Cisco Security Cloud Control (SCC) Platform to simplify Day-2 Operations with APIs, Event Notification and Integration

Vijayanand C.D (VCD), Solutions Engineer

DEVNET-1375

Abstract

Cisco Security Cloud Control (SCC) is a cloud-based multi-device manager that facilitates management of security policies in highly distributed environments.

In this session, we will focus on a step-by-step process on how to integrate in-built event notification to Webex using webhooks and how to automate work-flow for Firewall management using RESTful new SCC APIs.

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.

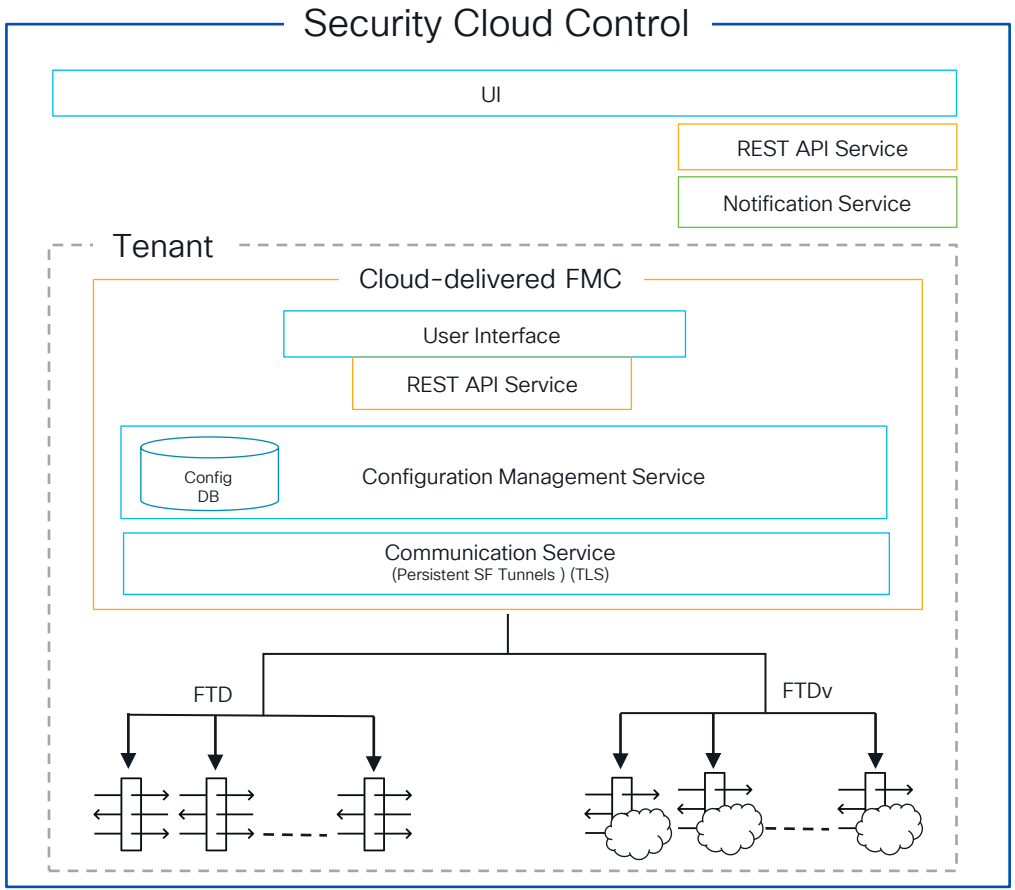
Agenda

- Introduction
- Security Cloud Control Architecture
- cdFMC API Construct
- Adding Webex Notification

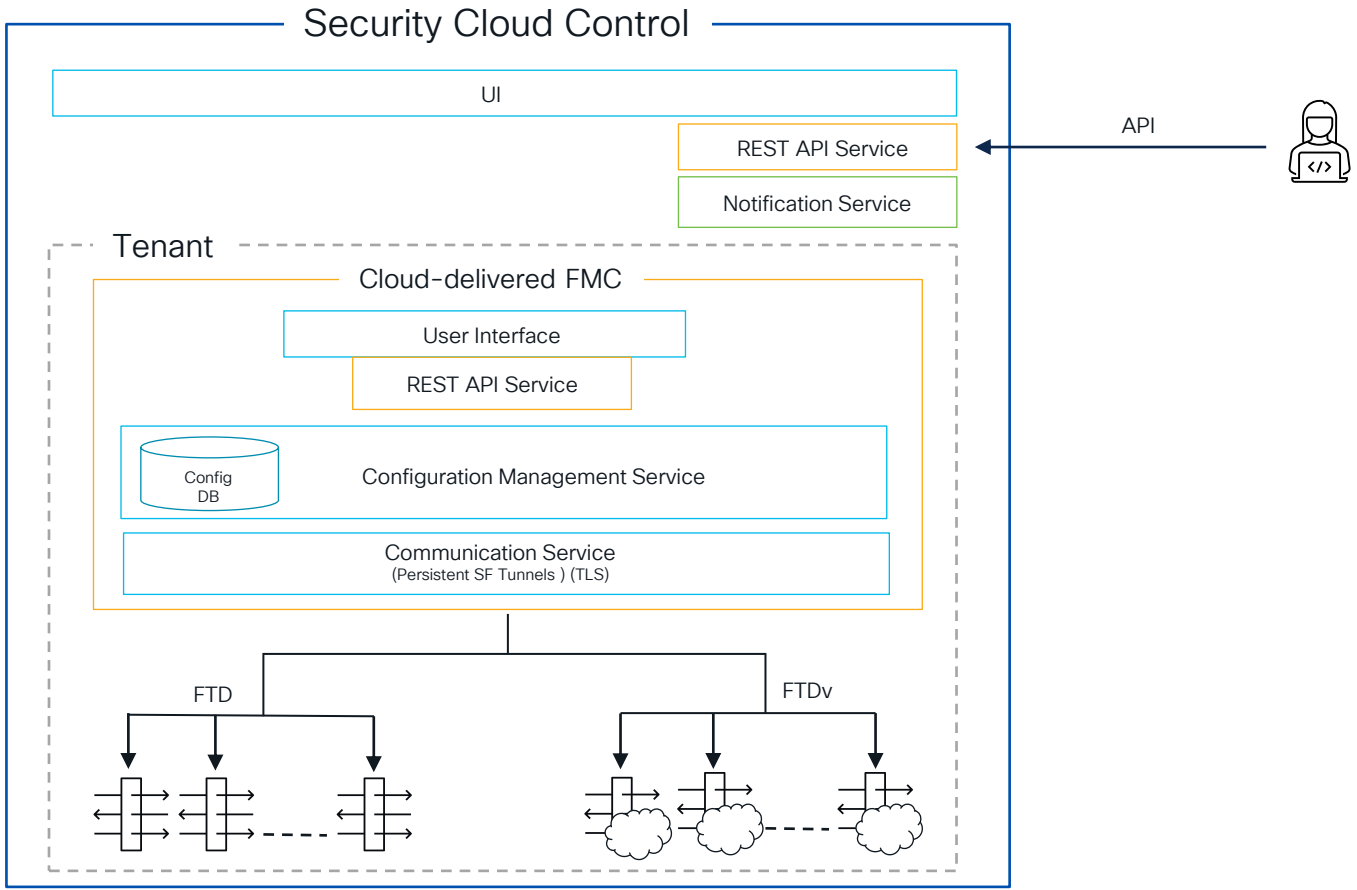
Vijayanand CD (VCD)

- A student with 21 years of industry experience
- 18 years with Cisco and 4 years with Cisco® partners
- Held various roles at Cisco:
  - Network Consulting Engineer
  - On Site Engineer
  - Focal Engineer
  - Technical Leader
  - Consulting System Engineer
  - Technical Solutions Architect
  - Solutions Engineer
- Dual CCIE # 20769 (Routing and Switching | Datacenter)
- MSc in Mobile Communication and Internet Technologies
- MSc in Software and Systems Security

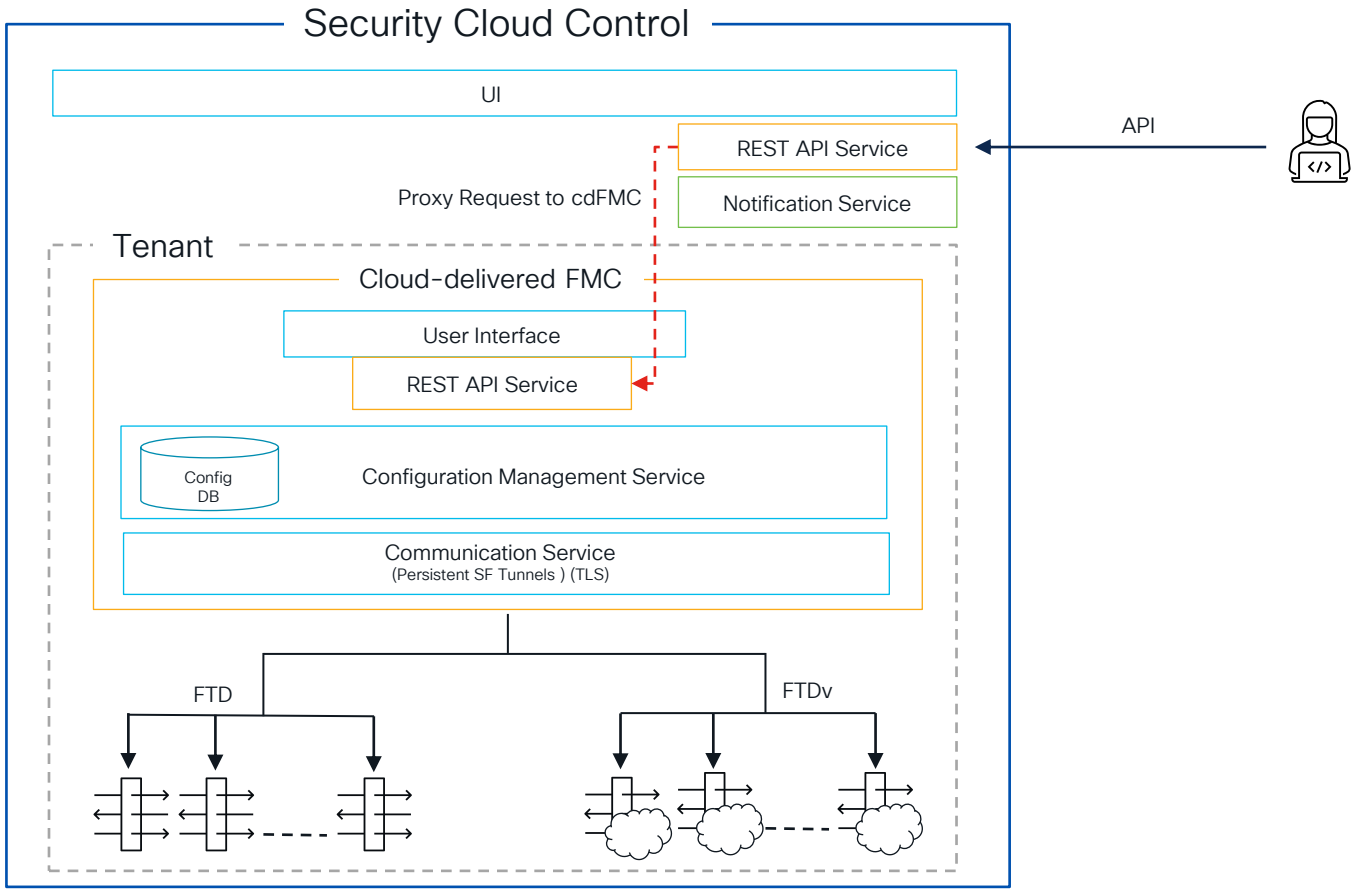
Cloud-delivered FMC Architecture



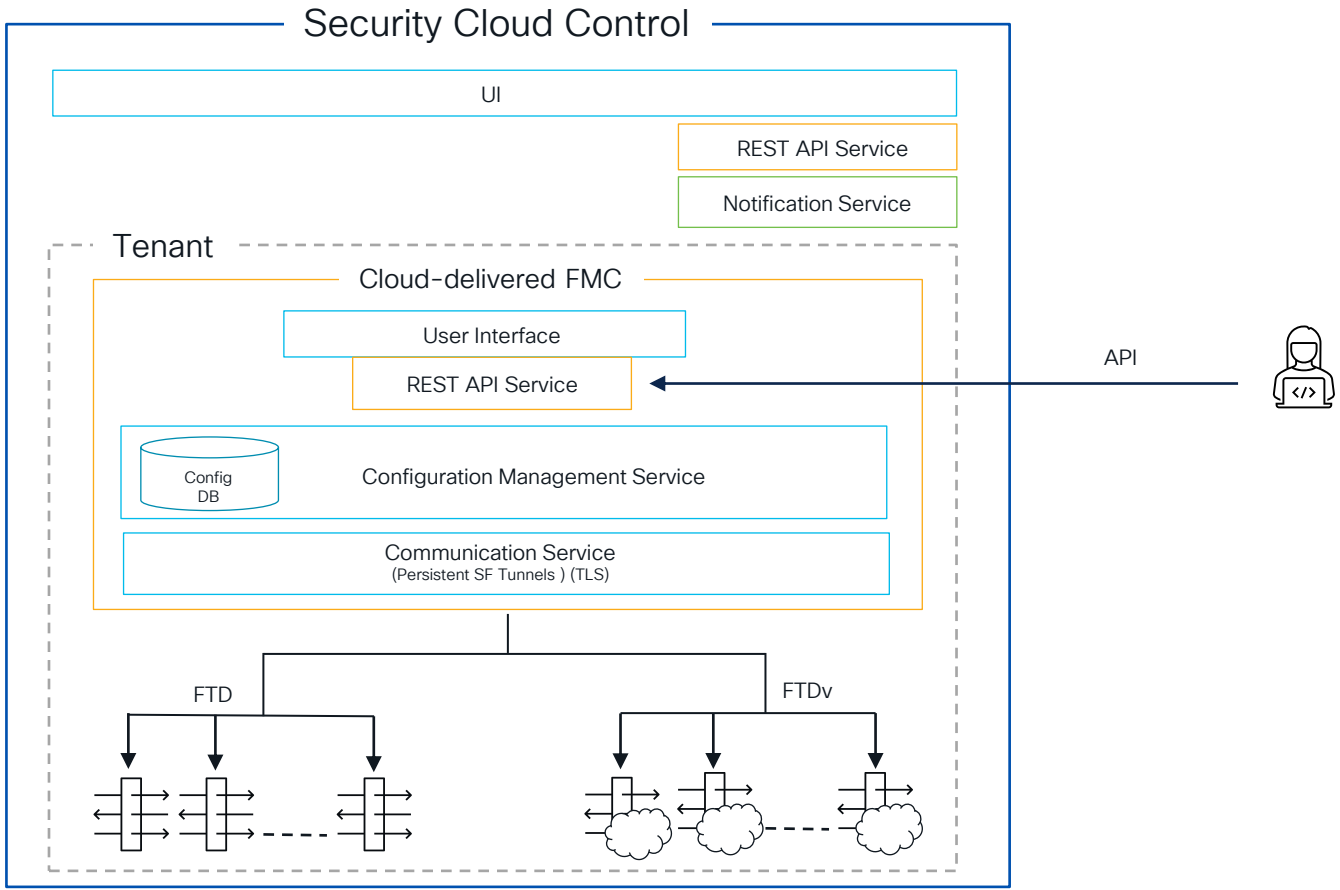
Cloud-delivered FMC Architecture



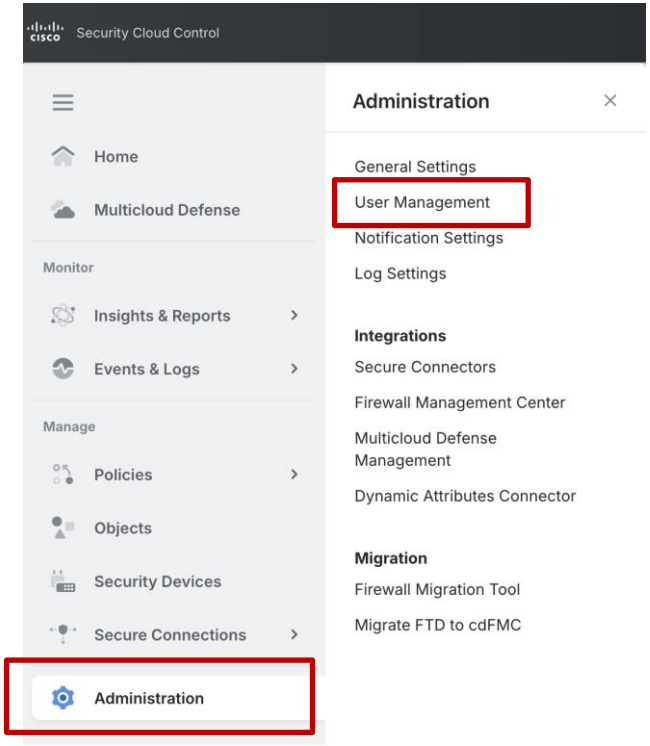
Cloud-delivered FMC Architecture



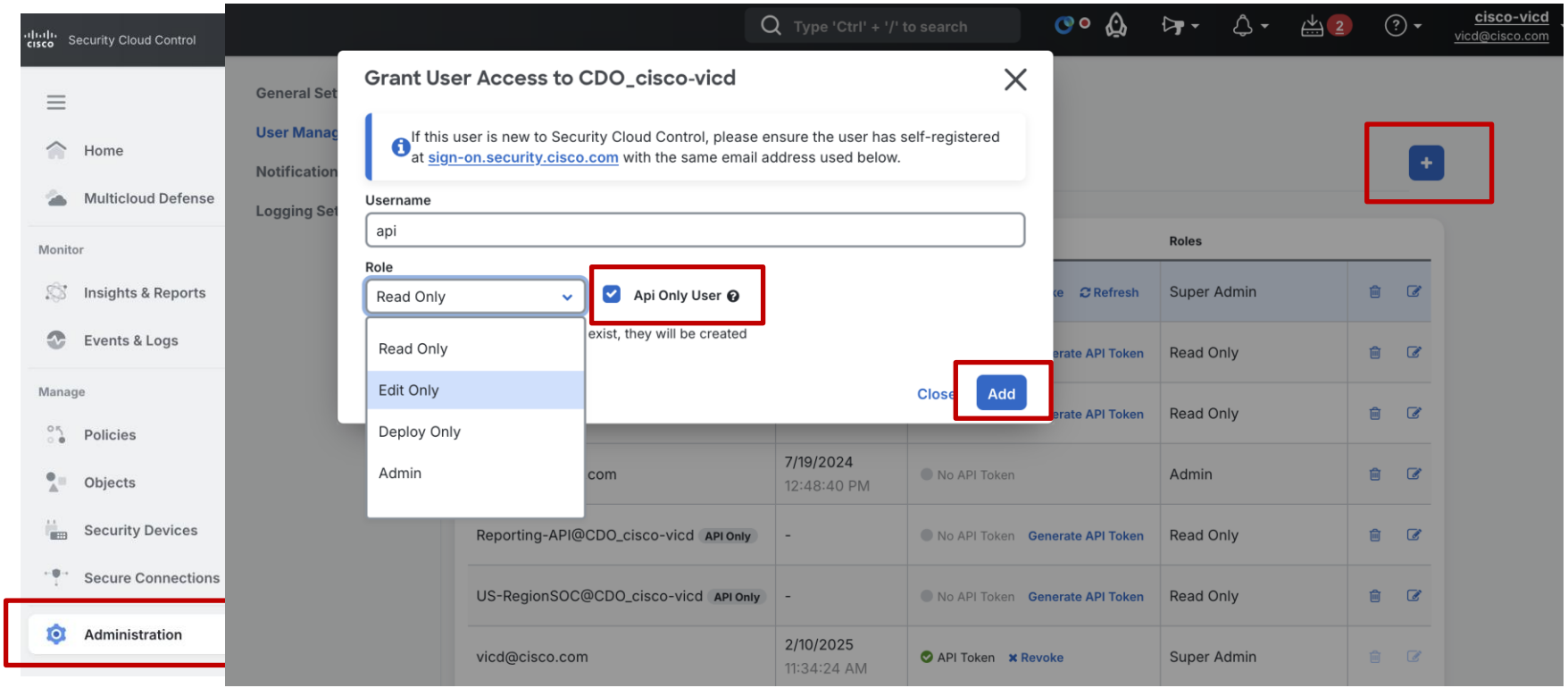
Cloud-delivered FMC Architecture



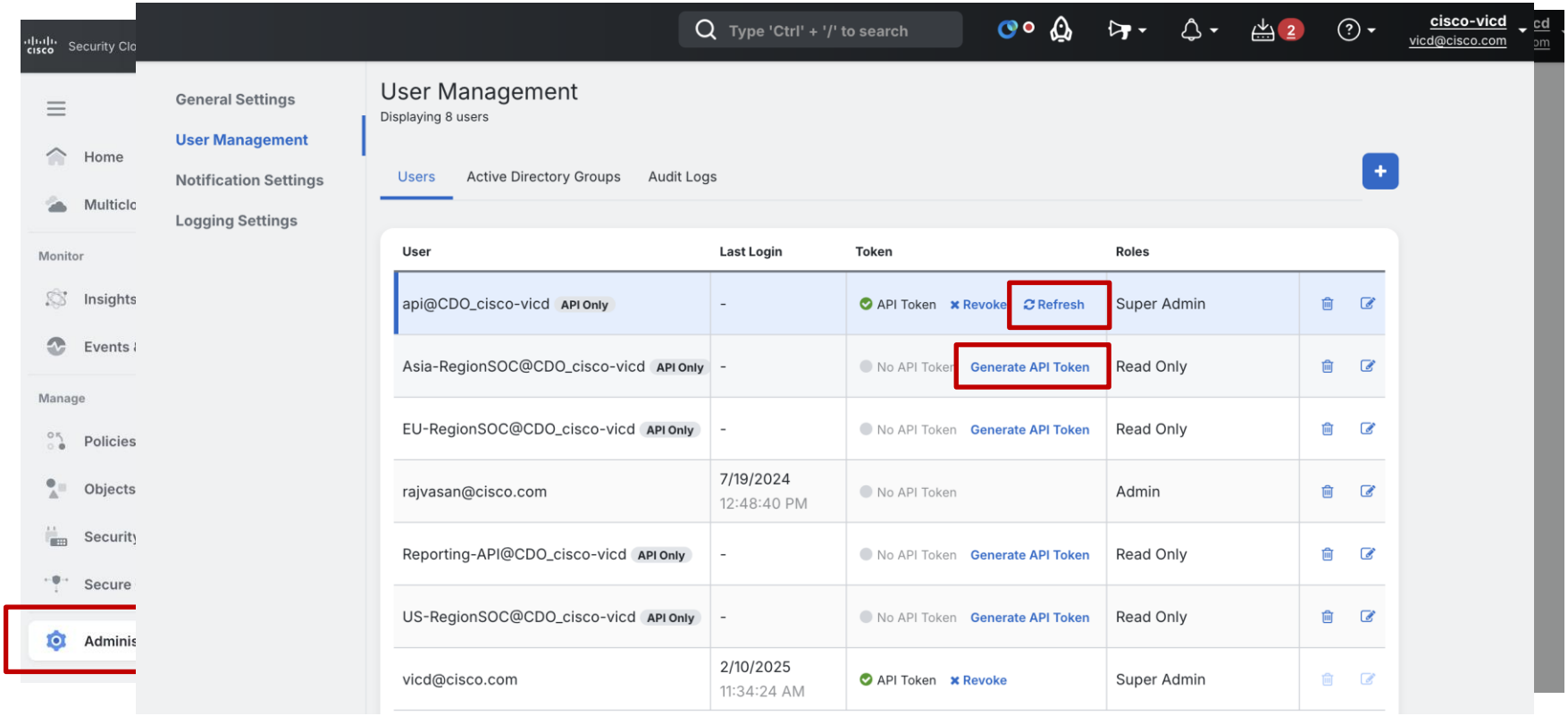
Create a user for API



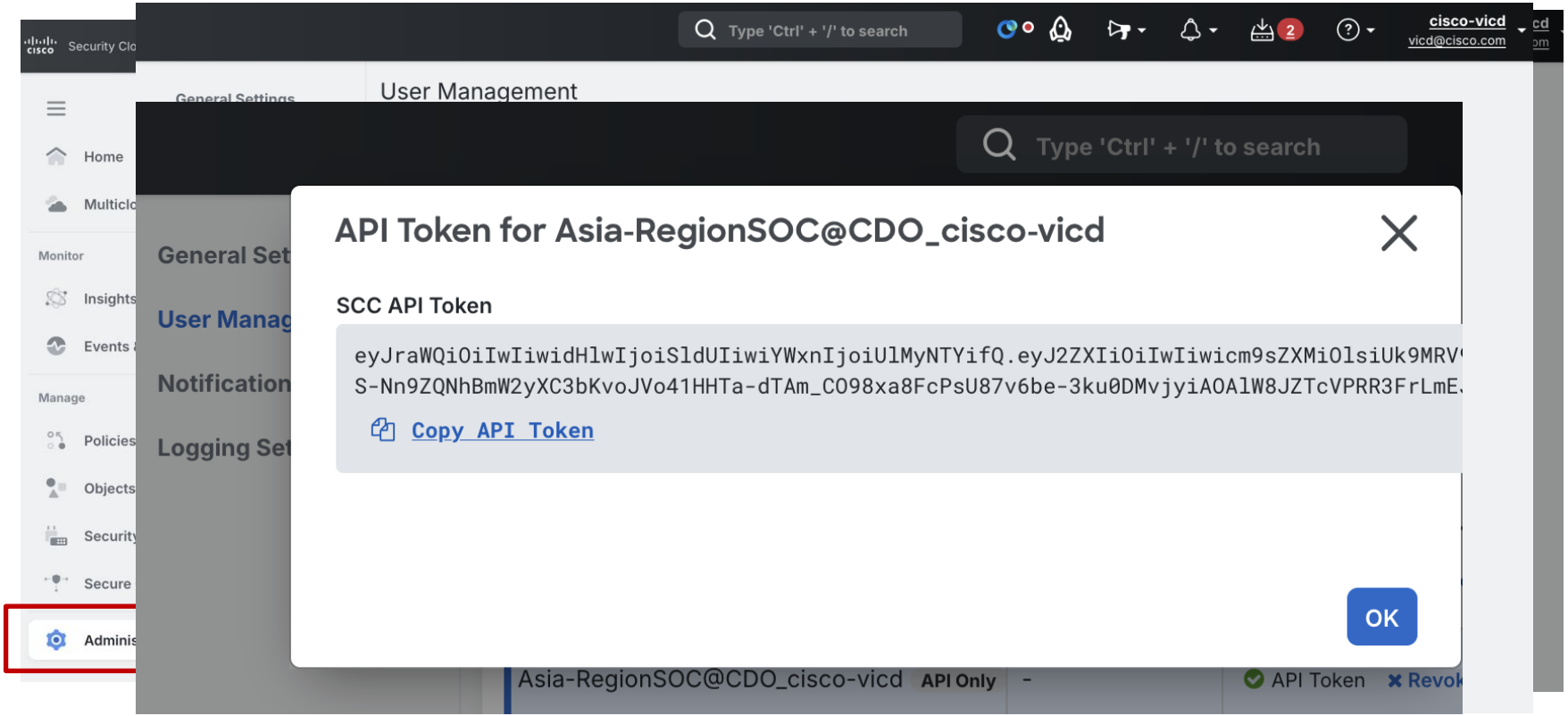
Create a user for API



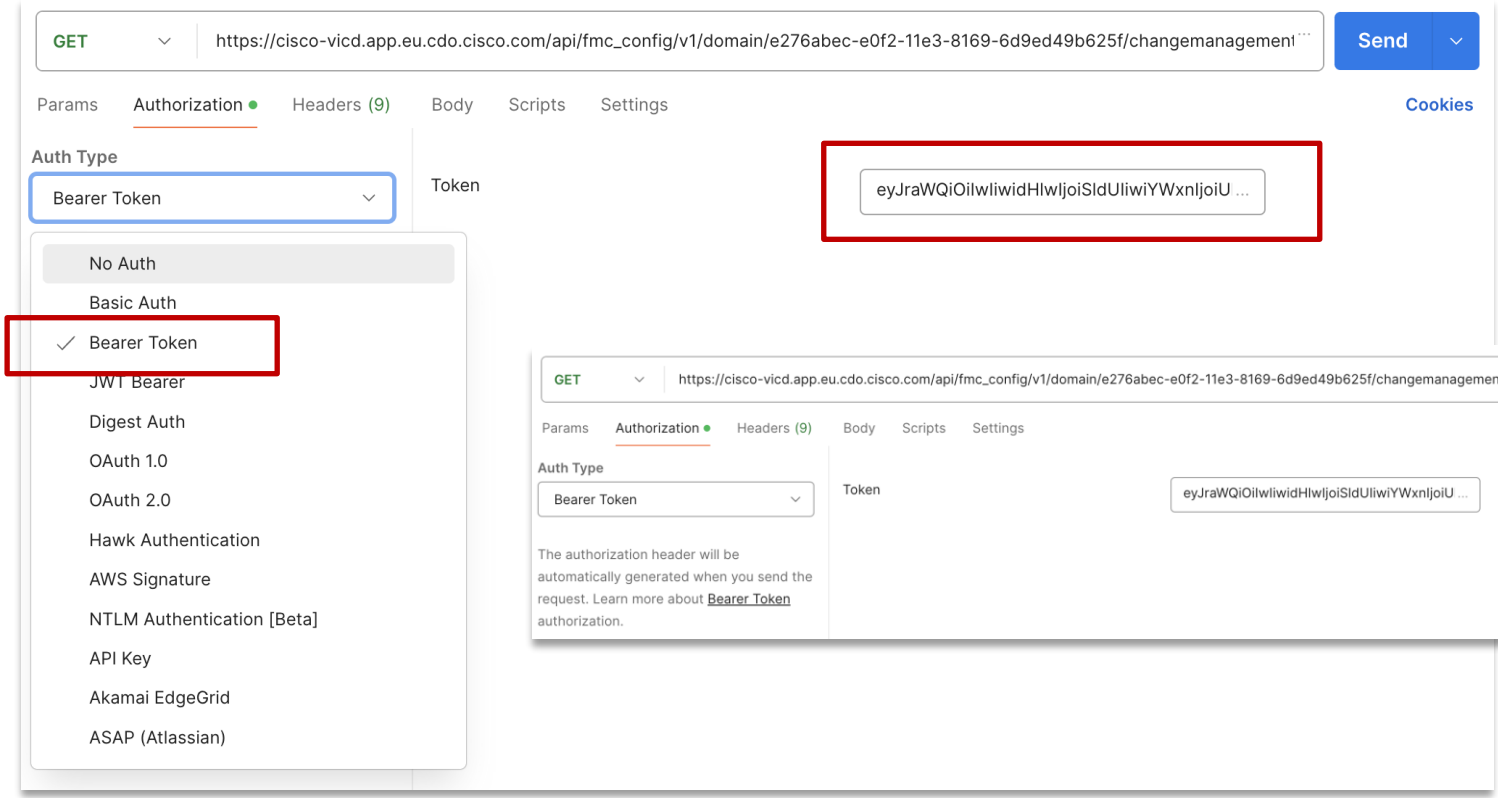
Create a user for API

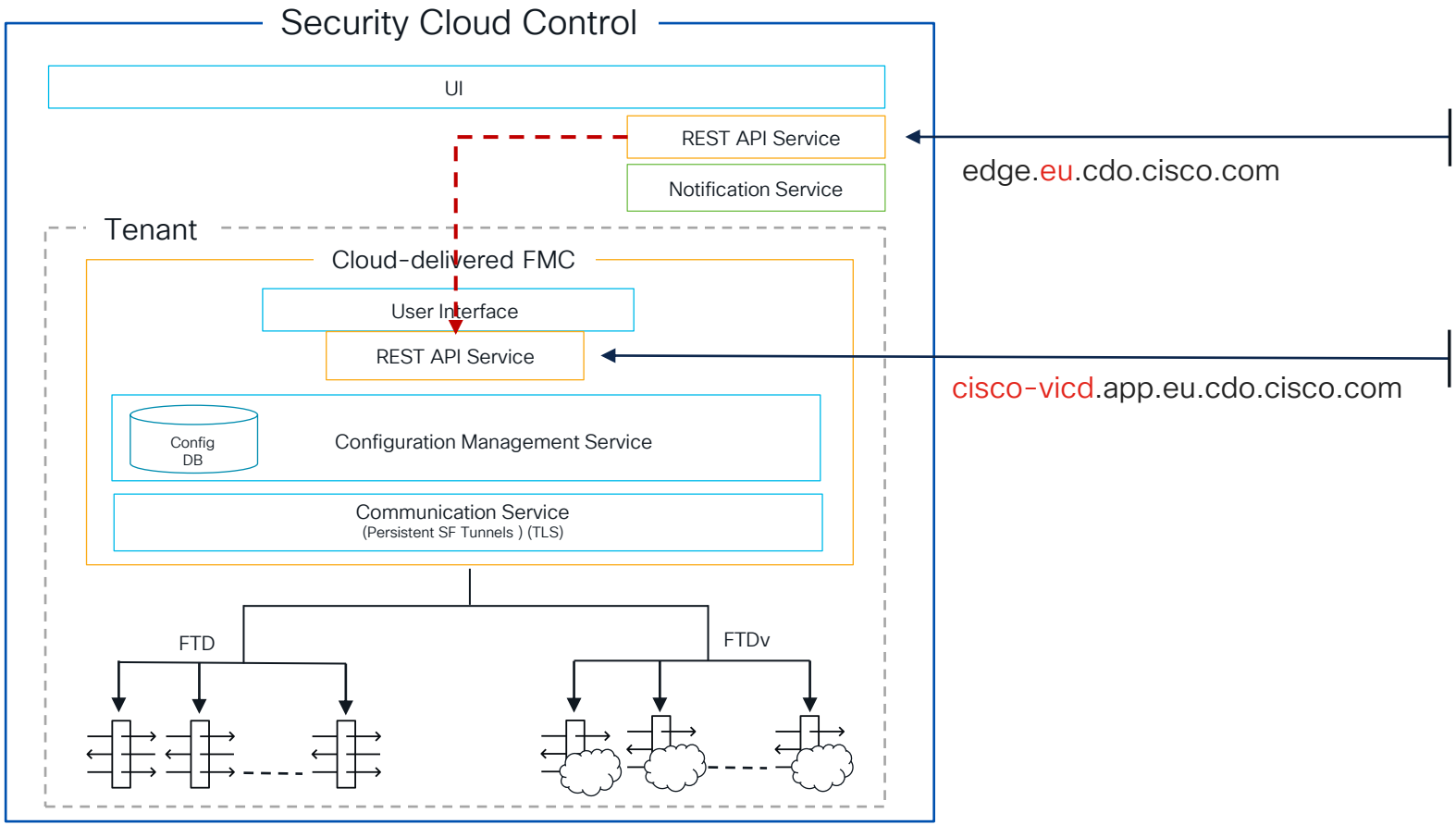


Create a user for API

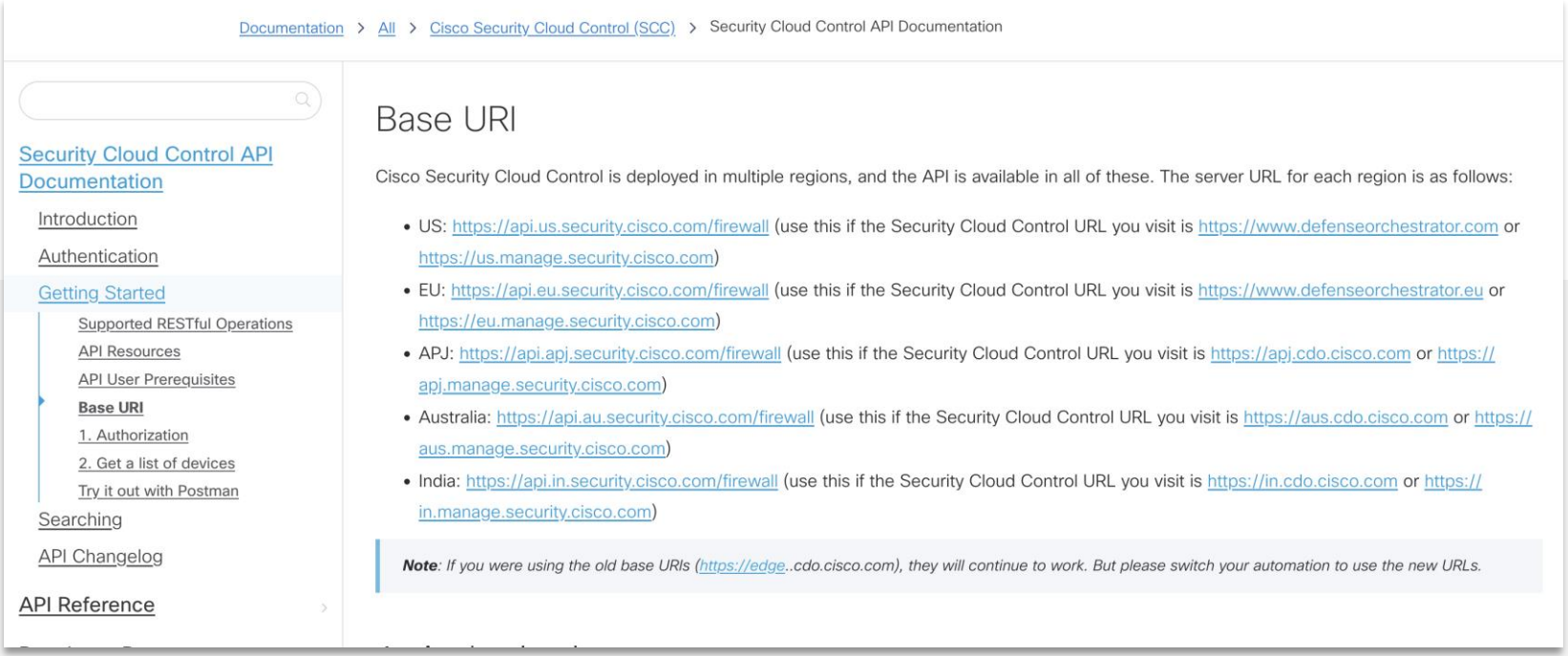


Add the API to the Client (Postman as example)

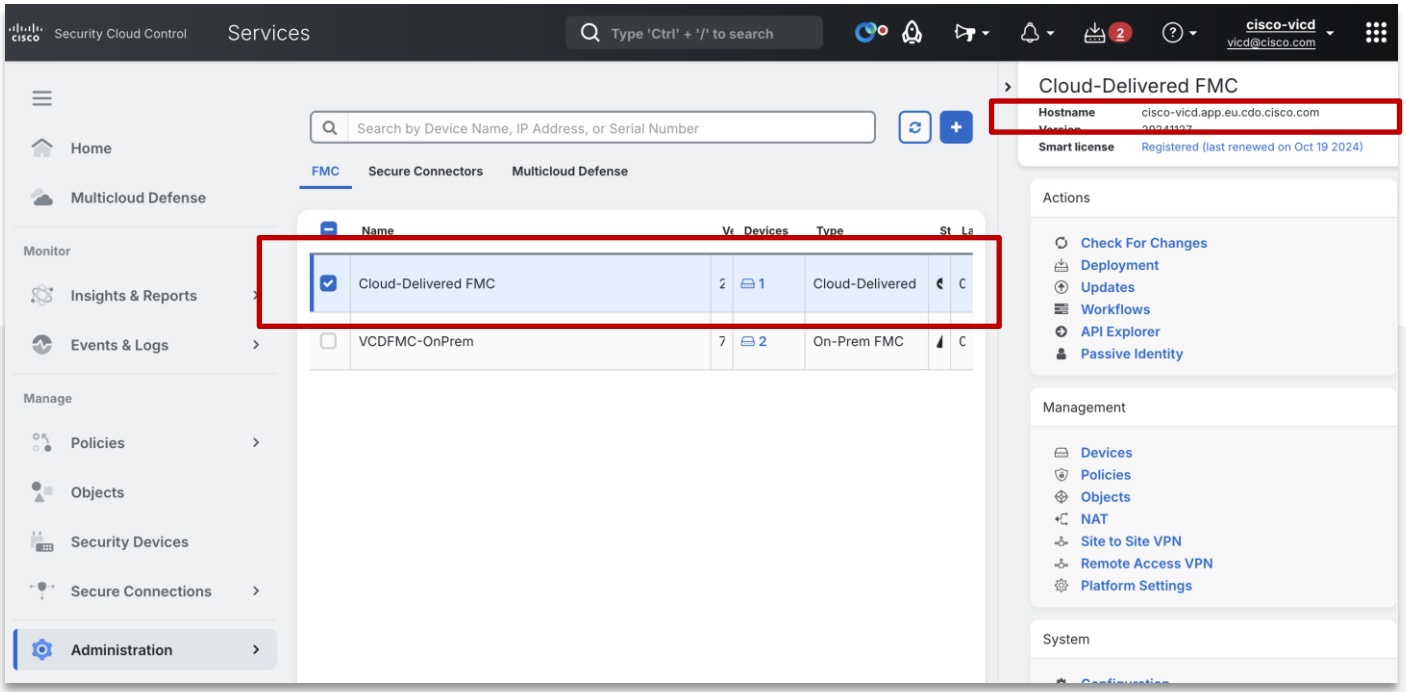




SCC API Hostname



cdFMC - Hostname



Find the {domainUUID}

https://{tenantname}.eu.cdo.cisco.com/api/api-explorer/

Health

Audit

System Information

- GET /api/fmc_platform/v1/info/serverversion/{objectId}
- GET /api/fmc_platform/v1/info/domain/{domainUUID}/{objectId}
- GET /api/fmc_platform/v1/info/serverversion
- GET /api/fmc_platform/v1/info/domain

Analysis

Object

Proxy request to cdFMC | FMC Endpoint

https://edge.eu.cdo.cisco.com/api/rest/v1/cdfmc/ api/fmc_platform/v1/info/domain

GET https://edge.eu.cdo.cisco.com/api/rest/v1/cdfmc/api/fmc_platform/v1/info/domain Send

Params Authorization Headers (7) Body Scripts Settings Cookies

Query Params

Key	Value	Description	Bulk Edit

Body Cookies Headers (24) Test Results 200 OK 536 ms 1.18 KB

{} JSON Preview Visualize


```
{
  "links": {
    "self": "https://eu.cdo.cisco.com/api/rest/v1/cdfmc/api/fmc_platform/v1/info/domain?offset=0&limit=25"
  },
  "items": [
    {
      "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
      "name": "Global",
      "type": "Domain"
    }
```

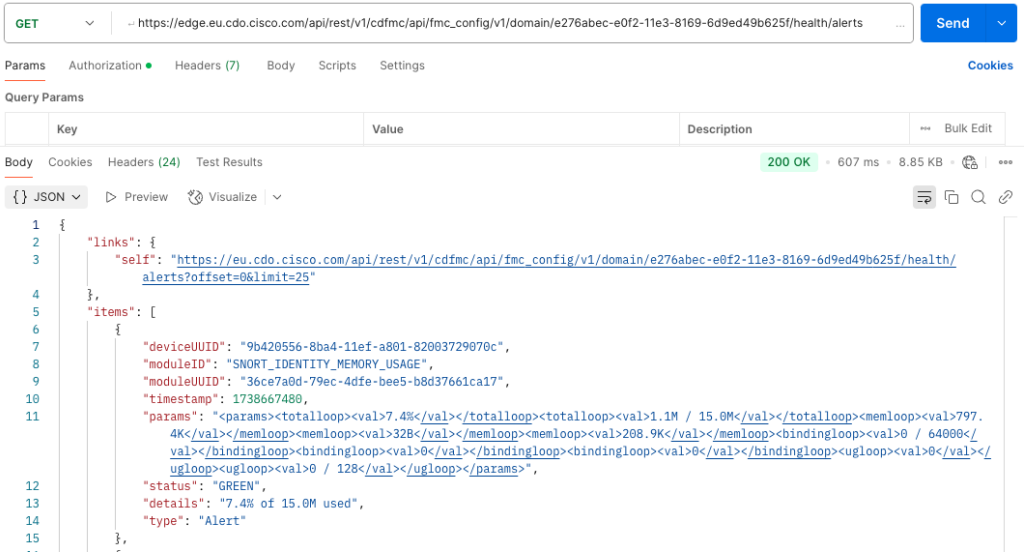
Construct an API query – cdFMC Proxy

Proxy Part + {DomainUUID} + FMC endpoint

Proxy request to cdFMC

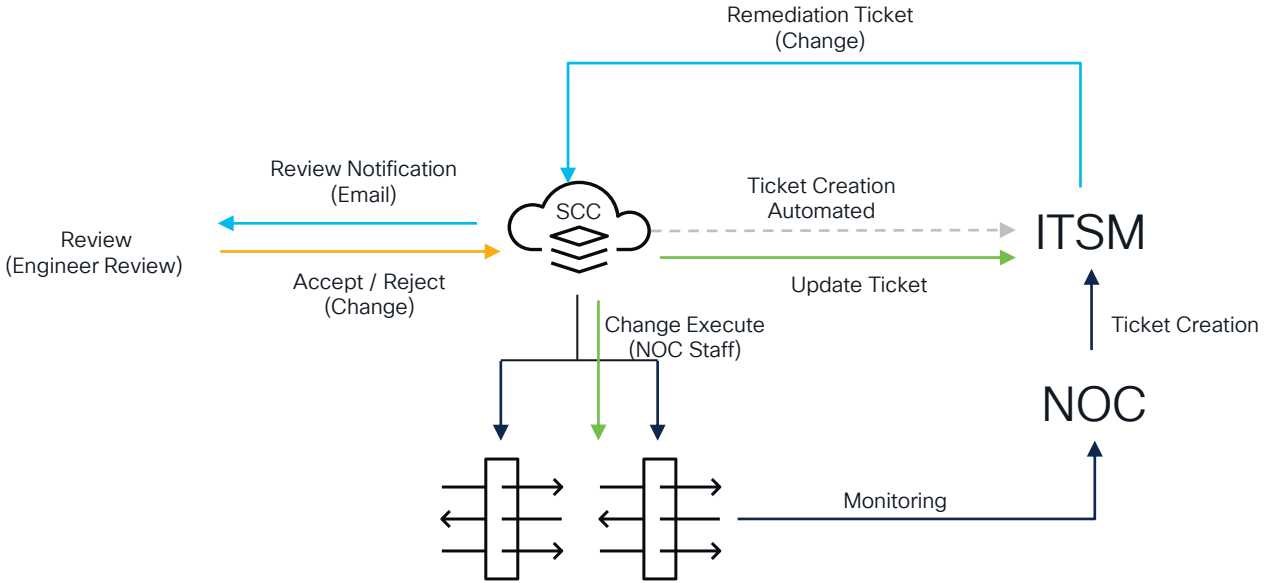
FMC Endpoint

https://edge.eu.cdo.cisco.com/api/rest/v1/cdfmc /api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/health/alerts



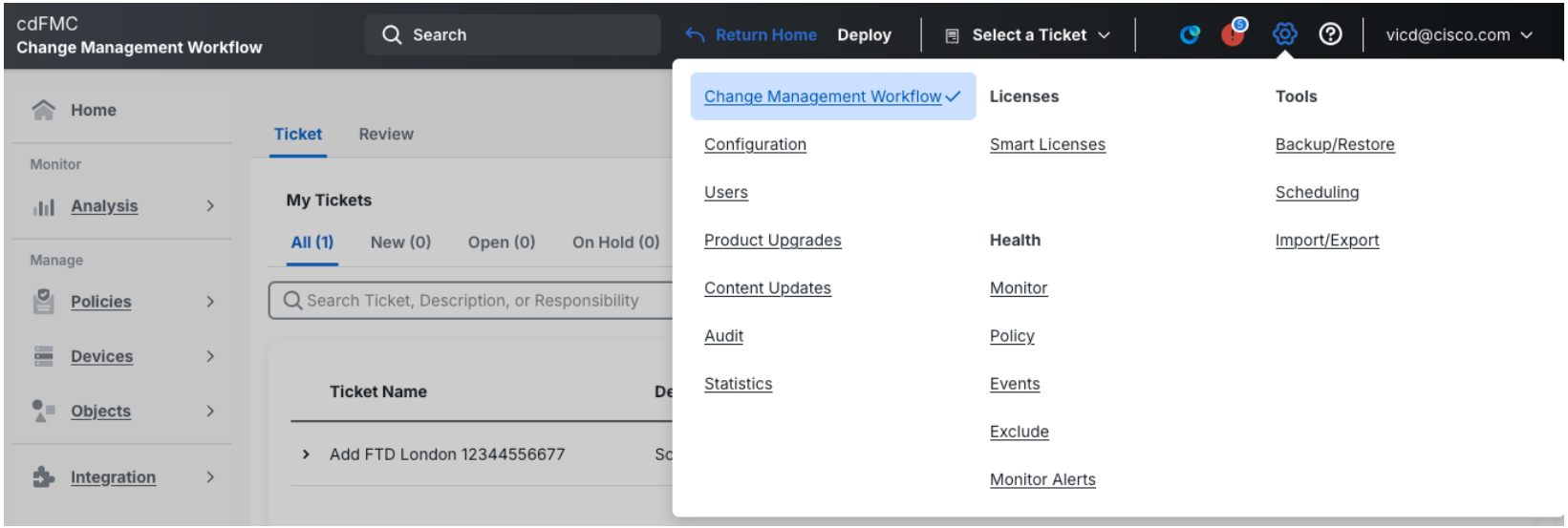
Change Request Management

Example



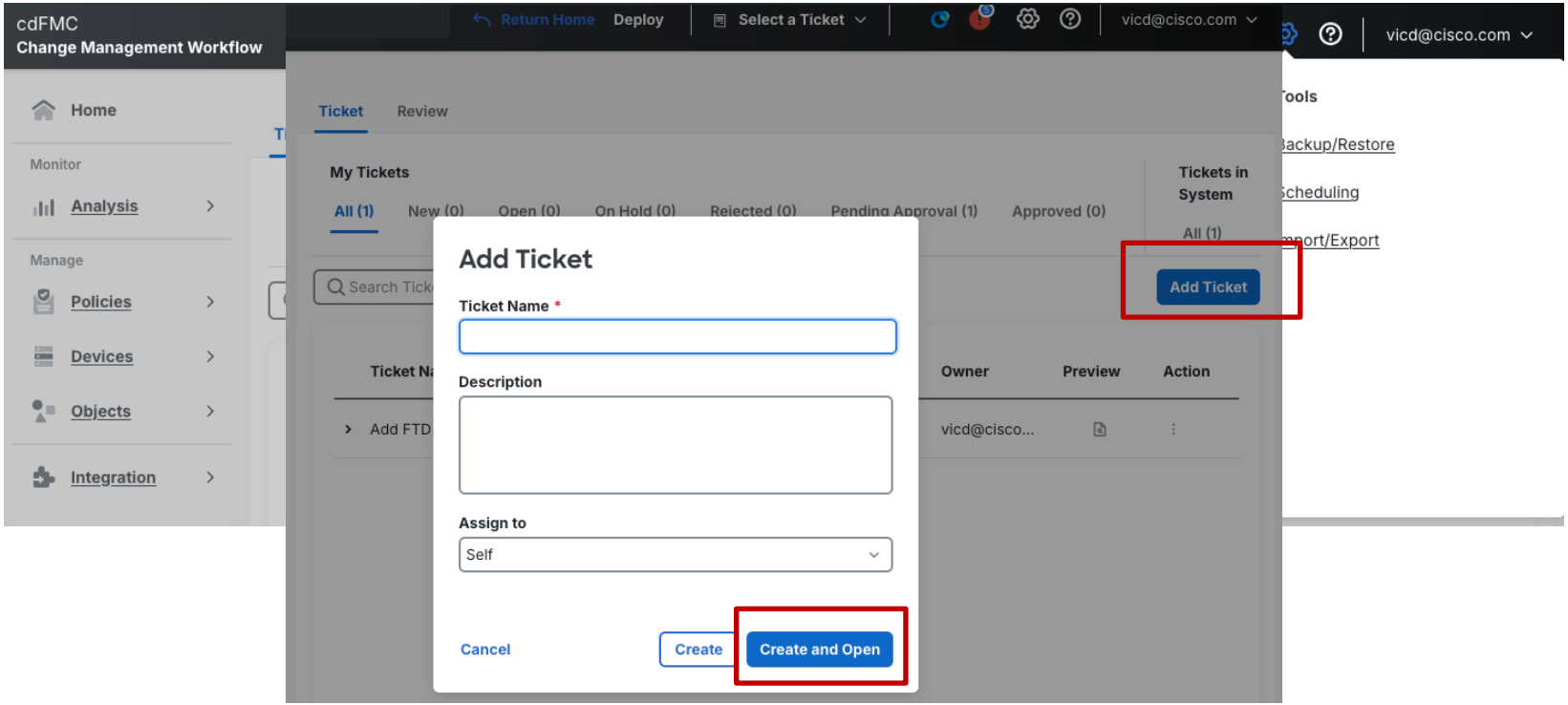
Change Management Workflow enables the linking of a Change Request and its Business Justification to a Change Log event.

Select the Change Management Workflow

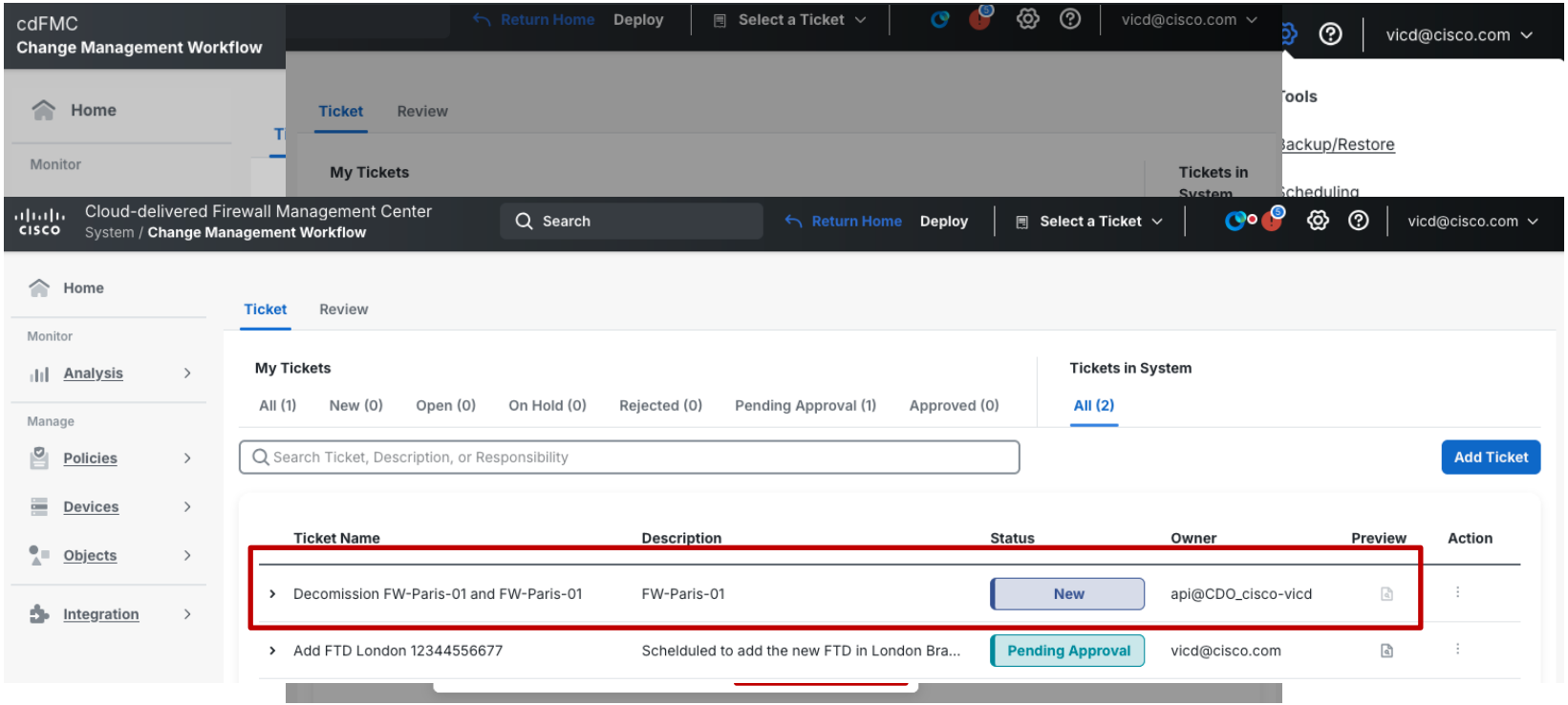


If the Change Management Workflow is not visible. Please enable it under the Configuration.

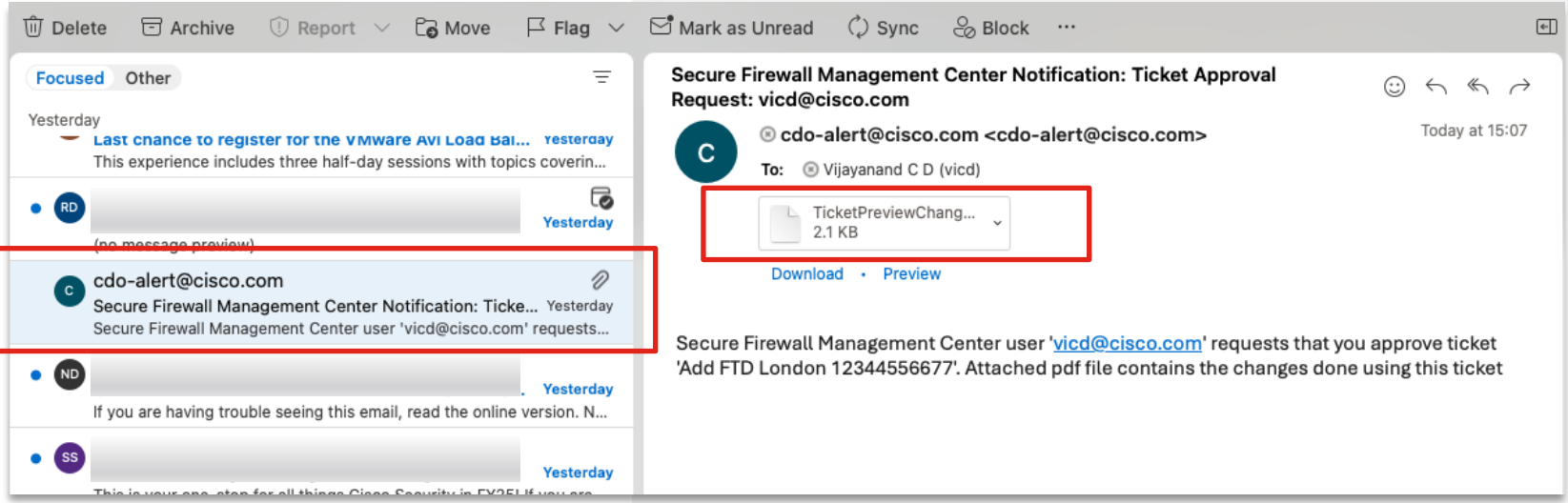
Create a Change Request Ticket Manually



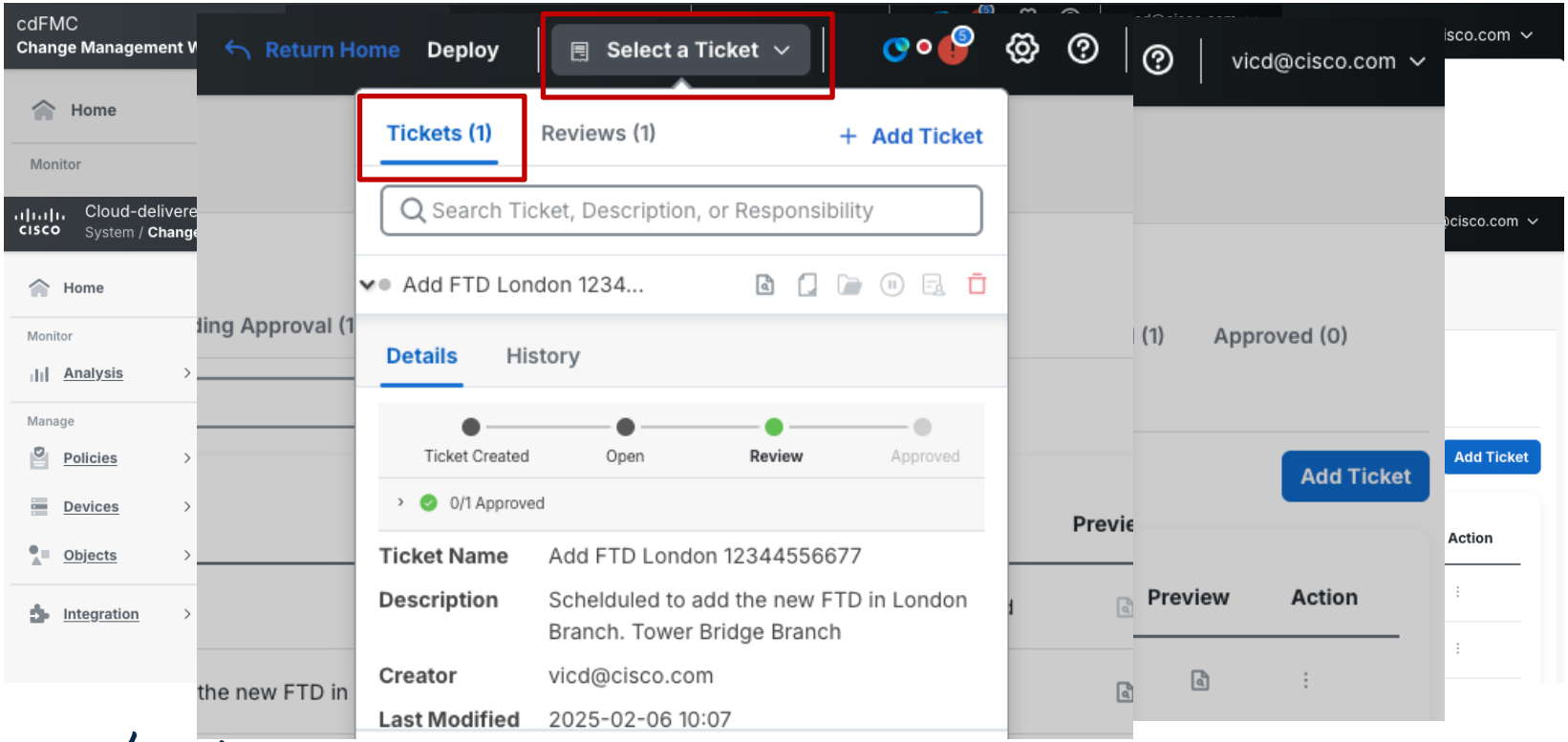
Create a Change Request Ticket Manually (Continue..)



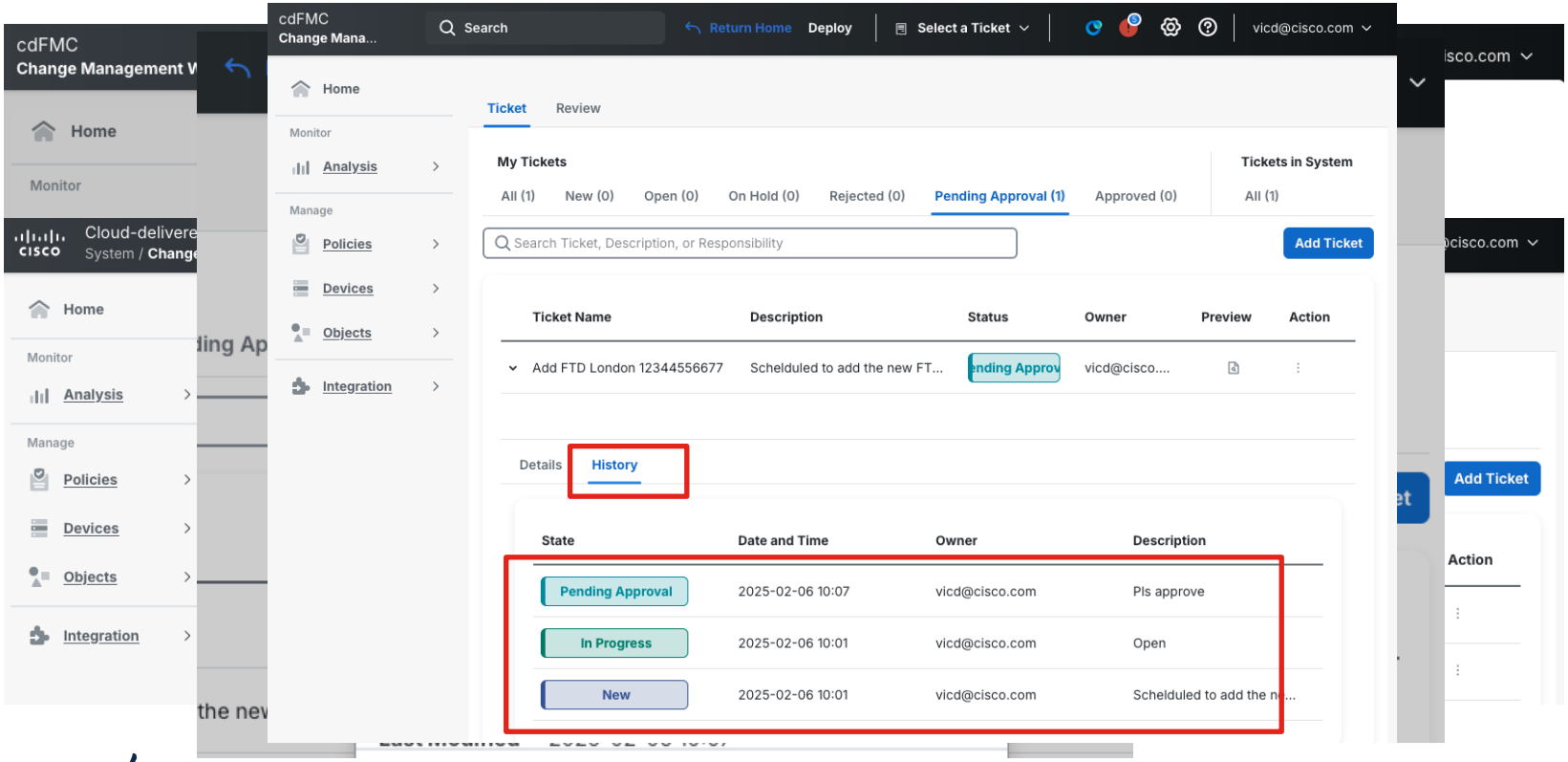
Change review - Email Alert to the Reviewer



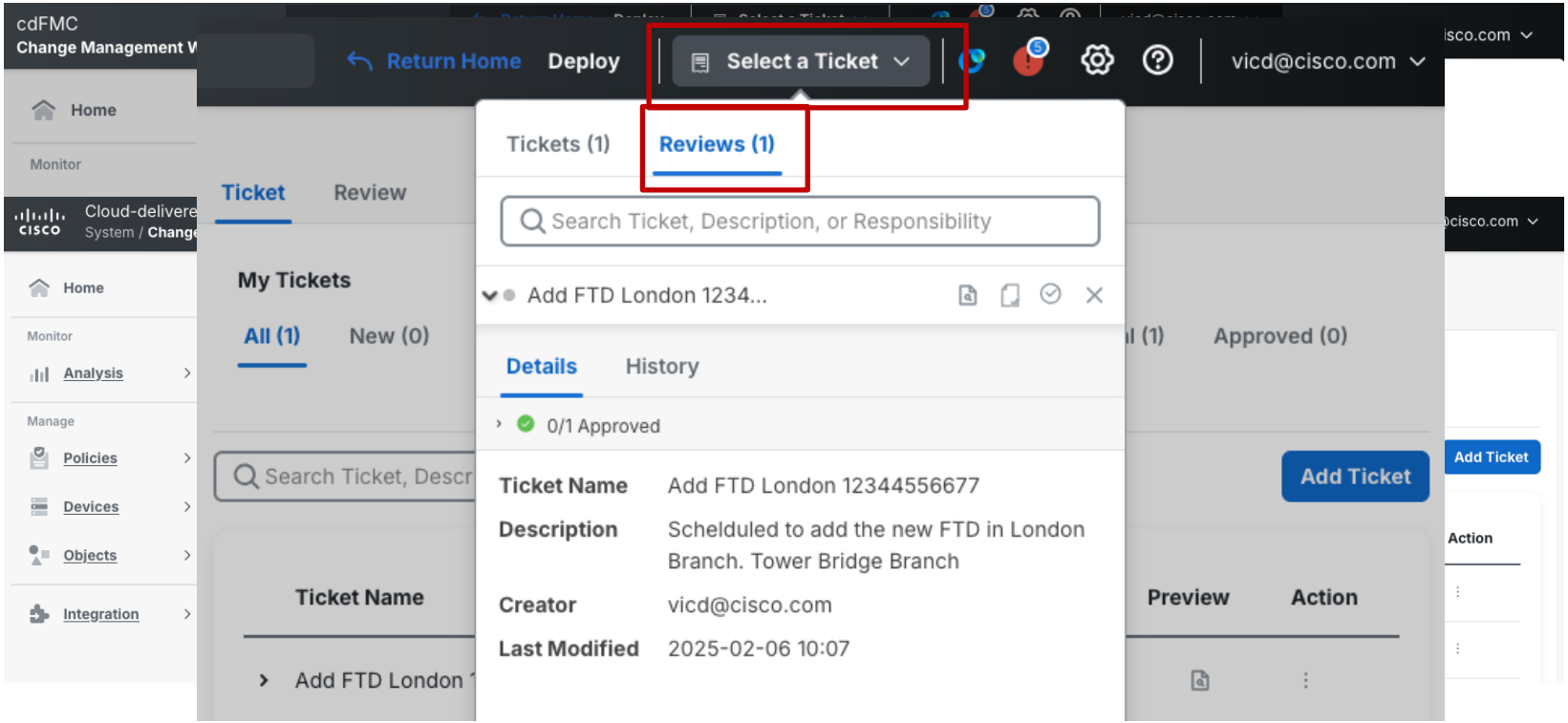
Ticket Bucket



View Ticket History

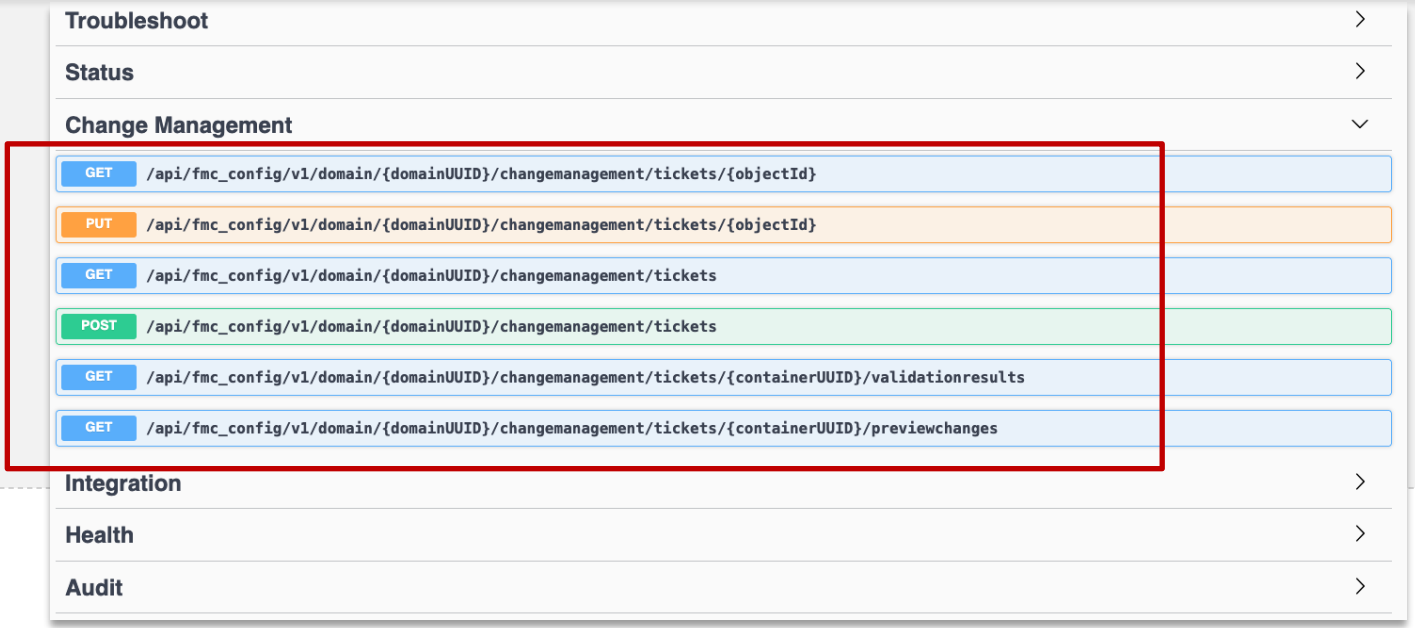


Review the assigned change request ticket



Automate the change request management in SCC

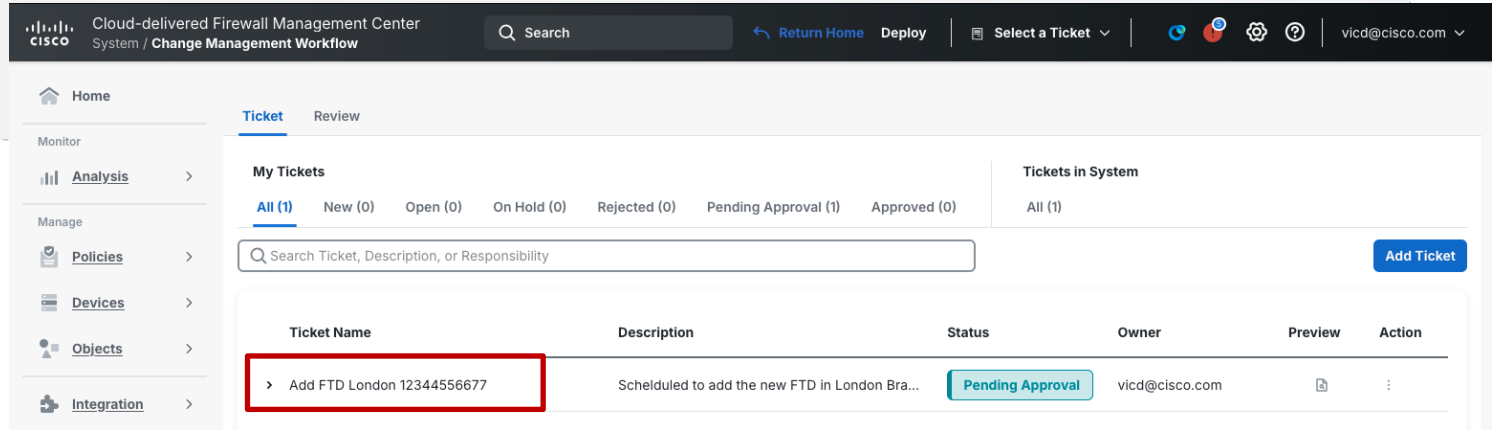
- https://{SCC tenant name}.app.eu.cdo.cisco.com/api/api-explorer/
- https://{on-premFMC IP}/api/api-explorer/



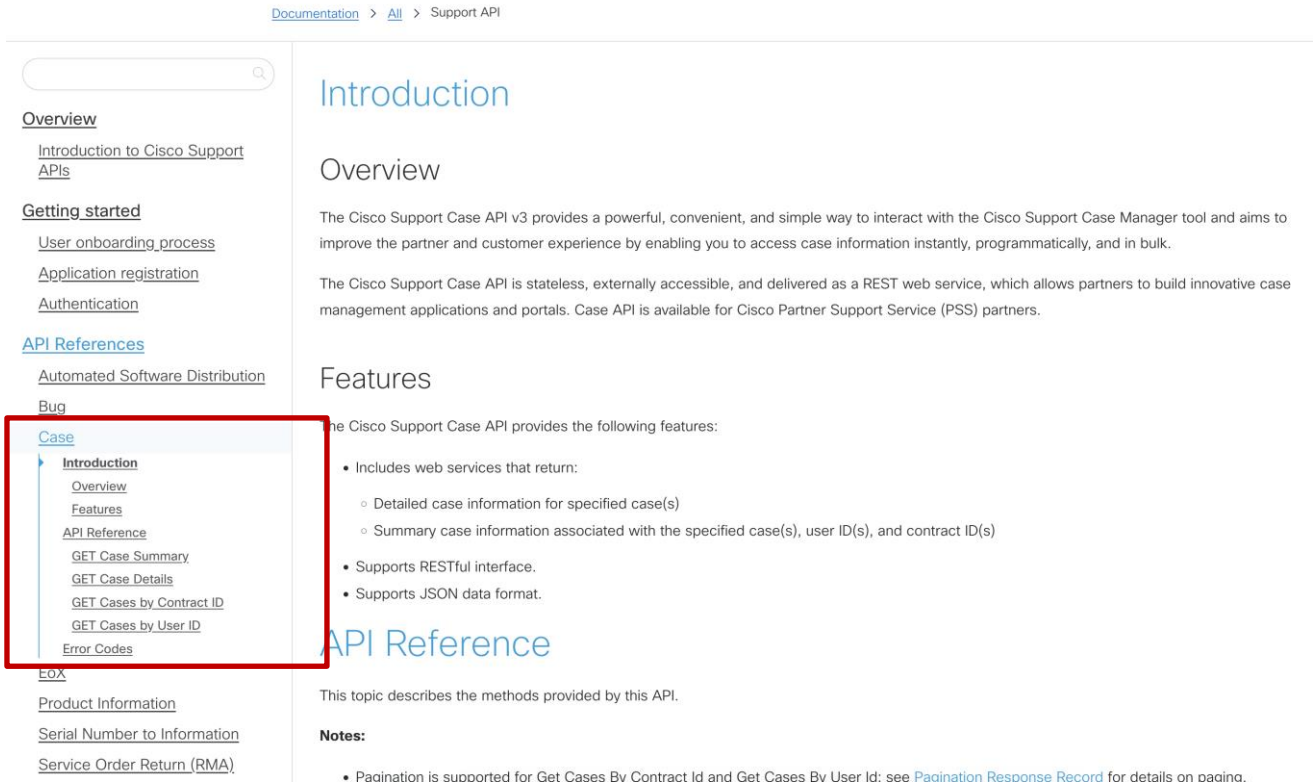
API Response

Example


```
{
 "links": {
"self": https://cisco-vicd.app.eu.cdo.cisco.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/changemanagement/tickets
 },
    "items": [
    {
        "id": "06007764-4C4C-0ed3-0000-073014523823",
        "name": "Add FTD London 12344556677",
        "type": "Ticket"
     }
],
```

Integrate TAC case APIs



Support Case Automation

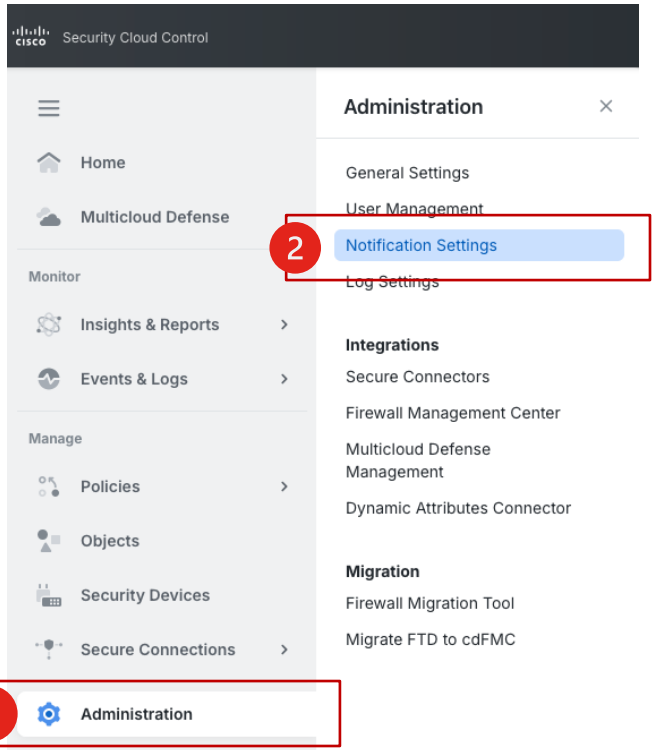
The Cisco Support Case API v3

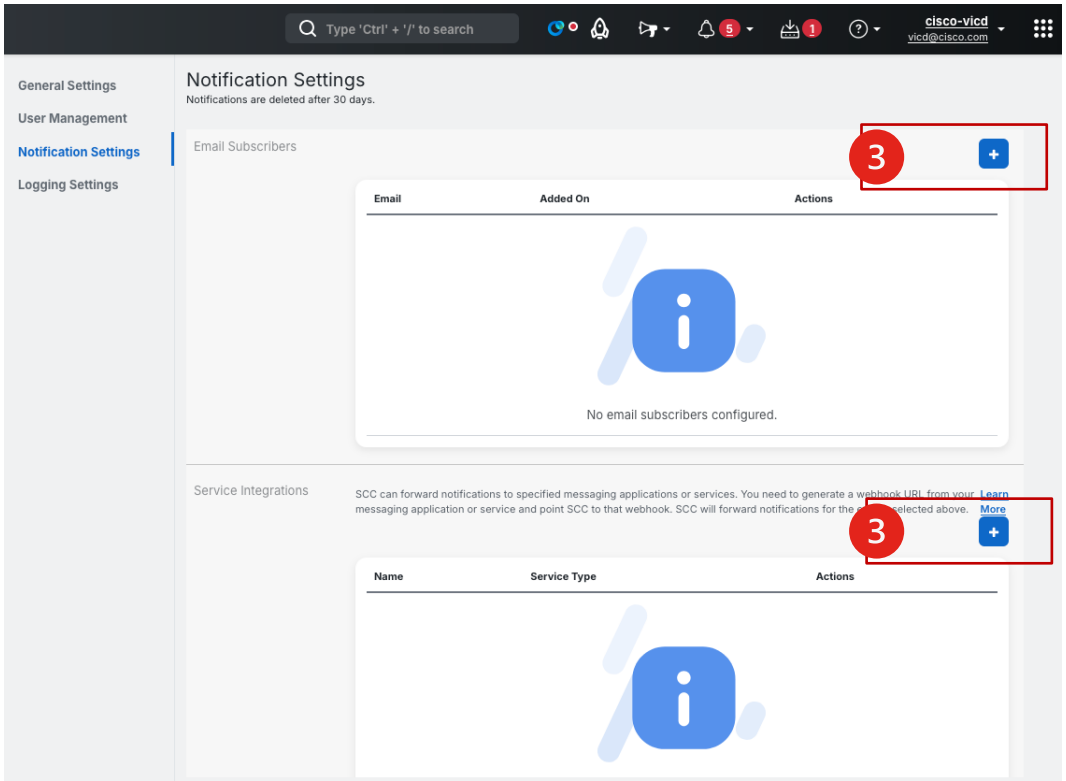
- API can return: Detailed case information for specified case(s)
- Summary case information associated with the specified case(s), user ID(s), and contract ID(s)
- Supports RESTful interface. Supports JSON data format.

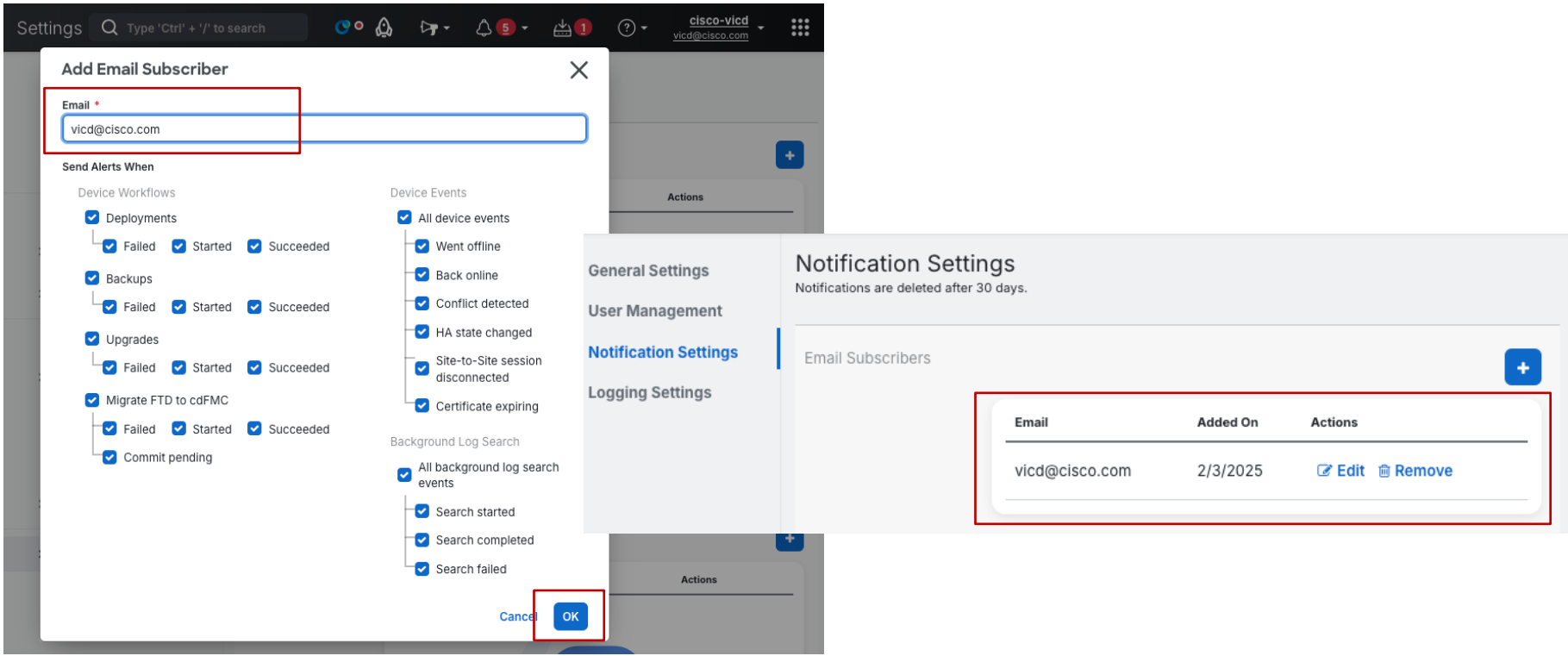
Reference

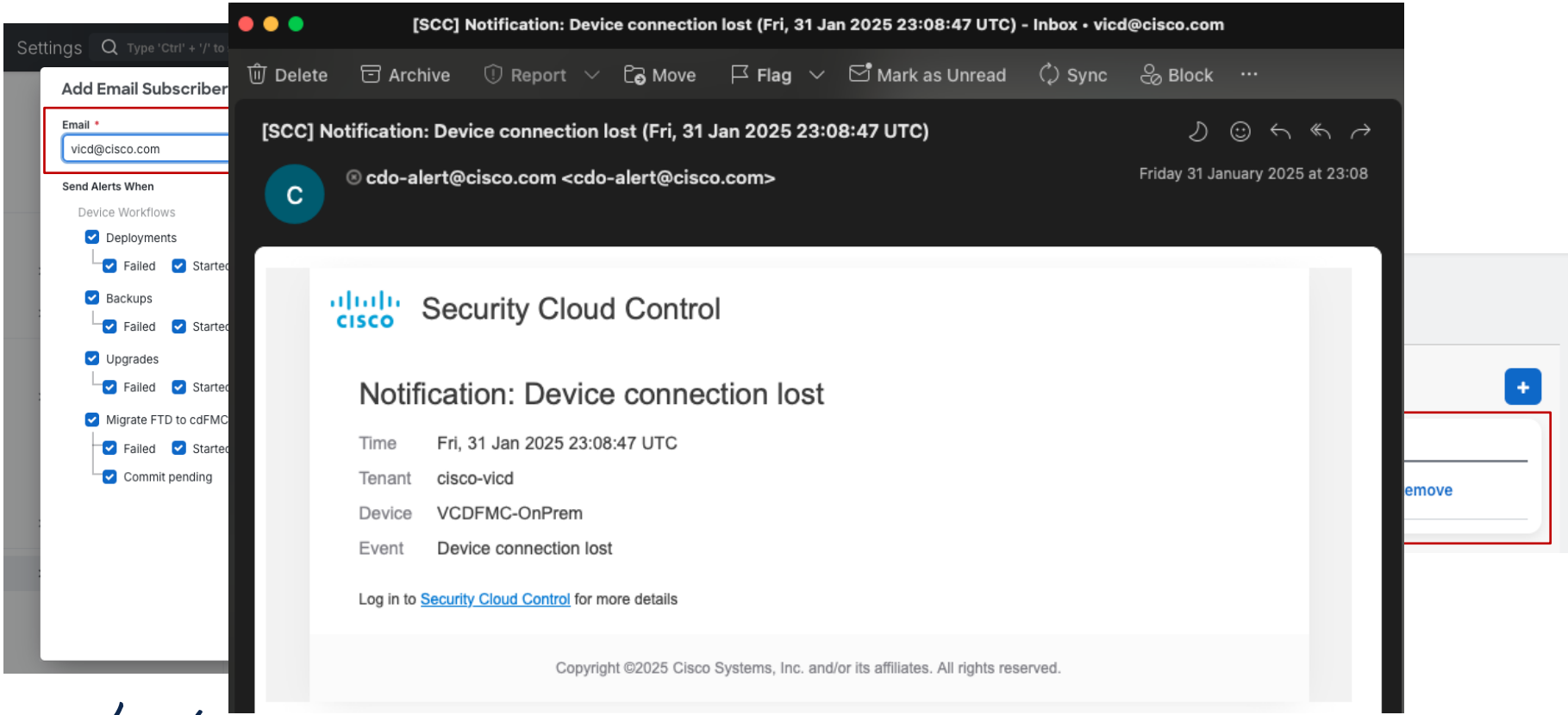
Cisco Support Case API version 3
Link


```
"cases": [
    {
        "item_entry_id": 1,
        "user_id": "directcust4",
        "case_id": "682299374",
        "title": "SNTC : Day 2 : NOS Handover Collector Training :TARGET CORPORATION",
        "severity": "3",
        "contact_name": "CPRSMOKE TESTER",
        "status_flag": "C",
        "status": "Closed",
        "creation_date": "2017-05-09T20:08:45.000Z",
        "updated_date": "2017-05-12T18:51:54.000Z",
        "serial_number": "", "contract_id": "",
        "technology_name": "Smart Services Capabilities",
        "sub_technology_name": "Collector Deployment SNTC (Contract Required)",
        "rmas": [],
        "bugs": []
    }
```



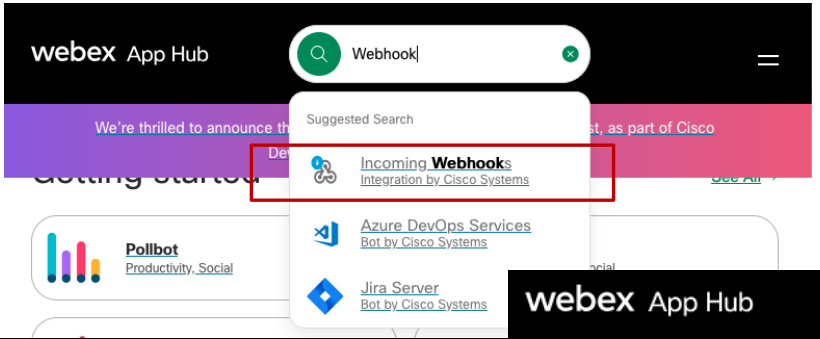


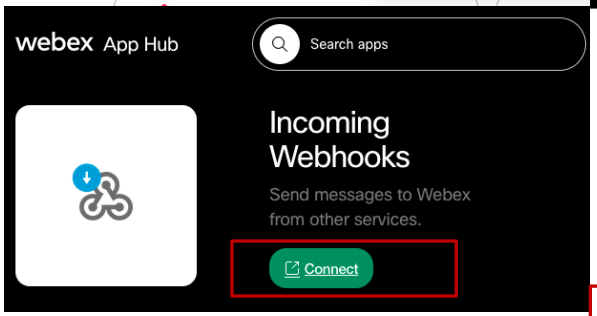


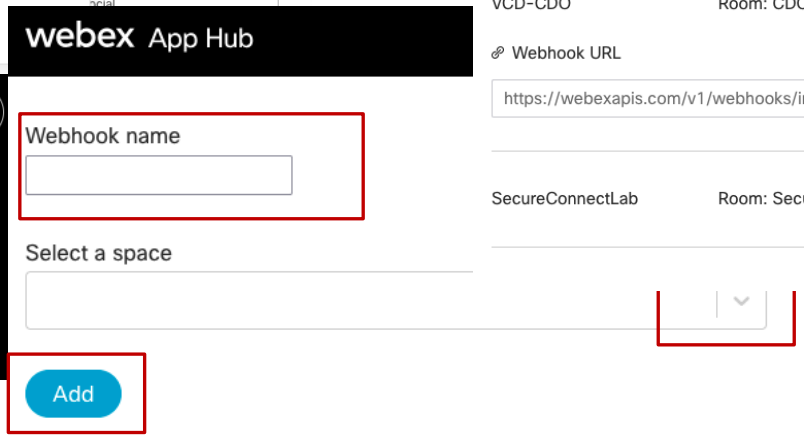


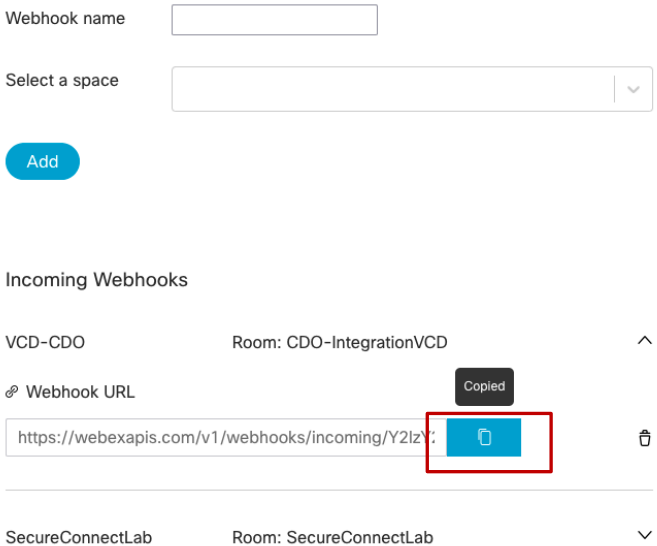
Create a Webhook URL in Webex

1. Create a space in Webex Team to receive webhook notifications
2. https://apphub.webex.com/

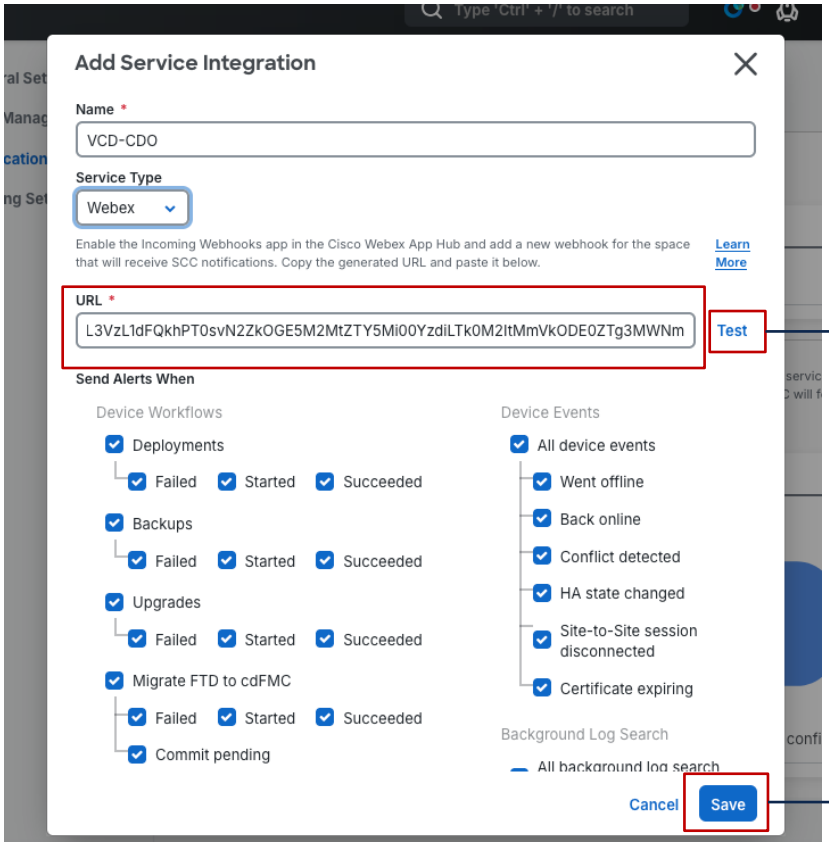




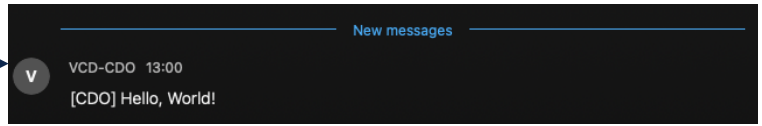


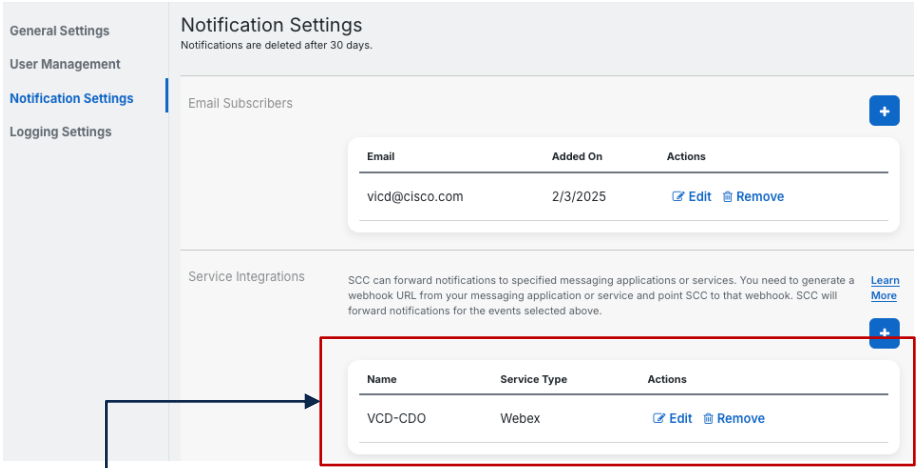


Add Webex Webhook URL in SCC

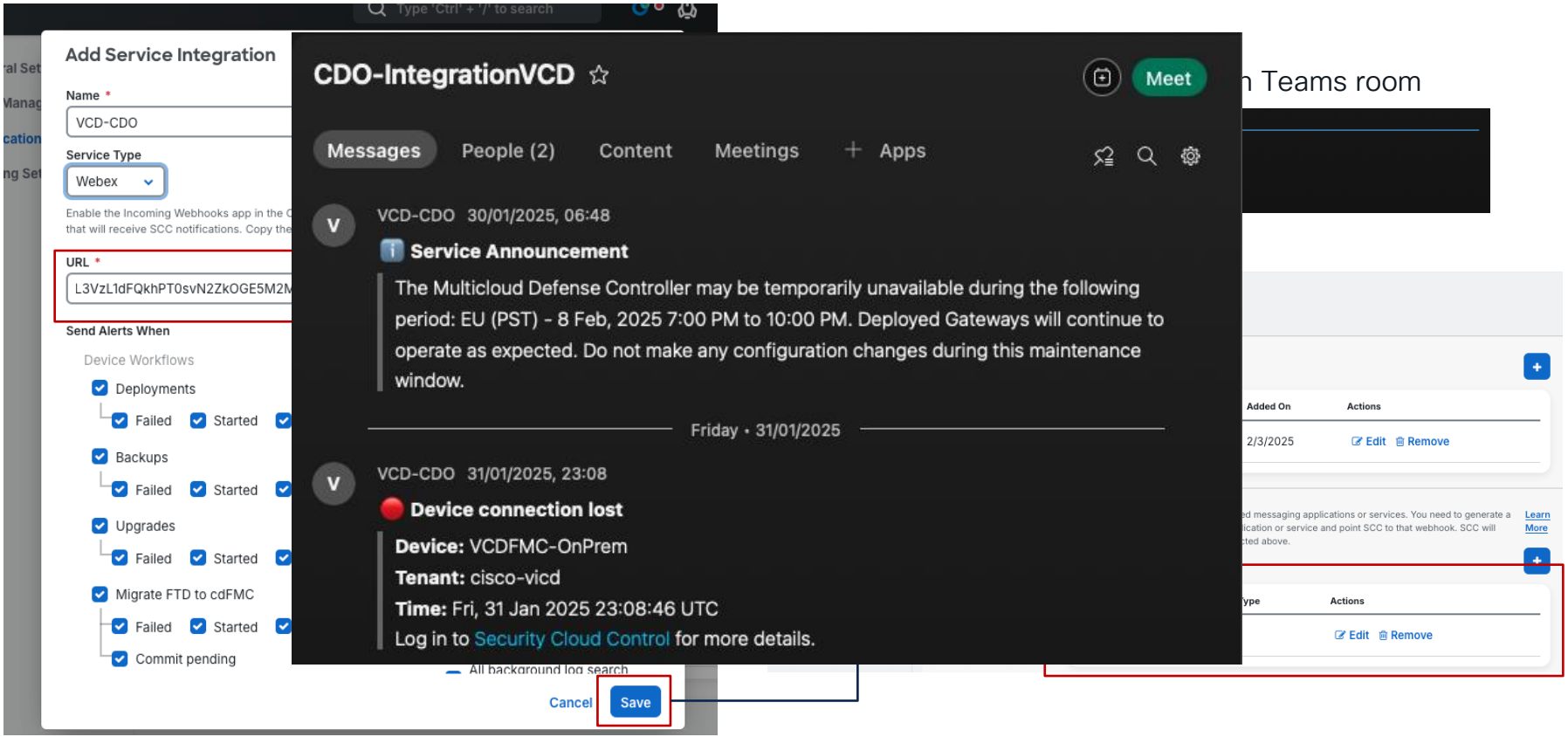


Test Webhook message in Teams room





Receiving Announcements & Notifications from SCC



Key Takeaways

As a best practice use separate API user in SCC

Cloud-delivered Proxy helps to reduce the API complexity

Leverage in-build notification to optimized workflow automation

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

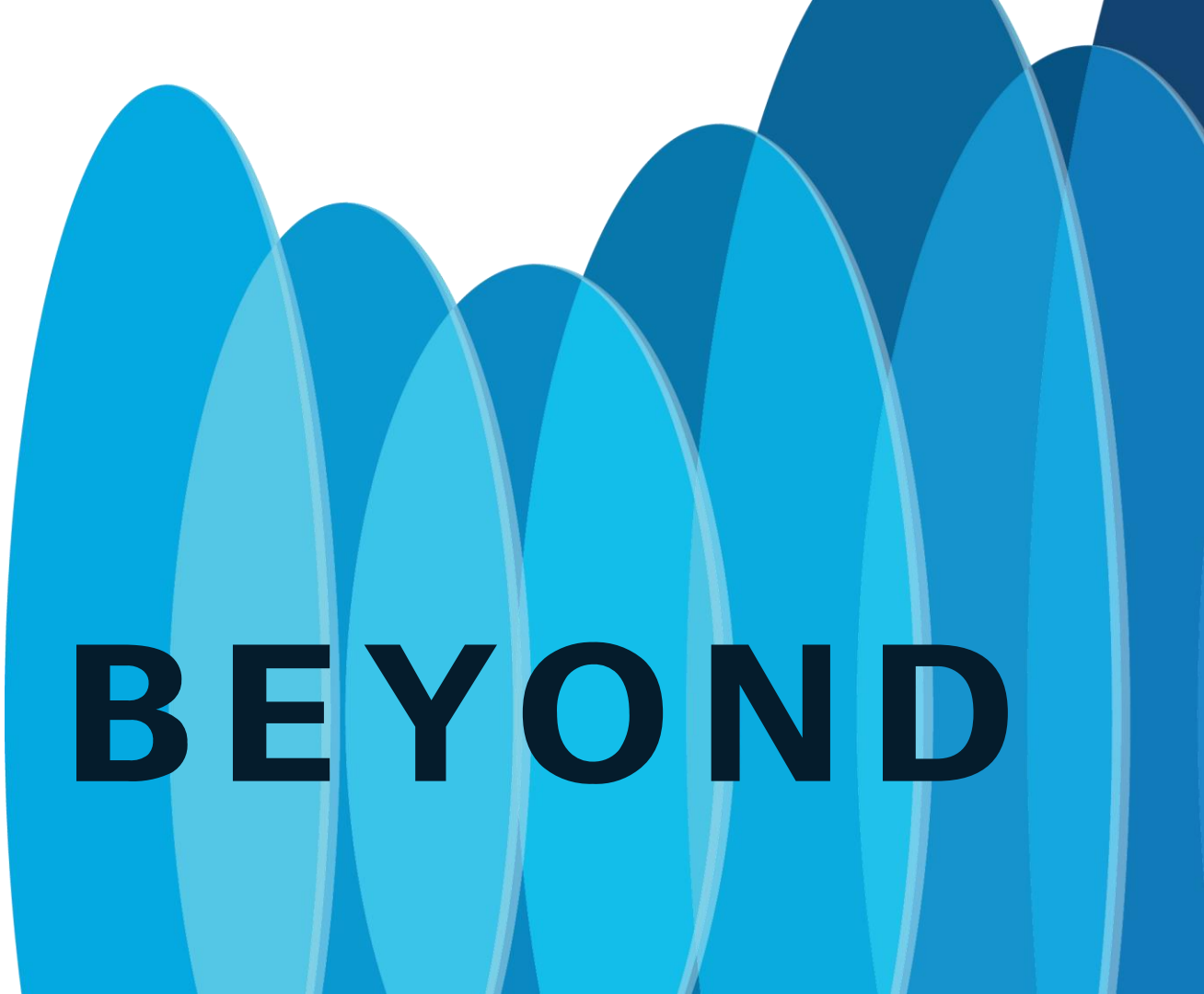
Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: VICD@CISCO.COM


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND