Security Cloud Control: Navigating Through Onboarding & Event Logging Challenges

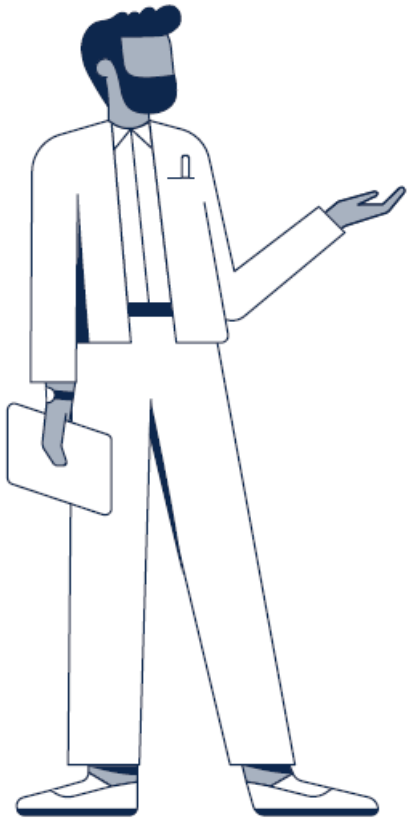
Leonel Matus Climaco
Cloud Security Escalation Engineer

Bashar Alsaeed
Cloud Security Engineer

Session ID: TACSEC-2021

June 2025

Agenda



01 Security Cloud Control

02 ASA Onboarding & Troubleshooting

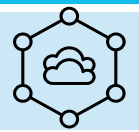
03 FTD Onboarding & Troubleshooting

04 Troubleshooting Event Logging

05 Q&A

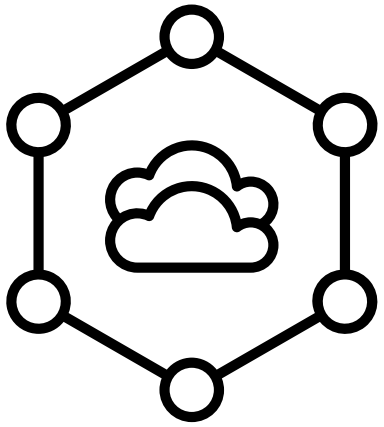
Security Cloud Control

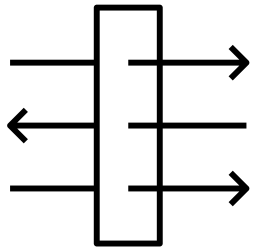
Acronyms Directory

Acronym	Full Term	Icon
SCC	Security Cloud Control	
SDC	Secure Device Connector	
SSX	Security Service Exchange	
cdFMC	Cloud-delivered Firewall Management Center	
FMC	Firewall Management Center	
FTD	Secure Firewall Threat Defense	
ASA	Adaptive Security Appliance	
GUI	Graphical User Interface	

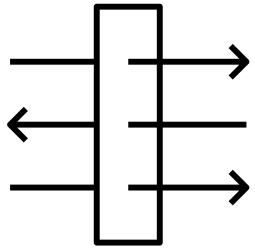
Security Cloud Control

Cloud-based multi-device on-boarding technology that enables security devices in distributed environments to achieve centralized device administration





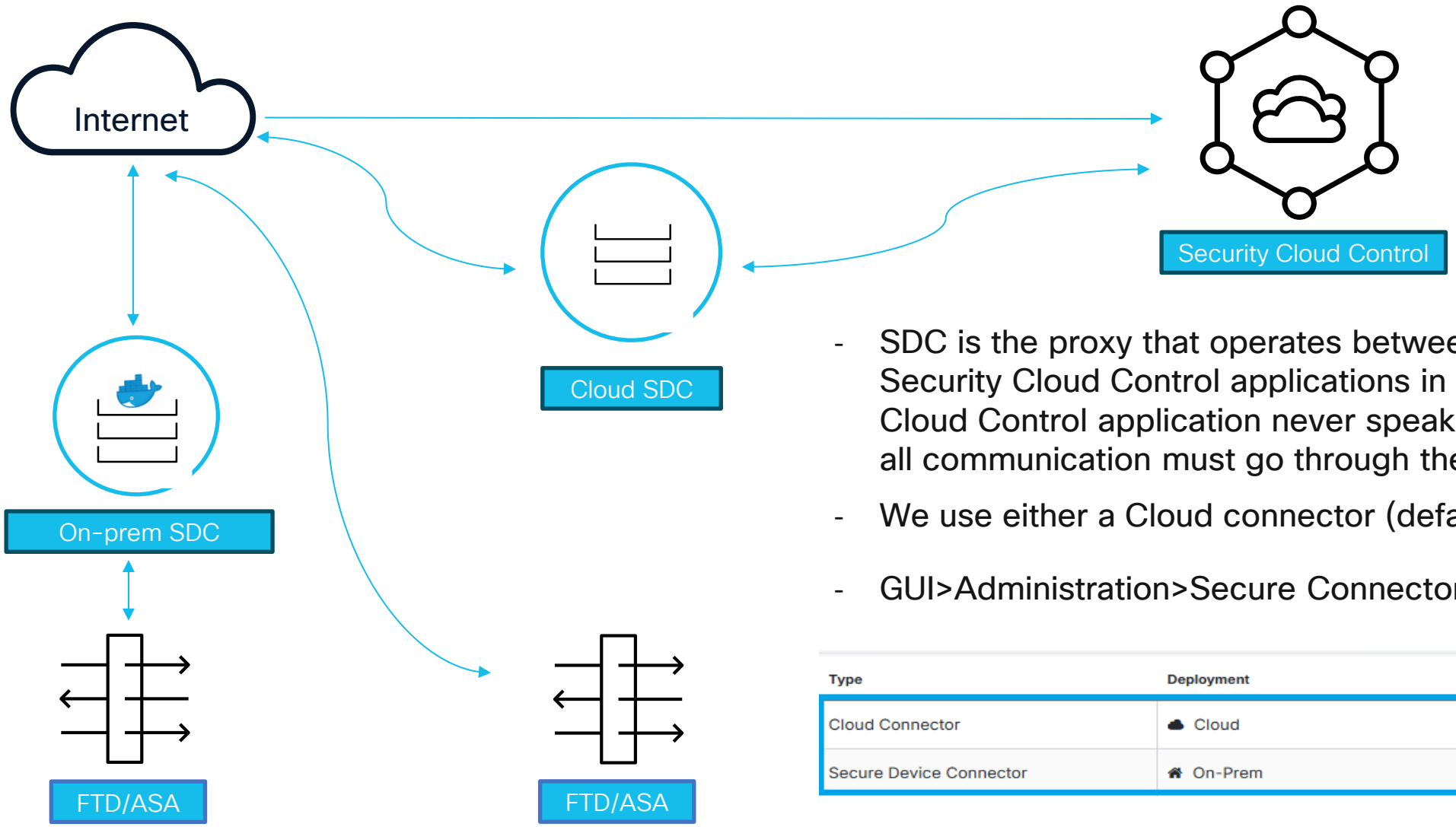
ASA



FTD

- Cisco IOS devices
- ASA (On-prem & Virtual)
- FTD (On-prem & Virtual)
- Cisco Meraki™ Organizations
- Umbrella Networks (Tunnel)
- AWS Virtual Private Clouds

Security Cloud Control Devices Onboarding Routes



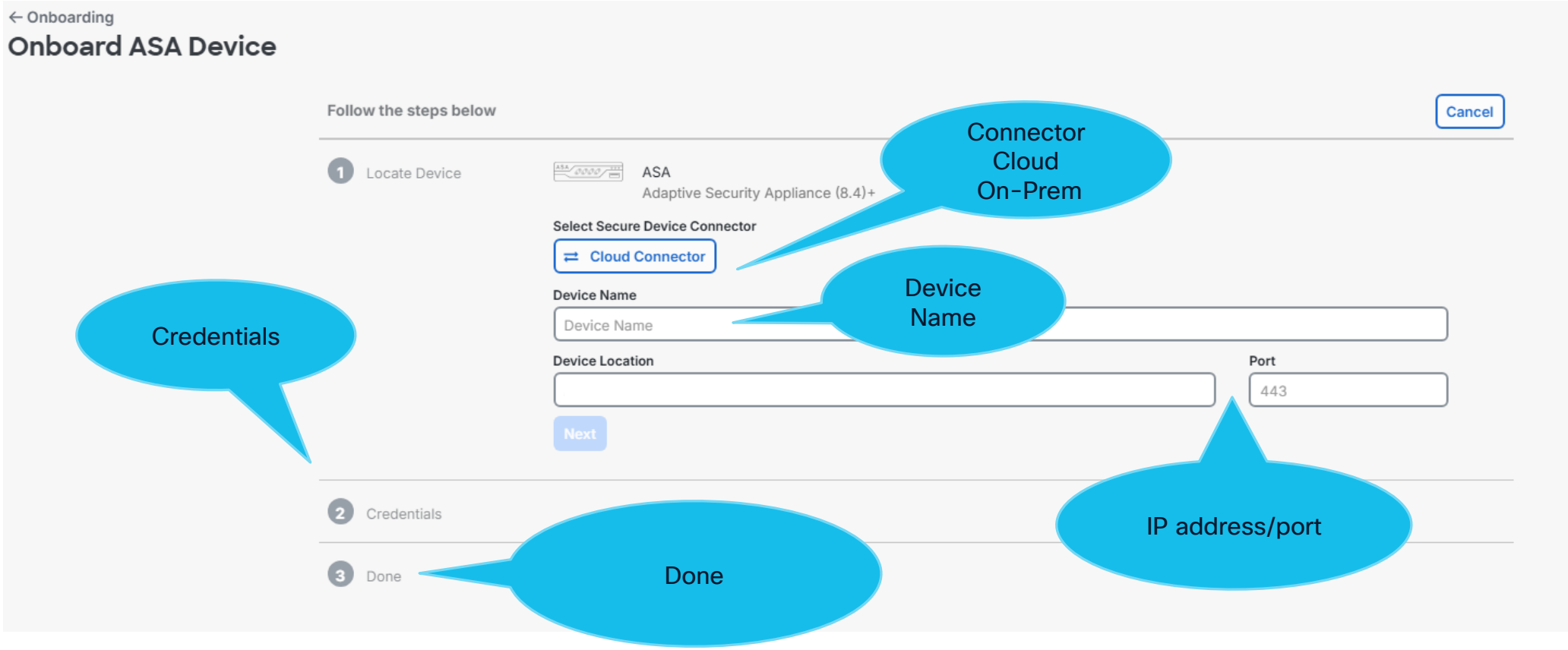
- SDC is the proxy that operates between the devices and the Security Cloud Control applications in the cloud (The Security Cloud Control application never speaks directly to the devices all communication must go through the SDC)
- We use either a Cloud connector (default) or an On-prem SDC
- GUI>Administration>Secure Connectors

Type	Deployment	Status
Cloud Connector	Cloud	Active
Secure Device Connector	On-Prem	Active

ASA Onboarding

Onboard ASA Device to Security Cloud Control

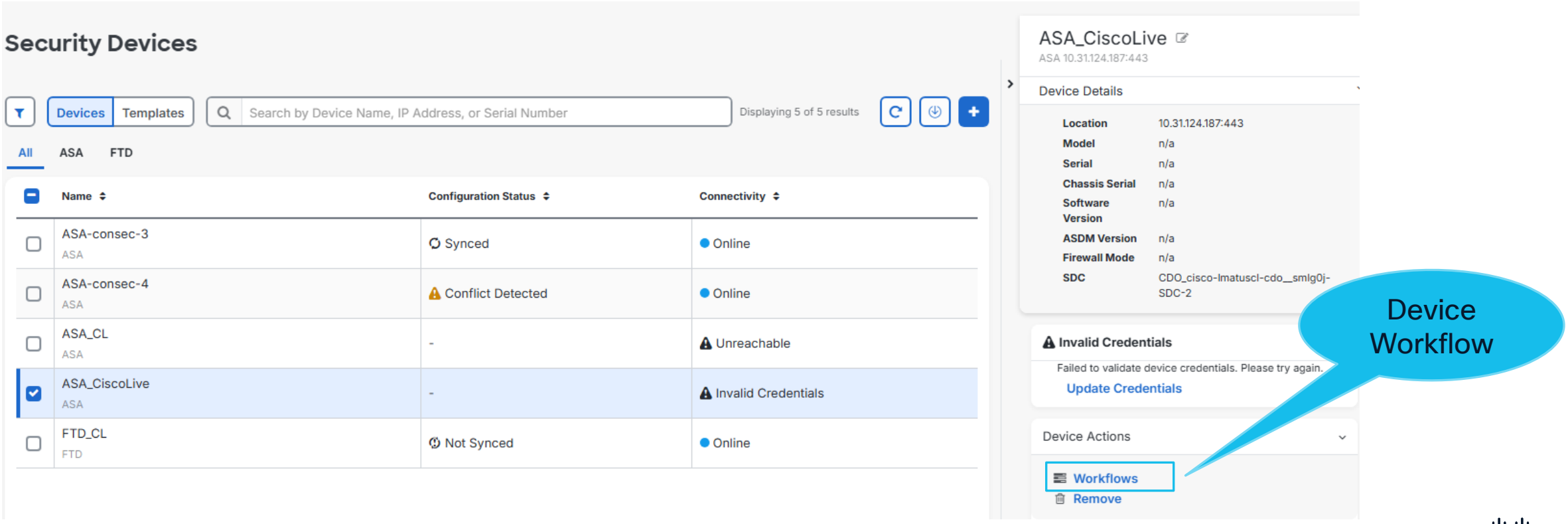
- GUI> Security Devices> Onboard device or service> ASA



ASA Onboarding Troubleshooting

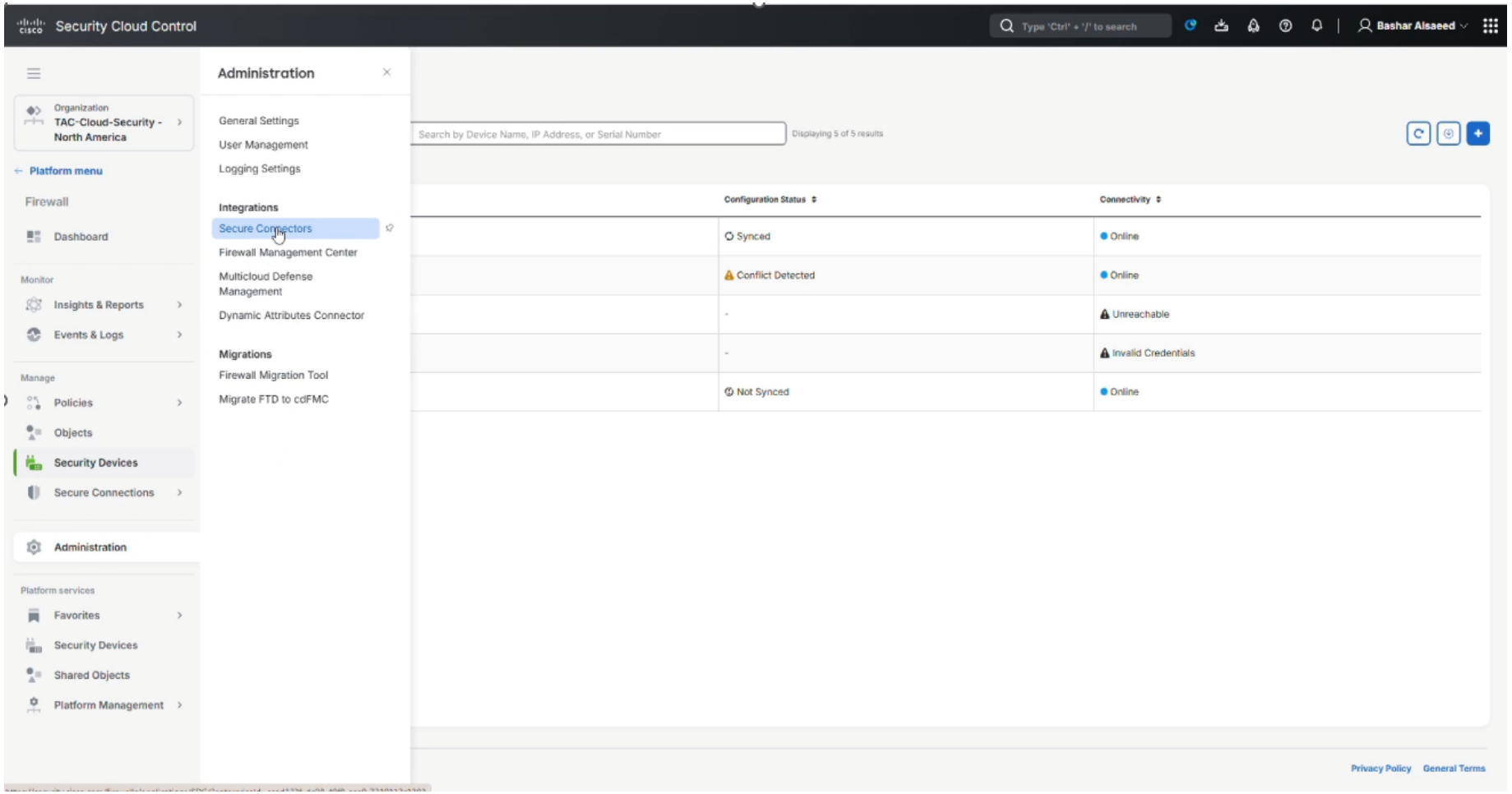
Troubleshooting Skills Checklist

- Make sure device is compatible with Security Cloud Control
- The device must meet the prerequisites outlined in the onboarding guides
- Check Workflows logs to see which job failed while onboarding



Onboarding Skills Checklist (Continued)

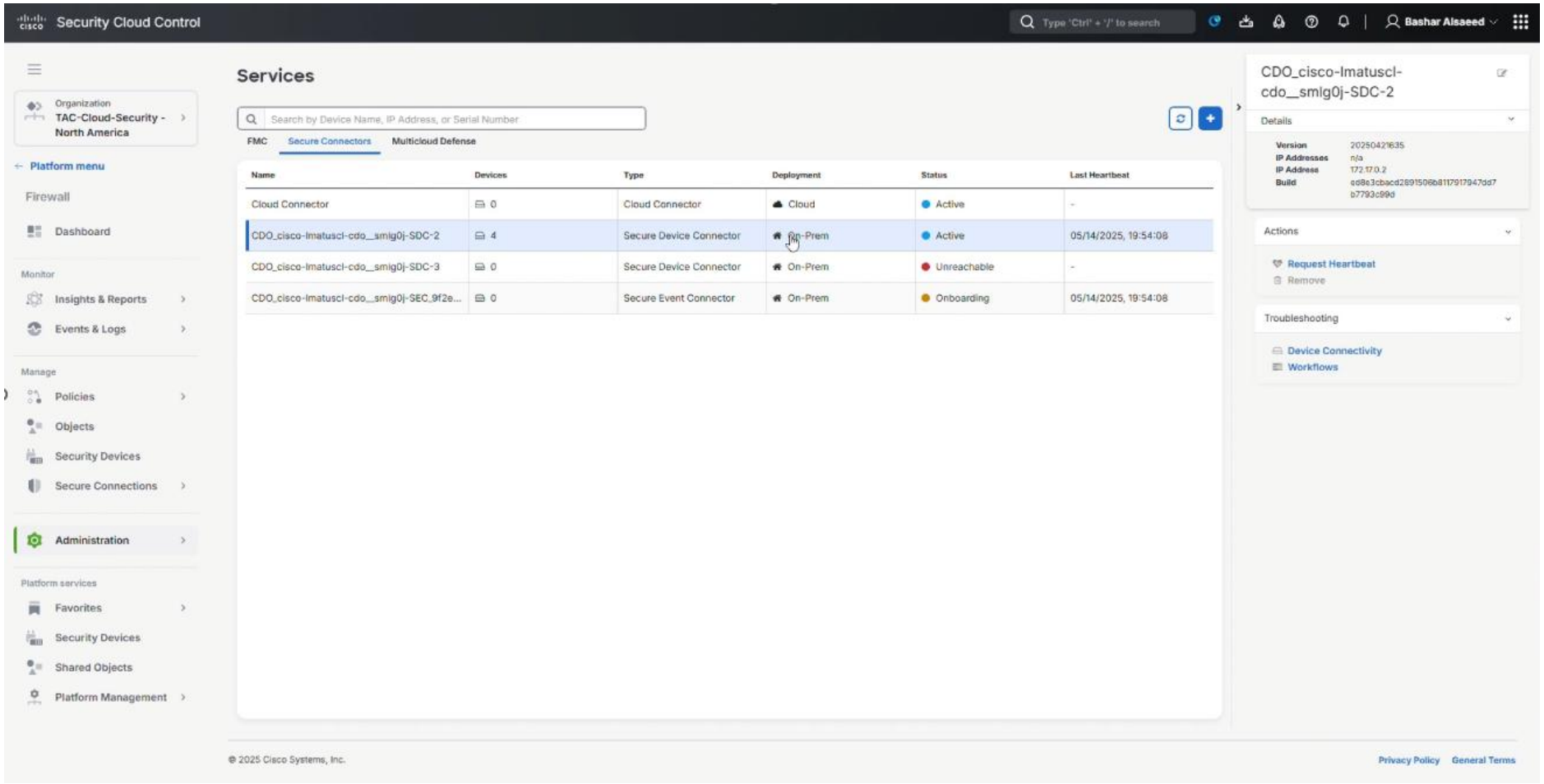
- Verify connectivity using Security Cloud Control ”Device Connectivity” tool
- Demo:



https://docs.defenseorchestrator.com/#!t-troubleshoot-device-connectivity-with-SDC.html

Onboarding Skills Checklist (Continued)

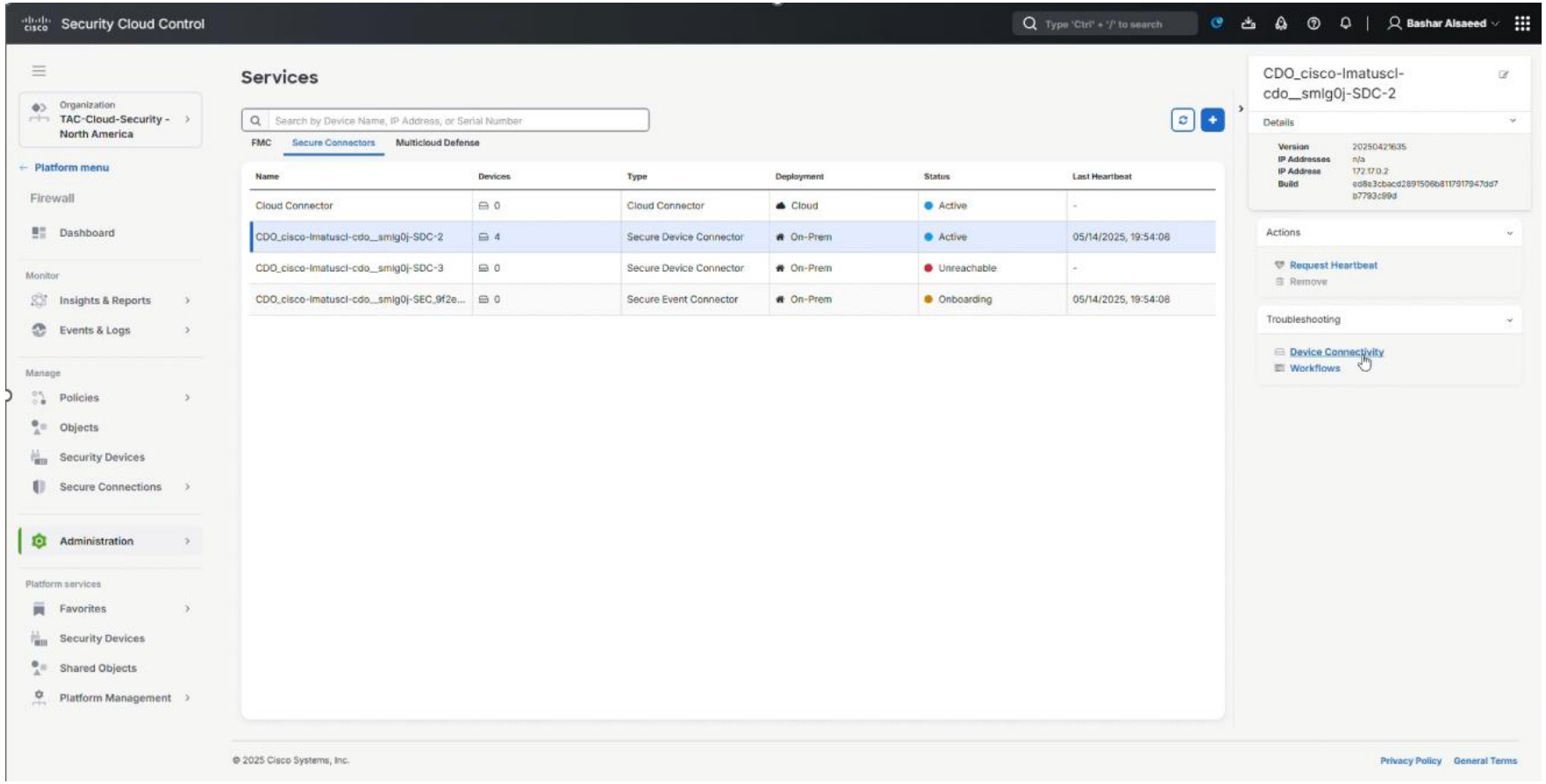
- Verify connectivity using Security Cloud Control ”Device Connectivity” tool
- Demo:



https://docs.defenseorchestrator.com/#!t-troubleshoot-device-connectivity-with-SDC.html

Onboarding Skills Checklist (Continued)

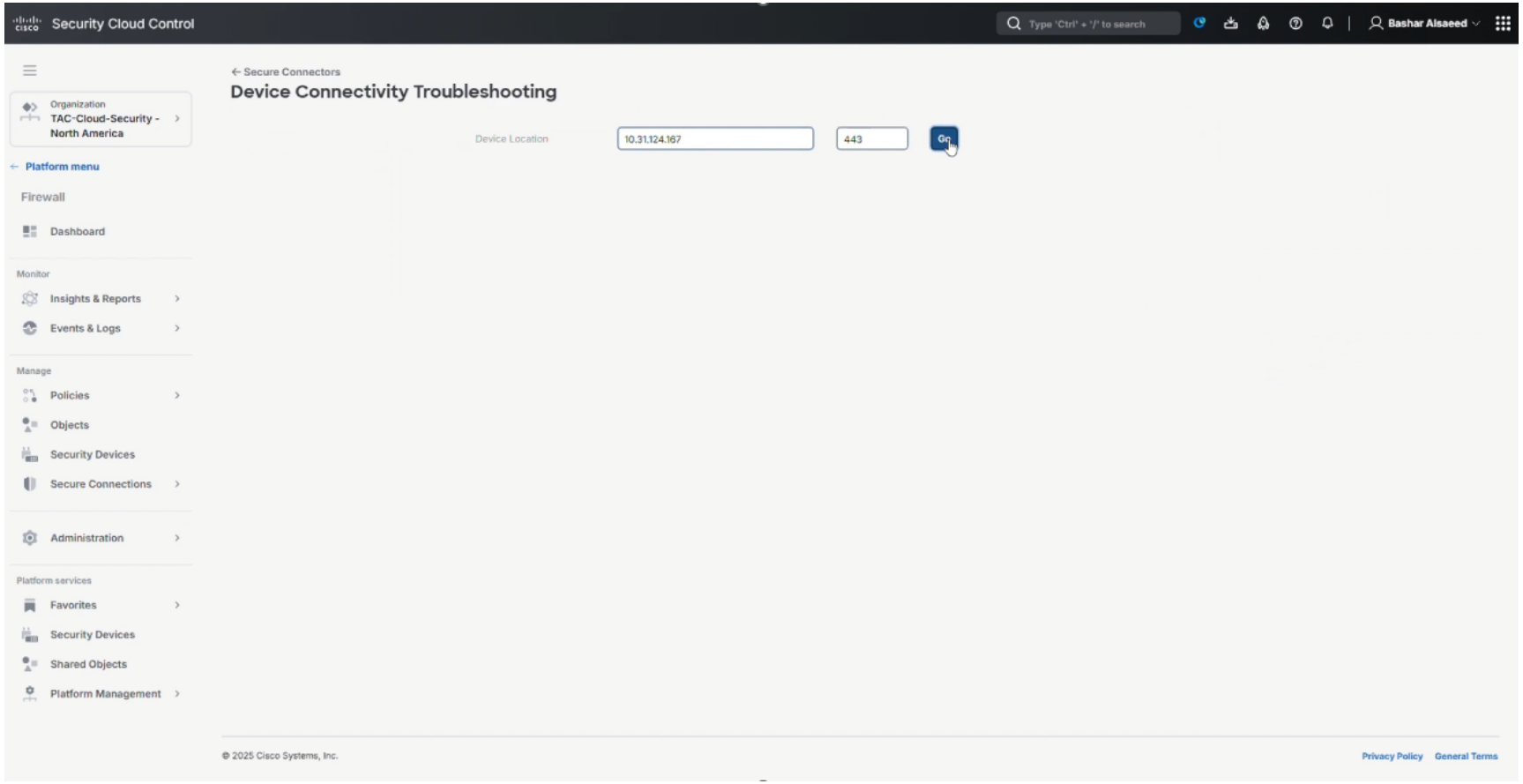
- Verify connectivity using Security Cloud Control ”Device Connectivity” tool
- Demo:



https://docs.defenseorchestrator.com/#!t-troubleshoot-device-connectivity-with-SDC.html

Onboarding Skills Checklist (Continued)

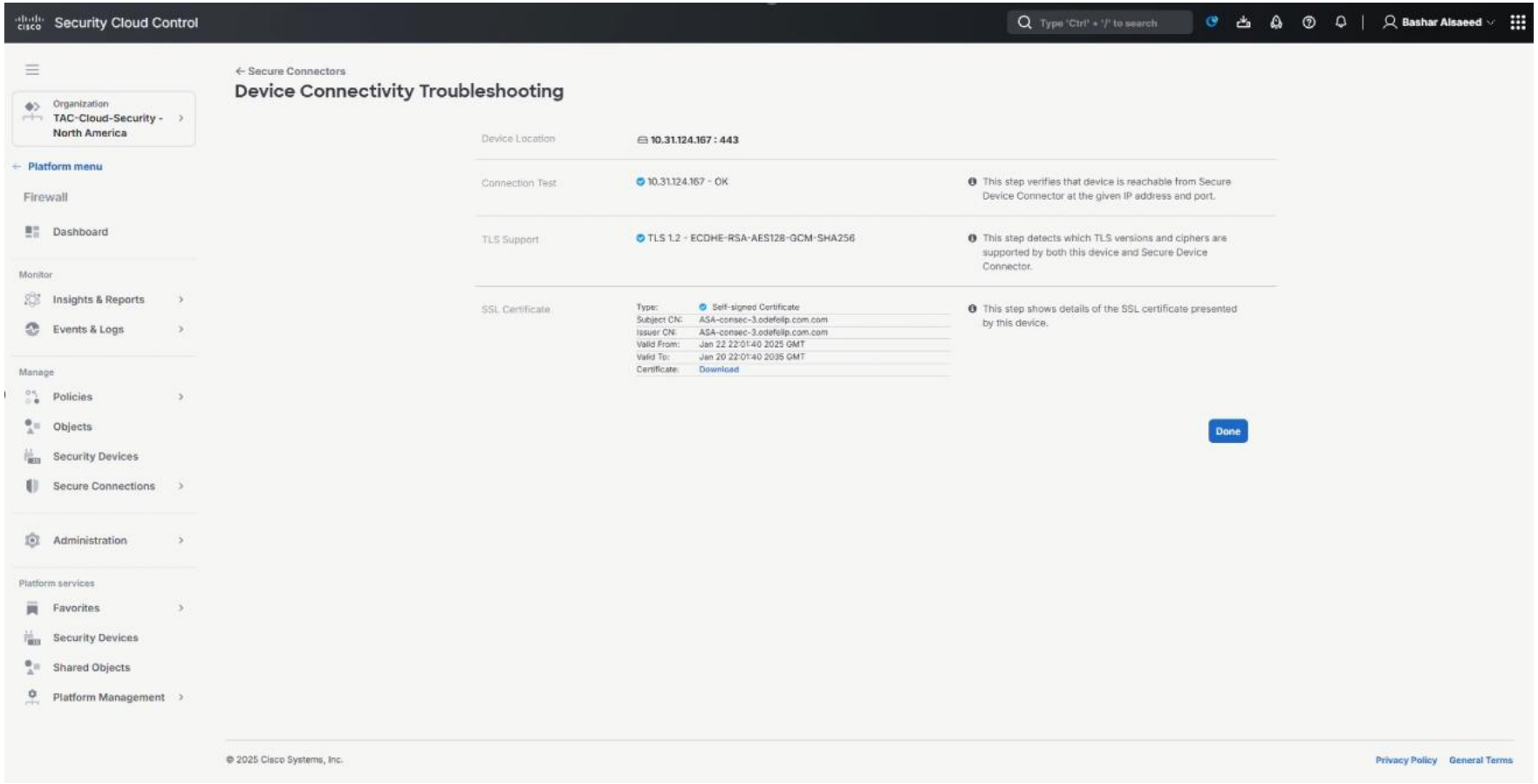
- Verify connectivity using Security Cloud Control ”Device Connectivity” tool
- Demo:



https://docs.defenseorchestrator.com/#!t-troubleshoot-device-connectivity-with-SDC.html

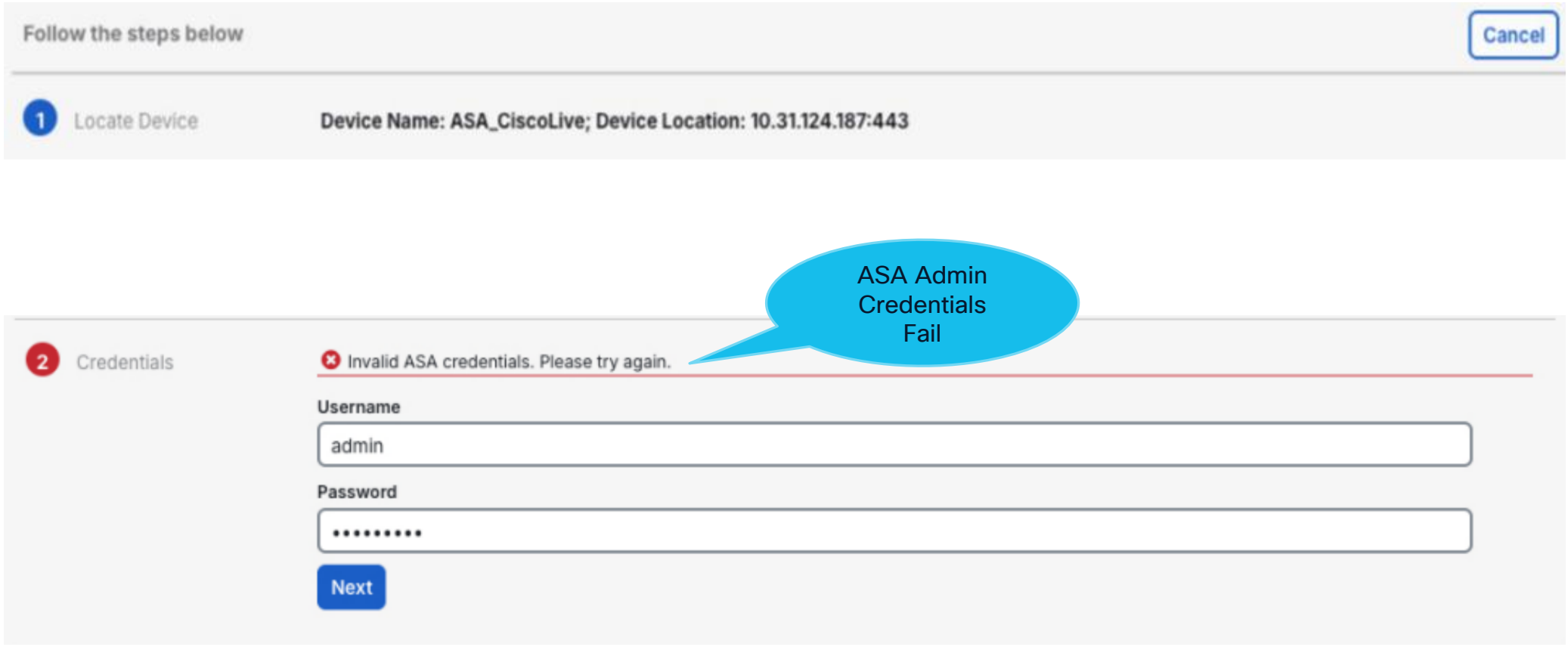
Onboarding Skills Checklist (Continued)

- Verify connectivity using Security Cloud Control ”Device Connectivity” tool
- Demo:



https://docs.defenseorchestrator.com/#!t-troubleshoot-device-connectivity-with-SDC.html

ASA Onboarding Failure to Security Cloud Control



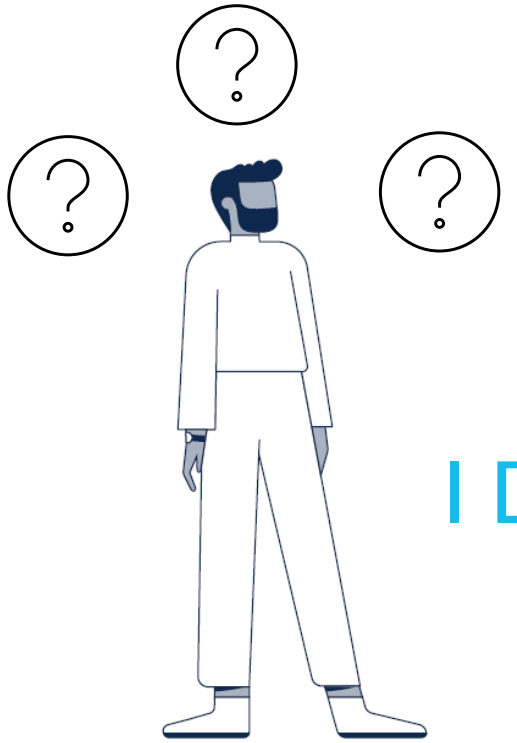
Let's Troubleshoot

Compatibility

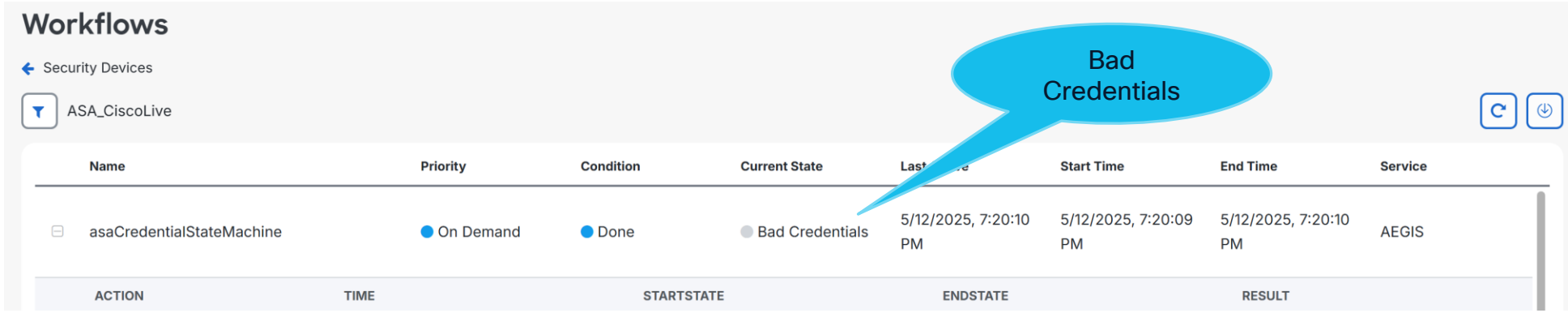
Prerequisites

Connectivity

Workflows



I Did My Homework!



Troubleshooting (Continued)

- ASAs support credential-based authentication as well as client-side certificate authentication

- CiscoLive-ASA# show run | include ssl

```
ssl certificate-authentication interface <interface> port 443
vpn-tunnel-protocol ssl-client
vpn-tunnel-protocol ssl-client
anyconnect ssl rekey time 4
anyconnect ssl rekey method new-tunnel
```

Client-Side Certificate Configured

- CiscoLive-ASA# show logging | include certificates

```
%ASA-7-725017: No certificates received during the handshake with client <interface>
:10.31.124.190/46088 to 10.31.124.187/443 for TLSv1.3 session
```

Certificate Exchange Failure

Root Cause and The Resolution

- ASA has been configured to utilize client-side certificate authentication
- Unfortunately, the Security Cloud Control does not support client-side certificate authentication
- Resolution: Disable client-side certificate authentication from the ASA side
- Procedure:

Step 1: Open a terminal window and connect to the ASA using SSH

Step 2: Enter global configuration mode

```
CiscoLive-ASA# configure terminal
```

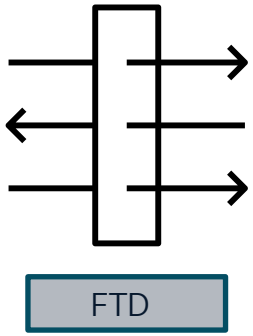
Step 3: Enter the below command:

```
CiscoLive-ASA (config)# no ssl certificate-authentication interface <interface> port 443
```

FTD Onboarding

Onboard FTD to Cloud-delivered Firewall Management Center

Port	Protocol / Feature	Details
8305/tcp	Appliance communications	• Securely communicate between appliances in a deployment.
443	HTTPS	• Send and receive data from the internet. • Communicate with the AMP cloud (public or private)



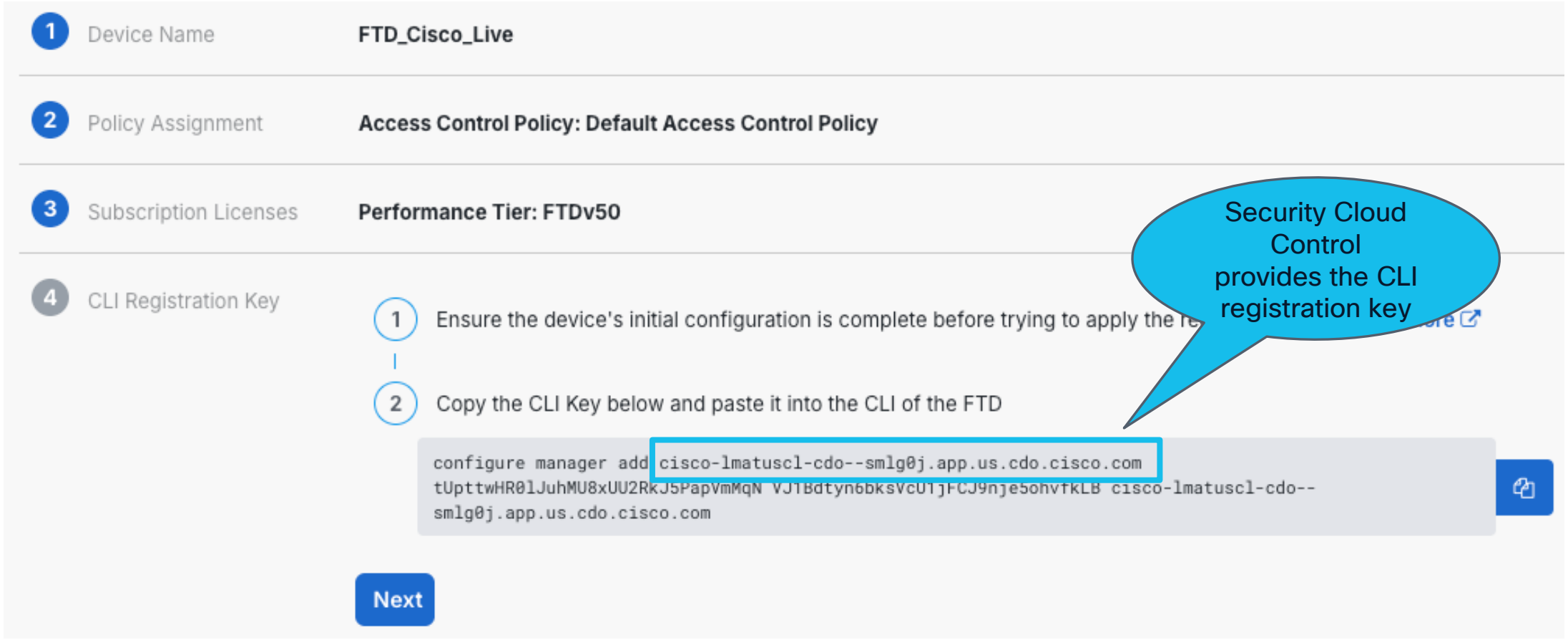
- You must ensure that the threat defense device ports have external and outbound access for the cloud-delivered Firewall Management Center.

Learn how to onboard FTD to cdFMC

Prerequisites

FTD Onboarding Troubleshooting

cdFMC Registration Key



FTD Cannot Establish Sftunnel with cdFMC

Resolve the cdFMC FQDN to identify the public IP address

FTD Expert Mode ~$:

```
admin@user-ftd:~$ nslookup cisco-test-cdo--smlg0j.app.us.cdo.cisco.com
Server: 10.0.0.5
Address: 10.0.0.5#53


Non-authoritative answer:
Name: cisco-test-cdo--smlg0j.app.us.cdo.cisco.com
Address: 44.243.34.123
```

You can collect a packet capture on the FTD adjacent device.

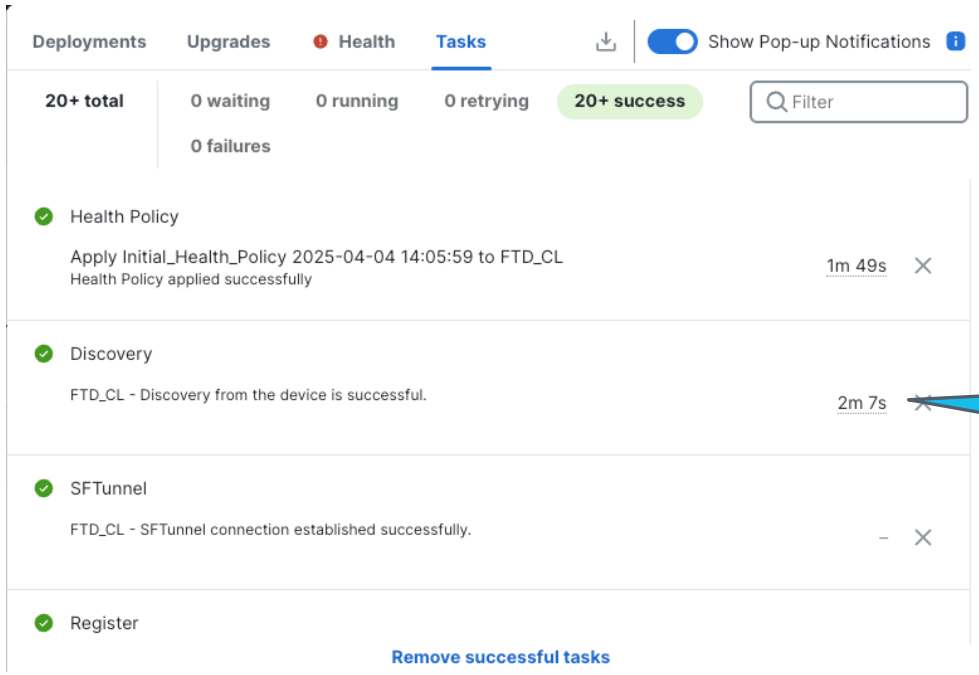
No.	Ti	Source	Destination	Proto	Le	Info
6	…	172.18.0.4	44.243.34.123	TCP	…	59099 → 8305 [SYN] Seq=0 Win=64240 Len=
7	…	172.18.0.4	44.243.34.123	TCP	…	[TCP Retransmission] 59099 → 8305 [SYN]
8	…	172.18.0.4	44.243.34.123	TCP	…	[TCP Retransmission] 59099 → 8305 [SYN]
9	…	172.18.0.4	44.243.34.123	TCP	…	[TCP Retransmission] 59099 → 8305 [SYN]
10	…	172.18.0.4	44.243.34.123	TCP	…	[TCP Retransmission] 59099 → 8305 [SYN]

FTD Successfully Onboarded

Collect a packet capture on the FTD management interface.

No.	Source	Destination	Protc	Le	Info
3	172.18.0.4	44.243.34.123	TCP	…	35123 → 8305 [SYN Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=506039641 TSecr=0 WS=128
4	44.243.34.123	172.18.0.4	TCP	…	8305 → 35123 [SYN ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1084691514 TSecr=506039641 WS=
5	172.18.0.4	44.243.34.123	TCP	…	35123 → 8305 [ACK Seq=1 Ack=1 Win=64256 Len=0 TSval=506039719 TSecr=1084691514
6	172.18.0.4	44.243.34.123	TL…	…	Client Hello
7	44.243.34.123	172.18.0.4	TCP	…	8305 → 35123 [ACK Seq=1 Ack=322 Win=64896 … 1084691593 TSecr=506039720
8	44.243.34.123	172.18.0.4	TL…	…	Server Hello, Change … ata, Application Data, Application Data
9	172.18.0.4	44.243.34.123	TCP	…	35123 → 8305 [ACK Seq=322 Ack … TSecr=1084691598
10	172.18.0.4	44.243.34.123	TL…	…	Change Cipher Spec, Applicatio
11	172.18.0.4	44.243.34.123	TL…	…	Application Data
12	44.243.34.123	172.18.0.4	TL	…	Application Data

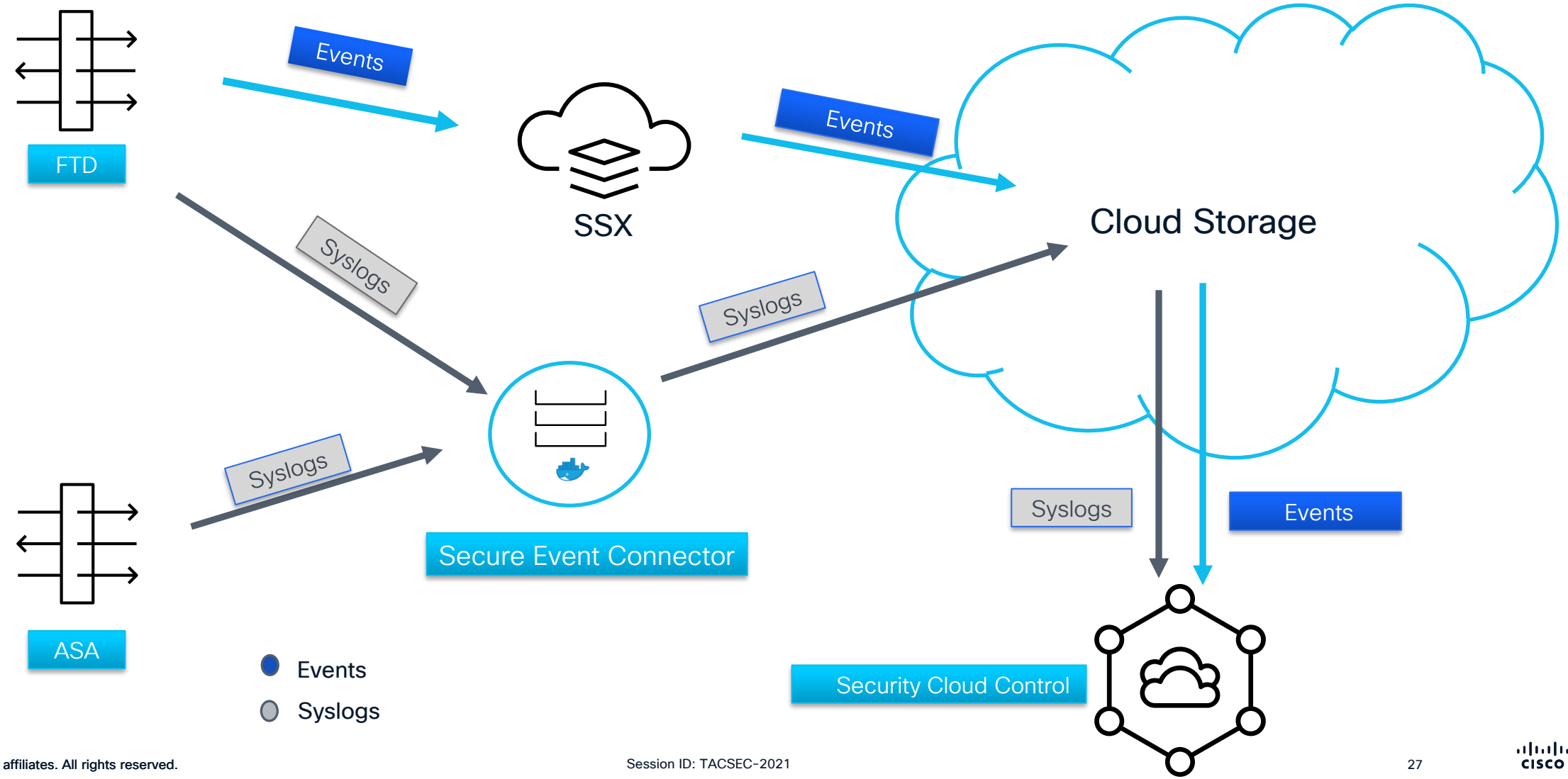
Sftunnel succesfully established



You can validate the tasks from cdFMC GUI

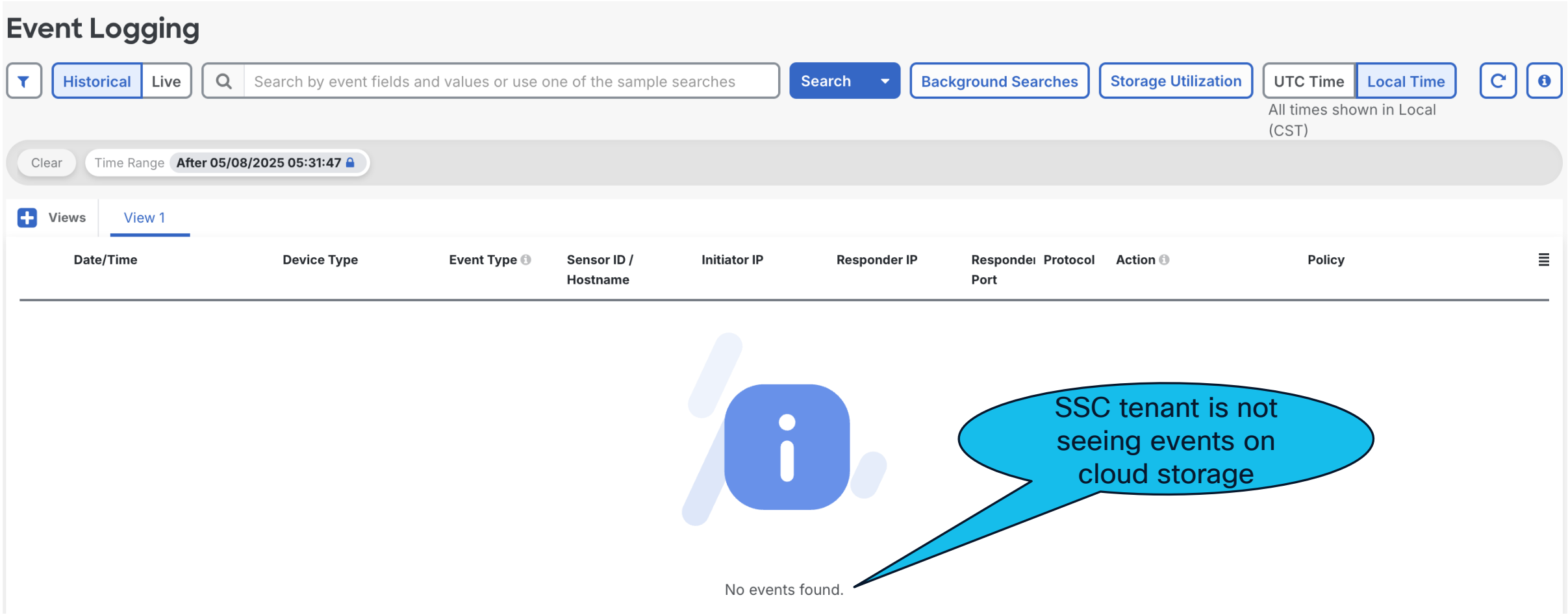
Troubleshooting Event Logging Issues

Event Logging Diagram



SCC Not Showing Events

SCC GUI > Events & Logs > Event Logging



FTD Debug and Packet Capture

FTD CLISH >

```
 > system support firewall-engine-debug


Caution: This could result in high CPU usage and lower throughput.
Use filters to mitigate the impact


Please specify an IP protocol:
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages
```

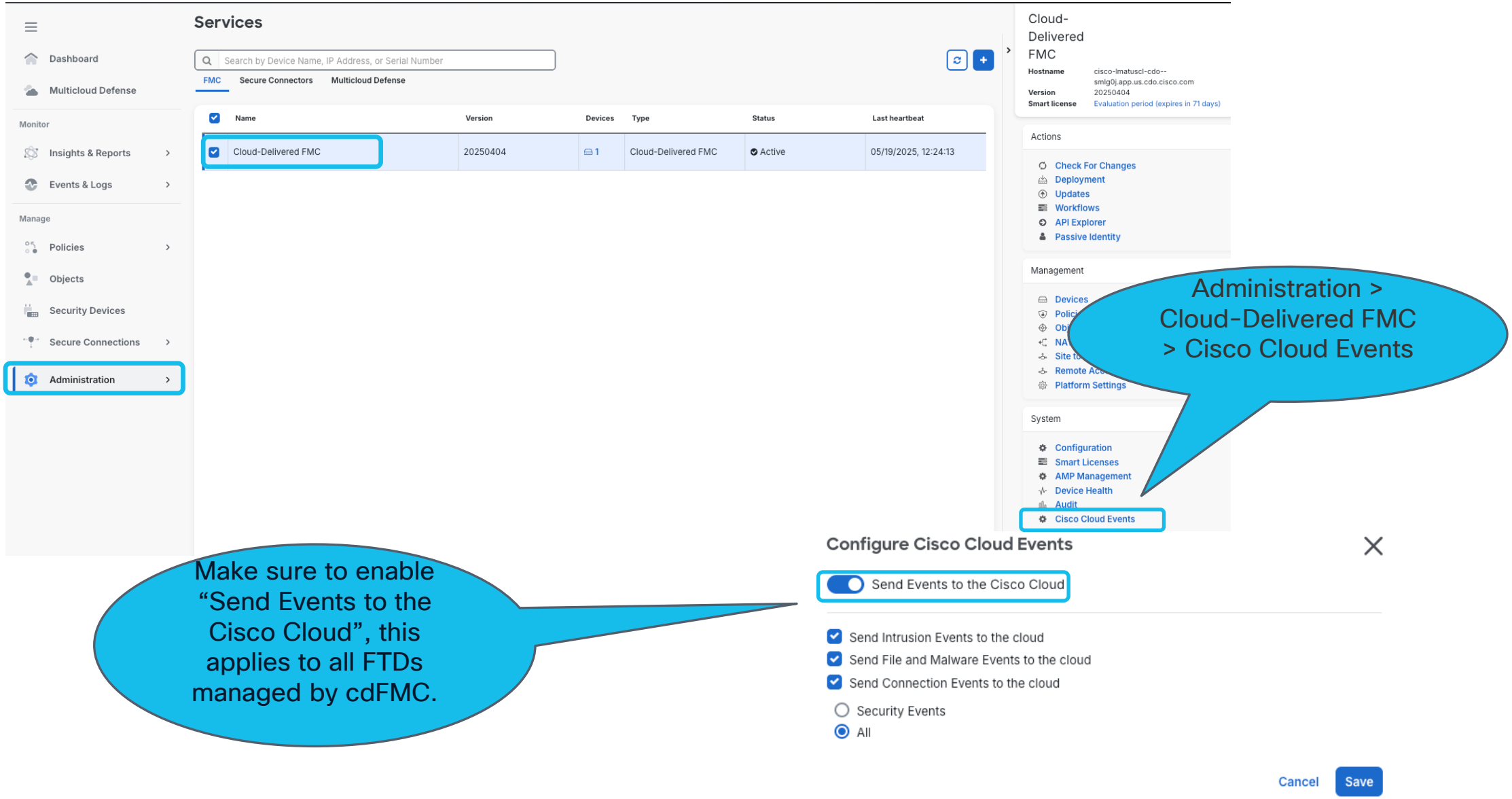
Collect a debug on your FTD clish

Collect a packet capture to validate if FTD is receiving the interested traffic

```
cap <capname> interface <interface_name> trace match <protocol> host <a.b.c.d> any eq <port>
```

```
> capture ciscocapture interface Inside trace match tcp host 172.18.2.5 any eq 443
> show capture ciscocapture

20 packet captured
```

Send Events to the Cisco Cloud



FTD tenancy info

FTD Expert Mode ~$:

```
admin@user-ftd:~$ curl localhost:8989/v1/contexts/default/tenant

{"registeredTenantInfo":{"companyName":"cisco-lmatuscl-cdo__smlg0j","id":"b684475e-e46c-4042-acf5-
4e0a0877b9d7","spId":"CDO"},"tenantInfo":[{"companyName":"cisco-lmatuscl-cdo__smlg0j","id":"b684475e-e46c-
4042-acf5-4e0a0877b9d7","spId":"CDO"}]}root@lmatuscl-ftd:/home/admin#
```

Command from expert mode

SCC tenancy info

SCC GUI > Platform Management > Settings

Tenant ID
b684475e-e46c-4042-acf5-4e0a0877b9d7

Secure Services Exchange Tenant ID
b684475e-e46c-4042-acf5-4e0a0877b9d7

Tenant Name
CDO_cisco-lmatuscl-cdo__smlg0j

Validate if the devices are connected to the correct SCC tenant and SSX instance

Event Service Module Status

FTD Expert Mode ~$:

```
admin@user-ftd:~$ curl localhost:8989/v1/contexts/default/status
```

Fault #1

```
admin@user-ftd:~$ curl localhost:8989/v1/contexts/default/status

 { "type": "Events", "status": "Failed", "name": "", "description": "Events service module failed, err: zmq4: could
not dial to \"ipc:///ngfw/var/sf/run/EventHandler_SSEConnector.sock\" (retry=250ms): dial unix
/ngfw/var/sf/run/EventHandler_SSEConnector.sock: connect: connection refused" }
```

Event service is not working due to an internal issue on SCC side

Fault #2

This error ussually indicates an issue from FTD side

```
admin@user-ftd:~$ curl localhost:8989/v1/contexts/default/status

{
      "type": "Events",
      "status": "Failed",
      "name": "",
      "description": "Events service module failed"
    }
```

Connector Log Error Message

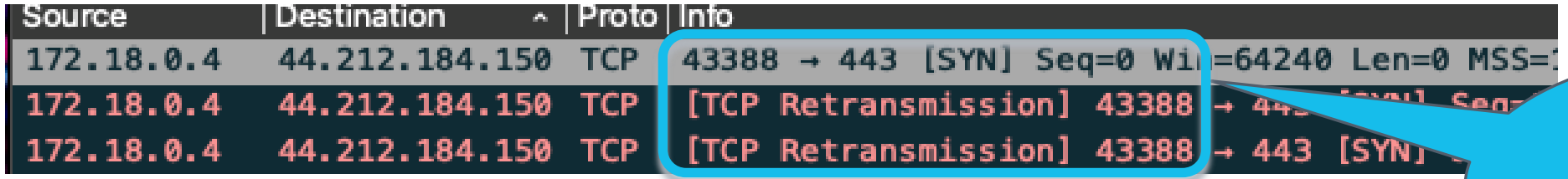
FTD Expert Mode ~$:

```
admin@user-ftd:~$ tail -10 /ngfw/var/log/connector/connector.log | grep -i "events”


time="2025-05-08T18:04:14.499530252Z" "
root@lmatuscl-ftd:/ngfw/var/log/connector# level=warning msg="[test-ftd.internal.cloudapp.net][events.go:181
events:(*Service).Start] Could not connect to WebSocket endpoint wss://eventing-ingest.sse.itd.cisco.com:443/ingest:
dial tcp 44.212.184.150:443: i/o timeout
```

FTD unable to stablish connection with SSX service

Communication Issue on Port 443

- Collect a packet capture on the FTD management interface.



Packet caputre displayed on wireshark showing the communication issue

Verification

FTD Expert Mode ~$:

FTD successfully connected to SSX service

```
admin@user-ftd:~$ curl localhost:8989/v1/contexts/default/status

 {
      "type": "Events",
      "status": "Success",
      "name": "",
      "description": "Events service module successful"
  }
```

connector.log path: /ngfw/var/log/connector

FTD using HTTPS channel to send events

```
admin@user-ftd:~$ grep -i "eventing" /ngfw/var/log/connector/connector.log | more

time="2025-05-07T23:44:35.632778934Z" level=info msg="[lmatuscl-
ftd.internal.cloudapp.net][srv_discovery.go:308 srvdisc.(*SrvReg).Start:func2]
Service Discovery successful response:
{\"services\":[{\"name\":\"Eventing\",\"tags\":[],\"apis\":[{\"type\":\"Events\",\"
version\":\"1.0\",\"url\":\"wss://eventing-ingest.sse.itd.cisco.com:443/ingest\"}
```

Total Events Recevided and Sent by FTD

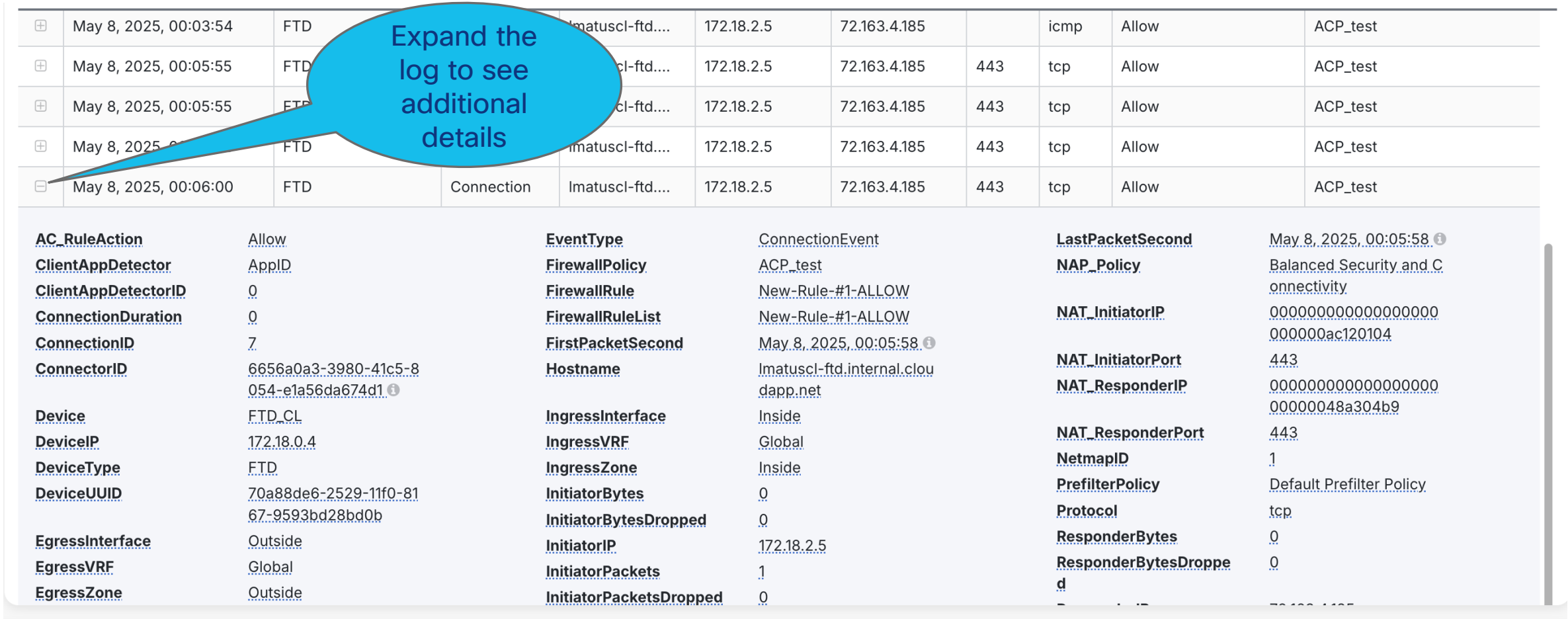
FTD Expert Mode ~$:

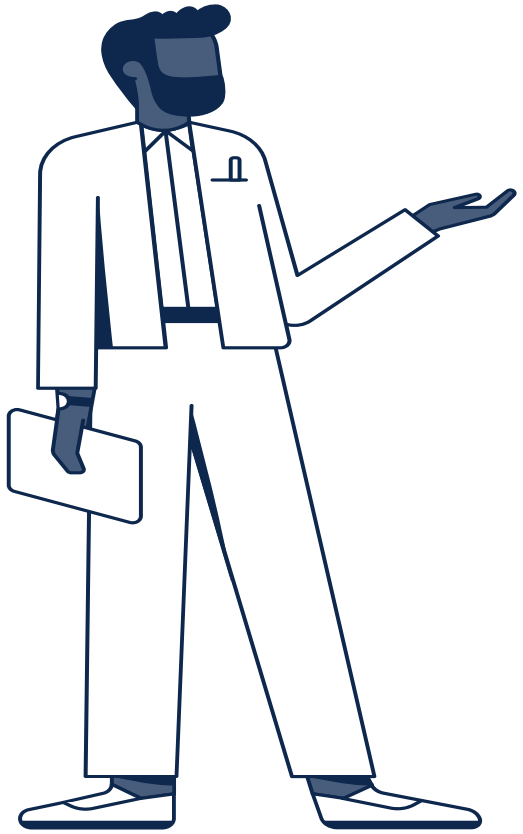
```
admin@user-ftd:~$ curl localhost:8989/v1/contexts/default/statistics

{
      "type": "Events",
      "statistics": {
        "ZmqStat": {
          "LastCloudConnectSuccess": "2025-05-07T23:37:05.594584935Z",
          "LastCloudConnectFailure": "",
          "LastCloudDisconnect": "",
          "TotalEventsReceived": 11,
          "TotalEventsSent": 11
        },
        "WsStat": {
          "ActiveConnections": 0,
          "LastClientConnectSuccess": "",
          "LastClientDisconnect": "",
          "LastCloudConnectSuccess": "",
          "LastCloudConnectFailure": "",
          "LastCloudDisconnect": "",
          "TotalEventsReceived": 0,
          "TotalEventsSent": 0
        }
```

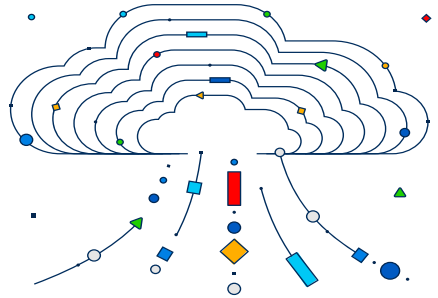
We can see when was the last success connection to the SSX service

We can validate how many events the FTD has sent to the cloud

SCC Displaying Events







- FTD successfully onboarded to SSC
- Sftunnel successfully created and device registered to cdFMC
- Understand how devices send events to the cloud.
- We can see events on Security Cloud Control.

Q&A

Kindly Join Us at The Booth

Resources

Resources

- Security Cloud Control

  https://docs.defenseorchestrator.com/#!g-managing-firewall-in-security-and-network-devices-with-cdo.html

- Manage Security Devices

  https://docs.defenseorchestrator.com/#!c-device-and-service-management.html

- Troubleshooting

  https://docs.defenseorchestrator.com/#!g-troubleshooting.html

- Cisco Secure Firewall ASA

  https://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html

- Cisco Secure Firewall Management Center

  https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html

Complete Your Session Evaluations

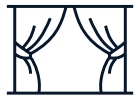
Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

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 www.CiscoLive.com/on-demand

Contact us: lmatuscl@cisco.com and balsaeed@cisco.com

Thank You

cisco Live !


CISCO