FY22 TAC 지원 New Product/Keyword 소개 및 협업 증대 방안

Customer Experience

강해명, 강도철, 이 연, 김 일 , 최경춘

Jul 29th 2022

Agenda

- Collaboration - 강해명 프로
- FTD - 강도철 프로
- Wifi6 - 이연 프로
- DCNM - 김일 프로
- ACI - 최경춘 프로

Collaboration

Cisco TAC - Collaboration

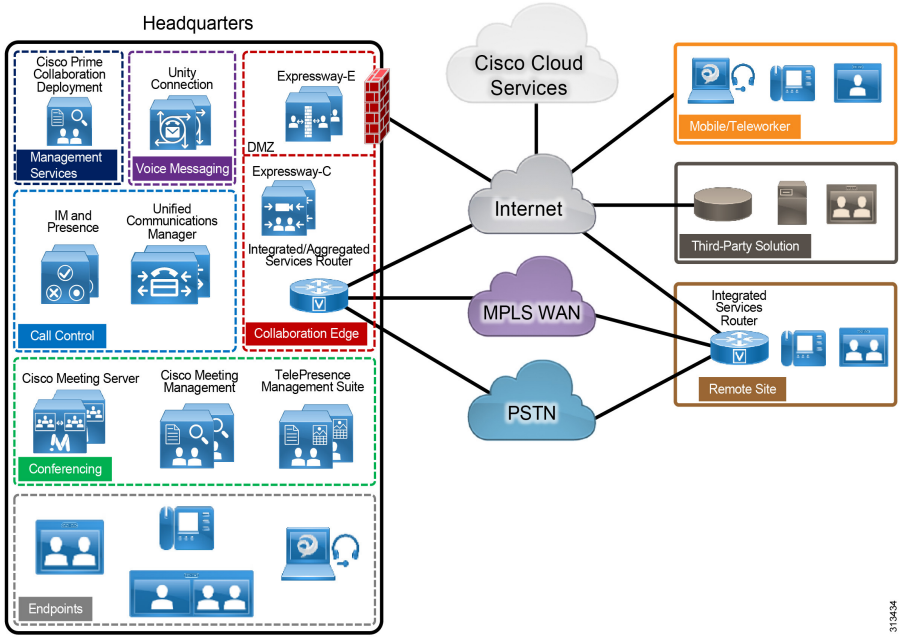
Started from Aug 2021, Collaboration products supported by Korea TAC

Telepresense
VCS/Expressway(CE1100/1200/Virtualization)
Cisco Meeting Server(CMS1000/2000/Virtualization)
Endpoint(IPPhone&Webex Device)

Voice-Communication Manager
Cisco Unified Communication Manager
(BE5000/6000/7000/Vitualization)

Voice-Gateway,Cube
ISR router&VG serise

Cisco Cloud Service
Webex Control Hub
Webex Meetings
Webex Messaging
Cisco Expressway-C Connector Host Management Connector



Cisco TAC - Collaboration

	Logs for TAC case **If the issue is reproducible**	**Logs for TAC case** **If the issue occurred in the past**
VCS/Expressway	• Reproduce issue after enable Diagnostic and packet capture • Collect Diagnostic Logs and Packet capture https://video.cisco.com/video/5810050375001	Collect System Full Snapshot https://video.cisco.com/video/6241488926001 *Recommend to collect full snapshot during off-hours as this job consumes CPU resource
CMS	• Reproduce issue after enable appropriate logging and packet capture • Generate call diagnostic logs(Webadmin-Configuration-API-Cospace-Diagnostic) • Collect logbundle.tar.gz from SFTP • Collect appropriate logs from other involved products https://video.cisco.com/video/5817647402001 https://video.cisco.com/video/5810051601001	Download following logs from SFTP • Log Bundle(Logbundle.tar.gz) • Diagnostic(Any call diagnostic logs generated) • Crash Cump(if a creash occurs) https://video.cisco.com/video/5810051601001
Video Endpoint	• Reproduce issue after enable packet capture • Download Full Call history logs include packet dump captured https://video.cisco.com/video/5810051574001	Download Full Call history logs https://video.cisco.com/video/5810051574001

Cisco TAC - Collaboration

	Logs for TAC case **If the issue is reproducible**	**Logs for TAC case** **If the issue occurred in the past**
CUCM(Call Manager)	• Reproduce issue after enable packet capture • Collect Trace data and Packet dump using RTMT https://video.cisco.com/video/6028728075001 https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/200787-How-to-Collect-Traces-for-CUCM-9-x-10-x.html	• Collect Trace data using RTMT • Collect Crash dump if the service crashed https://video.cisco.com/video/6039539294001 https://community.cisco.com/t5/collaboration-knowledge-base/troubleshooting-core-dumps/ta-p/3119142
VG/Cube	• Reproduce issue after enable Debug and packet capture • Collect Debug logs and packet dump • Collect Show tech-support voice https://video.cisco.com/video/6070396627001 https://community.cisco.com/t5/collaboration-knowledge-base/how-to-properly-and-safely-collect-debugs-on-an-ios-router/ta-p/3114693	Show tech-support voice
Webex Cloude Service	Reproduce the issue and collect HAR and fiddler logs Search Keyword in webex help center https://help.webex.com/	Collect Webex client log Search Keyword in webex help center https://help.webex.com/

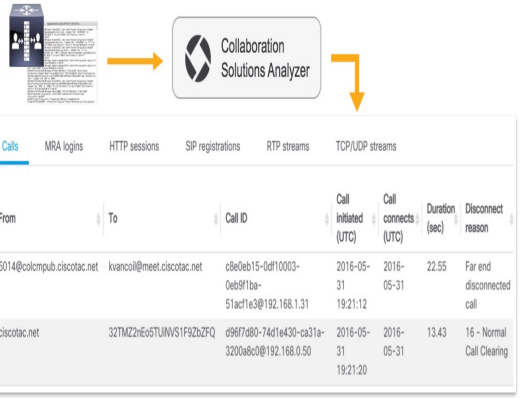
Cisco TAC - Collaboration

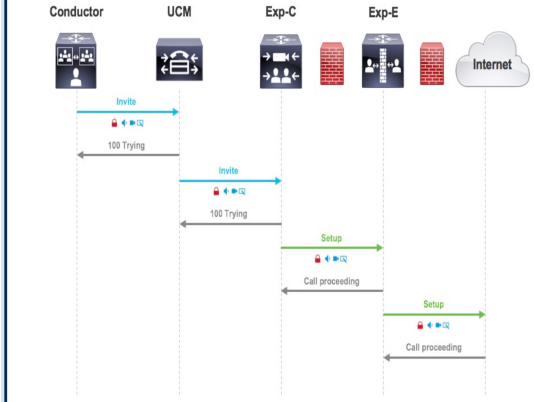
Useful Tool

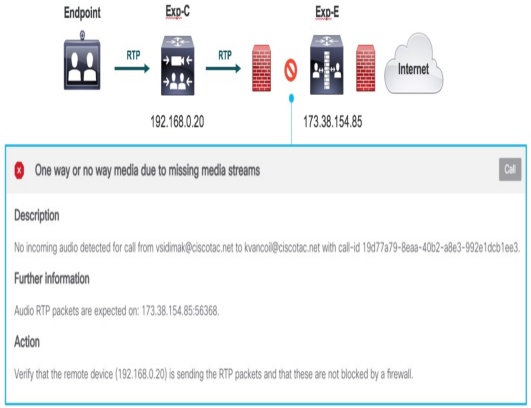
[Collaboration Solutions Analyzer]

[Collaboration Solutions Analyzer User Documentation]

Log visualisation	Data correlation	Automatic issue detection







Security - FTD

Cisco TAC Security - FTD

Cisco Firepower 1010/1100 Model

Cisco Firepower 2110/2120 Model

Cisco Firepower 2130/2140 Model

Cisco TAC Security – Firepower/ASA/VPN feature

Firepower/ASA/ VPN feature	• Firepower 플랫폼에서 장애 이슈 분석 요청 시 **미리 TS file을 이슈 발생 시 실시간으로 반출**해 놓으시면 더 효율적으로 케이스를 진행할 수 있음, Firepower 엔드 유저 측은 보통 뱅크, 금융 등 보안 등급이 매우 높기 때문에 케이스 오픈하고 나서 TAC에서 다시 TS file을 요청하게 되면 파트너사에서 또다시 TS file 수집 승인을 엔드 유저 측에서 받아와야 하기에 시간이 많이 소요됨. 1/ TS file generation procedures: https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html • ASA/FTD/Router 플랫폼의 **VPN 이슈**에서 보통 IPSec VPN session interruption이슈 발생되고(one-time/transient), restore(회선 변경/장비 리부팅 등등) 한 후 케이스 오픈 시, **Debug outputs**들이 제대로 수집 안 되었을 경우 많이는 RCA 정밀 분석이 어려움. 일반 IPSec VPN session interruption 이슈가 발생하게 되면 원인 분석하는데 Debug가 제일 효율적인 방법이기도 함. 1/ Collect Anyconnect DART https://community.cisco.com/t5/security-documents/how-to-collect-the-dart-bundle-for-anyconnect/ta-p/3156025 • FMC physical appliance는 로컬 코리아 택 에서 fully 지원하나 FMC Virtual Appliance는 코리아 택에서 지원하지 않기 때문에 **vFMC 연동 이슈**가 발생하게 되면 CIN team 통하여 직접 **글로벌 팀으로 케이스 오픈 요청**하시면 됨.

Cisco TAC Security – show commands

ASA/FTD Fireware Platform:
IPsec VPN (IKEv1):
(config)#logging monitor debugging
#terminal monitor
- show crypto isakmp sa [Collect it during problem occur]
- show crypto ipsec sa [Collect this outputs 5 times every 10sec during problem occurred]
- show crypto isakmp stats [Collect this outputs 5 times every 10sec during problem occurred]
- debug crypto condition peer ipv4 x.x.x.x
- debug crypto isakmp 255
- debug crypto ipsec 255

IPsec VPN (IKEv2):
(config)#logging monitor debugging
#terminal monitor
- show crypto isakmp sa [Collect it during problem occur]
- show crypto isakmp sa detail [Collect it during problem occur]
- show crypto ipsec sa [Collect this outputs 3 times every 10sec during problem occurred]
- show crypto ikev2 sa [Collect this outputs 3 times every 10sec during problem occurred]
- debug crypto ikev2 protocol 127
- debug crypto ikev2 platform 127
- debug crypto ca

Anyconnect VPN:
please carry out the following actions step by step,
- Enable the following on the ASA:
- terminal monitor
- logging monitor debugging
- debug webvpn 255
- Connect from an endpoint & Reproduce issue
- Collect the ASA debug output
- Collect DART
- Disable the above commands:
- terminal no monitor
- no logging monitor
- undebug webvpn 255

Collect Anyconnect DART
https://community.cisco.com/t5/security-documents/how-to-collect-the-dart-bundle-for-anyconnect/ta-p/3156025

Router Platform:
IPsec VPN (IKEv1):
- show crypto session [Collect it during problem occur]
- show crypto engine connection active [Collect it during problem occur]
- show crypto isakmp sa [Collect it during problem occur]
- show crypto isakmp stats [Collect it during problem occur]
- show crypto ipsec sa [Collect this outputs 3 times every 10sec during problem occurred]
- debug crypto condition peer ipv4 x.x.x.x
- debug crypto isakmp 255
- debug crypto ipsec 255

IPsec VPN (IKEv2):
- show crypto session [Collect it during problem occur]
- show crypto engine connection active [Collect it during problem occur]
- show crypto isakmp sa [Collect it during problem occur]
- show crypto isakmp sa detail [Collect it during problem occur]
- show crypto ipsec sa [Collect this outputs 3 times every 10sec during problem occurred]
- show crypto ikev2 sa [Collect this outputs 3 times every 10sec during problem occurred]
- debug crypto ikev2 protocol 127
- debug crypto ikev2 platform 127
- debug crypto ca

Firepower/FTD Platform:
TS file generation procedures:
https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html

Wireless – Wifi6

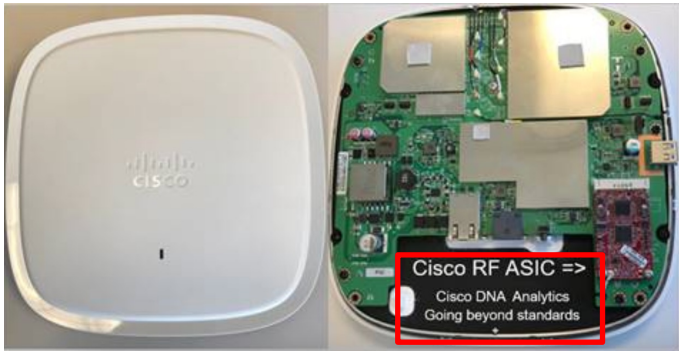
Cisco KR TAC – WIFI6 supported products

Supported keyword: Access Points	Supported keyword: Wireless LAN Controller
9105AX Serials Access Point	Catalyst 9800 Wireless LAN Controller 10 Gbps (**C9800-L**)
9115AX Serials Access Point	Catalyst 9800 Wireless LAN Controller 40 Gbps (**C9800-40**)
9117AX Serials Access Point	Catalyst 9800 Wireless LAN Controller 80 Gbps (**C9800-80**)
9120AX Serials Access Point	Catalyst 9800 Wireless LAN Controller for On-Premise Cloud (**C9800-CL**)
9124AX Serials Access Point	Catalyst 9800 Wireless LAN Controller on Public Cloud (**C9800-CL**)
9130AX Serials Access Point	Catalyst 9800 Wireless LAN Controller on Switch (**C9800-SW**) - Collab Only
91XX Series Access Point (with Embeded Wireless Controller)	

Cisco TAC Wireless

Integrated Cisco RF ASIC

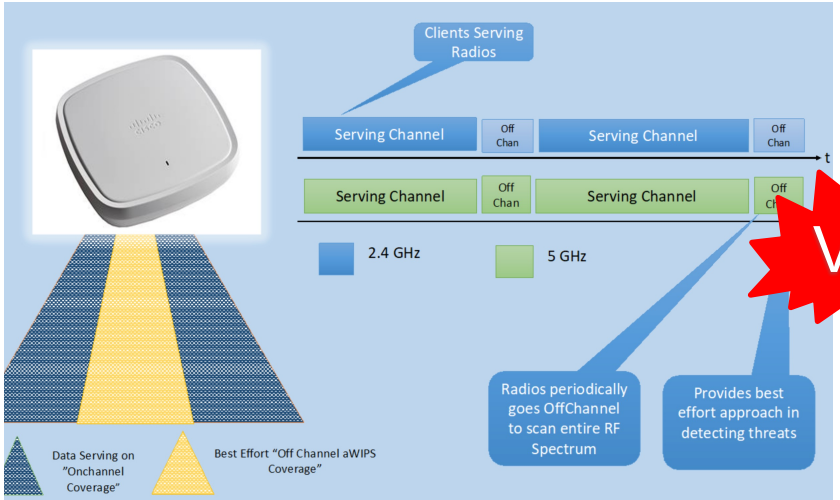
Catalyst 9120AX and 9130AX have integrated RF ASIC



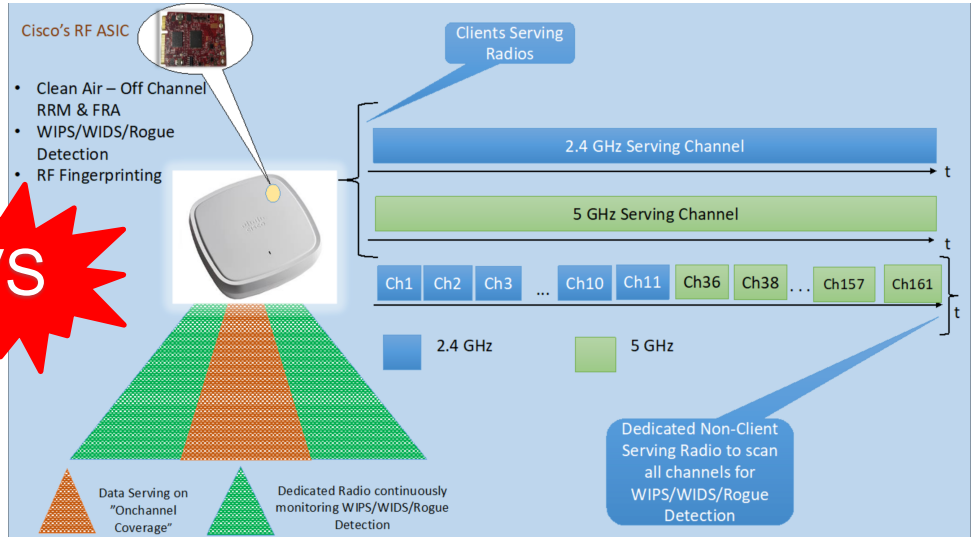
AP monitors 802.11 channels for rogue devices, noise,interference.

APs perform Off-channel scan (80ms per 2/3sec), during off-channel scan APs do not service clients. (Not friendly to voice traffic.)

But with RF ASIC, client Servicing Radios can always ‘‘online’’ , off-channel scan will be done by RF ASIC.



VS



Cisco TAC Wireless

AP Join Issue

On WLC(*9K only):

Basic Log:

- **show tech-support wireless**
- show wireless states ap join summary
- show wireless states ap discovery
- show logging profile wireless filter mac <AP ethernet MAC address> to-file <file-name.txt>
- more bootflash: <file-name.txt>
- copy bootflash:<file-name.txt> tftp:<TFTP-server-IPaddress>
- WLC uplink packet capture

On AP:

Basic Log:

- **show tech-support**
- console log of at least one cycle of AP boot up till join WLC
- AP uplink packet capture

Cisco TAC Wireless

Client Connection Issue

On WLC（*9K only）:

Basic Log:

- **show tech-support wireless**
- show logging profile wireless start last 2 days trace-on-failure (* some low version branch like 16.x does not have the CLI.)
- clear paltform condition all
- debug wireless mac <client-MAC-address> (*recreate issue after enabling debug.)
- no debug wireless mac <client-MAC-address> (*Use this command to disable debug after collecting done.)
- more bootflash:copy-file-name-and-attach-here (*After collecting, WLC will save the log in bootflash with file name in format ‘ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log’)
- over-the-air packet capture:

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/80211/200527-Fundamentals-of-802-11-Wireless-Sniffing.html#anc36

On AP:

Basic Log:

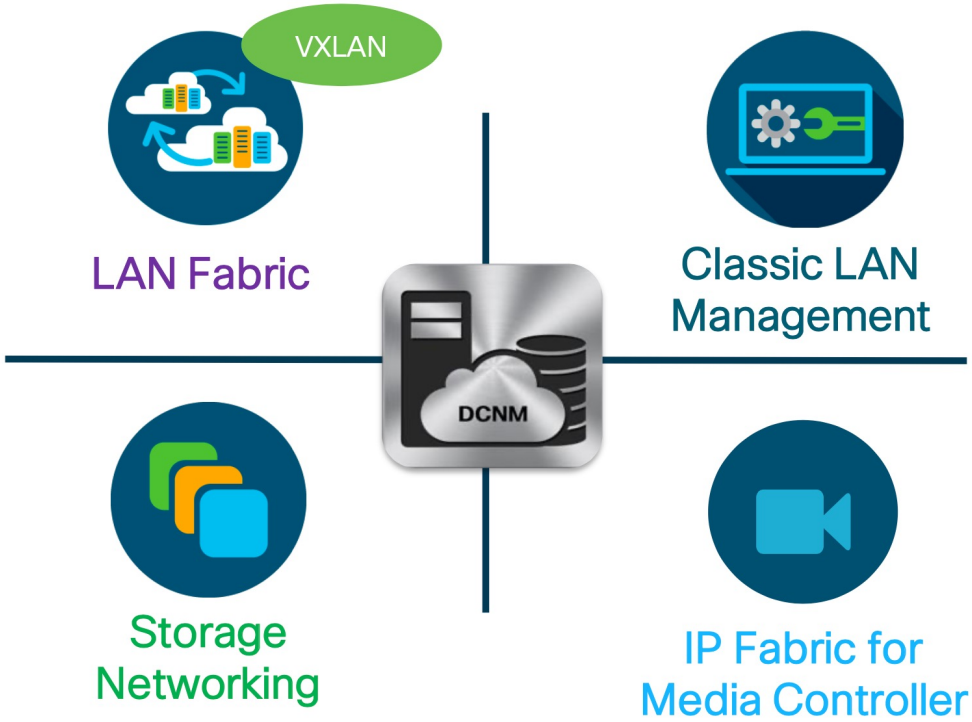
- **show tech-support**
- **show log**

Nexus- DCNM

Cisco TAC Nexus – DCNM

Data Center Network Manager (DCNM)

DCNM 10.x > DCNM 11.x > NDFC 12.x



Cisco TAC Nexus – DCNM

Automation

Visibility

Consistency

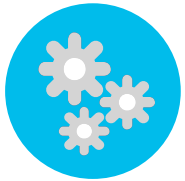
Inventory & Health

- Discovery & Fabric Builder
- CPU/Mem/Temp
- Traffic
- Health-Monitor
- Link View
- VM-connectivity

Configuration

- Image Management
- Backup / Restore
- Templates

Automation

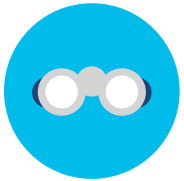


- VXLAN Fabric Builder
- Classic Underlay (POAP)
- Overlay (VRF/VNI)
- REST APIs

Trend Analysis and VM Analytics

- VM Net Trace
- Monitor Graphs
- Interface Monitoring

Host/Endpoint Monitoring



- VM Lifecycle
- Network Location
- Fabric-Wide View

Visualization and Troubleshooting

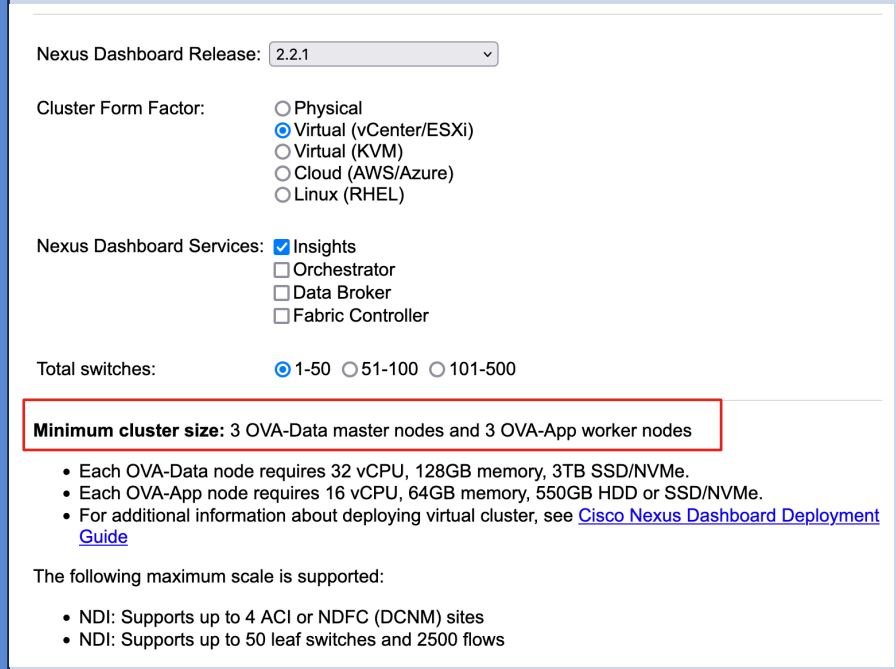
- Integrated Topology
- Search
- VXLAN-OAM

Cisco TAC Nexus – DCNM

• Nexus	• SSH to DCNM and Login as sysadmin or root (su root) • Appmgr tech-support • Appmgr backup / Appmgr –help ========== • SSH to ND with rescue-user (NDFC) • Acs techsupport collect -s cisco-ndfc (system) / acs -help • DCNM 11 Demos • https://blogs.cisco.com/datacenter/cisco-dcnm-demos-comprehensive-management-for-the-data-center • DCNM11 NIR & NIA Demo • https://video.cisco.com/video/6134793005001 • https://video.cisco.com/video/6134790957001 • Whats New in Cisco NDFC Release 12.0.1a • https://video.cisco.com/video/6277640922001 • Whats New in Cisco NDFC Release 12.1.1e (Latest version) • https://www.cisco.com/c/en/us/td/docs/dcn/ndfc/1211/videos/whats-new-in-ndfc-1211e.html

Cisco TAC Nexus – DCNM

- Nexus



Nexus Dashboard Capacity Planning

https://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/nd-sizing/index.html

ACI tech-support collection via Intersight Dashboard by TAC

- ACI Fabric controller/switch 외부 망 접속 가능 해야 함

  4.2 버전부터 intersight 연결 지원 됨

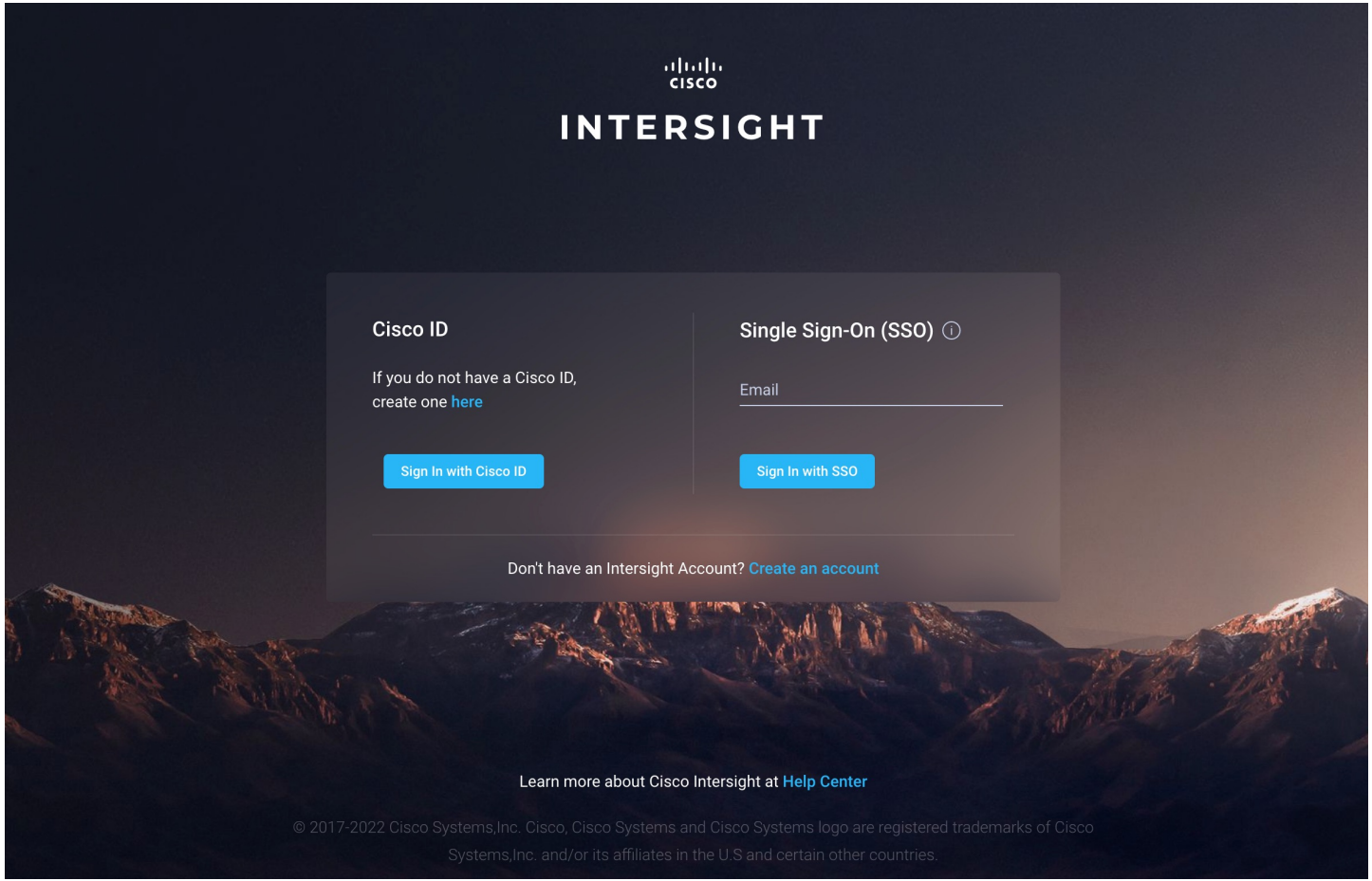
- Nexus Insight Cloud Connector App 설치

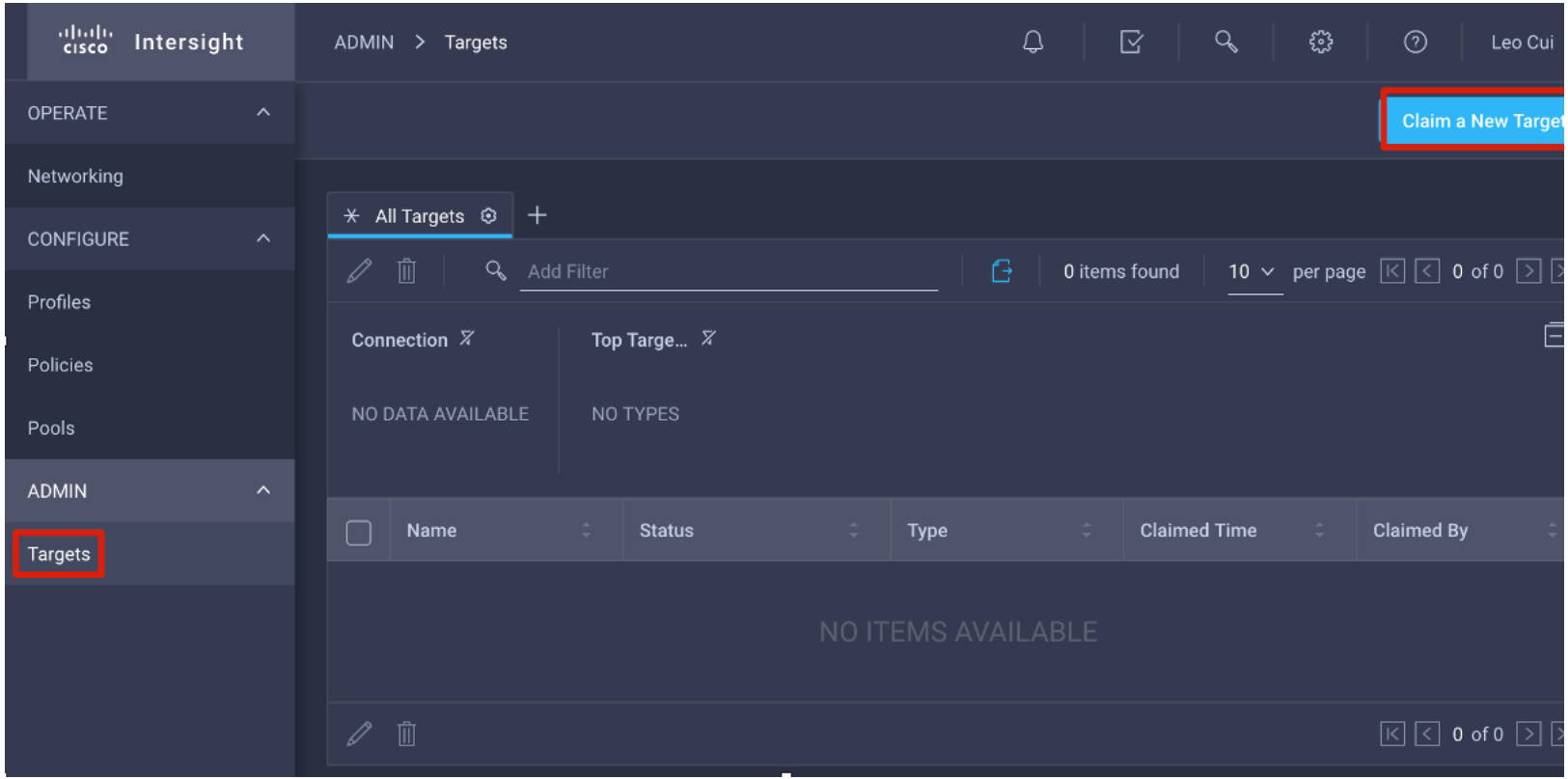
  https://dcappcenter.cisco.com/nexus-insights-cloud-connector.html

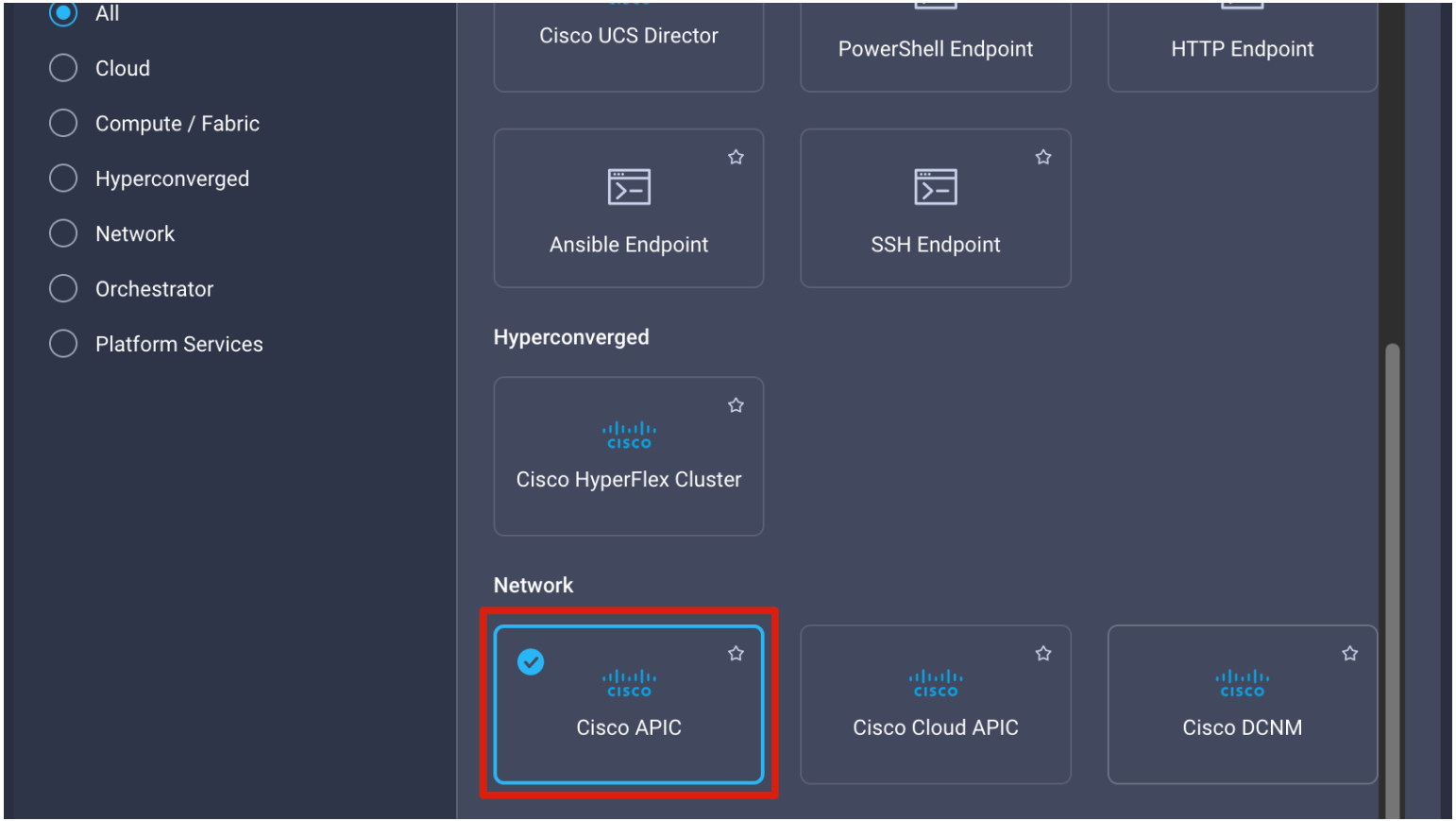
- Intersight dashboard site 접속

  https://www.intersight.com/an/dashboard

- SR case 필요 함


cisco
INTERSIGHT
Cisco ID
If you do not have a Cisco ID, create one here
Sign In with Cisco ID
Single Sign-On (SSO)
Email
Sign In with SSO
Don't have an Intersight Account? Create an account
Learn more about Cisco Intersight at Help Center
© 2017-2022 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc. and/or its affiliates in the U.S and certain other countries.


Intersight
ADMIN > Targets
Leo Cui
OPERATE
Networking
CONFIGURE
Profiles
Policies
Pools
ADMIN
Targets
Claim a New Target
All Targets
Add Filter
0 items found
10 per page
0 of 0
Connection
Top Targe...
NO DATA AVAILABLE
NO TYPES
Name
Status
Type
Claimed Time
Claimed By
NO ITEMS AVAILABLE
0 of 0


All
Cloud
Compute / Fabric
Hyperconverged
Network
Orchestrator
Platform Services
Cisco UCS Director
PowerShell Endpoint
HTTP Endpoint
Ansible Endpoint
SSH Endpoint
Hyperconverged
Cisco HyperFlex Cluster
Network
Cisco APIC
Cisco Cloud APIC
Cisco DCNM

Code and select the appropriate Resource Groups.

General

Device ID *

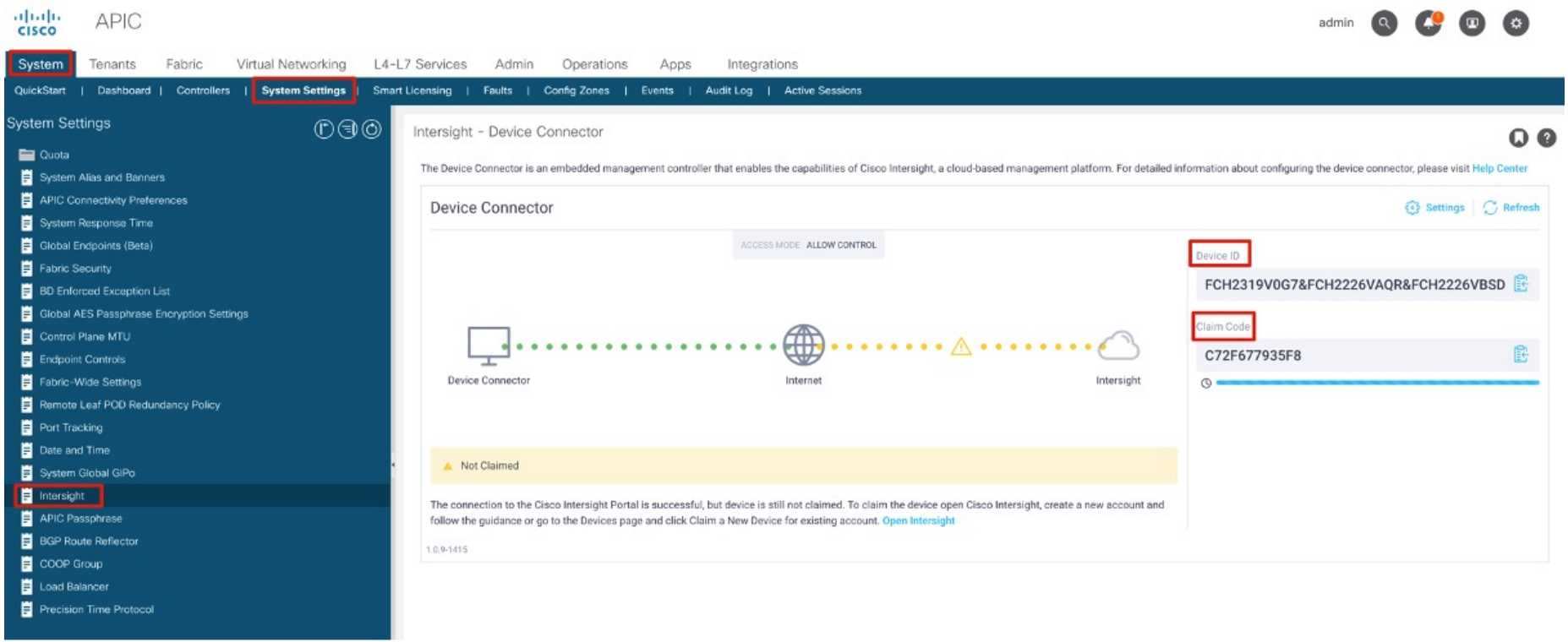
Claim Code *

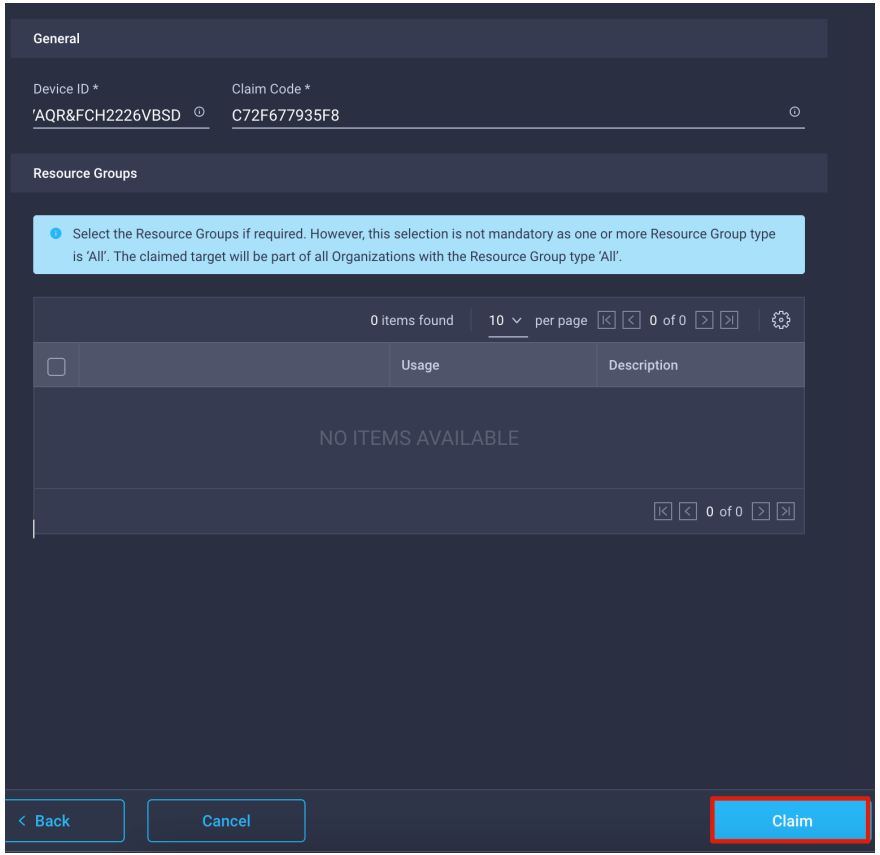
Resource Groups

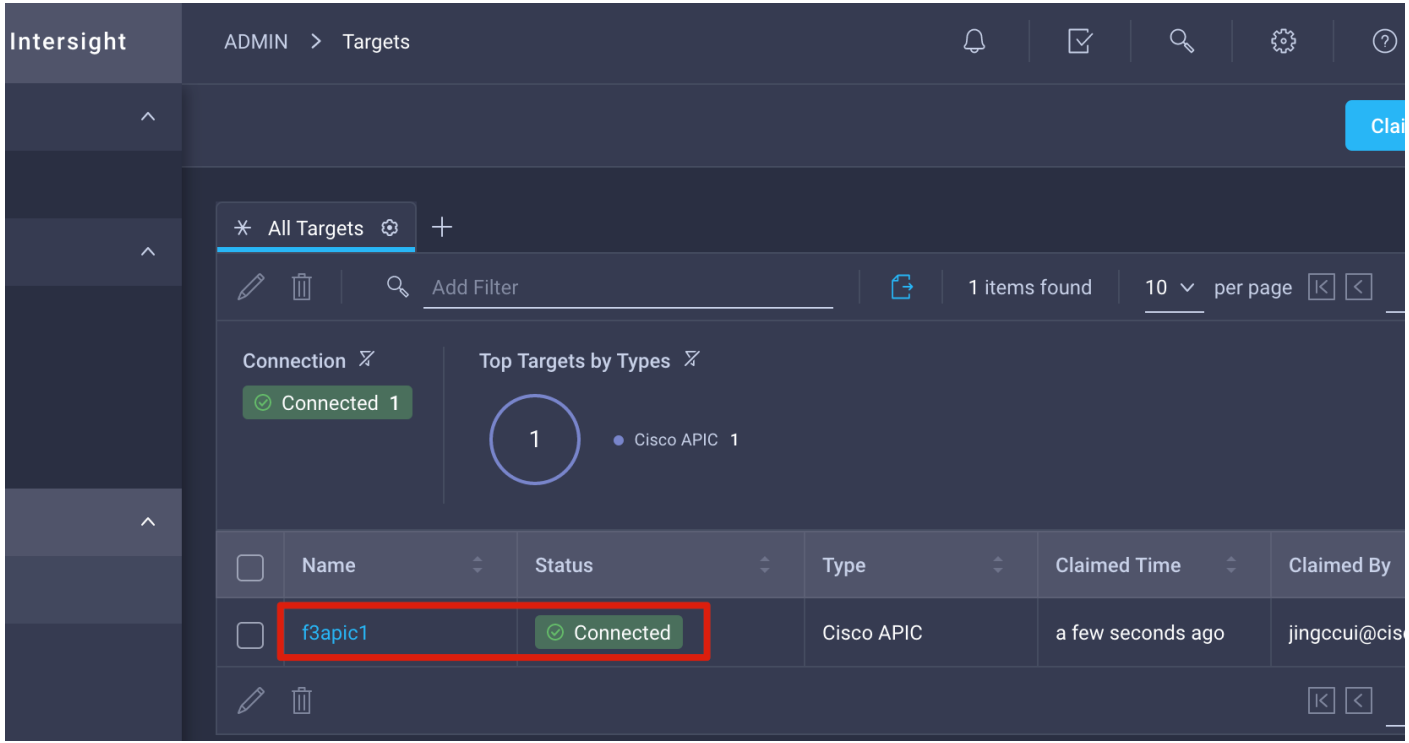
Select the Resource Groups if required. However, this selection is not mandatory as one or more Resource Group type is 'All'. The claimed target will be part of all Organizations with the Resource Group type 'All'.

0 items found | 10 per page | 0 of 0

	Usage	Description

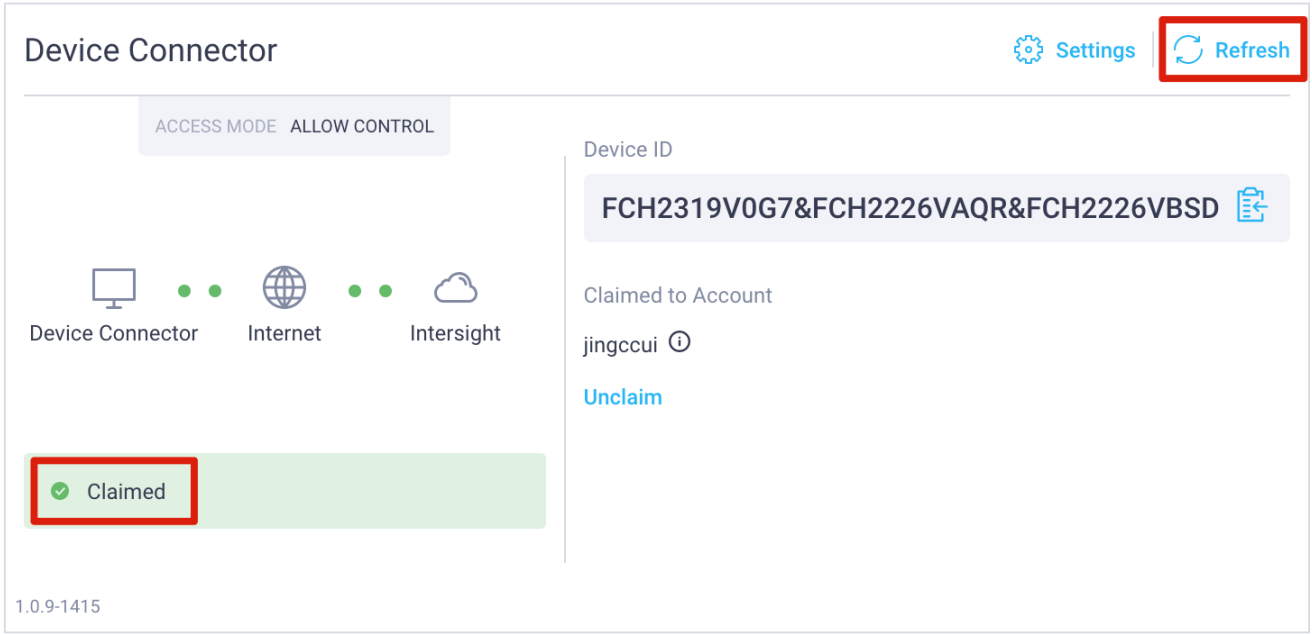

APIC
admin
System
Tenants
Fabric
Virtual Networking
L4-L7 Services
Admin
Operations
Apps
Integrations
QuickStart | Dashboard | Controllers | System Settings | Smart Licensing | Faults | Config Zones | Events | Audit Log | Active Sessions
System Settings
Quota
System Alias and Banners
APIC Connectivity Preferences
System Response Time
Global Endpoints (Beta)
Fabric Security
BD Enforced Exception List
Global AES Passphrase Encryption Settings
Control Plane MTU
Endpoint Controls
Fabric-Wide Settings
Remote Leaf POD Redundancy Policy
Port Tracking
Date and Time
System Global GIPo
Intersight
APIC Passphrase
BGP Route Reflector
COOP Group
Load Balancer
Precision Time Protocol
Intersight - Device Connector
The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, please visit Help Center
Device Connector
Settings
Refresh
ACCESS MODE: ALLOW CONTROL
Device Connector
Internet
Intersight
Not Claimed
The connection to the Cisco Intersight Portal is successful, but device is still not claimed. To claim the device open Cisco Intersight, create a new account and follow the guidance or go to the Devices page and click Claim a New Device for existing account. Open Intersight
1.0.9-1415
Device ID
FCH2319V0G7&FCH2226VAQR&FCH2226VBSD
Claim Code
C72F677935F8

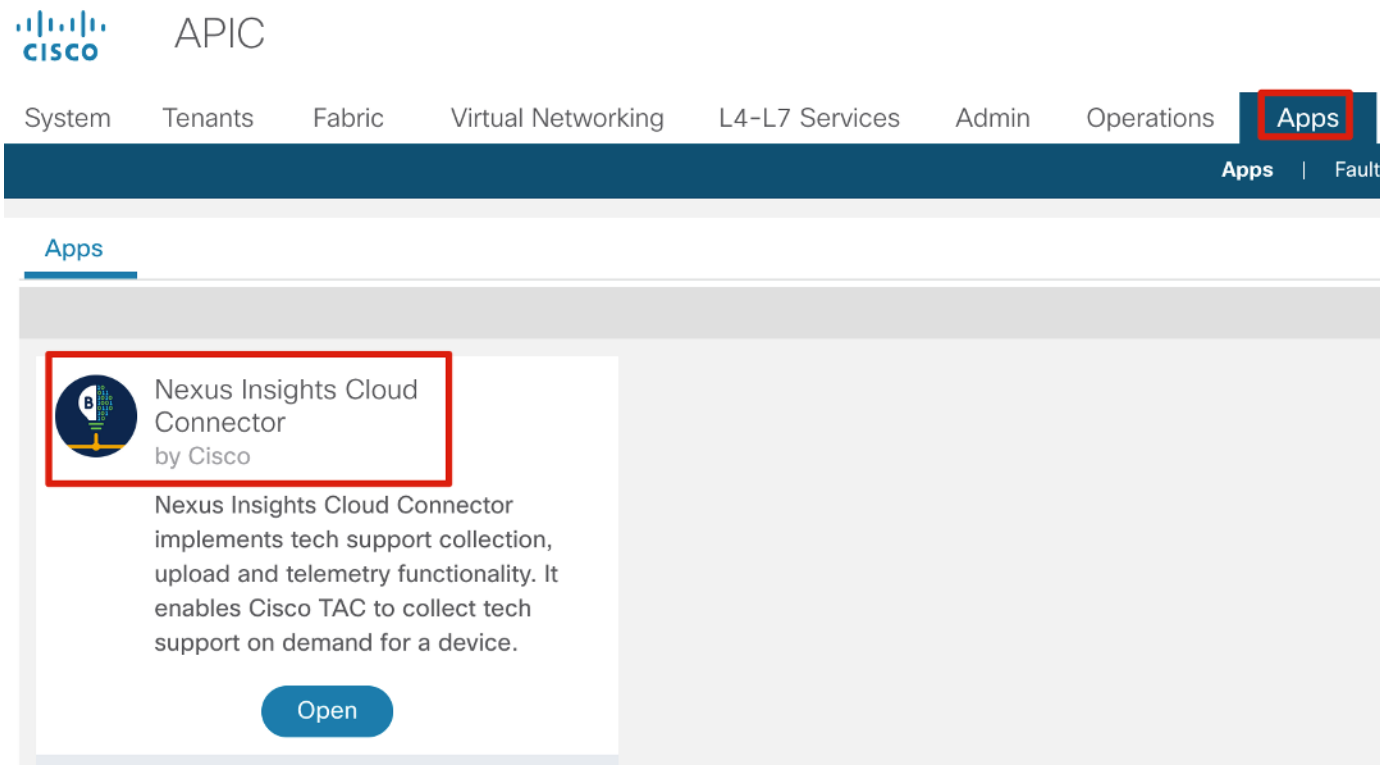

General
Device ID *
'AQR&FCH2226VBSD
Claim Code *
C72F677935F8
Resource Groups
Select the Resource Groups if required. However, this selection is not mandatory as one or more Resource Group type is 'All'. The claimed target will be part of all Organizations with the Resource Group type 'All'.
0 items found
10
per page
0 of 0
Usage
Description
NO ITEMS AVAILABLE
0 of 0
Back
Cancel
Claim

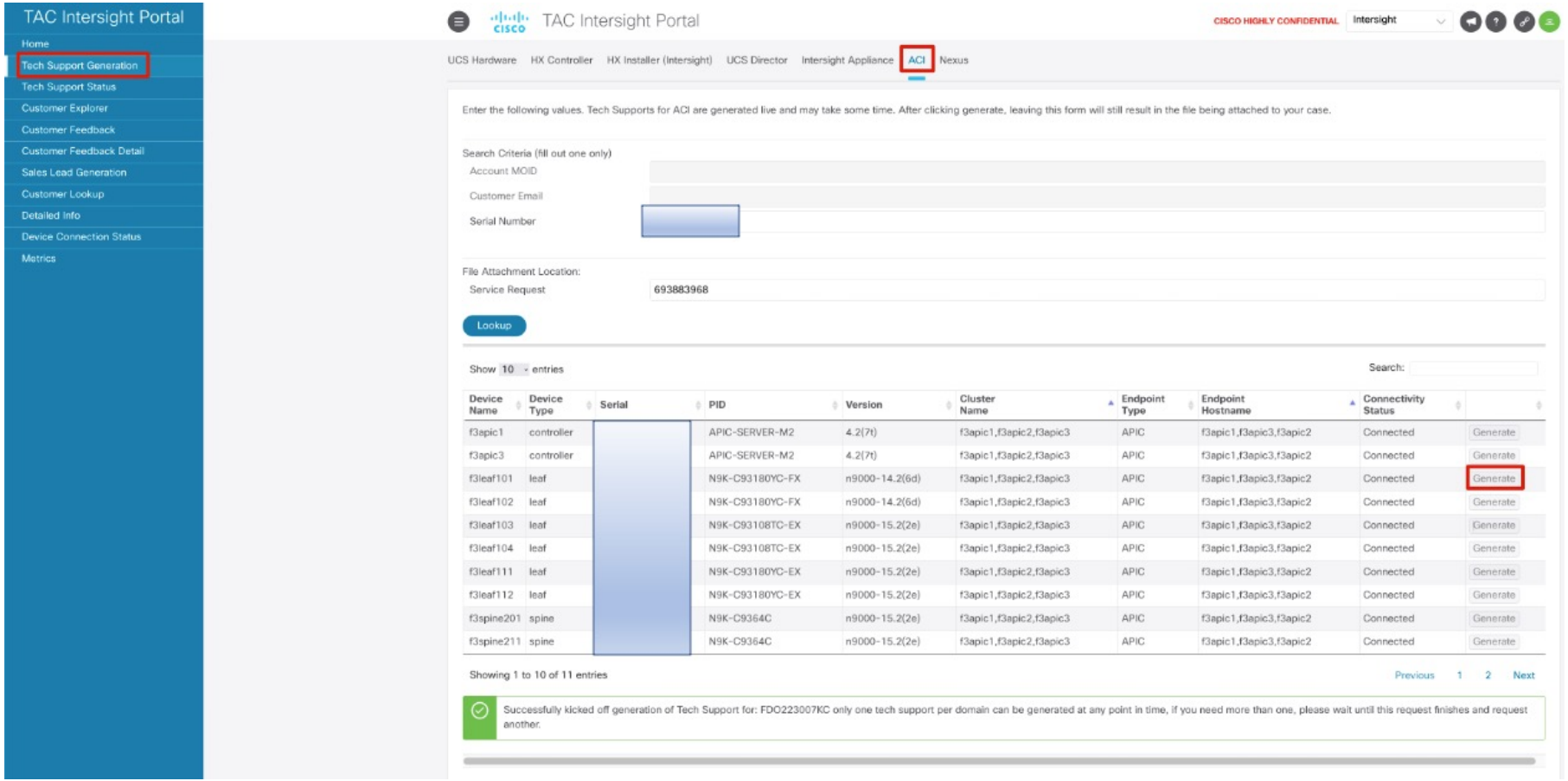

Intersight
ADMIN > Targets
All Targets
Add Filter
1 items found
10 per page
Connection
Connected 1
Top Targets by Types
1
Cisco APIC 1
Name
Status
Type
Claimed Time
Claimed By
f3apic1
Connected
Cisco APIC
a few seconds ago

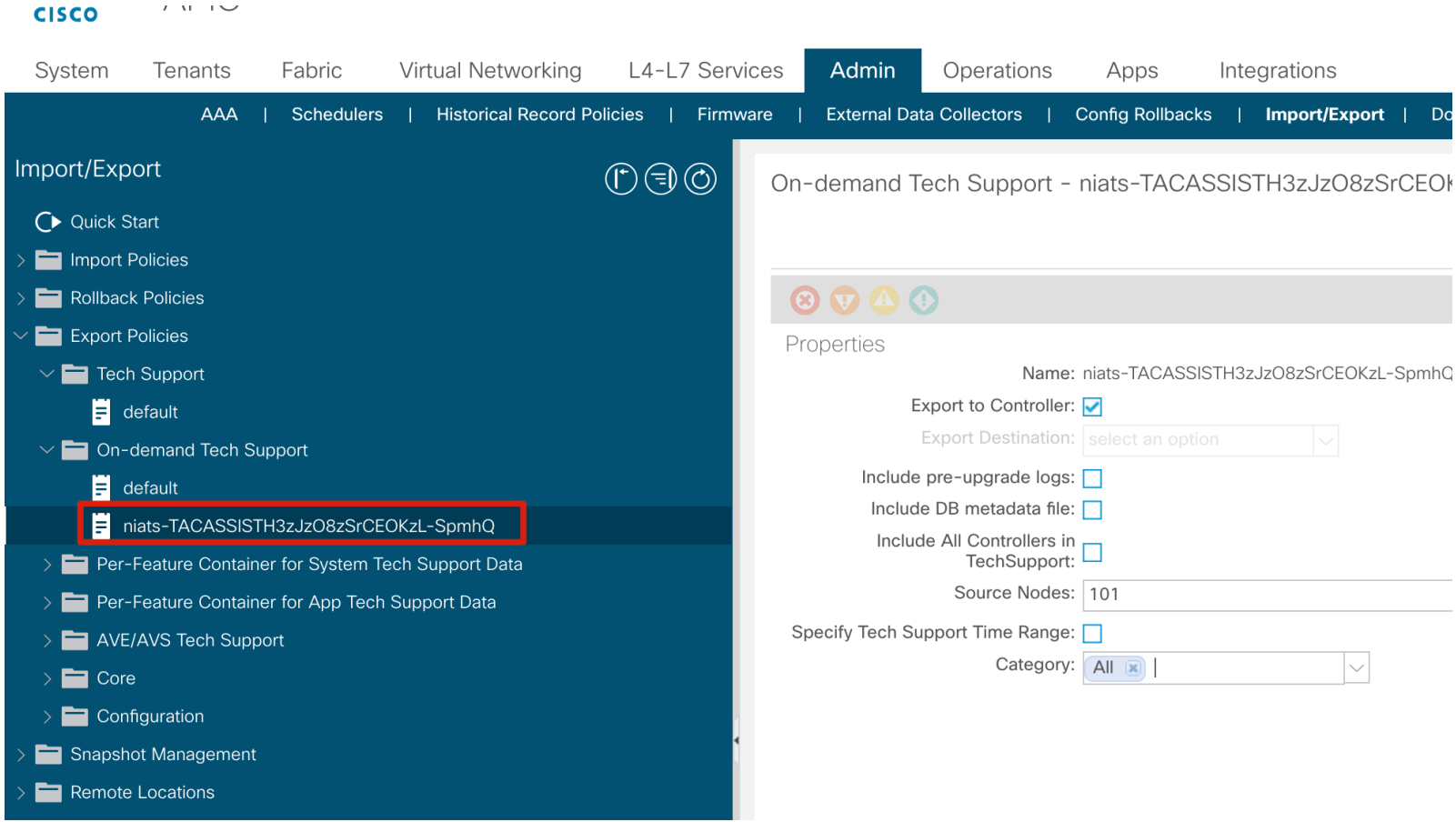
Intersight - Device Connector

The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, please visit Help Center




APIC
System
Tenants
Fabric
Virtual Networking
L4-L7 Services
Admin
Operations
Apps
Apps | Fault
Apps
Nexus Insights Cloud Connector
by Cisco
Nexus Insights Cloud Connector implements tech support collection, upload and telemetry functionality. It enables Cisco TAC to collect tech support on demand for a device.
Open


TAC Intersight Portal
Home
Tech Support Generation
Tech Support Status
Customer Explorer
Customer Feedback
Customer Feedback Detail
Sales Lead Generation
Customer Lookup
Detailed Info
Device Connection Status
Metrics
TAC Intersight Portal
CISCO HIGHLY CONFIDENTIAL
Intersight
UCS Hardware
HX Controller
HX Installer (Intersight)
UCS Director
Intersight Appliance
ACI
Nexus
Enter the following values. Tech Supports for ACI are generated live and may take some time. After clicking generate, leaving this form will still result in the file being attached to your case.
Search Criteria (fill out one only)
Account MOID
Customer Email
Serial Number
File Attachment Location:
Service Request
693883968
Lookup
Show 10 entries
Search:
Device Name
Device Type
Serial
PID
Version
Cluster Name
Endpoint Type
Endpoint Hostname
Connectivity Status
f3apic1 controller APIC-SERVER-M2 4.2(7t) f3apic1,f3apic2,f3apic3 APIC f3apic1,f3apic3,f3apic2 Connected Generate
f3apic3 controller APIC-SERVER-M2 4.2(7t) f3apic1,f3apic2,f3apic3 APIC f3apic1,f3apic3,f3apic2 Connected Generate
f3leaf101 leaf N9K-C93180YC-FX n9000-14.2(6d) f3apic1,f3apic2,f3apic3 APIC f3apic1,f3apic3,f3apic2 Connected Generate
f3leaf102 leaf N9K-C93180YC-FX n9000-14.2(6d) f3apic1,f3apic2,f3apic3 APIC f3apic1,f3apic3,f3apic2 Connected Generate
f3leaf103 leaf N9K-C93108TC-EX n9000-15.2(2e) f3apic1,f3apic2,f3apic3 APIC f3apic1,f3apic3,f3apic2 Connected Generate
f3leaf104 leaf N9K-C93108TC-EX n9000-15.2(2e) f3apic1,f3apic2,f3apic3 APIC f3apic1,f3apic3,f3apic2 Connected Generate
f3leaf111 leaf N9K-C93180YC-EX n9000-15.2(2e) f3apic1,f3apic2,f3apic3 APIC f3apic1,f3apic3,f3apic2 Connected Generate
f3leaf112 leaf N9K-C93180YC-EX n9000-15.2(2e) f3apic1,f3apic2,f3apic3 APIC f3apic1,f3apic3,f3apic2 Connected Generate
f3spine201 spine N9K-C9364C n9000-15.2(2e) f3apic1,f3apic2,f3apic3 APIC f3apic1,f3apic3,f3apic2 Connected Generate
f3spine211 spine N9K-C9364C n9000-15.2(2e) f3apic1,f3apic2,f3apic3 APIC f3apic1,f3apic3,f3apic2 Connected Generate
Showing 1 to 10 of 11 entries
Previous 1 2 Next
Successfully kicked off generation of Tech Support for: FDO223007KC only one tech support per domain can be generated at any point in time, if you need more than one, please wait until this request finishes and request another.


cisco
System
Tenants
Fabric
Virtual Networking
L4-L7 Services
Admin
Operations
Apps
Integrations
AAA
Schedulers
Historical Record Policies
Firmware
External Data Collectors
Config Rollbacks
Import/Export
Import/Export
Quick Start
Import Policies
Rollback Policies
Export Policies
Tech Support
default
On-demand Tech Support
default
niats-TACASSISTH3zJzO8zSrCEOKzL-SpmhQ
Per-Feature Container for System Tech Support Data
Per-Feature Container for App Tech Support Data
AVE/AVS Tech Support
Core
Configuration
Snapshot Management
Remote Locations
On-demand Tech Support - niats-TACASSISTH3zJzO8zSrCEOK
Properties
Name: niats-TACASSISTH3zJzO8zSrCEOKzL-SpmhQ
Export to Controller:
Export Destination: select an option
Include pre-upgrade logs:
Include DB metadata file:
Include All Controllers in TechSupport:
Source Nodes: 101
Specify Tech Support Time Range:
Category: All

FAQ

Q1: What does it mean to be 'claimed' in intersight?

A: "claimed" means that a customer has gone into intersight and claimed ownership of the device.

During this process, the end user accepts a EULA(End User License Agreement)
which gives us permission to pull the tech supports.

Q2: Are customers notified when tech supports are generated?

A: No, customers have signed a EULA allowing us to generate their tech support, no notification

Q3: Security Concern

A: It can only collect techsupport.
From customer side, they can unclaim the Intersight Connect after TS files had been collected

Q4: How to clean collected tech support files?

A: There's an auto delete policy. the techsupport files will get removed after a threshold
(90% of filesystem usage)
Or delete manually. File Path: "/data2/logs/Cisco_NIBASE/techsup"

Thank you