

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

# Cisco Defense Orchestrator

Manage Your Cisco Firewalls Anywhere

Aaron K. Hackney, Technical Product Owner

BRKSEC-1138



#CiscoLive

# Your Speaker

Aaron K. Hackney

[aahackne@cisco.com](mailto:aahackne@cisco.com)

Technical Product Owner  
Cisco Defense Orchestrator

Living in San Antonio, Texas, Aaron comes from a service provider background, specializing in large firewall fleet operations with an emphasis on devops and operating at scale. Aaron holds an MS in computer science and is also a 15+ year veteran instructor of the Cisco Networking Academy having taught at colleges in both Illinois and Texas.



# Cisco Webex App

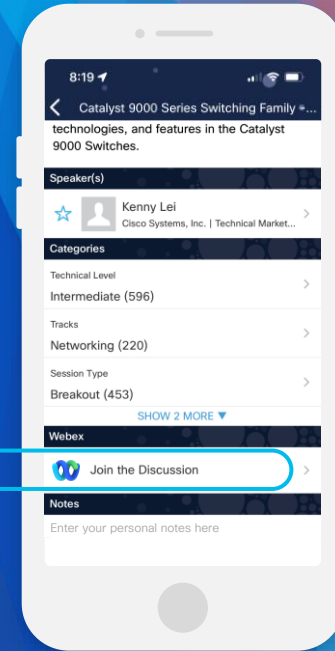
## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1138>

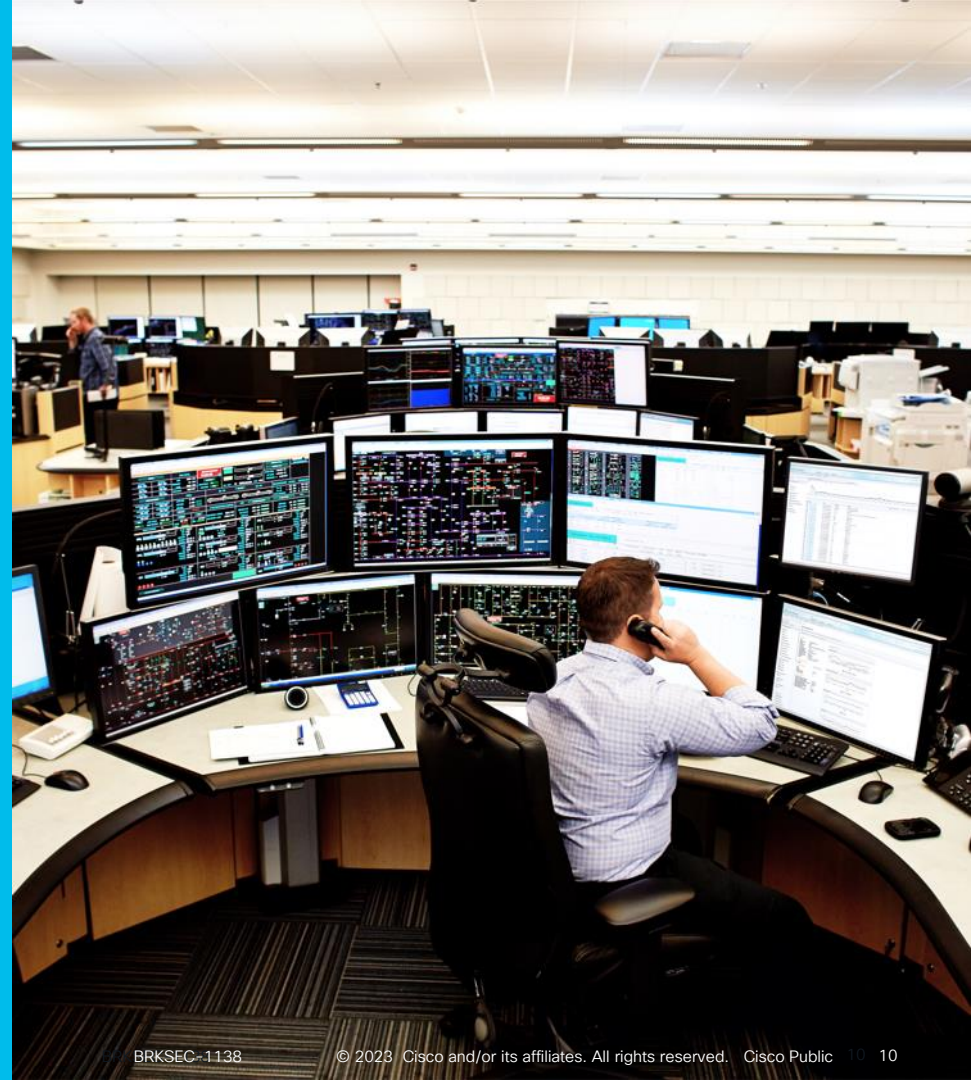
# Agenda

- Introduction/Overview – What, Where & Why?
- Cloud Delivered FMC and Managing FTD
- Multi-Cloud Defense
- Managing ASA and other Platforms
- Security Analytics and Logging
- API Integrations with API and Devops
- Wrap up

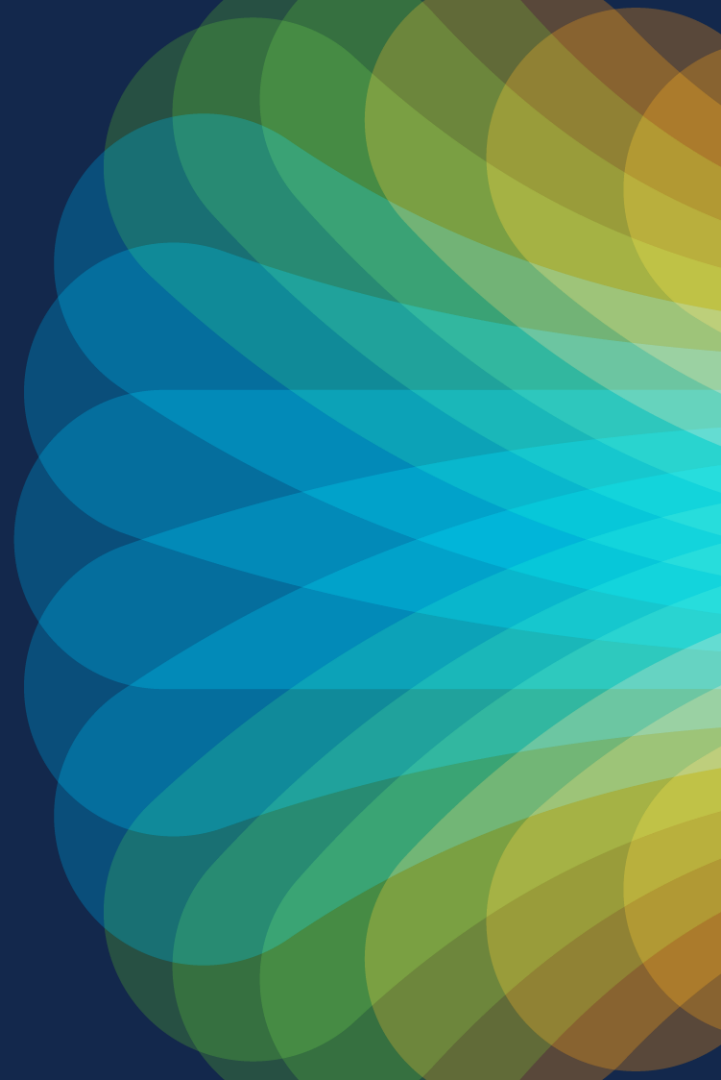
# Why Cisco Defense Orchestrator



Managing network  
and application  
security is hard  
work.



# CDO Solves Problems



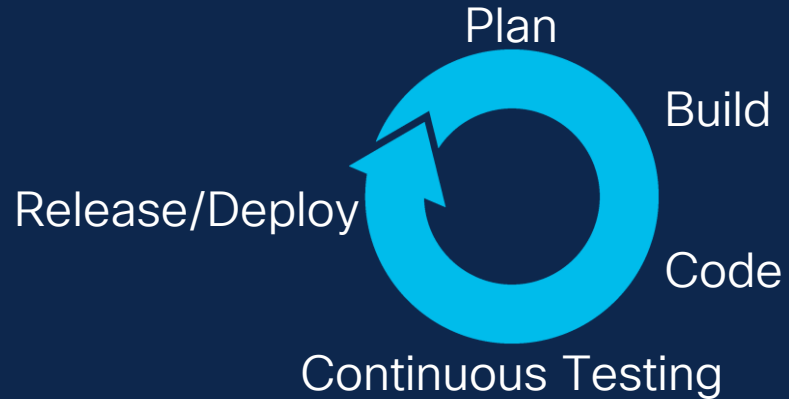


# CDO Solves Problems FAST

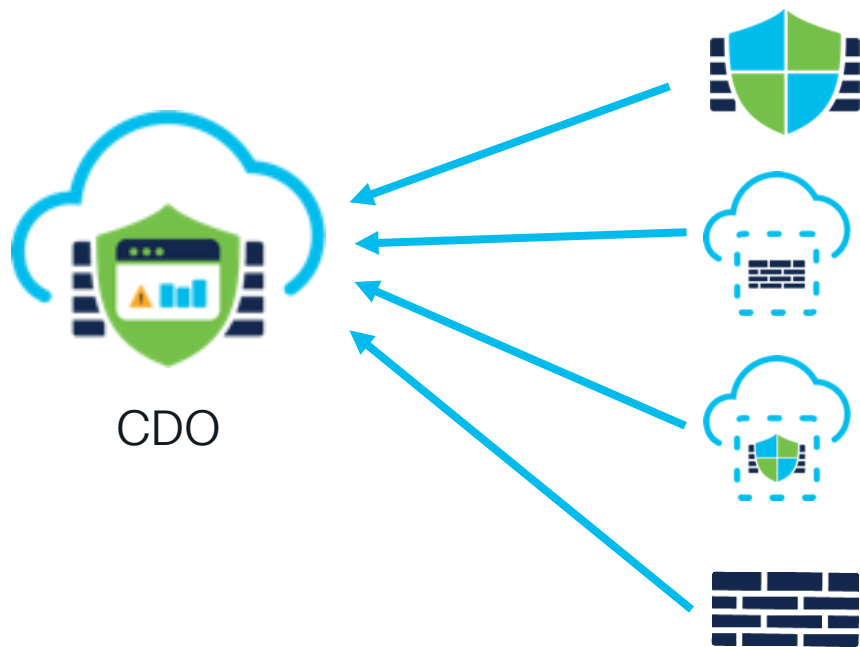
CDO is a SaaS leveraging a CI/CD Pipeline  
(Continuous Integration, Continuous Delivery)

## Releases/Sprints

- ❖ CDO 1 Week
- ❖ cdFMC 4-6 Weeks
- ❖ Customers ask...we deliver

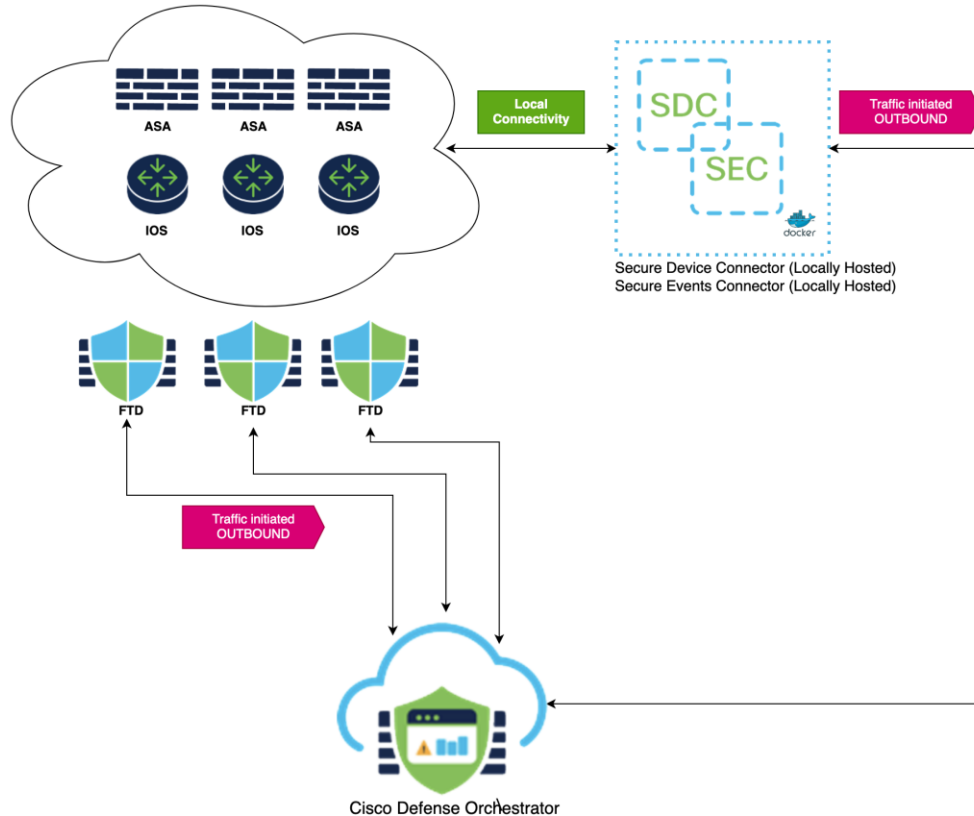


# CDO Needs NO Inbound Access



- ❖ Devices initiate connection via Internet
- ❖ CDO does not need inbound connectivity
- ❖ Flexible connectivity options
- ❖ CLI and API access via CDO
- ❖ SDC/SEC for ASA IOS

# CDO “Outbound Only” Connectivity



# CDO Manages Devices Anywhere

Physical Hardware, Public or Private Cloud Virtual, FTD Instances, ASA Contexts, and even containerized



# CDO Simplifies Advanced Tooling

## ❖ Migrate FTD from On-Prem FMC to cdFMC

The screenshot shows a web-based wizard titled "Migrate FTD to cdFMC" with the subtitle "Migrate FTD from OnPrem FMC to cloud". The interface includes a search bar and navigation icons at the top. The main content area displays a progress bar with three steps: "1 Select OnPrem FMC", "2 Select Devices", and "3 Finish". Step 1 is currently active and contains two numbered instructions: "1 Ensure that you have onboarded your OnPrem FMC to CDO via Credentials or SecureX. [Onboard an OnPrem FMC](#) or [learn more](#)" and "2 After your OnPrem FMC has been onboarded, select it from the list." Below these instructions, a label "Available OnPrem FMCs (7.2+ only)" is followed by a dropdown menu labeled "Select OnPrem FMC" and a "Next" button. A "Cancel" button is located in the top right corner of the wizard area.

Migrate FTD to cdFMC

Migrate FTD from OnPrem FMC to cloud

1 Select OnPrem FMC

2 Select Devices

3 Finish

1 Ensure that you have onboarded your OnPrem FMC to CDO via Credentials or SecureX. [Onboard an OnPrem FMC](#) or [learn more](#)

2 After your OnPrem FMC has been onboarded, select it from the list.

Available OnPrem FMCs (7.2+ only)

Select OnPrem FMC

Next

Cancel

# CDO Simplifies Advanced Tooling

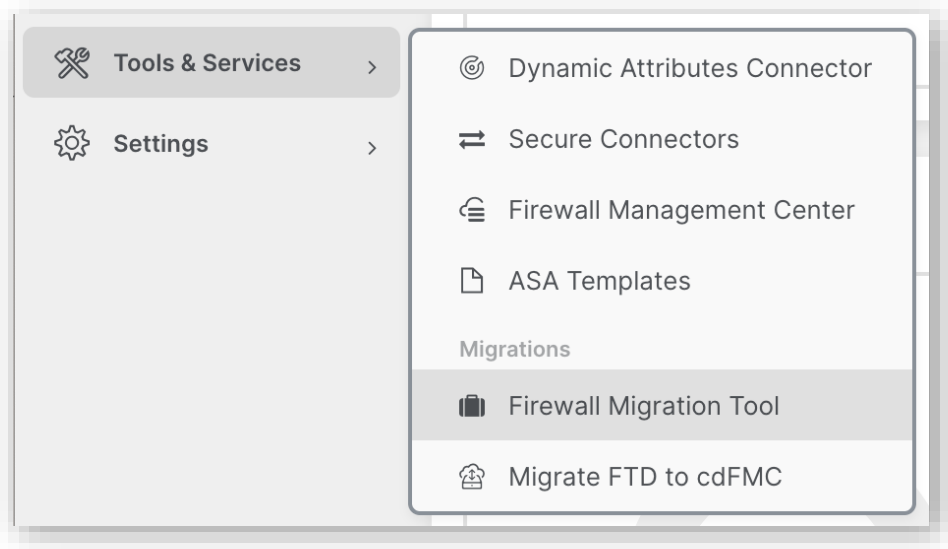
## ❖ Firewall Migration Tool

❖ ASA → cdFMC/FTD

❖ FDM → cdFMC/FTD

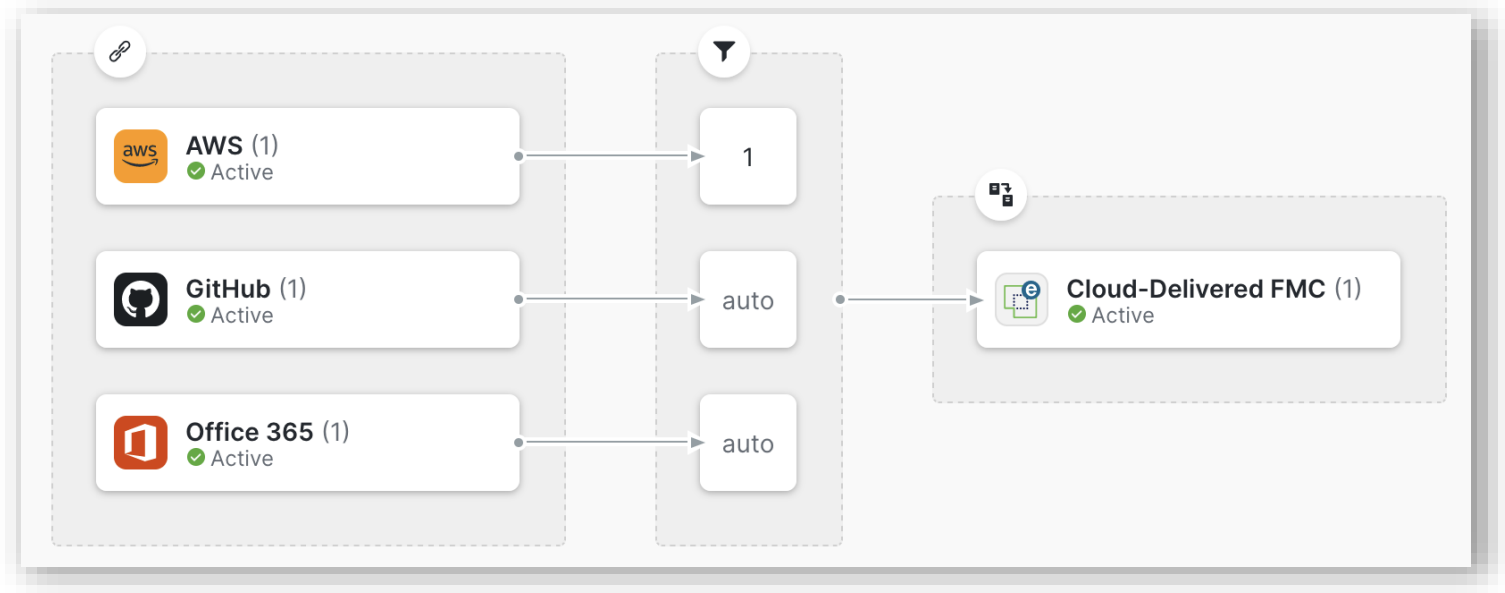
❖ PAN → cdFMC/FTD

❖ Fortinet → cdFMC/FTD



# CDO Simplifies Advanced Tooling

## ❖ Cisco Secure Dynamic Attributes Connector (CSDAC)





# CDO Simplifies Fleet Management

- ❖ Code version visibility
- ❖ Hardware/Serial number visibility
- ❖ High Availability

The screenshot displays the Cisco CDO Inventory management interface. At the top, there's a search bar and navigation tabs for 'Devices' and 'Templates'. Below this, a table lists several devices, with 'Berlin' selected. The table columns include Name, Version, Hostname, Location, HA Failover State, Last Deploy, Configuration Status, and Connectivity. To the right of the table, a sidebar provides detailed information for the selected 'Berlin' device, including its location, model, serial numbers, software versions, and configuration status. The device is shown as 'Synced' and 'Online'.

Name	Version	Hostname	Location	HA Failover State	Last Deploy	Configuration Status	Connectivity
Berlin ASA	9.19(1)	-	192.168.255.206:8443	-	5/11/2023 10:34:18 AM	Synced	Online
Clarksville ASA	9.16(3)19	-	10.10.6.42:8443	-	5/11/2023 10:34:48 AM	Synced	Online
Dayton ASA	9.16(3)19	-	10.10.6.44:44	-	5/11/2023 10:13:48 AM	Not Synced	Online
Dover-Branch ASA	9.14(2)15	-	12.181.219.112:443	-	5/15/2023 1:23:10 PM	Synced	Online
Minneapolis ASA	9.12(1)	-	10.10.6.6:443	Primary - Active	-	Synced	Online
Richmond ASA	9.15(1)	-	10.10.6.47:443	-	3/27/2023 4:56:39 PM	Synced	Online
VPN-Headend-Contractors ASA	9.14(3)	-	vasa-gb-ravpn-03-mgmt.dev.io:443	-	8/25/2021 9:42:23 AM	Synced	Online

**Device Details for Berlin**  
Location: 192.168.255.206:8443  
Model: ASA v (V01)  
Serial: 9A7N6H74W7M  
Chassis Serial: 9A7N6H74W7M  
Software Version: 9.19(1)  
ASDM Version: 7.19(1)  
Context Mode: Single Context  
Firewall Mode: Routed  
Uptime: 48 Days 21 Hours  
Failover Mode: Not Configured  
SDC: Demo-Red-AWS-SDC

**Synched**  
Your device's configuration is up-to-date.  
[Check for Changes](#)

**Scheduled Deployments**  
[Schedule](#)

**Device Actions**  
[Upgrade](#)  
[Command Line Interface](#)  
[Reconnect](#)  
[Update Credentials](#)


# CDO Simplifies Fleet Management

## ❖ Scheduled code upgrades

Device Upgrade / ASA: Berlin

Search

Return to Inventory



Device	Berlin
Model	ASAv (V01)
Location	192.168.255.206:8443
Fallover Mode	Not Configured

Disk Size 7.98 GB  
Disk Usage 188.41 MB

☒ Schedule Upgrade

May 31, 2023, 8:19 AM

1 ASA Software Image

ASA Software Image 9.19(1)  
☐ Skip Upgrade  
Image Source  
☒ Use CDO Image Repository  
☐ Specify Image URL  
Continue

Software Image  
Select an Image  
9.19(1.5) 142.33 MB

Select the ASA software image you want to upgrade to. Only compatible versions of ASA and ASDM are shown.

DNS must be properly configured on the device before attempting the upgrade. Please reference [Configure DNS on ASA](#) for details.

If you check "Skip Upgrade," the ASA software image on your device will not be changed. You may still upgrade ASDM.

2 ASDM Software Image

7.19(1) →

3 Perform Upgrade

CISCO Live!

#CiscoLive

BRKSEC-1138

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

20

# CDO Simplifies Fleet Management

## ❖ Notifications via email or webhooks

The screenshot displays the CDO configuration interface for notifications. It is divided into three main sections: 'Send Alerts When', 'Device Workflows', and 'Device Events'.

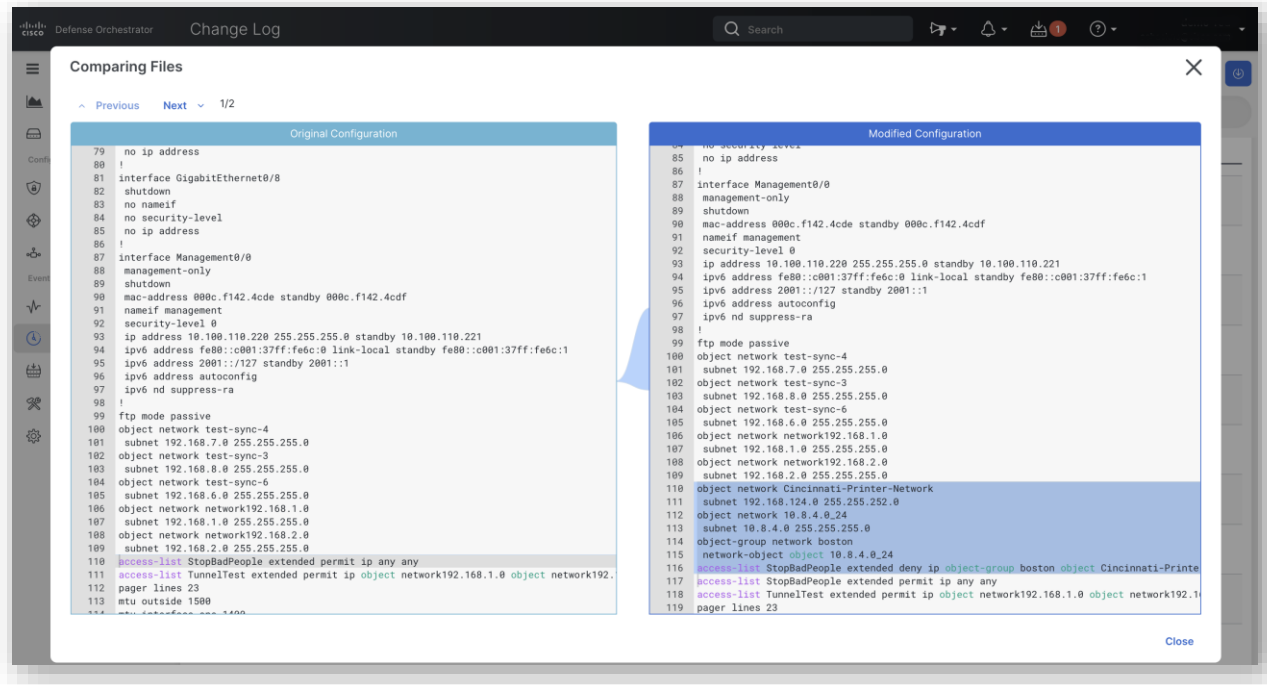
- Send Alerts When:** This section is currently empty.
- Device Workflows:** This section contains four categories of events, each with a checkbox for 'Failed', 'Started', and 'Succeeded' states.
  - Deployments:** All three checkboxes are unchecked.
  - Backups:** All three checkboxes are checked.
  - Upgrades:** All three checkboxes are checked.
  - Migrate FTD to cloud:** All three checkboxes are unchecked.
- Device Events:** This section contains a list of events, each with a checkbox.
  - All device events:** Checked.
  - Went offline:** Unchecked.
  - Back online:** Unchecked.
  - Conflict detected:** Unchecked.
  - HA state changed:** Checked.
  - Site-to-Site session disconnected:** Checked.

An 'Add Service Integration' modal is open in the bottom right corner. It has a title bar with a close button (X). The modal contains the following fields and options:

- Name:** A text input field containing 'CDO-Notifications'.
- Service Type:** A dropdown menu with 'Webex' selected. A list of options is visible below the dropdown: 'Webex', 'Slack', and 'Custom'.
- Webhook URL:** A text input field containing '1/webhooks/incoming/xxx'.
- Buttons:** 'Cancel' and 'Save' buttons are at the bottom right. A 'Test' button is located to the right of the webhook URL field.
- Help Links:** 'Learn More' links are present on the right side of the modal.

# CDO Simplifies Visibility

## ❖ Device configuration changes



# CDO Simplifies Visibility

## ❖ Remote Access VPN (Live and Historical)

The screenshot displays the Cisco Remote Access Monitoring interface. At the top, there's a search bar and navigation tabs for Historical, Live, RA VPN, and MFA. Below this is a table of active connections. A detailed view for user 'Karilyn' is shown on the right, providing information about her location, connection profile, and device details.

Username	Status	Device Name	Assigned IP (v4)	Assigned IP (v6)	Public IP	Login Time	Duration	Data TX	Data RX	Location
Juan	Active	Berlin	172.16.249.176	fcfe:eeee::77	173.38.117.79	08:14:41 05/31/2022	0h:5m:14s	3.79 KB	392 Bytes	Cary, North Carolina, United States
June	Active	Berlin	172.16.249.170	fcfe:eeee::72	173.38.117.79	08:19:41 05/31/2022	0h:0m:14s	3.79 KB	-	Cary, North Carolina, United States
Karilyn	Active	Berlin	172.16.249.138	fcfe:eeee::70	173.38.117.79	07:11:09 05/31/2022	1h:8m:46s	3.79 KB	560 Bytes	Cary, North Carolina, United States
Lee	Active	Berlin	172.16.249.153	fcfe:eeee::6c	173.38.117.79	07:35:10 05/31/2022	0h:44m:45s	3.79 KB	560 Bytes	Cary, North Carolina, United States
Madisen	Active	Berlin	172.16.249.175	fcfe:eeee::69	173.38.117.79	07:57:41 05/31/2022	0h:22m:14s	3.79 KB	504 Bytes	Cary, North Carolina, United States
Mirabel	Active	Berlin	172.16.249.137	fcfe:eeee::66	173.38.117.79	06:50:38 05/31/2022	1h:29m:17s	3.79 KB	616 Bytes	Cary, North Carolina, United States
Myron	Active	Berlin	172.16.249.169	fcfe:eeee::71	173.38.117.79	07:20:09 05/31/2022	0h:59m:46s	3.79 KB	560 Bytes	Cary, North Carolina, United States
Orlando	Active	Berlin	172.16.249.133	fcfe:eeee::66	173.38.117.79	07:40:10 05/31/2022	0h:39m:45s	3.79 KB	560 Bytes	Cary, North Carolina, United States
Ray	Active	Berlin	172.16.249.161	fcfe:eeee::6b	173.38.117.79	07:59:41 05/31/2022	0h:20m:14s	3.79 KB	504 Bytes	Cary, North Carolina, United States
Seth	Active	Berlin	172.16.249.166	fcfe:eeee::75	173.38.117.79	07:47:40 05/31/2022	0h:32m:15s	3.79 KB	560 Bytes	Cary, North Carolina, United States
Sherleen	Active	Berlin	172.16.249.139	fcfe:eeee::74	173.38.117.79	08:18:11 05/31/2022	0h:1m:44s	3.79 KB	280 Bytes	Cary, North Carolina, United States
Sue	Active	Berlin	172.16.249.163	fcfe:eeee::73	173.38.117.79	07:59:41 05/31/2022	0h:20m:14s	3.79 KB	504 Bytes	Cary, North Carolina, United States
Timothy	Active	Berlin	172.16.249.132	fcfe:eeee::64	173.38.117.79	07:46:10 05/31/2022	0h:33m:45s	3.79 KB	504 Bytes	Cary, North Carolina, United States
paul-1	Active	VPN-Headend-Controller	192.168.128.72		34.228.89.40	08:26:27 05/31/2022	0h:3m:40s	12.21 KB	79.03 MB	Ashburn, Virginia, United States
paul-10	Active	VPN-Headend-Controller	192.168.128.81		34.228.89.40	08:26:32 05/31/2022	0h:3m:35s	12.21 KB	77.12 MB	Ashburn, Virginia, United States
paul-2	Active	VPN-Headend-Controller	192.168.128.73		34.228.89.40	08:26:28 05/31/2022	0h:3m:39s	12.21 KB	78.84 MB	Ashburn, Virginia, United States
paul-3	Active	VPN-Headend-Controller	192.168.128.74		34.228.89.40	08:26:28 05/31/2022	0h:3m:39s	12.21 KB	78.26 MB	Ashburn, Virginia, United States
paul-4	Active	VPN-Headend-Controller	192.168.128.75		34.228.89.40	08:26:29 05/31/2022	0h:3m:38s	12.21 KB	78.42 MB	Ashburn, Virginia, United States

### Karilyn

Connected for 1h:8m:46s

#### User Details

**Location**  
Cary, North Carolina, United States

**Connection Profile**  
CERT-AUTH

**Group Policy**  
DemoRed

**Assigned IP (v4)**  
172.16.249.138

**Assigned IP (v6)**  
fcfe:eeee::70

**Public IP**  
173.38.117.79

**Data Received**  
560 Bytes

**Data Transmitted**  
3.79 KB

**Client OS Type**  
Linux (64-bit)

**Idle Timeout Left**  
30 Minutes

#### Device Details

**Device Name**  
Berlin

**Device Type**  
ASA

**Security Group Tag**  
none

# CDO Simplifies Visibility

## ❖ Site-to-Site VPN

The screenshot displays the Cisco CDO interface for configuring and monitoring a Site-to-Site VPN. The main window is titled "Edit Site-to-Site VPN" and shows a configuration form for a "Berlin-Clarksville" tunnel. The form is divided into two sections: "Peer 1" (Berlin) and "Peer 2" (Clarksville). The "Policy Based" option is selected. The "Protected Networks" section shows "Berlin-Inside-Net" and "Clarksville-Inside-Net" as protected networks. The "NAT Exempt Interface" is set to "inside".

Below the configuration form, there is a "Policies" section with a table showing the configured policy:

Action	Protocol	Source	Port	Destination	Port
PERMIT	ip	Berlin-Inside-Net	any	Clarksville-Inside-Net	any

On the right side of the interface, there is a "VPN Tunnels / Berlin" section showing a diagram of the tunnel connection between Berlin and Clarksville. Below the diagram, there is a "Tunnel Details" section with a table showing the tunnel's status:

Connectivity	Last Seen Active	Last Checked
idle	-	5/31/23 8:20 AM

# CDO Simplifies Visibility

## ❖ Centralized Logging and Analytics for ASA and FTD

The screenshot displays the Cisco CDO Event Logging interface. At the top, there's a search bar and navigation tabs for 'Historical' and 'Live'. Below this, a time range filter is set to '05/30/2023 04:00:28 to 05/31/2023 04:00:28'. A filter bar shows categories like 'FTD Events', 'Intrusion', 'Malware', 'Security Intelligence', 'Connection', and 'File'. The main table lists events with columns for Date/Time, Device Type, Event Type, Sensor ID / Hostname, Initiator IP, Responder IP, Port, Protocol, Action, and Policy. A detailed view of a specific event is shown below the table, listing various fields like AC\_RuleAction, AC\_RuleReason, CSV Generation Time, DeviceType, EgressInterface, EgressVRF, EgressZone, EventSecond, EventSubtype, EventType, FirewallPolicy, FirstPacketSecond, IP\_ReputationSI\_Category, IngressInterface, IngressVRF, IngressZone, InitiatorBytes, InitiatorIP, ConnectionEvent, Edge-Firewall, InitiatorPackets, InitiatorPort, PrefilterPolicy, Protocol, ResponderIP, ResponderPort, SI\_Direction, and timestamp.

Date/Time	Device Type	Event Type	Sensor ID / Hostname	Initiator IP	Responder IP	Port	Protocol	Action	Policy
May 30, 2023, 05:49:14	FTD	Connection		198.235.24.232	172.30.3.194	32400	tcp	Block	Edge-Firewall
May 30, 2023, 06:10:33	FTD	Connection		205.210.31.243	172.30.4.102	8443	tcp	Block	Edge-Firewall

Field	Value	Field	Value	Field	Value
AC_RuleAction	Block	Event Type	ConnectionEvent	InitiatorPackets	1
AC_RuleReason	IP Block	FirewallPolicy	Edge-Firewall	InitiatorPort	56729
CSV Generation Time	1685505641	FirstPacketSecond	May 30, 2023, 06:10:29	PrefilterPolicy	Default Prefilter Policy
DeviceType	FTD			Protocol	tcp
EgressInterface	lab_management	IP_ReputationSI_Category	Malware	ResponderIP	172.30.4.102
EgressVRF	Global	IngressInterface	outside	ResponderPort	8443
EgressZone	lab_management	IngressVRF	Global	SI_Direction	Source
EventSecond	May 30, 2023, 06:10:29	IngressZone	outside	timestamp	May 30, 2023, 06:10:33
EventSubtype	Start	InitiatorBytes	58		
		InitiatorIP	205.210.31.243		

May 30, 2023, 09:41:32	FTD	Connection		198.235.24.193	172.30.4.102	8443	tcp	Block	Edge-Firewall
May 30, 2023, 11:00:25	FTD	Connection		185.180.143.11	172.30.4.102	8443	tcp	Block	Edge-Firewall
May 30, 2023, 19:04:27	FTD	Connection		198.235.24.117	172.30.4.102	8443	tcp	Block	Edge-Firewall
May 30, 2023, 20:44:33	FTD	Connection		185.233.19.18	172.30.4.102	8443	tcp	Block	Edge-Firewall



# CDO Simplifies FTD Management at Scale

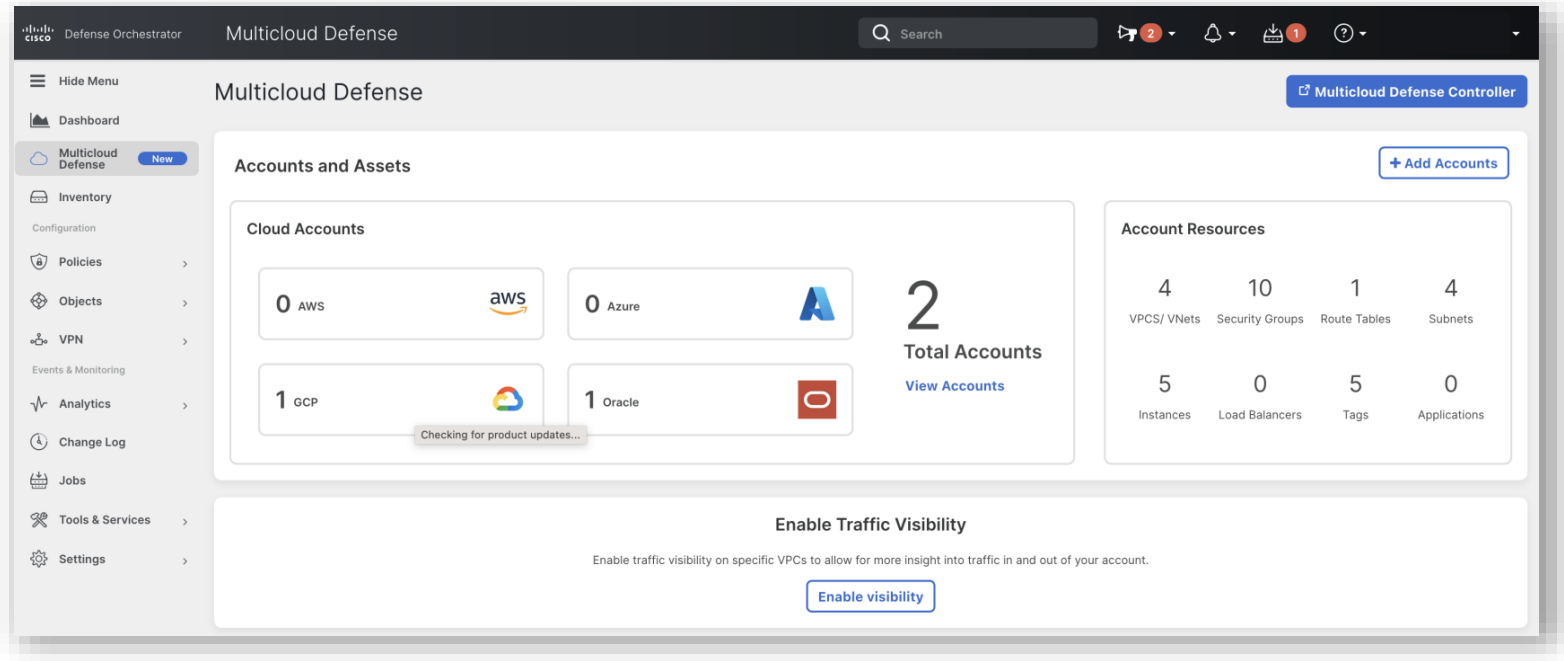
❖ Manage up to 1000 FTDs from a single instance of cdFMC

The screenshot displays the Cisco Defense Orchestrator (CDO) interface for managing Firepower Threat Devices (FTDs). The top navigation bar includes tabs for Analysis, Policies, Devices (selected), Objects, and Integration. The breadcrumb trail shows 'FMC / Devices / Device Management'. The interface features a 'View By: Group' dropdown and a status filter bar with counts for various states: All (6), Error (0), Warning (0), Offline (0), Normal (6), Deployment Pending (5), Upgrade (0), and Snort 3 (6). A search bar and an 'Add' button are also present. The main content area shows a table of FTDs, with a 'Collapse All' link at the top left. The table columns are Name, Model, Version, Chassis, Licenses, Access Control Policy, Auto RollBack, and a menu icon. The table lists several groups: Canada (2), Ottawa (High Availability), and Cloud (2). Under the Ottawa group, two FTDs are listed: 'Ottawa-PR1(Primary, Active)' and 'Ottawa-SEC(Secondary, Standby)', both with status 'N/A - Routed' and 'Snort 3'. Under the Cloud group, an 'AWS-FTD' is listed with status 'N/A - Routed' and 'Snort 3'. Each row includes a checkbox, a status indicator (green dot), a name, a status label, a model, version, chassis, licenses, access control policy, auto rollback, and a menu icon.

	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Canada (2)							
<input type="checkbox"/>	Ottawa High Availability							
<input checked="" type="checkbox"/>	Ottawa-PR1(Primary, Active) N/A - Routed	FTDv for VMware	7.2.0	N/A	Essentials, IPS (2 more...)	Default Access Control Policy		
<input checked="" type="checkbox"/>	Ottawa-SEC(Secondary, Standby) N/A - Routed	FTDv for VMware	7.2.0	N/A	Essentials, IPS (2 more...)	Default Access Control Policy		
<input type="checkbox"/>	Toronto N/A - Routed	FTDv for VMware	7.2.0	N/A	Essentials, IPS (2 more...)	Default Access Control Policy		
<input type="checkbox"/>	Cloud (2)							
<input type="checkbox"/>	AWS-FTD N/A - Routed	FTDv for AWS	7.2.0	N/A	Essentials, IPS (2 more...)	Default Access Control Policy		

# CDO Simplifies Cloud Security






## ❖ Integration with Multicloud Defense



# CDO to integrate with “all the things”



# ASA Object and Policy Management

Line	Action	Protocol	Source	Port	Destination	Port	Hits (Day)
1	 permit ▾	tcp ▾	192.168.0.1 ▾	any ▾	any ▾	eq https ▾	0000
2	 permit		10.10.10.0/24	any	any	www	0000
3	 deny		foobar2	any	any	any	0000
4	 Permit	tcp	6.6.6.8	any	1.1.0/24	domain	0000
5	 Permit	ip	anyconnect-net	any	any	any	0000


✕ Cancel

Save

Network Policy ▾

Edit Tools

+ ✂ 📄 📄 🗑

Active 

# AWS VPC Security Group Policy Management

Defense Orchestrator

AWS VPC Policies / vpc-28a5154d (AWS-DC-West-Demo-Red)

Return to Inventory

Packets → Security Groups

Search

Cisco Adaptive Security Virtual Appliance -ASA-- Standard Package-9-13-1-155 -9-13-1-10 ---AutogenByAWSMP-

Direction	Name	Action	Source	Destination
Inbound	Cisco Adaptive Security Virtual...	Allow	Any IPv4	PORTS TCP:22
Inbound	Cisco Adaptive Security Virtual...	Allow	Any IPv4	PORTS TCP:443
Outbound	Cisco Adaptive Security Virtual...	Allow	Any	Any IPv4

Cisco Firepower NGFW Virtual -NGFW-- - BYOL-6-6-0-90-AutogenByAWSMP-

Direction	Name	Action	Source	Destination
Inbound	Cisco Firepower NGFW Virtual ...	Allow	Any IPv4 12APR2019-...	PORTS TCP:80
Inbound	Cisco Firepower NGFW Virtual ...	Allow	Any IPv4	PORTS TCP:22
Inbound	Cisco Firepower NGFW Virtual ...	Allow	Any IPv4	PORTS TCP:443
Outbound	Cisco Firepower NGFW Virtual ...	Allow	Any	Any IPv4

# Meraki MX Policy Management

Defense Orchestrator

MX Policies / Hollis Regional Office

Return to Inventory

Packets → Access Control

3 rules

#	Name	Action	Source	Destination
1	BlockBadness	Block	Any	NETS: DangerDanger, ExpediteBlock
2	Hollis Regional Office_L3_Rule...	Block	NETS: 10.0.0.224/32 PORTS: TCP:80	NETS: 22.22.22.22/32, IT-Team-Valu... PORTS: TCP:80
3	AdamTest	Allow	Any	NETS: 10.31.12.90

# IOS Bulk CLI Access & Config Visibility

The screenshot displays the Cisco Bulk CLI web interface. On the left, a 'Macros' sidebar lists various pre-configured commands like 'Clear all connections', 'show version', 'GoogleDNS', 'Device Cert Check', 'License Review', 'Configure NSEL', 'DELETE NSEL', 'Create a S2S IPSEC...', 'Set My DNS', and 'LongReceipts'. The main panel shows a command 'show route' entered in the 'Command sent on 5/18/2022, 2:31:29 PM' field. Below the command input, a 'My List' sidebar shows two selected devices: 'Clarksville' and 'Austin'. The 'Execution' tab is active, showing a 'Send' button. On the right, a summary panel shows '2 By Response' and '2 By Device', with a list of '1 Devices' for each: 'Clarksville' and 'Austin'. The bottom section displays the 'Showing response for 1 Devices' output for the 'show route' command.

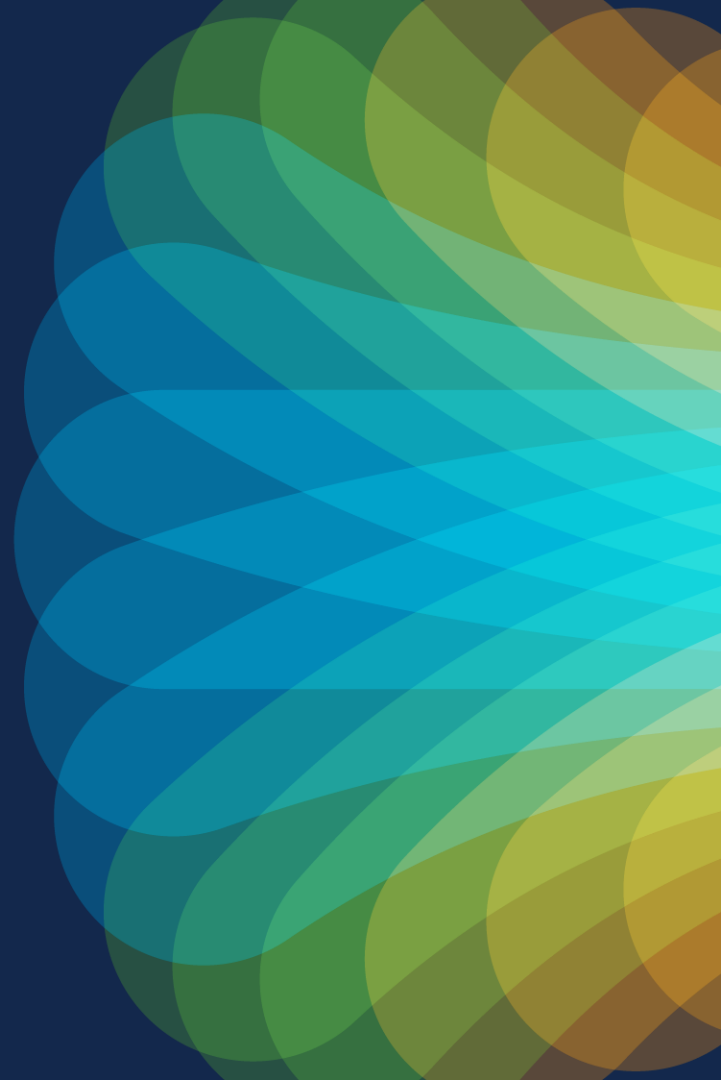
```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF

Gateway of last resort is 10.10.6.33 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.10.6.33, outside
C 10.10.6.0 255.255.255.192 is directly connected, outside
L 10.10.6.42 255.255.255.255 is directly connected, outside
S 10.252.184.224 255.255.255.224 [1/0] via 64.68.115.52, inside
C 192.168.228.0 255.255.255.0 is directly connected, inside
L 192.168.228.1 255.255.255.255 is directly connected, inside
```



# Multicloud Defense



# Multicloud Defense

The screenshot shows the Cisco Defense Orchestrator Multicloud Defense dashboard. The interface includes a top navigation bar with the Cisco logo, 'Defense Orchestrator', and 'Multicloud Defense' text. A search bar and notification icons are also present. A left sidebar contains a 'Hide Menu' button and a list of navigation items: Dashboard, Multicloud Defense (highlighted with a 'New' badge), Inventory, Configuration, Policies, Objects, VPN, Events & Monitoring, Analytics, Change Log, Jobs, Tools & Services, and Settings. The main content area is titled 'Multicloud Defense' and features a '+ Add Accounts' button. Below this, the 'Accounts and Assets' section displays 'Cloud Accounts' with a grid showing 0 AWS, 0 Azure, 1 GCP, and 1 Oracle account. A large '2 Total Accounts' summary is shown with a 'View Accounts' link. A 'Checking for product updates...' tooltip is visible over the GCP account. To the right, the 'Account Resources' section shows counts for VPCS/ V Nets (4), Security Groups (10), Route Tables (1), Subnets (4), Instances (5), Load Balancers (0), Tags (5), and Applications (0). At the bottom, an 'Enable Traffic Visibility' section provides instructions and an 'Enable visibility' button.

**Multicloud Defense**

**Accounts and Assets**

**Cloud Accounts**

- 0 AWS
- 0 Azure
- 1 GCP
- 1 Oracle

**2 Total Accounts**  
[View Accounts](#)

**Account Resources**

Resource	Count
VPCS/ V Nets	4
Security Groups	10
Route Tables	1
Subnets	4
Instances	5
Load Balancers	0
Tags	5
Applications	0

**Enable Traffic Visibility**

Enable traffic visibility on specific VPCs to allow for more insight into traffic in and out of your account.

[Enable visibility](#)

# Multicloud Defense

FULL CONFERENCE

IT LEADERSHIP

## Consistently Secure the Multicloud at Any Scale with Cisco - BRKSEC-2145



John Clark, Cisco

Schedule

Thursday, Jun 8 | 9:30 AM - 10:30 AM PDT | Level 3, Palm D

The multicloud introduces unique security concerns, fueled by dramatic implementation differences between public cloud providers. With the recent introduction of Cisco Multicloud Defense, Cisco can now provide an innovative approach to consolidating and improving security across your environment.

In this session you will learn in detail how Cisco Multicloud Defense delivers cloud-native firewalling along with automation and cloud networking to accelerate your transition to the multi-cloud.

# Cloud Delivered Firewall Management Center (cdFMC)

# Cloud Delivered Firewall Management Center



- ❖ Cloud native FMC platform provided by Cisco Defense Orchestrator
- ❖ Not just a lift-and-shift VM of FMC
- ❖ Manage any FTD from any form factor – physical or virtual
- ❖ Manage any FTD from anywhere

# Cloud Delivered Firewall Management Center



- ❖ Manage up to 1000 FTDs from a SINGLE INSTANCE of cdFMC
- ❖ Roadmap is 2000 FTDs from a single instance
- ❖ Rapid release CI/CD pipeline = new features in **weeks** instead of months
- ❖ SaaS – Cisco FULLY manages and maintains the FMC
- ❖ SaaS – Focus on managing security posture, not “managing the manager”

# Cloud Delivered Firewall Management Center




Requirements to be managed by cdFMC:

- ❖ FTD Version 7.0.3+ minimum
- ❖ FTD Version 7.2+ to use Low Touch Provisioning (LTP)
- ❖ OnPrem FMC 7.2+ to migrate FTD to cdFMC (Manager migration)
- ❖ Internet access from management-interface **or** from a data-interface
- ❖ Legacy FMC migration coming soon!




# Complete FTD Mgmt with cdFMC

 Defense Orchestrator  
Devices / Device Management

MonitoringPolicies**Devices**ObjectsIntegration

[Return to Inventory](#) Deploy 🔍 📢 ⚙️ ? aahackne@cisco.com












View By: Group

[Deployment History](#)

All (4) Error (1) Warning (0) Offline (1) Normal (2) Deployment Pending (3) Upgrade (0) Snort 3 (4)

Add

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	> Peoria (1)							
<input type="checkbox"/>	▼ Ungrouped (2)							
<input type="checkbox"/>	 <b>Ottawa</b> <span>Snort 3</span> <span>N/A - Routed</span>	FTDv for VMware	7.2.0	N/A	Base, Threat (2 more...)	 <a href="#">Corporate-FW-Policy</a> 		
<input type="checkbox"/>	 <b>Toronto</b> <span>Snort 3</span> <span>N/A - Routed</span>	FTDv for VMware	7.2.0	N/A	Base, Threat (2 more...)	 <a href="#">Default Access Control Policy</a> 		

# Deploy FTD to Cloud of Choice

Onboard FTD Device

Follow the steps below

Cancel

**Firewall Threat Defense**  
Management Mode:  
☒ FTD ☐ FDM  
(Recommended)

**Important:** After onboarding your FTD, it will be managed by Firewall Management Center in CDO. Note that use of the firewall device manager will not be available after onboarding, and all existing policy configurations will be reset. You will need to reconfigure policies from CDO after onboarding. [Learn more](#)

**Use CLI Registration Key**  
Onboard a device using a registration key generated from CDO and applied on the device using the Command Line Interface.  
(FTD 7.0.3+ & 7.2+)

**Use Serial Number**  
Use this method for low-touch provisioning or for onboarding configured devices using their serial number.  
(FTD 7.2+)

**Deploy an FTD to a cloud environment**  
Deploy an FTD to a supported cloud environment; AWS, GCP and Azure

1 Cloud Provider Selection

Select Cloud Provider

Select Cloud Provider

AWS

Azure

GCP

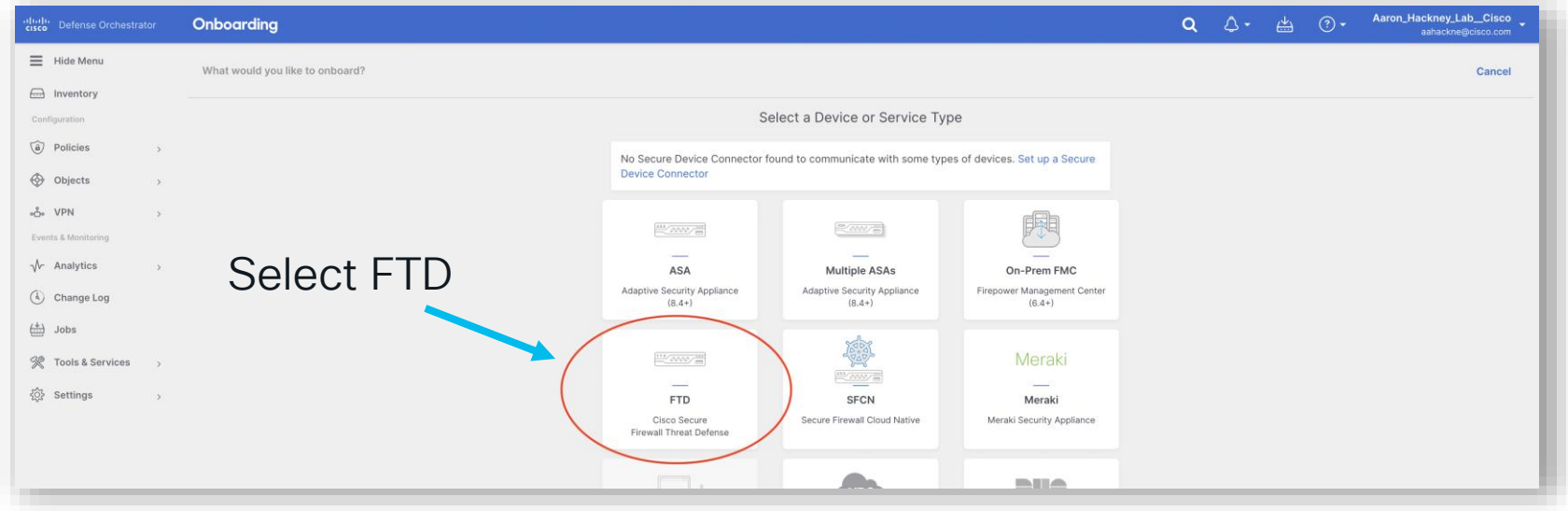
- ❖ Wizard Driven
- ❖ Deploy instance
- ❖ Auto-Add to cdFMC
- ❖ All from CDO

# Onboard Cisco Secure Firewall

The screenshot shows the Cisco Defense Orchestrator (DO) interface. The left sidebar contains a menu with options: Hide Menu, Inventory, Configuration (Policies, Objects, VPN, Migrations), Events & Monitoring (Monitoring, Change Log, Jobs), and Admin. The main content area is titled 'Inventory' and has tabs for 'Devices' and 'Templates'. A search bar is present with the text 'Search by Device Name, IP Address, or Serial Number'. Below the search bar, there is a table with columns: Name, Configuration Status, and Connectivity. The table contains one entry for 'arid-pirate' with a status of 'Synced' and connectivity 'Online'. A red circle highlights the '+' button in the top right corner of the table, with a callout bubble saying 'Click (+)'.

Name	Configuration Status	Connectivity
arid-pirate FTD High Availability Primary Standby Secondary Active	Synced	Online

# Onboard Cisco Secure Firewall



# Onboard Cisco Secure Firewall

Low touch provisioning for  
FPR1000, FPR2100, FPR3100

See demo video [here](#)

“configure manager” CLI method

**FTD**

**Firewall Threat Defense**

**Manage Smart License**

**Important:** After onboarding your FTD, it will be managed by Firewall Manager. Firewall Manager will not be available after onboarding, and all existing policy configurations will be lost after onboarding. [Learn more](#)

**Use CLI Registration Key**

Onboard a device using a registration key generated from CDO and applied on the device using the Command Line Interface.  
(FTD 7.0.3+ & 7.2+)

**Use Serial Number**

Use this method for low-touch provisioning or for onboarding configured devices using their serial number.  
(FTD 7.2+)

# Onboard Cisco Secure Firewall

The screenshot shows a multi-step onboarding wizard for a Cisco Secure Firewall. The steps are:

- 1 Device Name: CHICAGO-PRIMARY
- 2 Policy Assignment: Access Control Policy. A dropdown menu is open, showing 'Default Access Control Policy' as the selected option. A blue arrow points to the dropdown with the text 'Assign the default policy'.
- 3 Subscription License
- 4 Create Registration Key
- 5 Done

The 'Policy Assignment' step is currently active. The dropdown menu for 'Access Control Policy' is open, showing a search bar and a list of options. The 'Default Access Control Policy' is highlighted. The 'Select' button is visible at the bottom right of the dropdown.

# Onboard Cisco Secure Firewall

**3** Subscription License ⓘ



Please indicate if this FTD is physical or virtual:

☐ Physical FTD Device

☒ Virtual FTD Device

Performance Tier (FTDv 7.0 and above only)

FTDv10 - Tiered (4 core / 8 GB) ▼

License Type	Includes
<input checked="" type="checkbox"/> Base License	Base Firewall Capabilities
<input checked="" type="checkbox"/> Threat	 Intrusion Policy
<input checked="" type="checkbox"/> Malware	 File Policy
<input checked="" type="checkbox"/> URL License	URL Reputation
<input type="checkbox"/> RA VPN	VPNOnly ▼ RA VPN

**Next**

- ❖ Select the device form factor
- ❖ Select the tier (virtual only)
- ❖ Select the feature entitlements

# Onboard Cisco Secure Firewall

**4** Create Registration Key

**Copy registration command to clipboard**

1 Enable network connectivity for your FTD using either a management or data interface. [Learn more](#)

2 Copy registration command

```
configure manager add  
aahackne.app.  
QBxTbaEzY0AkCFzfEutvYgJwhjm87RG0  
fH9fDncshZ54V0HoYUh9PcXond17vHLU  
aahackne.app.
```

3 Paste the registration command copied above in the Command Line Interface of the FTD. [Learn more](#)

Next



# Onboard Cisco Secure Firewall

Refresh connectivity status

The screenshot displays the Cisco Secure Firewall onboarding interface. At the top, there are tabs for 'Devices' and 'Templates', a search bar, and a 'Displaying 2 of 2 results' indicator. Below this is a table with columns for 'Name', 'Configuration Status', and 'Connectivity'. The table lists a device named 'CHICAGO-PRIMARY' with a status of 'Pending Setup' and a connectivity of 'Online'. A red circle highlights the 'Pending Setup' status, with a callout box stating: 'If you need to re-copy the configuration command it is available from the inventory device level once you have completed the onboarding wizard. Status of the onboarding is also available here.'

On the right side, there is a 'CHICAGO-PRIMARY' device details panel. It shows 'Device Details' including Location, Model, Serial, Version, Onboarding Method, and Registration Key. Below this, a 'Registration Failed' error message is displayed, stating: 'Device registration failed. Please check Workflows for more details about the error. Complete the onboarding process by executing the following registration command on the device (ignore if already done). Make sure your FTD can connect to [aahackne.app.staging.cdo.cisco.com](https://aahackne.app.staging.cdo.cisco.com). To retry onboarding, click the 'Retry Onboarding' link below.'

Below the error message, there is a text box containing the command: 'configure manager add aahackne.app.s...' and a 'Retry Onboarding' button. A red circle highlights this area, with a callout box stating: 'Registration will retry every 5 minutes or We can click "Retry Onboarding" for on-demand retry.'

A blue arrow points from the 'Refresh connectivity status' text to a refresh icon in the top right corner of the interface.

# Onboard Cisco Secure Firewall

```
→ ~ ssh admin@172.30.4.117
Warning: Permanently added '172.30.4.117' (ECDSA) to the list of known hosts.
Password:
Last login: Mon May 16 15:43:30 UTC 2022 on tty0

Copyright 2004-2022, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.12.0 (build 16)
Cisco Firepower Threat Defense for VMware v7.2.0 (build 39)

> ping system cisco.com
PING cisco.com (72.163.4.185) 56(84) bytes of data.
64 bytes from redirect-ns.cisco.com (72.163.4.185): icmp_seq=1 ttl=240 time=10.3 ms
64 bytes from redirect-ns.cisco.com (72.163.4.185): icmp_seq=2 ttl=240 time=10.5 ms
^C
--- cisco.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2ms
rtt min/avg/max/mdev = 10.290/10.417/10.544/0.127 ms
>
```

Ensure **management-plane** has outbound Internet access and DNS resolution is working

```
ping system <hostname>
```

# Onboard Cisco Secure Firewall

Paste the CDO generated configuration to the FTD CLI

```
> configure manager add aahackne. [REDACTED] cdo.cisco.com QBxTbaEzY0AkCFzfEutvYgJwhjm8
7RG0 [REDACTED] LU aahackne [REDACTED] .com

If you enabled any feature licenses, you must disable them in Firepower Device Manager
before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco Smart Software Manager
.
Do you want to continue[yes/no]:yes
Local Manager successfully deleted.

No managers configured.
File HA_STATE is not found.
Manager aahackne.app.[REDACTED] successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

> [REDACTED]
```

# Onboard Cisco Secure Firewall

Displaying 2 of 2 results

Connectivity

- Onboarding
- Online

### CHICAGO-PRIMARY

FTD

Device Details

Location	n/a
Model	n/a
Serial	n/a
Version	n/a
Onboarding Method	Registration Key

**Syncing**

Successfully registered the device. Deployment is in progress. Please check back in a moment.

- ❖ SFTunnel was successfully built
- ❖ Initial device config and default policy are being pushed to the FTD

# Onboard Cisco Secure Firewall

The screenshot displays the Cisco Secure Firewall Management Center (FMC) Inventory page. The left sidebar shows the 'Inventory' section with 'Devices' selected. The main table lists two devices:

Name	Configuration Status	Connectivity
CHICAGO-PRIMARY FTD	Synced	Online
arid-pirate FTD High Availability Primary Standby Secondary Active	Synced	Online

The right sidebar shows the details for the selected device, CHICAGO-PRIMARY. The 'Device Details' section includes:

- Location: n/a
- Model: Cisco Firepower Threat Defense for VMware
- Serial: 9AG4K0V2BXE
- Version: 7.2.0
- Onboarding Method: Registration Key

The 'Synced' status is highlighted with a blue arrow pointing to the 'Synced' details panel, which states: 'Your device's configuration is up-to-date.' The 'Device Actions' section includes links for 'Check for Changes', 'Manage Licenses', 'Workflows', 'Remove', and 'More Actions'.

- ❖ Device fully onboarded
- ❖ Ready to manage with cdFMC

# Onboard Cisco Secure Firewall

Inventory

Devices Templates Search by Device Name, IP Address, or Serial Number Displaying 2 of 2 results

All FTD

Name	Configuration Status	Connectivity
CHICAGO-PRIMARY FTD	Synced	Online
arid-pirate FTD High Availability Primary Standby Secondary Active	Synced	Online

**CHICAGO-PRIMARY**  
FTD

Device Details

Location n/a  
Model Cisco Firepower Thru VMware  
Serial 9AG4K0V2BXE  
Version 7.2.0  
Onboarding Method Registration Key

Your device's configuration is up-to-date

Device Actions

- Check for Changes
- Manage Licenses
- Workflows
- Remove
- More Actions

Management

- Device Summary
- Objects
- Health
- Policy
- NAT
- High Availability

Launch into  
Cloud Delivered  
Firewall Management Center

# Onboard Cisco Secure Firewall

The screenshot shows the Cisco Defense Orchestrator (DO) interface. The top navigation bar includes tabs for Monitoring, Policies, Devices (selected), Objects, and Integration. Below the navigation bar, there's a 'View By:' dropdown set to 'Group'. A status bar shows counts for various states: All (3), Error (2), Warning (0), Offline (0), Normal (1), Deployment Pending (0), Upgrade (0), and Snort 3 (3). The main table lists devices with columns: Name, Model, Version, Chassis, and Licenses. The device 'CHICAGO-PRIMARY' is highlighted in blue. A pop-up window for 'CHICAGO-PRIMARY' shows details: 'Cisco Firepower Threat Defense for VMware (Version 7.2.0)', 'Device Information' (Context Explorer, Health Dashboard), and 'Health Modules' (Normal: 23, Disabled: 44).

Name	Model	Version	Chassis	Licenses
> arid-pirate (1)				
low-mercury (0)				
Swift-Halo (0)				
Ungrouped (1)				
<b>CHICAGO-PRIMARY</b> <span>Snort 3</span> N/A - Routed	FTDv for VMware	7.2.0	N/A	Base, Threat (2 more...)

**CHICAGO-PRIMARY**

Cisco Firepower Threat Defense for VMware (Version 7.2.0)

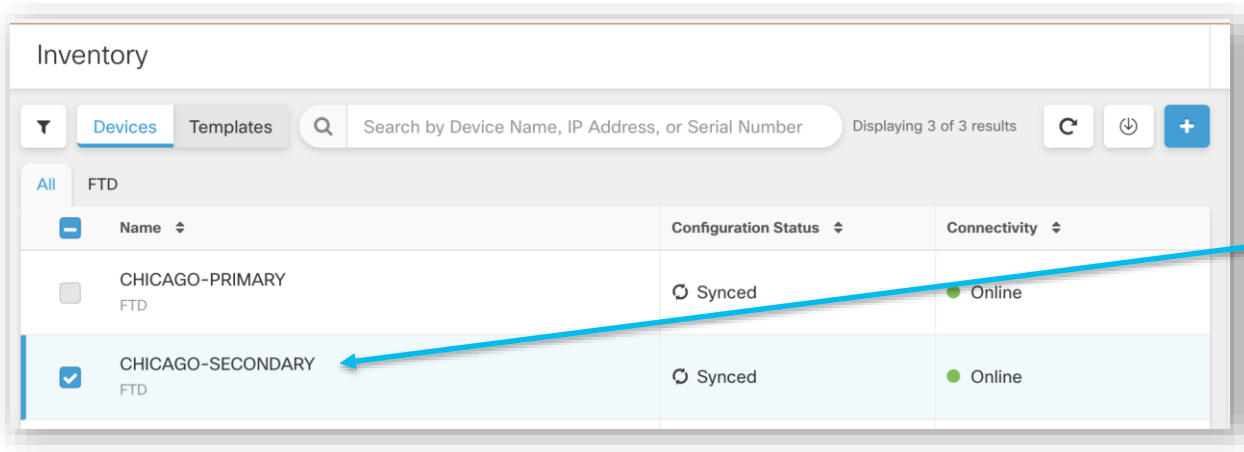
Device Information

- Context Explorer
- Health Dashboard

Health Modules

- Normal: 23
- Disabled: 44

# Onboard Cisco Secure Firewall



Inventory

Devices Templates

Search by Device Name, IP Address, or Serial Number

Displaying 3 of 3 results

All FTD

	Name	Configuration Status	Connectivity
<input type="checkbox"/>	CHICAGO-PRIMARY FTD	Synced	Online
<input checked="" type="checkbox"/>	CHICAGO-SECONDARY FTD	Synced	Online

When secondary device is initially added, it will show up as a distinct device



# Onboard Cisco Secure Firewall

Inventory	
Devices	
Search by Device Name, IP Address, or Serial Number	
All FTD	
Name	Configuration Status
CHICAGO	
FTD High Availability	Primary Active Secondary Standby

Once the HA has been configured in firewall management center, the CDO device objects will be automatically merged into 1 device

HA roles and status (green/red)

# Cloud Delivered FMC

FULL CONFERENCE

IT LEADERSHIP

## Introduction to cloud-delivered Firewall Management Center - BRKSEC-2318



Adam Bragg, CDO Product Owner, Cisco Systems, Inc.

Schedule

Wednesday, Jun 7 | 4:00 PM – 5:00 PM PDT | Level 2, Breakers DJ

A recently conducted study by Forrester for an independent analysis of organizations using Secure Firewall showed that customers realized a 195% in total ROI when managing their firewall fleet through Cisco Secure Firewall Management Center (FMC). With cloud-delivered FMC you can boost your productivity even further, it brings all the features from FMC into the cloud and consolidates firewall management. It brings the same FMC experience directly into Cisco Defense Orchestrator (CDO), and end-users enjoy the same look and functionality without the usual learning curve within a new experience. This session explains CDO and demonstrates how cdFMC simplifies greenfield and brownfield deployments of Cisco Secure Firewalls and also covers hybrid and cloud-based analytics options.

**Qualifies for Cisco Continuing Education Credit:** Yes

**Session Type:** Breakout

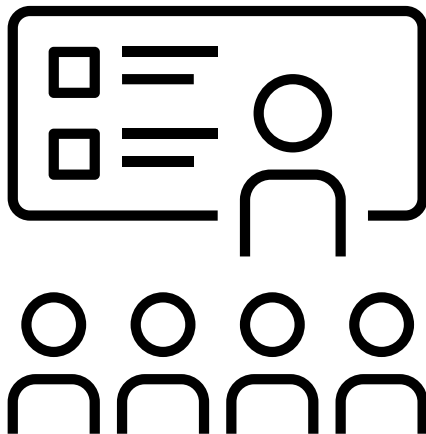
**Technical Level:** Intermediate

**Technology:** Cloud, Security

**Track:** Security



## Live demo of cdFMC and FTD management



# ASA Management

# ASA Management

## Objects and Policy Management

The screenshot displays the Cisco ASA Management Center interface, divided into two main panels. The left panel shows the 'Objects' configuration page, and the right panel shows the 'Access Control Policies' configuration page.

**Left Panel: Objects Configuration**

Search for objects by name, IP, or port number. Displaying 47 of 47 objects.

Name	Devices	Type
WebServer		
WebServer		
WebServer		
NETWORK ADDRESS		
192.168.1.10		
<input checked="" type="checkbox"/> _SmartCallHome_ServerCA	3	
<input type="checkbox"/> _SmartCallHome_ServerCA2	3	
<input type="checkbox"/> adam-test	2	
<input type="checkbox"/> cluster	3	
<input type="checkbox"/> foo		
ENCRYPTION		

**Right Panel: Access Control Policies Configuration**

ASA Access Policies / PointOfSale / Access Control Entries

Search for access rules by components or objects used. Displaying 28 rules.

Line	Action	Protocol	Source	Port	Destination	Port	Hits (Day)
1	Permit	ip	Network4	any	any	any	0000
2	Permit	ip	Network5	any	any	any	0000
3	Permit	ip	Network8	any	any	any	0000
4	Permit	ip	Network7	any	any	any	0000
5	Permit	ip	any	any	Network6	any	0000
6	Permit	ip	any	any	Network7	any	0000
7	Permit	ip	Network8	any	any	any	0000
8	Permit	ip	Network9	any	any	any	0000
9	Permit	ip	Network13	any	any	any	0000
10	Permit	ip	Network13point5	any	any	any	0000
11	Permit	ip	network16	any	any	any	0000
12	Permit	ip	network17	any	any	any	0000
13	Permit	ip	any	any	network18	any	0000
14	Permit	ip	any	any	network19	any	0000
15	Permit	ip	network18	any	any	any	0000
16	Permit	ip	network19	any	any	any	0000
17	Permit	ip	any	any	network20	any	0000
18	Permit	ip	network20	any	any	any	0000
19	Permit	ip	network21	any	any	any	0000
20	Permit	ip	network22	any	any	any	0000
21	Permit	ip	TempBlock1Jan2017	any	any	any	0000
22	Permit	ip	network23	any	any	any	0000
23	Permit	tcp	network24	any	AppleNetwork	ApplePushNotificat	0000

**Right Panel: PointOfSale Configuration**

PointOfSale (34 Access Control Entries (Shadowed))

Edit Policy

Troubleshoot

Network Policy

Access Control Entries

1

Logging

Default

Time Range

Select Time Range

Remarks

Add a remark for this rule...

Devices

Hits

Hourly hits on device for last:

Day

Week

Month

Year

Objects Used

Network4

# ASA Management

## Policy Based and VTI/Route-Based VPN Wizards

**Create Site-to-Site VPN**

Follow the steps below

1 Peer Devices

Configuration Name \*

Corp-HQ-Headend

☐ Policy Based ☒ Route Based

Peer 1

Device \*

Select Device

Search for devices.

Name	Type
Dayton	ASA
Minneapolis	ASA
Richmond	ASA
VPN-Headend-Contractors	ASA

Clear Selections Cancel Select

Peer 2

Extranet ☒

IP Address \*

☒ Static ☐ Dynamic

8.8.8.8

2 Tunnel Details

3 IKE Settings

4 IPSec Settings

5 Finish

# ASA Management

## ASA Bulk CLI and Macros

The screenshot displays the ASA Bulk CLI web interface. The top navigation bar is blue with a back arrow, the text "Bulk CLI", and several utility icons (search, notifications, help, and a user profile for "demo-red" with email "aahackne@cisco.com").

On the left side, there is a "Macros" section with a star icon and a plus button. Below it, a list of macros is shown, each with a clock icon, a title, and a description:

- ASA Add Static Route**: Add a simple static route to
- ASA Daily Tasks**: A series of commands that we run daily on our devices.
- ASA show version full**: Complete output of the show version command
- ASA Clear all connections**: Clear all connections from the connections table
- ASA show version**
- ASA GoogleDNS**: Set DNS to point to Google
- ASA Device Cert Check**: Identity Certificate check for RAVPN
- ASA License Review**

The main area is titled "Enter a command below:" and contains a text input field. The command "interface outside" is entered, and "shut" is being typed. Below the input field, there is a status bar with "Press Cmd+Enter to send command" and a "Clear" button.

On the right side, there is a "My List" section with a star icon and a power icon. It contains a list of items, each with a checkmark, a name, and an IP address:

- ☒ **Clarksville**: 10.10.6.42:443
- ☒ **Dayton**: 10.10.6.44:444
- ☒ **Dover-Branch**: 12.181.219.112:443
- ☒ **Minneapolis**: 10.10.6.11:443
- ☒ **Richmond**: 10.10.6.47:443
- ☒ **VPN-Headend-Contractors**: vasa-gb-ravpn-03-mgmt.dev.lockhart.io:443


At the bottom right of the "My List" section, there is a "Send" button with a count of 6.

# ASA Management

## Scheduled ASA Upgrades

Device Upgrade / ASA: VPN-Headend-Contractors

Return to Inventory



Device

VPN-Headend-Contractors

Model

ASAv (V01)

Location

vasa-gb-ravpn-03-mgmt.dev.lockhart.io:443

Failover Mode

Not Configured

Disk Size

7.98 GB

Disk Usage

733.99 MB

☒ Schedule Upgrade

Dec 14, 2022, 3:00 PM

1 ASA Software Image 9.14(3)

☐ Skip Upgrade

Image Source

☒ Use CDO Image Repository

☐ Specify Image URL

Continue

Software Image

Select an Image

9.17(1) 136.37 MB

9.16(3.23) 139.71 MB

9.16(3.19) 139.82 MB

9.16(2.14) 139.43 MB

9.16(2.7) 139.48 MB

9.16(2) 139.43 MB

2 ASDM Software Image 7.14(1) →

3 Perform Upgrade

Select the ASA software image you want to upgrade to. Only compatible versions of ASA and ASDM are shown.

DNS must be properly configured on the device before attempting the upgrade. Please reference [Configure DNS on ASA](#) for details.

If you check "Skip Upgrade," the ASA software image on your device will not be changed. You may still upgrade ASDM.



# ASA Management

## Detailed Changelogs and Diff Views Available

The screenshot displays the 'Change Log' interface in the ASA Management console. At the top, there's a blue header with the title 'Change Log'. Below it, a navigation bar includes a 'Return to Inventory' link, a search bar, and a filter for 'Devices Minneapolis'. The main content area features a table with columns for 'Last Updated', 'Device Name', and 'Last Description'. Two entries are visible: one from Nov 30, 2022, and another from Nov 29, 2022, which is highlighted. Below the table, a detailed view for the Nov 29, 2022 entry is shown, including a timeline of events and a diff view of the configuration changes.

Last Updated	Device Name	Last Description
Nov 30, 2022 6:30:34 AM	Minneapolis	CLI Execution
Nov 29, 2022 2:58:45 AM	Minneapolis	Changes written successfully

**Nov 29, 2022**

- 2:58:45 AM | Changes written successfully
- 2:58:44 AM | Changed ASA Config
- 2:57:49 AM | Changed ASA Config

**Diff View:**

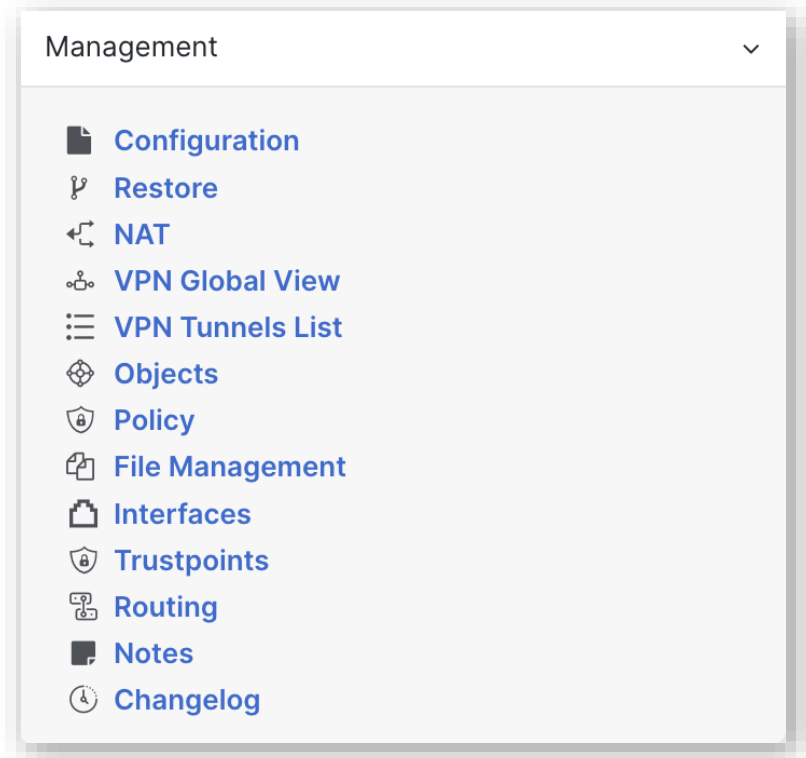
```
@@ -5,1 +5,1 @@
--: Written by lockhart at 16:45:58.006 UTC Fri Nov 18 2022
+: Written by lockhart at 15:57:43.796 UTC Mon Nov 28 2022
@@ -1429,1 +1429,1 @@
-Cryptochecksum:e52fd405c8973e0dd833f54d79736b9b
+Crvtocchecksum:aed84725c88b533530c9d029de6d5c46
```

# ASA Management

## Troubleshooting Tools From CDO – No CLI required

The screenshot displays the Cisco Defense Orchestrator (CDO) interface for ASA Management. The top navigation bar shows "ASA: Clarksville / Troubleshoot". The left sidebar contains a "Hide Menu" button and a list of navigation items: Inventory, Configuration, Policies, Objects, VPN, Events & Monitoring, Analytics, Change Log, Jobs, Tools & Services, and Settings. The main content area is titled "PACKET TRACER OUTPUT" and includes a "Clear" button. Below this, there are two buttons: "Run Packet Tracer" and "View Real-Time Log". The "Run Packet Tracer" section contains input fields for "Interface" (set to "inside"), "Packet Type" (with radio buttons for TCP, UDP, ICMP, and IP, where TCP is selected), "Source" (with a dropdown for "IP Address" and a text input "Enter Source"), "Port" (with a dropdown for "Enter Source Port"), "Destination" (with a dropdown for "IP Address" and a text input "Enter Destination"), "Port" (with a dropdown for "Enter Destination Port"), and "SGT Number (0-65535)" (with a text input "Enter SGT Number (optional)"). The "View Real-Time Log" section is titled "REAL-TIME LOG OUTPUT" and shows a separator line "\*\*\*". A warning message at the bottom states: "The device is not synced. You could encounter some unexpected results from packet-tracer."

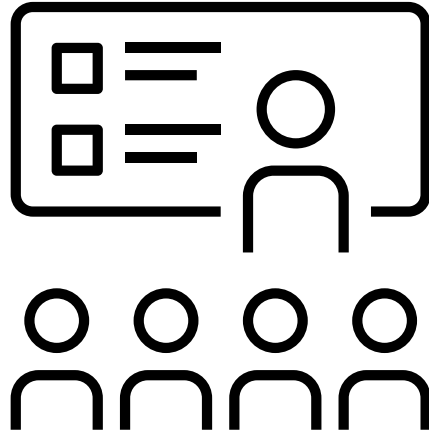
# ASA Management



Lots more functionality including:

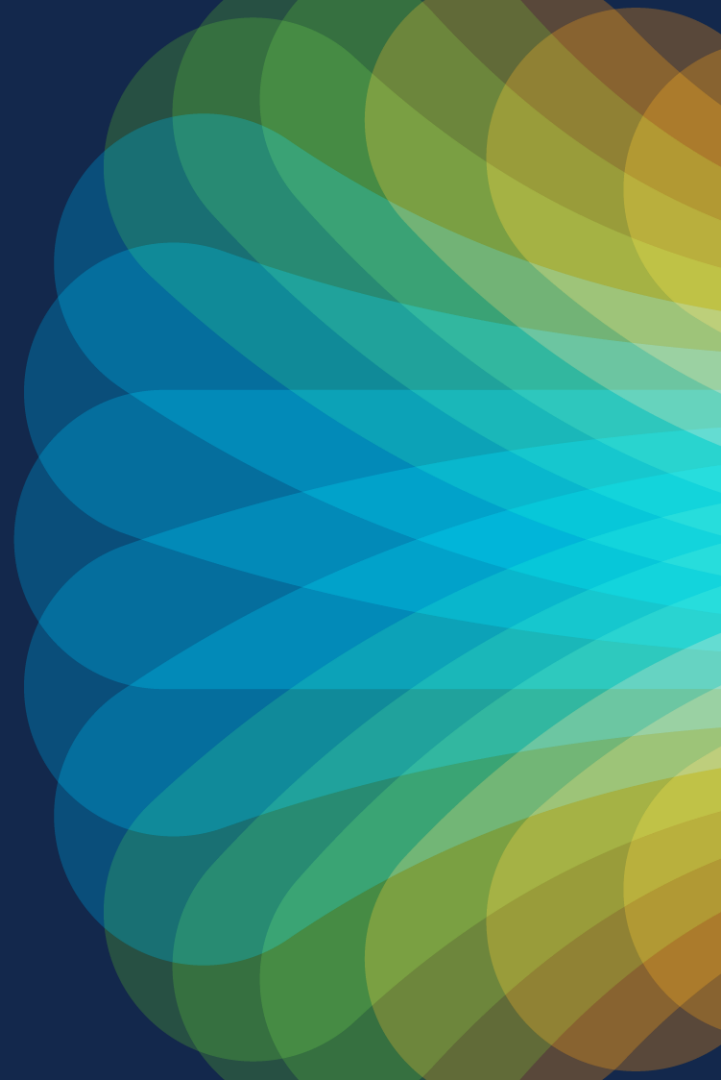
- ❖ Configuration visibility
- ❖ NAT policy
- ❖ Backups
- ❖ File management
- ❖ Certificate management
- ❖ Out of band change management
- ❖ Interface configuration
- ❖ Routing configuration
- ❖ Platform Settings Policy

## Live demo of common ASA tasks



# CDO Visibility

Security Analytics and Logging



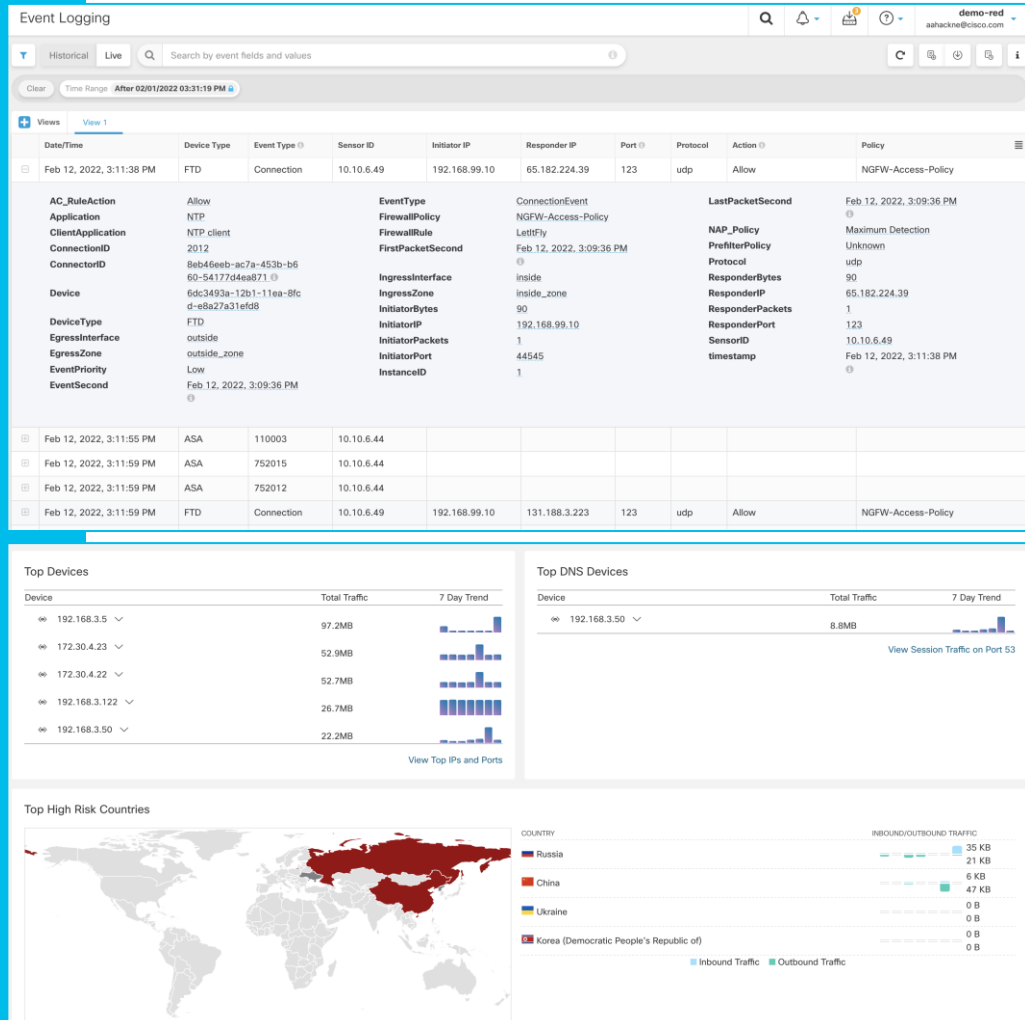
# Security Analytics and Logging

## Unified views:

- FTD Connection Events
- FTD IPS/Threat Events
- FTD Malware Events
- FTD URL Events
- FTD Threat Intelligence Events
- ASA Connections, Syslog, Netflow, etc.

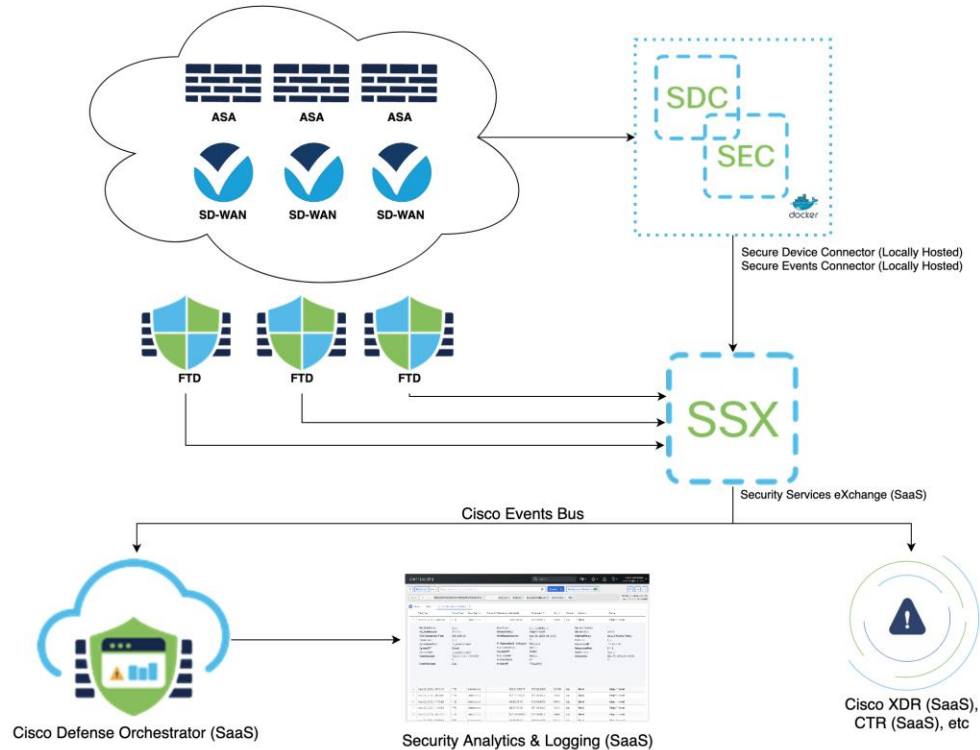
# SCALE

CISCO *Live!*



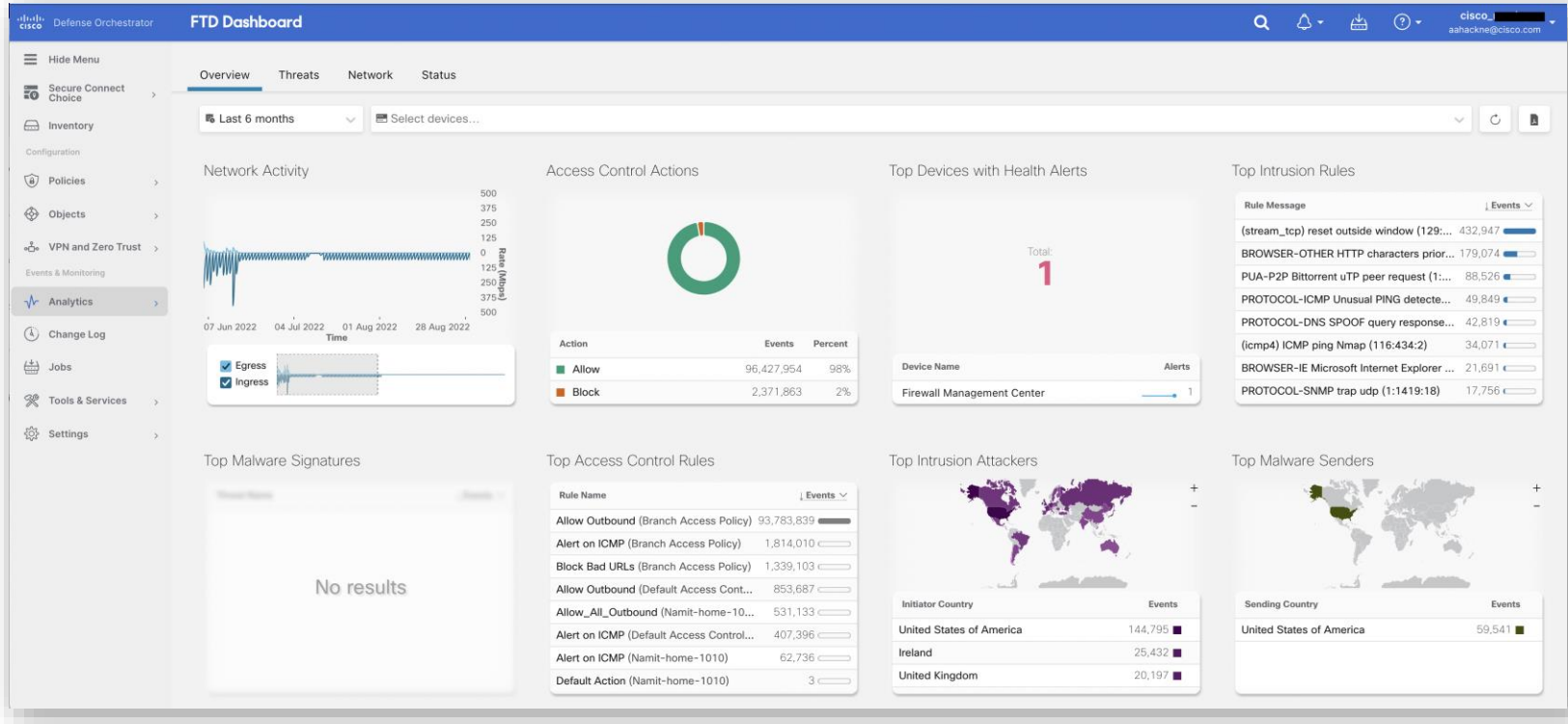
# Security Analytics and Logging

Log from anywhere securely



# Security Analytics and Logging

## FTD Analytics Dashboard





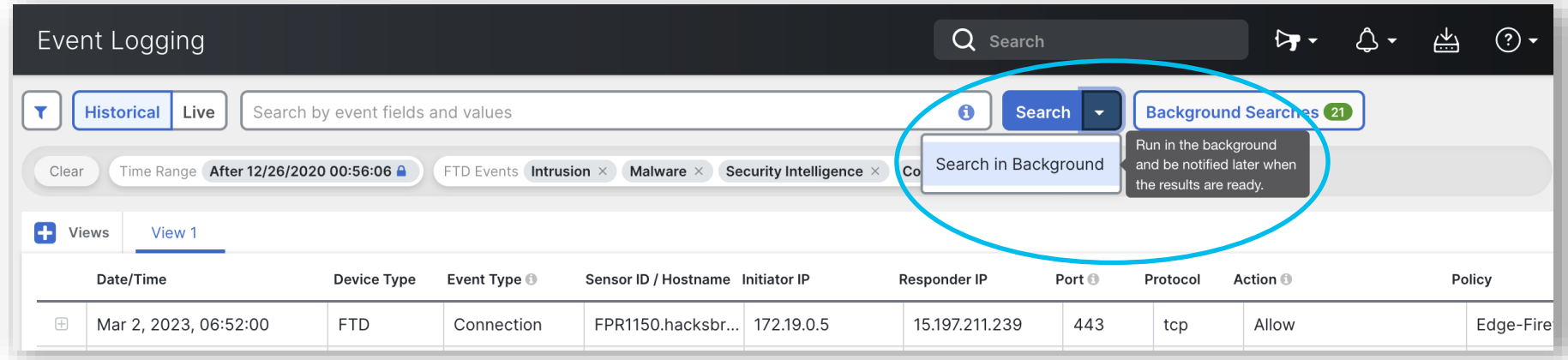
# Security Analytics and Logging

Telemetry for each event is visible

AC_RuleAction	Allow	EventSecond	Oct 1, 2022, 10:41:04 AM ⓘ	InitiatorPort	60464
Application	HTTPS	EventSubtype	End	InstanceID	7
ClientApplication	SSL_client	EventType	ConnectionEvent	LastPacketSecond	Oct 1, 2022, 10:41:04 AM ⓘ
ConnectionDuration	1	FirewallPolicy	Edge-Firewall	NAP_Policy	Balanced Security and Connecti vity
ConnectionID	56857	FirewallRule	Inside-to-Any	PrefilterPolicy	Default Prefilter Policy
ConnectorID	f55664b1-208f-476f-a544-f9de 75319cbe ⓘ	FirstPacketSecond	Oct 1, 2022, 10:41:03 AM ⓘ	Protocol	tcp
DeviceIP	192.168.30.2	Hostname	FPR1150-backbone.com	ResponderBytes	2085
DeviceType	FTD	IngressInterface	inside	ResponderIP	34.200.5.134
DeviceUUID	9b8eb11a-e932-11ec-96ae-b14f 5d04fec8 Q	IngressVRF	Global	ResponderPackets	15
EgressInterface	outside	IngressZone	inside	ResponderPort	443
EgressVRF	Global	InitiatorBytes	1480	URL	https://fw-update2.smartthings. com
EgressZone	outside	InitiatorIP	172.30.3.120	WebApplication	Web Browsing
EventPriority	Low	InitiatorPackets	17	timestamp	Oct 1, 2022, 10:41:06 AM ⓘ

# Security Analytics and Logging

## Background Search



The screenshot displays the Cisco Security Analytics and Logging interface. At the top, there's a dark header with 'Event Logging' and a search bar. Below this, a navigation bar includes 'Historical' and 'Live' tabs, a search input field, and a 'Search' button. A blue circle highlights the 'Search' button and the 'Background Searches' dropdown menu, which shows '21' results. A tooltip explains that background searches run in the background and notify when results are ready. Below the navigation bar, there's a section for filters including 'Clear', 'Time Range' (set to 'After 12/26/2020 00:56:06'), and event types like 'FTD Events', 'Intrusion', 'Malware', and 'Security Intelligence'. A 'Views' section shows 'View 1'. The main table displays event logs with columns: Date/Time, Device Type, Event Type, Sensor ID / Hostname, Initiator IP, Responder IP, Port, Protocol, Action, and Policy.

Date/Time	Device Type	Event Type	Sensor ID / Hostname	Initiator IP	Responder IP	Port	Protocol	Action	Policy
Mar 2, 2023, 06:52:00	FTD	Connection	FPR1150.hacksbr...	172.19.0.5	15.197.211.239	443	tcp	Allow	Edge-Fire

# Security Analytics and Logging

## Scheduled Searches

The screenshot shows a 'Logging' window with a search bar and a 'Search Logs in the Background' dialog box. The dialog box has a title bar with a close button (X). Inside, there is a 'Search Name' field with the text 'Daily-IPS-Search'. Below it is a 'Search Parameters' section with a dropdown arrow. The 'Search Query' field contains the text 'No search string...'. To the right of the 'Search Query' field is a 'Filters' section with a 'Time Range' dropdown set to 'After 12/26/2020 00:56:06' and a row of buttons: 'FTD Events', 'Intrusion', 'Malware', 'Security Intelligence', 'Connection', and 'File'. Below the 'Search Query' field are two checkboxes: 'Search now' (checked) and 'Setup recurrent schedule' (checked). Below these checkboxes is a 'Search Logs for the Last:' section with a dropdown set to '24' and a unit dropdown set to 'hours'. Below this is a 'Frequency' section with a dropdown set to 'Daily' and a 'Time (UTC+00:00)' section with two input fields: '03' and '00'. Below the 'Frequency' section is the text 'Daily at 03:00'. At the bottom right of the dialog box are two buttons: 'Cancel' and 'Schedule and Search Now'.

Logging

Search

Search Logs in the Background

Search Name \*

Daily-IPS-Search

Search Parameters

Search Query

No search string...

Filters

Time Range After 12/26/2020 00:56:06

FTD Events Intrusion Malware Security Intelligence Connection File

☒ Search now

☒ Setup recurrent schedule

Search Logs for the Last:

24 hours

Frequency

Daily

Time (UTC+00:00)

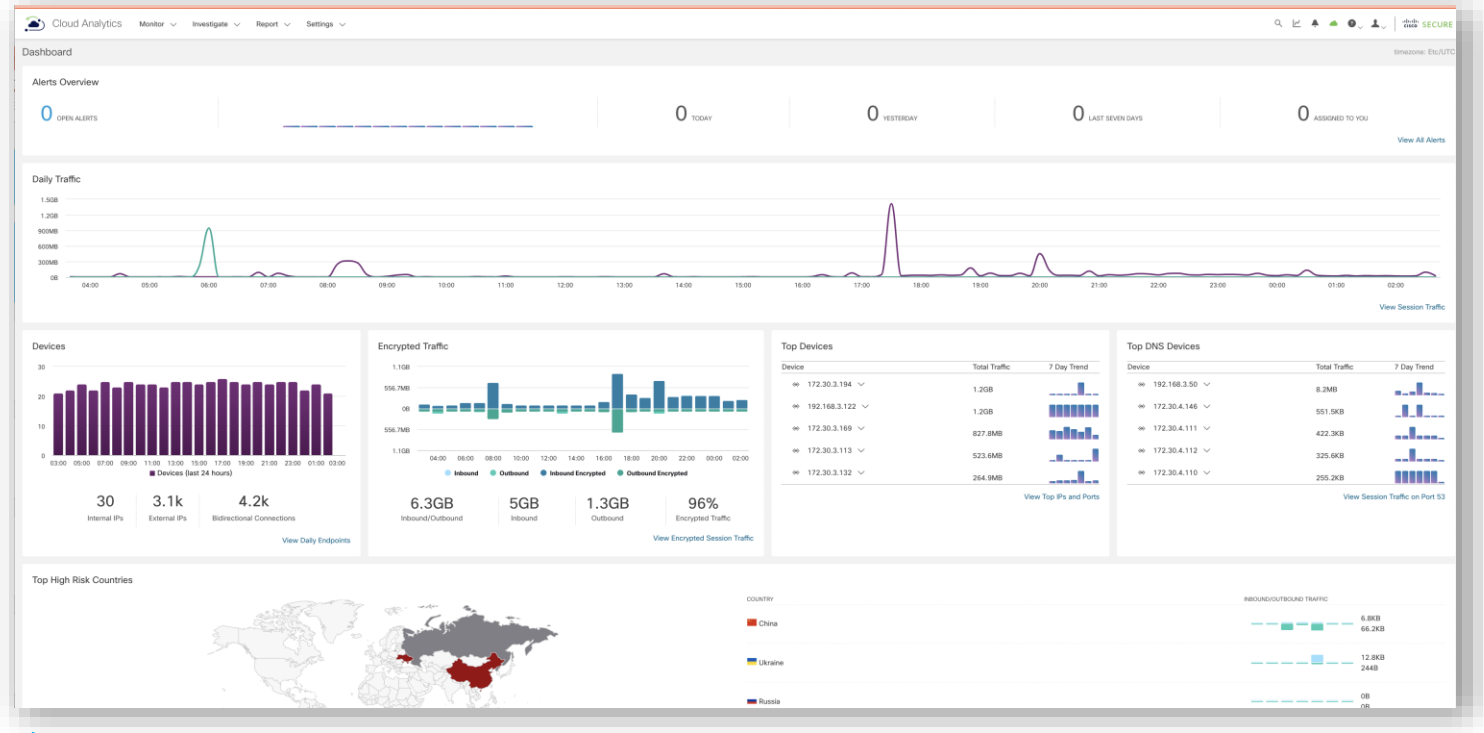
03 : 00

Daily at 03:00

Cancel Schedule and Search Now

# Security Analytics and Logging

## Feeds Telemetry to Cisco Secure Analytics (Formerly Stealthwatch Cloud)



# Security Analytics and Logging

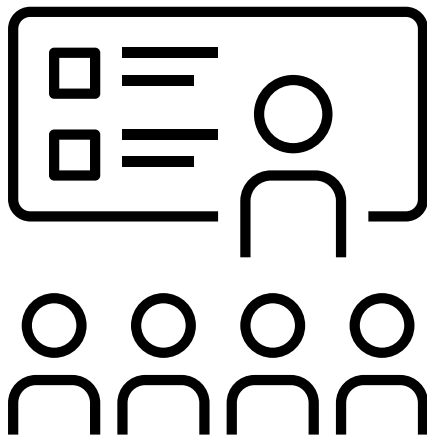
What's coming for Security Analytics and Logging\*

- ❖ Security Analytics and Logging 2.0
  - ❖ Improved search times
  - ❖ Closer alignment to OnPrem FMC event viewer
  - ❖ Packet Payload Capture for IPS Events

\* Subject to change

# Security Analytics and Logging

Live demo of SAL



# Devops

# CDO API

Step 1: Create an API only user for your tenant and select RBAC role

**Grant User Access to CDO\_cisco\_aahackne**

If this user is new to Cisco Defense Orchestrator, please ensure the user has self-registered at [sign-on.security.cisco.com](https://sign-on.security.cisco.com) with the same email address used below.

Username  
cdo\_api

Role  
Read Only ☒ API Only User

Read Only  
Edit Only  
Deploy Only  
Admin  
Super Admin  
VPN Sessions Manager

Cancel OK

\*Disclaimer: API is not fully supported (YET!) today but nothing is stopping your careful use of it.

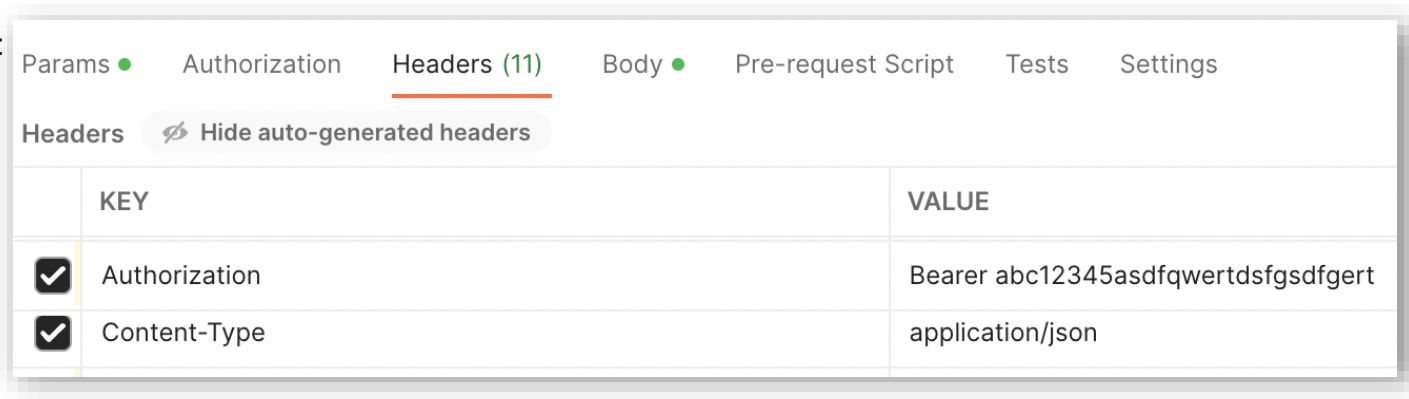


# CDO API

## Step 2: Authentication and content-type

- ❖ Each API call requires an HTTP authentication header
- ❖ It is a simple bearer token (Use API token from step 1)
- ❖ Must also include a content-type “application/json” header

Postman Example:

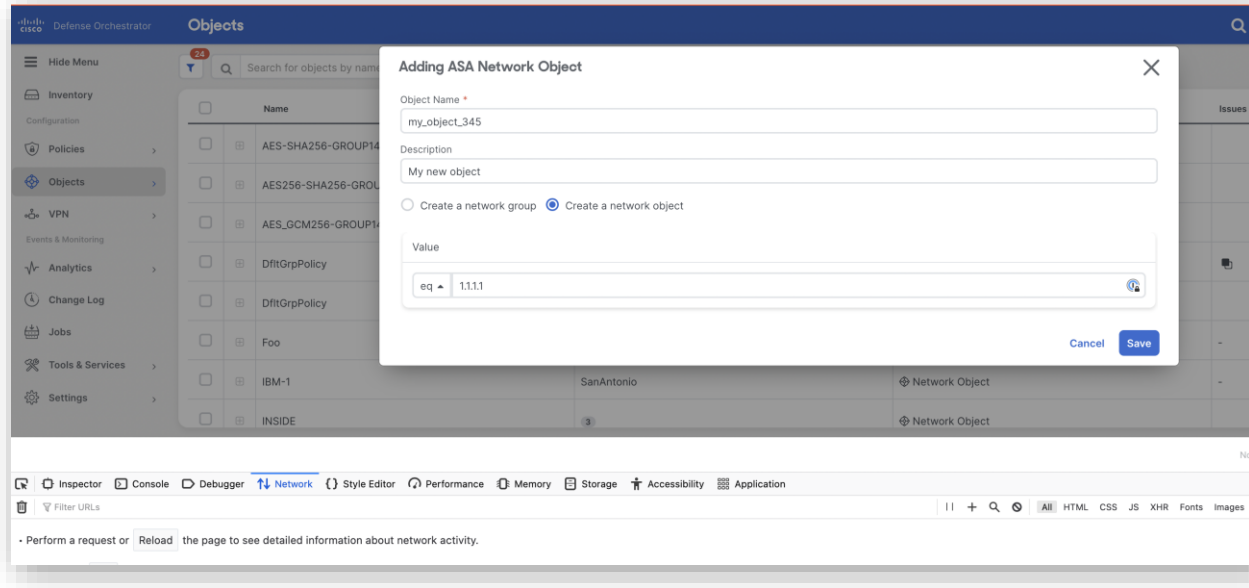


cURL Example: `curl --header 'Content-Type: application/json' --header 'Authorization: Bearer abc12345asdfqwertydsfgsdfgert'`

# CDO API

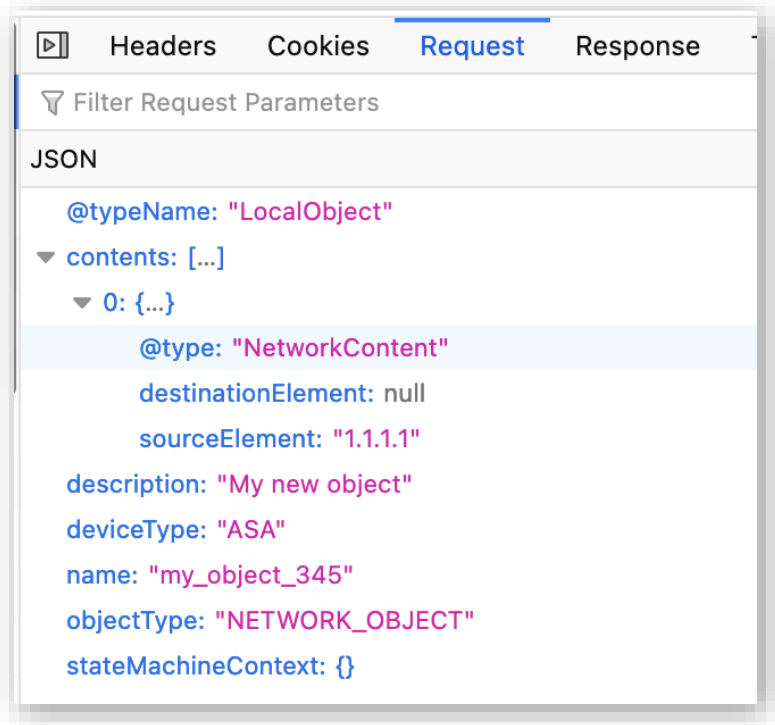
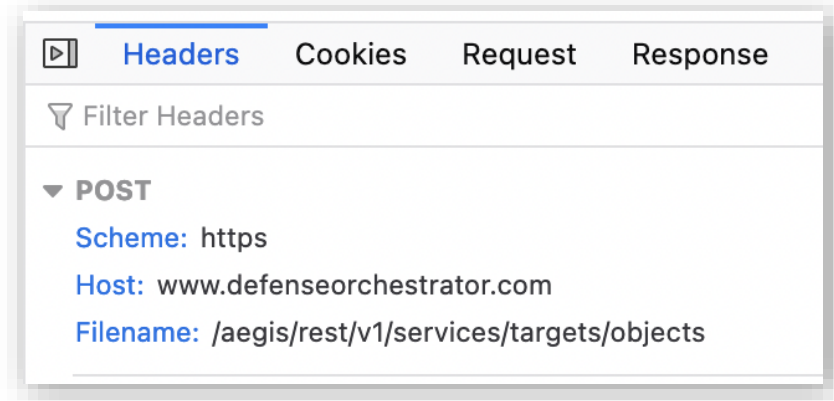
Step 3: How does the CDO UI do it?

Using “Developer Tools” in Firefox, you can see the API endpoints and the data structures of the POST/PUT payloads in the “network” tab.

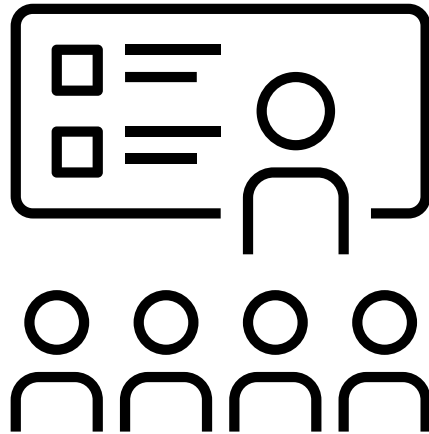


# CDO API

## Step 3: How does the CDO UI do it?



Live demo of API automation via some API and Ansible Playbooks



# Wrap-Up

# Try it out!

Register today for your **free** Demo/POV  
of CDO and cloud delivered FMC

[APJ] <https://apj.cdo.cisco.com>

[US]

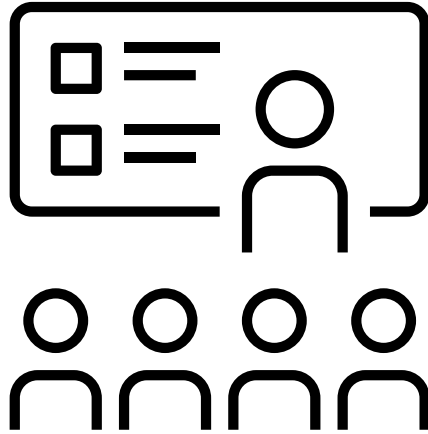
<https://www.defenseorchestrator.com>

[EMEA]

<https://www.defenseorchestrator.eu>

Or go to <https://getcdo.com>

## Demo of spinning up a CDO Tenant



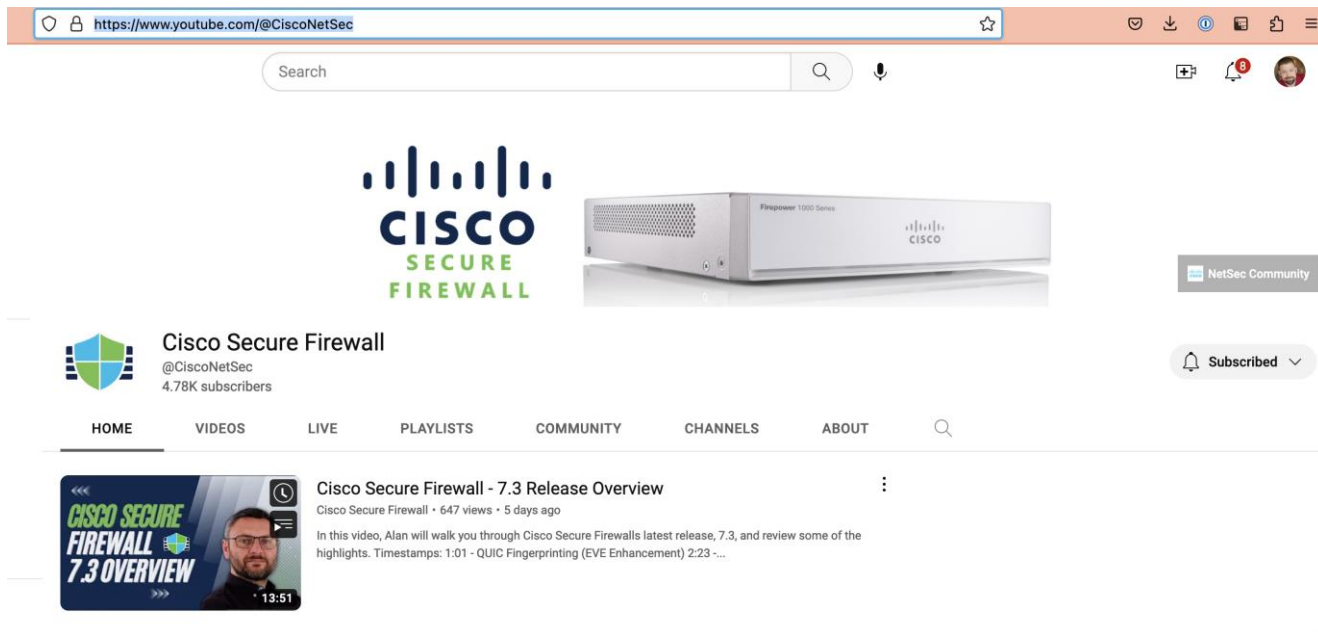
# Summary

- ❖ Firewall management platform and orchestration
- ❖ You ain't seen nothing yet! CI/CD = Rapid innovation!
- ❖ cdFMC is a game changer – Focus on policy not the manager
- ❖ cdFMC LTP makes remote branch deployments plug-and-play
- ❖ Shared Objects = more consistent policy and fewer mistakes
- ❖ RA VPN visibility is excellent for managing work-from-anywhere
- ❖ Operation at scale is possible



# Cisco Secure Firewall YouTube Channel

## [Cisco Secure Firewall YouTube Channel](https://www.youtube.com/@CiscoNetSec) [Low Touch Provisioning Demo](#)



The screenshot shows the YouTube channel page for Cisco Secure Firewall. The browser address bar displays <https://www.youtube.com/@CiscoNetSec>. The channel banner features the Cisco Secure Firewall logo and a photograph of a Cisco Firepower 1000 Series firewall unit. The channel name is "Cisco Secure Firewall" with the handle "@CiscoNetSec" and 4.78K subscribers. A "Subscribed" button is visible. The navigation menu includes Home, Videos, Live, Playlists, Community, Channels, and About. The featured video is titled "Cisco Secure Firewall - 7.3 Release Overview", posted 5 days ago with 647 views. The video description states: "In this video, Alan will walk you through Cisco Secure Firewalls latest release, 7.3, and review some of the highlights. Timestamps: 1:01 - QUIC Fingerprinting (EVE Enhancement) 2:23 - ...". The video thumbnail shows a man speaking, with the text "CISCO SECURE FIREWALL 7.3 OVERVIEW" and a duration of 13:51.

# Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. [www.cisco.com/go/certs](https://www.cisco.com/go/certs)

## Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



## Learn

### Cisco U.

IT learning hub that guides teams and learners toward their goals

### Cisco Digital Learning

Subscription-based product, technology, and certification training

### Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

### Cisco Learning Network

Resource community portal for certifications and learning



## Train

### Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

### Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

### Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



## Certify

### Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

### Cisco Guided Study Groups

180-day certification prep program with learning and support

### Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

# Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



**These points** help you get on the leaderboard and increase your chances of winning daily and grand prizes

# 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](https://www.CiscoLive.com/on-demand)

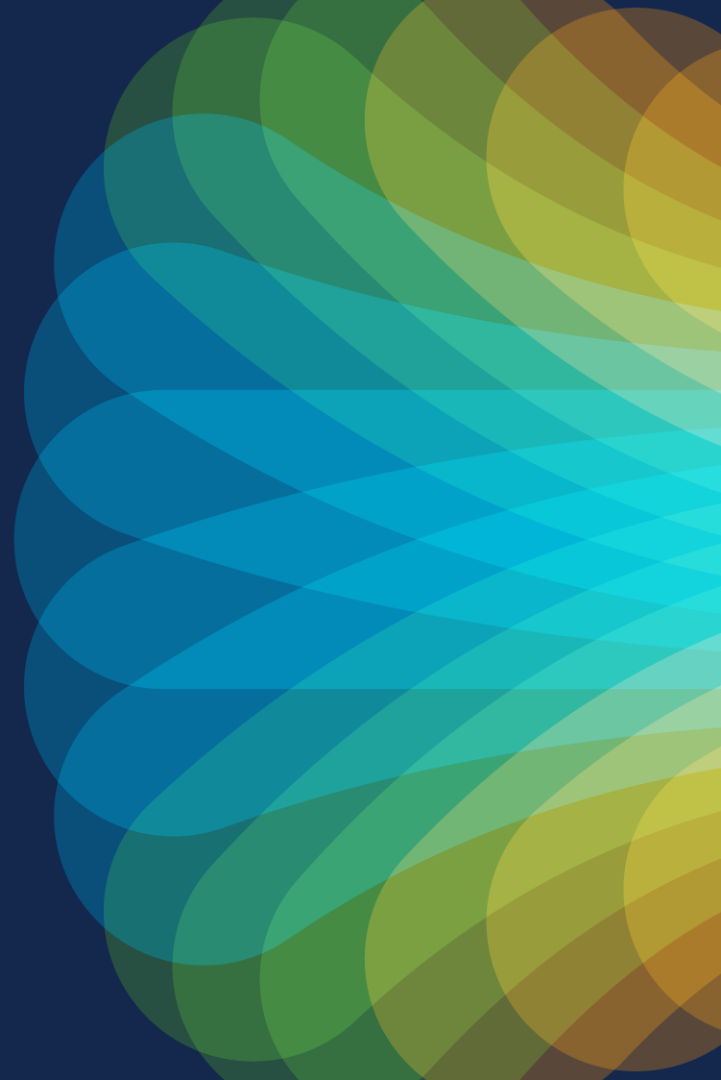


The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLive

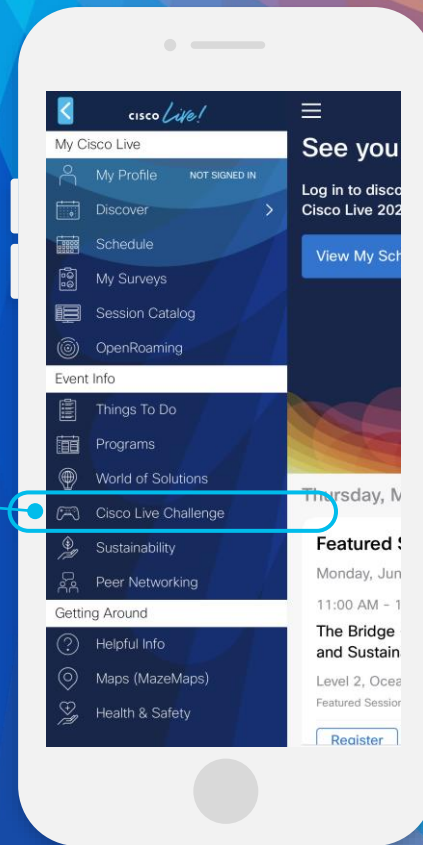
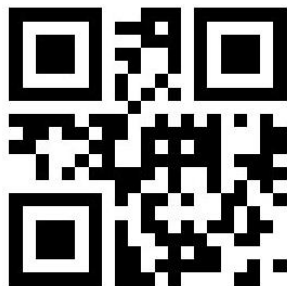


# Cisco Live Challenge

Gamify your Cisco Live experience!  
Get points for attending this session!

## How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are large, flowing, wavy shapes in similar colors, giving the impression of liquid or smoke. The overall effect is dynamic and energetic.

cisco *Live!*

Let's go

#CiscoLive