Cisco Catalyst Center Platform User Guide, Release 3.3.x

Cisco Catalyst Center
Updated September 9, 2026

© 2026 Cisco Systems, Inc. All rights reserved.

Abbreviated Cisco Trademarks

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)

Topics included

1 New and Changed Information....5
New and changed information....6

2 About Catalyst Center Platform....29
Features of Catalyst Center Platform....30
Intent APIs....30
Events and notifications....31

3 Deploy Catalyst Center Platform....33
Catalyst Center platform deployments....34
Installation of Catalyst Center Platform....34
Configure integration settings....34
API prerequisites....35
Supporting Role-Based Access Control....36

4 Platform Overview GUI....39
Platform overview....40
Navigate through the platform GUI....40

5 Platform Manage GUI....43
Bundle integrations and configurations....44
Bundle statuses....44
Bundle features....45
Configure a destination to receive events in a bundle....46
Configure ServiceNow access settings in a bundle....49
Configure CMDB data synchronization for ServiceNow....52

6 Configurations....63
Configurations....64
Configure event settings....64
Edit an instance in General Settings....66
Add an instance in General Settings....68
Configure a webhook destination....69
Configure email destinations for event and report notifications....71
Configure a syslog server destination....72
Configure a trap notification....73

7 Reports.....75
Reports.....76
Generate your first report.....76
Generate an access point report.....80
Generate an audit log report.....84
Generate a client report.....87
Generate a compliance report.....91
Generate a configuration archive report.....94
Generate an end-of-life report.....97
Generate an executive summary report.....100
Generate an inventory report.....103
Generate a license report.....107
Generate a network devices report.....110
Generate a rogue and aWIPS report.....114
Generate an ROI report.....117
Generate a security advisories report.....119
Generate a SWIM report.....122
Generate a flexible report.....126
Manage generated reports.....130

8 Developer Toolkit GUI.....133
Developer toolkit.....134
Work with APIs.....134
Manage integration flows.....136
Configure event notifications for network events.....139
Work with event notification simulations.....142

9 Runtime Dashboard.....145
Runtime dashboard.....146
Review the event summary.....146
Retry an ITSM event.....151
Review API summary.....153
Review the CMDB synchronization summary.....154
Review the integration flow summary.....156

1 New and Changed Information

Topics:

- New and changed information

New and changed information for this release.

New and changed information

This section details the new features and other modifications introduced in the Catalyst Center Platform across various 3.3.x releases, providing a summary of updates and where to find more information.

This table summarizes the new and changed features in Catalyst Center platform 3.3.1 release and tells you where they are documented.

Table 1: New and Changed features in Catalyst Center Platform, Release 3.3.1

Feature	Description
Reports	
Flexible Report	Catalyst Center platform supports a new entity under Flexible reports called **Network Interface**. Use the new **Network Interface** entity to generate Trend, TopN, Summary, and Distribution reports. This update integrates enhanced KPIs and advanced filtering to optimize data retrieval and provide granular visibility into network performance and health. For more information, see Generate a flexible report on page 126.
Events	
Assurance Events	Catalyst Center platform supports these new events: • NETWORK-DEVICES-4-401: This event triggers when the URWB AP Node is experiencing Packet Error Rate (PER) that is exceeding the defined URWB Critical PER threshold. • NETWORK-DEVICES-4-402: This event triggers when the URWB AP Node is experiencing MCS Index that is lower than the defined URWB Critical MCS Index threshold. • NETWORK-DEVICES-4-403: This event triggers when the URWB Link is experiencing Link Error Rate (LER) that is exceeding the defined URWB Critical LER threshold. • NETWORK-DEVICES-4-404: This event triggers when the URWB Link is experiencing RSSI that is lower than the defined URWB Link RSSI threshold. • NETWORK-DEVICES-2-900: This event triggers when there is a Traffic Steering Policy configuration failure. • NETWORK-FABRIC_WIRED-1-339: This event triggers when Fabric Control Plane Node loses connectivity to one or more Wireless Controllers. • NETWORK-DEVICES-2-157: This event triggers when the standby unit in Catalyst 9800 HA SSO pair is down, indicating redundancy failure.

Feature	Description
Rogue Events	Catalyst Center platform now provides email support to these existing events: • NETWORK-THREATS-ROGUE-01 • NETWORK-THREATS-AWIPS-01 **Note** We recommend that you use webhooks instead of email notifications if you anticipate a high volume of alerts due to scaling.
New API Operations	
Clients API Operations	With this release, Catalyst Center platform supports these API operations: • GET <cluster-ip>/dna/intent/api/v1/trackedClients Read tracked-client configurations. • POST <cluster-ip>/dna/intent/api/v1/trackedClients Create a tracked-client configuration. • POST <cluster-ip>/dna/intent/api/v1/trackedClients/query Query tracked-client configurations with request-body filters. • GET <cluster-ip>/dna/intent/api/v1/trackedClients/{id} Read a tracked-client configuration by client identifier. • PUT <cluster-ip>/dna/intent/api/v1/trackedClients/{id} Partially update a tracked-client configuration. • DELETE <cluster-ip>/dna/intent/api/v1/trackedClients/{id} Delete a tracked-client configuration. • POST <cluster-ip>/dna/intent/api/v1/trackedClients/bulkCreate Bulk create tracked-client configurations. • POST <cluster-ip>/dna/intent/api/v1/trackedClients/bulkUpdate Bulk partially update tracked-client configurations. • POST <cluster-ip>/dna/intent/api/v1/trackedClients/bulkDelete Bulk delete tracked-client configurations. To access the new Clients API operations, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Clients**.

Feature	Description
Connectivity API Operations	With this release, Catalyst Center platform supports these API operations: • GET <cluster-ip>/dna/campus/api/v1/networks Get all networks. • GET <cluster-ip>/dna/campus/api/v1/networks/${id} Get network by ID. • GET <cluster-ip>/dna/campus/api/v1/networks/count Get total number of networks. • PUT <cluster-ip>/dna/campus/api/v1/networks/${id} Update network. • POST <cluster-ip>/dna/campus/api/v1/networks Create a network. • DELETE <cluster-ip>/dna/campus/api/v1/networks/${id} Delete a network. To access the new Connectivity API operations, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**.

Feature	Description
Devices API Operations	

Feature	Description
	With this release, Catalyst Center platform supports these API operations: • GET <cluster-ip>/dna/data/api/v1/urwbNetworks Gets the URWB Network details based on the provided query parameters. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/count Gets the total URWB Network counts based on the provided query parameters. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{id} Get the URWB Network data for the given network ID. • POST <cluster-ip>/dna/data/api/v1/urwbNetworks/{id}/trendAnalytics The Trend analytics data for the URWB Network in the specified time range. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/query Gets the list of URWB Networks based on the provided complex filters and aggregation functions. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/query/count Gets the total number of URWB Networks based on the provided complex filters. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/summaryAnalytics Gets the summary analytics data related to URWB Networks. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/topNAnalytics Gets the Top-N analytics data for URWB Networks. GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/links Gets the URWB Link details for a specific network. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/links/count Gets the total URWB Link counts for a specific network. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/links/{id} Get the URWB Link data for the given link ID. • POST <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/links/{id}/trendAnalytics The Trend analytics data for the URWB Link in the specified time range. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/links/query Gets the list of URWB Links based on the provided complex filters and aggregation functions. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/links/query/count

Feature	Description
	Gets the total number of URWB Links based on the provided complex filters. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/links/summaryAnalytics Gets the summary analytics data related to URWB Links. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/links/topNAnalytics Gets the Top-N analytics data for URWB Links. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/nodes Gets the URWB Node details for a specific network. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/nodes/count Gets the total URWB Node counts for a specific network. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/nodes/{id} Get the URWB Node data for the given node ID. • POST <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/nodes/{id}/trendAnalytics The Trend analytics data for the URWB Node in the specified time range. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/nodes/query Gets the list of URWB Nodes based on the provided complex filters and aggregation functions. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/nodes/query/count Gets the total number of URWB Nodes based on the provided complex filters. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/nodes/summaryAnalytics Gets the summary analytics data related to URWB Nodes. • GET <cluster-ip>/dna/data/api/v1/urwbNetworks/{urwbNetworkId}/nodes/topNAnalytics Gets the Top-N analytics data for URWB Nodes. To access the new Devices API operations, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Devices**.

Feature	Description
Device Replacement API Operations	With this release, Catalyst Center platform supports these API operations: • GET <cluster-ip>/dna/intent/api/v1/networkDevices/refresh Requests Retrieve the status of all device refresh workflows. • POST <cluster-ip>/dna/intent/api/v1/networkDevices/refresh Requests Mark a network device for refresh. • GET <cluster-ip>/dna/intent/api/v1/networkDevices/refreshRequests/count Return refresh devices count. • GET <cluster-ip>/dna/intent/api/v1/networkDevices/refreshRequests/{id} Retrieve the status of a specific device refresh workflow. • DELETE <cluster-ip>/dna/intent/api/v1/networkDevices/refreshRequests/{id} Unmark a network device marked for refresh. • POST <cluster-ip>/dna/intent/api/v1/networkDevices/refreshRequests/bulk Mark network devices for refresh. • DELETE <cluster-ip>/dna/intent/api/v1/networkDevices/refreshRequests/bulkDelete Unmark network devices marked for refresh. • POST <cluster-ip>/dna/intent/api/v1/networkDevices/refreshRequests/deploy Deploy network device refresh workflows. • POST <cluster-ip>/dna/intent/api/v1/networkDevices/refreshRequests/validations Validate device compatibility for bulk refresh. To access the new Device Replacement API operations, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Device Replacement**.

Feature	Description
Industrial Configuration API Operations	

Feature	Description
	With this release, Catalyst Center platform supports these API operations: • POST <cluster-ip>/dna/intent/api/v1/iot/fabric/prp/configurationModels/create Create configuration model for adding PRP configuration. • POST <cluster-ip>/dna/intent/api/v1/iot/fabric/prp/configurationModels/update Create configuration model for updating PRP configuration. • POST <cluster-ip>/dna/intent/api/v1/iot/fabric/prp/configurationModels/delete Create configuration model for deleting PRP configuration. • GET <cluster-ip>/dna/intent/api/v1/iot/fabric/prp/configurationModels/{previewActivityId}/networkDeviceStatusDetails Retrieve configuration model generation status for PRP. • GET <cluster-ip>/dna/intent/api/v1/iot/fabric/prp/configurationModels/{previewActivityId}/networkDevices/{networkDeviceId}/config Retrieve generated PRP configuration for the given network device and PRP configuration model. • POST <cluster-ip>/dna/intent/api/v1/iot/fabric/prp/configurationModels/{previewActivityId}/networkDevices/{networkDeviceId}/config Generate PRP configuration for the given network device and PRP configuration model. • POST <cluster-ip>/dna/intent/api/v1/iot/fabric/prp/configurationModels/{previewActivityId}/deploy Deploy the configuration model for PRP on network devices. • DELETE <cluster-ip>/dna/intent/api/v1/iot/fabric/prp/configurationModels/{previewActivityId} Delete a PRP configuration model. • PUT <cluster-ip>/dna/intent/api/v1/iot/fabric/prp/deploy Update PRP configuration without generating config preview. • POST <cluster-ip>/dna/intent/api/v1/iot/fabric/prp/deploy Deploy PRP configuration without generating config preview. • DELETE <cluster-ip>/dna/intent/api/v1/iot/fabric/prp/deploy Delete PRP configuration without generating a config preview. • GET <cluster-ip>/dna/intent/api/v1/iot/fabric/prp Retrieve details of the PRP topologies configured. • GET <cluster-ip>/dna/intent/api/v1/iot/fabric/prp/count Retrieve total count of PRP topologies. • GET <cluster-ip>/dna/intent/api/v1/iot/repRings/query

Feature	Description
	Retrieves the list of REP rings. • POST <cluster-ip>/dna/intent/api/v1/iot/fabric/repRings Configure a REP Ring on FABRIC deployment. • POST <cluster-ip>/dna/intent/api/v1/iot/nonFabric/repRings Configure a REP Ring on NON-FABRIC deployment. • GET <cluster-ip>/dna/intent/api/v1/iot/repRings/{id} Get the REP ring based on the ring id. • DELETE <cluster-ip>/dna/intent/api/v1/iot/fabric/repRings/{id} Delete REP ring configured in the FABRIC deployment. • DELETE <cluster-ip>/dna/intent/api/v1/iot/nonFabric/repRings/{id} Delete REP ring configured in the NON-FABRIC deployment. • GET <cluster-ip>/dna/intent/api/v1/iot/repRings/query/count Retrieves the count of REP rings. To access the new Industrial Configuration API operations, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Industrial Configuration**.
Network Settings API Operations	With this release, Catalyst Center platform supports these API operations: • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/aaaTrustSecSettings Set aaa trustsec settings for a site. • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/aaaTrustSecSettings Retrieve aaa trustsec settings for a site To access the new Network Settings API operations, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Network Settings**.
Sensors API Operations	With this release, Catalyst Center platform supports these API operations: • POST <cluster-ip>/dna/data/api/v1/icap/captureFiles/${id}/analyze Analyzes a packet capture file. • PUT <cluster-ip>/dna/intent/api/v1/icap/settings/${id} Updates ICAP related settings. • GET <cluster-ip>/dna/intent/api/v1/icap/settings Fetches ICAP related settings. To access the new Sensors API operations, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Know Your Network** drop-down list and choose **Sensors**.

Feature	Description
Site Design API Operations	

Feature	Description
	With this release, Catalyst Center platform supports these API operations: • GET <cluster-ip>/dna/intent/api/v1/outdoorAreas/{outdoorAreaId}/accessPointPositions Get Outdoor Access Points Positions. • GET <cluster-ip>/dna/intent/api/v1/outdoorAreas/{outdoorAreaId}/accessPointPositions/count Get Access Outdoor Points Positions count. • POST <cluster-ip>/dna/intent/api/v1/outdoorAreas/{outdoorAreaId}/accessPointPositions/bulkChange Bulk change Outdoor Access Points Positions. • GET <cluster-ip>/dna/intent/api/v1/outdoorAreas/{outdoorAreaId}/plannedAccessPointPositions Get Planned Outdoor Access Points Positions. • DELETE <cluster-ip>/dna/intent/api/v1/outdoorAreas/{outdoorAreaId}/plannedAccessPointPositions/{id} Delete Outdoor Planned Access Point Position. • POST <cluster-ip>/dna/intent/api/v1/outdoorAreas/{outdoorAreaId}/plannedAccessPointPositions/assignAccessPointPositions Assign Planned Access Points to operations ones. • POST <cluster-ip>/dna/intent/api/v1/outdoorAreas/{outdoorAreaId}/plannedAccessPointPositions/bulk Bulk change Planned Outdoor Access Point Positions. • POST <cluster-ip>/dna/intent/api/v1/outdoorAreas/{outdoorAreaId}/plannedAccessPointPositions/bulkChange Bulk change Planned Outdoor Access Point Positions. • GET <cluster-ip>/dna/intent/api/v1/outdoorAreas/{outdoorAreaId}/plannedAccessPointPositions/count Get Planned Outdoor Access Points Positions Count. • POST <cluster-ip>/dna/intent/api/v1/outdoorAreas Create outdoor area. • GET <cluster-ip>/dna/intent/api/v1/outdoorAreas/{id} Get outdoor area. • PUT <cluster-ip>/dna/intent/api/v1/outdoorAreas/{id} Update outdoor area. • DELETE <cluster-ip>/dna/intent/api/v1/outdoorAreas/{id} Delete outdoor area. • POST <cluster-ip>/dna/intent/api/v1/outdoorAreas/{id}/uploadImage Upload outdoor area image.

Feature	Description
	• GET <cluster-ip>/dna/intent/api/v1/maps/accessPointAntennas Get Supported Access Point and Antenna Information. • GET <cluster-ip>/dna/intent/api/v1/maps/accessPointAntennas/count Get Supported Access Point and Antenna Information count. To access the new Site Design API operations, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Site Management** drop-down list and choose **Site Design**.
System Settings API Operations	With this release, Catalyst Center platform supports these API operations: • GET <cluster-ip>/intent/api/v1/ipam/serverSetting/validationReports Retrieves the most recent sync/validation report. • GET <cluster-ip>/intent/api/v1/ipam/serverSetting/exports Retrieves the most recent export report. • POST <cluster-ip>/intent/api/v1/ipam/serverSetting/validationReports API to create external IPAM validation report. Compares pools between Catalyst Center and the external IPAM and identifies conflicting and non-conflicting pools. • POST <cluster-ip>/intent/api/v1/ipam/serverSetting/exports Integrates the external IPAM to Catalyst Center and exports the selected pools to the external IPAM server. To access the new System Settings API operations, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**.

Feature	Description
Wireless API Operations	With this release, Catalyst Center platform supports these new Wireless API operations: • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/wlanSchedulers Create WLAN scheduler. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/wlanSchedulers Get all WLAN schedulers. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/wlanSchedulers/${id} Get WLAN scheduler by ID. • DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/wlanSchedulers/${id} Delete WLAN scheduler. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/wlanSchedulers/count Get WLAN scheduler count. • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/regulatoryActivations Download Regulatory Activation File. • POST <cluster-ip>/dna/intent/api/v1/wirelessControllers/regulatoryActivations Upload Regulatory Activation File. • DELETE <cluster-ip>/dna/intent/api/v1/wirelessControllers/regulatoryActivations Delete Regulatory Activation File. • POST <cluster-ip>/dna/intent/api/v1/wirelessControllers/regulatoryActivations/${fileId}/deploy Deploy Regulatory Activation File. To access the new Wireless API operations, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. Expand the **Connectivity** drop-down list and choose **Wireless**.
BETA API Operations	

Feature	Description
In this release, Catalyst Center platform supports new Beta API operations. To access them, click the menu icon and choose **Platform** > **Developer Toolkit** > **APIs**. **Note** You can identify the Beta API operations by the "BETA" banner on the GUI or the `x-rapi-banner` field within the swagger documentation.	

API Enhancements

Feature	Description
Compliance API Operations	

Feature	Description
	The `deviceRoles` attribute is included in the request payload of these API operations. This helps you specify the roles of the network devices to which the rule applies. If value is not provided, the rule will apply to all device roles. • POST <cluster-ip>/dna/intent/api/v1/compliancePolicys/${policyId}/rules Create a new rule. • PUT <cluster-ip>/dna/intent/api/v1/compliancePolicys/${policyId}/rules/${id} Update an existing rule. • GET <cluster-ip>/dna/intent/api/v1/compliancePolicys/${policyId}/rules/${id} Retrieve a specific rule. • GET <cluster-ip>/dna/intent/api/v1/compliancePolicys/${policyId}/rules Retrieve the rules. `potentialNoticeCount` is added as a query parameter in these API operations: • 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. With this release, `matchRemediationCommandsLanguage`, `matchRemediationCommands`, `doesNotMatchRemediationCommandsLanguage`, and `doesNotMatchRemediationCommands` attributes are added in the query of these API operations: • POST <cluster-ip>/dna/intent/api/v1/compliancePolicys/${policyId}/rules/${ruleId}/conditions Create a new condition. • PUT <cluster-ip>/dna/intent/api/v1/compliancePolicys/${policyId}/rules/${ruleId}/conditions/${id} Update an existing condition. With this release, `matchRemediationCommandsLanguage`, `matchRemediationCommands`, `doesNotMatchRemediationCommandsLanguage`, and `doesNotMatchRemediationCommands` attributes are available in the response of these API operations: • GET <cluster-ip>/dna/intent/api/v1/compliancePolicys/${policyId}/rules/${ruleId}/conditions/${id} Retrieve a specific condition.

Feature	Description
	• GET <cluster-ip>/dna/intent/api/v1/compliancePolicys/${policyId}/rules/${ruleId}/conditions Retrieve the conditions. With this release, `remediationSupported` attribute is available in the response of this API operation: • GET <cluster-ip>/dna/intent/api/v1/compliance/networkDevices/${networkDeviceId}/detail/policys Retrieve the violating policies. The **Compliance Details of Device**, **Device Compliance Status**, **Get Compliance Detail**, and **Get Compliance Status** API operations now support the `Non-Compliant`, `Compliant`, and `Compliant with Warning` states.
Devices API Operations	With this release, these network device API operations include a new **ENUM REACHABILITY_RECOVERED** error code which indicates that a device has successfully transitioned from unreachable to reachable status.The `syncProgress` and `fullSyncDuration` attibutes are also included in the response. • GET <cluster-ip>/dna/intent/api/v1/networkDevices/${id} Get details of a single network device. • POST <cluster-ip>/dna/intent/api/v1/networkDevices/query Query network devices with filters. • GET <cluster-ip>/dna/intent/api/v1/networkDevices Retrieve network devices. With this release, filter keys support is extended to these API operations: • GET <cluster-ip>/dna/intent/api/v1/networkDevices/query/count Count the number of network devices with filters. • GET <cluster-ip>/dna/intent/api/v1/networkDevices/query Query network devices with filters.
Device Replacement API Operation	An optional string parameter called `configKey` is included for the ‘SWITCH’ and ‘ROUTER’ types in the query of this API operation: • POST <cluster-ip>/dna/intent/api/v1/networkDeviceReplacements/workflow/deploy Deploy device replacement workflow.

Feature	Description
LAN Automation API Operations	With this release, there are new enhancements to the existing LAN Automation API operations to support OSPF-based underlay configuration, in addition to the existing IS-IS underlay support. The `routingProtocol`, `processId`, `areaId`, `authenticationKey` and `advertiseLANAutomationRoutesIntoBGP` OSPF-related parameters are introduced in the request and response schemas of these API operations: • POST <cluster-ip>/dna/intent/api/v2/lan-automation LAN Automation Start V2. • GET <cluster-ip>/dna/intent/api/v1/lan-automation/status LAN Automation status. • GET <cluster-ip>/dna/intent/api/v1/lan-automation/status/${id} LAN Automation Status by ID.

Feature	Description
Network Settings API Operations	These API operations now support `RADIUS_OVER_DTLS` and `TACACS_OVER_TLS` protocol. • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/aaaSettings Set AAA settings for a site. • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/aaaSettings Retrieve AAA settings for a site **Note** In these API operations, the `primaryServerName` and `secondaryServerName` attributes are introduced to facilitate SAN configuration on the device. • GET <cluster-ip>/dna/intent/api/v1/authentication-policy-servers Get authentication and policy servers. • POST <cluster-ip>/dna/intent/api/v1/authentication-policy-servers Add authentication and policy server access configuration. • PUT <cluster-ip>/dna/intent/api/v1/authentication-policy-servers Edit authentication and policy server access configuration. **Note** These API operations now support RADIUS over DTLS and TACACS+ over TLS, introducing the `radiusDtlsPort`, `radiusDtlsIdleTimeout`, `tacacsTlsPort`, and `tacacsTlsIdleTimeout` attributes, along with the AAA-only `radiusDtlsCert` and `tacacsTlsCert` attributes; the `serverName` attribute has also been added for AAA and ISE configurations.
SDA API Operations	

Feature	Description
	During the migration of a fabric site from LISP BGP to LISP PUBSUB, Catalyst Center platform now supports migration segmentation protocols for fabric sites, virtual networks, and transits to indicate the current stage of migration for each fabric entity. Each fabric site can now return `PHASE_1` or `PHASE_2` as `networkProtocol` value in the response of these API operations: • 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/${id} Read Fabric Sites with health summary from ID. Each virtual network can now return `HYBRID` as the `networkProtocol` value in the response of these API operations: • GET <cluster-ip>/dna/data/api/v1/transitNetworkHealthSummaries Read list of Transit Networks with their health summary. • GET <cluster-ip>/dna/data/api/v1/transitNetworkHealthSummaries/${id Read transit network with its health summary from ID. • GET <cluster-ip>/dna/data/api/v1/virtualNetworkHealthSummaries Read list of Virtual Networks with their health summary. • GET <cluster-ip>/dna/data/api/v1/virtualNetworkHealthSummaries/${id} Read virtual network with its health summary from ID. This release provides enhanced health visibility for Wireless LAN Controllers (WLCs) in multisite fabric deployments. The `wirelessControllerGoodHealthPercentage`, `wirelessControllerTotalHealthDeviceCount`, `wirelessControllerPoorHealthDeviceCount`, `wirelessControllerFairHealthDeviceCount` and `wirelessControllerNoDataDeviceCount` attributes are now available in the response of these `fabricSiteHealthSummaries`API operations: • GET <cluster-ip>/dna/data/api/v1/fabricSiteHealthSummaries Read list of Fabric Sites with their health summary. • GET <cluster-ip>/dna/data/api/v1/fabricSiteHealthSummaries/${id}/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/fabricSiteHealthSummaries/${id} Read Fabric Sites with health summary from ID.

Feature	Description
Site Design API Operation	With this release, `sortby` and `order` parameters are added in the query of the Get Sites API operation.
System Settings API Operations	This update extends the `IpamProvider` schema by introducing `BLUECAT_V2API` as a new enum value, allowing clients to configure BlueCat v2 as an external IPAM provider. `BLUECAT_V1API` continues to be supported for now but is planned for deprecation in a future release.
Task API Operation	`OccurrenceCount` and `RepeatInterval` attributes are included in the response of the Get activities by ID API operation. This addition extends support to recurring schedules via the Intent API.

Feature	Description
Wireless API Operations	With this release, these wireless profile API operations now include `"wlanProfileName": "trialSSIDProfile"` in the response for mapping wlans to SSIDs. • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles Get wireless profiles. • POST <cluster-ip>/dna/intent/api/v1/wirelessProfiles Create wireless profile. • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id} Get wireless profile by ID. • PUT <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id} Update wireless profile. • DELETE <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id} Delete wireless profile. • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/count Get wireless profiles count. With this release, these wireless profile API operations now include the `macSecSetting` object in the query to support MACsec (Media Access Control Security) configuration for AP authentication. • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles Create AP Profile. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles Get AP Profiles. • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles/${id} Get AP Profile by ID. • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles/${id} Update AP Profile by ID. With this release, the Get RF Profiles, Update RF Profile, Get RF Profile by ID and Create RF Profile API operations now include `minDbsWidth` and `maxDbsWidth` attributes under the 5-GHz `radioTypeAProperties` schema. The default value for both fields is 40. For 6-GHz, the `minDbsWidth` and `maxDbsWidth` values default to 80. The Wireless PDC and MDC API operations are streamlined by removing unused attributes, including `Layer 2 VTP`. They now support `AP Priming` with related child profiles and `matchServerIdentities` under TACACS servers.

2 About Catalyst Center Platform

Topics:

- Features of Catalyst Center Platform
- Intent APIs
- Events and notifications

This chapter introduces the Catalyst Center Platform, explaining its extensible architecture, the role of Intent APIs, and its event and notification services for optimizing network operations.

Features of Catalyst Center Platform

This section provides a high-level overview of the Catalyst Center platform, emphasizing its extensibility, value-added application creation capabilities, and its role in optimizing IT processes through Intent APIs, integration flows, and event or notification services.

Catalyst Center platform is a network management solution that

- provides extensibility for building value-added applications,
- enables optimization of IT processes through integrated APIs and workflows, and
- supports event and notification services to streamline operations.

Catalyst Center provides an extensible platform that allows customers and partners to create applications that can be built on top of its native capabilities. These platforms optimize end-to-end IT processes, reduce total cost of ownership (TCO), and help create new value networks by leveraging Intent APIs, integration flows, and event and notification services.

Features

- 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, 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, enabling IT operators to scale and accelerate operations in modern data centers with intelligent, end-to-end workflows built using 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

This section explains Intent APIs and how they provide Northbound REST interfaces to abstract business intent for policy-driven network management.

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.

Events and notifications

This section describes how Catalyst Center platform sends custom notifications for specific events. It highlights the utility for third-party systems to trigger business actions and explains how to view available events for customization

Catalyst Center platform event is a notification mechanism that

- triggers custom notifications when specific conditions are met,
- enables integration with third-party applications such as IT Service Management (ITSM) tools, and
- supports publishing events through webhook REST endpoints for automated workflows.

Catalyst Center platform supports sending custom notifications based on event triggers.

This feature is valuable for third-party systems that act on specific event types. For example, when a network device is not compliant, a custom application can receive notifications and initiate a software upgrade.

From the main menu, choose **Platform** > **Manage** > **Configurations** to view available events for a specific release. You can customize these events for IT Service Management (ITSM) incidents.

3 Deploy Catalyst Center Platform

Topics:

- Catalyst Center platform deployments
- Installation of Catalyst Center Platform
- Configure integration settings
- API prerequisites
- Supporting Role-Based Access Control

This chapter outlines the steps required to deploy the Catalyst Center Platform, covering installation, integration settings configuration, API prerequisites, and role-based access control.

Catalyst Center platform deployments

Use this concept to understand the deployment models, purposes, and foundational requirements for the Catalyst Center platform.

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 34.
2. To configure the integration settings, see Configure integration settings on page 34.

After you deploy the Catalyst Center platform, you must:

- Review the API prerequisites. For information, see API prerequisites on page 35.
- Review the brief feature descriptions in **Overview** in the GUI to understand the Catalyst Center platform. For information, see Platform overview on page 40.
- Go to **Bundles** in the GUI. Enable, configure, and activate the bundles needed for your network. For information, see Bundle features on page 45.

Installation of Catalyst Center Platform

This section clarifies that the Catalyst Center platform is installed automatically with Catalyst Center, eliminating the need for a separate installation procedure, and specifies that users with the SUPER-ADMIN-ROLE have full access to its GUI functionalities.

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

This section provides instructions for configuring integration settings, particularly for scenarios involving firewalls or external network access. After you complete a backup and restore operation, update the Callback URL Host Name or IP Address.

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.

> **Note**
>
> 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

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

3. Click **Apply**.

What to do next

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

> **Note**
>
> In dual-stack Catalyst Center clusters, IPv4 is the default source IP for ServiceNow callbacks, regardless of whether IPv6 is also configured in the **Integration Settings** window. Because the integration logic prioritizes IPv4, you must ensure the IPv4 address is explicitly configured in the **Cisco Catalyst Controller Properties** table within ServiceNow to guarantee successful callback operations. To maintain consistent connectivity, always define these settings manually rather than relying on auto-detection.

API prerequisites

This section details the necessary prerequisites for working with Catalyst CenterAPI, including supported programming languages (e.g., Python requests library) and authentication process based on tokens required for API access.

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

This section explains how Catalyst Center supports RBAC, alloOnly a user with SUPER-ADMIN-ROLE privileges can perform this procedure.wing users with the SUPER-ADMIN-ROLE to define custom roles with specific permissions (read, write, deny) for various platform features like APIs, bundles, events, and reports.

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

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.

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:

     a. 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.

     b. From the **Role List** drop-down list, choose the custom role, and then click **Save**.

   - To assign the custom role to a new user:

     a. Click **Add**.

        The **Create Internal User** slide-in pane appears.

     b. Enter the first name, last name, email, and username in the fields provided.

     c. From the **Role List** drop-down list, choose the custom role to assign to the new user.

     d. Enter the password and then confirm it.

     e. Click **Save**.

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

4 Platform Overview GUI

Topics:

- Platform overview
- Navigate through the platform GUI

This chapter describes the graphical user interface for the Catalyst Center platform's overview, providing quick access and summaries of bundles, the developer toolkit, runtime dashboard, and configuration options.

Platform overview

This section describes the main features and navigation of the Catalyst Center platform Overview page, which provides summaries and direct links to key GUI components such as Bundles, Developer Toolkit, Runtime Dashboard, and Configurations, along with bundle update notifications.

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:

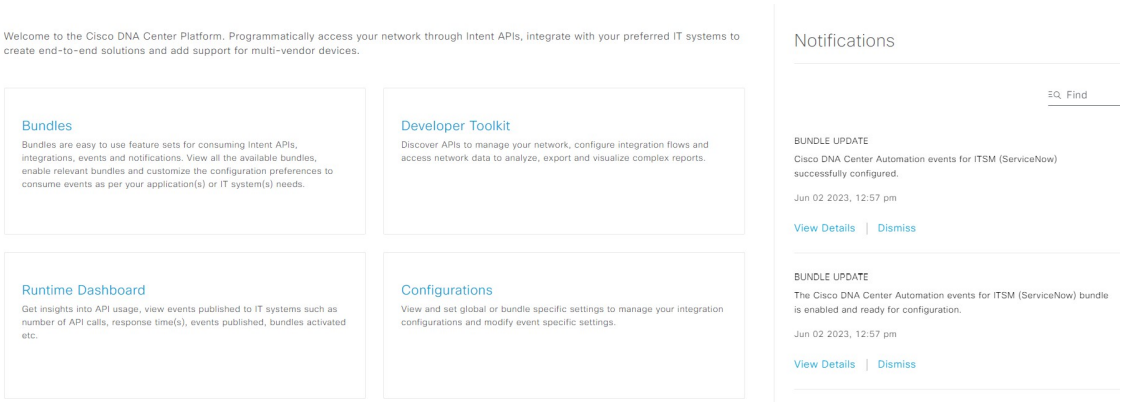
- View summaries and access direct links to important GUI features, including:
  - **Bundles**: Provides access to bundles, which are groupings of APIs, events, integration flows, data services, or applications. The **Bundles** section also includes a link to **Configurations**, where you can configure 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 navigate and review the features and functions available in the Catalyst Center platform **Overview** window. You can access individual features and check bundle update information.

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

1. From the main menu, choose **Platform** > **Overview**.
2. Review the options available in the **Overview** window.
3. Click the links to access individual Catalyst Center platform features directly.
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).

5 Platform Manage GUI

Topics:

- Bundle integrations and configurations
- Bundle statuses
- Bundle features
- Configure a destination to receive events in a bundle
- Configure ServiceNow access settings in a bundle
- Configure CMDB data synchronization for ServiceNow

This chapter details how to manage the Catalyst Center Platform via its GUI, focusing on enabling, configuring, and activating bundles for integration with services like ServiceNow.

Bundle integrations and configurations

This section explains how **Manage** window provides access to bundle integration and configuration features on the platform.

Use the Catalyst Center platform **Manage** window to access these integration and configuration features.

- **Bundles**: Use bundles to integrate Catalyst Center with your own applications or to enhance the performance of Catalyst Center. Each bundle includes APIs, events, integration flows, data services, or applications you can use.

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

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

Bundle statuses

This section defines bundles as groupings of APIs, events, integration flows, data services, or applications, and explains how the Catalyst Center GUI displays information about each bundle, including its status (NEW, ENABLED, DISABLED, ACTIVE, UPDATE, ERROR).

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.

You can access the bundle name, vendor, version, version release date, tags, and description, and bundle status details using the GUI.

The GUI shows one of these bundle statuses.

- **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.

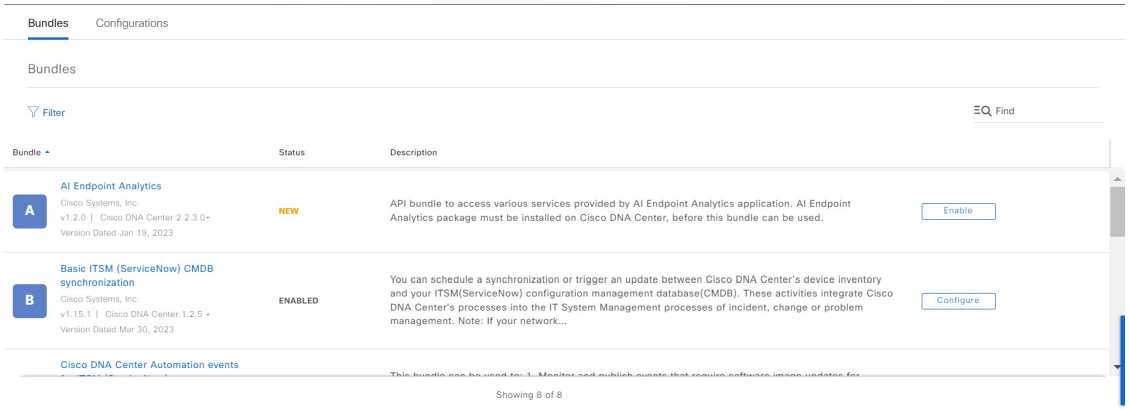
  The enablement and configuration of bundles are two separate operations. Usually, a business manager enables a bundle as a business decision. An IT or network administrator then configures the bundle.
- **DISABLED**: The bundle has been stopped from executing any further.
- **ACTIVE**: After either reviewing 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

This section highlights the capabilities offered by bundles, such as reviewing APIs, enabling Rogue Management and aWIPS, configuring event destinations for ServiceNow, setting access credentials, and synchronizing CMDB data, listing various available bundle types.

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 134.
- 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 134.
- 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 a destination to receive events in a bundle on page 46.
- 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 ServiceNow access settings in a bundle on page 49.
- 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 CMDB data synchronization for ServiceNow on page 52.

Catalyst Center consists of these bundles.

- **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 a destination to receive events in a bundle

Learn how to configure a destination to receive network and SWIM events for ServiceNow within specific bundles.

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

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

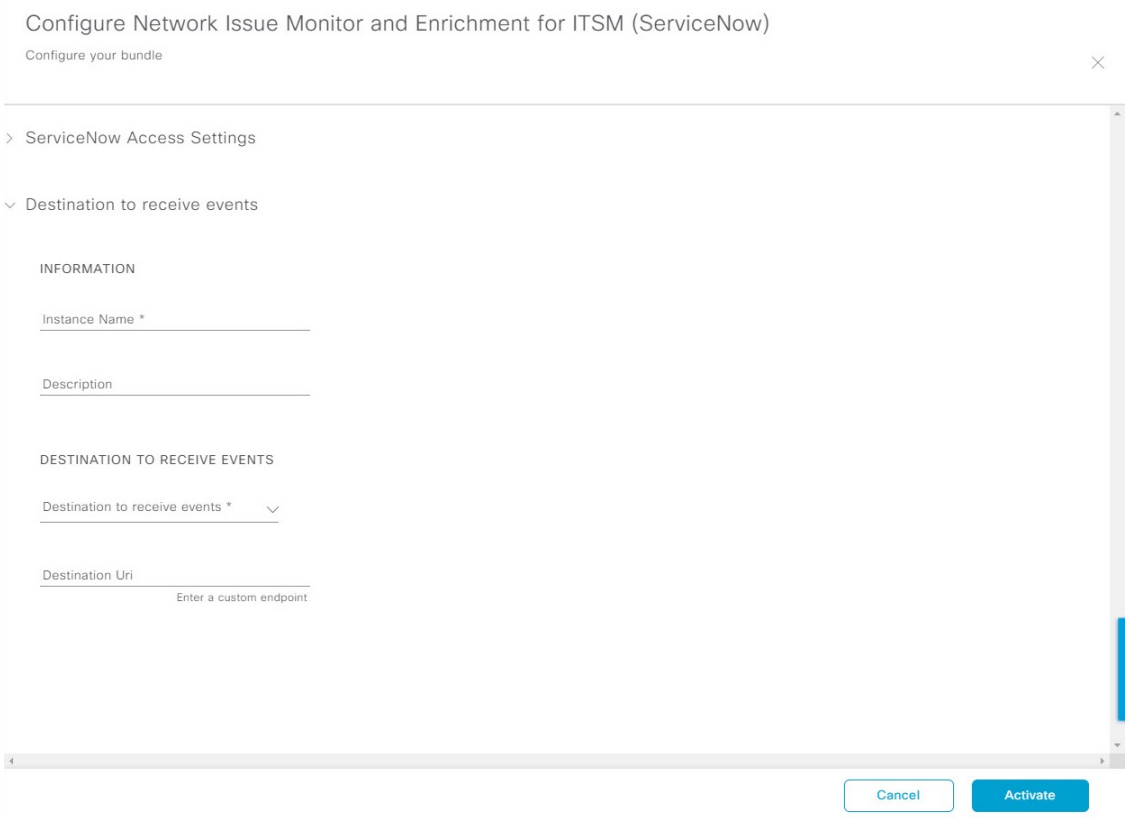
1. From the main menu, choose **Platform** > **Manage** > **Bundles**.
2. Click the **Network Issue Monitor and Enrichment for ITSM (ServiceNow)** or **Automation events for ITSM (ServiceNow)** bundle to access these details.
   - **General information**: Vendor, version, platform, and tags are shown under the square icon.

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

- **Information**: Use this tab to view general information about the bundle, including its purpose, how it works in the network, sample schemas, mapping notes, and configuration notes.
- **Contents**: Use this tab to view information about the integration flows within the bundle.
- **Release Notes**: Use this tab to view the latest release information about the bundle, including its version.

3. Review each tab to view information about the bundle.
4. Click **Enable** to enable the bundle.
5. In the **Information** field, click **Enable** to confirm enabling the bundle.
6. In the Success message, click **Okay**.
7. Click **Configure** to configure at the bundle level.
8. In the configuration slide-in pane, click **Destination to receive events** to set up 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. This allows you to create an incident, problem, or change ticket based on your selected configuration in Catalyst Center. For additional information about setting this up with ServiceNow, see the *Cisco Catalyst Center ITSM Integration Guide*.

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

   To configure an existing Destination instance, select it from the drop-down list and click **Activate**

10. Enter these details to configure a new Destination instance.

    - **Instance Name**: name of the instance.
    - **Description**: describe the instance using text.
    - **Destination to receive events**: to configure the 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, continue to the next step.

11. Click **Activate** to save your changes and activate the bundle. Click **Cancel** to close the slide without saving.

> **Note**
>
> When you click **Activate**, the bundle is updated immediately. The 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 Edit an instance in General Settings on page 66.

Configure ServiceNow access settings in a bundle

Configure ServiceNow access settings within a bundle, including providing instance details and verifying connectivity.

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

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

   Review bundle information in these available tabs.

   - **General information**: This tab displays vendor, version, platform, and tags.

     Note

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

   - **Information**: This tab 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**: This tab 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**: This tab displays the latest release information about the bundle, including its version.

3. Click each of the preceding tabs and review the information about the bundle.
4. Click **Enable** to activate the link.
5. In the **Information** field, click **Enable** to confirm enabling the bundle.
6. In the success message, click **Okay**.
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).

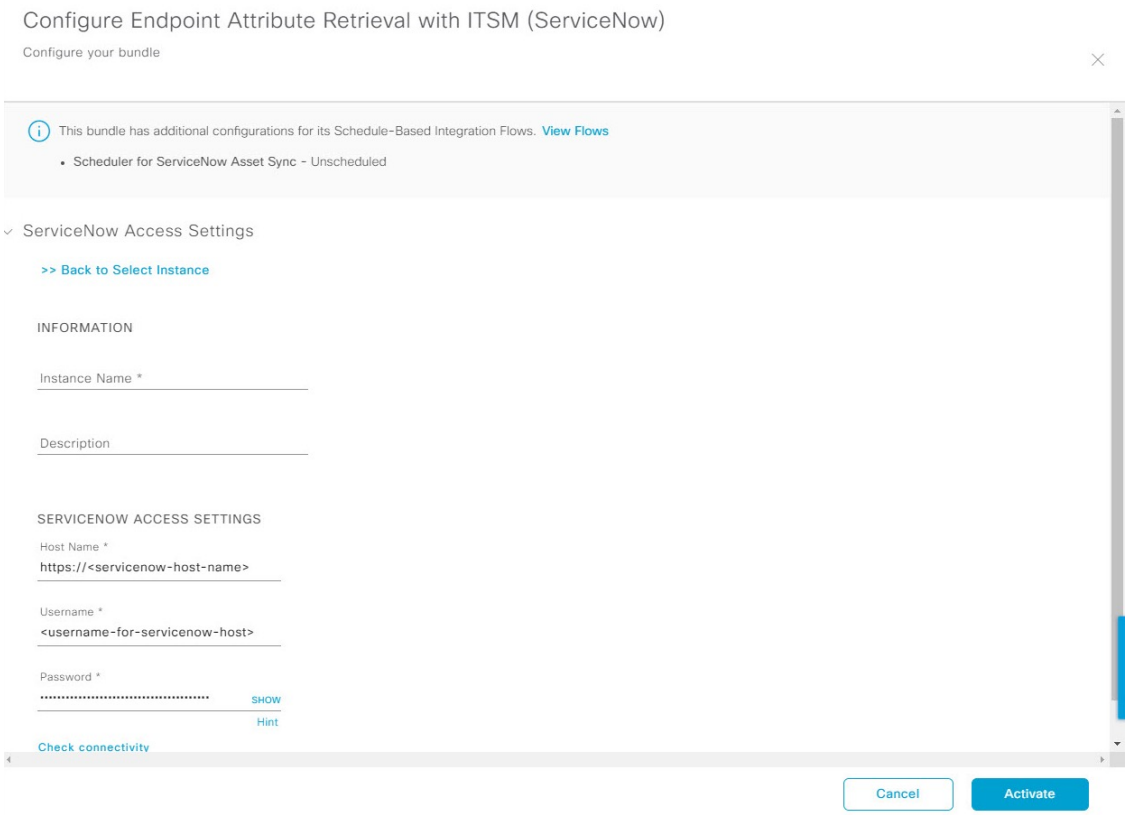
     For **Run Later**, you must select a date, time, and time zone. For **Recurring**, you must set a repeating interval (daily or weekly), an interval duration (minutes or hours), and a start and end date.
   - Click **Schedule** to enable the scheduler.

   > **Note**
   >
   > 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.

8. Click the **X** icon to close the window and return to the previous bundle window.
9. Click **Configure** to configure at the bundle level.
10. In the configuration slide-in pane, click **ServiceNow Access Settings** to configure a ServiceNow instance.
11. Click the radio button to configure either an existing ServiceNow instance or configure a new instance.

Figure 4: Example of ServiceNow instance configuration felds



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

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.
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.
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 Edit an instance in General Settings on page 66.

Configure CMDB data synchronization for ServiceNow

Configure synchronization of device inventory and configuration data between Catalyst Center and ServiceNow's CMDB using the Basic ITSM (ServiceNow) CMDB synchronization bundle. This process includes access settings, inventory settings, destination selection, data field synchronization, mapping, and operational limits.

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

1. From the main menu, choose **Platform** > **Manage** > **Bundles**.
2. Click the **Basic ITSM (ServiceNow) CMDB synchronization** bundle link or icon.

   Review bundle information in these available tabs.

   - **General information**: This tab displays vendor, version, platform, and tags.

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

   - **Information**: This tab displays 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**: This tab displays accesses the integration flows that make up the bundle, or provides information about the integration flows that make up the bundle.
   - **Release Notes**: This tab displays latest release information about the bundle, including its version.

3. Review the bundle data in the **Information** tab and click the **Contents** tab.
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 Manage integration flows on page 136.

5. Click **Enable** to activate the links.
6. In the **Information** field, click **Enable** to confirm enabling the bundle.

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

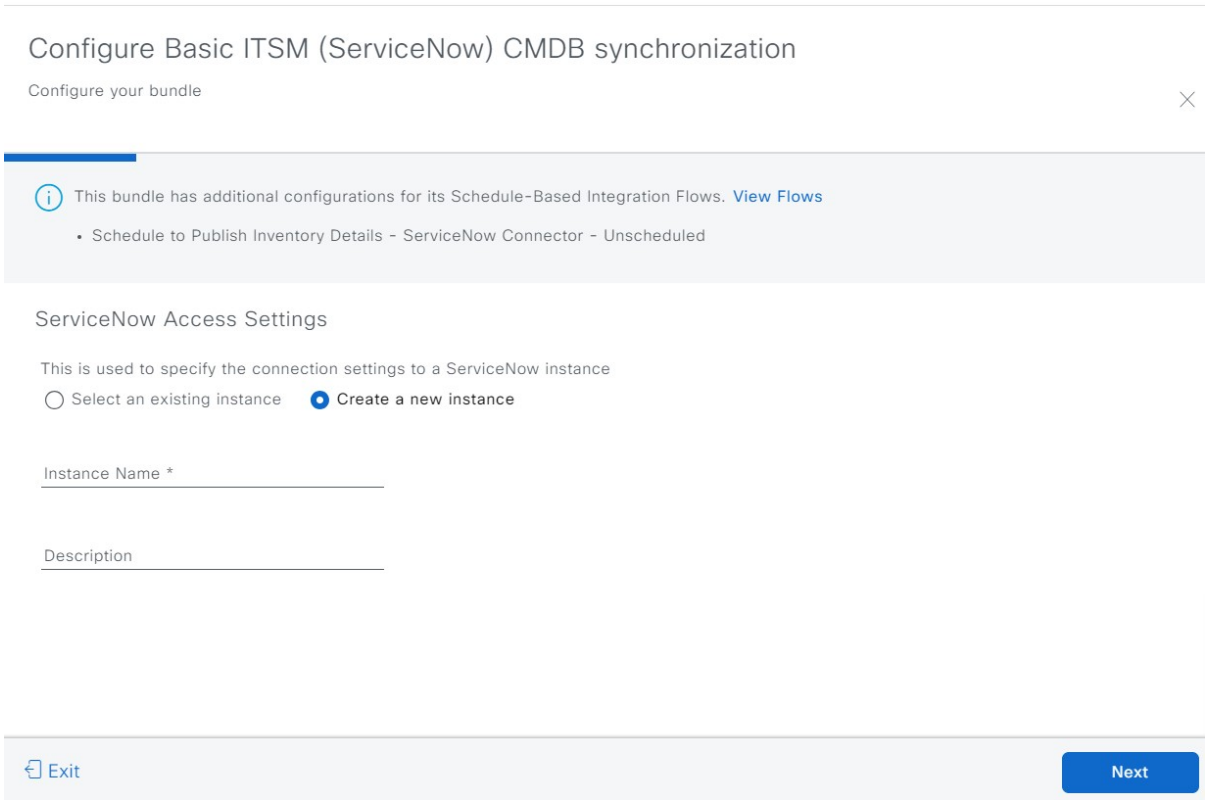
     For **Run Later**, you need to select a date, time, and time zone. For **Recurring**, you need to set a repeating interval (daily or weekly), an interval duration (minutes or hours), and a start and end date.
   - Click **Schedule** to enable the scheduler.

   > **Note**
   >
   > 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**.

9. Click the **X** icon at the upper right of the window to close it and return to the previous bundle window.
10. Click **Configure** to configure at the bundle level.

    A configuration slide-in pane appears. Review the CMDB synchronization information.
11. Click the radio button to configure either existing or new ServiceNow access settings for the CMDB synchronization.

Figure 5: ServiceNow Access Settings



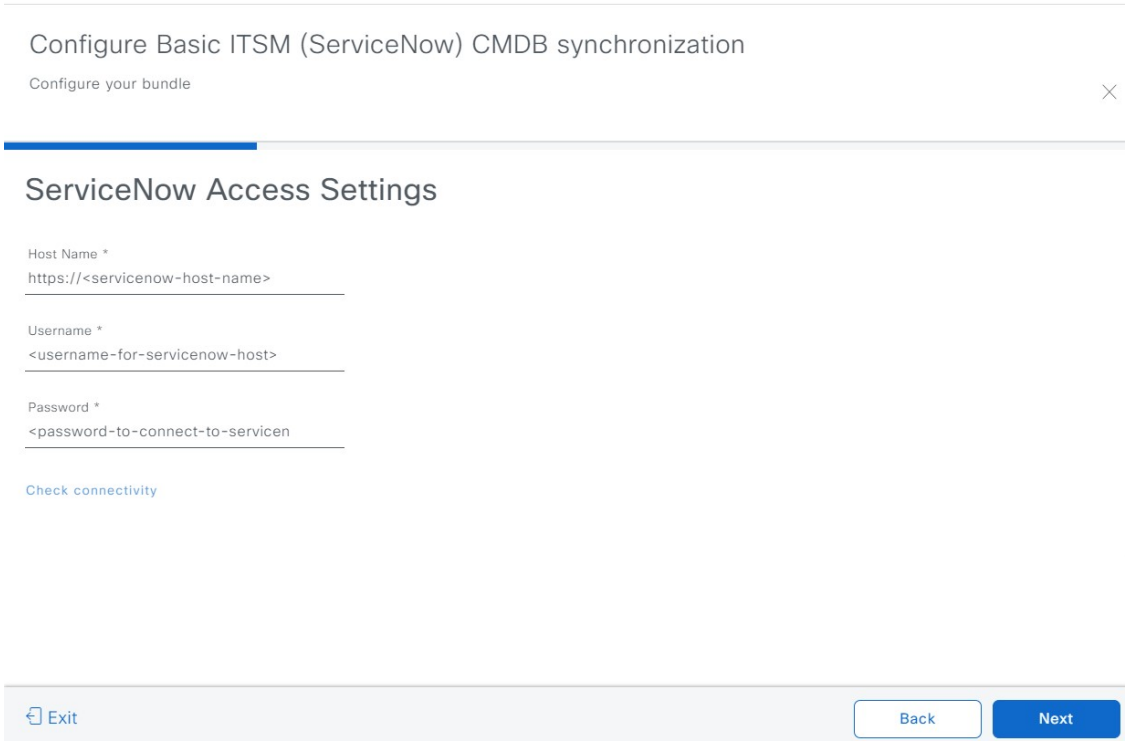
To configure an existing setting, choose it from the drop-down menu in the window and click **Next**.

12. To configure a new access setting, enter these details.
    - **Instance Name**: name of the instance.
    - **Description**: descriptive text of the instance.

    Click **Next**.

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

Figure 6: ServiceNow Access Settings



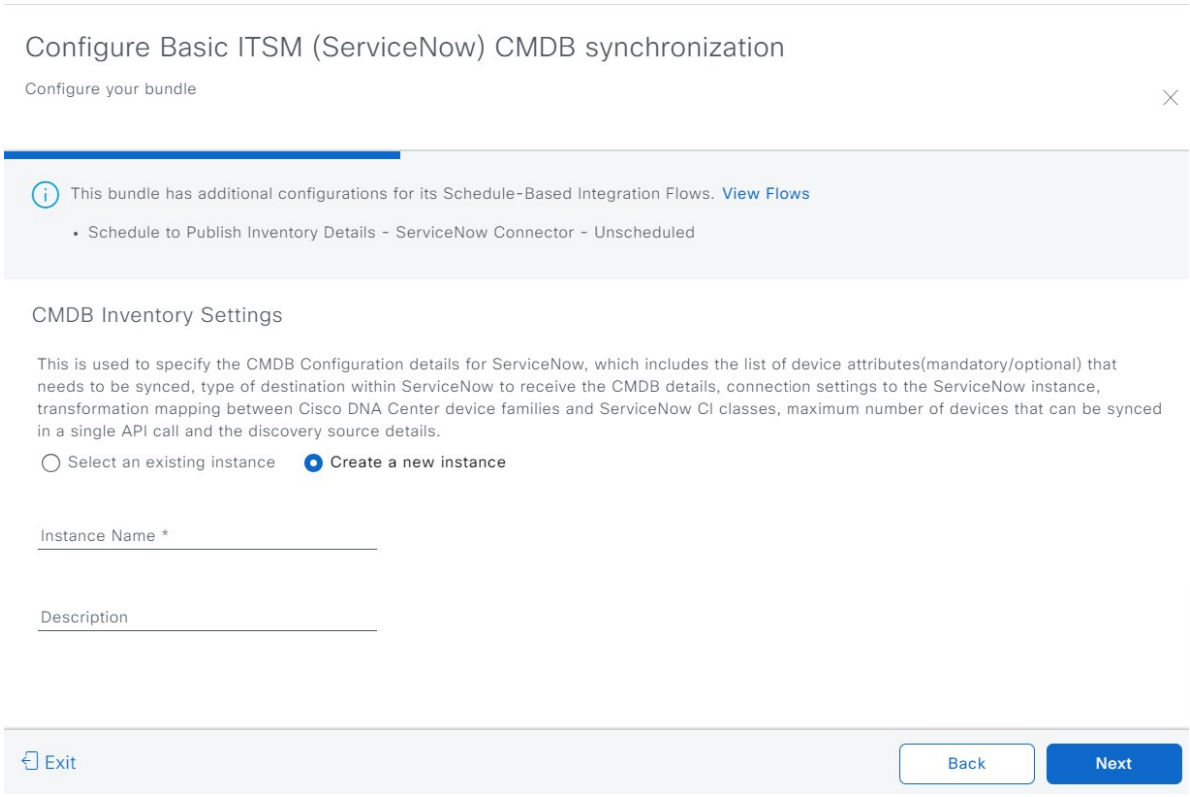
- **Hostname**: hostname or IP address of the ServiceNow server.
- **Username**: username for access to the ServiceNow server.
- **Password**: password for access to the ServiceNow server.

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

Click **Next**.

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**.

15. To configure a new instance, enter this additional information.
    - **Instance Name**: name of the instance.
    - **Description**: descriptive text of the instance.

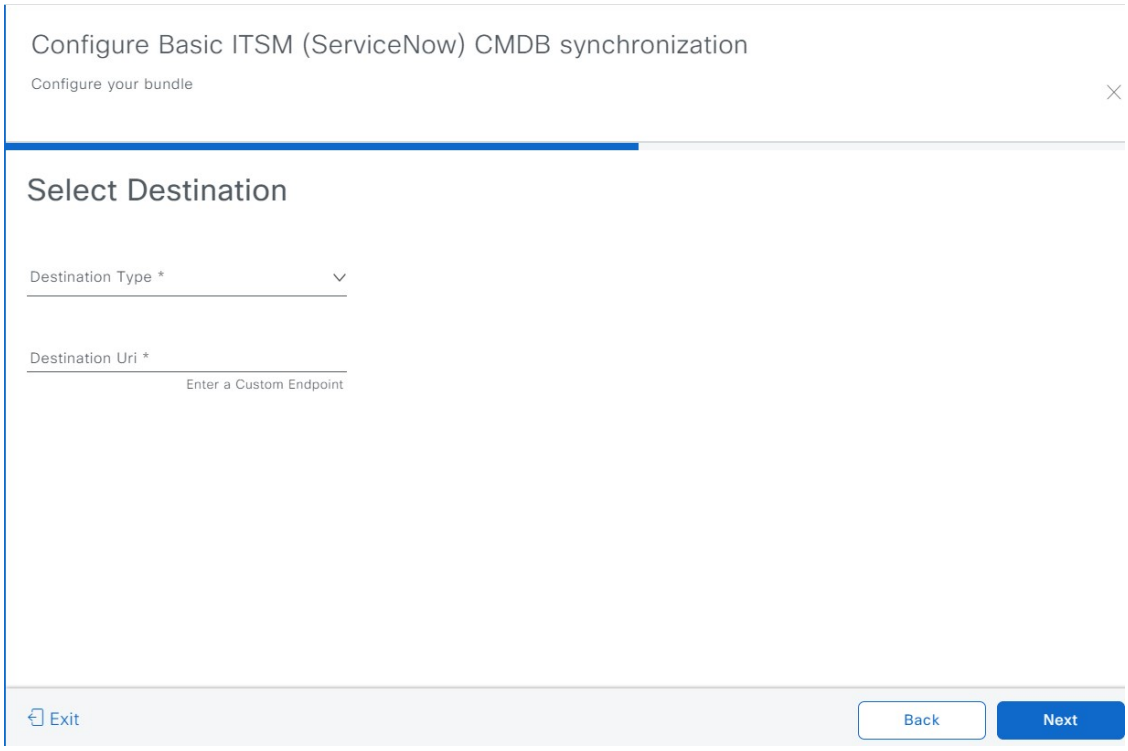
    Click **Next**.

16. In the **Select Destination** window, enter these details.
    - **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



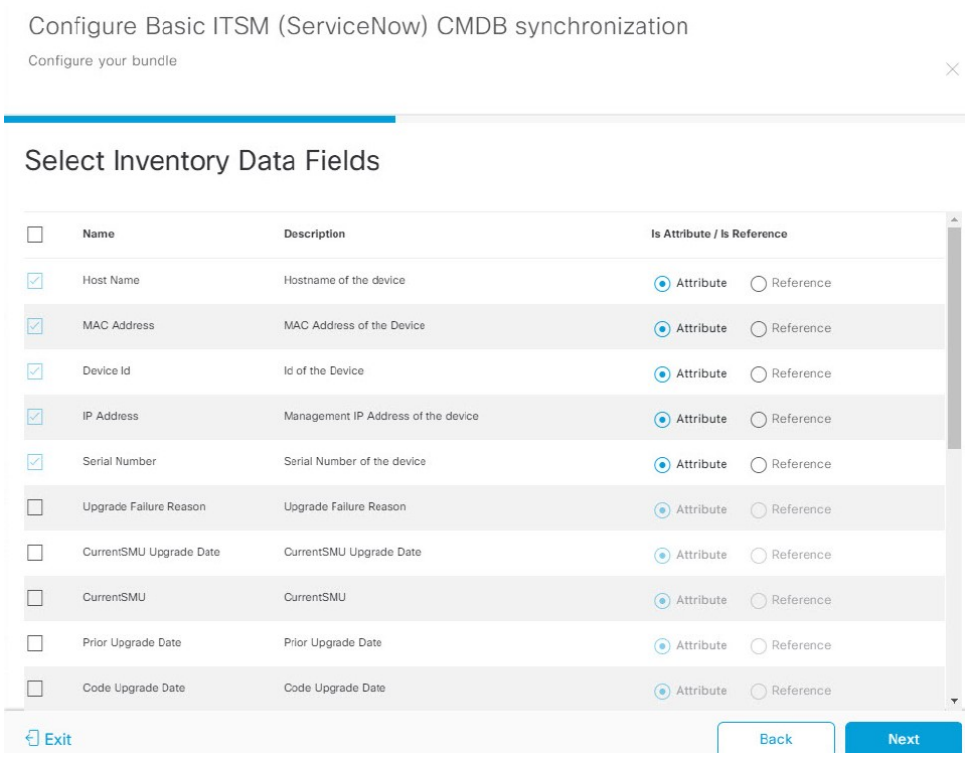
Click **Next**.

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.

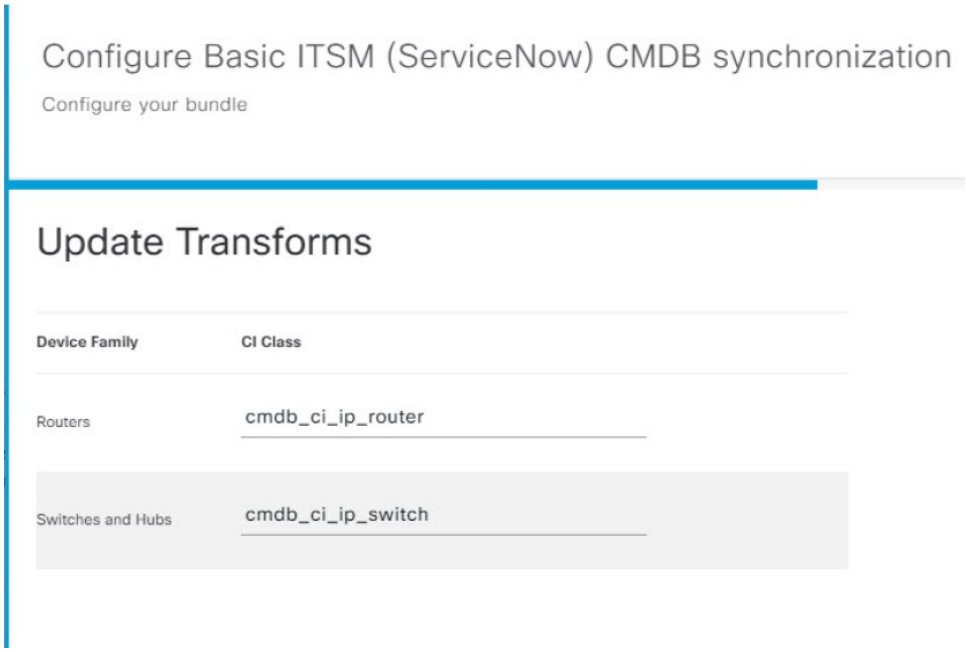
18. For the data fields selected to be synchronized in the preceding step, review their default designation as either an attribute or reference.

    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**.

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 2: Default device family to CI class mapping list

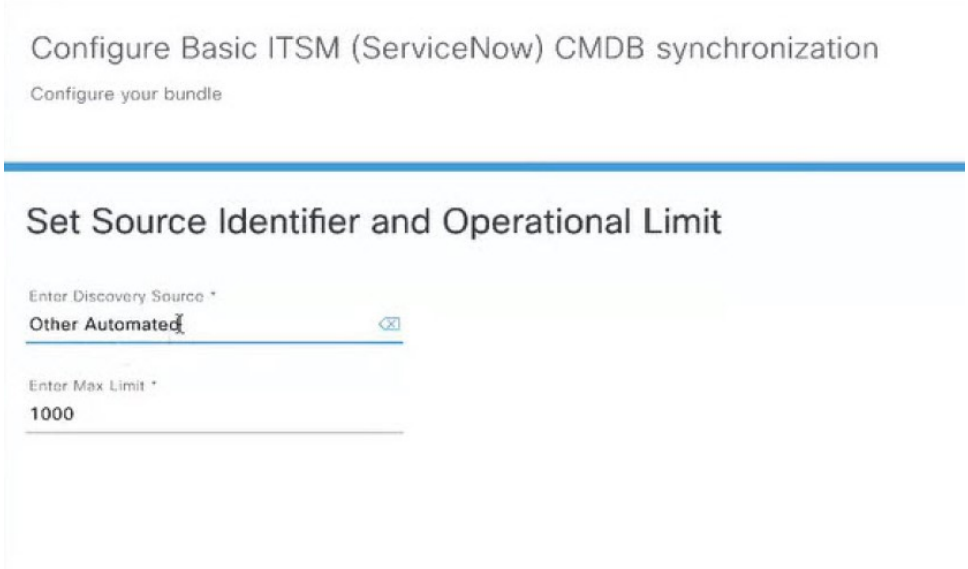
Device family	Corresponding CI class
Unified AP	cmdb_ci_wap_network
Wireless Controller	x_caci_cisco_dna_wireless_lan_controller
Routers	cmdb_ci_ip_router
Switches and Hubs	cmdb_ci_ip_switch
Meraki Access Point	cmdb_ci_wap_network
Meraki Cameras	cmdb_ci_netgear

Device family	Corresponding CI class
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**.

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

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

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 Edit an instance in General Settings on page 66.

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.

6 Configurations

Topics:

- Configurations
- Configure event settings
- Edit an instance in General Settings
- Add an instance in General Settings
- Configure a webhook destination
- Configure email destinations for event and report notifications
- Configure a syslog server destination
- Configure a trap notification

This chapter covers configuring various platform settings, including event settings (type, category, severity), general settings for instances, and destinations for webhooks, email, syslog, and SNMP trap notifications.

Configurations

This section introduces the Configurations feature of the Catalyst Center platform, explaining how it enables users to customize their network experience through Event Settings used for incident reporting and General Settings used for managing REST and ITSM endpoint instances.

A configuration is a network management feature that allows you to

- customize event and incident reporting,
- manage REST endpoint and ITSM endpoint instances, and
- enable delivery of events to various external destinations.

Catalyst Center platform offers the **Configurations** feature, enabling you to customize your 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 identifies these events. You can configure settings for the type, category, and severity under which Catalyst Center reports them. Configure this information in the GUI to customize details sent to external systems, such as ITSM endpoints or REST endpoints.
- **General Settings**: You can add or edit REST and ITSM endpoint instances within one or more 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.

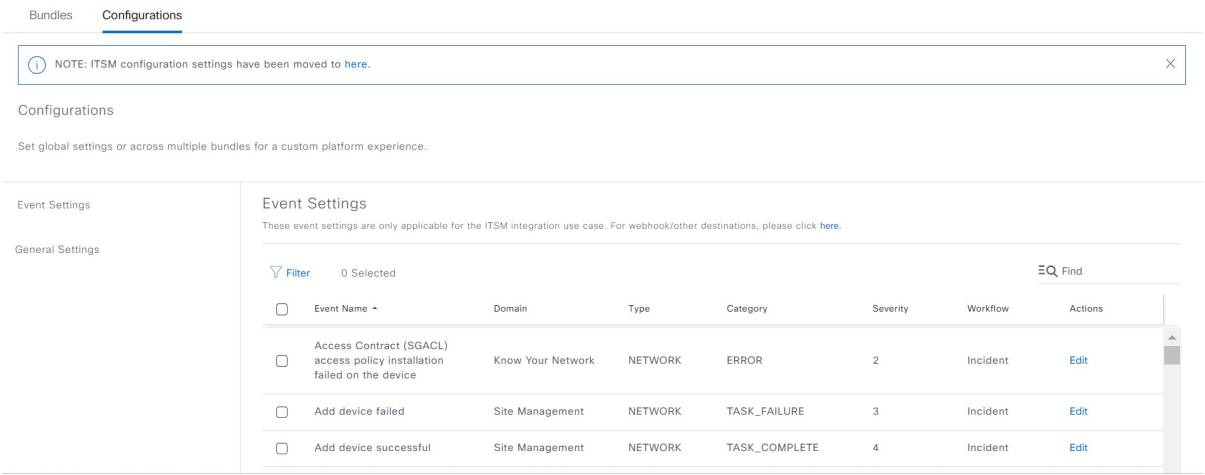
Configure event settings

Configure event settings to customize notification workflows and integration with ITSM, including event type, category, severity, and notification methods.

You can view a preset number of issues (or events) in **Event Settings** within the **Configurations** window. Configure the type, category, severity, and workflow for these events.

> **Note**
>
> The **Event Settings** window functionality is only applicable for an ITSM integration and not for generic event notifications. To understand the full integration process between Catalyst Center and ITSM, see the *Cisco Catalyst Center ITSM Integration Guide*. Review the instructions in 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, SNMP trap, or syslog server (using the REST API).

Figure 12: Event Settings window



Before you begin

- Ensure that ITSM integration has been configured in Catalyst Center.
- Verify that you have administrative access to Catalyst Center.

Procedure

1. From the main menu, choose **Platform** > **Manage** > **Configurations** > **Event Settings**.
2. Review these details in the **Event Settings** table.
   - **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

     Assign Severity 1 for the most important or critical priority events.

   - **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.

   Edit the event to customize notification settings to match your network standards.
3. Click **Edit** in the **Actions** column to edit an event.

Choose a setting, then 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.

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

   Notifications will be sent according to your chosen methods (email, webhook, SNMP trap, syslog).

5. Click **Save** to apply your changes.

What to do next

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

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

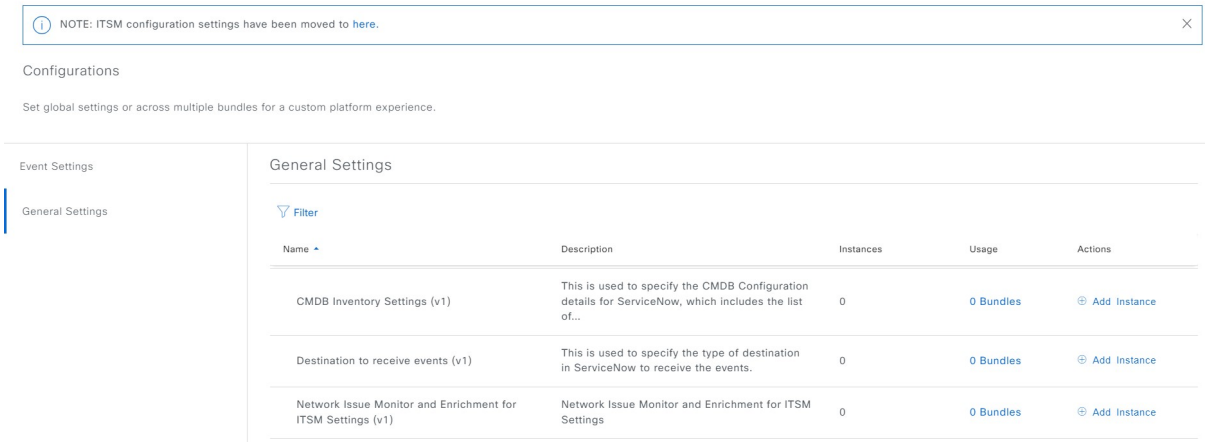
- Click **View Details** to view the notifications.

Edit an instance in General Settings

Edit existing instances within single or multiple bundles via the General Settings, allowing modifications to CMDB synchronization details or destination settings for events.

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 45.

Procedure

1. From the main menu, choose **Platform** > **Manage** > **Configurations** > **General Settings**.
2. Review the details in the **General Settings** table.
   - **Name**: name of the instance and version.
   - **Description**: description of the settings containing the instances.

- **Instances**: number of instances currently configured.
- **Usage**: number of bundles that use the instance or instances.
- **Actions**: specific tasks available 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.

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.

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

   Catalyst Center displays the bundles that use the specified instance.

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

   Edit the appropriate instance as required.

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.

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**: must 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.

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

   The edits to the instance immediately take effect.

Add an instance in General Settings

Add new instances to one or more bundles through General Settings. This enables users to define new CMDB Synchronization Settings instances or Destination to Receive Events instances.

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 more information, see Bundle features on page 45.

Procedure

1. From the main menu, choose **Platform** > **Manage** > **Configurations** > **General Settings**.
2. Review and fill these details in the **General Settings** table.
   - **Name**: name of the instance and version.
   - **Description**: description of the settings that contain the instances.
   - **Instances**: number of instances in the 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.
3. Click the arrow for one of the displayed instances, such as **CMDB Synchronization Settings (v1)** or **Destination to Receive Events (v1)**.

   The list of instances for that setting displays.
4. In the **Usage** column, hover your mouse pointer over **Bundles**.

   Catalyst Center displays the bundles that use the specified instance.
5. Click the **Add Instances** link in the **Actions** column to add an instance.

   Add the required instances.
6. (Optional) To add a **CMDB Synchronization Settings** instance, click **Add Instance** in the **Actions** column. Enter the 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 for 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.

7. (Optional) To add a **Destination to receive events** instance, click **Add Instance** in the **Actions** column. Enter these instance fields in the slide-in pane.
   - **Instance Name**: name of instance.
   - **Description**: description of the instance.
   - **Destination to Receive Events**: choose one of these options.
     - **Event Management**: When setting up Catalyst Center integration with ServiceNow without the Cisco Catalyst app, choose the **Event Management** option. This option requires that you have the Event Management plug-in configured within the ITSM 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.
8. Click **Add** to save your instance addition.

   The additions to the instance take effect immediately.

Configure a webhook destination

Configure a webhook destination to send events and reports. Specify the name, URL, method, authentication type, and custom headers.

Catalyst Center supports webhook destinations for events and reports. To configure a webhook destination for either, use the Catalyst Center GUI and complete these steps.

Before you begin

- Ensure you have the necessary access to the Catalyst Center GUI.
- Gather the details you need: webhook name, description, target URL, REST API method, and authentication information (if needed).

Procedure

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

2. Review the **Webhook** tab.

   The **Webhook** tab displays these fields.

   - **Name**: webhook name you enter.
   - **Description**: description that you provide.
   - **URL**: the webhook's callback URL you provide.
   - **Method**: REST API method you select for the webhook (for example, POST).
   - **Edit**: link you use 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.

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

   The slide-in pane for adding a webhook appears.

4. Enter values in the fields of 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).

5. Based on your webhook configuration, choose whether a trust certificate is associated with the webhook URL.

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

6. Choose the authentication type associated with your webhook URL, based on your webhook configuration.

   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**: indicates you do not need authentication.

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

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

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

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

What to do next

Configure a webhook destination for an event or for a report.

To configure an event or a report using the webhook destination, see Configure event notifications for network events on page 139 and Generate your first report on page 76.

Configure email destinations for event and report notifications

Configure email destinations to enable event and report notifications, including setting up primary and secondary Simple Mail Transfer Protocol (SMTP) servers, sender/receiver details, and testing connectivity.

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 **Integration 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 34.
- 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 remains blank for security. Update the password if required, or leave the window without changes.

To perform these tasks, ensure you have the necessary permissions. For details about role-based access control, see Supporting Role-Based Access Control on page 36.

Configure an email destination for events or reports using the Catalyst Center GUI.

Procedure

1. From the main menu, choose **System** > **Settings** > **External Services** > **Destinations** > **Email**.
2. Configure the required **Primary SMTP Server** fields.
   - **Hostname/IP**: Enter the host name 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 from the drop-down list.

     Note

     The default port number for SMTP is 25.

   - **Username**: Enter the username for authenticating the primary SMTP server.
   - **Password**: Enter the password for authenticating the primary SMTP server.
3. Configure the optional **Secondary SMTP Server** fields.
   - **Hostname/IP**: Enter the host name 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 from 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.

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

   After you click **Test**, the system sends a test email using your configured parameters for the primary and secondary SMTP servers, with **Cisco SMTP Configuration Test Email** as the subject line. The system shows a success or failure message based on the connectivity results.
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 Configure event notifications for network events on page 139 and Generate your first report on page 76.

Configure a syslog server destination

Configure a syslog server destination. Enter the server details and select the protocol so you receive event notifications.

Catalyst Center supports a syslog server destination for event notifications.

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

Before you begin

- Gather the syslog server details: name, description, hostname or IP address, port number, and protocol (TCP or UDP).
- Confirm that your computer can connect to the syslog server.

Procedure

1. From the main menu, choose **System** > **Settings** > **External Services** > **Destination** > **Syslog**.
2. In the **Syslog** tab, review the available fields for configuring the syslog server.
3. To configure a new syslog server, click the **Add** icon (**+**).
4. Enter your syslog server information into the fields.

- **Name**: Enter the name of the syslog server.
- **Description**: Enter a description of the syslog server.
- **Hostname/IP**: Enter the hostname or IP address of the syslog server.
- **Port**: Enter the port number used by the syslog server.
- **Protocol**: Select either TCP or UDP.

When you choose the **TCP** protocol, check the **isSecure** check box to ensure secure TCP communication.

5. Optional: To test the configuration, click **Validate**.
   After your configuration succeeds, a validation message appears.
6. To save your syslog server destination configuration, click **Save**.

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

What to do next

Configure a syslog server destination to receive event notifications. To learn more, see Configure event notifications for network events on page 139.

Configure a trap notification

This section provides instructions for configuring SNMP trap event notifications. You can define the trap name, description, receiver hostname or IP, port, and SNMP version (2C or 3) with authentication and privacy settings.

Catalyst Center supports SNMP trap event notifications.

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

Before you begin

- Ensure you have access rights to the system SNMP configuration settings.
- Gather SNMP trap receiver details (hostname or IP address and port).
- Determine whether you require SNMP version 2C or version 3, and obtain the corresponding credentials.

Procedure

1. From the main menu, choose **System** > **Settings** > **External Services** > **Destination** > **SNMP**.
2. Check the **SNMP** window for the available settings.
3. Click **Add** to configure a trap.
4. Enter information in each field.
   - **Name**: Enter a name for the event notification.
   - **Description**: Provide a brief description of the event.
   - **Hostname/IP Address**: Enter the hostname or IP address of the SNMP trap receiver; use either an IPv4 or IPv6 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 the username and select the mode
  - **No Authentication, No Privacy**: You do not need to configure any additional settings.
  - **Authentication, No Privacy**: Specify authentication type (SHA or MD5) and authentication password.
  - **Authentication and Privacy**: Specify authentication type (SHA or MD5), authentication password, privacy type (AES128 or DES), and privacy password.

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), then subscribe.

7 Reports

Topics:

- Reports
- Generate your first report
- Generate an access point report
- Generate an audit log report
- Generate a client report
- Generate a compliance report
- Generate a configuration archive report
- Generate an end-of-life report
- Generate an executive summary report
- Generate an inventory report
- Generate a license report
- Generate a network devices report
- Generate a rogue and aWIPS report
- Generate an ROI report
- Generate a security advisories report
- Generate a SWIM report
- Generate a flexible report
- Manage generated reports

This chapter provides instructions on generating and managing diverse network reports such as access point, audit log, client, compliance, configuration archive, end-of-life, executive summary, inventory, licensing, network devices, rogue and aWIPS, ROI, security advisories, SWIM, and flexible reports.

Reports

The Reports feature provides network insights through customizable data, multiple formats, and flexible scheduling to support diverse operational needs.

A report is a network analysis tool that helps you

- see data insights about your network's status and operation,
- customize report content, format, and scheduling, and
- support diverse operational use cases, such as capacity planning, usage trend analysis, and network health monitoring.

Examples of report use cases

- Capacity planning: Understand how your network devices are used within the application.
- Change of pattern: Track changes in usage patterns for clients, devices, bands, or applications on your 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 before proceeding.

Generate your first report

Configure and run your first network data report using Catalyst Center, including template selection, scope definition, file type, scheduling, and delivery options.

Run specialized data reports about your network using this procedure.

Before you begin

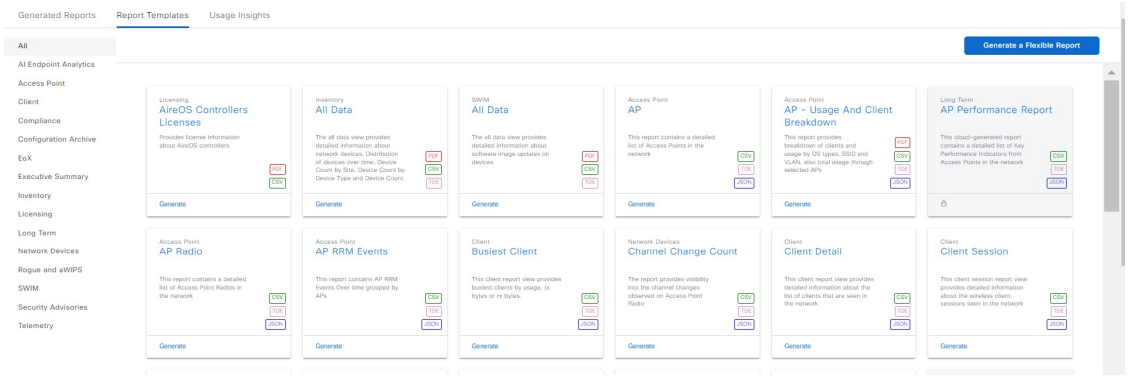
Run a successful **Discovery** job in Catalyst Center. You can check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

Procedure

1. From the main menu, choose **Reports**.
2. In the **Run Your First Report** window, click **Start**.

   You see the supported reporting categories in the **Report Templates** window. Each category has a link. Click the link to view the supported reports for that category.

   Figure 14: Report Templates window



Note

Available options depend on the type of report selected.

3. After you click a link, review the **Report Templates** window that corresponds to the selected category.

   Each tile represents a template, provides report information, and includes links you can use to generate a report. Decide which template you want to use to generate your report. Each tile includes icons for PDF, CSV, Tableau Data Extract (TDE), or JSON file types.

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

   A **Preview** window appears. Use the sidebar to scroll and review the entire sample report. The sample report includes

   - applied filters (data filters that are used in building the report,
   - data metrics and summaries,
   - graphical representations of the data, such as line graphs, bar graphs, and pie graphs, and
   - tables that help you analyze data.

Note

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

5. Close the preview window.
6. In the tile, click the **Generate** link to configure parameters to build a report.

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

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 to generate a new report.

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. Review an autogenerated sample in the same window.

Click **Next** to proceed to the **Setup Report Scope** window.

9. 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. Select the filter options for your report.

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

   Click **Next** to proceed to the **Select File Type**.

10. Select the file type for the report.

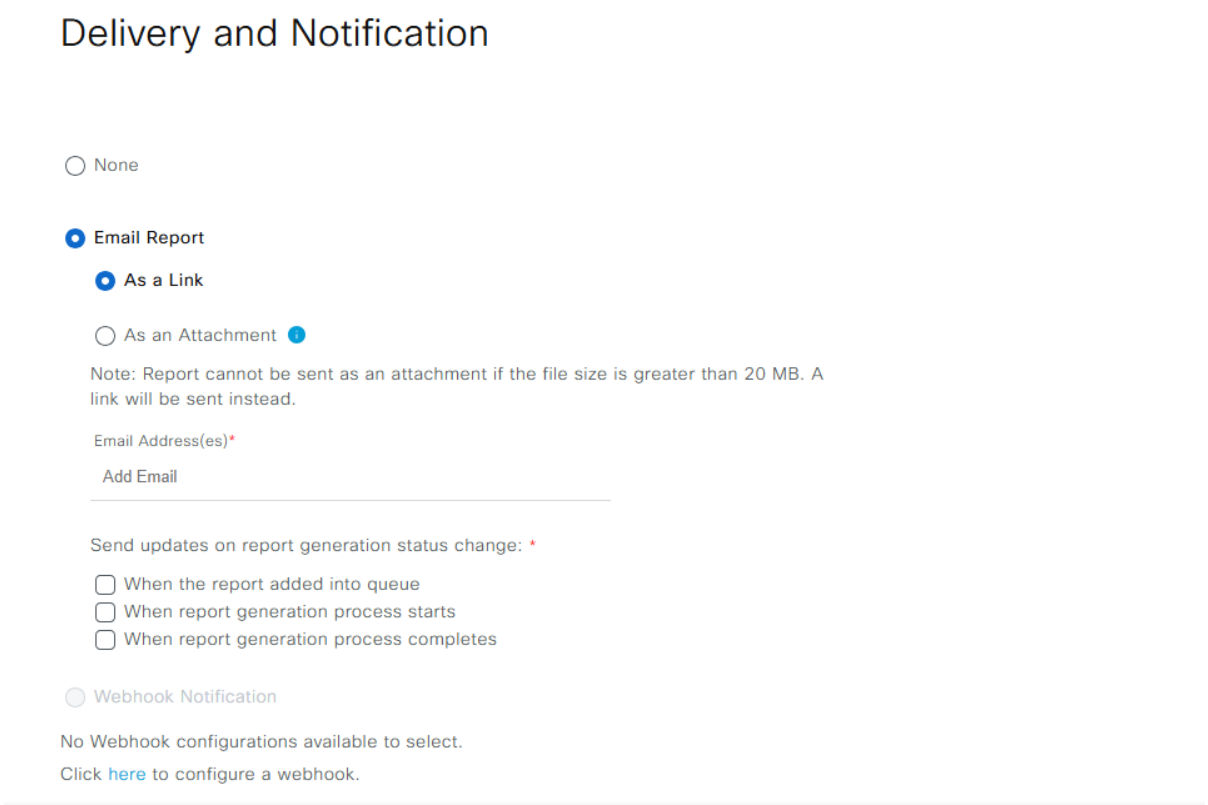
    The available **File Type** options for reports vary depending on the report you are creating.

    - **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.

11. In the **Schedule Report** window, select the schedule for the report. Then, click **Next** to proceed to the **Delivery and Notification** window.
12. Select the delivery mechanism for the report.

    Figure 15: Delivery and Notification window



- **None**: No email or webhook notifications are 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 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 updates for the report as webhook notifications such as 'In Queue', 'In Progress', and 'Success'. You can also view these notifications in the GUI.

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

    Click **Generate Report** to start generating the report.

    After you generate the report, a success window opens.

14. Click **View all Reports**.

    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 Manage generated reports on page 130.

Generate an access point report

Configure and generate an Access Point report to analyze AP-related data by specifying report details, filters, scheduling, and delivery options

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.

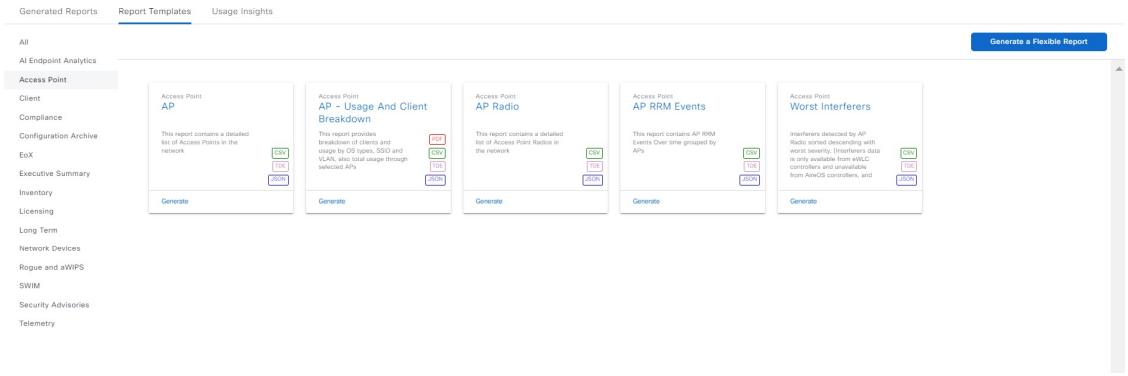
Procedure

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

   The **Report Templates** window, you can view the reporting categories. Each category is shown as a clickable link. Click the link for the category you want to review supported reports.

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

   Figure 16: AP report



   Each report template is shown as a tile with report information and links for generating reports. Select the template you want to use.

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

   When the sample report appears, use the sidebar to scroll through it.

   > **Note**
   >
   > Use the sample report to plan the layout and content of your custom report.

4. Click **X** to close the preview.
5. In the tile, click the **Generate** link to configure parameters to build a report.

   The **Generate** window lets you choose the report format, apply data filters, and schedule report generation.

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.

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

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

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

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

   Enter a name in the **Report Name** field, then click **Scope** to show the available filters. Select the filter options for the report and choose a **Time Range**.

   > **Note**
   >
   > The **Setup Report Scope** options change based on the selected **Template**. AP reports retain data for up to 90 days (3 months).

10. Click **Next**.
11. In the **Select File Type** window, choose the file type for the report.

    Depending on the report, these **File Type** options may be available:

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

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

12. Click **Next** to continue.
13. In the **Schedule Report** window, choose the schedule for the report. Then, click **Next**.
14. In the **Delivery and Notification** window, choose the delivery mechanism for the report:

    - **None**: No email or webhook notifications are 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, clear the check boxes you do not wish to use.

- **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

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

    Click **Generate Report**.

    When the report is generated, you see a success window.

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

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

    Download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see Manage generated reports on page 130.

Generate an audit log report

Configure and generate audit log reports to track and analyze configuration changes to network devices, with options for naming, filtering, scheduling, and choosing output format.

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

Before you begin

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

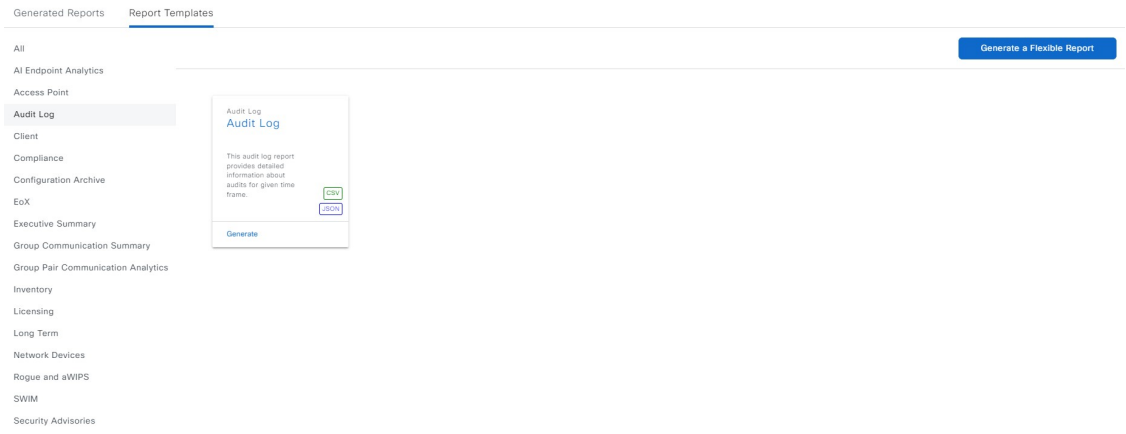
Procedure

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

   The **Report Templates** window displays the supported reporting categories. Each category is represented by a link. Click the link to view the available reports for that category.

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

   Figure 17: Audit Log report



   Each template appears as a tile that contains information about the report and provides links to generate it. Choose the template that best fits your reporting needs.

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

   A window appears containing the sample report. Use the sidebar in the window to review the sample report.

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

4. Click **X** to close the preview.
5. In the tile, click the **Generate** link to configure parameters to build a report.
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.

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.

8. Click **Next**.
9. In the **Setup Report Scope** window, name the report and select the scope.

   Enter a report name in the **Report Name** field. Click in the **Scope** field to display the available filter. Select the filter options for the report. Choose the **Time Range**.

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

   Click **Next**.

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, select attributes using the **Fields** option.

11. Click **Next**.
12. In the **Schedule Report** window, select the schedule for the report. Then, click **Next**.
13. In the **Delivery and Notification** window, select the delivery mechanism for the report:

    - **None**: No email notifications or webhook notifications are sent.
    - **Email Report**: The 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 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 in the **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.

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

    Click **Generate Report**.

    A success window appears after the report is generated.
16. Click **View the Generated Reports**.

    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 about managing generated reports, see Manage generated reports on page 130.

Generate a client report

Configure and generate specialized client reports to analyze client-related data, including roam events, by specifying report parameters and delivery methods.

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

Before you begin

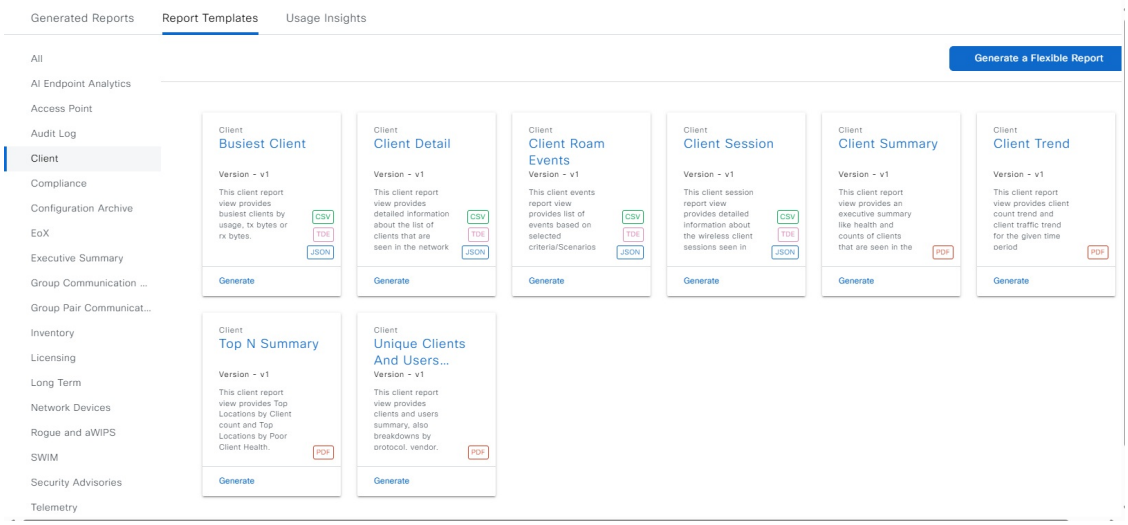
Run a successful **Discovery** job in Catalyst Center. Verify if a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

Procedure

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

   The **Report Templates** window displays the reporting categories. Each category is represented by a link. Select a link to view reports in that category.
2. After clicking a link, review the **Report Templates** window for the selected category.

   Figure 18: Client Report



Each template appears as a tile with information about the report and links for generating a report. To generate a report, select a template.

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

   A window appears showing the sample report. To view the complete report, use the sidebar to scroll. Some client reports include this data:

   - 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

   Use the sample report to plan your report's appearance.

4. Click **X** to close the preview.
5. In the tile, click the **Generate** link to configure parameters to build a report.

   In the **Generate** window, select a file format, apply data filters, and schedule when to generate the report.

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.

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.

8. Click **Next**.
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. Select the filter options for the report, and then choose the **Time Range**.

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

   Select **Next**.

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

    Depending on the report that you create, 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.

11. Select **Next**.
12. In the **Schedule Report** window, select the schedule for the report. Then, click **Next**.
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, a prompt appears 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.

Clear the corresponding check boxes to reduce the number of notifications.

- **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**.

Status webhook notifications are sent for the report. For example, you will receive "In Queue," "In Progress," and "Success" webhook notifications.

14. Click **Next**.
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.
16. Select 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 Manage generated reports on page 130.

Generate a compliance report

Configure and generate a compliance report to review the status of your network devices, filter by criteria, and receive the results in your preferred format.

Catalyst Center allows you to retrieve a consolidated compliance audit report that shows the compliance status of individual network devices. This report provides complete visibility of your network.

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

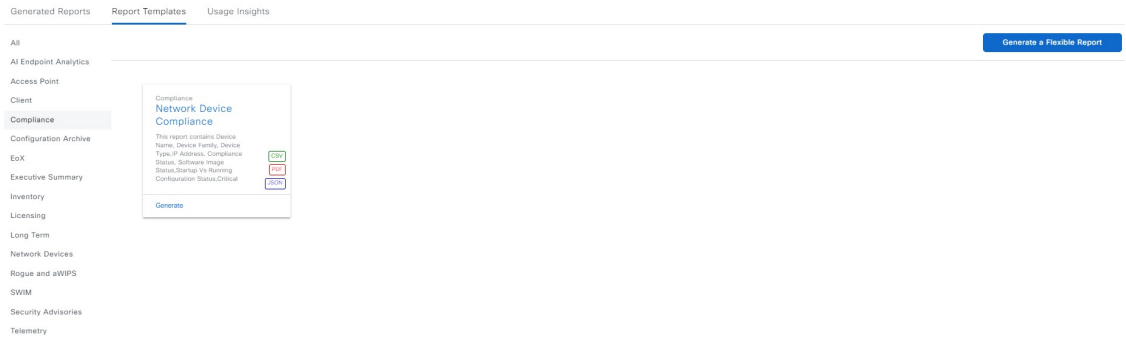
Procedure

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

   The **Report Templates** window displays the supported reporting categories.
2. Click **Compliance** to display the Compliance templates.

   Each template appears as a tile and includes report information and links for report generation.

   Figure 19: Compliance report



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

   The sample report window opens. Use the sidebar to scroll and review the entire sample report.

4. Click **X** to close the preview.
5. In the tile, click the **Generate** link to configure report parameters.
6. In the **Generate a New Report** window, click **Let's Do It**.

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

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.

8. Click **Next**.

   The **Setup Report Scope** window appears.

9. In the **Report Name** field, enter a report name.
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 template that you select.

11. Click **Next**.
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.

13. Click **Next**.
14. When the **Schedule Report** window appears, select the schedule for the report. Then, click **Next**.
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 the provided link.

    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 checks the email addresses for correct syntax and sends a notification if there is an error.

  - **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, uncheck the relevant check boxes.

- **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**.

16. Click **Next**.
17. In the **Summary** window, review the configuration and edit any of the files, if necessary.
18. Click **Generate Report**.

    After the report is generated, a success window appears.

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

    The **Generated Reports** window opens and displays the instance details of the scheduled report.

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

Generate a configuration archive report

Configure and generate a configuration archive report to track configuration changes on network devices. Specify change scope, device details, file format, scheduling, and notification options.

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

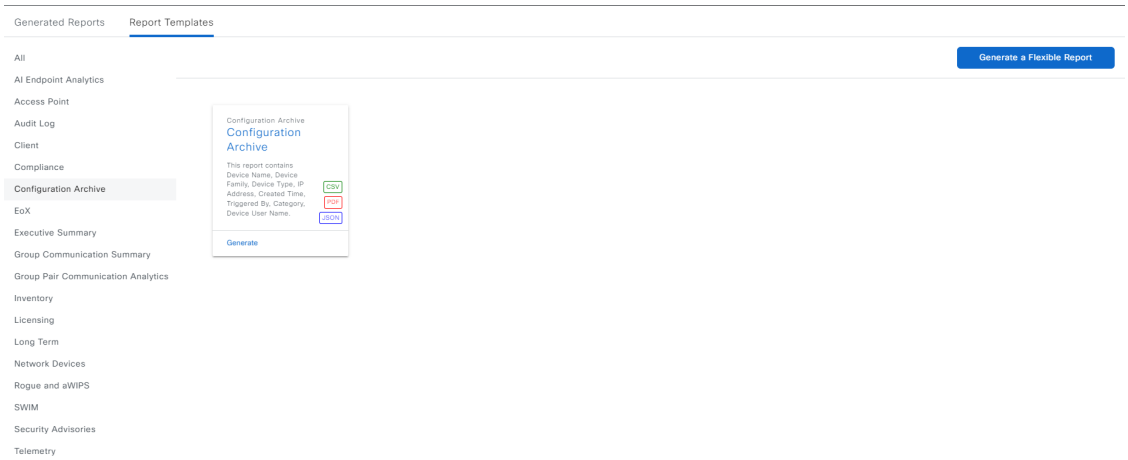
Procedure

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

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

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.

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

A window displays the sample report. Use the sidebar to scroll and review the entire sample report.

4. Click **X** to close the preview.
5. In the tile, click the **Generate** link to configure parameters to build a report.
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.

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.

8. Click **Next**.

   The **Setup Report Scope** window appears.

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

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.

12. Click **Next**.
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 **CSV** and **JSON** file types, you can use the **Fields** option to select attributes for the results..

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

17. Click **Next**.

18. In the **Summary** window, review the configuration and edit any of the files, if necessary.
19. Click **Generate Report**.

    After the report is generated, a success window appears.

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.

Generate an end-of-life report

Configure and generate an end-of-life (EoX) report for network devices to identify products nearing the end of their life cycle.

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. Check whether a **Discovery** job is successful in **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

Procedure

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

   The **Report Templates** window opens and displays supported reporting categories as links. Each category appears as a link.

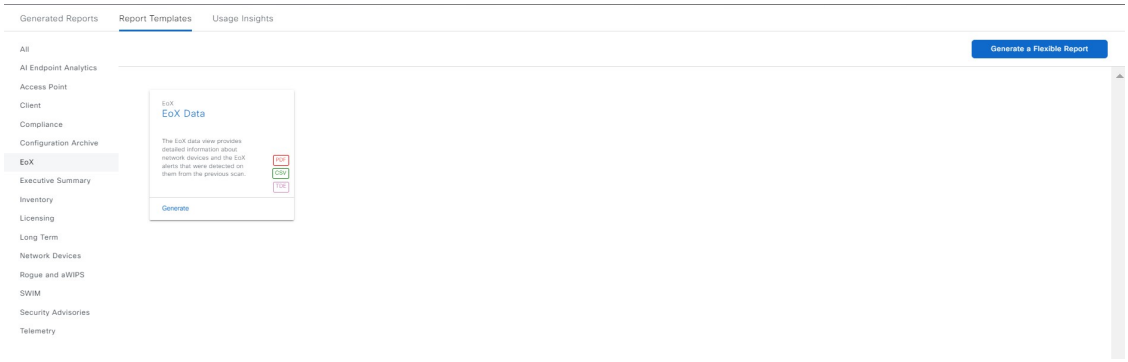
   In the **Report Templates** window, each template appears as a tile. The tile contains information about the report and links for report generation. Choose the template you want to use.

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

   A window opens with the sample report. Use the sidebar to review the complete sample report.

3. Click the close button to exit the preview.
4. In the tile, click the **Generate** link to configure parameters to build a report.

   Figure 21: EoX report



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.

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 report in the same window.

7. Click **Next**.

   The **Setup Report Scope** window displays.

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

10. Click **Next**.
11. In the **Select File Type** window, select the file type for the report.

    Based on your report, Catalyst Center shows several **File Type** options:

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

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

12. Click **Next**.

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

13. Click **Next**.

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

    - **None**: No email or webhook notifications are 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 twenty email addresses. To add multiple email addresses, after each addition, press **Enter** on your keyboard. Catalyst Center platform checks the email addresses and sends a notification 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 support up to ten 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, clear the 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.

15. Click **Next**.
16. In the **Summary** window, review the configuration and edit any files, if necessary.
17. Click **Generate Report**.

    After the report is generated, a success window appears.

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.

Generate an executive summary report

Configure and generate an Executive Summary report to review high-level network performance and health, and schedule its delivery.

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.

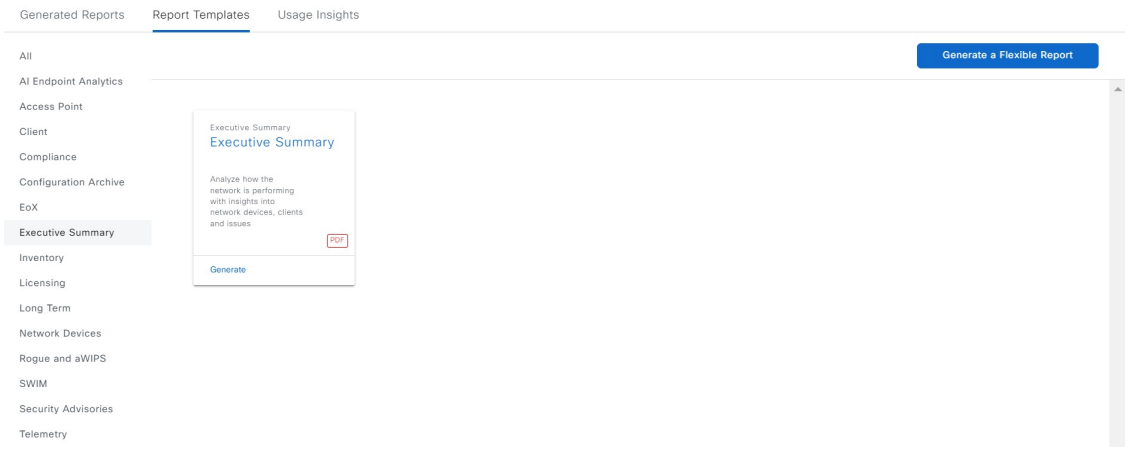
Procedure

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

   The **Report Templates** window displays the supported reporting categories. Each category appears as a link. Click a link to view the reports supported for that category.

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

   Figure 22: Executive Summary report



Each template appears as a tile containing report information and links for generating a report. Select your template to generate a report. The tile contains icons that represent the supported file types for the reports.

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

   A sample report appears in the window. Use the sidebar to scroll and review the report data.

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

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

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

6. In the **Generate a New Report** window, click **Let's Do It** to get started.
7. In the **Select Report Template** window, select the template for the report.

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

   > **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**.

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. Click **Scope** to display available filters. Select the filter options for the report. Choose 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**.

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 result files.

Click **Next**.

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

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.

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 Manage generated reports on page 130.

Generate an inventory report

Configure and generate an inventory report to obtain detailed information about network devices, customize report criteria, and select report delivery and scheduling options.

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

Before you begin

Run a successful **Discovery** job in Catalyst Center. To verify that the **Discovery** job succeeded, open **Device Inventory**. From the main menu, choose **Provision** > **Inventory** to view the results.

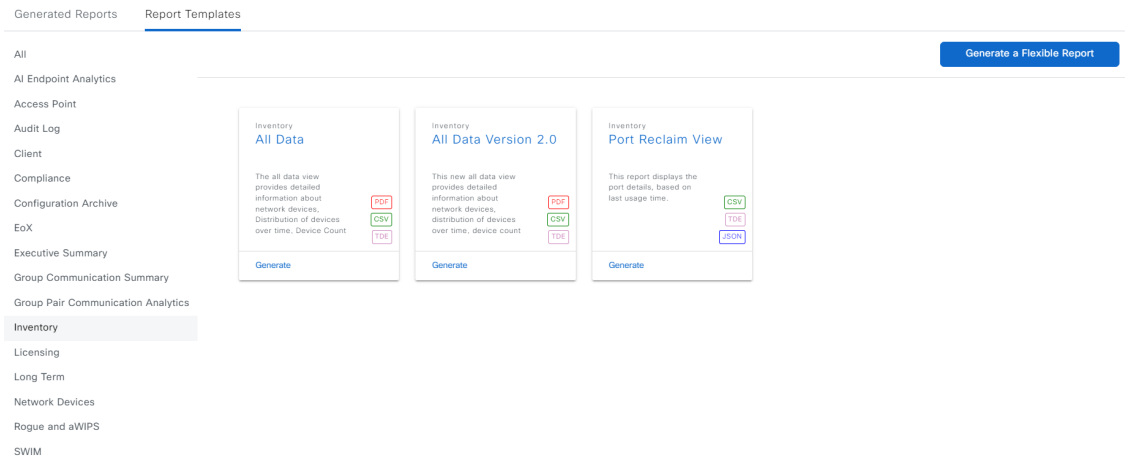
Procedure

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

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

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. Select the template you want to use to generate a report. Within the tile are icons that represent the supported file types for the reports.

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

   A window appears with the sample report. Use the sidebar in this window to scroll and review the sample report, which displays these details:

   - applied filters, which are data filters used to build the report,
   - data metrics and summaries,
   - graphical representation of the data, including line, bar, and pie graphs, and
   - tables that assist you in analyzing the data.

   > **Note**
   >
   > Use the sample report to plan your desired report layout.

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

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

   You can skip this screen in the future by checking the **Don't show this to me again** check box.

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**.

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. Select the filter options you want to apply for the report.

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

   Click **Next**.

9. In the **Select File Type** window, select the file type for the report.
10. Click **Next**.
11. In the **Schedule Report** window, select the schedule for the report.

    Click **Next**.

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, clear these check boxes, as desired.

- **Webhook Notification**: Notification is sent as a webhook to the configured webhook URL address, also called a callback URL. Select a webhook from the drop-down list in the **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**.

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.

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 Manage generated reports on page 130.

Generate a license report

Generate a license report for your network devices, including options for report scope, time range, file type, schedule, and delivery.

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.

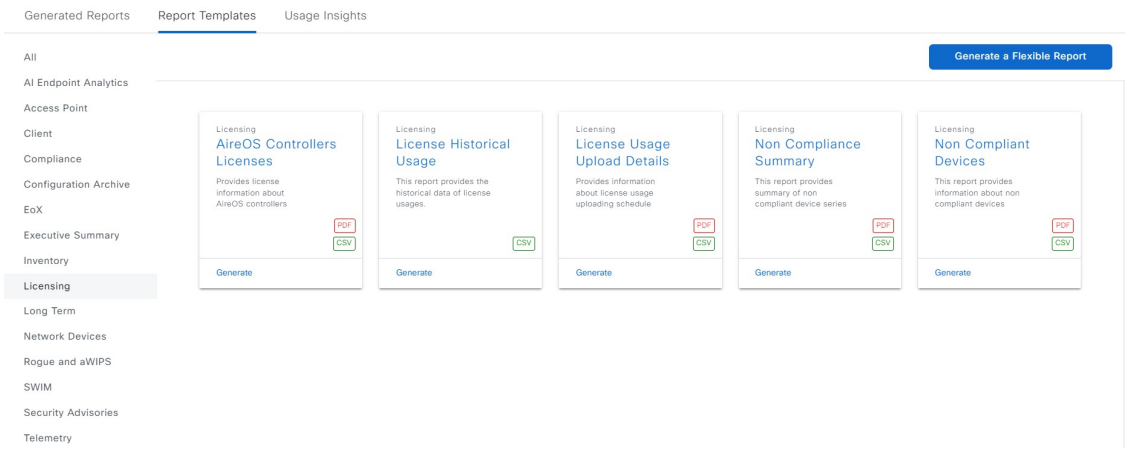
Procedure

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

   The **Report Templates** window displays the supported reporting categories. Each category appears as a link. Click a link to view only the supported reports for that category.

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. The tile contains information about the report and links that allow you to generate a report. Icons within the tile represent the supported file types for the reports.

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

   A window opens for the sample report. Use the sidebar to scroll and review the sample report. The report includes:

   - applied filters (data filters that were used to build the report),
   - data metrics and summaries, and
   - tables that assist you in analyzing the data.

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

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

   In the **Generate** window, select a format type, apply data filters, and set up a report schedule.
6. In the **Generate a New Report** window, click **Let's Do It**.

   To skip this screen next time, check **Don't show this to me again**.
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**.
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 name for the report. Select the **Scope** field to display available filters. Select the filter options you want for the report, and then choose the **Time Range**.

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

   Click **Next**.
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**.

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

    Click **Next**.

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 clear these 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**.

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.

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

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

    In the **Generated Reports** window, you can download, review, edit, duplicate, or delete the report. For more information, see Manage generated reports on page 130.

Generate a network devices report

Configure and generate a network devices report to obtain comprehensive data about your network infrastructure.

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.

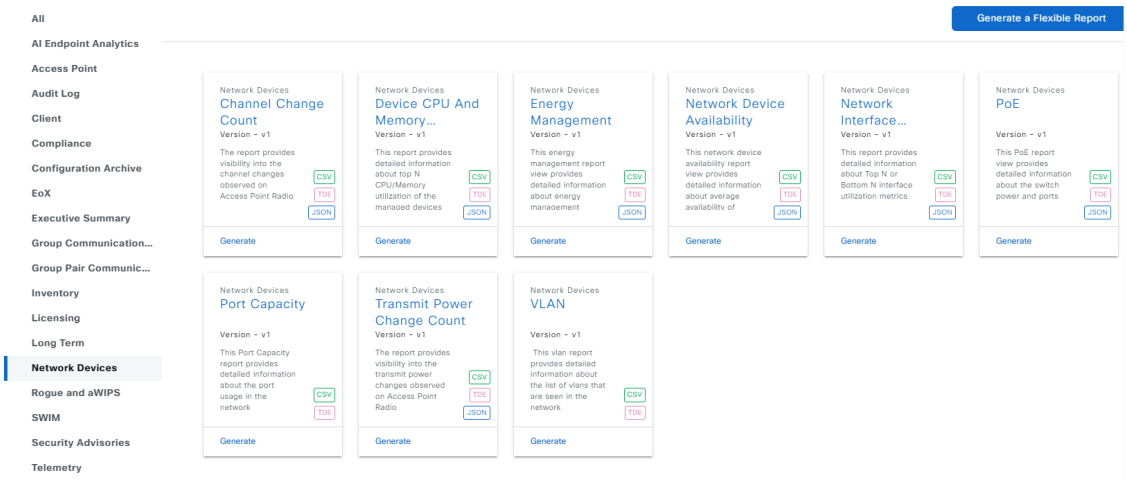
Procedure

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

   The **Report Templates** window displays the supported reporting categories. Each category is represented by a link. Click a link to view only the supported reports for that category.

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

   Figure 25: Network Devices report



Each template is represented by a tile. The tile contains information about the report and provides links to configure or 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.

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

   A window shows the sample report. Use the sidebar to review the sample report. The sample report displays:

   - applied filters, the data filters that were used to build the report,
   - data metrics and summaries,
   - graphical representation of the data (including line, bar, and pie graphs), and
   - tables that assist you analyze the data.

   Note

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

4. Close the preview window.
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.

6. In the **Generate a New Report** window, click **Let's Do It** to get started.
7. In the **Setup the Report Template** window, select the template for the report.

   Select a 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** to open the **Setup Report Scope** window.

8. Name the report and select the scope and the time range.

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

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

   Click **Next** to open the **Select File Type** window.

9. 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, use the **Fields** option to select attributes for your results.

   Click **Next** to open the **Schedule Report** window.

10. Select the schedule for the report.

    Click **Next** to open the **Delivery and Notification** window.

11. Select the delivery mechanism for the report:

    - **None**: No email or webhook notifications are 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 the appropriate 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 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** to open the **Summary** window.

12. Review your configuration and edit files if needed.

    Click **Generate Report**.

    After you generate the report, a success window appears.

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 Manage generated reports on page 130.

Generate a rogue and aWIPS report

Configure and generate rogue and aWIPS reports to monitor threats and wireless anomalies within your network.

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.

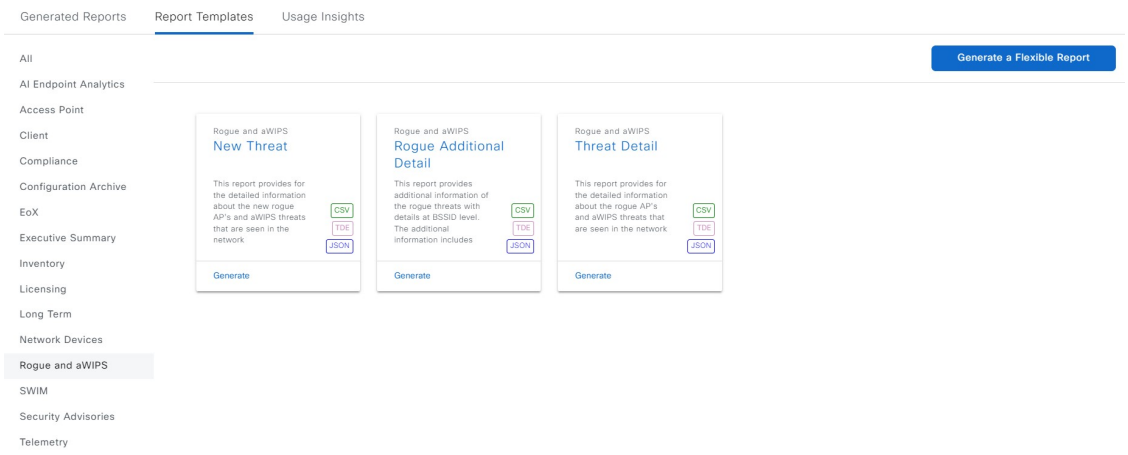
Procedure

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 see the supported reports in that category.

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. Each tile displays information about the report and links for generating a report. Choose the template you want to use to generate a report. Icons in each tile show the supported file types for reports.

3. Click the header to see a sample report.

   A window displays the sample report. Use the sidebar to review its contents. The sample report displays:

   - applied filters, which are the data filters used to build the report,
   - data metrics and summaries,
   - graphical representation of the data (including line, bar, and pie graphs), and
   - tables that help you analyze the data.

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

4. Close the preview window.
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.
6. In the **Generate a New Report** window, click **Let's Do It** to get started.
7. In the **Select Report Template** window, select the template for the report.

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

   > **Note**
   >
   > The **Template** contains individual report types for each release category.

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

   Click **Next** to proceed to the **Setup Report Scope** window.
8. Name the report, select the scope, and then select the time range.

   Enter a report name in the **Report Name** field and click the **Scope** field to display the available filters. Select the options you want for the report, and then select the **Time Range**.

   > **Note**
   >
   - The **Setup Report Scope** options vary based on the selected **Template**.
   - If all the access points (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 AP devices under the global hierarchy.

     To see threats for unassigned APs, leave the location filter empty.

   Click **Next** to open the **Select File Type** window.
9. Select the file type for the report.

   The available **File Type** options depend on the report that you are creating:

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

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

Click **Next** to open the **Schedule Report** window.

10. Select the schedule for the report.

    Click **Next**.

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, uncheck the 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 in the **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. 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.

Click **Next** to open the **Summary** window.

12. Review the configuration and edit any of the files, if necessary.

    Click **Generate Report**.

    After the report is generated, a success window appears.

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

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

    In the **Generated Reports** window, you can download, review, edit, duplicate, or delete the report. For more information, see Manage generated reports on page 130.

Generate an ROI report

Customize an ROI (Return on Investment) Insights report to quantify productivity improvements and cost savings from using Catalyst Center compared to a traditional NMS.

The Catalyst Center platform ROI Insights report shows you how your network operations improve in productivity with Catalyst Center and gives you ROI insights compared to a traditional NMS.

Use this procedure to configure an ROI report for your network operation.

Procedure

1. From the main menu, choose **Reports** > **Usage Insights**.

   The **Usage Insights** window shows these details.

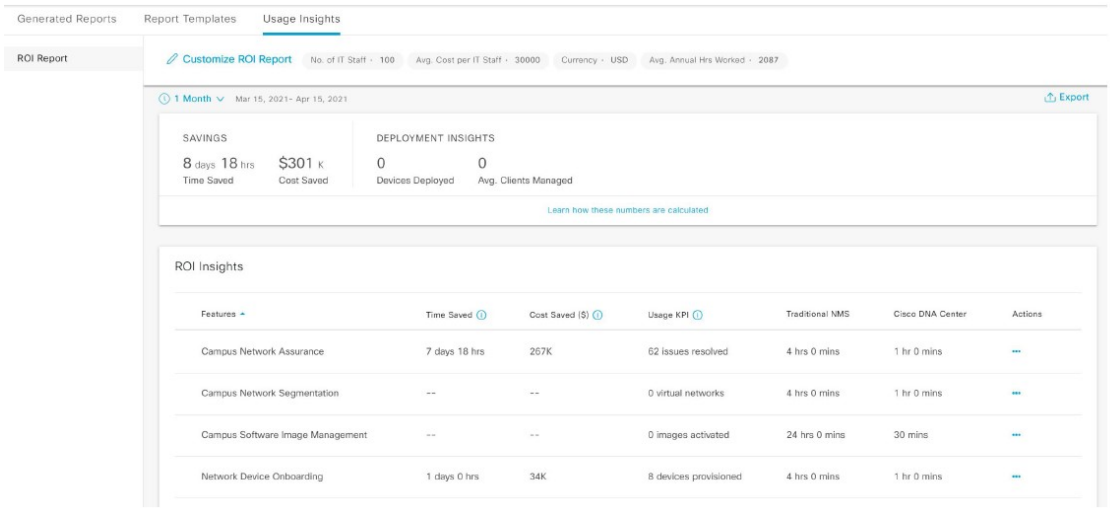
   - **SAVINGS**: displays the time and cost saved on network operation with Catalyst Center for a selected time range.
   - **ROI Insights**: lists the ROI Insights report which you create based on the report features, time saved, cost saved, usage KPIs, traditional NMS time, and actions.
   - **Savings 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.

2. In the **Campus Network Assurance**, **Network Device Onboarding**, **Campus Software Image Management**, and **Campus Network Segmentation** areas, enter the time savings for both a traditional NMS and Catalyst Center in the **Hours** and **Minutes** fields.
   - 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.
3. To change the **Cost Inputs** and **IT Inputs**, click **Customize ROI Insights** and make changes.

   The **Customize ROI Insights** area shows the preconfigured **Average Cost per IT Staff**, **Currency**, **Number of IT Staff**, and **Average Annual Hours Worked**.
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.
5. To view the ROI report for a specific time range, click the time range drop-down list in the **Customize ROI Insights** pane and select the desired 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



6. Click **Learn how these numbers are calculated** in the center pane to view details for the **ROI Insights** table calculations.

   The **Calculation Details** window shows how to calculate **Time Saved** and **Cost Saved**.
7. To export the ROI report, click **Export**.

   The supported file types for the reports are PDF and CSV files.

Generate a security advisories report

Configure and generate a Security Advisories report to help you identify vulnerabilities that affect your network devices.

Follow these steps to configure a **Security Advisories** report 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

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

   In the **Report Templates** window, you see the available report categories. Each category appears as a link. Click the link for the report category you want to view

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

   Figure 28: Security Advisories report



   Each template appears as a tile that contains information about the report and links to generate a report. Within the tile are icons that represent the supported file types for the reports.

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

   A window appears displaying the sample report. Use the sidebar to scroll and review the full report. The report data includes:

   - applied filters used to build the report,
   - data metrics and summaries, and
   - tables that assist you in analyzing the data.

> **Note**
>
> Use the sample report to plan your report.

4. Close the preview window.
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.
6. In the **Generate a New Report** window, click **Let's Do It** to get started.
7. In the **Select Report Template** window, select the template for the report.

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

   > **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**.
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. Click in the **Scope** field to display the available filter. Choose the filter options you want for the report. Select the **Time Range**.

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

   Click **Next**.
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**.

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

    Click **Next**.

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

- **Email Report**: You 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 includes a link so you can access the report and open 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, uncheck the 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, such as 'In Queue,' 'In Progress,' and 'Success.' You can also view these notifications in the GUI.

Click **Next**.

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

    Click **Generate Report** to create the report.

    After you generate the report, a success window appears.

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 Manage generated reports on page 130.

Generate a SWIM report

Configure and generate Software Image Management (SWIM) reports to review software image status and updates across your network devices.

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.

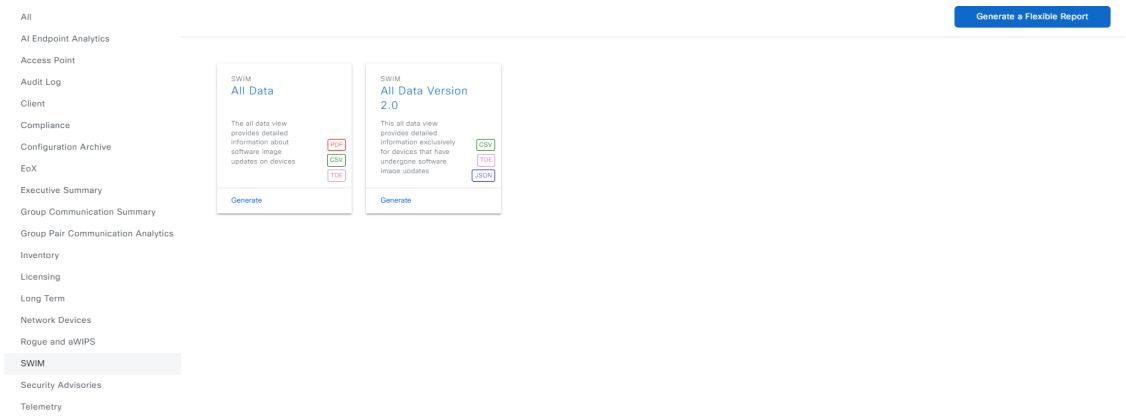
Procedure

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

   The **Report Templates** window displays the supported reporting categories. Each category is represented by a link. Click a link to view supported reports for that category.

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

   Figure 29: SWIM report



Each template appears as a tile. The tile contains information about the report and provides links to generate a report. Within the tile are icons that represent the supported file types for the reports.

3. Click the header within the tile to view a sample report.

   A window appears and shows the sample report. Use the sidebar to scroll and review the entire report. The sample report shows:

   - applied filters, which contains data filters that were used to build the report,
   - data metrics and summaries, and
   - tables that assist you in analyzing the data.

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

4. Close the preview window.
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.

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

   If you do not want to see this screen again, select the **Don't show this to me again** check box.

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**.

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. Click the **Scope** field to display available filters. Choose the filter options you want for the report, and select the **Time Range**.

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

   Click **Next**.

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

   Depending on the report 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 for the CSV, JSON, and Tableau Data Extract results.

   Click **Next**.

10. In the **Schedule Report** window, select the time range and schedule for the report.

    Click **Next**.

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

    - **None**: No email or webhook notifications are sent.
    - **Email Report**: The 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**: A successfully compiled report notification includes a link back to itself and to 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 email notification includes the report as an attachment.

> **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 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 messages as webhook notifications for the report. For example, you will receive status webhook notifications stating 'In Queue,' 'In Progress,' and 'Success.

Click **Next**.

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.

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 Manage generated reports on page 130.

Generate a flexible report

Configure and generate highly customized flexible reports by specifying entities, report types, filter criteria, attributes, aggregation, and sorting options, with CSV as the supported output format.

Catalyst Center allows you the flexibility to generate customized reports for your wired and wireless networks. This procedure describes how to configure **Flexible** reports. You can choose the entity, attributes, aggregation, and filters.

You can configure **Flexible** reports using the **Reports** window in the Catalyst Center GUI.

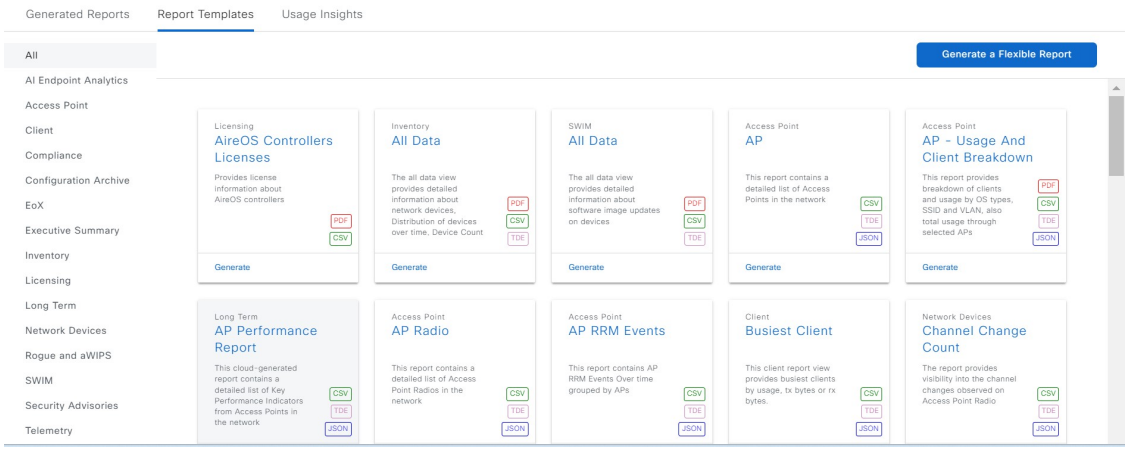
Before you begin

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

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

   Figure 30: Generate a flexible report



2. Click **Generate a Flexible Report**.

   Note

   Alternatively, click the menu icon and choose **Workflows** > **Flexible Report**.

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 avoid seeing the **Flexible Report** dialog box in the future, check the **Don't show this to me again** check box.

4. In the **Report Name** field, enter the name of your report. Select the **Time Range**.

> **Note**
>
> - You can generate the **AP**, **Client**, and **Network Device** reports for the past 180 days.
> - For the **PoE** reports, the supported time range is 30 days.
> - The supported time range for the **AP Ethernet Interface** reports is the last 30 days and the duration for each report is within 24 hours.

5. Click **Next**.
6. In the **Create a Subreport** window, enter the **Subreport Name**. Select the entity, report type, filter criteria, and respective attributes.

   In this release, the **Select an entity** drop-down list includes these options:

   - **Network Device**
   - **PoE**
   - **AP**
   - **SWIM**
   - **Client**
   - **AP Ethernet Interface**
   - **Network Interface**

   The **Report Type** options available are:

   - **Trend**
   - **Summary**
   - **Top N**
   - **Distribution**

   Select the filter criteria for the chosen report type.

   For example, for a **Trend** report type, select **Trending Interval** from the drop-down list.

   Select attributes in 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**
>
> For **Trend** and **Distribution** report types, you must select attributes that support group-by and aggregate options. For **Top N** report types, you must select an attribute that supports the sort-by option.

7. Click **Next**.
8. In the **Configure Group By, Aggregates and Sorting Options as Applicable** window, complete 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.
9. Click **Next**.

   The **Filters for the Current Subreport** window appears.
   - 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.

10. Click **Next**.

    The **Would you like to add another Subreport** window opens.
11. Select **Yes** to add another subreport.

    In the **Subreports Created** area, you can edit the parameters of any subreport, if necessary.

    Click **Next**.
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.

13. Click **Next**.

    In the **Summary** window, you can review the subreports and edit the parameters, if necessary.

14. Click **Generate Report**.

    After you generate the report, a success window appears with these options:

    - **Create Another Flexible Report**
    - **View the Generated Reports**

15. Click **View the Generated Reports**.

    The **Generated Reports** window shows details of the new flexible report.

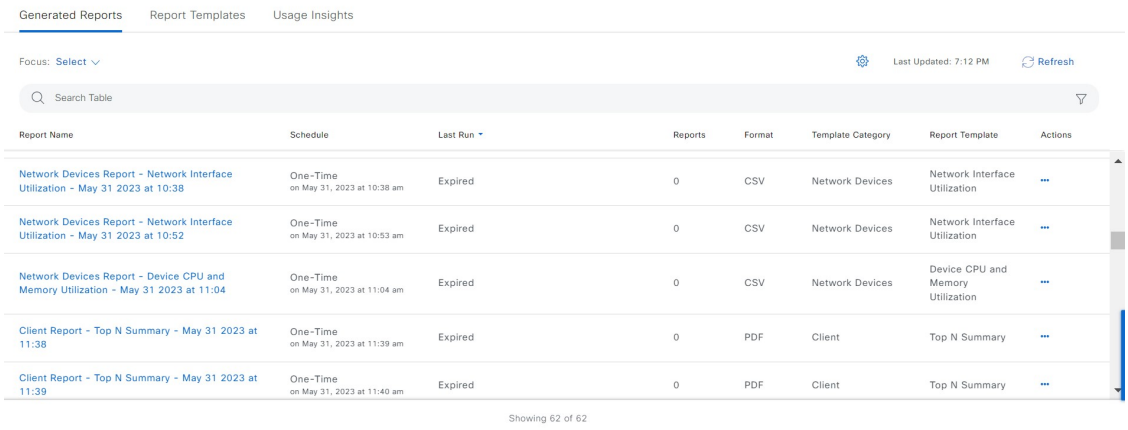
    You can download, review, edit, duplicate, or delete the report in the **Generated Reports** window. For more information, see Manage generated reports on page 130.

Manage generated reports

Configure, review, download, edit, duplicate, or delete previously generated reports, and monitor report retention and status indicators.

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

1. From the main menu, choose **Reports**.
2. Click **Generated Reports**.

   This information is shown:

- **Report Name**: Name of the report.

  If you did not name the report, the system assigns a default name that includes the report type, date, and time.

  > **Note**
  >
  > To view a report, click the report name link in the **Generated Reports** window. To download a report, click **Download**.

- **Schedule**: One-time generated report or recurring report. Also shown is a brief description of the schedule that generated the report.
- **Last Run**: Displays report execution status and details. The possible report execution status types include those that are:
  - **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.

    Click the downward-pointing arrow icon to download the last generated report.
  - **Expired**: Report expired and no longer available in Catalyst Center.
  - **Error**: Report execution failed.
- **Reports**: The number of generated reports, up to seven.

  Hover the mouse pointer over the displayed report number to see **View Report List**. Click **View Report List** to open a dialog box listing all report executions and their status (**Not Initiated**, **In Queue**, **In Progress**, **Completed**, **Expired**, and **Error**). The dialog box also shows a **Download** button to download a copy. Click **Error** to view any errors or warnings for the report execution.

  > **Note**
  >
  > Catalyst Center retains a total of seven reports. Specifically, it retains the last seven executed reports and the last seven executed over the last seven days. For example, if you run eight reports in a single day, only the most recent seven reports remain. If you schedule one report per day, only the seven most recent daily reports are kept. You can export reports in various formats 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.

To filter downloads in the GUI, click the **Filter** icon and use the filter or enter a keyword in the **Find** field.

3. Click **Actions** to perform one or more 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.

  > **Note**
  >
  > 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**. Click **Save** to delete all previous reports, even if you do not make any changes to the configuration.

- **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**
  >
  > To create a new report based on the configuration of an existing report, use **Duplicate** and modify the settings. The original report and its settings remain unchanged. To replace an existing report, use **View Config** and **Edit**
  >
  > .

- **Run Now**: Starts the process to execute the report. After the report runs successfully, a message confirms the successful execution.

  > **Note**
  >
  > If you try to run a report and seven reports already exist, the GUI warns you that only the last seven reports are saved. Use **Run Now** to generate a report outside the report schedule.

- **Delete**: Deletes the report. You are prompted to confirm the action before the report is deleted.

8 Developer Toolkit GUI

Topics:

- Developer toolkit
- Work with APIs
- Manage integration flows
- Configure event notifications for network events

This chapter introduces the developer toolkit within the GUI, explaining how to work with APIs, integration flows, and event notifications, including generating code previews and simulating events.

Developer toolkit

This section explains how the developer toolkit provides software development resources such as APIs, integration flows, and event notifications for easy access and integration with Catalyst Center.

Use a developer toolkit to access software development tools that

- offers APIs organized by specific functionality,
- provides integration flows sorted by category type, and
- enables event notifications for subscribing to and viewing network events.

Developer toolkits helps you access Catalyst Center, support programming tasks, and and make it easy to integrate with other applications through a standardized interface. These toolkits provide ease of use and interoperability.

Examples

- **APIs**: available API operations organized within categories by functionality, such as **Operational Tasks** or **Site Management** API operations.
- **Integration Flows**: workflow integrations organized by category type.
- **Event Notifications**: subscribe to network events for proactive management.

Work with APIs

Configure and test Catalyst Center APIs using the Developer Toolkit to review documentation, generate code previews, and test API calls with live responses.

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. This includes the request method and URL, query parameters, request header parameters, responses, schema, and methods for previewing or testing the request.

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

Before you begin

- Ensure you meet programming language and authentication prerequisites. For more information, see API prerequisites on page 35.
- Enable the **Rogue and aWIPS** bundle in Catalyst Center to access specific APIs. To enable the Rogue and aWIPS bundle, navigate to **Platform** > **Manage** > **Bundles** > **Rogue and aWIPS** and select **Enable**.

Procedure

1. From the main menu, choose **Platform** > **Developer Toolkit** > **APIs**.
2. Review the list of supported APIs.

   If necessary, click the **>** icon to display the API subdomains.
3. Select a domain or subdomain to view the APIs.

   Information about each API in that domain appears in columns.

   - **Method**: supported methods that 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.

  > **Note**
  >
  > 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**: a brief description of the API.
- **URL**: the URL value for the API.
- **Actions**: to create a code preview snippet with the **Try** option.

> **Note**
>
> A blue color-coded message may appear. This message indicates that the specific API configuration is still in progress. You should check again later. The screen refreshes automatically when the API is registered, enabling you to proceed with your API activity. If a red color-coded message appears stating that the API cannot be configured, contact your Catalyst Center administrator. The administrator should contact Cisco for help resolving the issue.

4. Click the name (link) of an API method.

   This information about the API method appears:

   - **DESCRIPTION**: a 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**: the 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.

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.

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**.

7. (Optional) Try the method by clicking **Try**.
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. 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.

Manage integration flows

Configure, review, and schedule integration flows to enable seamless interactions between Catalyst Center and external IT Service Management (ITSM) platforms.

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. It performs a task and pushes the information to a REST endpoint or another 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. Bundles also 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

- Ensure integration flows are enabled for the required bundles in 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**.

- Verify access to the Developer Toolkit and necessary permissions.

Procedure

1. From the main menu, choose **Platform** > **Developer Toolkit** > **Integration Flows**.
2. Review the integration flows displayed by the GUI.
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, clicking the integration flow name displays extra data. This data includes the description, tags, parameters, responses, model schemas, and policies.

     If the integration flow is a schedule-based trigger type, clicking the integration flow name opens a slide-in pane for setting the schedule. The slide-in pane displays **DESCRIPTION**, **TAGS**, and **HOW TO USE THIS FLOW** content.

   - **Description**: brief description of integration flow.
   - **Trigger**: schedule-based or REST-based.
   - Icon (**...**): provides links to create a code preview or access the **Try** option. If the integration flow is schedule-based, this icon accesses a **Schedule Flow** option.

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.

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.

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**.

7. To try a REST request path interactively, mouse over the icon (**...**) and click **Try**.
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). The Catalyst Center APIs use standard HTTP status codes to represent error conditions.

9. For the schedule-based integration flow, mouse over the icon (**...**) and click **Schedule Flow**.
10. Review this data:
    - **DESCRIPTION**: description and purpose of integration flow.
    - **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.

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.

Configure event notifications for network events

Configure notifications for specific network events, including REST API, email, syslog, SNMP trap, and Webex channels. View, edit, and manage event notifications and their settings.

You can associate a notification to specific events that may occur in your network. After you associate a notification with an event, and when that event occurs, you receive a notification by REST API or email You associate a notification with an event by using the **Event Notifications** window in the Catalyst Center platform GUI.

Before you begin

- Ensure webhook destination is configured for REST API notifications 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 69.
- Configure email destination for email notifications 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 email destinations for event and report notifications on page 71.
- Set up syslog server destination for syslog notifications 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 72.
- Configure an SNMP trap destination for SNMP notifications 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 73.
- Access the **Event Settings** window and review or edit 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

1. From the main menu, choose **Platform** > **Developer Toolkit** > **Event Notifications**.

   The **Events Notifications** window appears.

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.

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.

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**: the 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**.

5. In the **Notification Details** slide-in pane, click the toggle button at the top-right corner to enable or disable the respective notification.
6. To edit a particular notification, click the **Actions** drop-down list and select **Edit**.
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.

8. Click the toggle button at the top-right corner to toggle between the tile view and list view.
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.

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.

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

Use event simulation to test an event's subscription (email, REST API, SNMP trap notification, syslog server, or Webex).

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 72.
- 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 email destinations for event and report notifications on page 71.
- 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 69.
- 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

1. From the main menu, choose **Platform** > **Developer Toolkit** > **Event Notifications** > **Event Catalog**.
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.

3. Click **X** to exit from the field.
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.

9 Runtime Dashboard

Topics:

- Runtime dashboard
- Review the event summary
- Review API summary
- Review the CMDB synchronization summary
- Review the integration flow summary

This chapter describes the Runtime Dashboard, which offers summaries of API calls, events, CMDB synchronization, and integration flows, helping users monitor the platform's performance and troubleshoot issues like ITSM event retries.

Runtime dashboard

This section explains how the Runtime dashboard summarizes business API performance, event statuses, CMDB synchronization, and integration flow execution for monitoring and troubleshooting.

A runtime dashboard is a system monitoring tool that

- displays real-time summaries of business API (BAPI) activity and performance,
- presents event statuses such as REST endpoint interactions and integration flows, and
- shows device synchronization status with Configuration Management Database (CMDB).

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. You can click **View Details** to access 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

Verify event publication and troubleshooting status using the Event Summary in the Runtime Dashboard.

Follow these steps to review the Catalyst Center platform **Event Summary**.

> **Note**
>
> 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. Review the **Event Summary** in the **Runtime Dashboard** window in the Catalyst Center GUI.

Before you begin

- Ensure bundles are enabled, configured, and activated in **Bundles**.
- Enable associated event notifications for bundles in Event Settings.

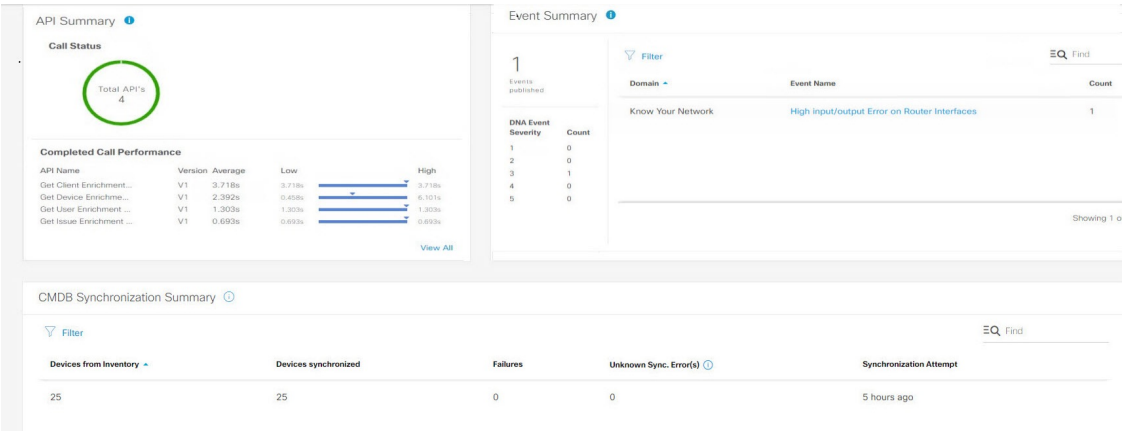
For information about **Bundles**, see Bundle features on page 45. For information about **Event Settings**, see Configure event settings on page 64.

Procedure

1. From the main menu, choose **Platform** > **Runtime Dashboard**.
2. Choose a time interval for the event summary by clicking **Last 1 Week** at the top of the GUI menu bar.

   You can view the event summary for the last six-hour, twelve-hour, or twenty-four-hour period, or for the last week.
3. Review the **Event Summary** section in the **Runtime Dashboard** window.

   Figure 32: Events Summary



   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 from one to five.
   - **Count**: Number of events.
   - **Events**: The list shows events grouped by domain (category), with event name (as links), and count (number of events).

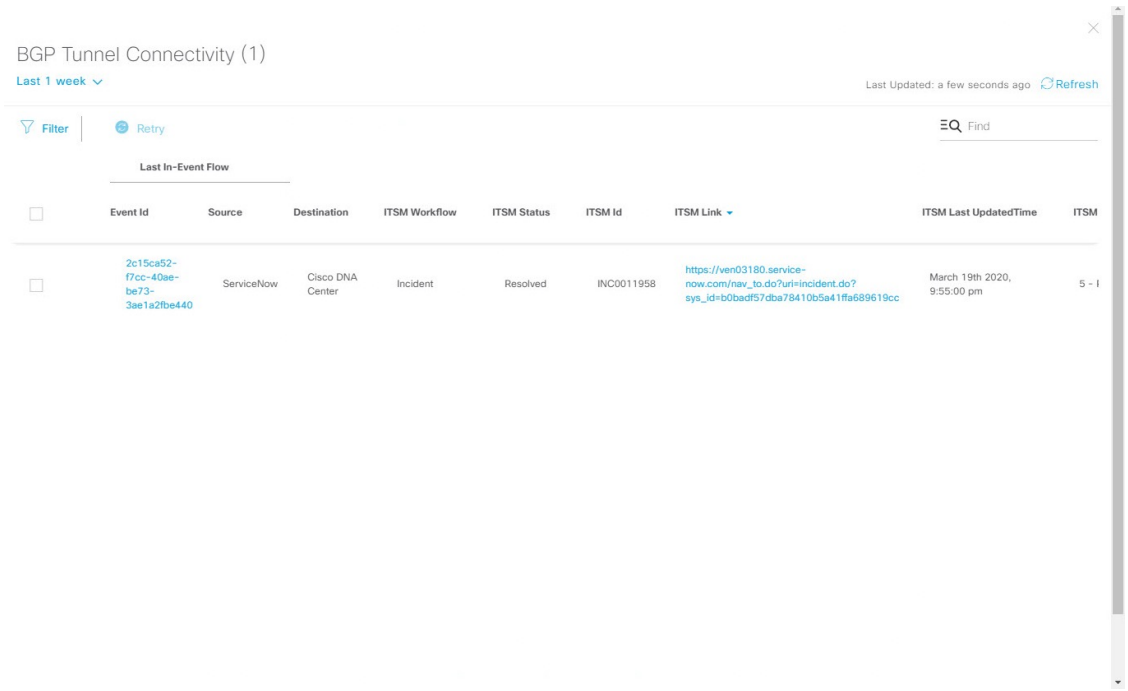
   Note

   Scroll to view the entire list using the scroll bar.
4. Click an event name (link) to view additional detailed data.

   For example, if the events **Router Unreachable** or **BGP Tunnel Connectivity** exist in your GUI window, click the link.

   After clicking an event name (link), the system opens a slide-in pane.
5. View a list of this type of event (history) in the slide-in pane.

   Figure 33: Event history



Each event includes these details.

- **Event ID**: displays the Catalyst Center event identification number generated by Catalyst Center.
- **Source**: indicates the location from where event originated. For example, the Catalyst Center platform or an IT Service Management (ITSM) system, such as ServiceNow.
- **Destination**: indicates the location to which the event was directed. For example, the Catalyst Center platform or an ITSM system, such as ServiceNow.
- **ITSM Workflow**: displays the type of ITSM workflow, such as an **Incident** or **Problem**.
- **ITSM Status**: shows the current status of the event. For example, an event can have a status of **Open**, **New**, **Closed**, or **N/A**.
- **ITSM ID**: displays the ITSM event identification number generated by the ITSM, such as ServiceNow.
- **ITSM Link**: displays a link to the ITSM server for the ITSM event.
- **ITSM Last Updated Time**: shows the last date and time of event update.
- **ITSM Entity Severity/Priority**: indicates ITSM severity or priority assigned to the event.
- **Event Severity**: indicates the Catalyst Center severity assigned to the event from one to five.

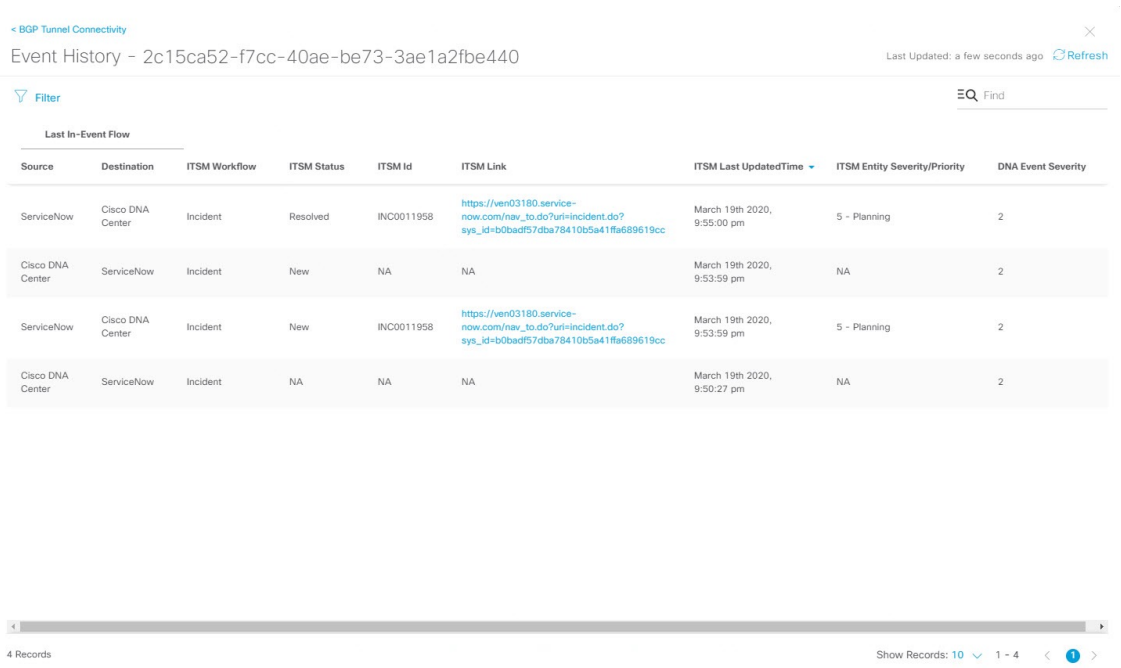
You can adjust the events that show in the table by clicking the **Filter** icon and using the filter, or by entering a keyword in **Find**.

6. Click an event ID number (link) to view only data associated with that specific event.

   When you click an event ID number (link), the system opens a slide-in pane.

7. View the event ID data in the slide-in pane.

Figure 34: Event ID data



The slide-in pane shows information of this single event.

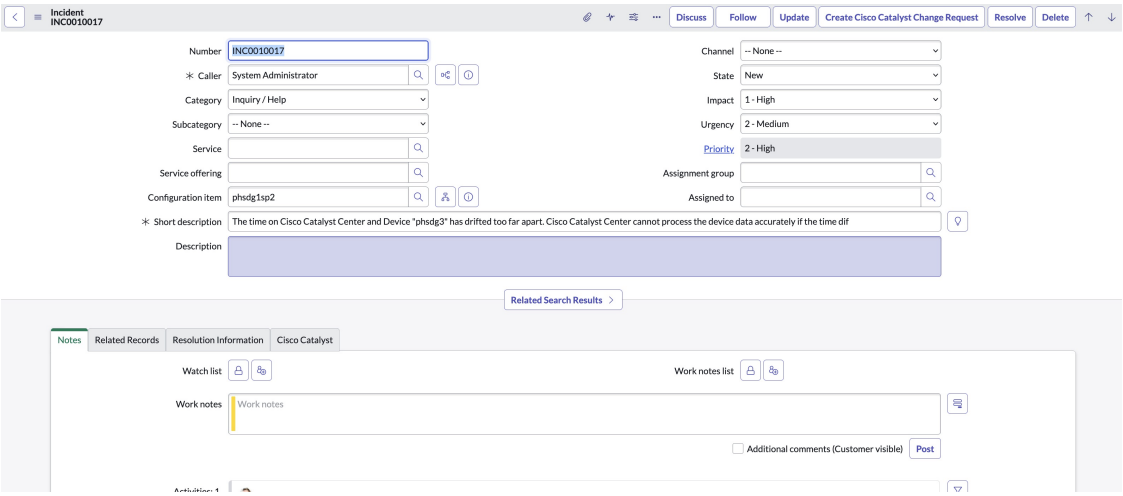
- **Source**: shows the location from where the event originated, such as the Catalyst Center platform.
- **Destination**: indicates the location to which the event was directed to. For example, the REST Endpoint.
- **ITSM Workflow**: shows the type of ITSM workflow, such as an **Incident** or **Problem**).
- **ITSM Status**: indicates the current status of the event. For example, an event can have a status of **Open**, **New**, or **Resolved**.
- **ITSM ID**: displays the ITSM event identification number.
- **ITSM Link**: gives the link to the ITSM, such as ServiceNow.
- **ITSM Last Updated Time**: indicates the last date and time of event update.
- **ITSM Entity Severity/Priority**: displays the ITSM severity or priority assigned to the event.
- **Event Severity**: shows the Catalyst Center severity assigned to the event from one to five.

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.

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

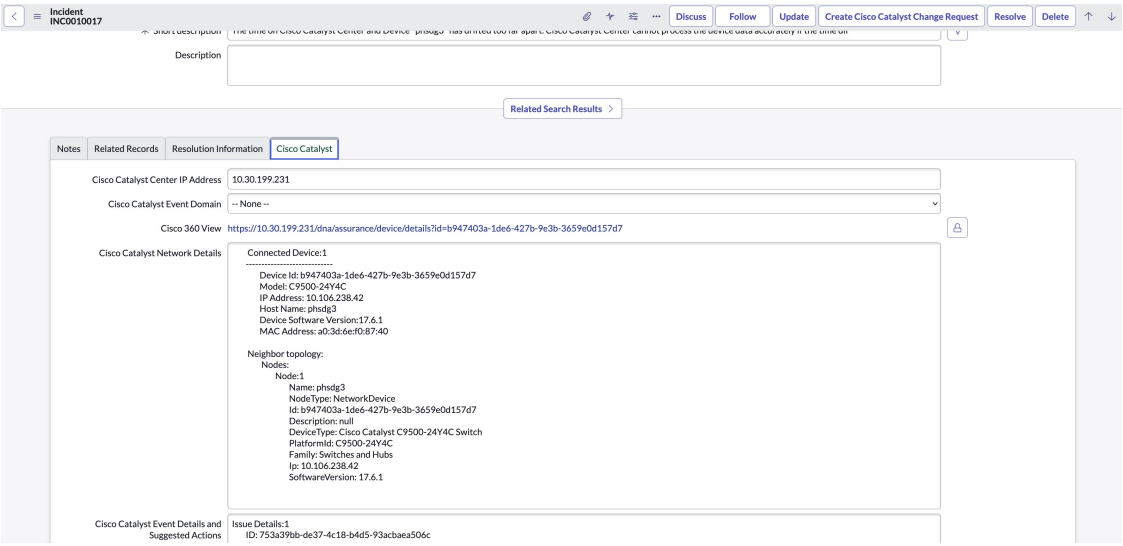


Note

To make the **Runtime** event link to the ITSM program operational, set up the Catalyst Center platform integration to ServiceNow as described in the *Cisco Catalyst Center ITSM Integration Guide*.

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

Retry, resend and reprocess IT Service Management (ITSM) events—such as those sent to ServiceNow—from the Event Summary window to resolve integration issues.

You can retry, resend and reprocess an IT Service Management (ITSM) event from the Catalyst Center platform to an ITSM, such as 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. Use the **Event Summary** to monitor and troubleshoot the Catalyst Center platform and its integration with other systems.

Before you begin

- Enable, configure, and activate the necessary bundles in **Bundles**.
- Enable associated event notifications for these bundles in **Event Settings**.

Procedure

1. From the main menu, choose **Platform** > **Runtime Dashboard**.
2. Choose a time interval for the event summary. Click **Last 1 Week** in the GUI menu bar.

   You can view the event summary for the past six-hour, twelve-hour, or twenty-four-hour period, or for the week.
3. Review the **Event Summary** section in the **Runtime Dashboard** window.

   View these details about any of the current events.

   - **Events Published**: indicates the total number of events that are captured and published (displayed in the GUI) by the Catalyst Center platform.
   - **Event Severity**: shows event totals by severity number, from one to five.
   - **Count**: indicates the number of events.
   - **Events**: lists events by domain (category), event name (links), and count (the number of events).

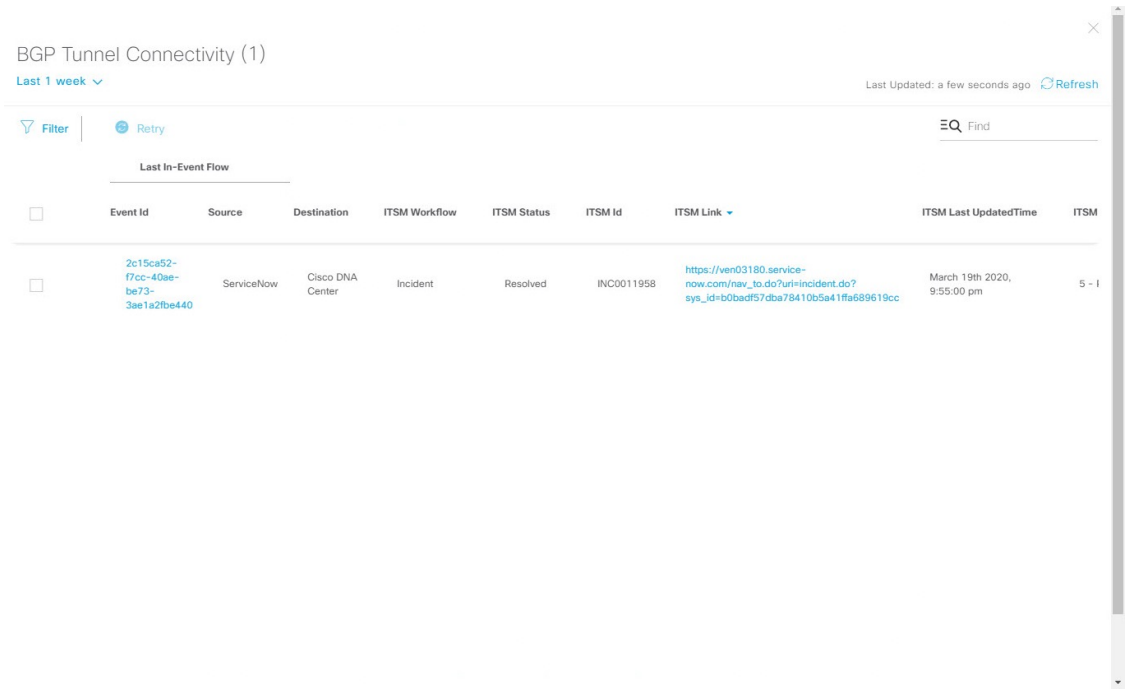
   > **Note**
   >
   > Use the scroll bar to view all events in the list.

4. Click an ITSM event name (link) to view detailed data.

   If the ITSM event **SWIM Upgrade Request Creation Image Activation** appears, click the link.

   After you click an event name (link), a slide-in pane opens.
5. Review the event history for this type of event in the slide-in pane.

   Figure 37: Event history



Each event provides these details.

- **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 such as ServiceNow.
- **Destination**: location for where the event was directed to. For example, the Catalyst Center platform or an ITSM system such as 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 such as 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, from one to five.

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.

6. Determine which ITSM events must be resent and reprocessed.

   If an ITSM event displays **N/A** for **ITSM Workflow**, **ITSM Status**, or **ITSM ID** and the source is ServiceNow, and the destination is Catalyst Center, retry the event. A check box appears under the **Filter** column for these events.

7. Check the check box in the **Filter** column to select an ITSM event and enable the **Retry** button.
8. Click **Retry**.

   After the event is resent to the ITSM destination, one of these may occur:

- Retry Success: appropriate values are displayed 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.

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.

10. Click **Try It** and enter the instance ID (**instanceId**) for the failed event from the **Runtime Dashboard**.
11. Click **Run**.

    You can retrieve this response data using the 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 API summary

Verify API call status and performance in the Runtime Dashboard. Review call counts and durations to monitor API activity.

Before you begin

- Enable, configure, and activate the bundles that generate the events you want to monitor.
- Locate and manage these in the **Bundles** list.

For information about **Bundles**, see Bundle features on page 45.

Procedure

1. From the main menu, choose **Platform** > **Runtime Dashboard**.
2. To select a time interval for the API summary, click **Last 1 Week** at the upper right side of the GUI.

   You can view the API summary for the last six-hour, twelve-hour, or twenty-four-hour period, or for the last week.

3. Review the **API Summary** field.

   You see these details in the **API Summary** field.

   - **Call Status**: displays the total number of API calls and status display. Green represents successful API calls, and red represents unsuccessful API calls.
   - **Completed Call Performance**: this section lists API calls in alphabetical order with completed-call performance in seconds: low, average, high.
   - **View Details**: use this link to view additional API details.

4. Click **View Details** to see more details about the APIs.

   The **All APIs calls** slide-in pane opens.

5. Review these details in the **All APIs calls** slide-in pane.

   - API name
   - API version
   - API call count table

   > **Note**
   >
   > The table 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

   > **Note**
   >
   > The table includes minimum, maximum, and average duration.

   To adjust the APIs that display in the tables, click the **Filter** icon and apply a filter, or enter a keyword in the **Find** field.

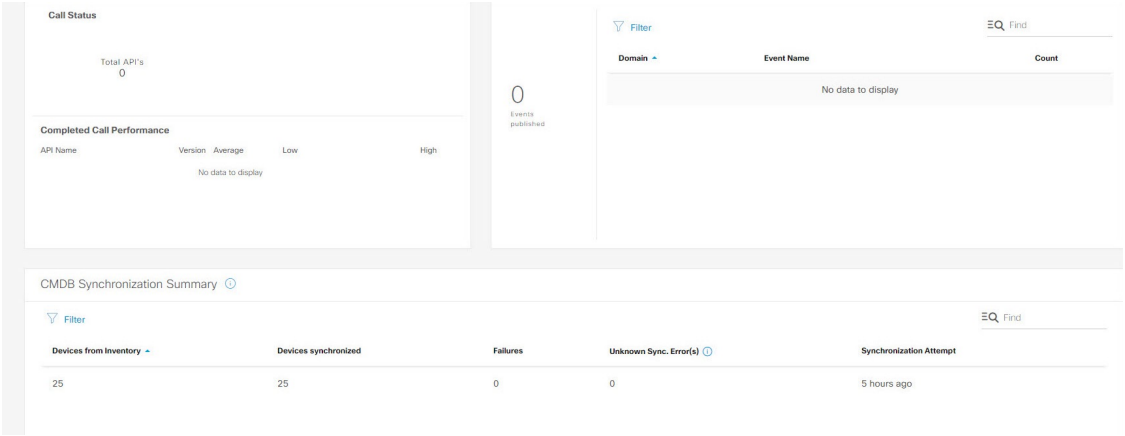
Review the CMDB synchronization summary

Verify CMDB device synchronization status and troubleshoot inventory synchronization issues using the Runtime Dashboard.

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, which helps you monitor and troubleshoot device data synchronization issues.

To check the **CMDB Synchronization Summary**, use the **Runtime Dashboard** window in the Catalyst Center GUI.

Figure 38: Catalyst Center Platform Runtime window



Before you begin

- Ensure that bundles are enabled, configured, and activated in the **Bundles** section.
- Enable associated event notifications for these bundles in **Event Settings**.

  For details about bundles and event settings, see Bundle features on page 45 and Configure event settings on page 64.

Procedure

1. From the main menu, choose **Platform** > **Runtime Dashboard**.
2. Check the **CMDB Synchronization Summary** field, which displays these details.
   - **Devices from inventory**: displays the total number of devices from **Inventory** collected from Catalyst Center.
   - **Devices synchronized**: shows the list of devices that were successfully synchronized with ServiceNow.
   - **Failures**: shows the number of failed synchronization attempts between Catalyst Center and ServiceNow.

     Click **Learn More** for additional information.
   - **Unknown Synch Errors**: shows the number of partially successful synchronization attempts between Catalyst Center and ServiceNow

     Click **Learn More** for additional information.
   - **Synchronization Attempt**: displays details about when the last synchronization attempt was made between Catalyst Center and ServiceNow.
3. (Optional) Click the **Learn More** link for any synchronization failure.
4. Check the device's synchronization failure data on the screen.

   This information appears in a table.
   - **Device ID**: is the device identification number.
   - **Host Name**: name of the host to which the device is connected.
   - **Device Type**: type of device, such as a switch, a router, or an access point.
   - **MAC Address**: is the MAC address of the device.
   - **Management IP Address**: the management address of the device that can be used to access and troubleshoot the device.

- **Serial Number**: serial number of the device.

5. Click the **DeviceID** link to review additional information about the device in the **Inventory** window.

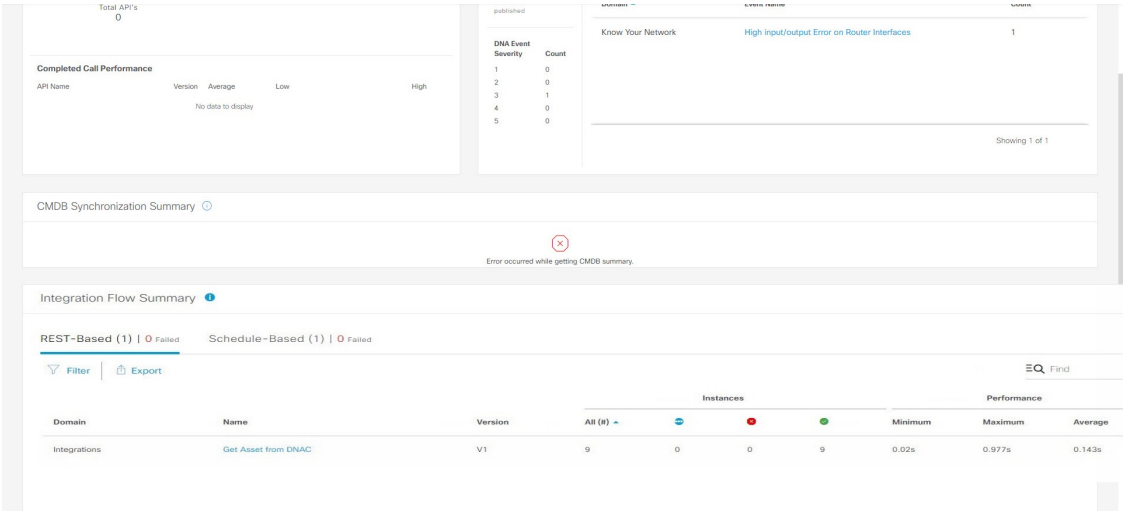
Review the integration flow summary

Verify integration flow performance and status using the Runtime Dashboard.

Review the Catalyst Center platform **Integration Flow Summary**. Use the **Integration Flow Summary** to monitor the performance of the Catalyst Center platform integration flows. Use this information to monitor or troubleshoot 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

Enable, configure, and activate the bundles that provide the events you want to monitor in **Bundles** to display data in the **Integration Flow Summary** fields (two tabs). For information about **Bundles**, see Bundle features on page 45.

Procedure

1. From the main menu, choose **Platform** > **Runtime Dashboard**.
2. Click **Last 1 Week** at the upper right side of the GUI menu bar to choose a time interval for the integration flow summary.

   You can view the integration flow summary for the last six-hour, twelve-hour, or twenty-four-hour period, or for the last week.

3. Review the details in the **Integration Flow Summary** field.

   - **REST-Based**: displays domain, integration flow name and link, version, instance totals, instance status (successful [green], fail [red], in progress [blue]), and performance that gives the minimum, maximum, and average call performance times (in milliseconds).

- **Schedule-Based**: displays domain, integration flow name and link, version, instance totals, instance status (successful [green], fail [red], in progress [blue]), and performance that gives the minimum, maximum, and average call performance times (in milliseconds).

4. Click the **REST-Based** tab to view a summary of data generated by REST-based integration flows
5. Review the **REST-Based** data.

   Click an integration flow name (link) to see more details about the instances. This information appears in a slide-in pane:

   - **Instance ID**: identification number (and link) of the instance to the integration flow.

     > **Note**
     >
     > 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 the call in seconds.

6. Click an instance ID (link) to view its details.

   The slide-in pane shows these additional information.

   - **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 screen.

7. Click the **Schedule-Based** tab to view a summary of data generated by schedule-based integration flows.
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.

9. Click an individual instance ID (link) to view detailed information about it.

   The slide-in pane displays these details.

   - **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.