

Security Cloud Control: Navigating Through Onboarding & Event Logging Challenges

cisco Live !

Leonel Matus Climaco
Cloud Security Escalation Engineer

Bashar Alsaeed
Cloud Security Engineer

Session ID: TACSEC-2021

June 2025

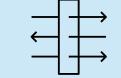
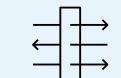
Agenda



- 01 Security Cloud Control
- 02 ASA Onboarding & Troubleshooting
- 03 FTD Onboarding & Troubleshooting
- 04 Troubleshooting Event Logging
- 05 Q&A

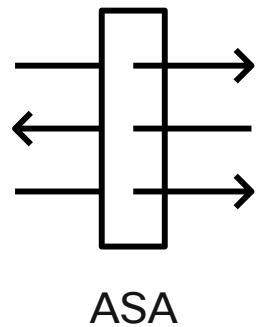
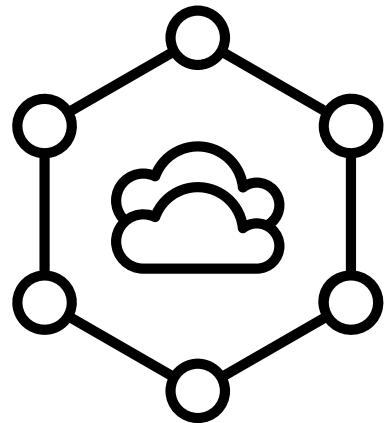
Security Cloud Control

Acronyms Directory

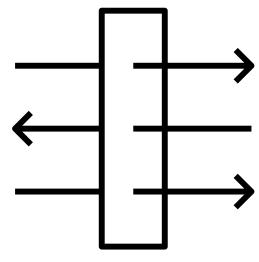
Acronym	Full Term	Icon
SCC	Security Cloud Control	
SDC	Secure Device Connector	
SSX	Security Service Exchange	
cdFMC	Cloud-delivered Firewall Management Center	
FMC	Firewall Management Center	
FTD	Secure Firewall Threat Defense	
ASA	Adaptive Security Appliance	
GUI	Graphical User Interface	

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)

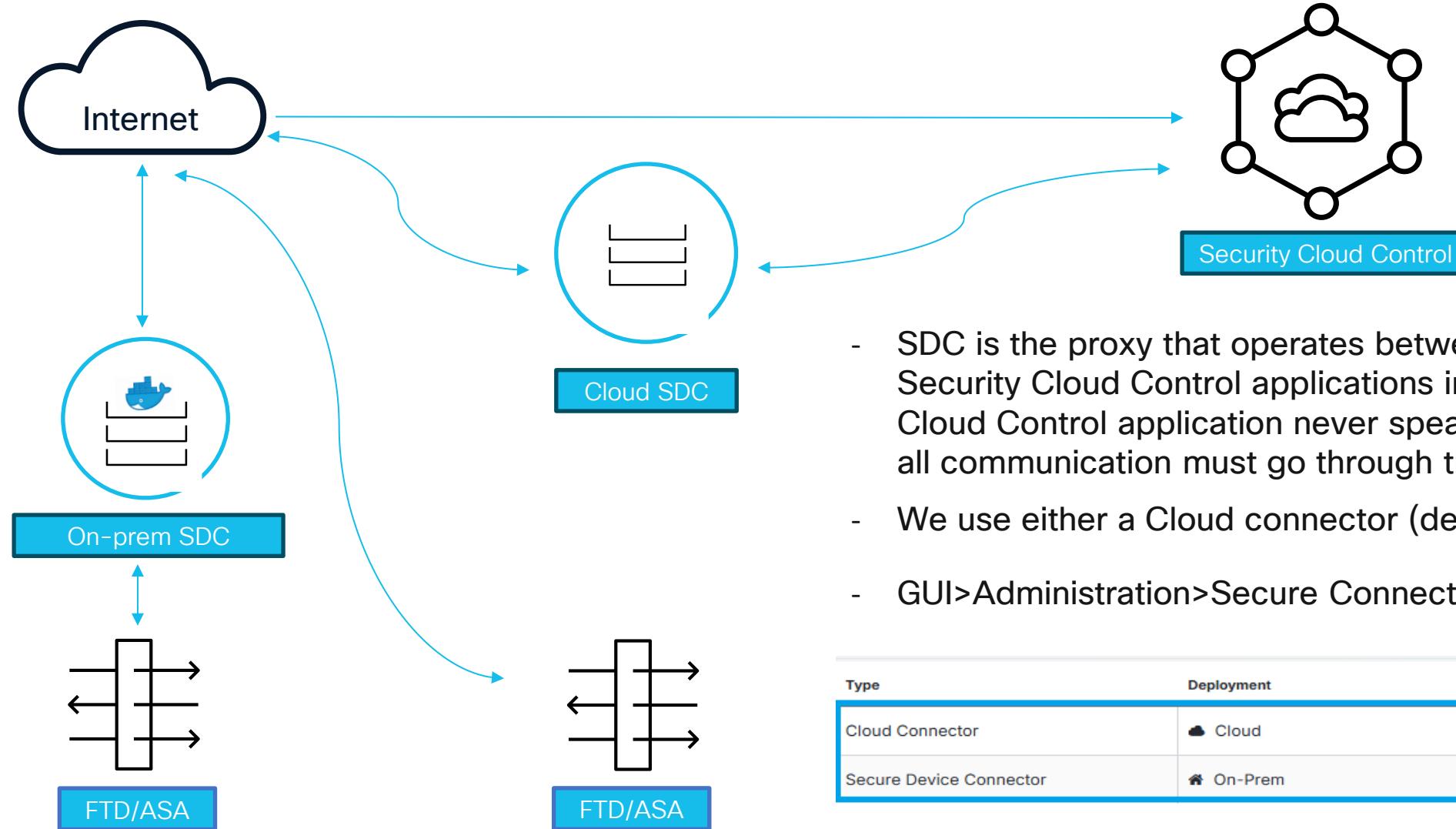
FTD (On-prem & Virtual)

Cisco Meraki™ Organizations

Umbrella Networks (Tunnel)

AWS Virtual Private Clouds

Security Cloud Control Devices Onboarding Routes



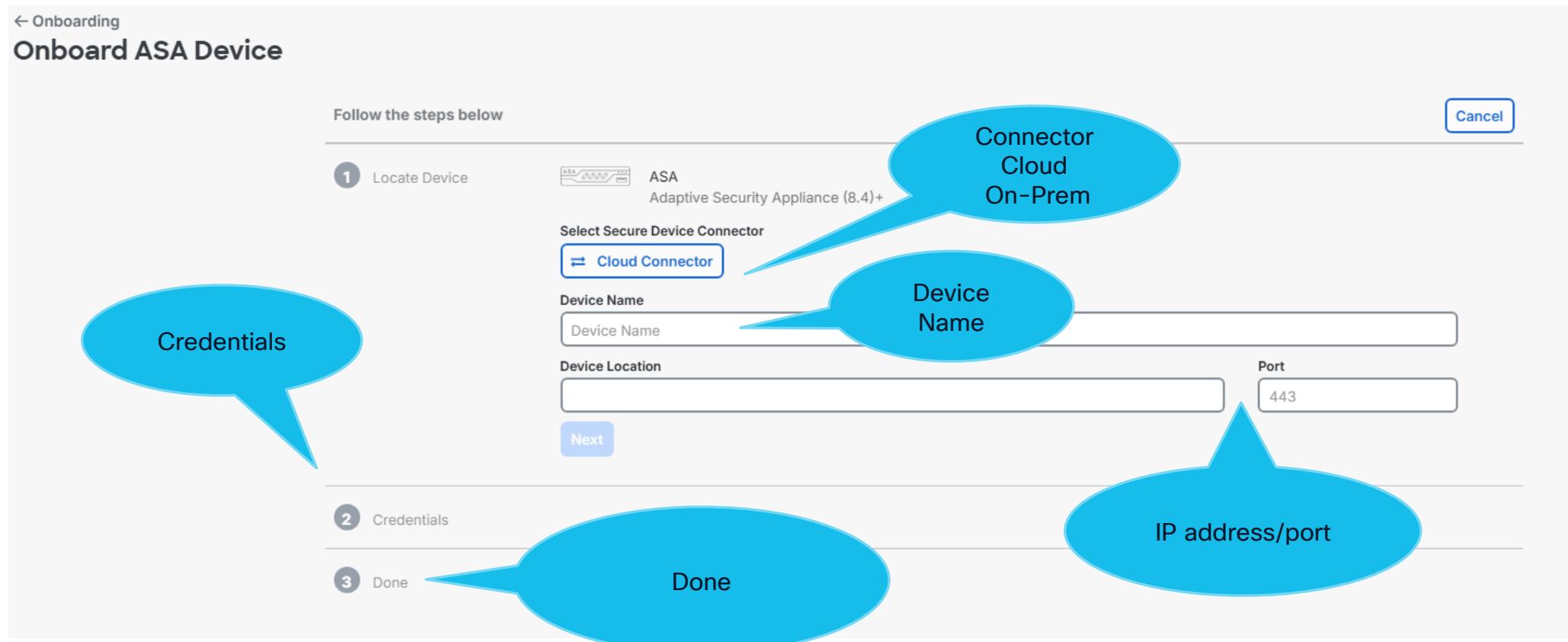
- SDC is the proxy that operates between the devices and the Security Cloud Control applications in the cloud (The Security Cloud Control application never speaks directly to the devices all communication must go through the SDC)
- We use either a Cloud connector (default) or an On-prem SDC
- GUI>Administration>Secure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

Security Devices

Devices Templates Displaying 5 of 5 results   

All ASA FTD

Name	Configuration Status	Connectivity
ASA-consec-3 ASA	Synced	Online
ASA-consec-4 ASA	Conflict Detected	Online
ASA_CL ASA	-	Unreachable
ASA_CiscoLive ASA	-	Invalid Credentials
FTD_CL FTD	Not Synced	Online

ASA_CiscoLive

ASA 10.31.124.187:443

Device Details

Location	10.31.124.187:443
Model	n/a
Serial	n/a
Chassis Serial	n/a
Software Version	n/a
ASDM Version	n/a
Firewall Mode	n/a
SDC	CDO_cisco-lmatuscl-cdo_smlg0j-SDC-2

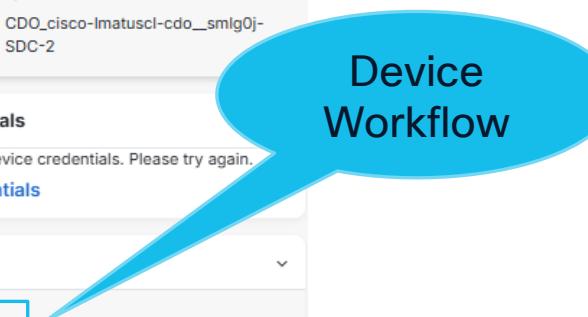
Invalid Credentials

Failed to validate device credentials. Please try again.

[Update Credentials](#)

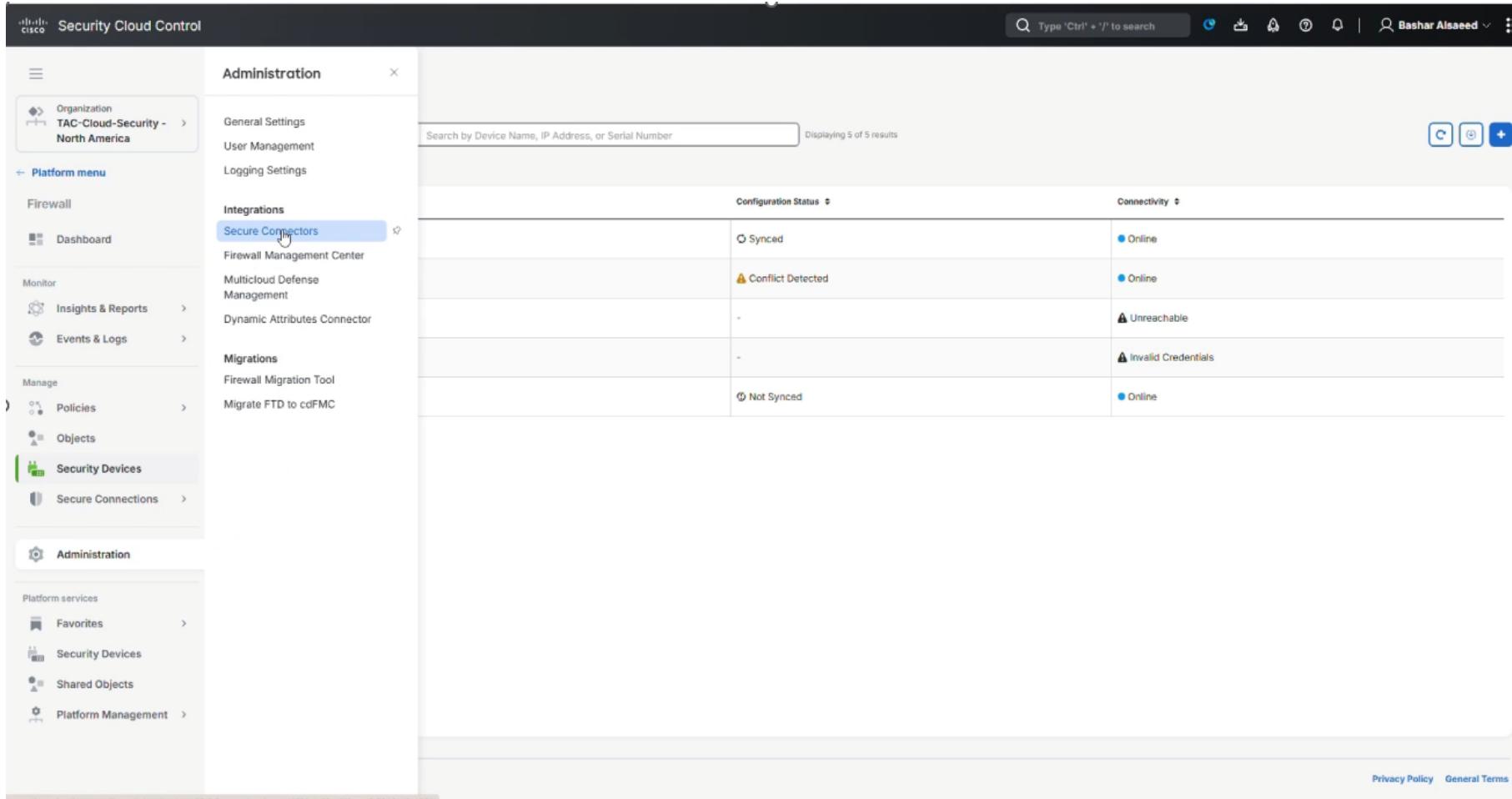
Device Actions

 [Workflows](#)  [Remove](#)



Onboarding Skills Checklist (Continued)

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

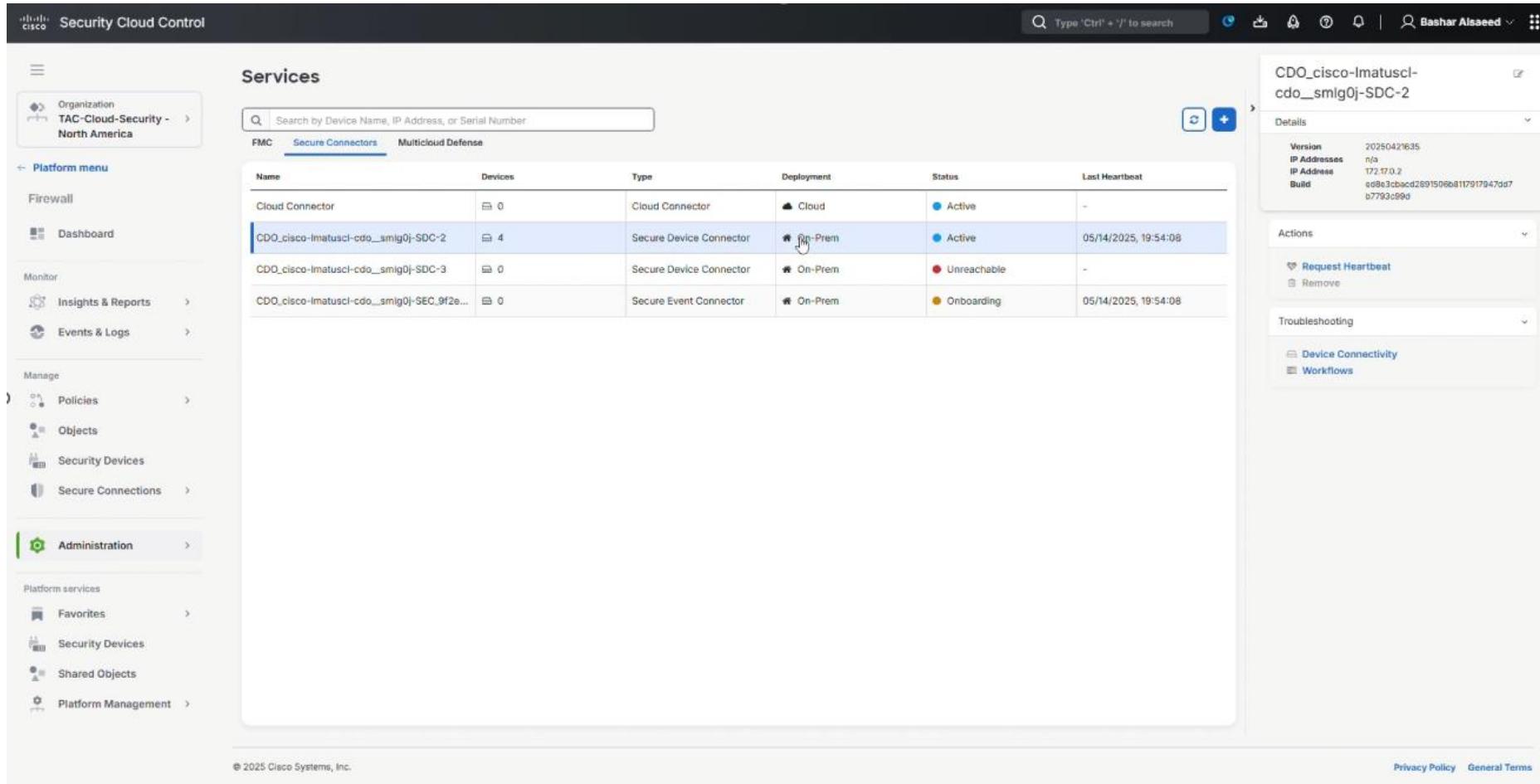


The screenshot shows the Cisco Security Cloud Control web interface. The left sidebar contains a navigation menu with sections like Organization, Platform menu, Firewall, Monitor, Insights & Reports, Events & Logs, Manage, and Administration. Under the Administration section, the 'Secure Connectors' option is selected. The main content area is titled 'Device Connectivity' and displays a table with columns for Configuration Status and Connectivity. The table shows five rows: 1. Synced (Online), 2. Conflict Detected (Online), 3. (Unreachable), 4. (Invalid Credentials), and 5. Not Synced (Online). A search bar at the top of the main area allows searching by Device Name, IP Address, or Serial Number. The bottom right of the interface includes links for Privacy Policy and General Terms.

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

Onboarding Skills Checklist (Continued)

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

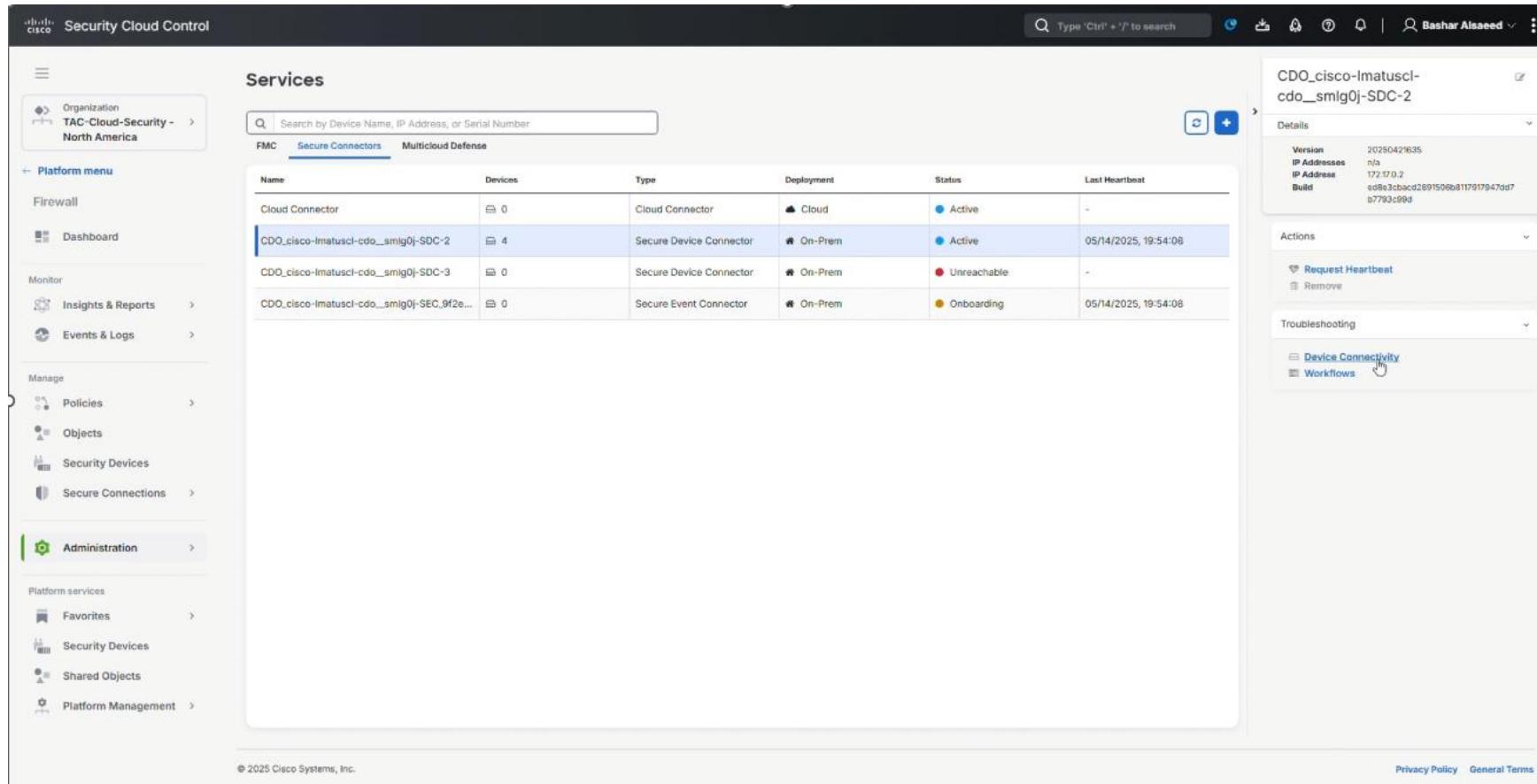


The screenshot shows the Cisco Security Cloud Control interface. The left sidebar includes sections for Platform menu, Firewall, Dashboard, Monitor, Insights & Reports, Events & Logs, Manage (with Policies, Objects, Security Devices, Secure Connections), Administration, Platform services (Favorites, Security Devices, Shared Objects), and Platform Management. The main content area is titled 'Services' and shows a table with columns: Name, Devices, Type, Deployment, Status, and Last Heartbeat. The table lists three entries: 'Cloud Connector' (Cloud Connector, Cloud, Active, 0 devices), 'CDO_cisco-lmatuscl-cdo_smig0j-SDC-2' (Secure Device Connector, On-Prem, Active, 4 devices), and 'CDO_cisco-lmatuscl-cdo_smig0j-SDC-3' (Secure Device Connector, On-Prem, Unreachable, 0 devices). A detailed view of the second entry is shown on the right, including fields for Version (2025042635), IP Addresses (n/a, 172.17.0.2), and Build (a88e3cbacd289150868117917947dd7b7793c99d). The right sidebar includes sections for Actions (Request Heartbeat, Remove), Troubleshooting (Device Connectivity, Workflows), and a search bar at the top right.

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

Onboarding Skills Checklist (Continued)

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

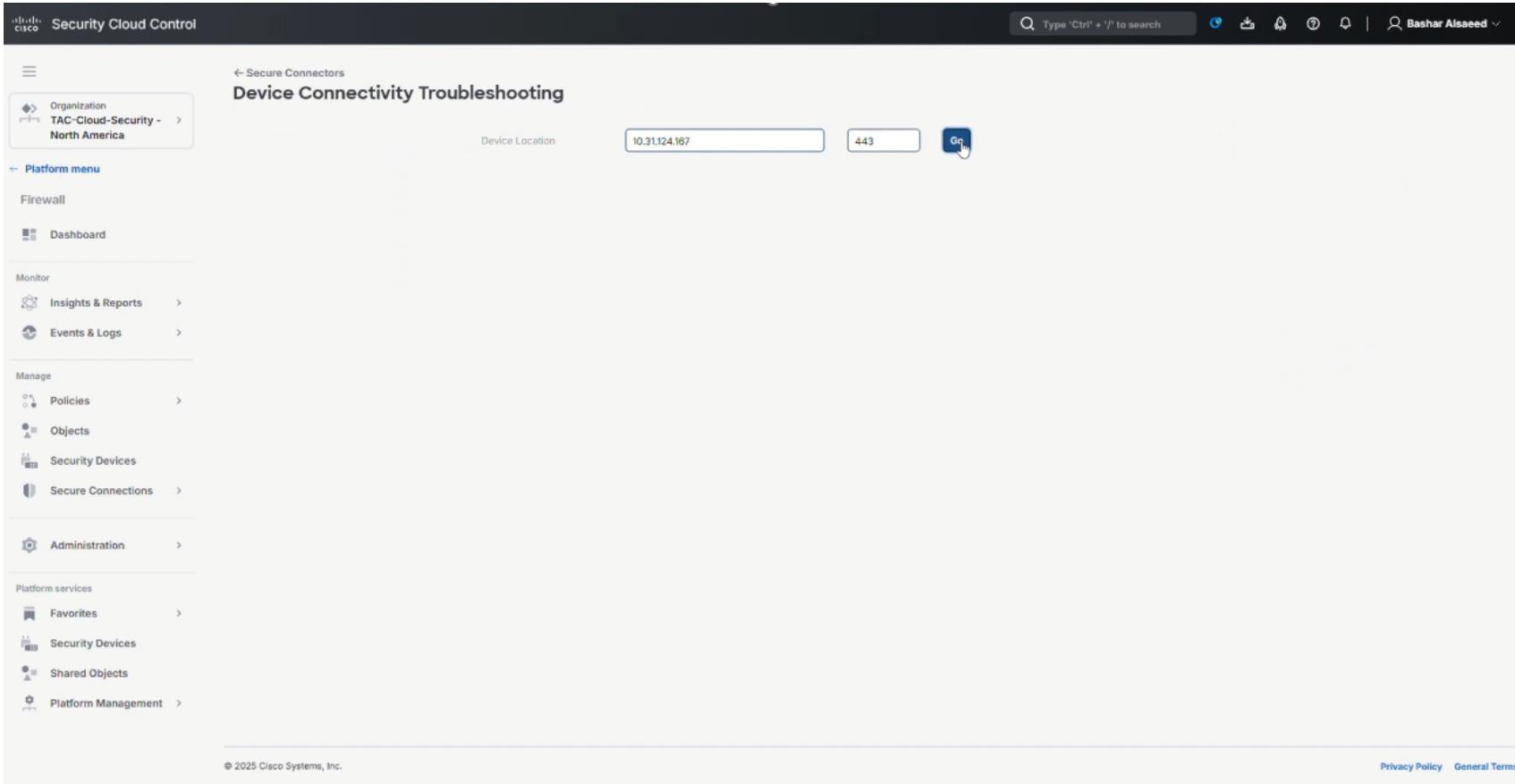


The screenshot shows the Cisco Security Cloud Control interface. On the left, the Platform menu includes Firewall, Dashboard, Monitor, Insights & Reports, Events & Logs, Manage (Policies, Objects, Security Devices, Secure Connections), Administration, and Platform services (Favorites, Security Devices, Shared Objects, Platform Management). The main area is titled 'Services' and shows a table of connectors. The table has columns: Name, Devices, Type, Deployment, Status, and Last Heartbeat. The table contains four rows: 1. Cloud Connector (0 devices, Cloud Type, Cloud Deployment, Active Status, Last Heartbeat: 05/14/2025, 19:54:08). 2. CDO_cisco-lmatuscl-cdo_sm1g0j-SDC-2 (4 devices, Secure Device Connector Type, On-Prem Deployment, Active Status, Last Heartbeat: 05/14/2025, 19:54:08). 3. CDO_cisco-lmatuscl-cdo_sm1g0j-SDC-3 (0 devices, Secure Device Connector Type, On-Prem Deployment, Unreachable Status, Last Heartbeat: -). 4. CDO_cisco-lmatuscl-cdo_sm1g0j-SEC_9f2e... (0 devices, Secure Event Connector Type, On-Prem Deployment, Onboarding Status, Last Heartbeat: 05/14/2025, 19:54:08). A search bar at the top allows searching by Device Name, IP Address, or Serial Number. On the right, a detailed view of the CDO_cisco-lmatuscl-cdo_sm1g0j-SDC-2 connector is shown. It includes a 'Details' section with Version 20250421635, IP Addresses 172.17.0.2, and Build 60863cbac2269750808117917947d7. Below it are 'Actions' (Request Heartbeat, Remove) and 'Troubleshooting' (Device Connectivity, Workflows). The 'Device Connectivity' link is highlighted with a blue box.

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

Onboarding Skills Checklist (Continued)

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

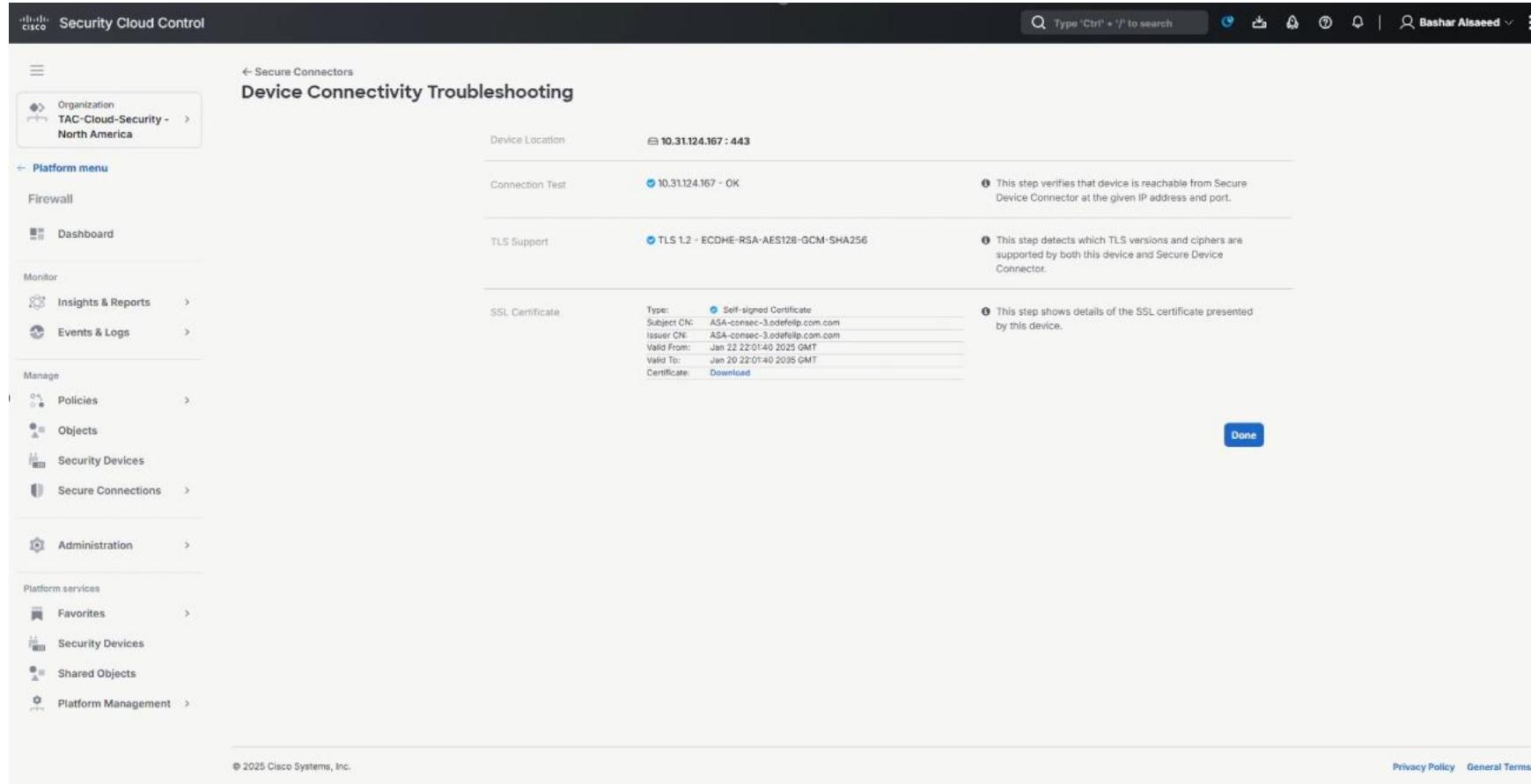


The screenshot shows the Cisco Security Cloud Control interface. The left sidebar contains a navigation menu with sections like Firewall, Dashboard, Monitor, Manage, Administration, and Platform services. The main content area is titled "Device Connectivity Troubleshooting" and shows a search bar with the IP address "10.31.124.167" and port "443", with a "Go" button being clicked. The URL in the address bar is https://docs.defenseorchestrator.com/#!troubleshoot-device-connectivity-with-SDC.html.

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

Onboarding Skills Checklist (Continued)

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



Security Cloud Control

Device Connectivity Troubleshooting

Device Location: 10.31.124.167:443

Connection Test: 10.31.124.167 - OK

This step verifies that device is reachable from Secure Device Connector at the given IP address and port.

TLS Support: TLS 1.2 - ECDHE-RSA-AES128-GCM-SHA256

This step detects which TLS versions and ciphers are supported by both this device and Secure Device Connector.

SSL Certificate

Type: Self-signed Certificate
Subject CN: ASA-consec-3.0.dcfelp.com
Issuer CN: ASA-consec-3.0.dcfelp.com
Valid From: Jan 22 22:01:40 2025 GMT
Valid To: Jan 20 22:01:40 2035 GMT
Certificate: Download

Done

© 2025 Cisco Systems, Inc.

Privacy Policy General Terms

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

ASA Onboarding Failure to Security Cloud Control

Follow the steps below

1 Locate Device Device Name: ASA_CiscoLive; Device Location: 10.31.124.187:443 **Cancel**

2 Credentials  Invalid ASA credentials. Please try again.

ASA Admin Credentials Fail

Username

Password

Next

Let's Troubleshoot

Compatibility



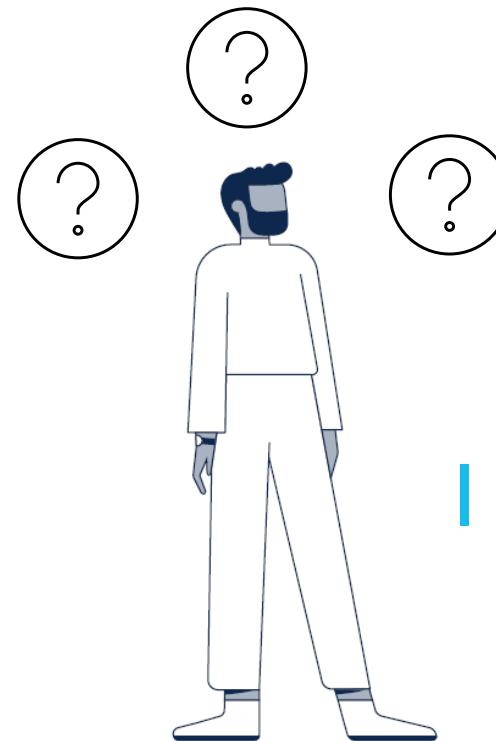
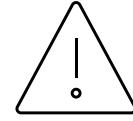
Prerequisites



Connectivity



Workflows



I Did My Homework!

Workflows

← Security Devices

ASA_CiscoLive

Name	Priority	Condition	Current State	Last Update	Start Time	End Time	Service
asaCredentialStateMachine	On Demand	Done	Bad Credentials	5/12/2025, 7:20:10 PM	5/12/2025, 7:20:09 PM	5/12/2025, 7:20:10 PM	AEGIS

Bad Credentials

© 2025 Cisco and/or its affiliates. All rights reserved.

Session ID: TACSEC-2021

17

CISCO

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

Certificate
Exchange Failure

- 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
```

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
```

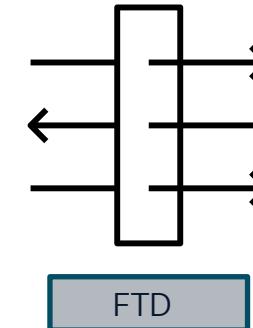


Disable client-side certificate

FTD Onboarding

Onboard FTD to Cloud-delivered Firewall Management Center

Port	Protocol / Feature	Details
8305/tcp	Appliance communications	<ul style="list-style-type: none">Securely communicate between appliances in a deployment.
443	HTTPS	<ul style="list-style-type: none">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

1 Device Name

FTD_Cisco_Live

2 Policy Assignment

Access Control Policy: Default Access Control Policy

3 Subscription Licenses

Performance Tier: FTDv50

4 CLI Registration Key

1 Ensure the device's initial configuration is complete before trying to apply the registration key.

2 Copy the CLI Key below and paste it into the CLI of the FTD

```
configure manager add cisco-lmatuscl-cdo--smlg0j.app.us.cdo.cisco.com  
tUpttwHR01JuhMU8xUU2RkJ5PapVmMqN VJ1Bdtyn6bksVcU1jFCJ9nje5onvfkLB cisco-lmatuscl-cdo--  
smlg0j.app.us.cdo.cisco.com
```

Security Cloud
Control
provides the CLI
registration key

Next

FTD Cannot Establish Sftunnel with cdFMC

FTD Expert Mode ~\$:

Resolve the cdFMC FQDN to identify the public IP address

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

```
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
```

No.	Ti	Source	Destination	Protocol	Info
6	...	172.18.0.4	44.243.34.123	TCP	... 59099 → 8305 [SYN] Seq=0 Win=64240 Len=0
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	Prot	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=128
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=64800 TSval=1084691593 TSecr=506039720
8	44.243.34.123	172.18.0.4	TL	Server Hello, Change	data, Application Data, Application Data
9	172.18.0.4	44.243.34.123	TCP	35123 → 8305	[ACK] Seq=322 Ack=323 Win=64800 TSval=1084691598 TSecr=1084691598
10	172.18.0.4	44.243.34.123	TL	Change Cipher Spec, Application	
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
successfully
established

Deployments Upgrades Health Tasks Show Pop-up Notifications

20+ total 0 waiting 0 running 0 retrying 20+ success Filter

0 failures

Health Policy
Apply Initial_Health_Policy 2025-04-04 14:05:59 to FTD_CL
Health Policy applied successfully 1m 49s X

Discovery
FTD_CL - Discovery from the device is successful. 2m 7s X

SFTunnel
FTD_CL - SFTunnel connection established successfully. - X

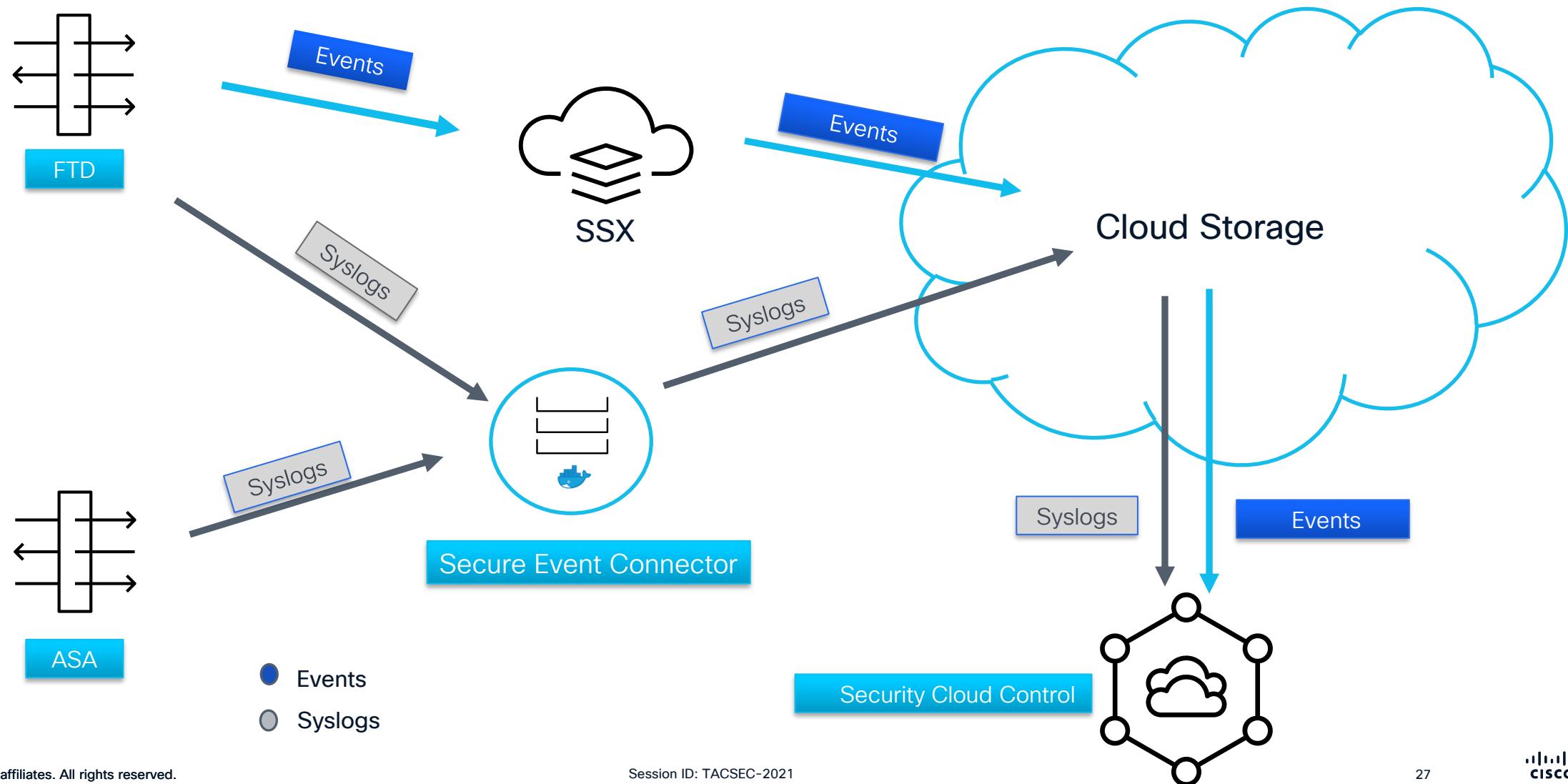
Register

[Remove successful tasks](#)

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

Event Logging

Historical Live Search by event fields and values or use one of the sample searches Search Background Searches Storage Utilization UTC Time Local Time C i

All times shown in Local (CST)

Clear Time Range After 05/08/2025 05:31:47

Views View 1

Date/Time	Device Type	Event Type i	Sensor ID / Hostname	Initiator IP	Responder IP	Responder Protocol	Action i Port	Policy	⋮
-----------	-------------	---------------------------	----------------------	--------------	--------------	--------------------	-------------------------------	--------	---

 No events found.

SSC tenant is not seeing events on cloud storage

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

```
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

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

Send Events to the Cisco Cloud

Cloud-Delivered FMC

Hostname: cisco-imatuscl-cdo--sm1g0j.app.us.cdo.cisco.com

Version: 20250404

Smart license: Evaluation period (expires in 71 days)

Actions:

- Check For Changes
- Deployment
- Updates
- Workflows
- API Explorer
- Passive Identity

Management:

- Devices
- Policy
- Objects
- NA
- Site to Site
- Remote Access
- Platform Settings

System:

- Configuration
- Smart Licenses
- AMP Management
- Device Health
- Audit
- Cisco Cloud Events

Configure Cisco Cloud Events

Send Events to the Cisco Cloud

Send Intrusion Events to the cloud

Send File and Malware Events to the cloud

Send Connection Events to the cloud

Security Events

All

Cancel Save

Services

Search by Device Name, IP Address, or Serial Number

FMC Secure Connectors Multicloud Defense

Name Version Devices Type Status Last heartbeat

Cloud-Delivered FMC 20250404 1 Cloud-Delivered FMC Active 05/19/2025, 12:24:13

Actions:

- Check For Changes
- Deployment
- Updates
- Workflows
- API Explorer
- Passive Identity

Administration > Cloud-Delivered FMC > Cisco Cloud Events

Make sure to enable “Send Events to the Cisco Cloud”, this applies to all FTDs managed by cdFMC.

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 usually 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 establish connection with SSX service

Communication Issue on Port 443

- Collect a packet capture on the FTD management interface.

Source	Destination	Proto	Info
172.18.0.4	44.212.184.150	TCP	43388 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1
172.18.0.4	44.212.184.150	TCP	[TCP Retransmission] 43388 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1
172.18.0.4	44.212.184.150	TCP	[TCP Retransmission] 43388 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1

Packet capture 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="[{latuscl-
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 Received 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 validate
how many
events the FTD
has sent to the
cloud

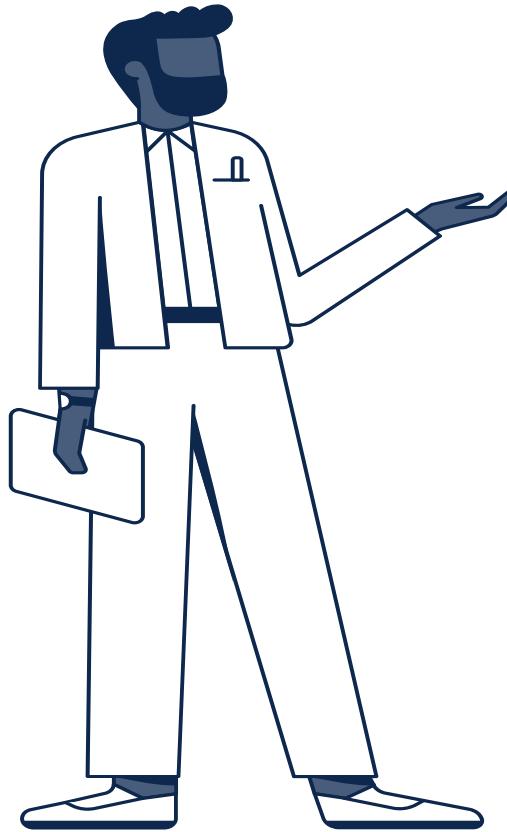
We can see when
was the last
success
connection to the
SSX service

SCC Displaying Events

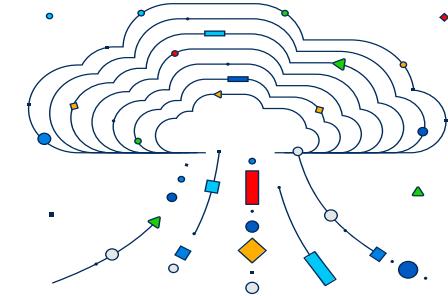
⊕	May 8, 2025, 00:03:54	FTD	Imatuscl-ftd....	172.18.2.5	72.163.4.185		icmp	Allow	ACP_test
⊕	May 8, 2025, 00:05:55	FTD	Imatuscl-ftd....	172.18.2.5	72.163.4.185	443	tcp	Allow	ACP_test
⊕	May 8, 2025, 00:05:55	FTD	Imatuscl-ftd....	172.18.2.5	72.163.4.185	443	tcp	Allow	ACP_test
⊕	May 8, 2025, 00:05:55	FTD	Imatuscl-ftd....	172.18.2.5	72.163.4.185	443	tcp	Allow	ACP_test
⊖	May 8, 2025, 00:06:00	FTD	Connection	Imatuscl-ftd....	172.18.2.5	72.163.4.185	443	tcp	Allow

Expand the log to see additional details

AC_RuleAction	Allow	EventType	ConnectionEvent	LastPacketSecond	May 8, 2025, 00:05:58 ⓘ
ClientAppDetector	AppID	FirewallPolicy	ACP_test	NAP_Policy	Balanced Security and C...
ClientAppDetectorID	0	FirewallRule	New-Rule-#1-ALLOW	NAT_InitiatorIP	connectivity
ConnectionDuration	0	FirewallRuleList	New-Rule-#1-ALLOW	NAT_InitiatorPort	00000000000000000000000000000000
ConnectionID	7	FirstPacketSecond	May 8, 2025, 00:05:58 ⓘ	NAT_ResponderIP	00000000000000000000000000000000
ConnectorID	6656a0a3-3980-41c5-8054-e1a56da674d1 ⓘ	Hostname	Imatuscl-ftd.internal.cloudapp.net	NAT_ResponderPort	443
Device	FTD CL	IngressInterface	Inside	NetmapID	443
DeviceIP	172.18.0.4	IngressVRF	Global	PrefilterPolicy	1
DeviceType	FTD	IngressZone	Inside	Protocol	Default Prefilter Policy
DeviceUUID	70a88de6-2529-11f0-8167-9593bd28bd0b	InitiatorBytes	0	ResponderBytes	tcp
EgressInterface	Outside	InitiatorBytesDropped	0	ResponderBytesDropped	0
EgressVRF	Global	InitiatorIP	172.18.2.5
EgressZone	Outside	InitiatorPackets	1
		InitiatorPacketsDropped	0



- 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 !

