

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



# Transform Your Network

Automation and Management with Catalyst Center APIs

Hector Morales  
Senior Solutions Engineer  
BRKOPS-2321

CISCO *Live!*

#CiscoLiveAPJC

# Cisco Webex App

## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



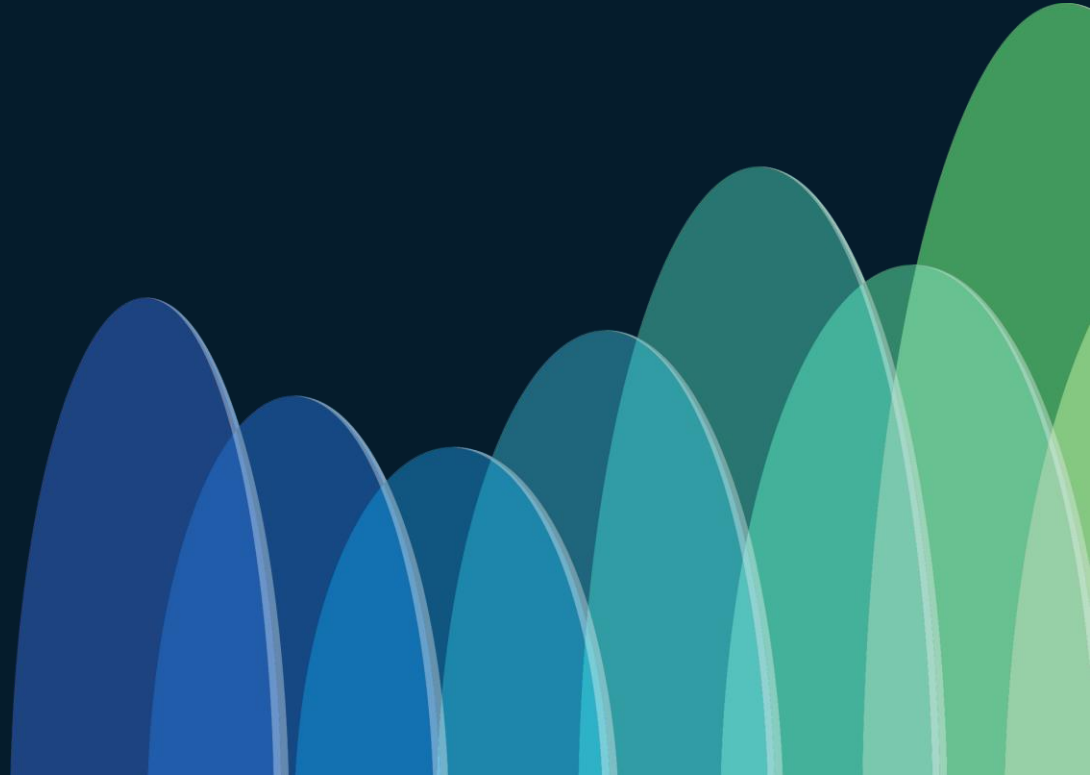
<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKOPS-2321>



# Agenda

- Customer challenges and opportunities
- Catalyst center headless deployments
- Catalyst center APIs
- Implementation guidelines
- Best practices
- Conclusion

# Customer Challenges and Opportunities



# Top 5 issues for IT

Annual OpEx spent  
on changes  
and troubleshooting

**\$45B**

Network administrators must balance the need for a high-performing network with the cost of implementing and maintaining it.

**1**

Network complexity

**2**

Security

**3**

Network performance

**4**

Network visibility

**5**

Cost

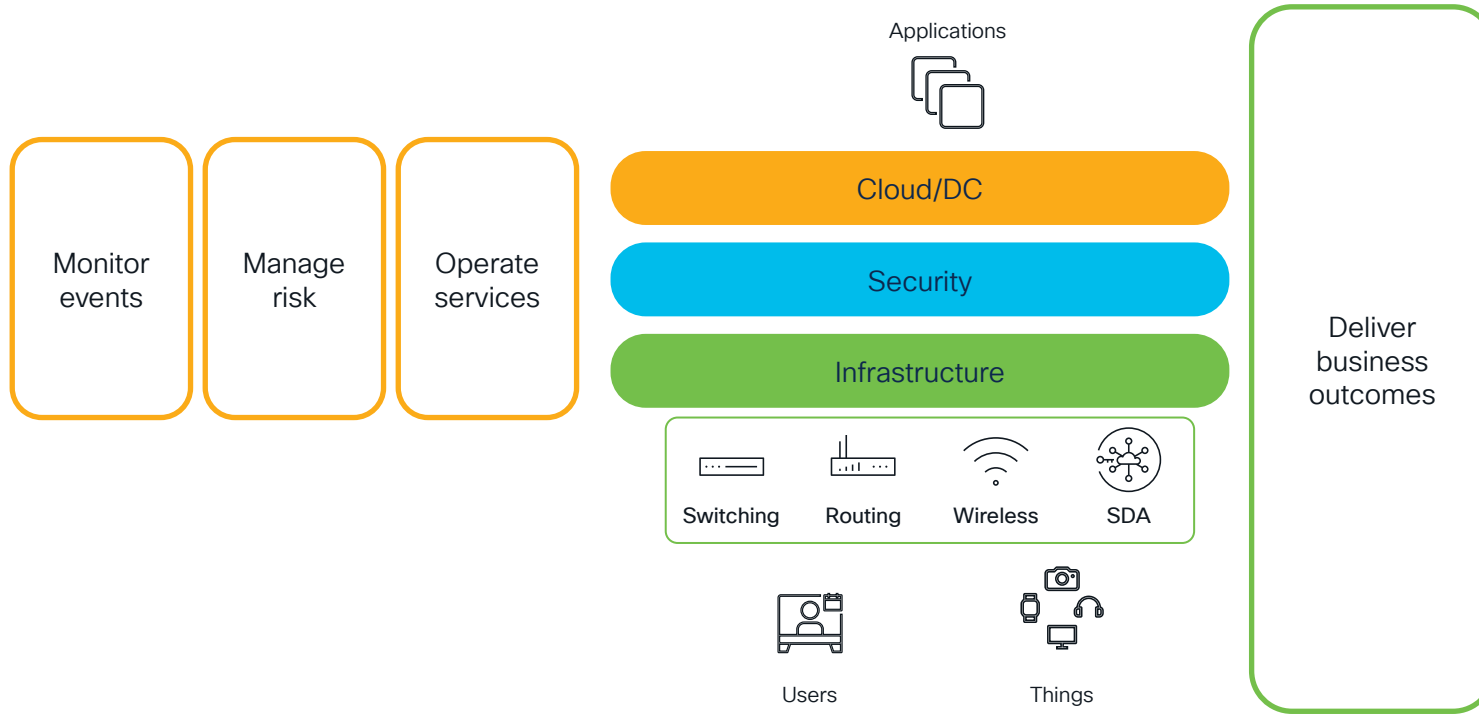
As networks grow in complexity, network administrators must find ways to automate network management tasks to reduce the risk of human error and improve efficiency.

**5%**

of large enterprises have an automated operation to decrease human errors

Source: Own research with public data from top 100 customers and service providers, 2024

# Customer's desired outcomes



# Practical realities of digital transformation

It can be hard and expensive

**\$60B**

Annually spent on  
Network operations,  
Labour and tools<sup>1</sup>



**95%**

Network changes  
performed manually



**75%**

of opex spent on changes  
and troubleshooting



**70%**

of policy violations are  
due to human error

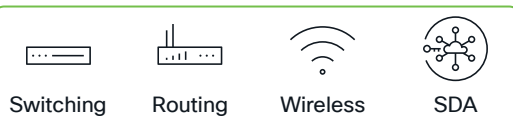


<sup>1</sup> Cisco McKinsey Study

# Catalyst Center Headless Deployments



# The complexity to operate large networks



```
Router# show running-config
Building configuration...

Current configuration : 5980 bytes
!
! Last configuration change at 13:56:48 PST Fri Nov 3 2017 by admin
!
version 16.6
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
platform shell
!
hostname Router
!
boot-start-marker
boot system tftp /auto/tftp-sjc-users5/c1100-universalk9_ias.16.06.02.SPA.bin 223.255.254.254
boot-end-marker
!
!
vrf definition VRF-example
description VRF-example
!
no logging console
!
aaa new-model
!
!
aaa login success-track-conf-time 1
!
!
!
aaa session-id common
```

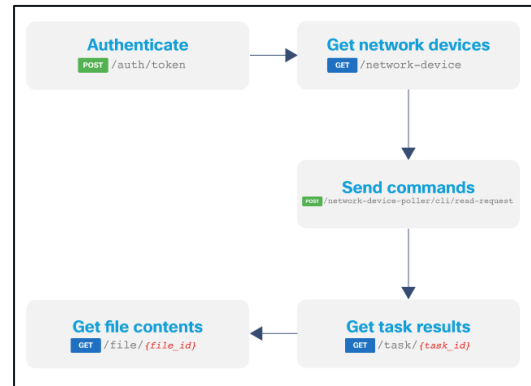
IOS XE CLI

```
- name: Check the running-config against master config
cisco.ios.ios_config:
  diff_against: intended
  intended_config: "{{ lookup('file', 'master.cfg') }}"

- name: Check the startup-config against the running-config
cisco.ios.ios_config:
  diff_against: startup
  diff_ignore_lines:
    - ntp clock .*

- name: Save running to startup when modified
cisco.ios.ios_config:
  save_when: modified
```

IOS XE Ansible  
Collection



Cisco Catalyst Center  
APIs

# The complexity to operate large networks

## Pros and Cons

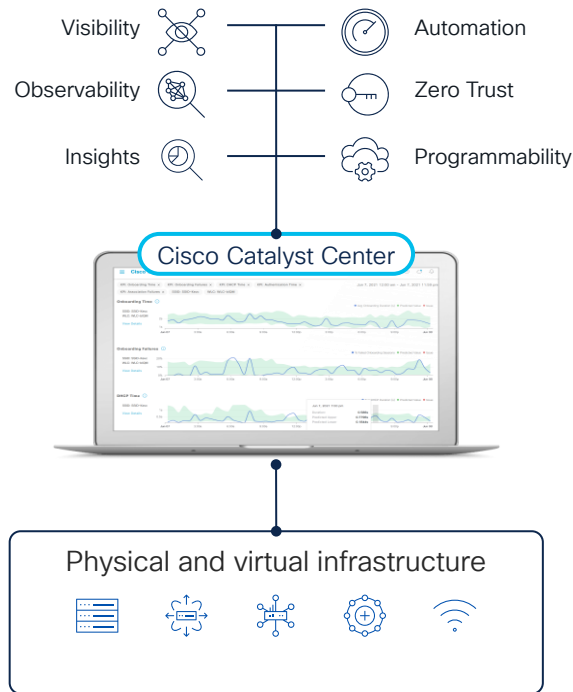
|                              | IOS XE CLI                                           | IOS XE Ansible Collection                                | Cisco Catalyst Center APIs                             |
|------------------------------|------------------------------------------------------|----------------------------------------------------------|--------------------------------------------------------|
| Day 0                        | ✓✓✓✓✓<br>Fine configuration<br>Prone to human errors | ✓✓✓✓✓<br>IaC, CI/CD pipelines<br>Requires more expertise | ✓✓✓✓✓<br>API Platform<br>Single tenant                 |
| Day 1                        | ✓✓✓✓<br>Data rich<br>Requires additional infra       | ✓✓✓<br>Leverage community<br>Prone to errors             | ✓✓✓✓✓<br>Extensive integration<br>Requires more coding |
| Day 2                        | ✓✓✓✓<br>Information rich<br>Complex to troubleshoot  | ✓✓<br>Leverage community<br>Not ready for Day 2          | ✓✓✓✓✓<br>Event management<br>Requires more coding      |
| Complexity <sup>1</sup>      | Very complex                                         | Mid complexity                                           | Low complexity                                         |
| IDEAL Team size <sup>2</sup> | 10-15 engineers                                      | 5-7 engineers                                            | 3-5 engineers                                          |

REALITY CHECK: We operate with reduced teams

Source: Own research with public data from top 100 customers and service providers, 2024  
1 - Network size: 20,000 devices in a single campus  
2 - Necessary team to support single campus

# Catalyst Center simplifies network operations

Enabling IT admin to deliver business outcomes, smarter and faster at scale



Small teams' productivity increase through automation

## NetOps

### Increase Scale

- Providing customers with business resiliency, continuity, and quick time to value
- Enabling customers to achieve Compliance of network with config policies
- Automation to simplify the creation and maintenance of customers networks

## SecOps

### Improved Security

- AI-driven security to classify endpoints and enforce security policies for a complete zero trust workplace solution
- Automate end point visibility, classification, and grouping

## DevOps

### Improved Service Delivery

- Mature APIs, SDKs, and closed-loop integrations to simplify and streamline ecosystem integration
- Faster service delivery using API-based automation workflows
- Early issue detection and integration with 3rd party platforms through enhanced notification channels

## AIOps

### Improved Performance Insights

- Reduced proactive problem resolution through faster Root Cause Analysis
- AI-driven visibility, observability, insights, and troubleshooting to ensure the health your customers applications, infrastructure and user experience

# Catalyst Center as a platform

Powered for headless integration

## Event Notifications

- Assurance Issues
- AI/ML Insights
- System Health
- Integration Connectivity
- License Management
- Webhooks
- PagerDuty
- Email
- Syslog
- SNMP

## Northbound REST APIs

- Network Inventory
- Network Topology
- Network Design
- Provisioning
- SWIM, PnP
- Path Trace
- Assurance
- SDA
- Templates
- RMA
- Config Archive
- Sensors

## IT Ecosystem Integrations

- IT Service Management
- IP Address Management
- Reporting
- Wireless Planning
- Alerting
- SIEM

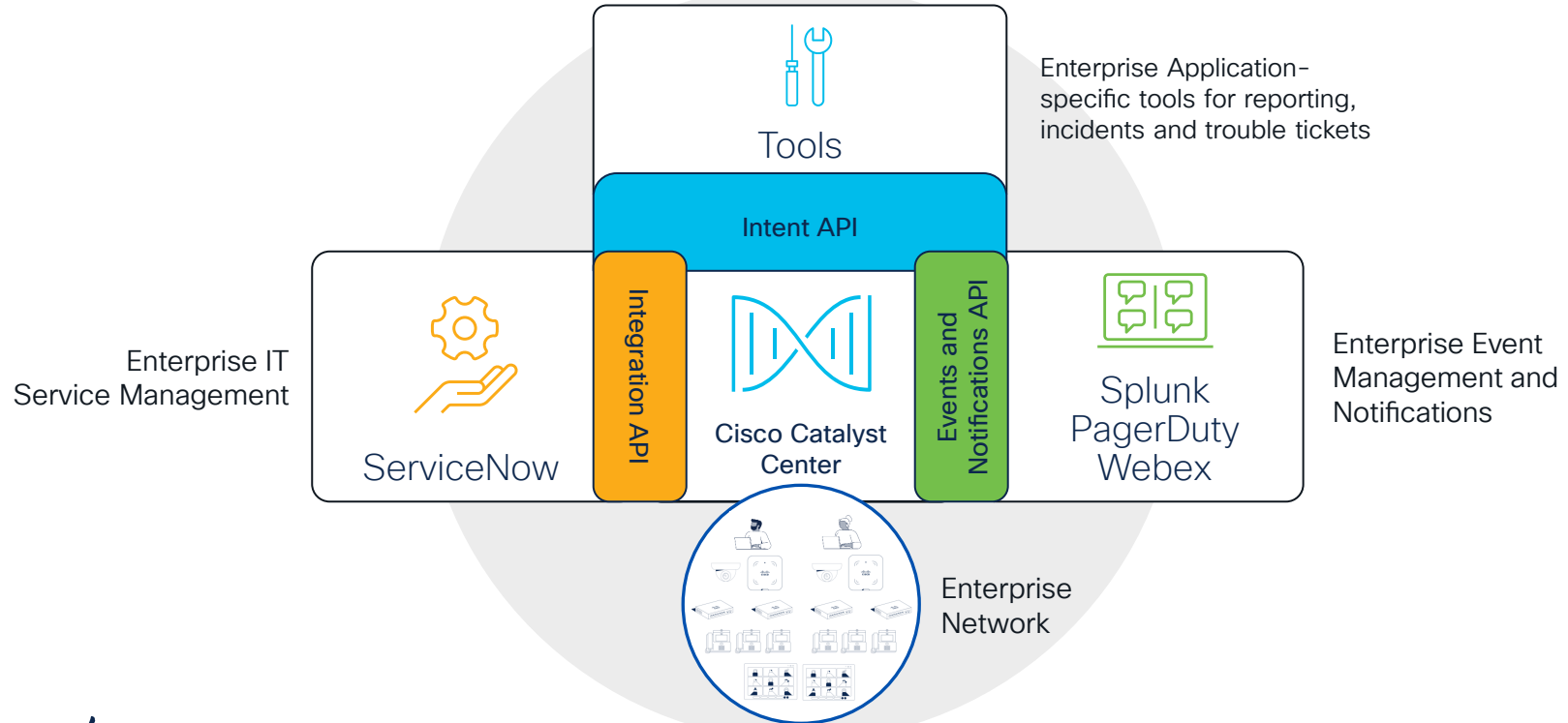
## Developer Resources

- Sample Code, Videos
- Python SDK, Ansible, Terraform
- Cisco DevNet
  - Sandboxes, Learning Labs
  - Developer Guides
  - Sample Code



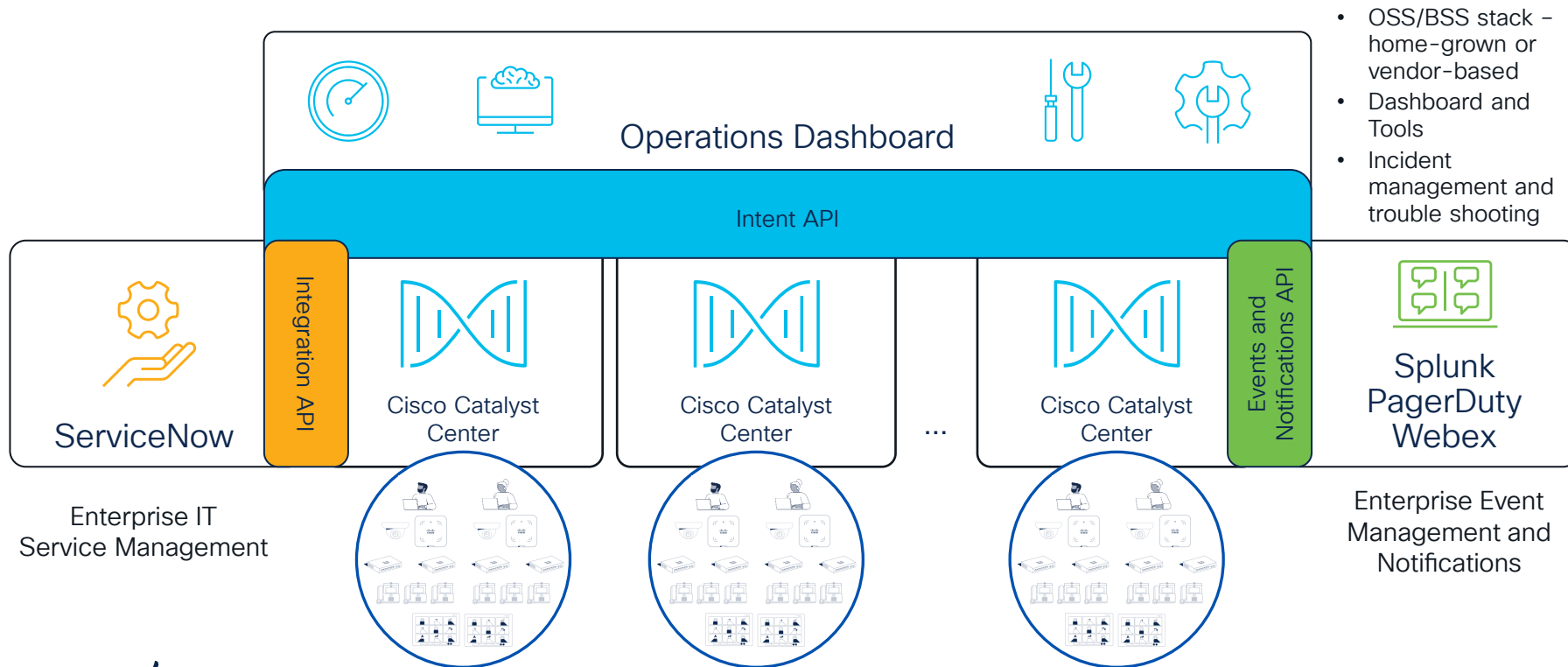
# Cisco Catalyst Center enterprise architecture

Align to ITIL framework



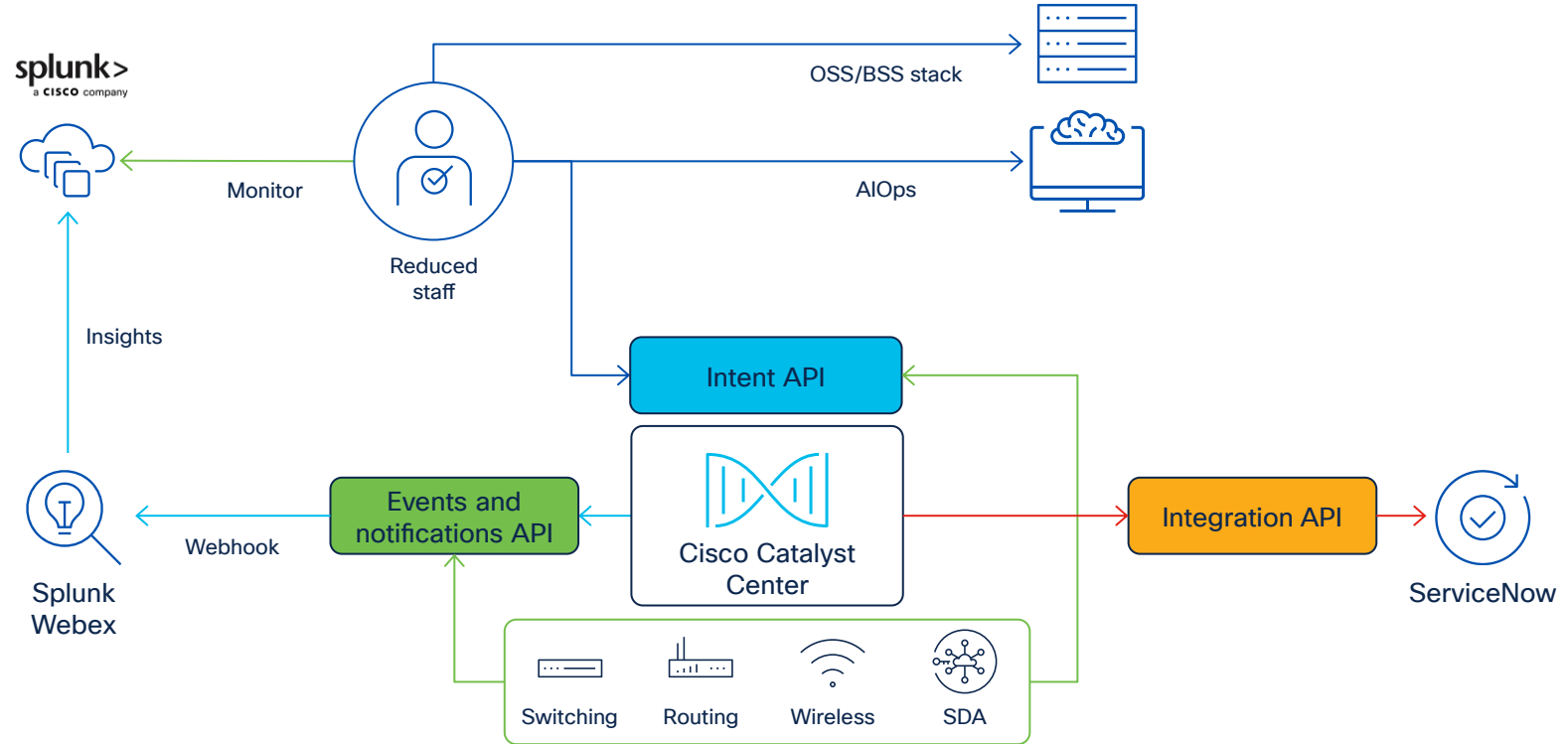
# Cisco Catalyst Center architecture

Headless operations: operate Catalyst Center at scale

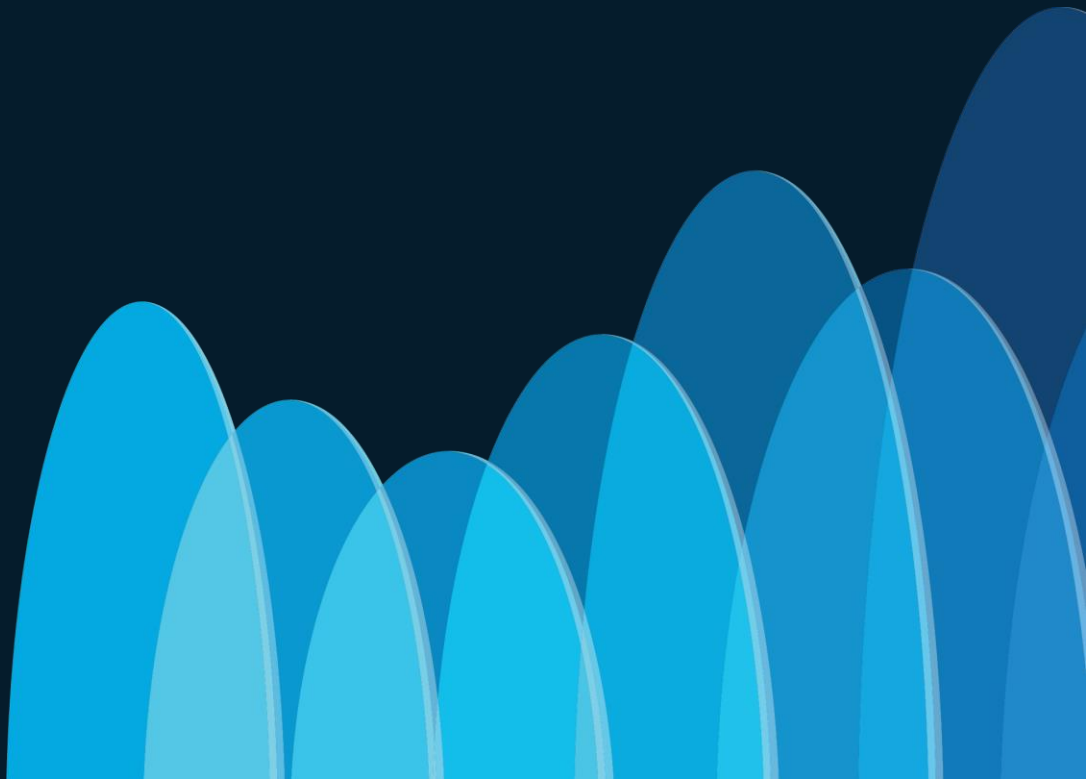


# A high-level view

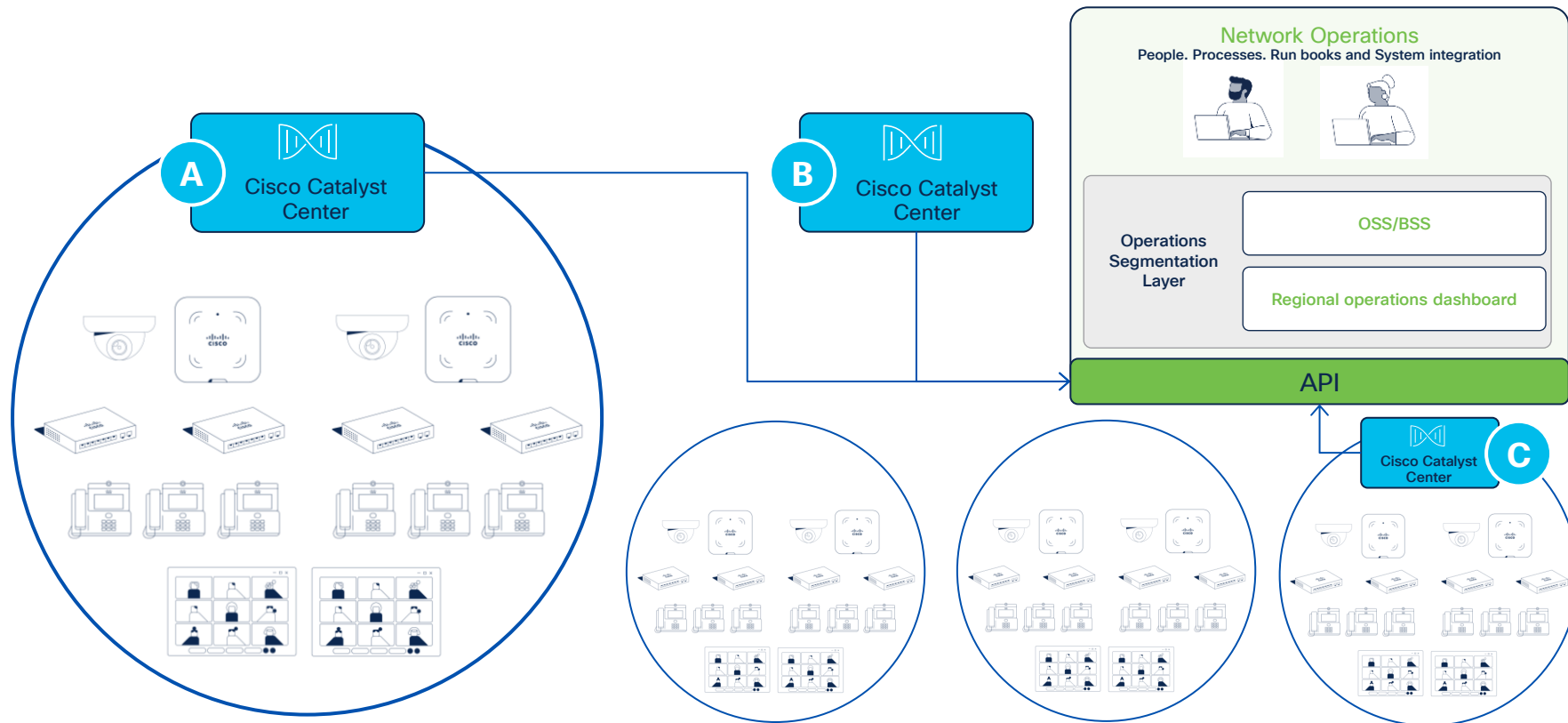
## Catalyst Center headless deployment example



# Catalyst Center APIs



# What a headless scenario looks like



# Cisco Catalyst Center API platform

## Event and Notifications API

Provides a notification handler when specific events are triggered, such as Network Assurance and Automation (SWIM) events.

Enables external systems to take actions in response to an event: execute a software upgrade action in response to an out of compliance notification of network devices

Notifications may also be triggered by internal Catalyst Center events. For example, Assurance events can be customised for IT Service Management incidents.

## Intent API

The Intent API is a REST API that exposes specific capabilities of the Cisco Catalyst Center platform.

Provides policy-based abstraction of business intent, allowing focus on an outcome rather than struggling with individual mechanisms steps.

The RESTful Cisco Catalyst Center Intent API uses HTTPS verbs (GET, POST, PUT, and DELETE) with JSON structures to discover and control the network.

## Integration API

Provides mechanisms for integrating Network Assurance end-to-end workflows and data with third-party IT Service Management (ITSM) solutions.

ITSM integration minimises handoffs, reduces duplication of issues, and optimizes processes such as approval- and pre-approval chains,

Cisco Catalyst Center also Integrates with Reporting and Analytics capabilities for capacity planning, asset management, compliance control, and auditing.

# Cisco Catalyst Center

## Platform overview

**Cisco DNA Center** Platform · Overview

Welcome to the Cisco DNA Center Platform. Programmatically access your network through Intent APIs, integrate with your preferred IT systems to create end-to-end solutions and add support for multi-vendor devices.

### Bundles

Bundles are easy to use feature sets for consuming Intent APIs, integrations, events and notifications. View all the available bundles, enable relevant bundles and customize the configuration preferences to consume events as per your application(s) or IT system(s) needs.

### Developer Toolkit

Discover APIs to manage your network, configure integration flows and access network data to analyze, export and visualize complex reports.

### Runtime Dashboard

Get Insights into API usage, view events published to IT systems such as number of API calls, response time(s), events published, bundles activated etc.

### Configurations

View and set global or bundle specific settings to manage your integration configurations and modify event specific settings.

### Notifications

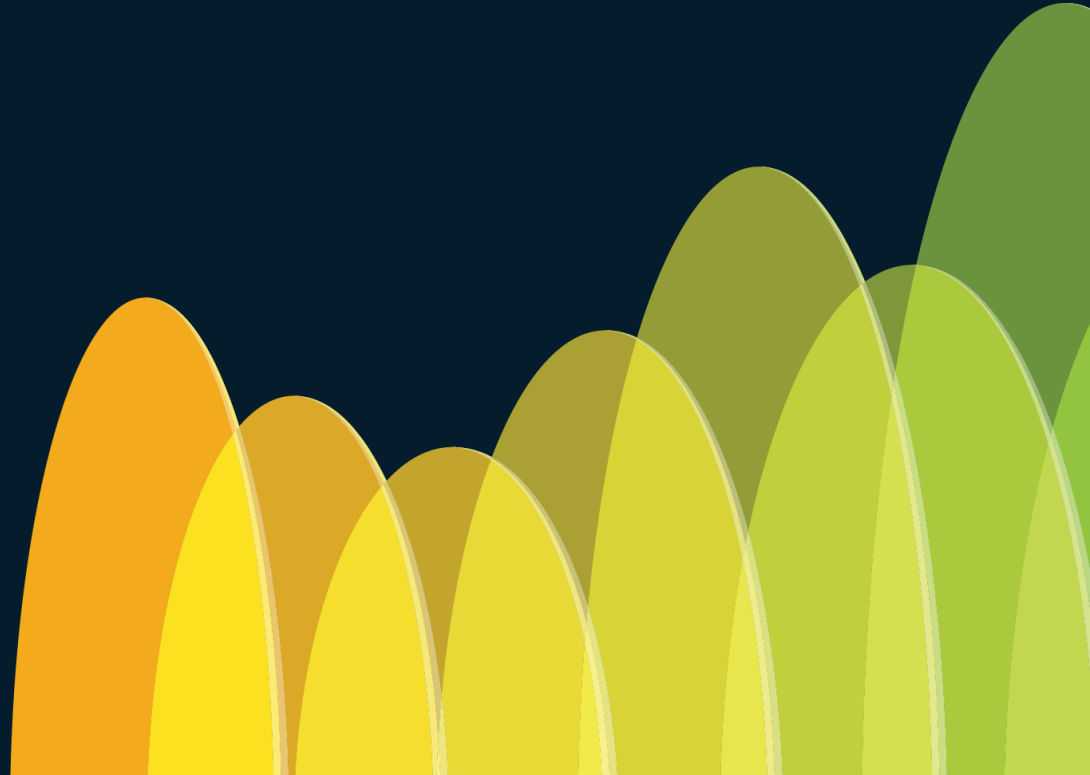
Find

**BUNDLE UPDATE**  
The Cisco DNA Center REST API bundle is enabled.  
Sep 20 2022, 08:47 am  
[View Details](#) | [Dismiss](#)

**BUNDLE UPDATE**  
Disabled the Cisco DNA Center REST API bundle.  
Sep 20 2022, 08:47 am  
[View Details](#) | [Dismiss](#)

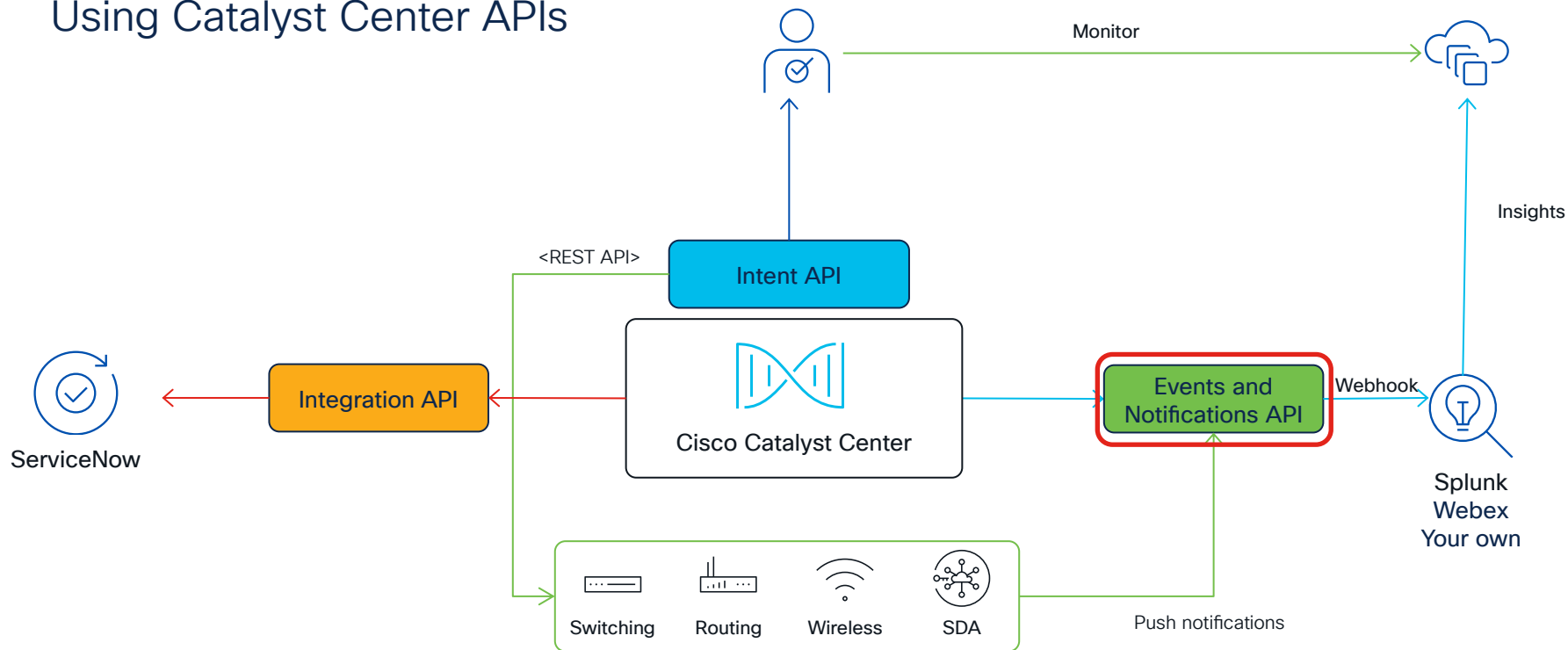
**BUNDLE UPDATE**  
The Cisco DNA Center REST API bundle is enabled.  
Aug 19 2022, 07:37 pm  
[View Details](#) | [Dismiss](#)

# Implementation Guidelines

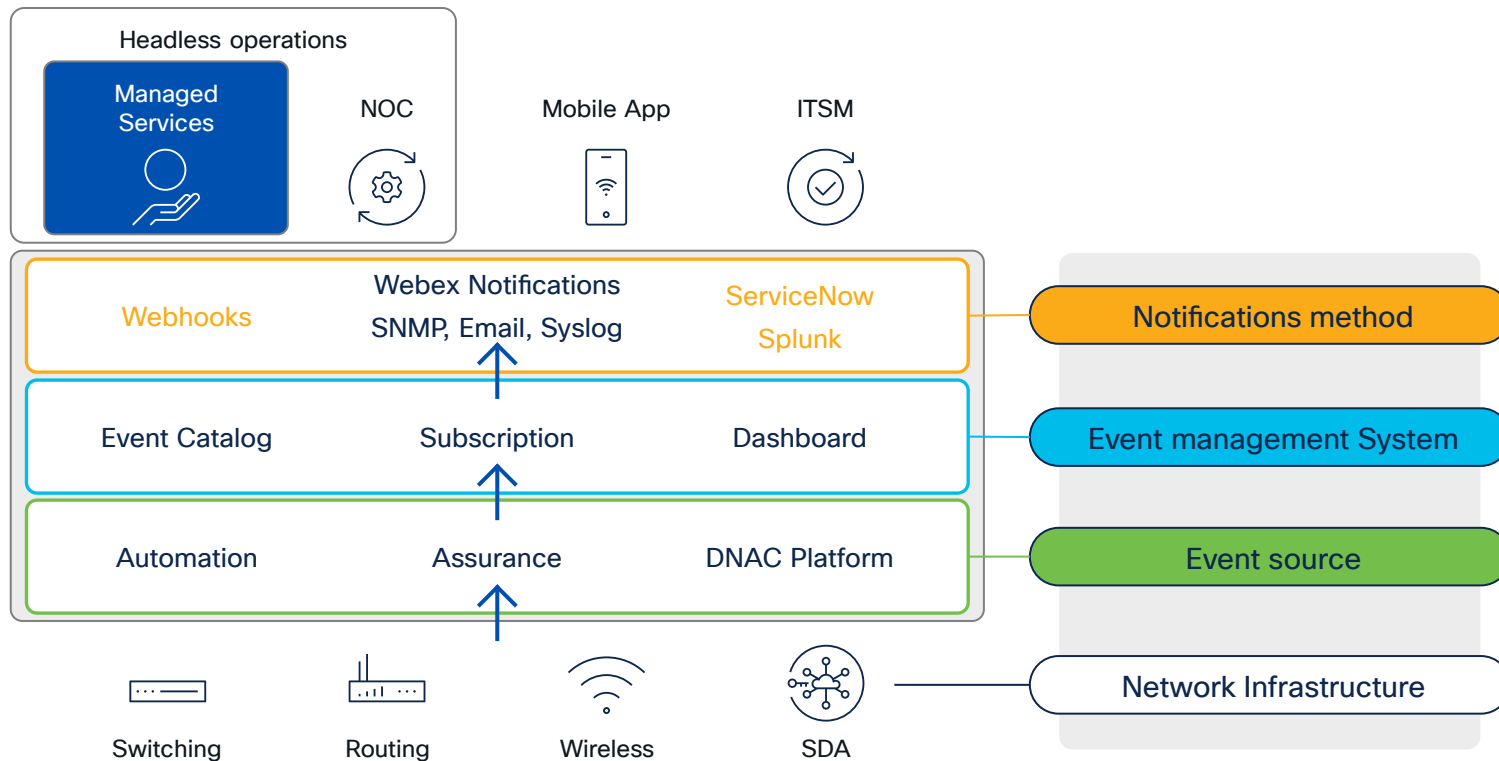


# Headless operations

## Using Catalyst Center APIs



# Catalyst Center notifications framework



# Better using event notifications

## Event subscription



Monitor



NETWORK-NON-  
FABRIC\_WIRELESS-1-150

WLC Unreachable

Device is unreachable

NETWORK

ALERT

1

Not  
Subscribed

Subscribe to event



Cisco Catalyst Center

Issue created



Switching



Routing



Wireless

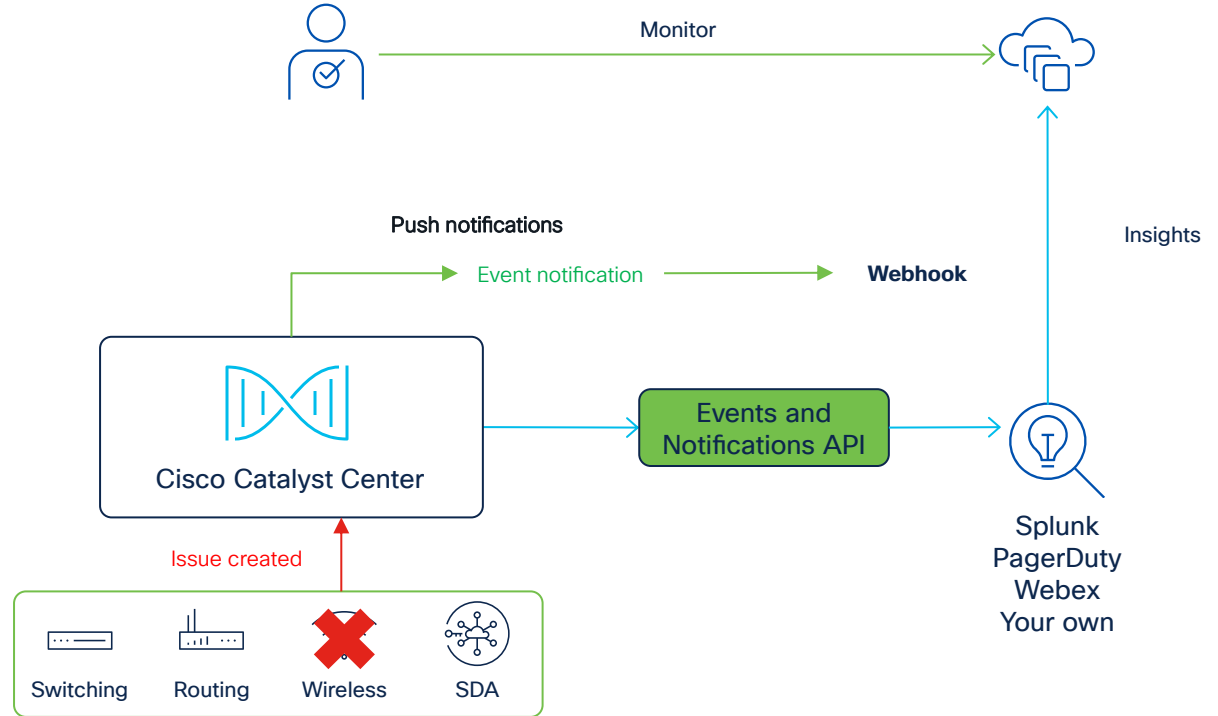


SDA

# Better using event notifications

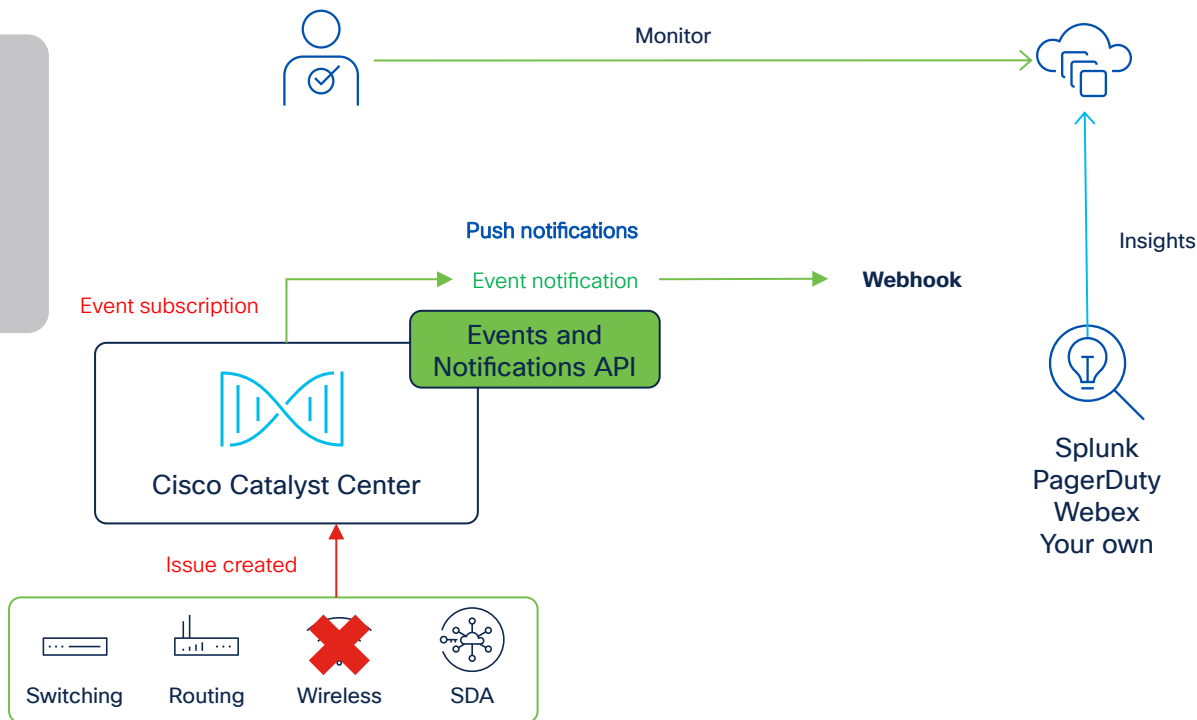
## Event subscription

Once an issue is triggered by the assurance engine and if the event is subscribed, an event is sent out to the remote webhook location



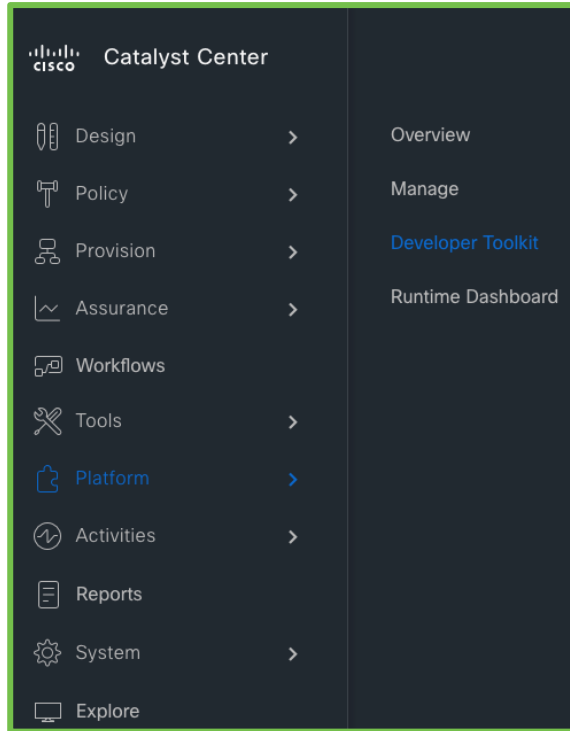
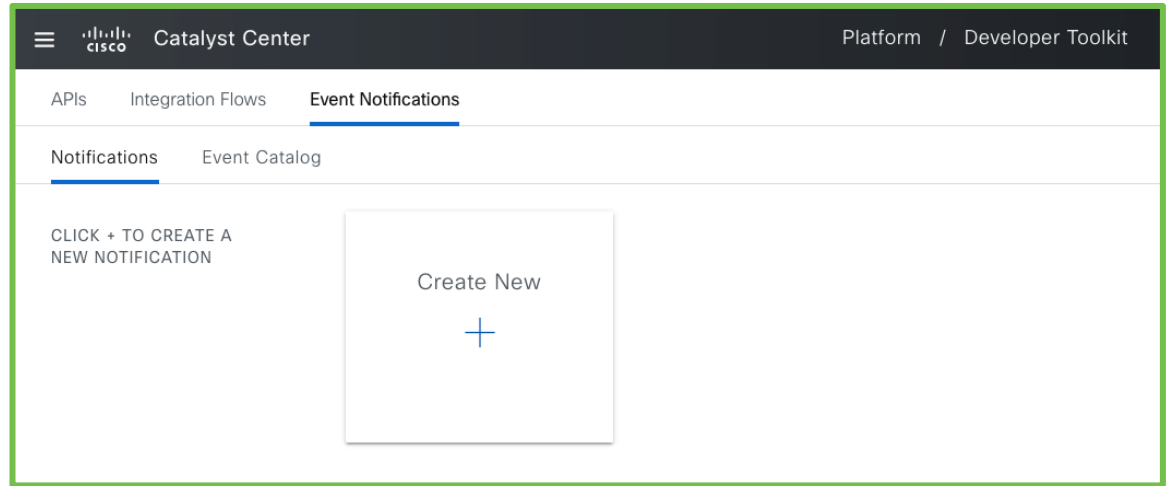
# Event notifications flow

1. Setup a new webhook destination
2. Subscribe event
3. Test notification



# Catalyst Center event notifications

## Creating a new event



# Setting up a destination

## Webhook

The screenshot shows the Cisco DNA Center interface. On the left is a dark sidebar with a menu. The 'System' menu item is highlighted with a blue gear icon. To the right of the sidebar is a light-colored main area. A green rectangular overlay highlights the 'External Services' section, which contains links for 'Umbrella', 'Authentication Tokens', 'vManage', 'Cisco AI Analytics', 'Destinations' (highlighted with a blue box), and 'Machine Reasoning Engine'. Another green rectangular overlay highlights the 'Destinations' configuration page. This page has a breadcrumb 'Settings / External Services' and a title 'Destinations'. Below the title is a subtitle 'Configure various types of destinations to deliver event notifications from Cisco DNA Center Platform'. There is a horizontal tab bar with five tabs: 'Webhook' (selected with a blue underline), 'Email', 'Syslog', 'SNMP', and 'ITSM'. Below the tabs is a section titled 'Configure the REST Endpoint to receive Audit logs and Events from Cisco DNA Center Platform'.

**Cisco DNA Center**

- Design > System 360
- Policy > Software U
- Provision > Settings
- Assurance > Data Platfo
- Workflows > System He
- Tools > Users & Ro
- Platform > Backup & F
- Activities > Disaster Re
- Reports
- System** >
- Explore

**External Services**

- Umbrella**  
Register Umbrella with your Cisco DNA Center
- Authentication Tokens**  
Manages connection between
- vManage**  
Connect Cisco DNA Center
- Cisco AI Analytics**  
Set up the Cisco artificial in
- Destinations**  
Configure various types of e
- Machine Reasoning Engine**  
Update the Machine Reason

**Settings / External Services**

## Destinations

Configure various types of destinations to deliver event notifications from Cisco DNA Center Platform

**Webhook**   Email   Syslog   SNMP   ITSM

Configure the REST Endpoint to receive Audit logs and Events from Cisco DNA Center Platform

# Webhook provisioning

The screenshot shows the 'Add Webhook' configuration form. It includes fields for Name (Webhook Test), Description (Webhook Test), and URL (webhook.cisco.com). The Trust Certificate section has 'Yes' selected. The Method is set to POST. The Authentication section has 'Basic' selected. The Headers section shows 'Authorization' with the value 'Basic YWRtaW46Q2lzY29MaXZlMTAwJQ=='. There are 'Add' and 'Save' buttons at the bottom.

Trust Certificate: **YES**

Method: **POST**

Authentication: **Basic**

Headers:

'Authorization': 'Basic Encoded64(Username+Password)'

```
import base64

# Define valid credentials
VALID_USERNAME = 'admin'
VALID_PASSWORD = 'CiscoLive100%'

# Encode the credentials
credentials = f"{VALID_USERNAME}:{VALID_PASSWORD}"
encoded_credentials = base64.b64encode(credentials.encode()).decode()

print(encoded_credentials)
print(f'Basic {encoded_credentials}')
```

```
YWRtaW46Q2lzY29MaXZlMTAwJQ==
Basic YWRtaW46Q2lzY29MaXZlMTAwJQ==
```

| Name         | Description  | URL                       | Method |
|--------------|--------------|---------------------------|--------|
| Webhook Test | Webhook Test | https://webhook.cisco.com | POST   |

# Subscribe to events

The image shows a multi-step process for subscribing to events in Cisco DNA Center. It includes a sidebar menu, a list of events, and a detailed 'Subscribe' dialog box.

**Cisco DNA Center Sidebar:**

- Design
- Policy
- Provision
- Assurance
- Workflows
- Tools
- Platform
- Activities
- Reports
- System
- Explore

**Events List:**

| Event ID                          | Name                               |
|-----------------------------------|------------------------------------|
| NETWORK-DEVICES-2-106             | AP disconnected from WLC           |
| NETWORK-DEVICES-2-152             | WLC Reboot Crash                   |
| NETWORK-DEVICES-2-153             | WLC Power Supply Failure           |
| NETWORK-DEVICES-3-154             | WLC Memory High Utilization        |
| NETWORK-DEVICES-3-155             | AP License Exhausted on WLC        |
| NETWORK-FABRIC_WIRELESS-1-307     | Fabric WLC to MapServer            |
| NETWORK-NETWORKS-3-352            | Wireless clients failed to connect |
| NETWORK-NON-FABRIC_WIRELESS-1-150 | WLC Unreachable                    |
| NETWORK-NON-FABRIC_WIRELESS-3-156 | WLC Monitor                        |

**Subscribe Dialog (WLC Unreachable):**

**1 Event selected**

Name\*: WLC unreachable

Subscription Type: REST

Select an existing instance. Or Click [here](#) to create a new instance.

Subscription Endpoint: Webhook Test

TAGS: ASSURANCE wlc\_unreachable

MODEL SCHEMA: Details REST Schema

```
1 {
2   "Type": "$eventSource",
3   "Assurance Issue Priority": "$priority$",
4   "Assurance Issue Details": "This network device $mDeviceName$ is unreachable from Cisco DNA Center. The device role is $fabricOrDev",
5   "Device": "$eventUniqueId$",
6   "Assurance Issue Category": "$category$",
7   "Assurance Issue Name": "Network Device $managementIpAddress$ Is Unreachable From Controller",
8   "Assurance Issue Status": "$status$"
9 }
```

Cancel Subscribe

# Catalyst Center webhooks notifications workflow

Notification

Event Name: WLC Unreachable      Event Id: NETWORK-NON-FABRIC\_WIRELESS-1-150

|           |          |          |
|-----------|----------|----------|
| Namespace | Context  | Source   |
| ASSURANCE | EXTERNAL | EXTERNAL |

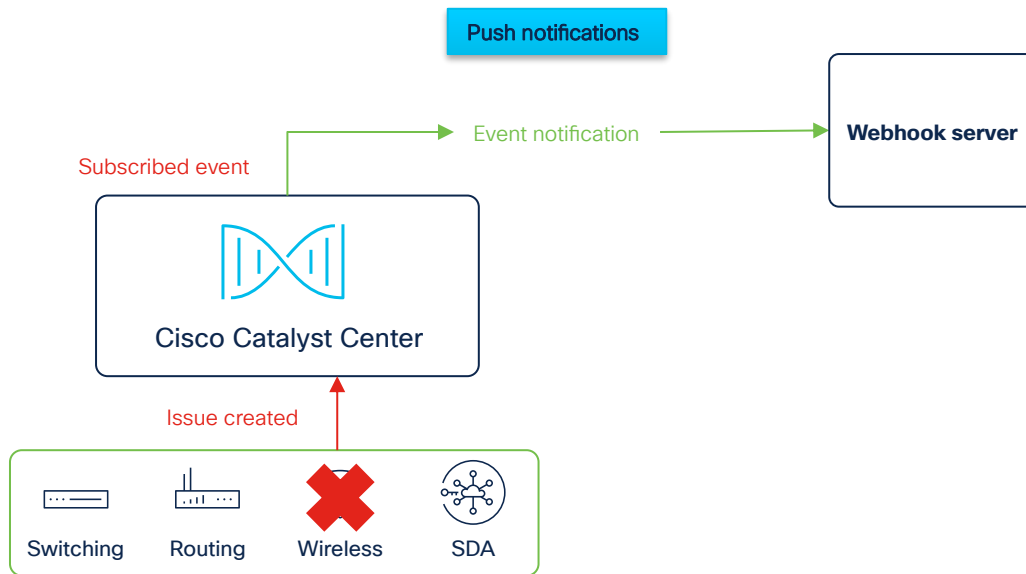
|         |          |          |
|---------|----------|----------|
| Type    | Category | Severity |
| NETWORK | ALERT    | 1        |

|              |            |
|--------------|------------|
| Domain       | Sub Domain |
| Connectivity |            |

Details

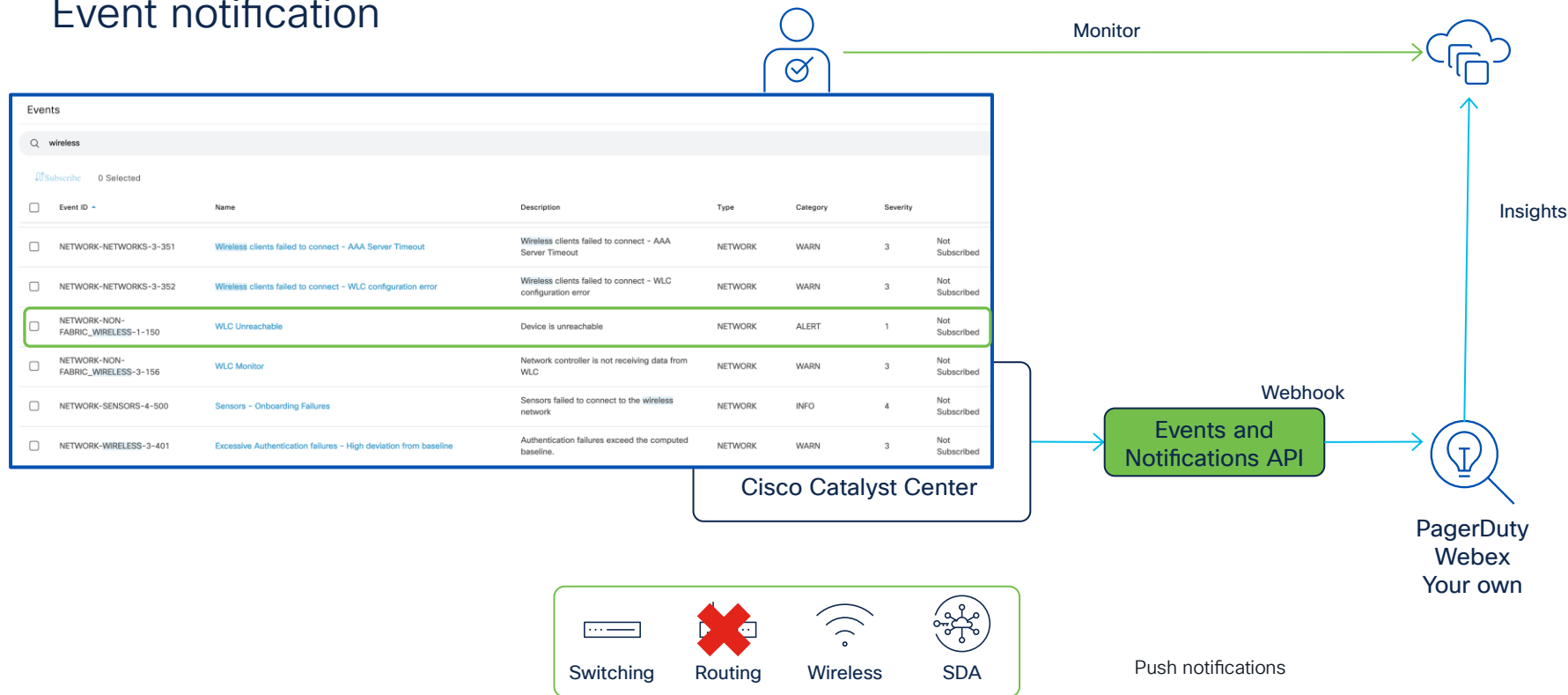
```
1 {
2   "Type": "SeventSource$",
3   "Assurance Issue Priority": "$priority$",
4   "Assurance Issue Details": "This network device $nwDeviceName$ is unreachable from Cisco DNA Center. Th
5   "Device": "SeventUniqueId$",
6   "Assurance Issue Category": "$category$",
7   "Assurance Issue Name": "Network Device $managementIpAddress$ Is Unreachable From Controller",
8   "Assurance Issue Status": "$status$"
9 }
```

Cancel Publish



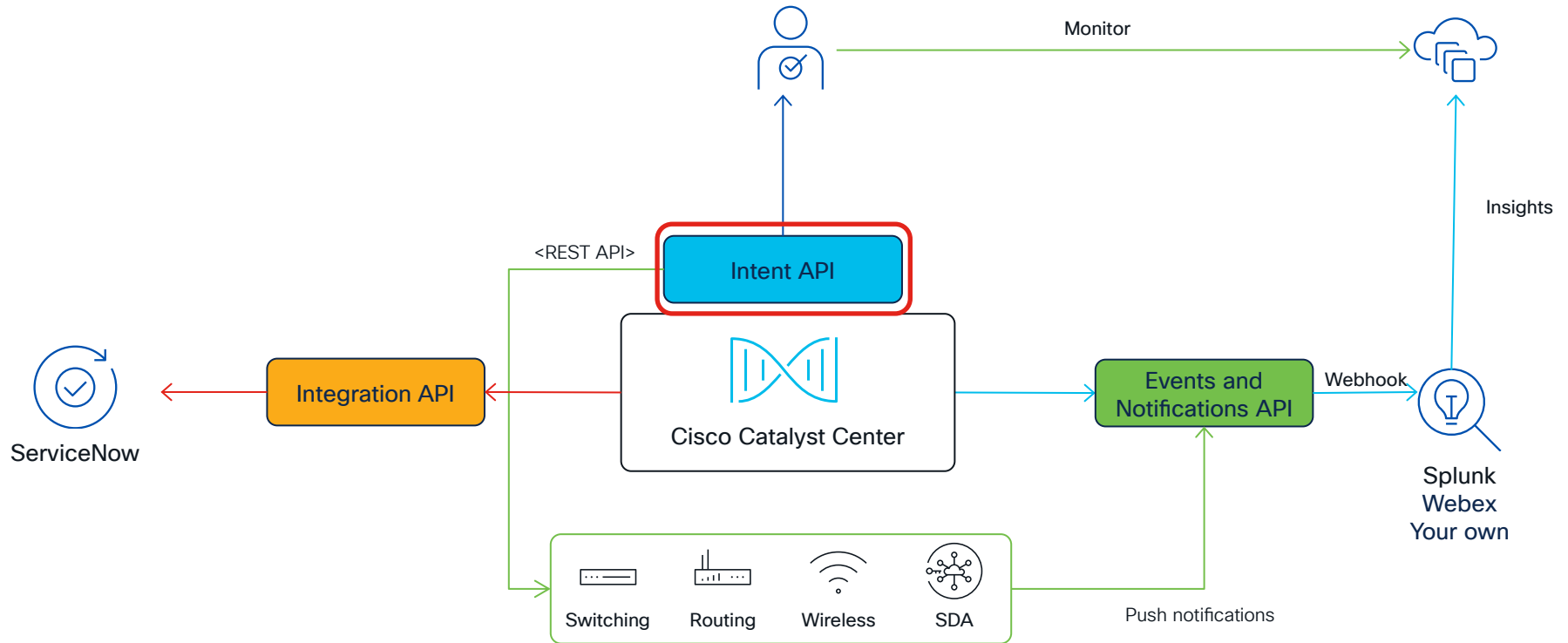
# Managing your campus at scale

## Event notification



# Headless operations

## Using Catalyst Center APIs



# Cisco Catalyst Center

## Intent APIs usage and documentation

The screenshot displays the Cisco Catalyst Center Developer Toolkit interface. The top navigation bar includes the Cisco logo, the text 'Catalyst Center', and the path 'Platform / Developer Toolkit'. On the right side of the top bar are icons for favorites, search, refresh, help, notifications, and a user profile labeled 'admin'.

Below the top bar, there are three tabs: 'APIs' (selected), 'Integration Flows', and 'Event Notifications'. A left-hand sidebar contains a search bar and a list of categories: 'Authentication' (selected), 'Cisco DNA Center System', 'Health and Performance', 'Licenses', 'Platform', 'User and Roles', 'Connectivity', 'Fabric Wireless', 'SDA', and 'Wireless'. The 'Authentication' category is expanded, showing a list of APIs.

The main content area is titled 'Authentication' and contains the following text:

Authentication APIs provide an authorized token for accessing any REST API.

**\*Prerequisite\*:** Add the request header 'x-auth-token' with the generated authorized token to get a successful API response.

Below the text is a table listing the Authentication APIs:

| Method | Name                                 | Description                                                                                                                                                 | URL              | Actions |
|--------|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------|
| POST   | <a href="#">Authentication API</a>   | API to obtain an access token, which remains valid for 1 hour. The token obtained using this API is required to be set as value to the X-Auth-Token HTTP... | /auth/token      | ... ▾   |
| POST   | <a href="#">importCertificate</a>    | This method is used to upload a certificate                                                                                                                 | /certificate     | ... ▾   |
| POST   | <a href="#">importCertificateP12</a> | This method is used to upload a PKCS#12 file                                                                                                                | /certificate-p12 | ... ▾   |

# Cisco Catalyst Center

## Intent APIs usage and documentation

### Authentication API

POST

https://rtp-4-dnac-02.lab.ciscomsx.com/dna/system/api/v1/auth/token

REST action and server end point

API to obtain an access token, which remains valid for 1 hour. The token obtained using this API is required to be set as value to the X-Auth-Token HTTP Header for all API calls to Cisco DNA Center.

[Cisco DevNet API Guide](#)

Parameters

Responses

Code Preview

Options for coding

#### Request Header Parameters

| Name          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | DataType | Required | Default Value    |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----------|------------------|
| Content-Type  | Request body content type                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | string   | Yes      | application/json |
| Authorization | API supports both Basic auth and AES key encryption as Authorization token in header. AES key encryption is optional and can be enabled under DNAC System configuration. For Basic Auth: Authorization header is Base64 encoded string of "username:password", For example Authorization header will contain "Basic YWRtaW46TWFnbnGV2MTIz", where YWRtaW46TWFnbnGV2MTIz is the Base64 encoded string. For AES key encryption, Authorization header is Base64 encoded string of AES key. For example Authorization header will contain "CSCO-AES-256 credentials=2k/wGz48lp3ma9sM+2xiyQ==", where "2k/wGz48lp3ma9sM+2xiyQ==" is base64 encoded string of 256 bits AES key encrypted "username:password". | string   | Yes      |                  |

# Cisco Catalyst Center

## Supported coding languages

The screenshot displays the Cisco Catalyst Center interface with three overlapping windows. The top window shows the 'Code Preview' tab with a search bar and a list of supported languages: Shell, Node - HTTP, Node - Unirest, Node - Request, Python, and Ruby. The middle window shows a Python code snippet for an HTTP POST request. The bottom window shows a JavaScript code snippet for an XMLHttpRequest.

**Supported Coding Languages:**

- Shell
- Node
- Python
- Ruby
- Javascript
- jQuery
- PHP
- Go
- Ansible

**Python Code Snippet:**

```
1 //  
2 /  
3 i  
4  
5 co  
6  
7 he  
8  
9  
10  
11  
12 co  
13  
14 re  
15 da  
16  
17 print(data.decode("utf-8"))
```

**JavaScript Code Snippet:**

```
1 //  
2 //  
3 const  
4  
5 const x  
6 xhr.wit  
7  
8 xhr.addEventListener("readystatechange", function () {  
9   if (this.readyState === this.DONE) {  
10     console.log(this.responseText);  
11   }  
12 });  
13  
14 xhr.open("POST", "https://rtp-4-dnac-02.lab.ciscoms.com/dna/system/api/v1/auth/token");  
15 xhr.setRequestHeader("Content-Type", "application/json");  
16 xhr.setRequestHeader("Authorization", "<Authorization>");  
17  
18 xhr.send(data);
```

# Authentication

POST

Authentication API

API to obtain an access token. The token obtained using this API is required to be set as value to the X-Auth-Token HTTP Header for all API calls to Cisco DNA...

/auth/token

```
def get_token(dnac_ip,uname,passwd):  
    token = requests.post(  
        'https://' + str(dnac_ip)+ '/dna/  
        auth=HTTPBasicAuth(  
            username=uname,  
            password=passwd  
        ),  
        headers={'content-type': 'applica  
        verify=False,  
    )  
    data = token.json()  
    return data['Token']
```

# DNAC code

# Define variables

dnac\_ip = <Your DNAC DNS/IP>

username = <Your DNAC username>

password = <Your DNAC password>

token = get\_token(dnac\_ip, username, password)

print(token)

# General instructions to call a CatC API

## Python example

```
# Headers
headers = {'content-type': 'application/json', 'x-auth-token': token}

sites = get_sites(BASE_URL, SITE_URL, headers)
```

```
# Authentication
BASE_URL = 'https://dnac-79.infra.ciscomsx.com'
AUTH_URL = '/dna/system/api/v1/auth/token'

# URLs
SITE_URL = '/dna/intent/api/v1/site'
SITE_COUNT_URL = '/dna/intent/api/v1/site/count'
MEMBERSHIP_SITE_URL = '/dna/intent/api/v1/membership/{site_id}'
SITE_HEALTH_URL = '/dna/intent/api/v1/site-health'
ISSUES = url = '/dna/intent/api/v1/issues'
```

```
# Get list of sites
def get_sites(BASE_URL, URL, headers):
    response = requests.get(BASE_URL + URL,
                             headers=headers, verify=False)
    return response.json()['response']
```

# Monitoring your network

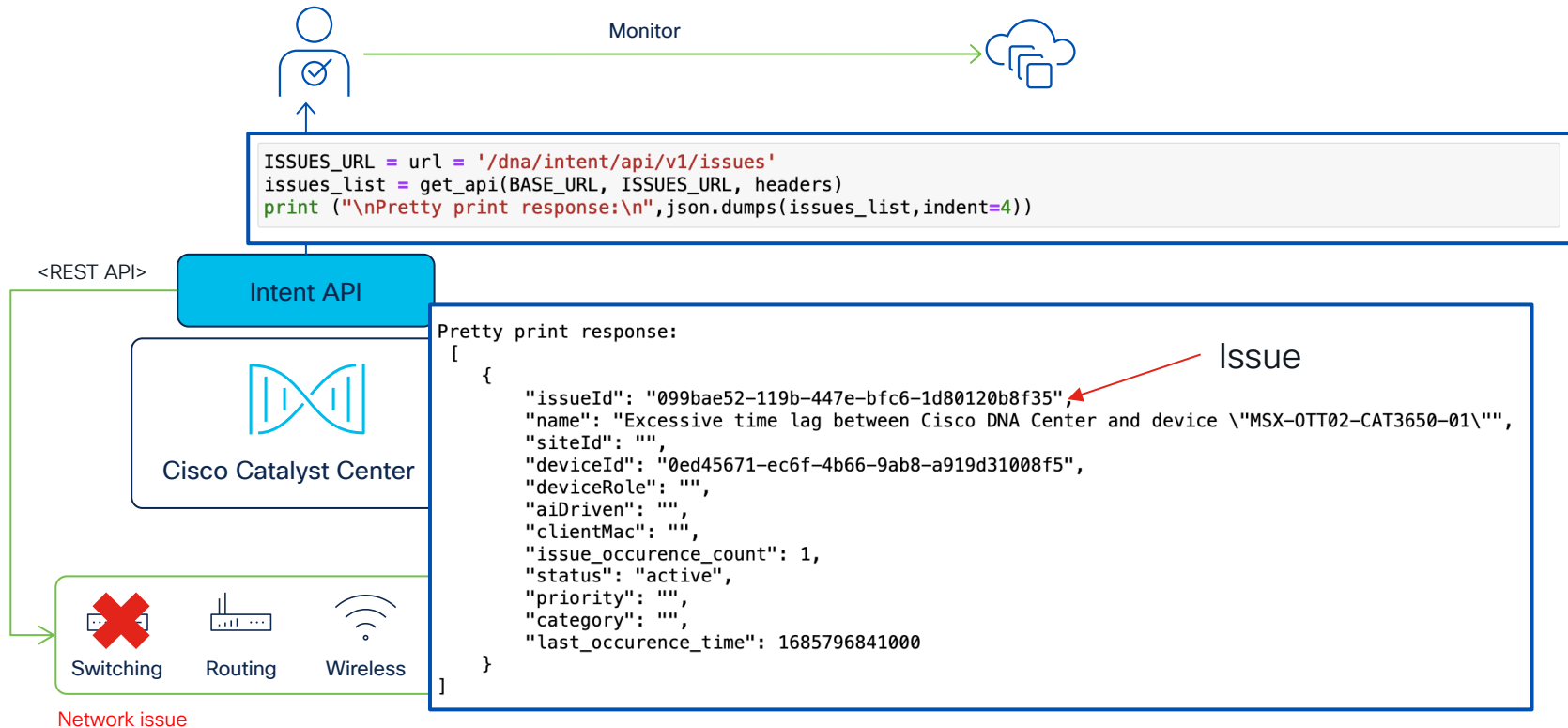
## Health and Performance

```
# Get System Health
def get_system_health (BASE_URL, URL, headers):
    response = requests.get(BASE_URL + URL,
                            headers=headers, verify=False)
    print(response)
    return response.json()
```

|     |                                                     |                                                                                                             |                                         |
|-----|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| GET | System Health Count API <sup>Intent</sup>           | This API gives the count of the latest system events                                                        | /diagnostics/system/health/count        |
| GET | System Health API <sup>Intent</sup>                 | This API retrieves the latest system events                                                                 | /diagnostics/system/health              |
| GET | System Performance Historical API <sup>Intent</sup> | This API retrieves the historical performance indicators . The data can be retrieved for the last 3 months. | /diagnostics/system/performance/history |
| GET | System Performance API <sup>Intent</sup>            | This API gives the aggregated performance indicators. The data can be retrieved for the last 3 months.      | /diagnostics/system/performance         |

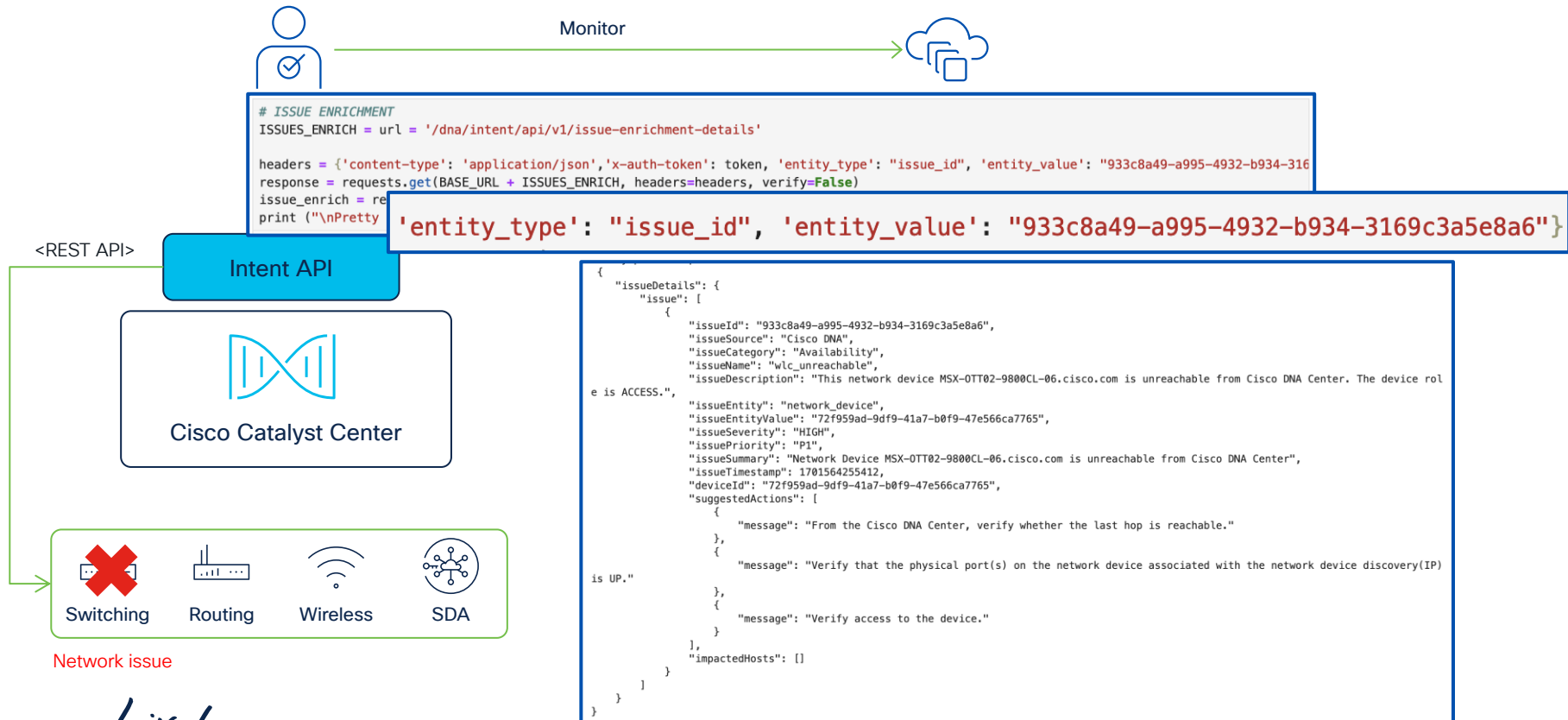
# Managing your campus at scale

## Get issue using Intent API



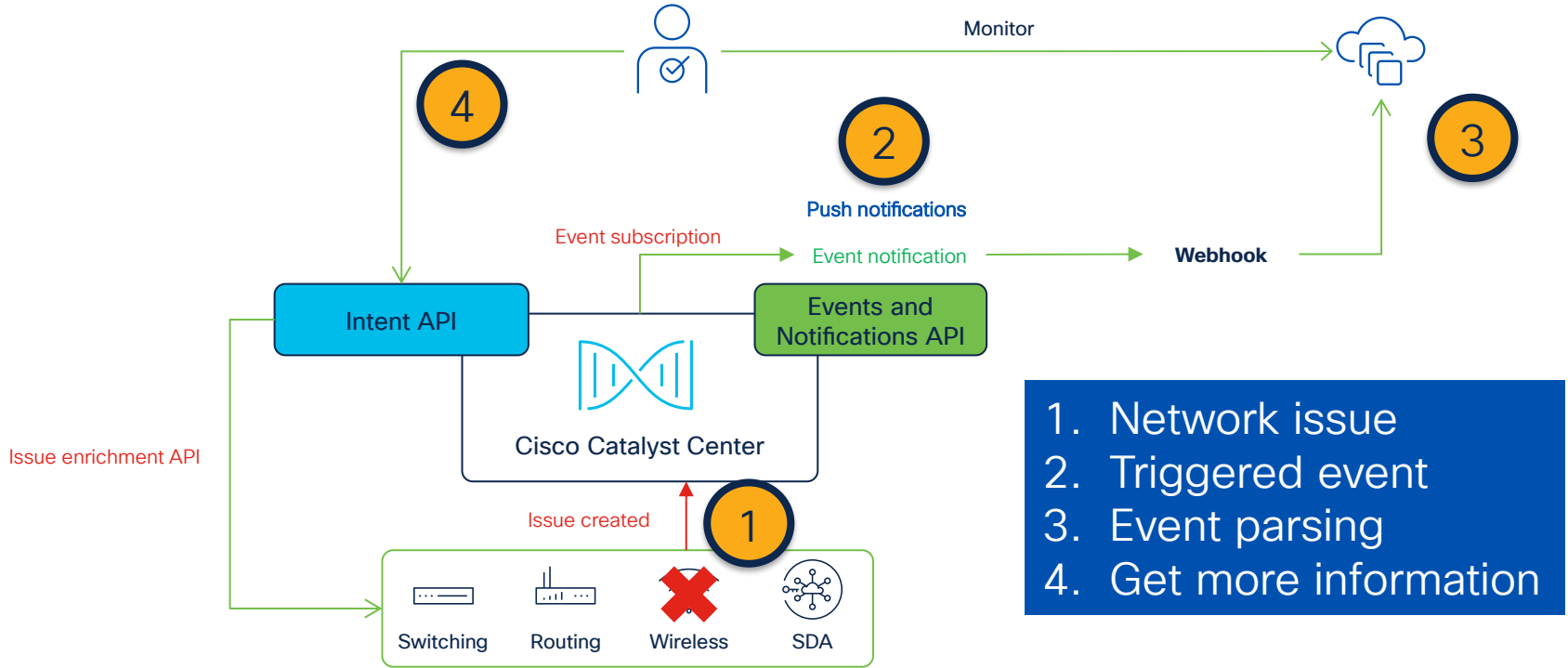
# Managing your campus at scale

## Issue enrichment using Intent API



# Better using event notifications...

... and enrich with intent API



# Simple flask app running locally

Received POST request with data: {

```
"version": "1.0.0",
"instanceId": "8b3d20dc-f161-4f4d-97fc-56cb6d1dec8a",
"eventId": "NETWORK-NON-FABRIC_WIRELESS-1-150",
"namespace": "ASSURANCE",
"name": "WLC Unreachable",
"description": "Device is unreachable",
"type": "NETWORK",
"category": "ALERT",
"domain": "Connectivity",
"subDomain": "Non-Fabric Wireless",
"severity": 1,
"source": "EXTERNAL",
"timestamp": 1701690738552,
"details": {
  "Type": "",
  "Assurance Issue Priority": "",
  "Assurance Issue Details": "This network device is unreachable from Cisco DNA Center. The device role is .",
  "Device": "",
  "Assurance Issue Category": "",
  "Assurance Issue Name": "Network Device Is Unreachable From Controller",
  "Assurance Issue Status": ""
},
"ciscoDnaEventLink": "https://&lt;DNAC_IP_ADDRESS&gt;/dna/assurance/issueDetails?issueId=",
"note": "To programmatically get more info see here - https://<ip-address>/dna/platform/app/consumer-portal/developer-toolkit/apis?apiId=8684-39bb-4e89-a6e4",
"context": "EXTERNAL",
"userId": null,
"i18n": null,
"eventHierarchy": null,
"message": null,
"messageParams": null,
"parentInstanceId": null,
"network": null,
"dnaIP": null
}
```

127.0.0.1 -- [04/Dec/2023 22:52:22] "POST /dna/events/ HTTP/1.1" 200 -

## Notification

**Event Name**  
WLC Unreachable

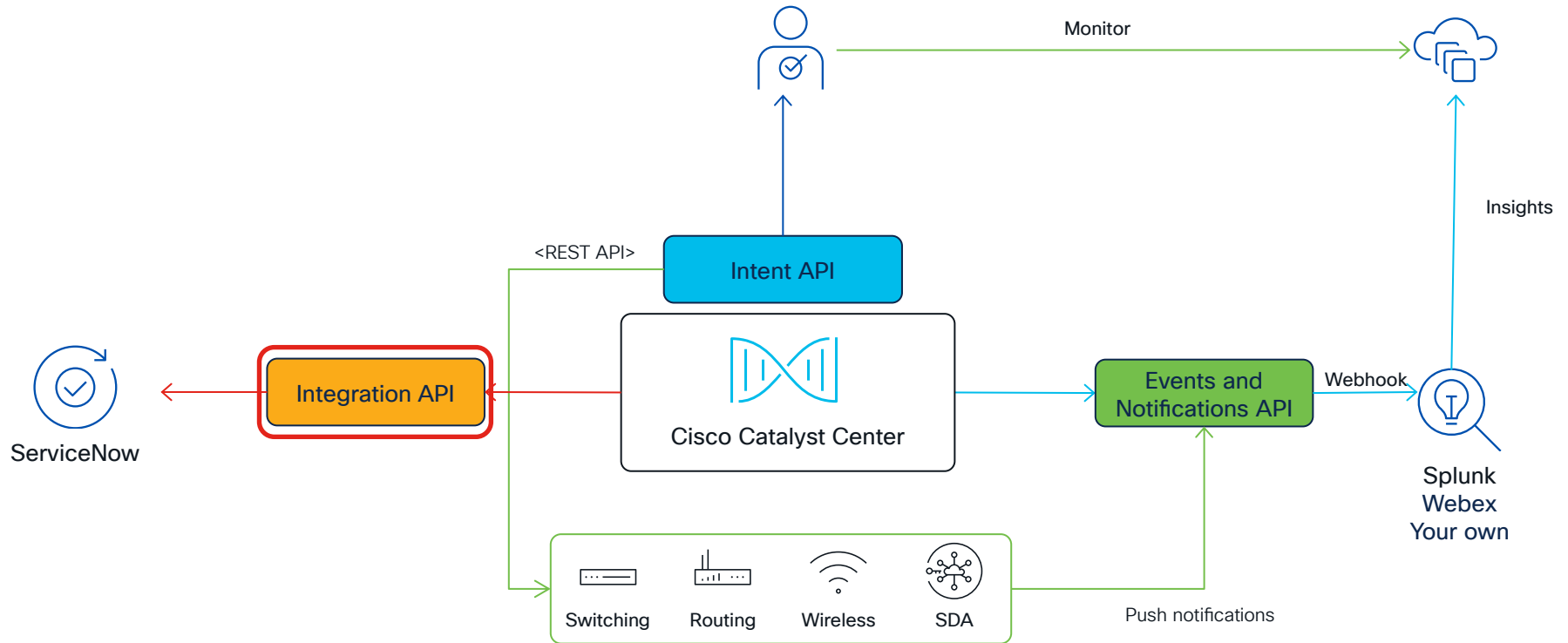
**Event Id**  
NETWORK-NON-FABRIC\_WIRELESS-1-150

### Result

| Subscription Name ^ | Connector Type | Status    | Message |
|---------------------|----------------|-----------|---------|
| WLC unreachable     | REST           | ● SUCCESS | OK      |

# Headless operations

## Using Catalyst Center APIs



# Bundles

## ServiceNow



Bundles

Configurations

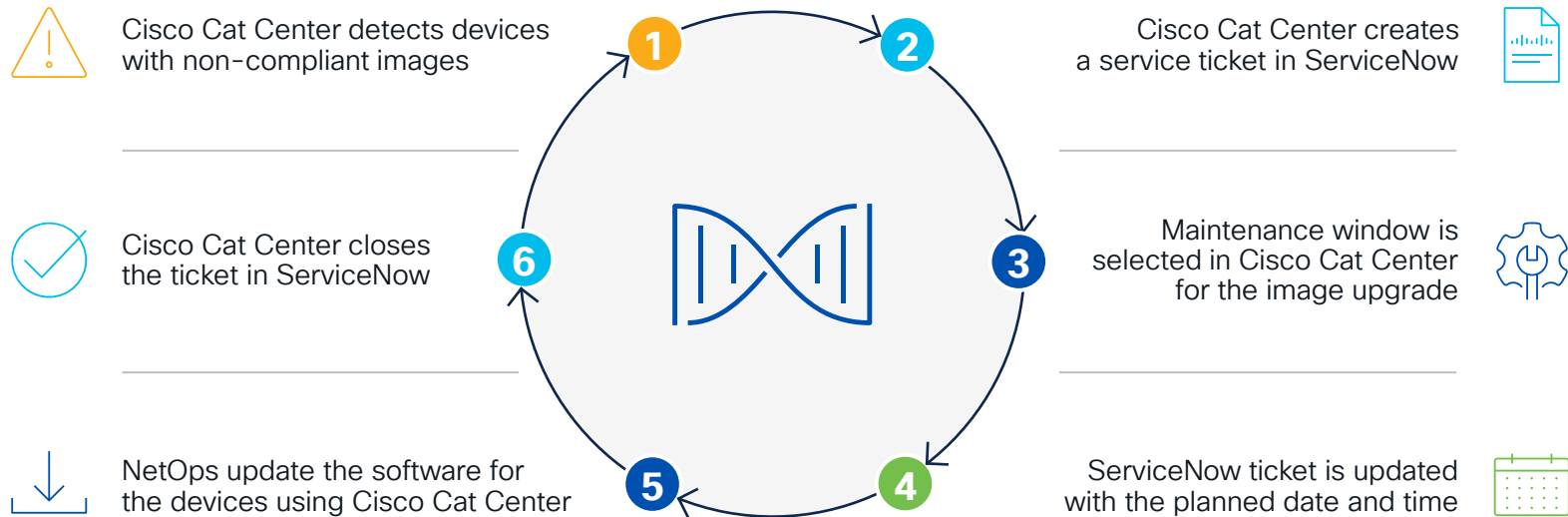
Bundles

Filter

Find

| Bundle                                                                                                                                                                                                                | Status  | Description                                                                                                                                                                                                                                                                                                                                |                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <div><div>B</div><div><div>Basic ITSM (ServiceNow) CMDB synchronization</div><div>Cisco Systems, Inc.</div><div>v1.7.0   Cisco DNA Center 1.2.5 +</div><div>Version Dated Jan 22, 2021</div></div></div>              | ENABLED | You can schedule a synchronization or trigger an update between Cisco DNA Center's device inventory and your ITSM(ServiceNow) configuration management database(CMDB). These activities integrate Cisco DNA Center's processes into the IT System Management processes of incident, change or problem management. Note: If your network... | <div>Configure</div> |
| <div><div>C</div><div><div>Cisco DNA Center Automation events for ITSM (ServiceNow)</div><div>Cisco Systems, Inc.</div><div>v1.7.1   Cisco DNA Center 1.2.5 +</div><div>Version Dated May 25, 2021</div></div></div>  | ENABLED | This bundle can be used to: 1. Monitor and publish events that require software image updates for compliance, security or any other operational triggers, to an ITSM(ServiceNow) system. 2. Monitor and publish events that require Fabric Role updates for security or other operational triggers, to an ITSM(ServiceNow) system. ...     | <div>Configure</div> |
| <div><div>C</div><div><div>Cisco DNA Center REST API</div><div>Cisco Systems, Inc.</div><div>v1.7.12   Cisco DNA Center 1.2.5 +</div><div>Version Dated Jan 13, 2022</div></div></div>                                | ACTIVE  | This bundle contains the REST API supported by Cisco DNA Center. These REST APIs provide a rich set of capabilities, including the ability to discover network devices, query network health and provision network devices.                                                                                                                |                      |
| <div><div>D</div><div><div>Disaster Recovery API</div><div>Cisco Systems, Inc.</div><div>v1.0.0   Cisco DNA Center 2.2.2.0+</div><div>Version Dated Mar 8, 2021</div></div></div>                                     | ACTIVE  | This bundle contains the REST APIs supported by Disaster Recovery. These REST APIs provide support to monitor the Disaster Recovery system. Please enable this bundle after installation of Disaster Recovery package.                                                                                                                     |                      |
| <div><div>E</div><div><div>Endpoint Attribute Retrieval with ITSM (ServiceNow)</div><div>Cisco Systems, Inc.</div><div>v1.3.0   Cisco DNA Center 2.1.1 +</div><div>Version Dated Dec 8, 2020</div></div></div>        | ENABLED | You can schedule a synchronization or trigger an update between the Endpoint Inventory and your ITSM (ServiceNow) configuration management database (CMDB). Endpoint attribute information from ServiceNow can be used to help profile endpoints on your network. ServiceNow appears in the endpoint profiling workspace as an...          | <div>Configure</div> |
| <div><div>N</div><div><div>Network Issue Monitor and Enrichment for ITSM (ServiceNow)</div><div>Cisco Systems, Inc.</div><div>v1.7.0   Cisco DNA Center 1.2.5 +</div><div>Version Dated Dec 1, 2020</div></div></div> | ENABLED | You can use this bundle to monitor your network for assurance and maintenance issues, and then publish the event details about these issues to an ITSM(ServiceNow) system. This bundle also contains APIs that extract rich network context data. Please note that, if your network devices have not yet been synchronized between...      | <div>Configure</div> |

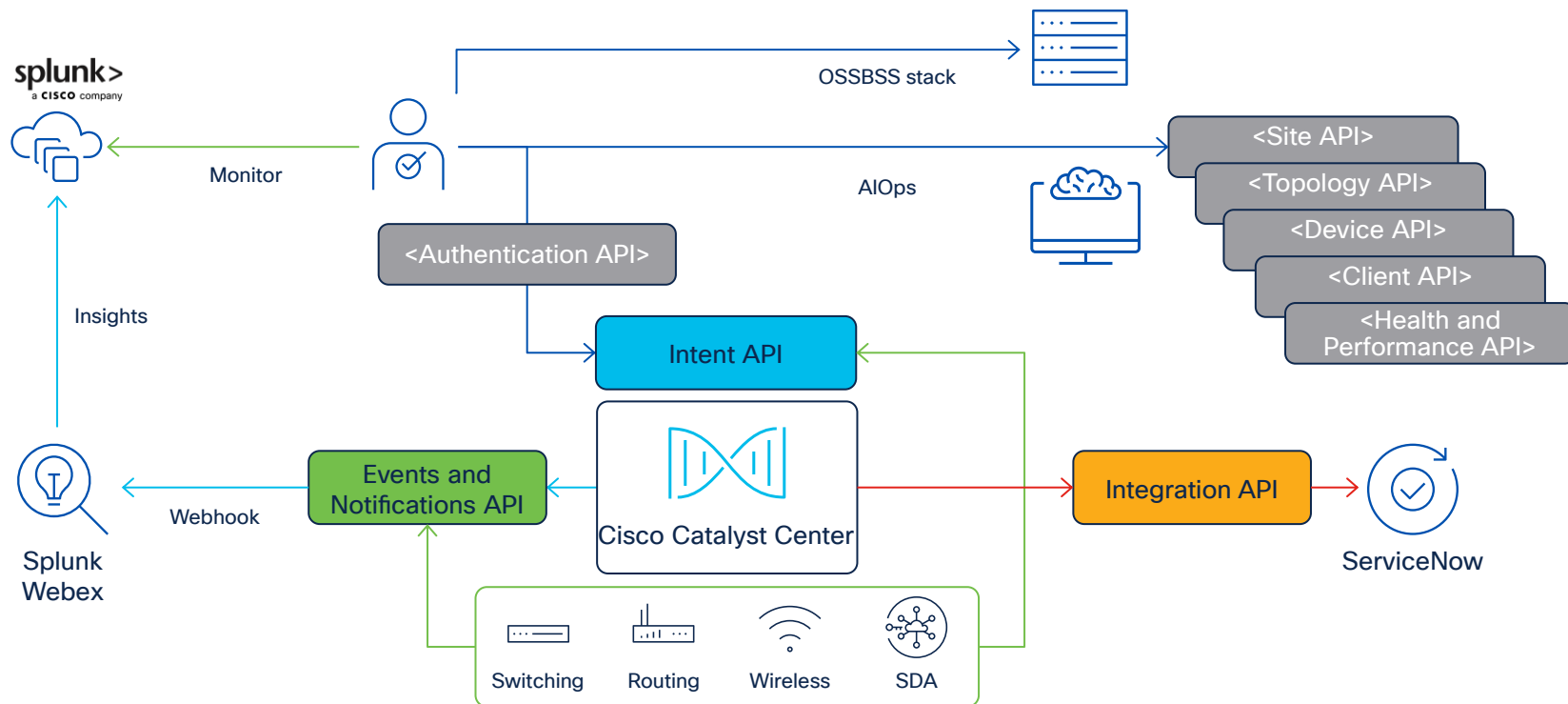
# Closed-loop ServiceNow integration



<https://developer.cisco.com/dnacenter/integrationapis/>

# Catalyst Center headless operations

## Recap



# Best Practices



# Webex Bot as webhook destination

The image is a collage of four screenshots from the Cisco DNA Center and Webex Developer console, illustrating the process of setting up a Webex Bot as a webhook destination.

**Top Left Screenshot: New Bot**

This screenshot shows the 'New Bot' form in the Webex Developer console. The bot name is 'Cisco DNA Center Event Notification Bot1'. The bot username is '@webex.bot'. The bot icon is a yellow circle with a white 'B'. The description is 'Cisco DNA Center BOT to be used for Event Notifications using Webex admin APIs through the use of an authentication token. The BOT will post Event Notifications in your designated Webex Teams Room.' The 'Add Bot' button is highlighted.

**Top Right Screenshot: Step 3 - WEBEX Settings**

This screenshot shows the 'Step 3 - WEBEX Settings' page. The 'Service Configuration' section is active. The 'Instance Name' is 'Webex\_notify'. The 'Webex URL' is 'https://webexapis.com/v1/messages'. The 'Webex Room ID' is highlighted.

**Bottom Left Screenshot: Step 2 - Select Channels**

This screenshot shows the 'Step 2 - Select Channels' page. The 'WEBEX' channel is selected, and the 'Add Bot' button is highlighted.

**Bottom Right Screenshot: Cisco DNA Center Notification**

This screenshot shows a notification from the Webex Bot. The notification is titled 'Cisco DNA Center Notification' and contains the following details:

- Source DNA Center IP: 198.18.129.100
- Severity: 1
- Category: ALERT
- Timestamp: 2024-07-14 13:14:00
- Issue Name: Interface GigabitEthernet1/0/2 (Interface description: --) is Down on Network Device 100.126.0.2
- Issue Description: Interface GigabitEthernet1/0/2 (Interface description: --) connecting the following two network devices is down: Local Node: FiaB.dcloud.cisco.com, Peer Node: FiaB.dcloud.cisco.com
- Issue Status: resolved

The notification also includes a button labeled 'Cisco DNA Center Issue Details'.

More information on [salesconnect](#) (access for partners)

**cisco** Live!

# Automated bulk upgrade of network devices

## Vulnerability assessment for devices managed by multiple Catalyst-Center

The objective of this use case is to streamline and provision the process of upgrading network devices managed by multiple Catalyst Centers driven by vulnerability assessments to ensure that all network devices are up-to-date with the recommended security patches and firmware versions as suggested by Catalyst Center.

1

Perform Security Advisory Retrieval

```
post_url = "https://" + ip + "/api/system/v1/auth/token"
url_sites = f"https://{ip_address}/dna/intent/api/v1/site"
url_membership = f"https://{ip_address}/dna/intent/api/v1/membership/{site_id}"
url_advisory = f"https://{ip_address}/dna/intent/api/v1/security-advisory/device/{key}/advisory"
```

2

Perform Software Image Management on the devices on network

```
url_images = f'https://{ip}/dna/intent/api/v1/image/importation'
url_distribute = f'https://{ip}/dna/intent/api/v1/image/distribution'
url_device = f'https://{ip}/dna/intent/api/v1/network-device'
url = f'https://{host}/api/v1/task/{taskid}'
url_activate = f'https://{ip}/dna/intent/api/v1/image/activation/device'
```

# Pushing customised template

Devices spread across multiple sites (topology, inventory, template)

To automate the deployment of customised configuration templates to network devices distributed across multiple sites by leveraging APIs to manage topology, inventory, and template application, thereby ensuring consistent and efficient configuration management, and reducing manual intervention.

Network Devices

Network Templates

```
post_url = "https://" + ip + "/api/system/v1/auth/token"
url_device = f'https://{ip}/dna/intent/api/v1/network-device'
url_show_template = f'https://{ip}/dna/intent/api/v1/template-programmer/template'
url_search_template = f'https://{ip}/dna/intent/api/v1/template-programmer/template'
url_template = f'https://{ip}/dna/intent/api/v1/template-programmer/template/{templateId}'
url_template_apply = f'https://{ip}/dna/intent/api/v2/template-programmer/template/deploy'
url = f'https://{host}/api/v1/task/{taskId}'
url = f'https://{host}/dna/intent/api/v1/template-programmer/template/deploy/status/{deploymentId}'
```

# Conclusions and recommendations

- Your campus network can be managed using Catalyst Center events and notifications.
- Enrich events and get to know your campus network with Intent APIs.
- Integrate with ITSM API to get closed-loop automation
- Your campus network can be completely automated and managed using Catalyst Center

# Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

---



Complete your surveys in the **Cisco Live mobile app**.

---



# Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](http://www.CiscoLive.com/on-demand)



# Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC