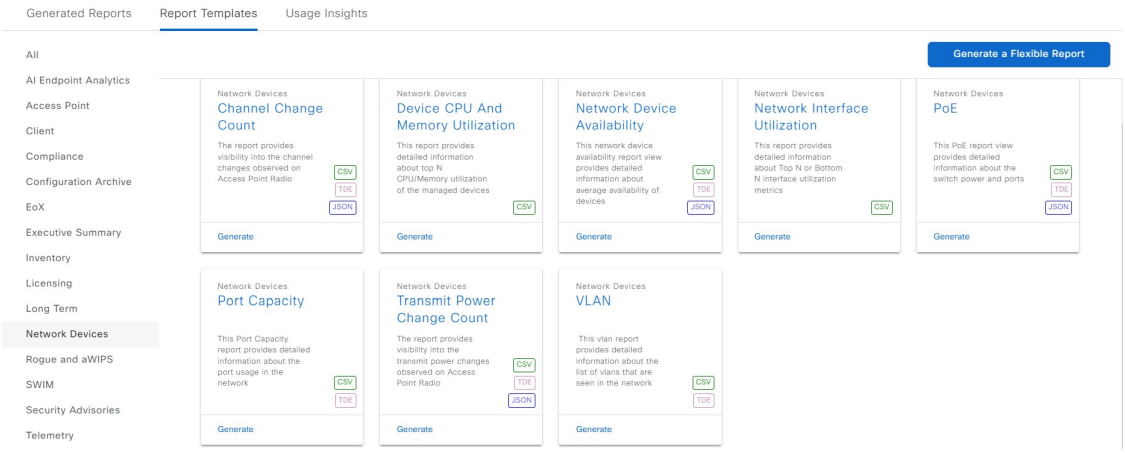
Procedure

Step 1 From the main menu, choose **Reports** > **Report Templates**.

The **Report Templates** window displays the supported reporting categories. Each category is represented by link. Click a link to view only the supported reports for that category.

Step 2 After clicking a link, review the **Report Templates** window for that selected category.

Figure 25: Network Devices report



Each template is represented by a tile and contains information about the report and links to configure (generate) a report. Determine which template you want to use to generate a report. Within the tile are icons that represent the supported file types for the reports.

Step 3 In the tile, click the header to view a sample report.

A window displayss for the sample report. Use the side bar in the window to scroll down and review the entire sample report. This data is presented:

- Applied filters (data filters that were used to build the report)
- Data metrics and summaries
- Graphical representation of the data (including line, bar, and pie graphs)
- Tables that assist you in analyzing the data

Note
You can use the sample report to plan how you want your report to look.

Step 4 Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window lets you select a format type for the report, apply data filters for your reports, and set up schedules for the actual report generation.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

Step 7 In the **Setup the Report Template** window, select the template for the report.

Select the **Template** from the drop-down menus.

Note
The **Template** consists of the individual report types within the categories for the release.

You can review an autogenerated sample in the same window.

Click **Next**.

Step 8 In the **Setup Report Scope** window, name the report and select the scope and the time range.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report and select the **Time Range**.

Note
The **Setup Report Scope** options change depending on the selected **Template**.

Click **Next**.

Step 9 In the **Select File Type** window, select the file type for the report.

Depending on the report that you are creating, these **File Type** options may be available:

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option lets you select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Click **Next**.

Step 10 In the **Schedule Report** window, select the schedule for the report.

Click **Next**.

Step 11 In the **Delivery and Notification** window, select the delivery mechanism for the report:

- **None**: No email or webhook notifications sent.
- **Email Report**: Email report is sent as a link or attachment.

  Note
  If you have not yet configured an SMTP server for the emails, you are prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Choose **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **Link**: The email notification of a successfully compiled report will have a link back to itself and the **Generated Reports** window under **Reports**. You can view and download the report from this link and location.

    Note
    Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **Attachment**: Report is attached to the email notification.

    Note
    PDF reports support email notification attachments of up to 20 MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

Catalyst Center sends this email notifications for the report:

- Report is in the queue waiting to be processed.
- Report processing is in progress.
- Report has successfully been compiled and is completed.

To reduce the number of notifications, you can uncheck the preceding check boxes, as desired.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down menu **(Subscription Profile** field).

  Note
  If you have not yet created a webhook, you are prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

  You will receive status webhook notifications for the report. For example, you will receive "In Queue," "In Progress," and "Success" webhook notifications. You will also be able to view these notifications in the GUI.

Click **Next**.

Step 12 In the **Summary** window, review the configuration and edit any of the files, if necessary.

Click **Generate Report**.

After the report is generated, a success window appears.

Step 13 Click the **View the Generated Reports** link.

The **Generated Reports** window shows instance details of the report that was scheduled.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View generated reports, on page 187.

Run a rogue and aWIPS report

Follow this procedure to configure **Rogue and aWIPS** reports for your network.

Before you begin

Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

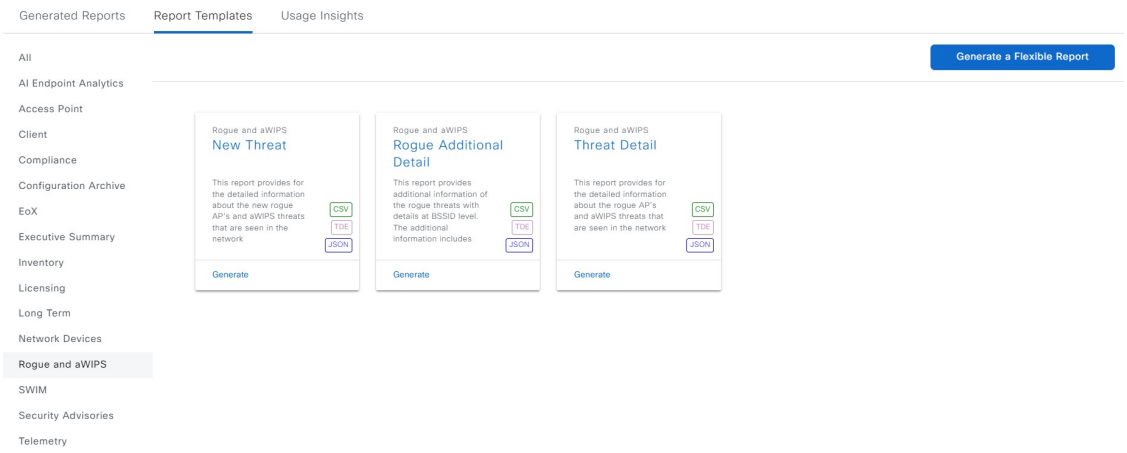
Procedure

Step 1 From the main menu, choose **Reports** > **Report Templates**.

The **Report Templates** window displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

Step 2 After clicking a link, review the **Report Templates** window for that selected category.

Figure 26: Rogue and aWIPS report



Each template is represented by a tile and contains information about the report and links to generate a report. Determine which template you want to use to generate a report. Within the tile are icons that represent the supported file types for the reports.

Step 3 In the tile, click the header to view a sample report.

A window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report. This data is presented:

- Applied filters (data filters that were used to build the report).
- Data metrics and summaries
- Graphical representation of the data (including line, bar, and pie graphs).
- Tables that assist you in analyzing the data.

Note
You can use the sample report to plan how you want your report to look.

Step 4 Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window lets you select a format type for the report, apply data filters for your reports, and set up schedules for the actual report generation.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

Step 7 In the **Select Report Template** window, select the template for the report.

select the **Template** from the drop-down lists.

Note
The **Template** consists of the individual report types within the categories for the release.

You can review an auto-generated sample in the same window.

Click **Next**.

Step 8 In the **Setup Report Scope** window, name the report and select the scope and the time range.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report and select the **Time Range**.

Note

- The **Setup Report Scope** options change depending on the selected **Template**.
- If all the APs in your network are not assigned to a floor and you select **Global** in the **Location** filter, the **Rogue and aWIPS** report displays only the threats associated with assigned APs under the global hierarchy. To view the threats associated with unassigned APs, you must keep the location filter empty.

Click **Next**.

Step 9 In the **Select File Type** window, select the file type for the report.

Depending on the report that you are creating, these **File Type** options may be available:

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option lets you select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Click **Next**.

Step 10 In the **Schedule Report** window, select the schedule for the report.

Click **Next**.

Step 11 In the **Delivery and Notification** window, select the delivery mechanism for the report:

- **None**: No email or webhook notifications sent.
- **Email Report**: Email report is sent as a link or attachment.

  Note
  If you have not yet configured an SMTP server for the emails, you are prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Choose **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** window under **Reports**. You can view and download the report from this link and location.

    Note
    Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **Attachment**: Report is attached to the email notification.

    Note

PDF reports support email notification attachments of up to 20 MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

Catalyst Center sends these email notifications for the report:

- Report is in the queue waiting to be processed.
- Report processing is in progress.
- Report has successfully been compiled and is completed.

To reduce the number of notifications, you can uncheck the preceding check boxes, as desired.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). select a webhook from the drop-down list **(Subscription Profile** field).

  Note
  If you have not yet created a webhook, you are prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

  You will receive status webhook notifications for the report. For example, you will receive "In Queue," In Progress," and "Success" webhook notifications. You will also be able to view these notifications in the GUI.

Click **Next**.

Step 12 In the **Summary** window, review the configuration and edit any of the files, if necessary.

Click **Generate Report**.

After the report is generated, a success window appears.

Step 13 Click the **View the Generated Reports** link.

The **Generated Reports** window shows instance details of the report that was scheduled.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View generated reports, on page 187.

Run an ROI report

The Catalyst Center platform ROI Insights report is a customized report that shows the productivity improvement of network operations with Catalyst Center and comparative ROI insights with a traditional NMS.

This procedure describes how to configure an ROI report for a network operation.

Procedure

Step 1 From the main menu, choose **Reports** > **Usage Insights**.

The **Usage Insights** window displays this information:

- **SAVINGS**: Displays the time and cost saved on network operation with Catalyst Center for a selected time range.
- **ROI Insights**: Lists the ROI Insights report that is created based on features, time and cost saved, usage KPIs, traditional NMS time, and actions.
- **Savings Trends**: Displays the savings trend of **Cost** and **Time** for an ROI Insights report.

  Note
  The **Savings Trends** area appears only if the selected time range is more than a month.

Step 2 In the **Campus Network Assurance**, **Network Device Onboarding**, **Campus Software Image Management**, and **Campus Network Segmentation** areas, enter the time savings in the **Hours** and **Minutes** name fields for a traditional NMS and Catalyst Center.

- Traditional NMS: Average time to detect and resolve an issue in the network without Catalyst Center.
- Catalyst Center: Average time to detect and resolve an issue in the network with Catalyst Center.

Step 3 To modify the **Cost Inputs** and **IT Inputs**, click **Customize ROI Insights** and make the changes.

The **Customize ROI Insights** area displays the preconfigured **Avg. Cost per IT Staff**, **Currency**, **No. of IT Staff**, and **Avg. Annual Hrs Worked**.

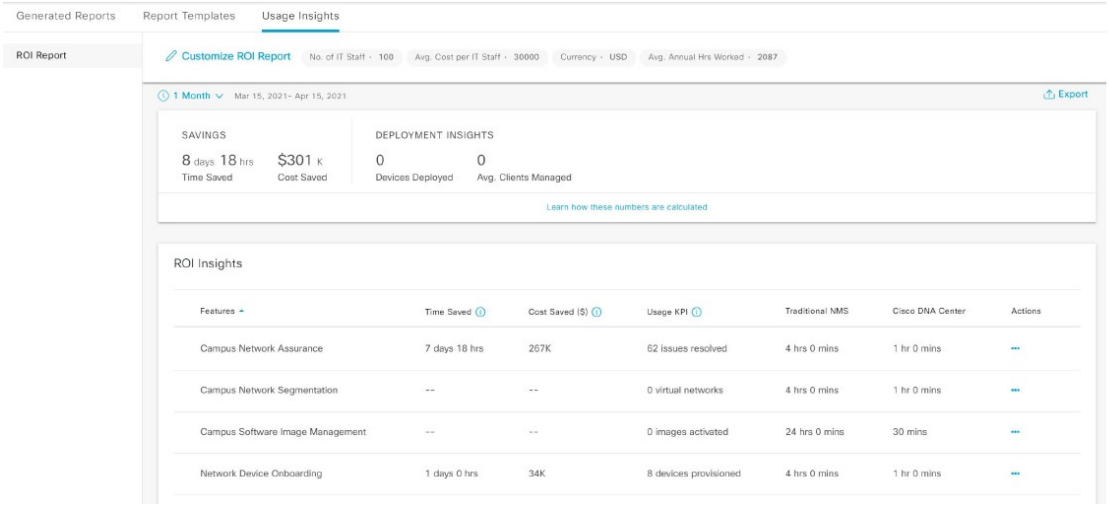
Step 4 To edit the time savings for a feature, click the corresponding **Edit** link under the **Actions** column and update the time in the subsequent pop-up window.

Step 5 To select the time range for which you want to see the ROI report, click the time range drop-down list below the **Customize ROI Insights** pane and click a time range radio button.

a) Select from the available time range options: **1 Month**, **3 Months**, **6 Months**, and **1 Year**.

b) To customize the time range of ROI reports, click the time range drop-down list, click **Custom**, and define the **Start Date** and **End Date**.

Figure 27: Usage Insights report dashboard



Step 6 Click **Learn how these numbers are calculated** above the **ROI Insights** table in the middle pane to see the calculation details.

The **Calculation Details** window shows how to calculate **Time Saved** and **Cost Saved**.

Step 7 To export the ROI report, click **Export**.

The supported file types for the reports are PDF and CSV.

Run a security advisories report

Perform this procedure to configure a **Security Advisories** report about your network.

Before you begin

Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

Procedure

Step 1 From the main menu, choose **Reports** > **Report Templates**.

The **Report Templates** window displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

Step 2 After clicking a link, review the **Report Templates** window for that selected category.

Figure 28: Security Advisories report



Each template is represented by a tile and contains information about the report and links to generate a report. Determine which template you want to use to generate a report. Within the tile are icons that represent the supported file types for the reports.

Step 3 In the tile, click the header to view a sample report.

A window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report. This data is presented:

- Applied filters (data filters that were used to build the report).
- Data metrics and summaries.
- Tables that assist you in analyzing the data.

Note
You can use the sample report to plan how you want your report to look.

Step 4 Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window lets you select a format type for the report, apply data filters for your reports, and set up schedules for the actual report generation.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

Step 7 In the **Select Report Template** window, select the template for the report.

Select the **Template** from the drop-down lists.

Note
The **Template** consists of the individual report types within the categories for the release.

You can review an auto-generated sample in the same window.

Click **Next**.

Step 8 In the **Setup Report Scope** window, name the report and select the scope and time range.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report and select the **Time Range**.

Note
The **Setup Report Scope** options change depending on the selected **Template**.

Click **Next**.

Step 9 In the **Select File Type** window, select the file type for the report.

Depending on the report that you are creating, these **File Type** options may be available:

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option lets you select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Click **Next**.

Step 10 In the **Schedule Report** window, select the schedule for the report.

Click **Next**.

Step 11 In the **Delivery and Notification** window, select the delivery mechanism for the report:

- **Email Report**: Email report is sent as a link or attachment.

  Note
  If you have not yet configured an SMTP server for the emails, you are prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Choose **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** window under **Reports**. You can view and download the report from this link and location.

    Note
    Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **Attachment**: Report is attached to the email notification.

    Note
    PDF reports support email notification attachments of up to 20 MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  Catalyst Center sends thse email notifications for the report:

  - Report is in the queue waiting to be processed.

- Report processing is in progress.
- Report has successfully been compiled and is completed.

To reduce the number of notifications, you can uncheck the preceding check boxes, as desired.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list **(Subscription Profile** field).

  Note
  If you have not yet created a webhook, you are prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

  You will receive status webhook notifications for the report. For example, you will receive "In Queue," "In Progress," and "Success" webhook notifications. You will also be able to view these notifications in the GUI.

Click **Next**.

Step 12 In the **Summary** window, review the configuration and edit any of the files, if necessary.

Click **Generate Report**.

After the report is generated, a success window appears.

Step 13 Click the **View the Generated Reports** link.

The **Generated Reports** window shows instance details of the report that was scheduled.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View generated reports, on page 187.

Run a SWIM report

Follow this procedure to configure **SWIM** reports about your network.

Before you begin

Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

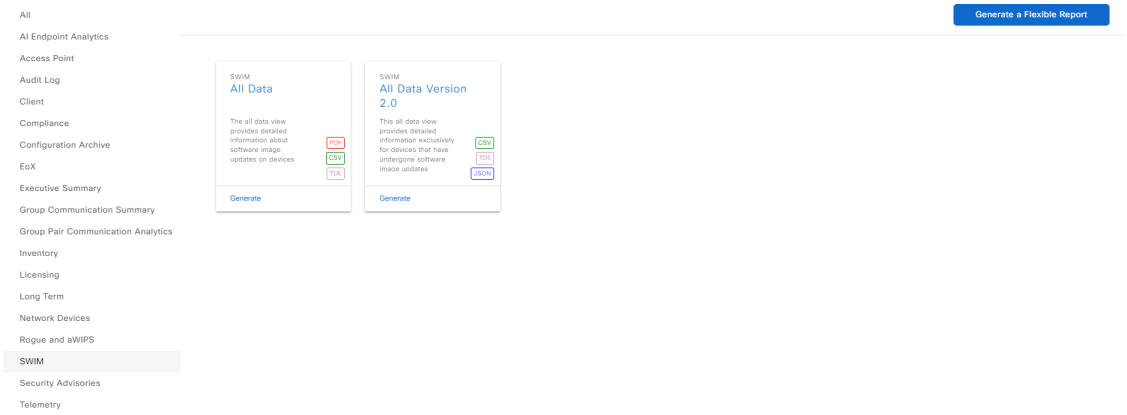
Procedure

Step 1 From the main menu, choose **Reports** > **Report Templates**.

The **Report Templates** window displays the supported reporting categories. A link represents each category. Click a link to view only the supported reports for that category.

Step 2 After clicking a link, review the **Report Templates** window for that selected category.

Figure 29: SWIM report



Each template is represented by a tile and contains information about the report and links to generate a report. Determine which template you want to use to generate a report. Within the tile are icons that represent the supported file types for the reports.

Step 3 In the tile, click the header to view a sample report.

A window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report. This data is presented:

- Applied filters (data filters that were used to build the report).
- Data metrics and summaries.
- Tables that assist you in analyzing the data.

Note
You can use the sample report to plan how you want your report to look.

Step 4 Click **X** to close the preview.

Step 5 In the tile, click the **Generate** link to configure parameters to build a report.

The **Generate** window lets you select a format type for the report, apply data filters for your reports, and set up schedules for the actual report generation.

Step 6 In the **Generate a New Report** window, click **Let's Do It** to get started.

To skip this screen in the future, check the **Don't show this to me again** check box.

Step 7 In the **Select Report Template** window, select the template for the report.

Select the **Template** from the drop-down lists.

Note
The **Template** consists of the individual report types within the categories for the release.

You can review an auto-generated sample in the same window.

Click **Next**.

Step 8 In the **Setup Report Scope** window, name the report and select the scope and time range.

Enter a report name in the **Report Name** field and click in the **Scope** field to display the available filter. Click the filter options that you want for the report and select the **Time Range**.

Note
The **Setup Report Scope** options change depending on the selected **Template**.

Click **Next**.

Step 9 In the **Select File Type** window, select the file type for the report.

Depending on the report that you are creating, these **File Type** options may be available:

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

For the **CSV**, **JSON**, and **Tableau Data Extract** file types, a **Fields** option lets you select attributes (additional fields) for the CSV, JSON, and Tableau Data Extract results.

Click **Next**.

Step 10 In the **Schedule Report** window, select the time range and schedule for the report.

Click **Next**.

Step 11 In the **Delivery and Notification** window, select the delivery mechanism for the report:

- **None**: No email or webhook notifications sent.
- **Email Report**: Email report is sent as a link or attachment.

  Note
  If you have not yet configured an SMTP server for the emails, you are prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Choose **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **Link**: The email notification of a successfully compiled report has a link back to itself and the **Generated Reports** window under **Reports**. You can view and download the report from this link and location.

    Note
    Email notifications with embedded links to reports support up to 20 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  - **Attachment**: Report is attached to the email notification.

    Note
    PDF reports support email notification attachments of up to 20 MB in size and up to 10 email addresses. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Catalyst Center platform validates the email addresses and notifies you if the syntax is incorrect.

  Catalyst Center sends these email notifications for the report:

- Report is in the queue waiting to be processed.
- Report processing is in progress.
- Report has successfully been compiled and is completed.

To reduce the number of notifications, you can uncheck the preceding check boxes, as desired.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list **(Subscription Profile** field).

  Note
  If you have not yet created a webhook, you are prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

  You will receive status webhook notifications for the report. For example, you will receive "In Queue," "In Progress," and "Success" webhook notifications. You will also be able to view these notifications in the GUI.

Click **Next**.

Step 12 In the **Summary** window, review the configuration and edit any of the files, if necessary.

Click **Next**.

After the report is generated, a success window appears.

Step 13 Click the **View the Generated Reports** link.

The **Generated Reports** window shows instance details of the report that was scheduled.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View generated reports, on page 187.

Generate a flexible report

Catalyst Center allows you the flexibility to generate customized reports for your wired and wireless networks. This procedure describes how to configure **Flexible** reports based on your choice of entity, attributes, aggregation, and filters.

You can configure **Flexible** reports using the **Reports** window in the Catalyst Center GUI.

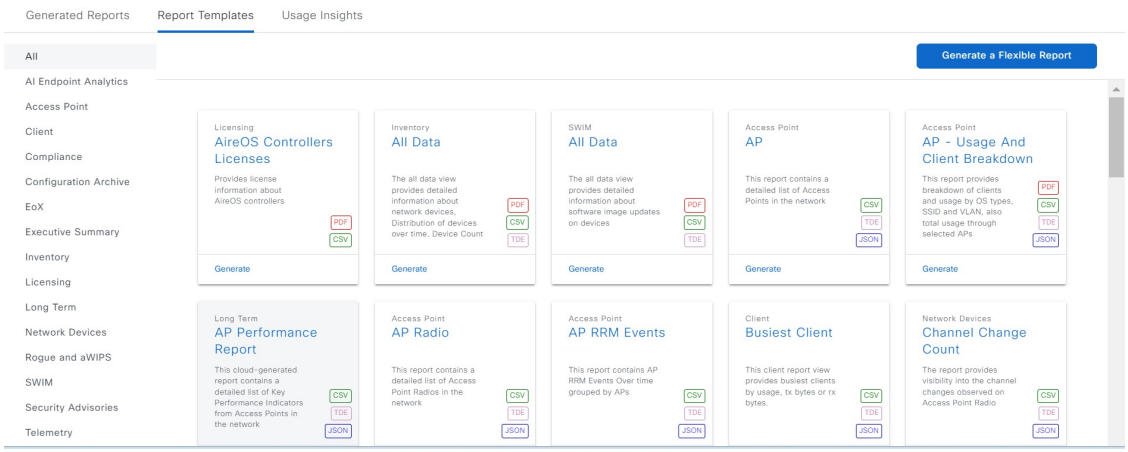
Before you begin

Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

Procedure

Step 1 From the main menu, choose **Reports** > **Report Templates**.

Figure 30: Generate a flexible report



Step 2 Click **Generate a Flexible Report**.

Note
Alternatively, click the menu icon and choose **Workflows** > **Flexible Report**.

Step 3 In the **Flexible Report** window, click **Let's Do it** to get started.

The **Name Your Report and Select a Time Range for this Report** window appears.

Note
To skip the **Flexible Report** dialog box in the future, check the **Don't show this to me again** check box.

Step 4 In the **Report Name** field, enter the name of your report. Select the **Time Range**.

Note
- The supported time range for **Client** reports is 90 days.
- For **Network Device**, **PoE** and **AP** reports, the supported time range is 30 days.

Step 5 Click **Next**.

Step 6 In the **Create a Subreport** window, enter the **Subreport Name** and select the entity, report type, filter criteria, and respective attributes.

In this release, these options are available in the **Select an entity** drop-down list:

- **Network Device**
- **PoE**
- **AP**
- **SWIM**
- **Client**

These **Report Type** options are available:

- **Trend**

- **Summary**
- **Top N**
- **Distribution**

Select the filter criteria for the selected report type.

For example, for a **Trend** report type, select **Trending Interval** from the drop-down list.

Select the attributes from the **Attributes available for this report type** area.

You can configure groups based on the group-by, sort-by, and aggregate options available for each attribute.

Note
Selection of attributes supporting group-by and aggregate options is mandatory for **Trend** and **Distribution** report types. Selection of an attribute supporting the sort-by option is mandatory for **Top N** report type.

Step 7 Click **Next**.

Step 8 In the **Configure Group By, Aggregates and Sorting Options as Applicable** window, do these tasks

- Select **Configure Group By**.

  Note
  Configure Group By is required or optional based on the chosen report type.

- Select **Aggregate Options** for each of the supported attributes from the drop-down list.
- In **Configure Sorting Option**, you can select either **Target Attributes** or **Sort Type** for each subreport, and then select respective options from the drop-down list.

Step 9 Click **Next**.

The **Filters for the Current Subreport** window opens.

- Select a filter option from the drop-down list and set corresponding filter values.

  Check the **Apply this filter for the entire report** check box, if necessary.

- Configure the field filters available for the report.

  Select a filter from the drop-down list. Based on the selection, configure the **Operator** and **Value** options, or select a range, and then select the corresponding **Unit**.

  Note
  In this release, the operator-based filter options are available for the Client, AP and Network Device entities.

Step 10 Click **Next**.

The **Would you like to add another Subreport** window opens.

Step 11 Select **Yes** to add another subreport.

In the **Subreports Created** area, you can edit the parameters of any subreport, if necessary.

Click **Next**.

Step 12 In the **Schedule the Report, Select Output Format and Choose the Delivery Method** window, do these tasks:

- Select the schedule for the report.

- Select the output file format.

  Note
  In this release, the supported report file format is **CSV**. The flexible report allows you to generate or view separate **CSV** files for each subreport, or download or view related subreports together as a **ZIP** file.

- Select the delivery mechanism for the report.

  Note
  You can configure Integration Settings using the link available to enable delivery options.

  The report delivery options include:

  - **None**: You can select to only view the report.
  - **Email Report**: Email report is sent as a link or attachment.

    Note
    If you have not yet configured an SMTP server for the emails, you are prompted to configure one. Follow the prompts to the **Email** tab in the GUI to configure an SMTP server. Choose **System** > **Settings** > **External Services** > **Destinations** > **Email**.

  - **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address (callback URL). Select a webhook from the drop-down list (**Subscription Profile** field).

    Note
    If you have not yet created a webhook, you are prompted to create one. Follow the prompts to the **Webhook** tab in the GUI to configure a webhook. In general, to configure a webhook, choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**.

    Catalyst Center sends these status webhook notifications for the report:

    - In Queue
    - In Progress
    - Success

  You can also view these notifications in the GUI.

Step 13 Click **Next**.

In the **Summary** window, you can review the subreports and edit the parameters, if necessary.

Step 14 Click **Generate Report**.

After you generate the report, a success window appears with these options:

- **Create Another Flexible Report**
- **View the Generated Reports**

Step 15 Click **View the Generated Reports**.

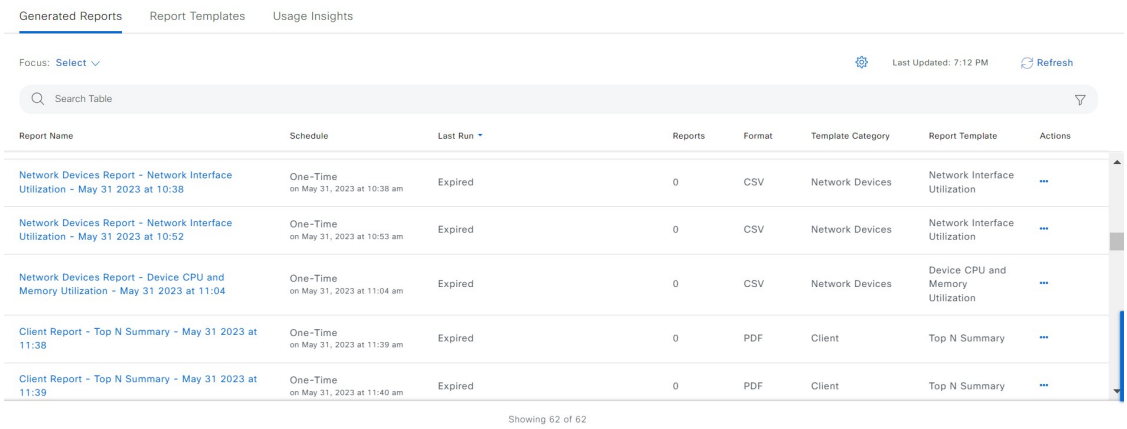
The **Generated Reports** window shows details of the new flexible report.

You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see View generated reports, on page 187.

View generated reports

Follow this procedure to download, review, edit, duplicate, or delete a previously generated report.

Figure 31: Generated reports



Before you begin

- Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.
- Create a report using the **Schedule** functionality in the **Catalog**.

Procedure

Step 1 From the main menu, choose **Reports**.

Step 2 Click **Generated Reports**.

This information appears:

- **Report Name**: Name of the report.

  If you did not give the report a name, a default name is given to the report that contains the report type with the date and time of the report.

  Note
  The report name is a link that opens up a view of the report itself within the **Generated Reports** window. Use the **Download** link to download a copy of the report.

- **Schedule**: One-time generated report or reoccurring report. Also displayed is a brief description of the schedule that generated the report.

- **Last Run**: Displays report execution status and details. These report execution status types may appear:
  - **Not Initiated**: Report scheduled but not yet started.
  - **In Queue**: Report scheduled and in the processing queue to be executed.
  - **In Progress**: Report currently being executed.
  - **Completed**: Report execution completed displaying the date and time.

    Clicking on the icon (downward pointing arrow) downloads the last generated report.
  - **Expired**: Report expired and no longer available in Catalyst Center.
  - **Error**: Report execution failed.

- **Reports**: Number of reports up to a total of seven.

  Hover (mouse) over the displayed report number and **View Report List** appears. Click **View Report List** to display a reports dialog box. The reports dialog box lists all the report executions, their status (**Not Initiated**, **In Queue**, **In Progress**, **Completed**, **Expired**, and **Error**) and a **Download** button to download a copy. Clicking **Error** displays any errors and warnings for the report execution.

  Important
  Catalyst Center retains a total of seven reports. Specifically, Catalyst Center retains the last seven reports that are executed, as well as the last seven reports executed over the last seven days (week). For example, if you run eight reports in a single day, Catalyst Center only retains the last seven reports. If you schedule one report for each day, Catalyst Center retains only the most recent seven reports over the last seven days (week). You can export the reports in their various formats from Catalyst Center and archive them to a safe location.

- **Format**: File format type, such as PDF or CSV.
- **Template Category**: Type of report based on the catalog options (Client, Executive Summary, SWIM, or Inventory).
- **Report Template**: Template used when generating the report.
- **Actions**: List of tasks you can perform with the reports.

You can adjust the downloads that display in the GUI by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

Step 3 Click **Actions** to do one or more of these tasks:

- **View Config**: Opens a window where the configured parameters for the report are displayed (including the schedule). You can review the configured report parameters in this window. You cannot make any changes to the report configuration in this read-only window. If you must edit the configuration, click **Edit**. You can both view and edit a report configuration by clicking **Edit**.
- **Edit**: Opens a window where configured parameters for the report are displayed (including the schedule). You can review the parameters and also edit them in this window. Click **Save** after making any edits to the report.

  Important
  After you edit and update the report configuration, any future report executions reflect this new configuration. This is important if reports are being generated on a reoccurring schedule. Also, if you edit and update a report configuration, all the previous reports in Catalyst Center will be deleted. The GUI displays a warning about the deletion when clicking **Save**. You do not have to make any edits in the configuration to click **Save** and delete all previous reports.

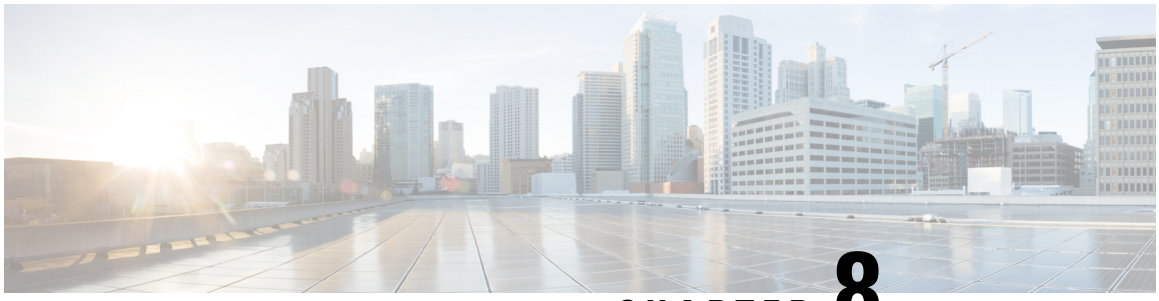
- **Duplicate**: Opens the **Duplicate** window, where you can either view or configure the parameters for the report. Click **Generate Report** to generate the report again.

  Note
  If you want to create a new report based on an existing report and its configuration, use the **Duplicate** option and make changes to the configuration. This lets you create a new report similar to the existing one, while retaining the existing report and its configuration. If you want to discard the existing report and completely replace it with a new report, use the **View Config** and **Edit** options as described previously.

- **Run Now**: Starts the process to execute the report. A success message appears after a successful report execution.

  Note
  If you try to execute a report and there are seven previous reports, the GUI displays a warning that only the last seven reports are saved. You use the **Run Now** option when you must generate a report outside of an existing schedule for the reports.

- **Delete**: Deletes the report. You are prompted to confirm the action before the report is deleted.



CHAPTER 8

Developer Toolkit GUI

- About developer toolkit, on page 191
- Work with APIs, on page 191
- Work with integration flows, on page 193
- Work with event notifications, on page 195

About developer toolkit

The Catalyst Center platform provides you with these software developer tools to access and program with Catalyst Center, as well as to integrate Catalyst Center with other applications:

- **APIs**: Available APIs organized within categories by functionality (for example, **Operational Tasks** or **Site Management** APIs).
- **Integration Flows**: Available integration flows organized by category type.
- **Event Notifications**: Lets you view and subscribe to specific events that may occur in your network.

Work with APIs

Follow this procedure to review available APIs, generate example code for using the APIs, and try out the APIs interactively on the Catalyst Center platform.

The Catalyst Center GUI displays documentation about each API call, including the request method and URL, query parameters, request header parameters, responses, and schema, and ways to preview or test the request.

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

Before you begin

- Ensure that you have met the supported programming language and authentication prerequisites, as described in the previous section. For more information, see API prerequisites, on page 103.
- You must first enable the **Rogue and aWIPS** bundle to view these specific APIs. From the main menu, choose **Platform** > **Manage** > **Bundles** > **Rogue and aWIPS** > **Enable**. After enabling this bundle, you can view the APIs within the bundle under the **Contents** tab, or choose **Platform** > **Developer Toolkit** > **APIs** > **Know Your Network** > **Devices**.

Procedure

Step 1 From the main menu, choose **Platform** > **Developer Toolkit** > **APIs**.

Step 2 Review the list of supported APIs.

If necessary, click the > icon to display the API subdomains.

Step 3 Select the domain or subdomain to view the APIs.

This information about each API under that appears in columns:

- **Method**: Supported methods include GET, POST, PUT, and DELETE.
- **Name**: Link to access the slide-in pane and additional information, including description, features, tags, parameters, responses, model schemas, and so on. A Sunset, Deprecated or an Intent banner indicates status of the API. For more information about the API Lifecycle, see Cisco Catalyst Center APIs on DevNet.
- **Description**: Brief description of the API.
- **URL**: URL value for the API.
- **Actions**: Create a code preview snippet with the **Try** option.

Note
A blue color-coded message may appear, stating that the specific API configuration is still in progress and to check back at a later time. The screen auto refreshes when the API is registered and you may proceed with your API activity. In the highly unlikely event that a red color-coded message appears stating that the API cannot be configured, contact your Catalyst Center administrator to contact Cisco for assistance in resolving the issue.

Step 4 Click the name (link) of an API method.

This information about the API method appears:

- **DESCRIPTION**: Brief description of the API operation.
- **TAGS**: API identifiers, including where and under what circumstances you would use the API. Note that some APIs may not have tags.
- **PARAMETERS**: Parameters of API, including description, data type (Boolean or string), default value, and required value.
- **FEATURES**: Objective of the API operation, information related to the Deprecated or Beta status of the API operation, and details of the alternative API operation.
- **REQUEST BODY**: Details of the data you must provide in the body of an HTTP request when interacting with an API endpoint.
- **RESPONSES**: Possible HTTP responses. **Schema** presents response as a data model (**Model** tab) or JSON format of the actual response (**Model Schema** tab). Click **Sample** to view the sample code.
- **POLICIES**: An API rate limiting feature, where policies are applied to certain APIs. These policies set the number of API calls per time interval per client IP address.

Step 5 (Optional) Generate a code preview by clicking **Code Preview**.

Note
If you are creating your own program, you can cut and paste the code preview sample into your own program.

Step 6 (Optional) In the **Code Preview** window, select a language from the drop-down to generate the code.

These languages are supported:

- **Shell**
- **Node - HTTP**
- **Node - Unirest**
- **Node - Request**
- **Python**
- **Ruby**
- **JavaScript**
- **JQuery**
- **PHP**
- **Go**
- **Ansible**

After reviewing or copying the code preview sample for use, click **Close**.

Step 7 (Optional) Try the method by clicking **Try**.

Step 8 (Optional) In the **Try** window, fill in the requested values (for example, URL address or value) and click **Run**.

After reviewing the response and/or error code, click **Close**.

When Catalyst Center returns a 202 (Accepted) HTTP status code, the result body includes a task ID and a URL that you can use to query for more information about the asynchronous task that your original request spawned. For example, you can use this information to determine whether a lengthy task has completed.

Note
The response is a live response from Catalyst Center itself, and the results reflect the actual state of your network. In contrast, the code previews are static and contain placeholders for values that you must supply.

Work with integration flows

An integration flow defines the interaction between Catalyst Center platform and a third-party system, such as an ITSM system that is used to track, troubleshoot, and resolve network issues.

Catalyst Center platform supports schedule-based integration flows. This type of integration flow runs on a schedule, performs a task, and pushes the information to a REST endpoint or other vendor-specific destination. Schedule-based integration flows can be edited in the GUI using the **Integration Flows** window to specify the schedule on which they execute.

Note The integration flows available in the **Developer Toolkit** are used by various bundles in **Manage** > **Bundles**. Bundles are used to integrate your own applications with Catalyst Center or to enhance the performance of Catalyst Center itself. You can view the integration flows used in a bundle by clicking the bundle in **Manage** and clicking the **Contents** tab. Integration flows for the bundle are listed under the **Contents** tab.

Before you begin

Before you can view and manage integration flows in the **Integration Flows** window, you must enable them. You enable integration flows from the individual bundles in the Catalyst Center platform. For example, click the menu icon and choose **Platform** > **Manage** > **Bundles** > **Basic ITSM (ServiceNow) CMDB synchronization**. Click the **Contents** tab and then click **Enable**.

Procedure

Step 1 From the main menu, choose **Platform** > **Developer Toolkit** > **Integration Flows**.

Step 2 Review the integration flows displayed by the GUI.

Step 3 Select an integration flow from the ITSM Integration group.

This information appears:

- **Name**: Name of the integration flow and link to access a slide-in pane where additional information is available.

  If the integration flow is a REST-based trigger type, after you click the integration flow name additional data such as description, tags, parameters, responses, model schemas, and policies appear.

  If the integration flow is a schedule-based trigger type, after you click the integration flow name a slide-in pane for setting the schedule appears. This slide-in pane displays **DESCRIPTION**, **TAGS**, and **HOW TO USE THIS FLOW** content.

- **Description**: Brief description of integration flow.

- **Trigger**: REST-based or schedule-based.

- Icon (**…**): Accesses links to create a code preview or the **Try** option. If the integration flow is schedule-based, this icon accesses a **Schedule Flow** option.

Step 4 For a REST-based integration flow, click on the name (link) of the integration flow.

A slide-in pane opens with details about the REST-based integration flow. Review the details and then close the slide-in pane.

Step 5 For a REST-based integration flow, generate a code preview snippet by mousing over the icon (**…**) and clicking **Generate Code Preview**.

These choices appear only for REST-based triggered integration flows. Schedule-based integration flows provide a Schedule Flow menu item on hover.

Step 6 In the **Code Preview** window, select a programming language from the drop-down to generate the code.

After reviewing or copying the code for use, click **Close**.

Step 7 To try a REST request path interactively, mouse over the icon (**…**) and click **Try**.

Step 8 In the **Try** window, fill in the requested values (for example, URL address or value) and click **Run**.

After trying the method, review the response and/or error code within the **Try** window, and click **Close**.

When Catalyst Center returns a 202 (Accepted) HTTP status code, the result body includes a task ID and a URL that you can use to query for more information about the asynchronous task that your original request spawned. For example, you can use this information to determine whether a lengthy task has completed. For more information, see Getting Information about Asynchronous Operations.

Note
For responses, Catalyst Center APIs use a task-based response architecture so that multiple requests and responses can be sent concurrently. Therefore, all PUT, POST, and DELETE requests have a task-based response. To view more details about the response, send a GET request to the task URL (either from a script or as a URL). For error codes, the Catalyst Center APIs follow the standard HTTP status codes.

Step 9 For the schedule-based integration flow, mouse over the icon (**…**) and click **Schedule Flow**.

Step 10 Review this data:

- **DESCRIPTION**: Description and purpose of integration flow.
- **TAGS**: Tags indicate what the Catalyst Center component is used for or affected by the bundle.
- **HOW TO USE THIS FLOW**: Schedule configuration options.

You can schedule the integration flow using the GUI.

Step 11 Configure a schedule for the integration flow using these GUI options:

- **Run Now**: Select **Run Now** and then click **Schedule** to run the integration flow.
- **Run Later**: Select **Run Later** and then enter a date, time, and time zone. Click **Schedule** to run the integration flow at the specified date, time, and time zone.
- **Recurring**: Select **Recurring** and then configure these options:
  - **Repeats**: Select daily or weekly repeating occurrences for the integration flow
  - **Run at Interval**: Set the time interval between integration flows.
  - **Set Schedule Start**: Set a start date.
  - **Set Schedule End**: Set an end date.

Click **Schedule** to run the integration at the configured times.

Work with event notifications

You can associate a notification to specific events that may occur in your network. After the notification is associated with event and even if the event does occur, you receive a notification by REST API or email. You associate a notification to an event by using the **Event Notifications** window in the Catalyst Center platform GUI.

Before you begin

- For a REST API notification, you configured the webhook destination in the **Webhook** tab in Catalyst Center. To access the **Webhook** tab, click the menu icon and choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**. For detailed information about configuring a webhook destination, see Configure a webhook destination, on page 133.
- For email notification of events, you configured the email destination in the **Email** tab in Catalyst Center. To access the **Email** tab, click the menu icon and choose **System** > **Settings** > **External Services** > **Destinations** > **Email**. For detailed information about configuring an email destination, see Configure an email destination, on page 134.
- For a syslog server notification of events, you configured the syslog server destination in the **Syslog** tab in Catalyst Center. To access the **Syslog** tab, click the menu icon and choose **System** > **Settings** > **External Services** > **Destinations** > **Syslog**. For detailed information about configuring a syslog server destination, see Configure a syslog server destination, on page 135.
- For an SNMP trap notification of events, you configured the SNMP trap destination in the **SNMP** tab in Catalyst Center. To access the **SNMP** tab, click the menu icon and choose **System** > **Settings** > **External Services** > **Destinations** > **SNMP**. For detailed information about configuring a trap destination, see Configure a trap notification, on page 136.
- You have accessed the **Event Settings** window and reviewed or edited the list of events that may occur within your network for ITSM integration and can be captured by Catalyst Center. To access the **Event Settings** window, click the menu icon and choose **Platform** > **Manage** > **Configurations** > **Event Settings**.

Procedure

Step 1 From the main menu, choose **Platform** > **Developer Toolkit** > **Event Notifications**.

The **Events Notifications** window appears.

Step 2 Click the **Notifications** tab to view the notification tiles.

Each notification is represented by a tile and contains a link to view notification details.

Step 3 From the **CHANNELS** area in the left pane, click the radio button next to the channels for which you want to view the respective notification tiles.

The supported channels are **REST**, **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX** and **EMAIL**. Assurance events do not support SNMP.

Note

- You must create a notification for an event with respective channels and trigger the notification. For more information, see **Create an Event Notification** in the *Cisco Catalyst Center User Guide*.
- One event notification supports more than one channel.

Step 4 Click a notification tile link for which you want to view the notification details.

The **Notification Details** slide-in pane displays these notification details based on the selected channel:

- **Name**: Name of the event.

- **Description**: Event description
- **Sites**
- **Events**
- **REST**: Appears only when you want to view REST notification details. The **REST** area shows this information:
  - **URL**: URL address of the REST API endpoint that event will be sent to.
  - **Method**: Either the PUT or POST method.
  - **Trust certificate**: Whether a trust certificate is required for REST API endpoint notification.
  - **Headers**: The **Header Name** and **Header Value**.
- **PAGERDUTY**: Appears only when you want to view PAGERDUTY notification details. The **PAGERDUTY** area shows this information:
  - PagerDuty Events API URL
  - PagerDuty Integration Key
  - PagerDuty Events API Version
- **SNMP**: Appears only when you want to view **SNMP** notification details.
- **SYSLOG**: Appears only when you want to view **SYSLOG** notification details.
- **WEBEX**: Appears only when you want to view **WEBEX** notification details.
- **EMAIL**: Appears only when you want to view **EMAIL** notification details. The **EMAIL** area shows the email recipients **From** and **To** along with email **Subject**.

Step 5 In the **Notification Details** slide-in pane, click the toggle button at the top-right corner to enable or disable the respective notification.

Step 6 To edit a particular notification, click the **Actions** drop-down list and select **Edit**.

Step 7 In the **EDIT NOTIFICATION** window, do this configuration based on the selected channel:

a. In the **Name** field, enter a unique name.

b. In the **Description** field, enter the description of respective event.

c. Expand the **Site and Events** and select a site from the **Select a site** drop-down list.

d. Click the plus icon next to an event, or click **Add All** to add all the events to the respective notification.

e. To remove an event from the notification, click the cross icon next to an event that you want to remove, or click **Remove All** to remove all events from the respective notification.

f. Expand **Configuration** to edit the configuration of the selected notification channel.

To specify details in the **Configuration** area, see **Create an Event Notification** in the *Cisco Catalyst Center User Guide*.

Note
In the **Configuration** area, the fields shown depend on the type of selected notification channel.

Step 8 Click the toggle button at the top-right corner to toggle between the tile view and list view.

Step 9 Click the **Event Catalog** tab to view the list of created events.

Note
You can adjust the events that appear by entering a keyword in the **Search** field.

Step 10 Review the data on an individual event within the table.

This **Event Details** tab data appears:

- **Description**: Brief description of the event and how it is triggered.
- **Event ID**: Identification number of the event.
- **Version**: Version number of the event.
- **Namespace**: Namespace of the event.
- **Severity**: 1 through 5.

  Note
  Severity 1 is the most important or critical priority and should be assigned for this type of an event.

- **Domain**: REST API domain to which the event belongs.
- **Subdomain**: Subgroup under the REST API domain to which the event belongs.
- **Category**: Error, Warn, Info, Alert, Task Progress, Task Complete.
- **Note**: Additional information about the event or to assist in further understanding the event.
- **Event Link**: Event broadcast using REST URL.
- **Tags**: Tags indicate what Catalyst Center component is affected by the event.
- **Channels**: What channels are supported for the event notifications (REST API, email, webex, and so on).
- **Model Schema**: Presents model schema about the event:
  - **Details**: Example of model schema detail for the event.
  - **REST Schema**: REST schema format for the event.

Step 11 Click the **Notifications** tab to view the active notification associated to the respective event.

When you associate a notification to an event, a **Try-It Now** button appears in the **Event Catalog** tab. To run an event notification simulation, click **Try-It Now**. For information, see Work with Event Notification Simulations.

Work with event notification simulations

Catalyst Center platform supports event simulation, which lets you test an event's subscription (email, REST API, SNMP trap notification, syslog server, or Webex). After running an event simulation, the results (success or failure) are displayed in the GUI.

Before you begin

- For a syslog server notification of events, you configured the syslog server destination in the **Syslog** tab in Catalyst Center. To access the **Syslog** tab, click the menu icon and choose **System** > **Settings** > **External Services** > **Destinations** > **Syslog**. For detailed information about configuring a syslog server destination, see Configure a syslog server destination, on page 135.
- For an email notification, you configured the email destination in the **Email** tab in Catalyst Center. To access the **Email** tab, click the menu icon and choose **System** > **Settings** > **External Services** > **Destinations** > **Email**. For detailed information about configuring an email destination, see Configure an email destination, on page 134.
- For a REST API notification, you configured the webhook destination in the **Webhook** tab in Catalyst Center. To access the **Webhook** tab, click the menu icon and choose **System** > **Settings** > **External Services** > **Destinations** > **Webhook**. For detailed information about configuring a webhook destination, see Configure a webhook destination, on page 133.
- You have accessed the **Event Settings** window and reviewed or edited the list of events that may occur within your network for ITSM integration and can be captured by Catalyst Center. To access the **Event Settings** window, click the menu icon and choose **Platform** > **Manage** > **Configurations** > **Event Settings**.

Procedure

Step 1 From the main menu, choose **Platform** > **Developer Toolkit** > **Event Notifications** > **Event Catalog**.

Step 2 In the **Event Catalog** tab, click an event. The slide-in pane shows a **Try-It Now** button if Catalyst Center is subscribed to that event. Click **Try-It Now**.

When this data appears, you can edit only the **Details** field:

- **Event Name**: Catalyst Center system name for the event.
- **Event ID**: Identification number of the event.
- **Instance ID**: Identification number of the event's instance.
- **Name**: Name of the event.
- **Description**: Brief description of the event and how it is triggered.
- **Namespace**: Namespace of the event.

  For this release, the default value for all events is ASSURANCE.
- **Context**: Event context field.

  The default value is EXTERNAL.
- **Source**: Source field.

  The default value is EXTERNAL.
- **Type**: **Network**, **App**, **System**, **Security**, or **Integrations** type of event.
- **Category**: **Error**, **Warn**, **Info**, **Alert**, **Task Progress**, **Task Complete**.
- **Severity**: 1 through 5.

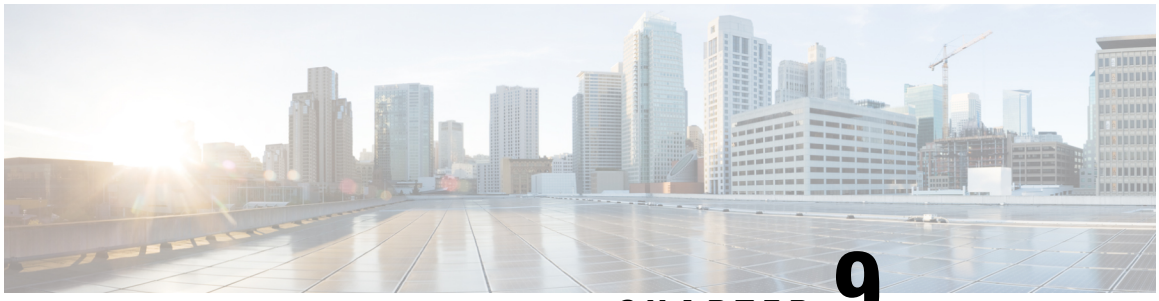
- **Domain**: REST API domain to which the event belongs.
- **Sub Domain**: Subgroup under the REST API domain to which the event belongs.
- **Details**: Field for additional user detail about the event.

Step 3 Click **X** to exit from the field.

Step 4 Click **Publish** to run the event simulation and review results.

These results appear:

- **Subscription Name**: User-created subscription name.
- **Connector Type**: Email, REST API, SNMP trap, or Syslog.
- **Status**: Loading, Success, or Fail.
- **Message**: For a REST connector type (REST API subscription), an HTTPS response appears.



CHAPTER 9

Runtime Dashboard

- About Runtime Dashboard, on page 201
- Review the event summary, on page 201
- Review the API summary, on page 208
- Review the CMDB synchronization summary, on page 209
- Review the integration flow summary, on page 211

About Runtime Dashboard

At a high level, APIs are categorized into *business APIs* (BAPIs) and *registered APIs* (RAPIs). The Runtime Dashboard only displays information for BAPIs, not RAPIs. It offers a quick overview of these summaries:

- **API Summary**: Summary of recent API calls, results, and performances. Click **View Details** to open a slide-in pane with information about individual API call counts and call durations.

  The **Runtime Dashboard** only displays data from a Catalyst Center-to-ServiceNow API integration.

- **Event Summary**: Catalyst Center events involving REST endpoints or integration flows. Click an event name (link) to open a slide-in pane with additional detailed event information.

- **CMDB Synchronization Summary**: Summary that displays the Configuration Management Database (CMDB) synchronization status of devices selected from **Inventory**.

- **Integration Flow Summary**: Summary of integration flow instances, results, and performance. Click the appropriate tab to view additional detailed information about either the REST-based or schedule-based integration flows.

Review the event summary

Follow this procedure to review the Catalyst Center platform **Event Summary**. The **Event Summary** displays the total number of events published to external systems, based on the type of event. You can use the **Event Summary** to assist in monitoring and troubleshooting the Catalyst Center platform and its integration with other systems.

You review the **Event Summary** in the **Runtime Dashboard** window in the Catalyst Center GUI.

Before you begin

For the **Event Summary** field to display events, you need to enable, configure, and activate the bundles in **Bundles**. Additionally, you need to enable associated event notifications for the bundles in **Event Settings**. For information about **Bundles**, see Bundle features, on page 110. For information about **Event Settings**, see Configure event settings, on page 127.

Procedure

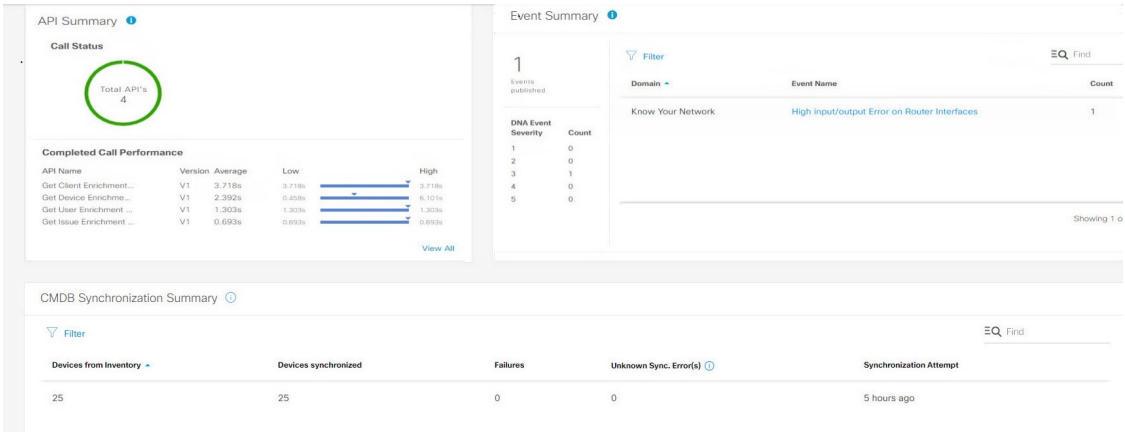
Step 1 From the main menu, choose **Platform** > **Runtime Dashboard**.

Step 2 Choose a time interval for the event summary by clicking **Last 1 Week** at the upper right side of the GUI menu bar.

You can view the event summary for the last 6, 12, and 24 hour period or for the week.

Step 3 Review the **Event Summary** field in the **Runtime Dashboard** window.

Figure 32: Events Summary field



This information appears for any current events:

- **Events Published**: Total number of events that are captured and published (displayed in the GUI) by the Catalyst Center platform.
- **Event Severity**: Event totals by severity number (1 through 5).
- **Count**: Number of events.
- **Events**: List of events by domain (category), event name (links), and count (number of events).

Note
Scroll down to view the entire list by using the scroll bar at the right of the field.

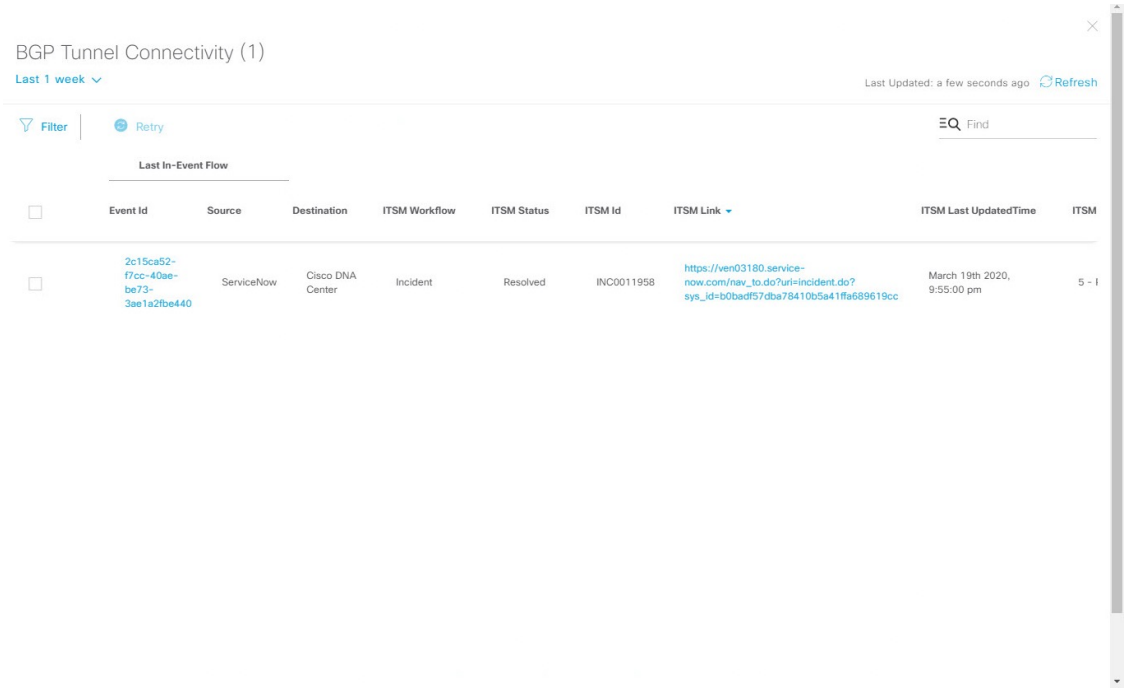
Step 4 Click an event name (link) to view additional detailed data.

As an example, if the events **Router Unreachable** or **BGP Tunnel Connectivity** exist in your GUI window click the link.

After clicking an event name (link), a slide-in pane opens.

Step 5 Review a list of this type of event (history) in the slide-in pane.

Figure 33: Event history



Individual events list this information:

- **Event ID**: Catalyst Center event identification number generated by Catalyst Center.
- **Source**: Location from where event originated. For example, the Catalyst Center platform or an ITSM system (ServiceNow).
- **Destination**: Location for where the event was directed to. For example, the Catalyst Center platform or an ITSM system (ServiceNow).
- **ITSM Workflow**: Type of ITSM workflow (for example, an **Incident** or **Problem**).
- **ITSM Status**: Current status of the event. For example, an event can have a status of **Open**, **New**, **Closed**, or **N/A**.
- **ITSM ID**: ITSM event identification number generated by the ITSM (ServiceNow).
- **ITSM Link**: Link to ITSM server for the ITSM event.
- **ITSM Last Updated Time**: Last date and time of event update.
- **ITSM Entity Severity/Priority**: ITSM severity or priority assigned to the event.
- **Event Severity**: Catalyst Center severity assigned to the event (1 through 5).

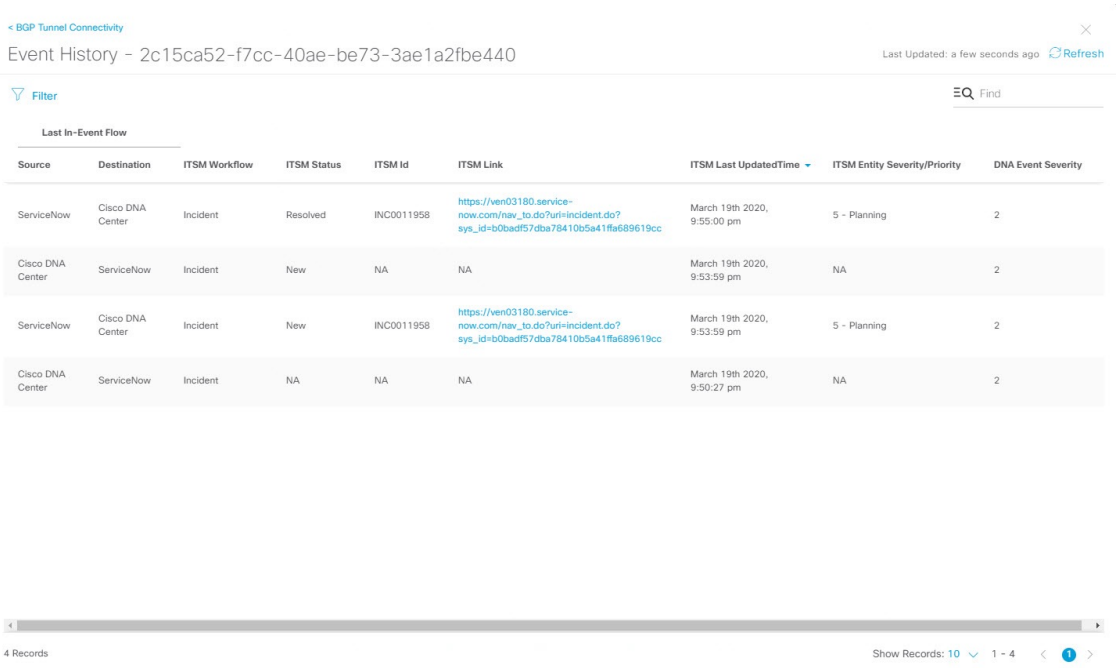
You can adjust the events that show in the table by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

Step 6 Click an event ID number (link) to view only data associated with that specific event.

After clicking an event ID number (link), a slide-in pane opens.

Step 7 Review the event ID data in the slide-in pane.

Figure 34: Event ID data



This single event information appears:

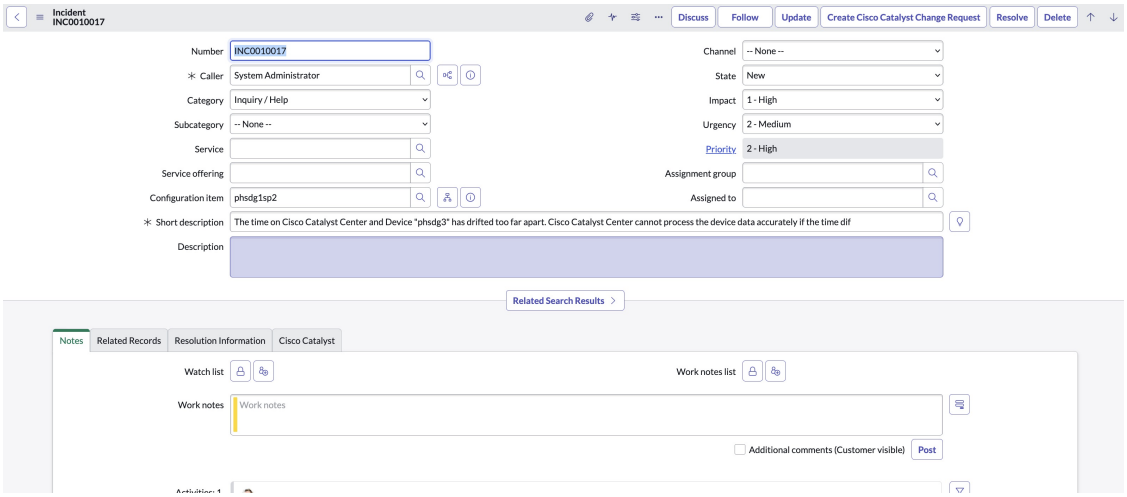
- **Source**: Location from where event originated (for example, the Catalyst Center platform).
- **Destination**: Location for where the event was directed to. For example, the REST Endpoint.
- **ITSM Workflow**: Type of ITSM workflow (for example, an **Incident** or **Problem**).
- **ITSM Status**: Current status of the event. For example, an event can have a status of **Open**, **New**, or **Resolved**.
- **ITSM ID**: ITSM event identification number.
- **ITSM Link**: Link to the ITSM (ServiceNow).
- **ITSM Last Updated Time**: Last date and time of event update.
- **ITSM Entity Severity/Priority**: ITSM severity or priority assigned to the event.
- **Event Severity**: Catalyst Center severity assigned to the event (1 through 5).

To close the slide-in pane and return to the previous window, click the event link at the top left of the window.

To close the slide-in pane in the new window and return to the **Runtime Dashboard**, click the link at the top left again.

Step 8 (Optional) Click the **ITSM Link** to open up and access the ITSM program (ServiceNow Service Management GUI) and specific incident.

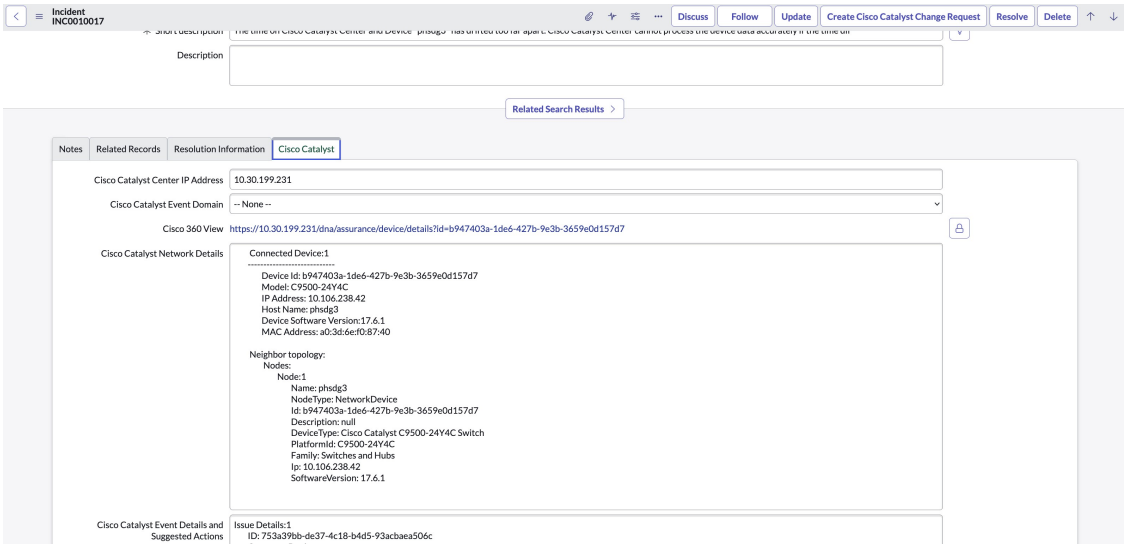
Figure 35: ServiceNow Incident



Note
For the **Runtime** event link to ITSM program to be operational, you must follow the procedures to set up the Catalyst Center platform to ServiceNow integration as described in the Cisco Catalyst Center ITSM Integration Guide.

Step 9 (Optional) Click the **Cisco Catalyst** tab in the ServiceNow Service Management GUI to review details about the event.

Figure 36: Cisco Catalyst tab



This information is available from the **Cisco Catalyst** tab:

- **Cisco Catalyst Center IP Address**
- **Cisco 360 View**
- **Cisco Catalyst Network Details**
- **Cisco Catalyst Event Domain**

- **Cisco Catalyst Event Details and Suggested Actions**
- **Cisco Catalyst Event ID**
- **Approval Status**

Retry an ITSM event

You can retry (resend and reprocess) an ITSM event from the Catalyst Center platform to an ITSM (ServiceNow) using the **Event Summary** window of the Catalyst Center GUI.

The **Event Summary** window in **Runtime Dashboard** displays the total number of events that are published to external systems, based on the type of event. You use the **Event Summary** to help monitoring and troubleshooting the Catalyst Center platform and its integration with other systems.

Before you begin

For the **Event Summary** field to display events, you must enable, configure, and activate the bundles in **Bundles**. Also, you must enable associated event notifications for the bundles in **Event Settings**.

Procedure

Step 1 From the main menu, choose **Platform** > **Runtime Dashboard**.

Step 2 Choose a time interval for the event summary by clicking **Last 1 Week** at the upper right side of the GUI menu bar.

You can view the event summary for the last 6, 12, and 24-hour period or for the week.

Step 3 Review the **Event Summary** field in the **Runtime Dashboard** window.

This information shows for any current events:

- **Events Published**: Total number of events that are captured and published (displayed in the GUI) by the Catalyst Center platform.
- **Event Severity**: Event totals by severity number (1–5).
- **Count**: Number of events.
- **Events**: List of events by domain (category), event name (links), and count (number of events).

Note
Scroll down to view the entire list by using the scroll bar at the right of the field.

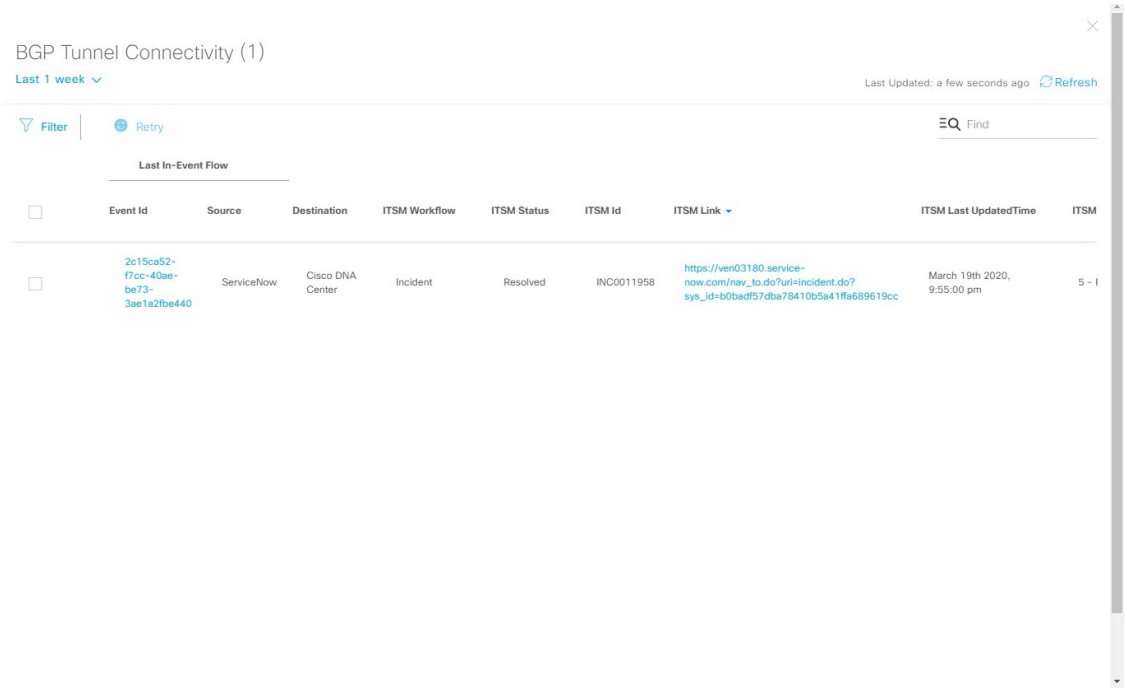
Step 4 Click an ITSM event name (link) to view more detailed data.

As an example, if the ITSM event **SWIM Upgrade Request Creation Image Activation** exists in your GUI window click the link.

After clicking an event name (link), a slide-in pane opens.

Step 5 Review a list of this type of event (history) in the slide-in pane.

Figure 37: Event history



Individual events list this information:

- **Event ID**: Catalyst Center event identification number generated by Catalyst Center.
- **Source**: Location from where event originated. For example, the Catalyst Center platform or an ITSM system (ServiceNow).
- **Destination**: Location for where the event was directed to. For example, the Catalyst Center platform or an ITSM system (ServiceNow).
- **ITSM Workflow**: Type of ITSM workflow (for example, an **Incident** or **Problem**).
- **ITSM Status**: Current status of the event. For example, an event can have a status of **Open**, **New**, **Closed**, **N/A** or, **Resolved**.
- **ITSM ID**: ITSM event identification number generated by the ITSM (ServiceNow).
- **ITSM Link**: Link to ITSM server for the ITSM event.
- **ITSM Last Updated Time**: Last date and time of event update.
- **ITSM Entity Severity/Priority**: ITSM severity or priority that is assigned to the event.
- **Event Severity**: Catalyst Center severity that is assigned to the event (1–5).

You can adjust the events that are displayed in the table by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

Step 6 Determine what ITSM events must be resent and reprocessed.

If an ITSM event displays **N/A** as a value for **ITSM Workflow**, **ITSM Status**, or **ITSM ID** (and the source of the event is ServiceNow and the destination of the event is Catalyst Center), this indicates an issue that would require a retry attempt. Also, a check box appears under the **Filter** column for an ITSM event that requires a retry attempt.

Step 7 Check the check box in the **Filter** column to select an ITSM event and enable the **Retry** button.

Step 8 Click **Retry**.

After the event is resent to the ITSM destination, one of these events occurs:

- Retry Success: Appropriate values display in the **ITSM Workflow**, **ITSM Status**, and **ITSM ID** columns for the event. For example, *RFC* in the **ITSM Workflow** column, *New* in the **ITSM Status** column, and an alphanumeric ID for the **ITSM ID**.
- Retry Failure: If the event retry fails, then the ITSM event will still display **N/A** as a value for **ITSM Workflow**, **ITSM Status**, or **ITSM ID**. See the next step for working with a second retry failure.

Step 9 (Optional) After another retry failure, in the Catalyst Center GUI, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs** > **Ecosystem Integrations** > **ITSM** > **Get Failed ITSM Events**.

Access this API method to retrieve information about the ITSM integration failure.

Step 10 Click **Try It** and enter the instance ID (**instanceId**) of the failed event from the **Runtime Dashboard**.

Step 11 Click **Run**.

This response data can be retrieved using this API:

- **eventStatus**: ITSM (ServiceNow) event status
- **errorCode**: ITSM (ServiceNow) event error code
- **errorDescription**: Description of the ITSM (ServiceNow) event error
- **responseReceivedFromITSMSystem**: ITSM (ServiceNow) response

Use the information retrieved by the API to understand and correct the event failure.

Review the API summary

Before you begin

To display events in the **API Summary** field, use bundles. Enable, configure, and activate the bundles that provide the events to monitor in the **Bundles** list. For information about **Bundles**, see Bundle features, on page 110.

Procedure

Step 1 From the main menu, choose **Platform** > **Runtime Dashboard**.

Step 2 Select a time interval for the API summary by clicking **Last 1 Week** at the upper right side of the GUI.

You can view the API summary for the last 6, 12, or 24 hour period, or for the week.

Step 3 Review the **API Summary** field.

The **API Summary** field displays this information:

- **Call Status**: Total number of API calls and status display. The color green represents the successful API calls and the color red represents the unsuccessful API calls.
- **Completed Call Performance**: List of API calls in alphabetical order with completed call performance in seconds (Low, Average, High).
- **View Details**: Link to view additional API details.

Step 4 Click **View Details** to review additional details about the APIs.

The **All APIs calls** slide-in pane opens.

Step 5 Review the information in the **All APIs calls** slide-in pane.

This information appears:

- API name
- API version
- API call count table that includes the total number of API calls, number of successful API calls (green icon), and number of unsuccessful API calls (red icon)
- API call duration table that includes minimum, maximum, and average duration

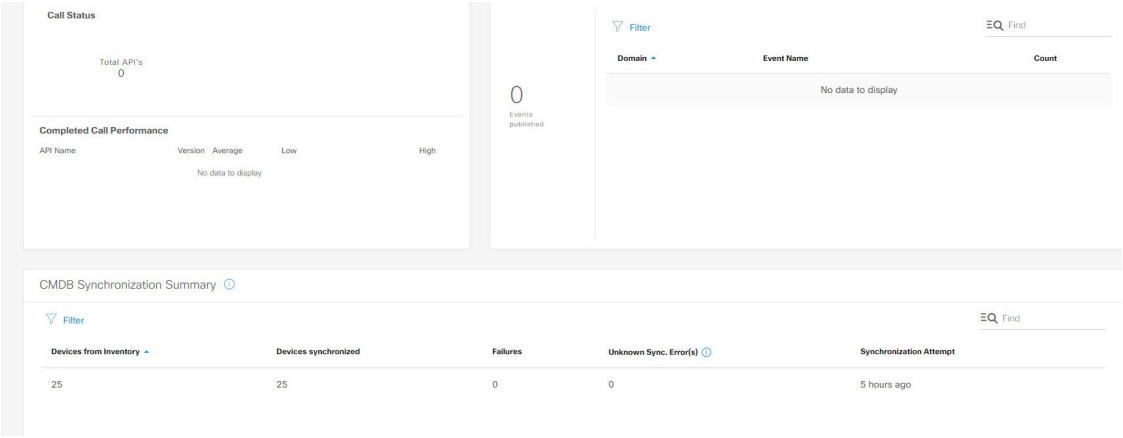
You can adjust the APIs that display in the tables by clicking the **Filter** icon and using the filter, or by entering a keyword in the **Find** field.

Review the CMDB synchronization summary

Follow this procedure to review the Catalyst Center platform **CMDB Synchronization Summary**. The **CMDB Synchronization Summary** displays the synchronization status of inventory device data to ServiceNow. You can use the summary to help monitor and troubleshoot device data synchronization with ServiceNow.

You review the **CMDB Synchronization Summary** using the **Runtime Dashboard** window in the Catalyst Center GUI.

Figure 38: Catalyst Center Platform Runtime window



Before you begin

For the **CMDB Synchronization Summary** field to display events, you must enable, configure, and activate the bundles in **Bundles**. Additionally, you must enable associated event notifications for the bundles in **Event Settings**. For information about **Bundles**, see Bundle features, on page 110. For information about **Event Settings**, see Configure event settings, on page 127.

Procedure

Step 1 From the main menu, choose **Platform** > **Runtime Dashboard**.

Step 2 Review the **CMDB Synchronization Summary** field, which displays this information:

- **Devices from inventory**: Total number of devices from **Inventory** collected from Catalyst Center.
- **Devices synchronized**: List of devices that were successful synchronized with ServiceNow.
- **Failures**: Number of failed synchronization attempts between Catalyst Center and ServiceNow.

  Click **Learn More...** for additional information.
- **Unknown Synch Errors**: Number of partially successful synchronization attempts between Catalyst Center and ServiceNow

  Click **Learn More...** for additional information.
- **Synchronization Attempt**: When the last synchronization attempt was made between Catalyst Center and ServiceNow.

Step 3 (Optional) Click the **Learn More** link for any synchronization failure.

Step 4 Review the displayed data about the synchronization failure for the device.

This information appears in a table:

- **Device ID**: Device identification number.
- **Host Name**: Name of the host to which the device is connected to.
- **Device Type**: Type of device, such as a switch, router, or AP.

- **MAC Address**: MAC address of the device.
- **Management IP Address**: Device's management address that can be used to access and troubleshoot the device.
- **Serial Number:** Serial number of the device.

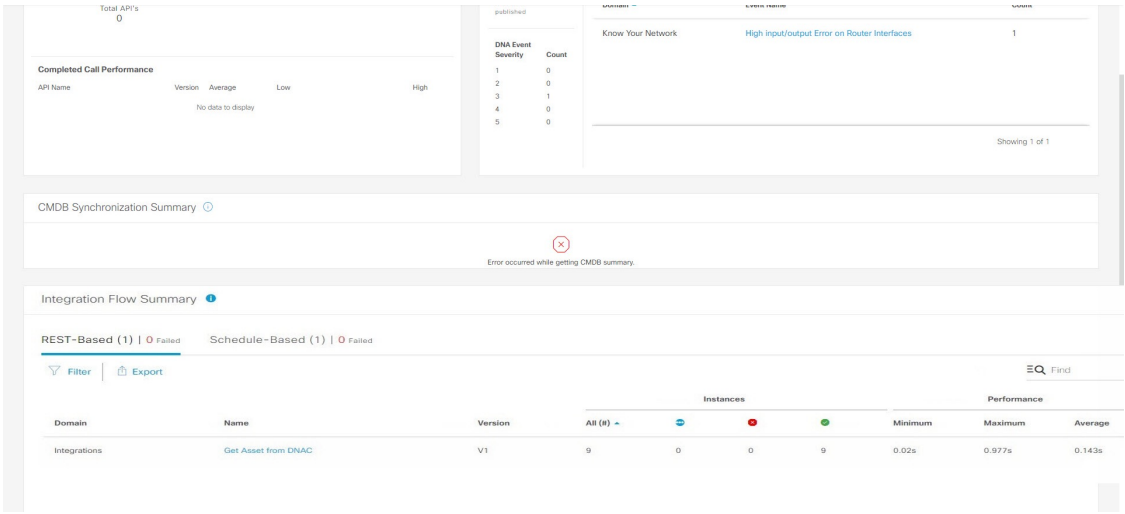
Step 5 Click the **DeviceID** link to review additional information about the device in the **Inventory** window.

Review the integration flow summary

Perform this procedure to review the Catalyst Center platform **Integration Flow Summary**. You can use the **Integration Flow Summary** to assist in monitoring performance of the Catalyst Center platform integration flows. This information can be helpful when monitoring or troubleshooting Catalyst Center platform and its integration with other systems.

You review the **Integration Flow Summary** using the **Runtime Dashboard** window in the Catalyst Center GUI.

Figure 39: Catalyst Center Platform Runtime Dashboard window



Before you begin

For the **Integration Flow Summary** fields (two tabs) to display data, you need to enable, configure, and activate the bundles that provide the events to monitor in **Bundles**. For information about **Bundles**, see Bundle features, on page 110.

Procedure

Step 1 From the main menu, choose **Platform** > **Runtime Dashboard**.

Step 2 Choose a time interval for the integration flow summary by clicking **Last 1 Week** at the upper right side of the GUI menu bar.

You can view the integration flow summary for the last 6, 12, 24 hour period or for the week.

Step 3 Review the **Integration Flow Summary** field, which displays this information:

- **REST-Based**: Domain, integration flow name and link, version, instance totals, instance status (successful [green], fail [red], in progress [blue]), and performances (minimum, maximum, and average call performance times, in milliseconds).
- **Schedule-Based**: Domain, integration flow name and link, version, instance totals, instance status (successful [green], fail [red], in progress [blue]), and performances (minimum, maximum, and average call performance times, in milliseconds).

Step 4 For a summary of the data generated by REST-based integration flows, click the **REST-Based** tab.

Step 5 Review the **REST-Based** data.

Click an integration flow name (link) to view additional information about the instances. This additional information appears in a slide-in pane:

- **Instance ID**: Identification number (and link) of the instance to the integration flow. You can configure an instance to more than one integration flow.
- **Status**: Status of the instance (success or fail).
- **Start Time**: Start date and time of the instance call.
- **End Time**: End date and time of the instance call.
- **Duration**: Duration of call, in seconds.

Step 6 Click an individual instance ID (link) to view detailed information about it.

This additional information appears in a slide-in pane:

- **RUN SUMMARY**: Start and end times and dates, time taken, status.
- **ERRORS**: Error responses (if any).
- **LOGS**: Log entries (if available).

Click the **X** icon to close the slide-in pane and return to the previous window.

Step 7 For a summary of the data generated by schedule-based integration flows, click the **Schedule-Based** tab.

Step 8 Review the **Schedule-Based** data.

Click an integration flow name (link) to view additional information about the instances. This additional information appears in a slide-in pane:

- **Instance ID**: Identification number of the instance within the integration flow.
- **Status**: Status of the instance (success or fail).
- **Start Time**: Start date and time of the instance call.
- **End Time**: End date and time of the instance call.
- **Duration**: Duration of call, in seconds.

Step 9 Click an individual instance ID (link) to view detailed information about it.

This additional information appears in a slide-in pane:

- **RUN SUMMARY**: Start and end times and dates, time taken, status.
- **ERRORS**: Error responses (if any).
- **LOGS**: Log entries (if available).

Click the **X** icon to close the slide-in pane and return to the previous window.