

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







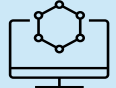

03 FTD Onboarding & Troubleshooting

04 Troubleshooting Event Logging

05 Q&A

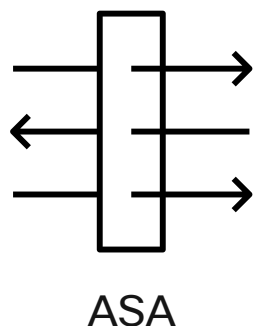
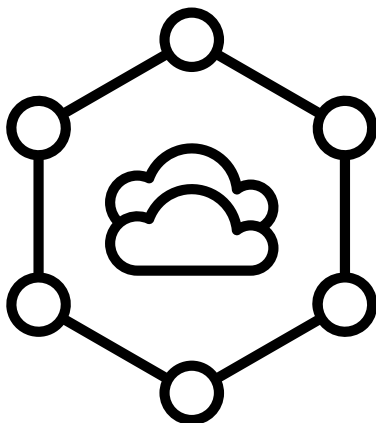
Security Cloud Control

Acronyms Directory

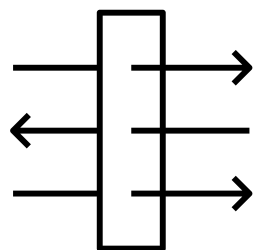
Acronym	Full Term	Icon
SCC	Security Cloud Control	
SDC	Secure Device Connector	
SSX	Security Service Exchange	
cdFMC	Cloud-delivered Firewall Management Center	
FMC	Firewall Management Center	
FTD	Secure Firewall Threat Defense	
ASA	Adaptive Security Appliance	
GUI	Graphical User Interface	

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)

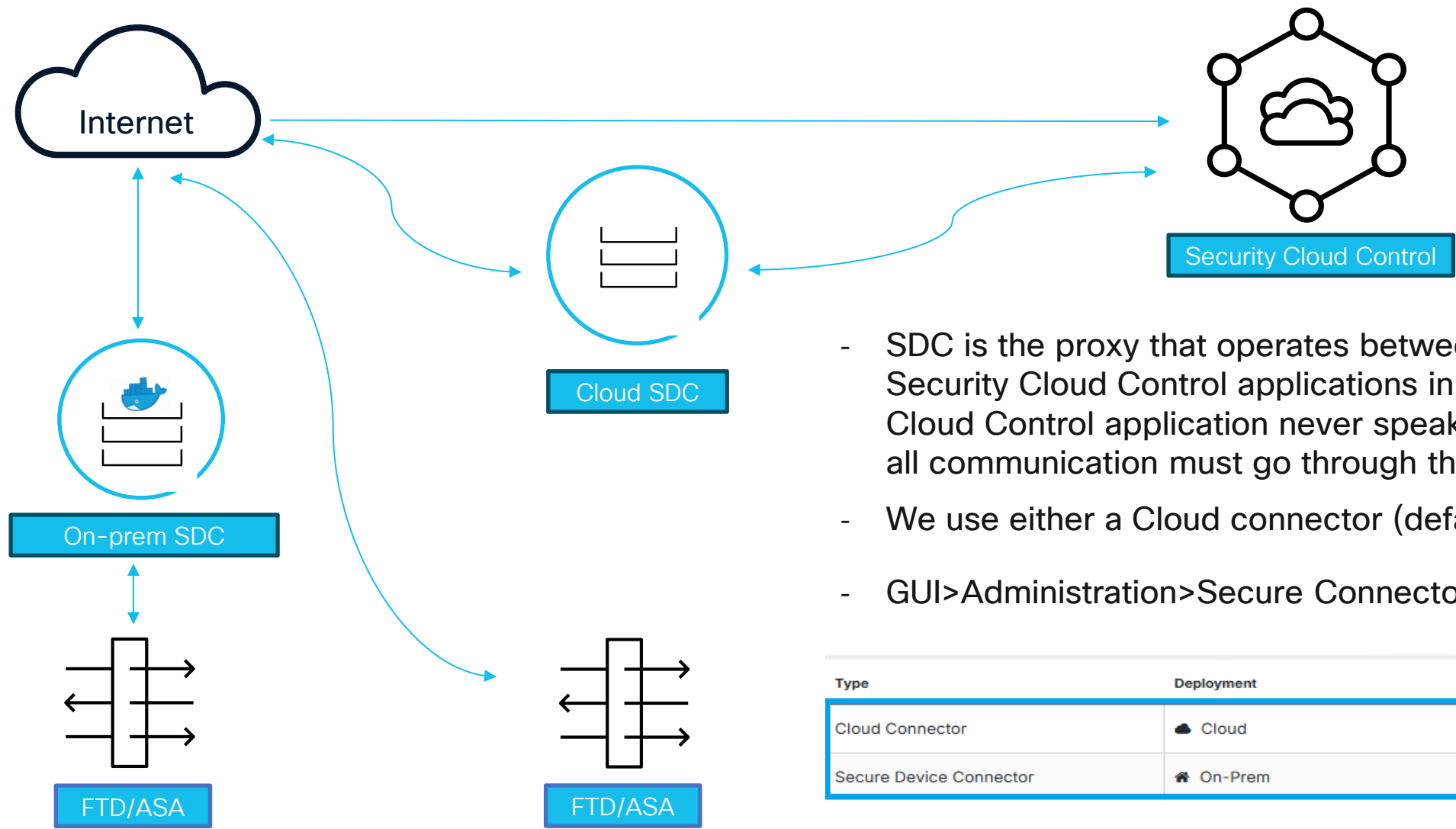
FTD (On-prem & Virtual)

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

← Onboarding
Onboard ASA Device

Follow the steps below Cancel

1 Locate Device

 **ASA**
Adaptive Security Appliance (8.4)+

Select Secure Device Connector

Cloud Connector

Connector Cloud On-Prem

Device Name

Device Name

Device Location

Port

443

Next

2 Credentials

Credentials

3 Done

Done

IP address/port

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

The screenshot displays the 'Security Devices' management interface. At the top, there are tabs for 'Devices' and 'Templates', a search bar, and a 'Displaying 5 of 5 results' indicator. Below the tabs, a table lists the devices. The 'ASA_CiscoLive' device is selected, and its details are shown on the right. The details include location, model, serial, chassis serial, software version, ASDM version, firewall mode, and SDC. A blue callout bubble points to the 'Workflows' button in the 'Device Actions' section, with the text 'Device Workflow' inside.

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:

Search by Device Name, IP Address, or Serial Number

Configuration Status	Connectivity
Sync'd	Online
Conflict Detected	Online
-	Unreachable
-	Invalid Credentials
Not Sync'd	Online

<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

Organization: TAC-Cloud-Security - North America

Platform menu

- Firewall
- Dashboard
- Monitor
 - Insights & Reports
 - Events & Logs
- Manage
 - Policies
 - Objects
 - Security Devices
 - Secure Connections
- Administration
- Platform services
 - Favorites
 - Security Devices
 - Shared Objects
 - Platform Management

Services

Search by Device Name, IP Address, or Serial Number

FMC Secure Connectors Multicloud Defense

Name	Devices	Type	Deployment	Status	Last Heartbeat
Cloud Connector	0	Cloud Connector	Cloud	Active	-
CDO_cisco-lmatucl-cdo_smig0j-SDC-2	4	Secure Device Connector	On-Prem	Active	05/14/2025, 19:54:08
CDO_cisco-lmatucl-cdo_smig0j-SDC-3	0	Secure Device Connector	On-Prem	Unreachable	-
CDO_cisco-lmatucl-cdo_smig0j-SEC_9f2e...	0	Secure Event Connector	On-Prem	Onboarding	05/14/2025, 19:54:08

Details for CDO_cisco-lmatucl-cdo_smig0j-SDC-2

Version: 20250421635
IP Addresses: n/a
IP Address: 172.17.0.2
Build: e08e3cbacd2891506b81179179479d7b7793c99d

Actions

- Request Heartbeat
- Remove

Troubleshooting

- Device Connectivity
- Workflows

© 2025 Cisco Systems, Inc. Privacy Policy 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 displays the Cisco Security Cloud Control interface. The main content area shows a table of services under the 'Secure Connectors' tab. The table has columns for Name, Devices, Type, Deployment, Status, and Last Heartbeat. One connector, 'CDQ_cisco-lmatusci-cdo_smlg0j-SDC-2', is highlighted and its details are shown in the right sidebar. The sidebar includes a 'Details' section with version and IP address information, an 'Actions' section with 'Request Heartbeat' and 'Remove' buttons, and a 'Troubleshooting' section with a 'Device Connectivity' link.

Name	Devices	Type	Deployment	Status	Last Heartbeat
Cloud Connector	0	Cloud Connector	Cloud	Active	-
CDQ_cisco-lmatusci-cdo_smlg0j-SDC-2	4	Secure Device Connector	On-Prem	Active	05/14/2025, 19:54:08
CDQ_cisco-lmatusci-cdo_smlg0j-SDC-3	0	Secure Device Connector	On-Prem	Unreachable	-
CDQ_cisco-lmatusci-cdo_smlg0j-SEC_9f2e...	0	Secure Event Connector	On-Prem	Onboarding	05/14/2025, 19:54:08

Details for CDQ_cisco-lmatusci-cdo_smlg0j-SDC-2:

- Version: 20250427635
- IP Addresses: n/a
- IP Address: 172.17.0.2
- Build: ed8a3cbac2891506b8117917947dd7b7793c99d

Actions:

- Request Heartbeat
- Remove

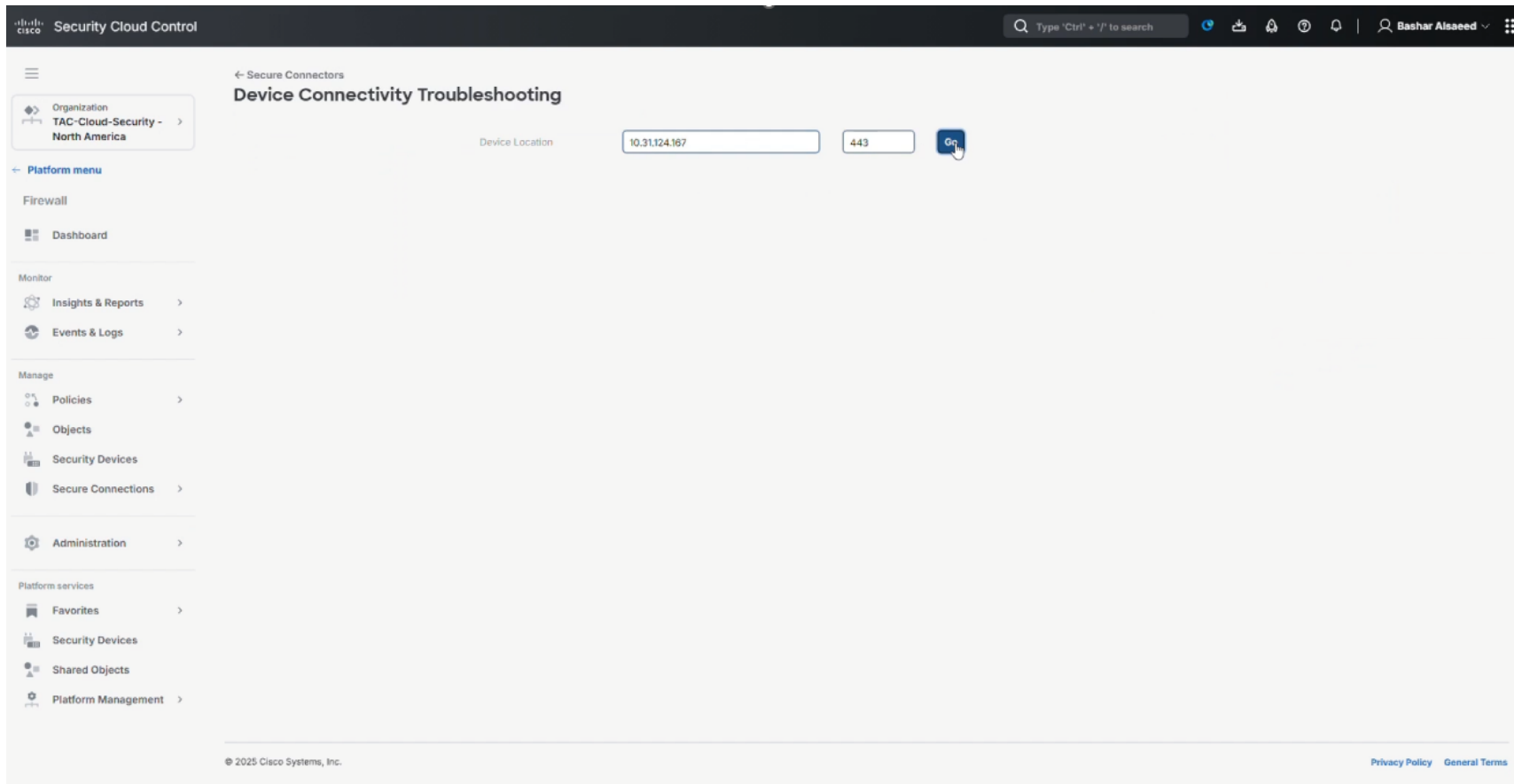
Troubleshooting:

- Device Connectivity
- Workflows

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

Onboarding Skills Checklist (Continued)

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



<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 top navigation bar includes the Cisco logo, the text 'Security Cloud Control', a search bar, and user information for 'Bashar Alsaed'. The left sidebar contains a 'Platform menu' with sections for '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 content area is titled 'Secure Connectors' and 'Device Connectivity Troubleshooting'. It displays a table with four rows: 'Device Location' (10.31.124.167 : 443), 'Connection Test' (10.31.124.167 - OK), 'TLS Support' (TLS 1.2 - ECDHE-RSA-AES128-GCM-SHA256), and 'SSL Certificate' (Self-signed Certificate). Each row has a corresponding description of the step. A 'Done' button is located at the bottom right of the table.

Device Location	10.31.124.167 : 443
Connection Test	10.31.124.167 - OK <small>This step verifies that device is reachable from Secure Device Connector at the given IP address and port.</small>
TLS Support	TLS 1.2 - ECDHE-RSA-AES128-GCM-SHA256 <small>This step detects which TLS versions and ciphers are supported by both this device and Secure Device Connector.</small>
SSL Certificate	Type: Self-signed Certificate Subject CN: ASA-consec-3.odef@ip.com Issuer CN: ASA-consec-3.odef@ip.com Valid From: Jan 22 22:01:40 2025 GMT Valid To: Jan 20 22:01:40 2035 GMT Certificate: Download <small>This step shows details of the SSL certificate presented by this device.</small>

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

ASA Onboarding Failure to Security Cloud Control

Follow the steps below Cancel

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

2 Credentials

✖ Invalid ASA credentials. Please try again.

Username

Password

Next

ASA Admin Credentials Fail

Let's Troubleshoot

Compatibility

Prerequisites

Connectivity

Workflows



I Did My Homework!

Workflows

← Security Devices

ASA_CiscoLive

⌂

⌂

Name	Priority	Condition	Current State	Last State	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

ACTION

TIME

STARTSTATE

ENDSTATE

RESULT

Bad Credentials

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
```

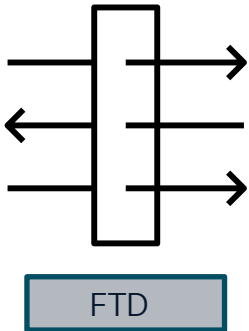


Disable client-side
certificate

FTD Onboarding

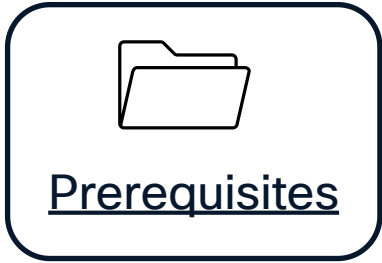
Onboard FTD to Cloud-delivered Firewall Management Center

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](#)



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 re

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 VJ1Bdtyn6bksVcU1jFCJ9nje5ohvfkLB cisco-lmatuscl-cdo--
smlg0j.app.us.cdo.cisco.com

Next

Security Cloud Control provides the CLI registration key

FTD Cannot Establish Sftunnel with cdFMC

Resolve the cdFMC FQDN to identify the public IP address

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

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
```

No.	Ti	Source	Destination	Prot	Le	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=
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 Len=0 TSval=1084691593 TSecr=506039720
8	44.243.34.123	172.18.0.4	TL...	...	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data
9	172.18.0.4	44.243.34.123	TCP	...	35123 → 8305 [ACK Seq=322 Ack=1 Win=64256 Len=0 TSval=506039720 TSecr=1084691598
10	172.18.0.4	44.243.34.123	TL...	...	Change Cipher Spec, Application Data
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

20+ total

0 waiting

0 running

0 retrying

20+ success

0 failures

Health Policy

Apply Initial_Health_Policy 2025-04-04 14:05:59 to FTD_CL

Health Policy applied successfully

1m 49s

Discovery

FTD_CL - Discovery from the device is successful.

2m 7s

SFTunnel

FTD_CL - SFTunnel connection established successfully.

-

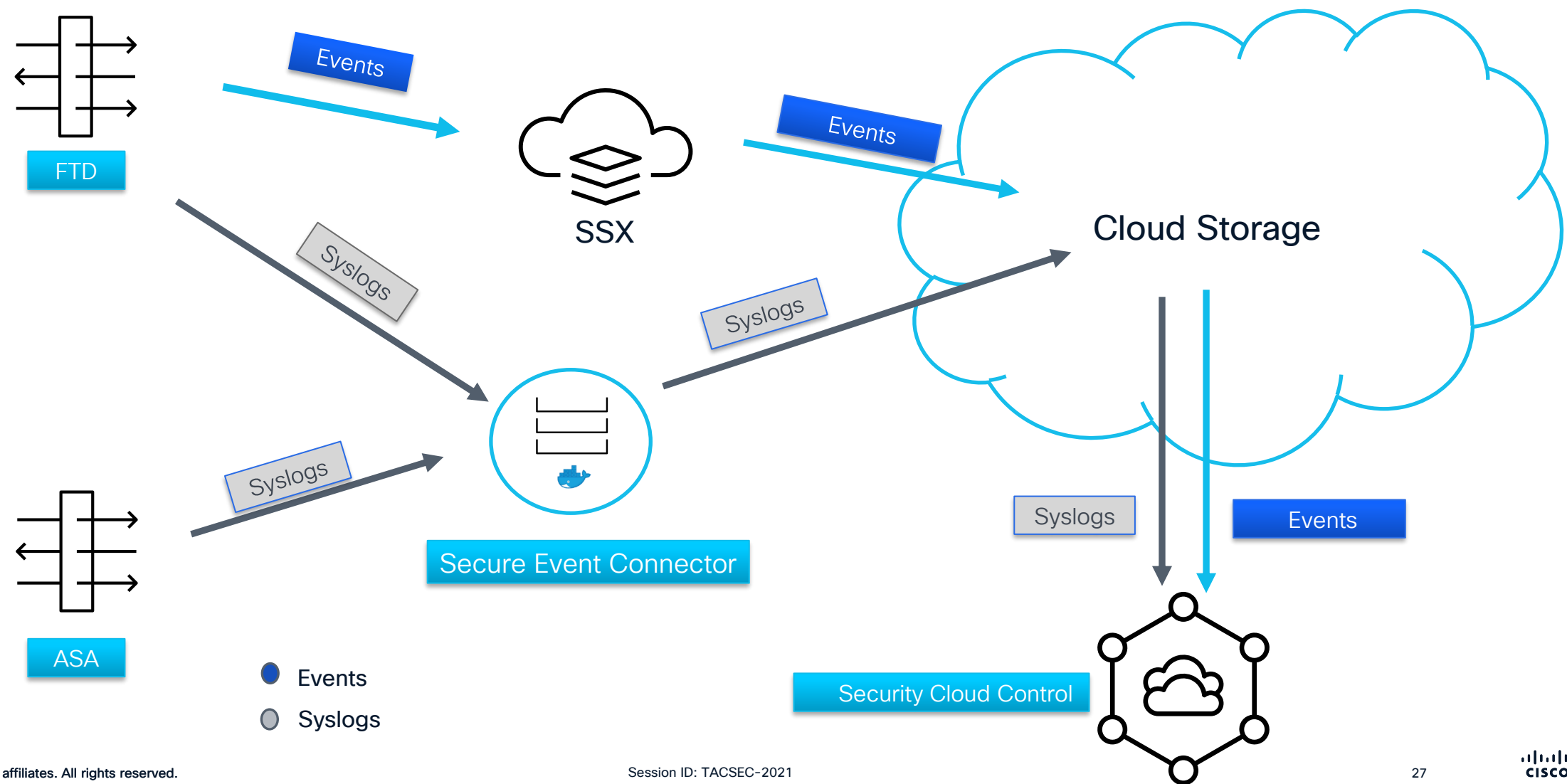
Register

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

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	Sensor ID / Hostname	Initiator IP	Responder IP	Responder Port	Protocol	Action	Policy
<div><div></div><div>No events found.</div></div> <div>SSC tenant is not seeing events on cloud storage</div>									

FTD Debug and Packet Capture

FTD CLISH >

```
> system support firewall-engine-debug
```

Collect a debug on your FTD clish

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 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

The screenshot shows the Cisco FMC 'Services' page. The left sidebar has 'Administration' highlighted. The main table lists services, with 'Cloud-Delivered FMC' selected. The right sidebar shows the service details and a list of actions, with 'Cisco Cloud Events' highlighted in the 'System' section.

Name	Version	Devices	Type	Status	Last heartbeat
Cloud-Delivered FMC	20250404	1	Cloud-Delivered FMC	Active	05/19/2025, 12:24:13

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.

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

FTD tenancy info

FTD Expert Mode ~\$:

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

Command
from expert
mode

```
{"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#
```

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@lmatusc1-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.

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

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 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 see when
was the last
success
connection to the
SSX service

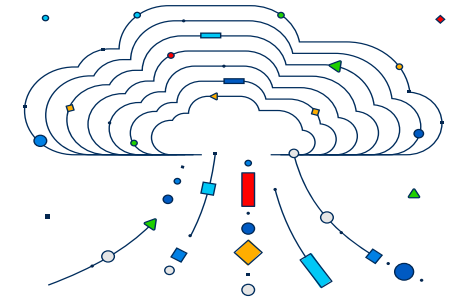
We can validate
how many
events the FTD
has sent to the
cloud





SCC Displaying Events

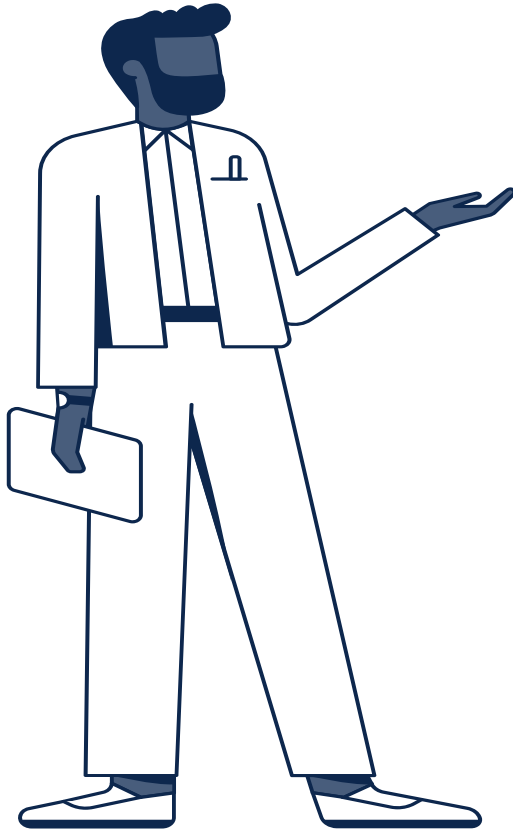
⊕	May 8, 2025, 00:03:54	FTD		Imatuscl-ftd....	172.18.2.5	72.163.4.185		icmp	Allow	ACP_test
⊕	May 8, 2025, 00:05:55	FTD		cl-ftd....	172.18.2.5	72.163.4.185	443	tcp	Allow	ACP_test
⊕	May 8, 2025, 00:05:55	FTD		cl-ftd....	172.18.2.5	72.163.4.185	443	tcp	Allow	ACP_test
⊕	May 8, 2025, 00:05:58	FTD		Imatuscl-ftd....	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	ACP_test

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 Connectivity
ClientAppDetectorID	0	FirewallRule	New-Rule-#1-ALLOW	NAT_InitiatorIP	00000000000000000000000000000000ac120104
ConnectionDuration	0	FirewallRuleList	New-Rule-#1-ALLOW	NAT_InitiatorPort	443
ConnectionID	7	FirstPacketSecond	May 8, 2025, 00:05:58 ⓘ	NAT_ResponderIP	0000000000000000000000000000000048a304b9
ConnectorID	6656a0a3-3980-41c5-8054-e1a56da674d1 ⓘ	Hostname	Imatuscl-ftd.internal.cloudapp.net	NAT_ResponderPort	443
Device	FTD_CL	IngressInterface	Inside	NetmapID	1
DeviceIP	172.18.0.4	IngressVRF	Global	PrefilterPolicy	Default Prefilter Policy
DeviceType	FTD	IngressZone	Inside	Protocol	tcp
DeviceUUID	70a88de6-2529-11f0-8167-9593bd28bd0b	InitiatorBytes	0	ResponderBytes	0
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 !

