

The Cisco Live! logo, featuring the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, cursive script font.

CISCO *Live!*

The text "Let's go" in a large, dark blue, sans-serif font, positioned to the left of a bright white sunburst graphic that radiates across the right side of the image.

Let's go

#CiscoLiveAPJC



The bridge to possible

Cisco Defense Orchestrator

Manage Your Cisco Firewalls Anywhere

Anshul Kaushik
Technical Solutions Architect

Lookman Kurusumuthu
Director, System Engineering

BRKSEC-1138

CISCO *Live!*

#CiscoLiveAPJC



“Reconciliation”- Dustin Koa Art

Abstract

Cisco Defense Orchestrator is a SaaS that provides management to your Firewall wherever it sits: Physical, Virtual, On Prem, Public Cloud, Private Cloud even in a container.

Cisco Defense Orchestrator (CDO) is a SaaS that is delivered from the Cloud but provides management to your Firewall wherever it sits: Physical, Virtual, On Prem, Public Cloud, Private Cloud, or even in a container. Cloud Delivered Firewall Management Center (cdFMC) is a cloud delivered, turnkey SaaS for managing all of your FTD needs without the need to manage FMC infrastructure. Cisco Secure Analytics and Logging (SAL) is a SaaS that enables Firewalls to send their logs safely and securely to the Cloud while providing one convenient place to troubleshoot, audit, and analyze your events. In this session, you will learn:

1. How these services integrate and work together to provide a comprehensive, end to end Firewall Management solution, no matter the platform.
2. The architecture of the CDO, cdFMC, Multi-Cloud Defense (MCD), & SAL deployment models
3. How to use CDO to operationalize your logging views under a single pane of glass
4. How SAL leverages log data to provide actionable analytics using an embedded Cisco Secure Analytics integration
5. Best practices for operationalizing CDO, cdFMC, MCD & SAL together in your environment

The session will include a mixture of lecture and real product demos.

A basic understanding of Cisco Firewalls (ASA and/or FTD) by attendees is assumed for this session.

Cisco Webex App

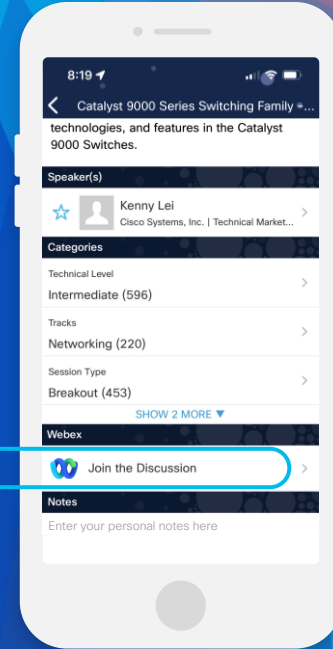
Questions?

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 December 22, 2023.



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

Your Speaker

Anshul Kaushik

- ankaushi@cisco.com
- CCIE Security #23790
- 20 Years in Industry, 18 with Cisco
- TAC – Presales – Channels
- Drive end to end Security Enablement
- Lives in Melbourne and like outdoors



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

What is Cisco Defense Orchestrator (CDO)?

Consistently manage policies across your Cisco security products. CDO is a cloud-based application that cuts through complexity to save time and keep your organization protected against the latest threats.

Key Benefits

Streamline security management

Reduce time spent on security management tasks up to 90%

Achieve better security while reducing complexity

Prioritize response

Visibility

Lower TCO

Features

Consistent policy enforcement

Faster device deployments

Configuration management

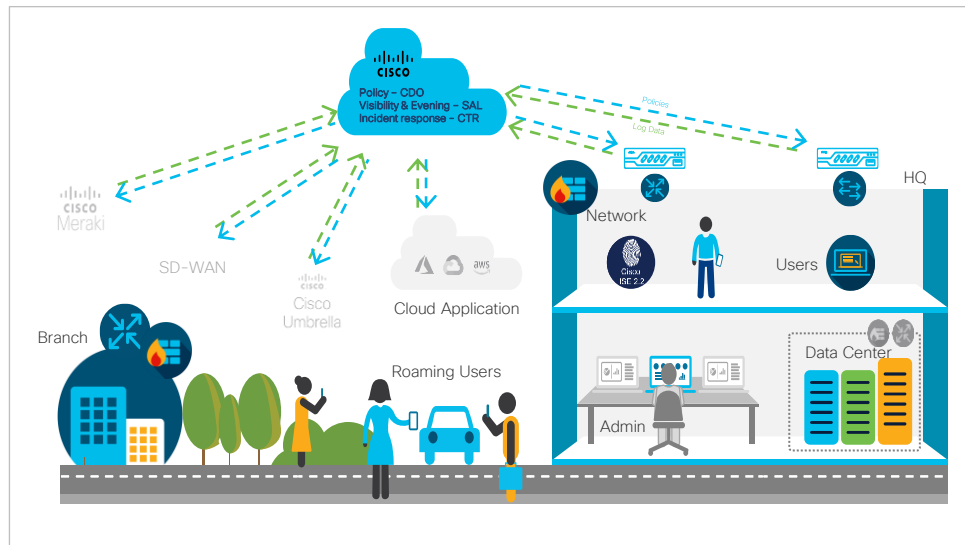
API Integrations

Manage Anywhere

Turnkey SaaS

Low Touch Provisioning

Shared Objects



Challenges to Securing an Enterprise

Perimeters are no longer geographically defined, so a single perimeter firewall is no longer the norm.

Single control point is not adequate

Every environment needs its own
micro-perimeter

Evolving form factor

Singe control points are now replaced by multiple firewalls, both physical and virtual

Policy sprawl

Harmonizing policies across micro-perimeters is challenging



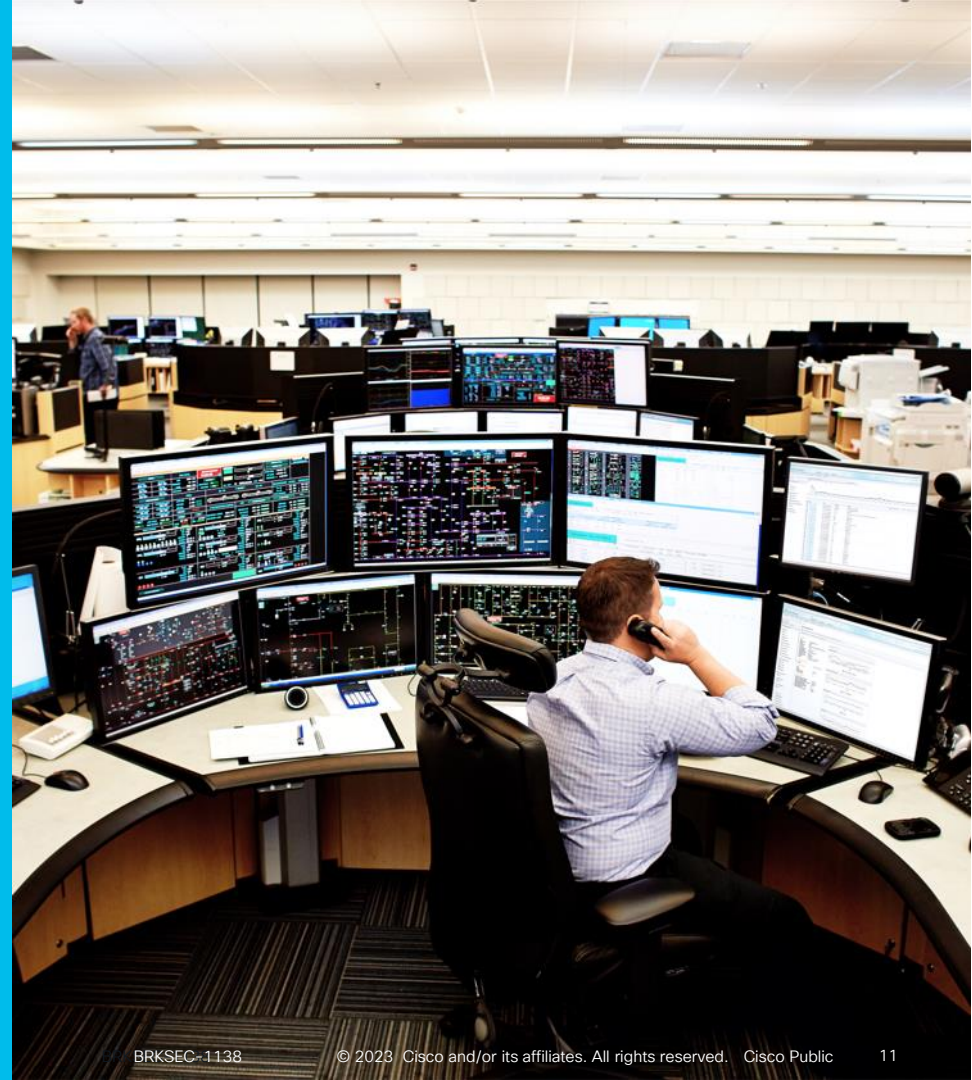
Management complexity

NetSec and IT use dozens of point products, each with its own management console

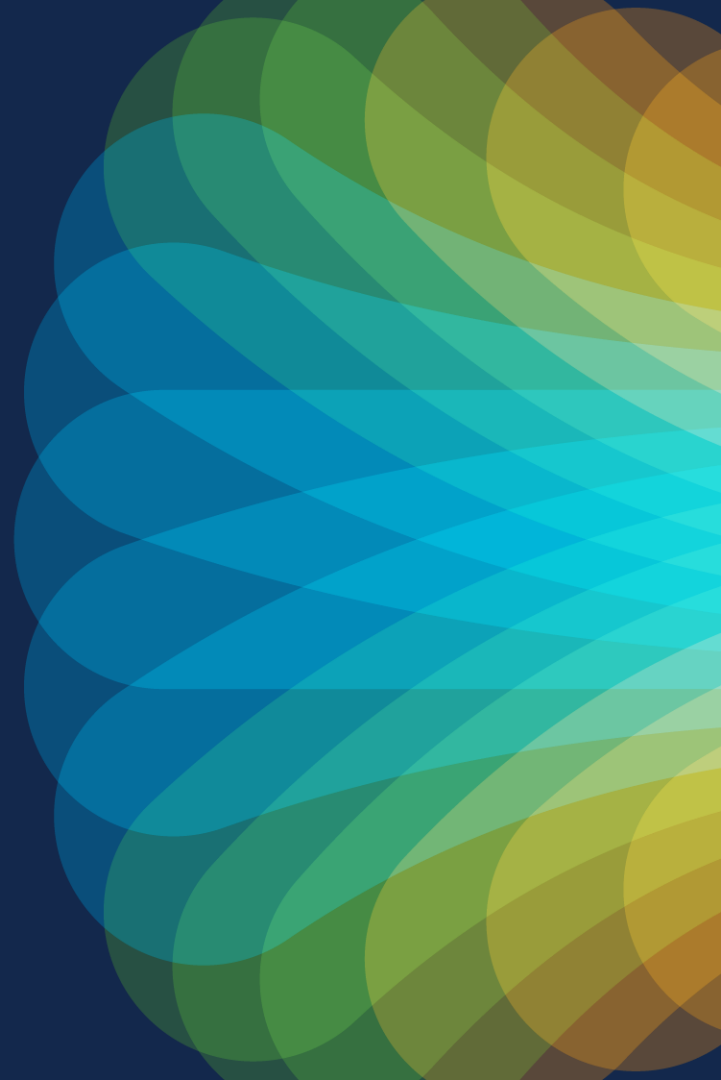
Evolving threat landscape

Security products need a continuous feed of threat intelligence to stay ahead of attackers

Managing network
and application
security is hard
work.



CDO Solves Problems

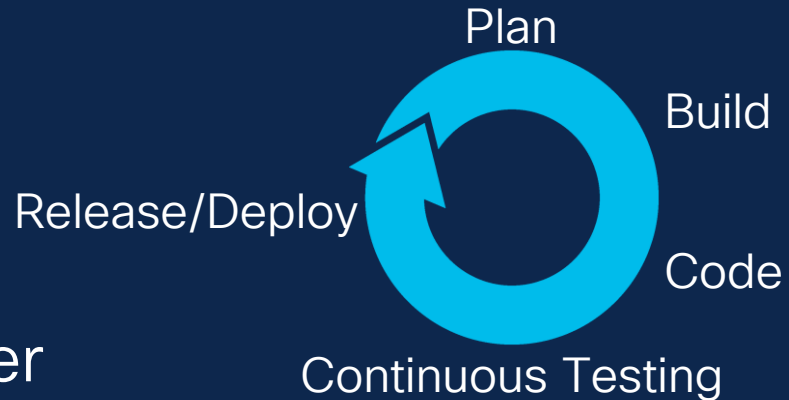


CDO Solves Problems FAST

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

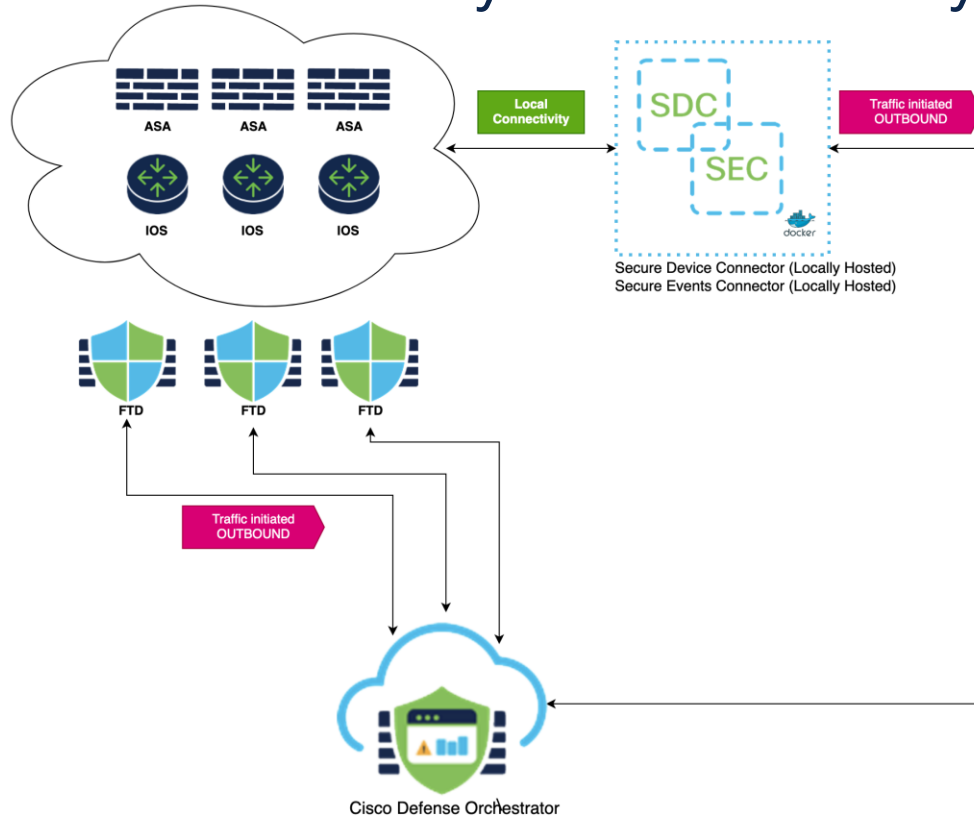


CDO Needs NO Inbound Access



- 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 is divided into three steps: 1. Select OnPrem FMC, 2. Select Devices, and 3. Finish. Step 1 is currently active and contains instructions: "Ensure that you have onboarded your OnPrem FMC to CDO via Credentials or SecureX. [Onboard an OnPrem FMC](#) or [learn more](#)". A second instruction states: "After your OnPrem FMC has been onboarded, select it from the list." Below this, a dropdown menu is labeled "Available OnPrem FMCs (7.2+ only)" and contains the text "Select OnPrem FMC". A "Next" button is positioned below the dropdown. A "Cancel" button is located in the top right corner of the wizard panel.

Migrate FTD to cdFMC

Migrate FTD from OnPrem FMC to cloud

1 Select OnPrem FMC

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

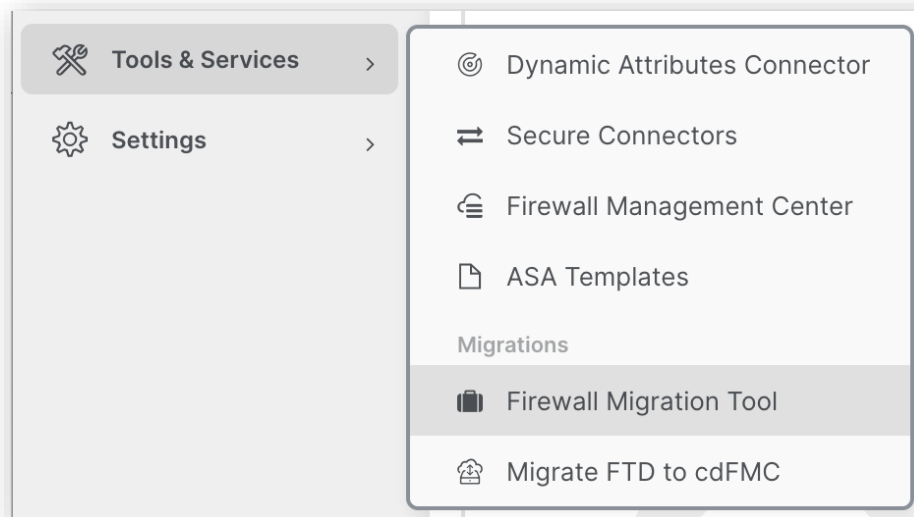
Next

2 Select Devices

3 Finish

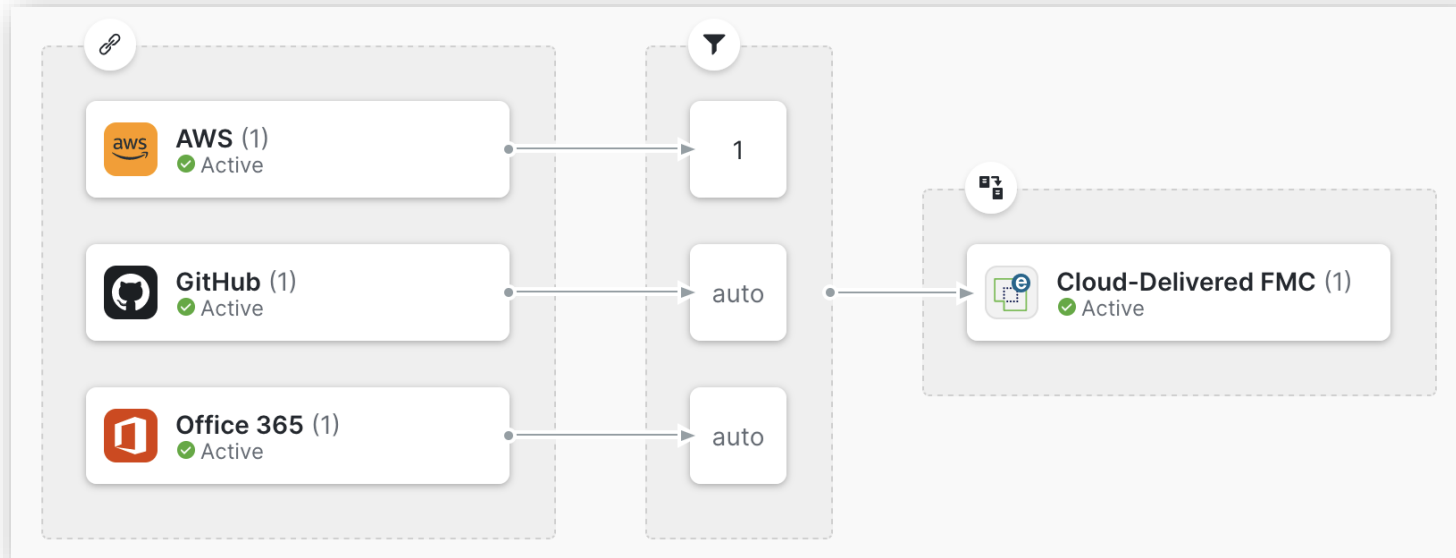
CDO Simplifies Advanced Tooling

- Firewall Migration Tool
 - ASA → cdFMC/FTD
 - FDM → cdFMC/FTD
 - PAN → cdFMC/FTD
 - Fortinet → cdFMC/FTD



CDO Simplifies Advanced Tooling

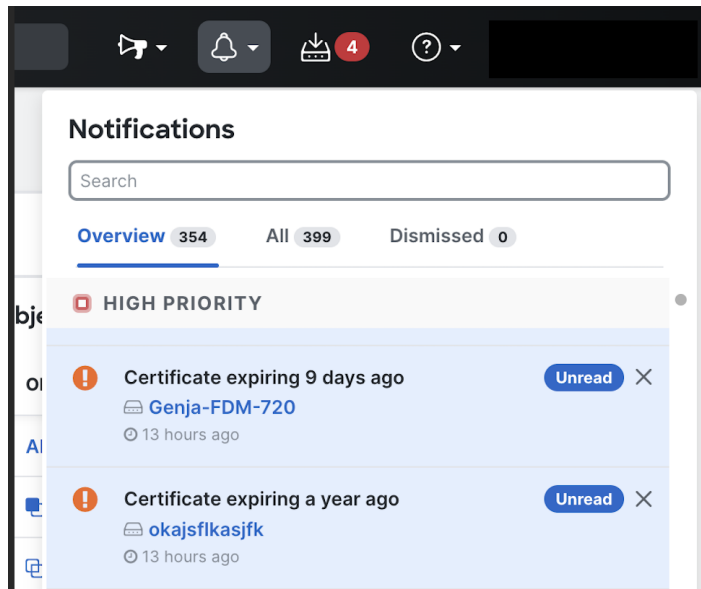
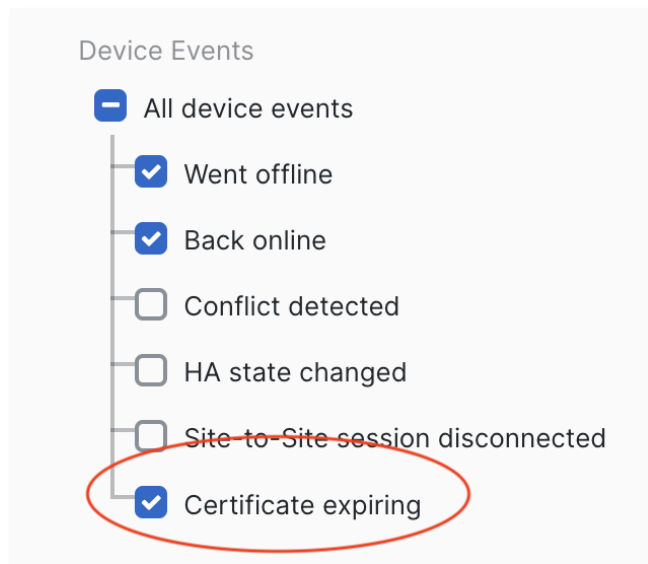
- Cisco Secure Dynamic Attributes Connector (CSDAC)



CDO Simplifies Fleet Management



❖ New notifications coming for AnyConnect Certificate Expiration



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

2 ASDM Software Image 7.19(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.

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 allows selecting specific workflow events for alerts. The options are:

- ☐ Deployments
 - ☐ Failed
 - ☐ Started
 - ☐ Succeeded
- ☒ Backups
 - ☒ Failed
 - ☒ Started
 - ☒ Succeeded
- ☒ Upgrades
 - ☒ Failed
 - ☒ Started
 - ☒ Succeeded
- ☐ Migrate FTD to cloud
 - ☐ Failed
 - ☐ Started
 - ☐ Succeeded
- ☐ Commit pending

Device Events: This section allows selecting specific device events for alerts. The options are:

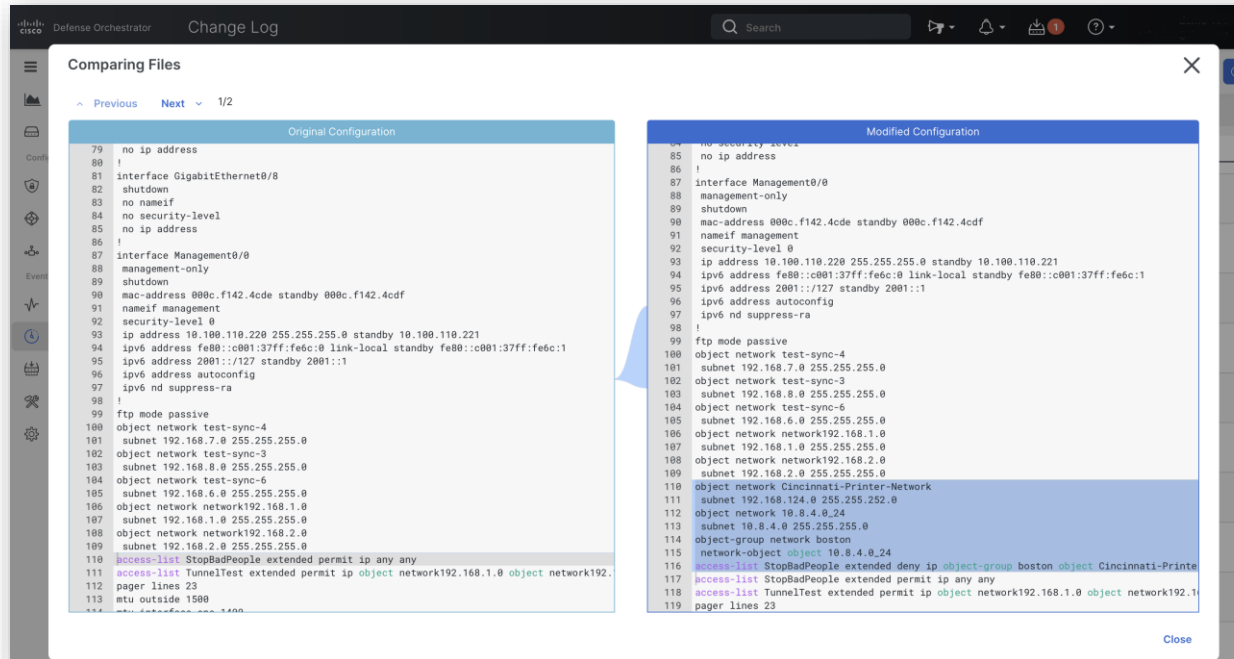
- ☒ All device events
 - ☐ Went offline
 - ☐ Back online
 - ☐ Conflict detected
 - ☒ HA state changed
 - ☒ Site-to-Site session disconnected

Add Service Integration Modal: This modal is open, showing the configuration for a new service integration. The fields are:

- Name:** CDO-Notifications
- Service Type:** Webex (selected from a dropdown menu)
- Webhook URL:** /1/webhooks/incoming/xxx
- Buttons:** Cancel, Save, Test, Learn More

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 VPN connections. A detailed view for user Karilyn is shown on the right, displaying 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 05/31/202	0h:5m:14s	3.79 KB	392 Bytes	Cary, North Caroli
June	Active	Berlin	172.16.249.170	fcfe:eeee::72	173.38.117.79	08:19:41 05/31/202	0h:0m:14s	3.79 KB	-	Cary, North Caroli
Karilyn	Active	Berlin	172.16.249.138	fcfe:eeee::70	173.38.117.79	07:11:09 05/31/202	1h:8m:46s	3.79 KB	560 Bytes	Cary, North Caroli
Lee	Active	Berlin	172.16.249.153	fcfe:eeee::6c	173.38.117.79	07:35:10 05/31/202	0h:44m:45s	3.79 KB	560 Bytes	Cary, North Caroli
Madisen	Active	Berlin	172.16.249.175	fcfe:eeee::69	173.38.117.79	07:57:41 05/31/202	0h:22m:14s	3.79 KB	504 Bytes	Cary, North Caroli
Mirabel	Active	Berlin	172.16.249.137	fcfe:eeee::76	173.38.117.79	06:50:38 05/31/202	1h:29m:17s	3.79 KB	616 Bytes	Cary, North Caroli
Myron	Active	Berlin	172.16.249.169	fcfe:eeee::71	173.38.117.79	07:20:09 05/31/202	0h:59m:46s	3.79 KB	560 Bytes	Cary, North Caroli
Orlando	Active	Berlin	172.16.249.133	fcfe:eeee::66	173.38.117.79	07:40:10 05/31/202	0h:39m:45s	3.79 KB	560 Bytes	Cary, North Caroli
Ray	Active	Berlin	172.16.249.161	fcfe:eeee::6b	173.38.117.79	07:59:41 05/31/202	0h:20m:14s	3.79 KB	504 Bytes	Cary, North Caroli
Seth	Active	Berlin	172.16.249.166	fcfe:eeee::75	173.38.117.79	07:47:40 05/31/202	0h:32m:15s	3.79 KB	560 Bytes	Cary, North Caroli
Sherleen	Active	Berlin	172.16.249.139	fcfe:eeee::74	173.38.117.79	08:18:11 05/31/202	0h:1m:44s	3.79 KB	280 Bytes	Cary, North Caroli
Sue	Active	Berlin	172.16.249.163	fcfe:eeee::73	173.38.117.79	07:59:41 05/31/202	0h:20m:14s	3.79 KB	504 Bytes	Cary, North Caroli
Timothy	Active	Berlin	172.16.249.132	fcfe:eeee::64	173.38.117.79	07:46:10 05/31/202	0h:33m:45s	3.79 KB	504 Bytes	Cary, North Caroli
paul-1	Active	VPN-Headend-Co	192.168.128.72		34.228.89.40	08:26:27 05/31/202	0h:3m:40s	12.21 KB	79.03 MB	Ashburn, Virginia,
paul-10	Active	VPN-Headend-Co	192.168.128.81		34.228.89.40	08:26:32 05/31/202	0h:3m:35s	12.21 KB	77.12 MB	Ashburn, Virginia,
paul-2	Active	VPN-Headend-Co	192.168.128.73		34.228.89.40	08:26:28 05/31/202	0h:3m:39s	12.21 KB	78.84 MB	Ashburn, Virginia,
paul-3	Active	VPN-Headend-Co	192.168.128.74		34.228.89.40	08:26:28 05/31/202	0h:3m:39s	12.21 KB	78.26 MB	Ashburn, Virginia, United S
paul-4	Active	VPN-Headend-Co	192.168.128.75		34.228.89.40	08:26:29 05/31/202	0h:3m:38s	12.21 KB	78.42 MB	Ashburn, Virginia, United S

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 "VPN Tunnels / Berlin" and shows a search bar and a list of tunnels. A "Tunnel Details" panel is open, showing the configuration for the "Berlin-Clarkville" tunnel. The configuration includes Peer 1 (Berlin) and Peer 2 (Clarkville) with their respective VPN Access Interfaces (outside) and Protected Networks (Berlin-Inside-Net and Clarkville-In-Net). The NAT Exempt Interface is set to inside. A "Policies" table is also visible, showing a single policy with Action PERMIT, Protocol ip, Source Berlin-Inside-Net, Port any, Destination Clarkville-Inside-Net, and Port any.

Edit Site-to-Site VPN

Follow the steps below

Peer Devices

Configuration Name *
Berlin-Clarkville

☒ Policy Based ☐ Route Based

Peer 1

Device *
Berlin

VPN Access Interface *
outside

Protected Networks *
Berlin-Inside-Net

NAT Exempt Interface *
inside

Peer 2

Device *
Clarkville

VPN Access Interface *
outside

Protected Networks *
Clarkville-In-Net

NAT Exempt Interface *
inside

Tunnel Details

Key Exchange

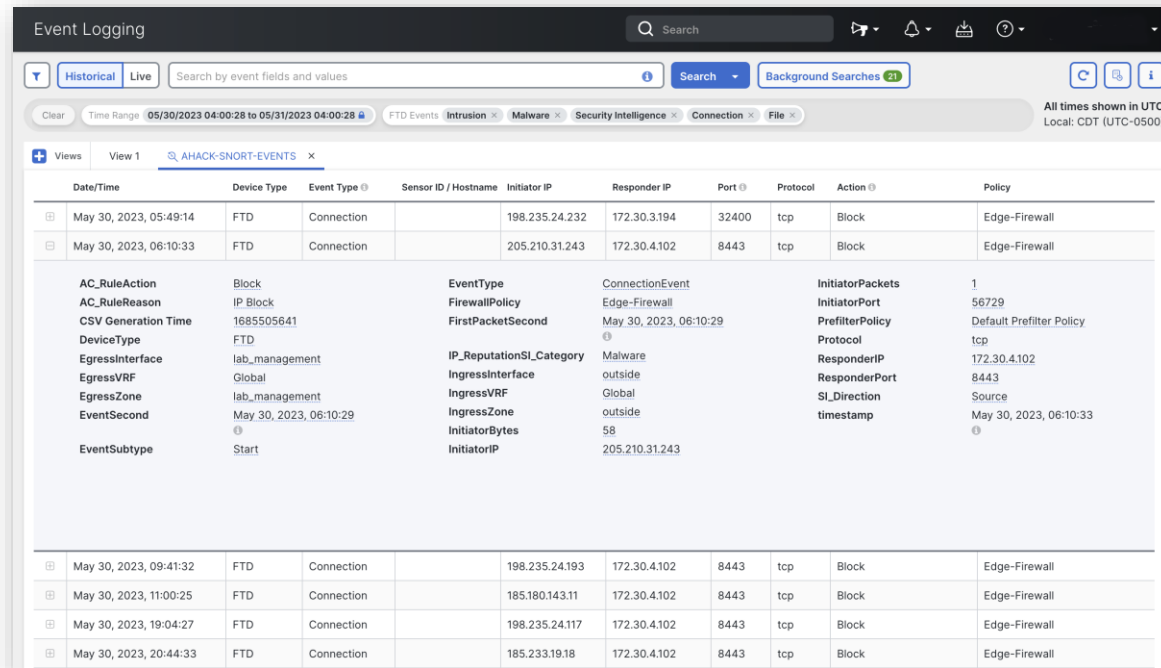
Connectivity	Last Seen Active	Last Checked
idle	-	5/31/23 8:20 AM

Policies

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

CDO Simplifies Visibility

- Centralized Logging and Analytics for ASA and FTD



The screenshot displays the Cisco 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 row of category filters includes '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 main table, listing various attributes 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
AC_RuleAction Block AC_RuleReason IP Block CSV Generation Time 1685505641 DeviceType FTD EgressInterface lab_management EgressVRF Global EgressZone lab_management EventSecond May 30, 2023, 06:10:29 EventSubtype Start EventType FirewallPolicy FirstPacketSecond May 30, 2023, 06:10:29 IP_ReputationSI_Category Malware IngressInterface outside IngressVRF Global IngressZone outside InitiatorBytes 58 InitiatorIP 205.210.31.243 ConnectionEvent Edge-Firewall InitiatorPackets 1 InitiatorPort 56729 PrefilterPolicy Default Prefilter Policy Protocol tcp ResponderIP 172.30.4.102 ResponderPort 8443 SI_Direction Source timestamp May 30, 2023, 06:10:33									
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

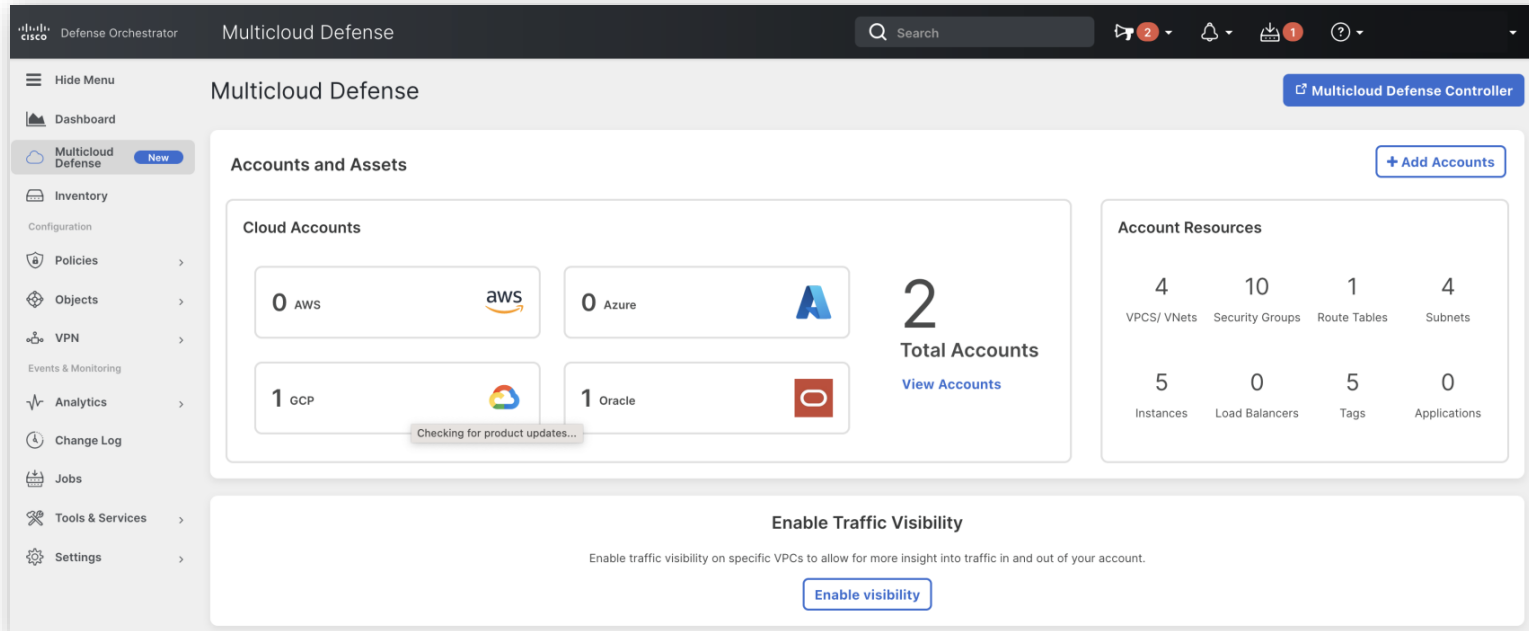
The screenshot displays the Cisco Defense Orchestrator (CDO) interface for managing Fire Threat Detection (FTD) devices. The top navigation bar includes tabs for Analysis, Policies, Devices (selected), Objects, and Integration. The breadcrumb trail shows 'FMC / Devices / Device Management'. The interface features a 'View By:' dropdown set to 'Group' and a status filter bar showing 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 FTD devices, grouped by location. The table columns are Name, Model, Version, Chassis, Licenses, Access Control Policy, Auto RollBack, and a actions column. The groups shown are Canada (2), Ottawa (High Availability), Toronto, and Cloud (2). The 'Ottawa' group is expanded, showing two devices: 'Ottawa-PR1(Primary, Active)' and 'Ottawa-SEC(Secondary, Standby)', both with status 'N/A - Routed' and 'Snort 3'. The 'Toronto' group shows one device 'Toronto' with status 'N/A - Routed' and 'Snort 3'. The 'Cloud' group is collapsed. The 'AWS-FTD' group is also visible at the bottom with status 'N/A - Routed' and 'Snort 3'.

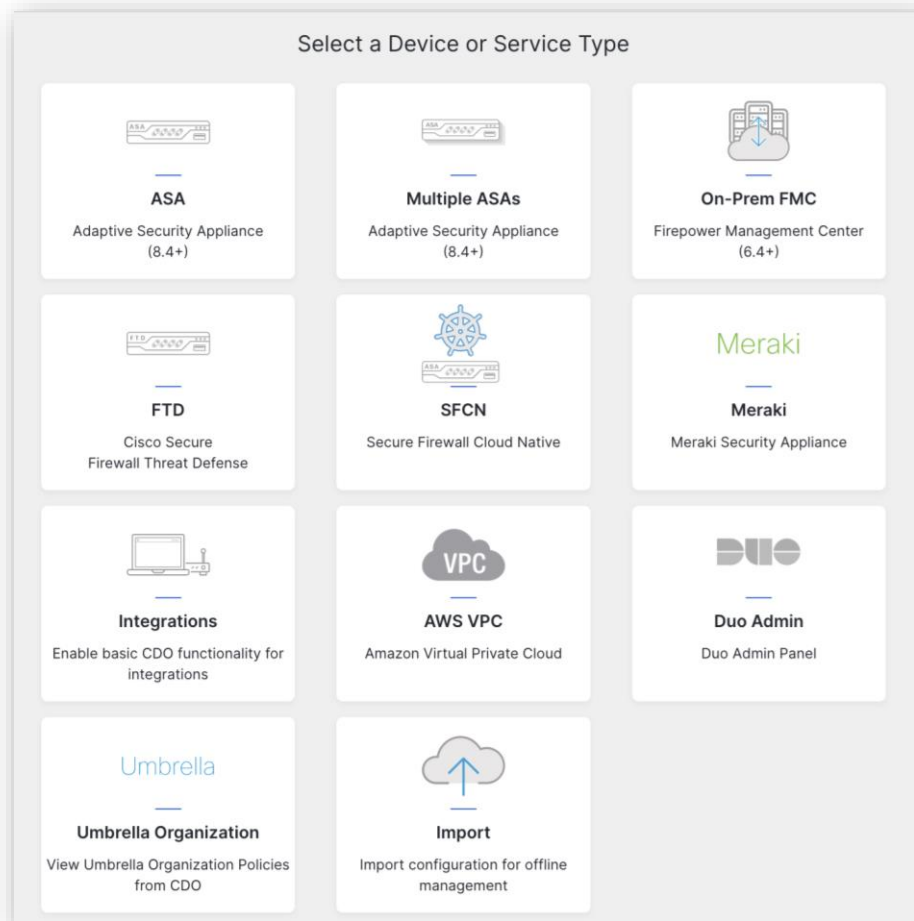
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	Actions
Canada (2)							
Ottawa (High Availability)							
Ottawa-PR1(Primary, Active) <small>Snort 3</small> N/A - Routed	FTDv for VMware	7.2.0	N/A	Essentials, IPS (2 more...)	Default Access Control Policy		
Ottawa-SEC(Secondary, Standby) <small>Snort 3</small> N/A - Routed	FTDv for VMware	7.2.0	N/A	Essentials, IPS (2 more...)	Default Access Control Policy		
Toronto <small>Snort 3</small> N/A - Routed	FTDv for VMware	7.2.0	N/A	Essentials, IPS (2 more...)	Default Access Control Policy		
Cloud (2)							
AWS-FTD <small>Snort 3</small> 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”



OnPrem FMCs

Auto-Discover and share
objects with OnPrem FMCs



Auto onboard On-Prem FMCs from SecureX tenant



FMC

Secure Connectors

☐	Name	Version	Devices	Type
☐	Cloud-Delivered FMC	20230929	 6	Cloud-Delivered FMC
☐	fmc1.hacksbrain.pvt_172.30.4.115	7.3.1-build 19	 2	On-Prem FMC

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	1.1.1.0/24	domain	0000
5	 Permit	ip	anyconnect-net	any	any	any	0000

✕ Cancel

Save

Network Policy ▼

Edit Tools Active

AWS VPC Security Group Policy Management

The screenshot shows the Cisco Defense Orchestrator (DO) interface. The top navigation bar includes the Cisco logo, the title "Defense Orchestrator", and the breadcrumb "AWS VPC Policies / vpc-28a5154d (AWS-DC-West-Demo-Red)". The left sidebar contains a "Hide Menu" button and a list of navigation items: "Secure Connect Choice", "Inventory", "Configuration", "Policies" (selected), "Objects", "VPN and Zero Trust", "Templates", "Migrations", "Events & Monitoring", "Monitoring", "Change Log", "Jobs", and "Admin".

The main content area displays a list of security groups under the heading "Security Groups". There are two tables of policies:

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	NETS Any IPv4	PORTS TCP:22
Inbound	Cisco Adaptive Security Virtual...	Allow	NETS Any IPv4	PORTS TCP:443
Outbound	Cisco Adaptive Security Virtual...	Allow	Any	NETS Any IPv4

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

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

Meraki MX Policy Management

Defense Orchestrator

Hide Menu

Secure Connect Choice

Inventory

Configuration

Policies

Objects

VPN and Zero Trust

Templates ASA

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 Bulk CLI web interface. On the left, a sidebar lists various macros such as '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' section. Below the command input, a 'Send' button is visible. The right sidebar shows the execution results for 1 device, 'Clarksville', under the 'By Response' tab. The response text is as follows:

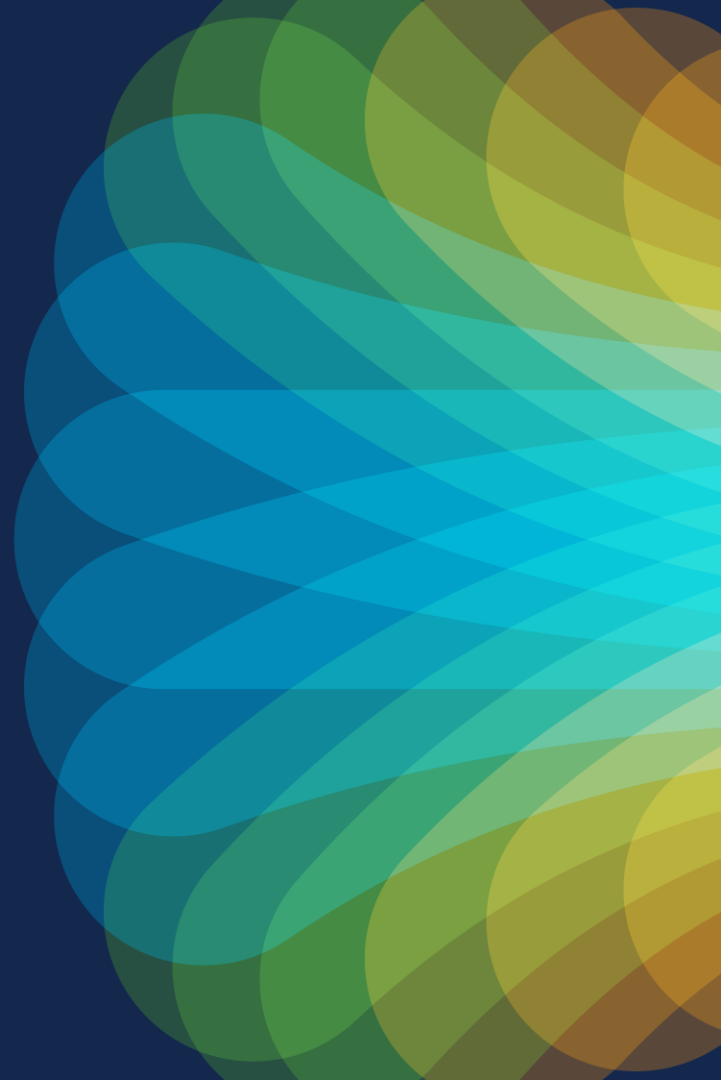
```
Showing response for 1 Devices

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 interface. The top navigation bar includes the Cisco logo, 'Defense Orchestrator', and 'Multicloud Defense'. A search bar and notification icons are on the right. The 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 is the 'Accounts and Assets' section, which displays 'Cloud Accounts' and 'Account Resources'. The 'Cloud Accounts' section shows 0 AWS, 0 Azure, 1 GCP, and 1 Oracle accounts, with a '2 Total Accounts' summary and a 'View Accounts' link. A tooltip 'Checking for product updates...' is visible over the GCP account. The 'Account Resources' section shows 4 VPCS/ Vnets, 10 Security Groups, 1 Route Tables, and 4 Subnets, along with 5 Instances, 0 Load Balancers, 5 Tags, and 0 Applications. At the bottom, there is an 'Enable Traffic Visibility' section with a description 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 Type	Count
VPCS/ Vnets	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 MultiCloud Defense [BRKSEC-2145]



John M. Clark Clark, Director, Solutions Engineering, Cisco

Schedule

Wednesday, Dec 6 | 1:00 PM - 2:00 PM AEDT | Meeting Room 212

Public cloud environments offer unique challenges to delivering protection and security, fueled by the requirements of speed, automation, simplicity, service consumption, and auto-scaling and self-healing. This is compounded by the desire to operate uniformly and consistently across multiple public clouds that each speak different languages and support different architectures. With the recent introduction of Cisco Multicloud Defense, Cisco can now provide customers with an innovative approach to delivering protection across single- and multi- public cloud environments, improving security and simplifying operations.

In this session you will learn how Cisco Multicloud Defense delivers cloud-native security across multiple public clouds in a simple and consistent way. Through automation of multicloud networking and protection through advanced segmentation and threat detection policy, Multicloud Defense delivers security as a service to accelerate your public cloud journey.

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](#)

☐	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
☐	> Peoria (1)							 
☐	▼ Ungrouped (2)							
☐	 Ottawa Snort 3 N/A - Routed	FTDv for VMware	7.2.0	N/A	Base, Threat (2 more...)	 Corporate-FW-Policy 		 
☐	 Toronto Snort 3 N/A - Routed	FTDv for VMware	7.2.0	N/A	Base, Threat (2 more...)	 Default Access Control Policy 		 

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

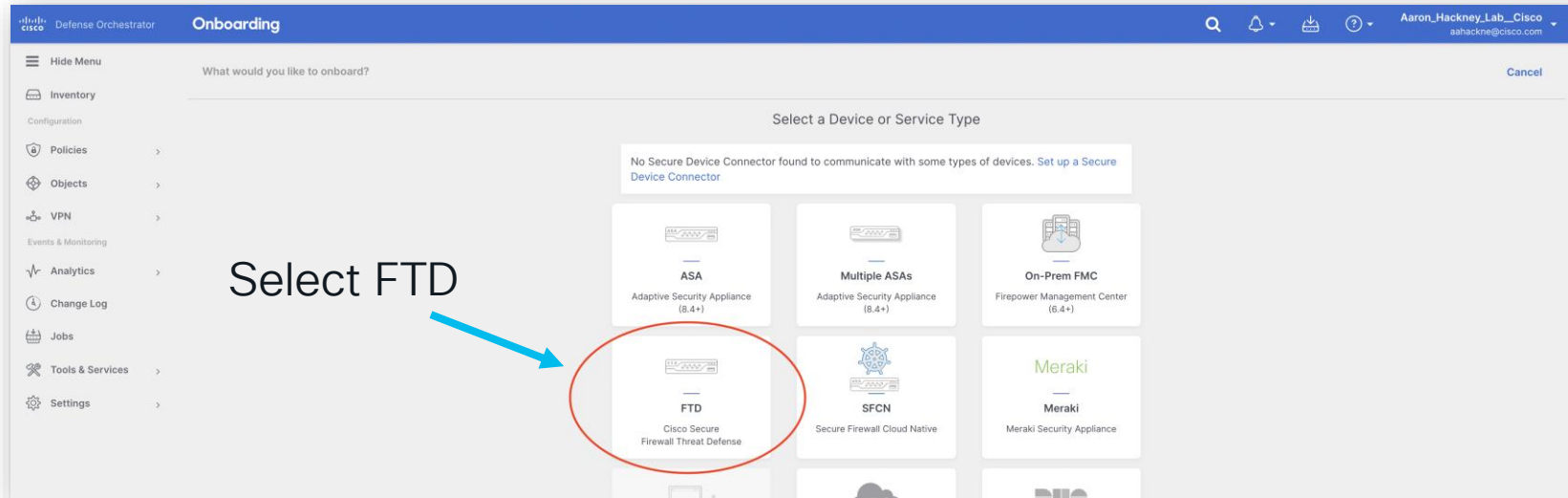
- ❖ Wizard Driven
- ❖ Deploy instance
- ❖ Auto-Add to cdFMC
- ❖ All from CDO

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: 'arid-pirate' with a status of 'Synced' and connectivity of '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

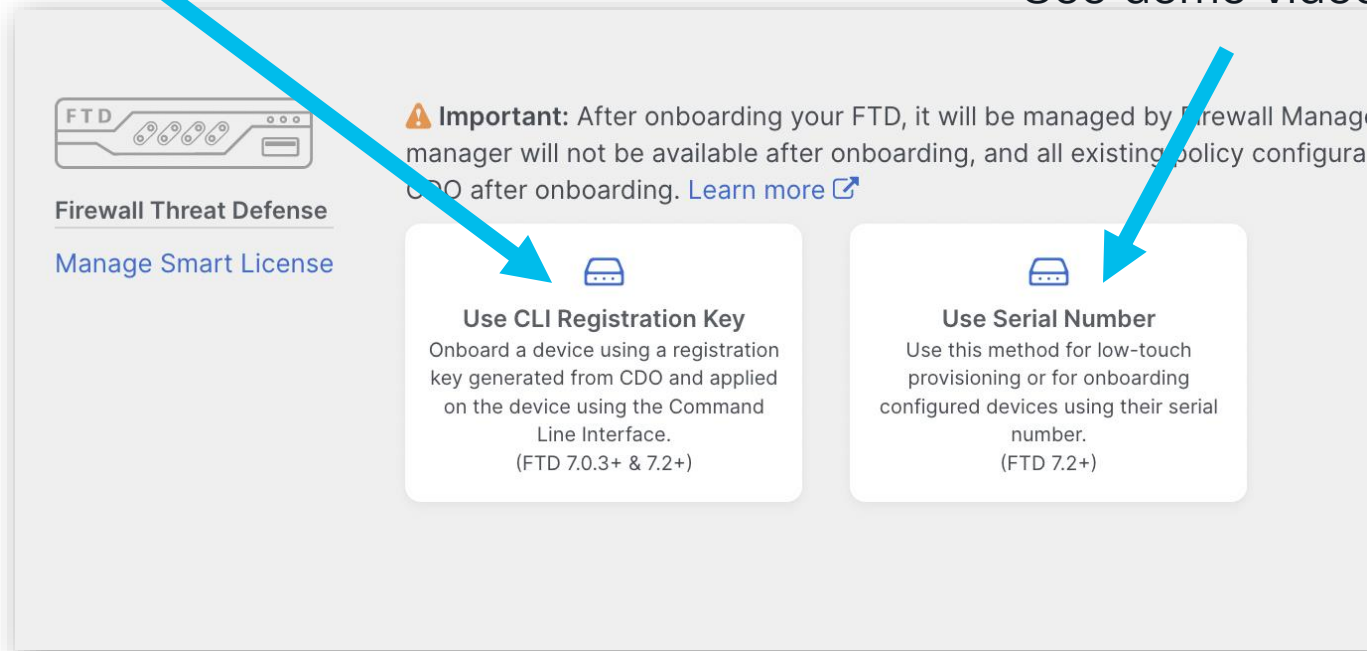


Onboard Cisco Secure Firewall

“configure manager” CLI method

Low touch provisioning for
FPR1000, FPR2100, FPR3100

See demo video [here](#)



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 displays a five-step onboarding wizard for a Cisco Secure Firewall. The steps are: 1. Device Name (CHICAGO-PRIMARY), 2. Policy Assignment, 3. Subscription License, 4. Create Registration Key, and 5. Done. In the 'Policy Assignment' step, the 'Access Control Policy' dropdown menu is open, showing 'Default Access Control Policy' as the selected option. A blue arrow points from the text 'Assign the default policy' to the dropdown menu. The dropdown menu also includes a search bar and a 'Select' button.

1 Device Name **CHICAGO-PRIMARY**

2 Policy Assignment

Access Control Policy

Default Access Control Policy ▼

Q Select Access Control Policy

Default Access Control Policy

Cancel Select

3 Subscription License

4 Create Registration Key

5 Done

Assign the default policy

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)

Next

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

Onboard Cisco Secure Firewall

4

Create Registration Key

1

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

2

Copy registration command

3

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

Next

Copy registration command to clipboard

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

Onboard Cisco Secure Firewall

Refresh connectivity status

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

Name	Configuration Status	Connectivity
CHICAGO-PRIMARY FTD	-	Pending Setup
		Online

CHICAGO-PRIMARY
FTD

Device Details

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

Registration Failed

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. To retry onboarding, click the 'Retry Onboarding' link below.

Additional Information

Registration timed out. Please check connectivity and registration id

configure manager add aahackne.app.s... [Retry Onboarding](#)

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.

Registration will retry every 5 minutes or
We can click “Retry Onboarding” for on-demand retry.

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

The screenshot displays the Cisco Secure Firewall onboarding interface. On the left, a 'Connectivity' filter shows 'Onboarding' (green circle) and 'Online' (green circle). The main panel shows details for 'CHICAGO-PRIMARY' (FTD). Below the 'Device Details' section, a 'Syncing' status is shown with a loading icon and the message: 'Successfully registered the device. Deployment is in progress. Please check back in a moment.' A blue arrow points from the 'Syncing' status to the 'Onboarding Method' field in the 'Device Details' section.

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

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

Onboard Cisco Secure Firewall

Inventory

Search by Device Name, IP Address, or Serial Number

Displaying 2 of 2 results

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 Threat Defense for VMware
- Serial: 9AG4K0V2BXE
- Version: 7.2.0
- Onboarding Method: Registration Key

Synced
Your device's configuration is up-to-date.

Device Actions

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

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

Onboard Cisco Secure Firewall

The screenshot displays the Cisco Secure Firewall Management Center (FMC) interface. The main panel shows the 'Inventory' page with a table of devices. The 'CHICAGO-PRIMARY' device is selected, and its details are shown on the right. The 'Management' section on the right is circled in blue.

Inventory

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

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 Threat Defense
- Serial: 9AG4K0V2BXE
- Version: 7.2.0
- Onboarding Method: Registration Key

Your device's configuration is up-to-date

Device Actions

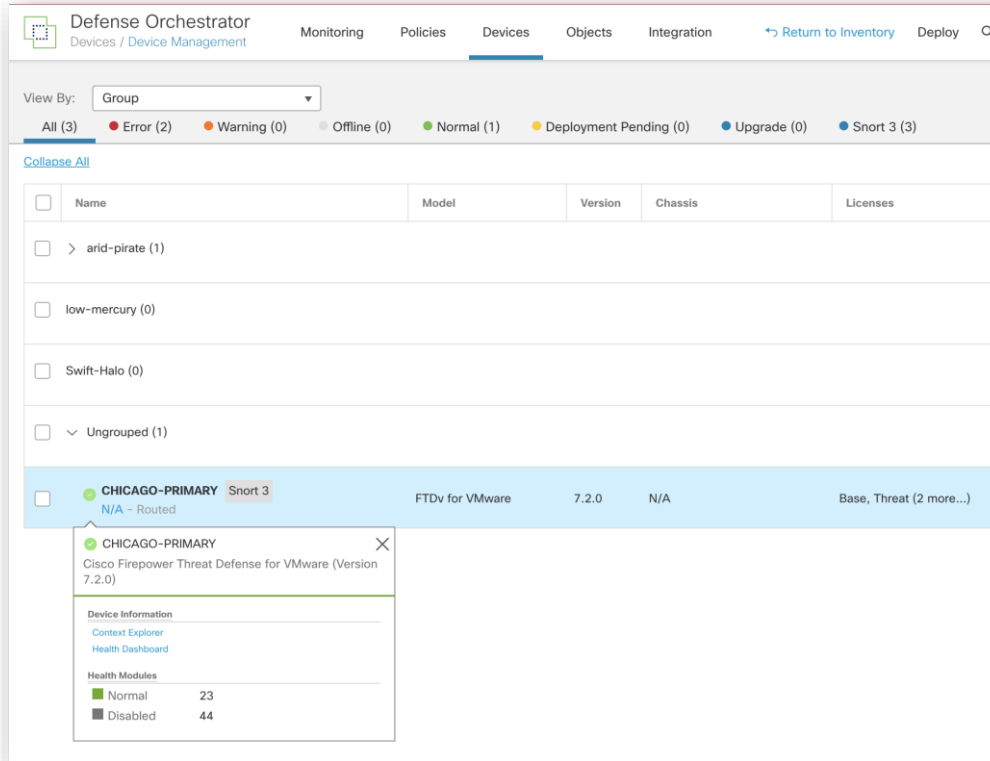
- Check for Changes
- Manage Licenses
- Workflows
- Remove
- More Actions

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, specifically the 'Devices' tab under 'Device Management'. The interface displays a list of devices with columns for Name, Model, Version, Chassis, and Licenses. A device named 'CHICAGO-PRIMARY' is highlighted, and a pop-up window shows its details, including 'Cisco Firepower Threat Defense for VMware (Version 7.2.0)' and health status: Normal (23) and Disabled (44).

Defense Orchestrator
Devices / Device Management

Monitoring Policies **Devices** Objects Integration [Return to Inventory](#) Deploy

View By: Group

[All \(3\)](#) [Error \(2\)](#) [Warning \(0\)](#) [Offline \(0\)](#) [Normal \(1\)](#) [Deployment Pending \(0\)](#) [Upgrade \(0\)](#) [Snort 3 \(3\)](#)

[Collapse All](#)

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

CHICAGO-PRIMARY Snort 3
Cisco Firepower Threat Defense for VMware (Version 7.2.0)

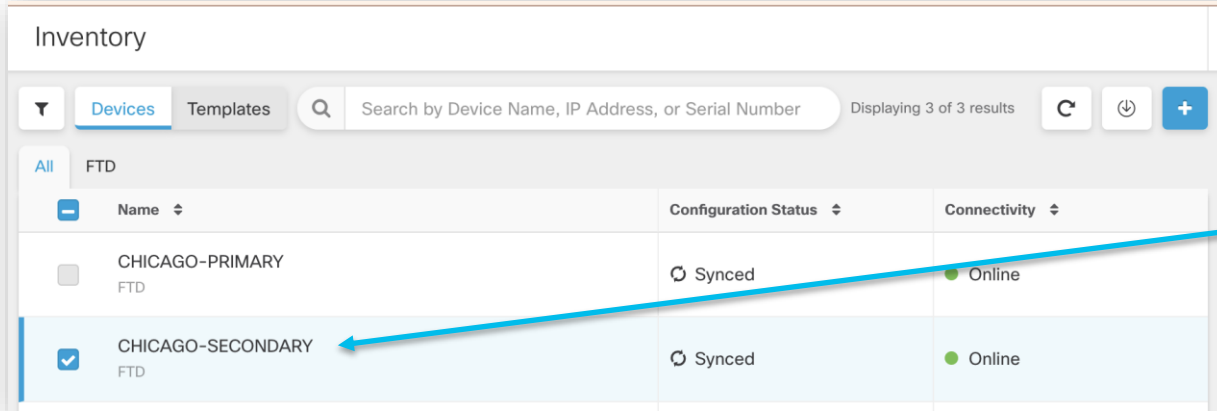
Device Information

[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

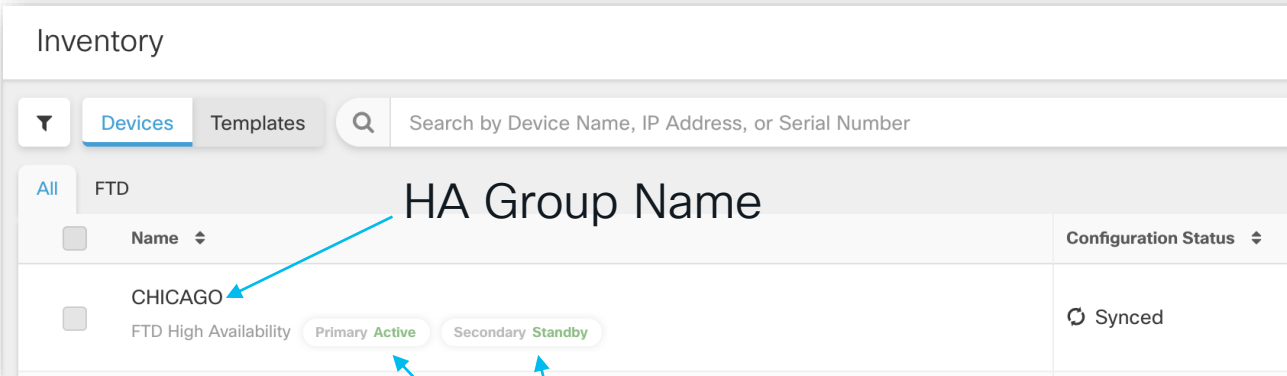
Displaying 3 of 3 results

All FTD

	Name	Configuration Status	Connectivity
☐	CHICAGO-PRIMARY FTD	Synced	Online
☒	CHICAGO-SECONDARY FTD	Synced	Online

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

Onboard Cisco Secure Firewall



The screenshot shows the 'Inventory' page in the Cisco Secure Firewall management center. The 'Devices' tab is selected. A search bar is present with the placeholder text 'Search by Device Name, IP Address, or Serial Number'. Below the search bar, there are filters for 'All' and 'FTD'. The main table has columns for 'Name', 'HA Group Name', 'Configuration Status', and 'HA roles and status (green/red)'. A device named 'CHICAGO' is listed with the HA Group Name 'FTD High Availability', Configuration Status 'Synced', and HA roles 'Primary Active' and 'Secondary Standby'. Blue arrows point from the text labels to the corresponding columns in the table.

	Name	HA Group Name	Configuration Status
☐	CHICAGO	FTD High Availability	Synced
		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

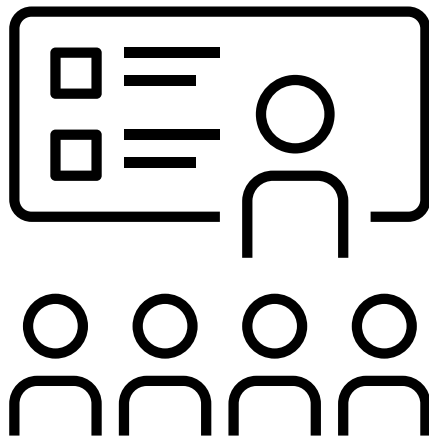
Technical Level: Intermediate

Technology: Cloud, Security

Track: Security



Live demo of cdFMC and FTD management



ASA Management

ASA Management

Platform Settings



Parent Policy: ⚙️ None ...

DNS

HTTP

NTP Not Configured

SSH

Syslog

Sysopt

DNS

Configure servers

Interface Name	IP Address	Actions
-	208.67.222.222	
-	208.67.220.220	
-	8.8.8.4	
-	8.8.4.4	

Domain name:

DNS Lookup

To configure DNS, enable DNS lookup on at least one interface.

Interface Name	Actions
outside	

ResetSave

ASA Management

Interface Settings



Interfaces / Clarksville

Search

Return to Inventory

Search for interfaces by name or ip address

Displaying 10 of 10 results

Name	Logical Name	State	Link State	IP Address	Interface Type	Mode
GigabitEthernet0/1	outside	Enabled	UP	10.10.6.42 STATIC	Physical Interface	Routed
GigabitEthernet0/1.99		Enabled	UP		Subinterface	Routed
GigabitEthernet0/1.100		Enabled	UP	99.99.99.1 STATIC	Subinterface	Routed
GigabitEthernet0/6		Disabled	DOWN		Physical Interface	Routed
GigabitEthernet0/4		Disabled	DOWN		Physical Interface	Routed
GigabitEthernet0/5		Disabled	DOWN		Physical Interface	Routed
GigabitEthernet0/2	test1	Disabled	DOWN		Physical Interface	Routed
GigabitEthernet0/2.999		Enabled	DOWN		Subinterface	Routed
GigabitEthernet0/3	stella	Enabled	UP		Physical Interface	Routed
GigabitEthernet0/0	inside	Enabled	UP	192.168.228.1 STATIC	Physical Interface	Routed
GigabitEthernet0/7		Disabled	DOWN		Physical Interface	Routed
Management0/0		Disabled	DOWN		Physical Interface	Routed
GigabitEthernet0/8		Disabled	DOWN		Physical Interface	Routed

ASA Management

Static Routing



Routing / Clarksville

Return to Inventory

Search static routes

Displaying 2 of 2 results

Interface	IP Version	Destination	Gateway IP	Metric
outside	IPv4	0.0.0.0 0.0.0.0	10.10.6.33	1
inside				1

Add Static Route

Description

COLD

IP Version *

☒ IPv4 ☐ IPv6

Interface *

Null0

Search interfaces

Null0 ✓

outside
10.10.6.42/27

Gateway IP (Next Hop)

e.g. 192.168.1.1

Metric *

1

1-255

Destination Mask

e.g. 255.255.255.0

Tracking

None

Cancel Save

ASA Management

New Policy Editor Coming Soon!



ASA Policies / Clarksville

Search

Return to Inventory

Destination

Access Groups +

Global-Policy-Branch
Global

outside
-

global_access
test1 / in

cvs_tes
outside / out

new-asa-policy
inside / out

inside_access_in
inside / in

Berlin-Clarksville
-

Search rules

Displaying 3 of 3 results

Go to

	Action	Protocol	Source	Port	SGT Group	Destination	Port	SGT Group	Logging	Remark
☐	1 Allow	ip	Any	Any	Any	Any	Any	Any		
☐	2 Allow	ip	HOSTS	Any	Any	Any	Any	Any		
☐	3 Block	tcp	PrinterNetwo...	Adam1	Any	18Feb21-Obj1	Any	Any	warnings	

ASA Management

Objects and Policy Management

The screenshot displays the Cisco ASA Management Center interface, divided into three main sections:

- Left Panel (Object Management):** Shows a list of objects under the 'Name' column. The 'WebServer' object is selected. Below the list, the 'NETWORK ADDRESS' section shows the IP address '192.168.1.10'. The 'ENCIPHERMENT' section shows the object '_SmartCallHome_ServerCA' selected.
- Center Panel (Policy Management):** Displays the 'ASA Access Policies / PointOfSale / Access Control Entries' configuration page. It shows a table of 28 rules, all of which are 'Permit' actions. The table columns are: Line, Action, Protocol, Source, Port, Destination, Port, and Hits (Day). The rules are numbered 1 through 28.
- Right Panel (Policy Details):** Shows the 'PointOfSale' configuration page. It includes a search bar, a 'Previous' button, and a 'Next' button. The 'Access Control Entries' section shows a list of entries, with '1' selected. The 'Logging' section shows the 'Default' logging level. The 'Time Range' section shows a 'Select Time Range' dropdown. The 'Remarks' section shows a text area for adding remarks. The 'Devices' section shows a list of devices, with 'Network4' selected.

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 star icon and a trash icon:

- 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 with the command `> interface outside` and `shut` entered. Below the input field, there is a hint: "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 icon and a name:

- 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, there is a "Send" button with a plus icon.

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

2 ASDM Software Image 7.14(1) →

3 Perform Upgrade

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

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.

CISCO *Live!*

#CiscoLiveAPJC

BRKSEC-1138

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

69

ASA Management

Detailed Changelogs and Diff Views Available

The screenshot displays the 'Change Log' interface for ASA Management. At the top, there is a blue header with the title 'Change Log'. Below the header, a navigation bar includes a 'Return to Inventory' link, a search bar, and a filter button set to 'Devices Minneapolis'. The main content area features a table with columns for 'Last Updated', 'Device Name', and 'Last Description'. The table lists two entries for the device 'Minneapolis': one from Nov 30, 2022, at 6:30:34 AM for 'CLI Execution', and another from Nov 29, 2022, at 2:58:45 AM for 'Changes written successfully'. Below the table, a detailed view for the Nov 29, 2022, entry is shown. This view includes a timeline of events for that date, with the most recent event at 2:58:45 AM being 'Changes written successfully'. The diff view for this event shows the following changes:

```
object network Cincinnati-Printer-Network
-subnet 192.168.124.0 255.255.252.0
```

Below this, another event at 2:58:44 AM is listed as 'Changed ASA Config'. The diff view for this event shows the following changes:

```
@@ -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
+Cryptochecksum:aed84725c88b533530c9d029de6d5c46
```

Finally, an event at 2:57:49 AM is listed as 'Changed ASA Config'. The diff view for this event shows the following changes:

```
@@ -90,1 +90,1 @@
-subnet 192.168.124.0 255.255.254.0
+subnet 192.168.124.0 255.255.252.0
```

ASA Management

Troubleshooting Tools From CDO – No CLI required

The screenshot shows the Cisco Defense Orchestrator (CDO) interface for ASA Management. The top navigation bar includes the Cisco logo, "Defense Orchestrator", and the current path "ASA: Clarksville / Troubleshoot". On the right of the bar are search, notifications, and user profile icons.

A left-hand 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 "Clear PACKET TRACER OUTPUT". It features a "Run Packet Tracer" button and a "View Real-Time Log" button. Below these are configuration fields for a packet trace:

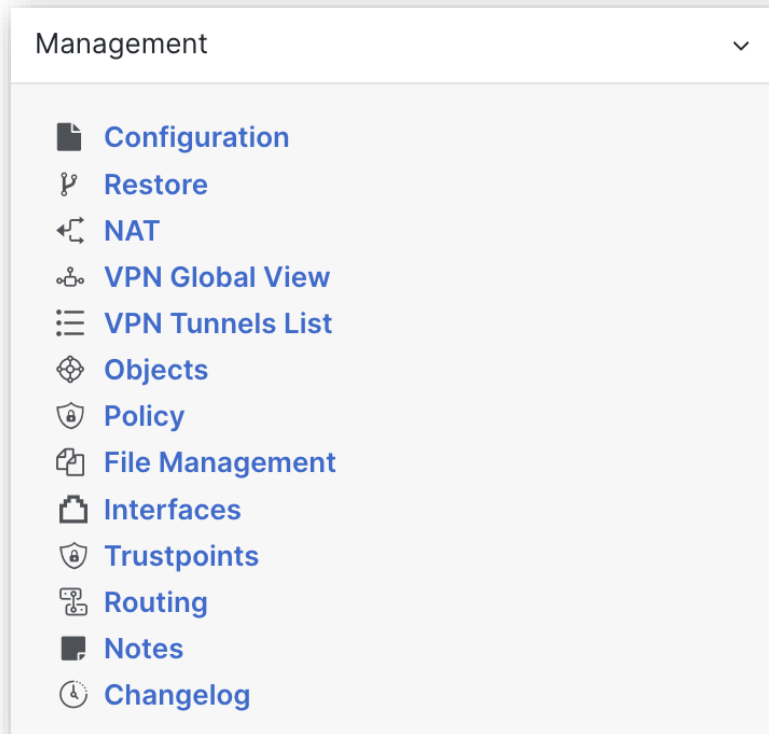
- Interface:** A dropdown menu currently set to "inside".
- Packet Type:** Radio buttons for TCP (selected), UDP, ICMP, IP, and SCTP.
- Source:** A dropdown menu set to "IP Address" and a text input field labeled "Enter Source".
- Port:** A dropdown menu labeled "Enter Source Port".
- Destination:** A dropdown menu set to "IP Address" and a text input field labeled "Enter Destination".
- Port:** A dropdown menu labeled "Enter Destination Port".
- SGT Number (0-65535):** A text input field labeled "Enter SGT Number (optional)" with a help icon.

Below the configuration fields is a section titled "REAL-TIME LOG OUTPUT".

Instructions and a warning are displayed in the center of the main area:

- To run the Packet Tracer tool fill out the required inputs and click the "Run Packet Tracer" button in the left panel
- To monitor System Log Messages fill out some inputs to filter messages by and click the "View Real-Time Log" button in the left panel
- A warning icon and text: "The device is not synced. You could encounter some unexpected results from packet-tracer."

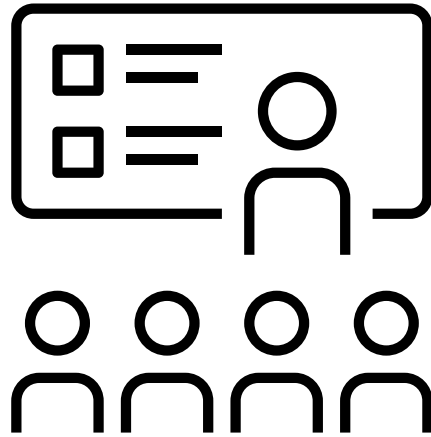
ASA Management



Lots more functionality including:

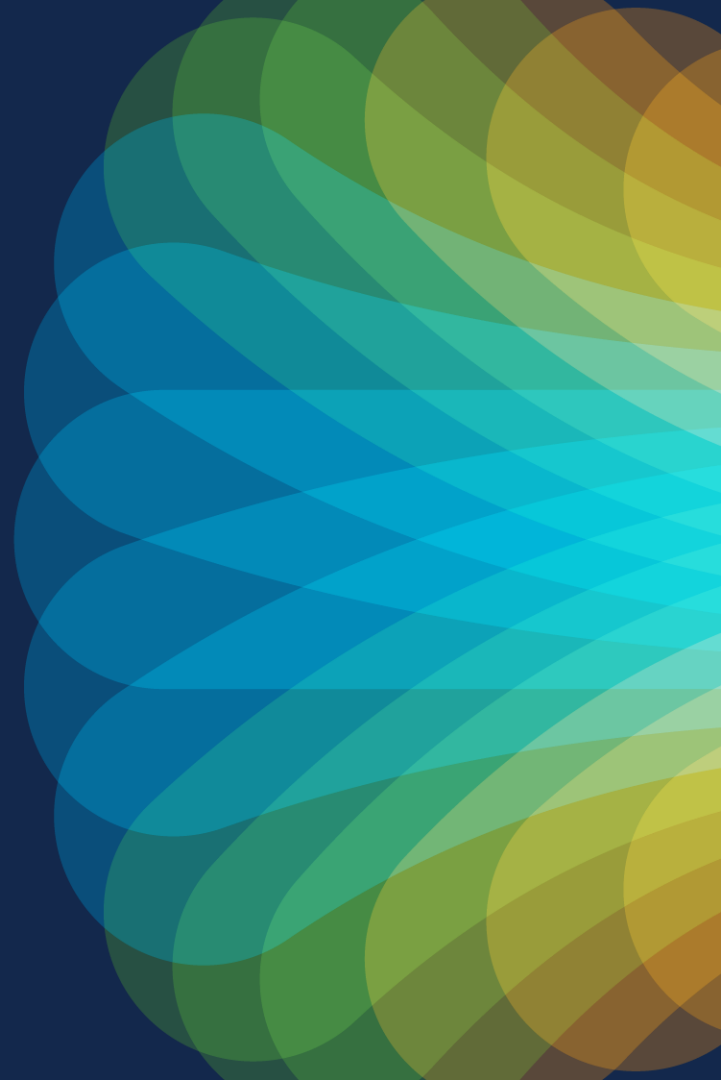
- Configuration visibility
- NAT policy
- Backups
- File management
- Certificate management
- Out of band change management
- Interface configuration
- Routing configuration
- Platform Settings Policy

Live demo of common ASA tasks



CDO Visibility

Security Analytics and Logging



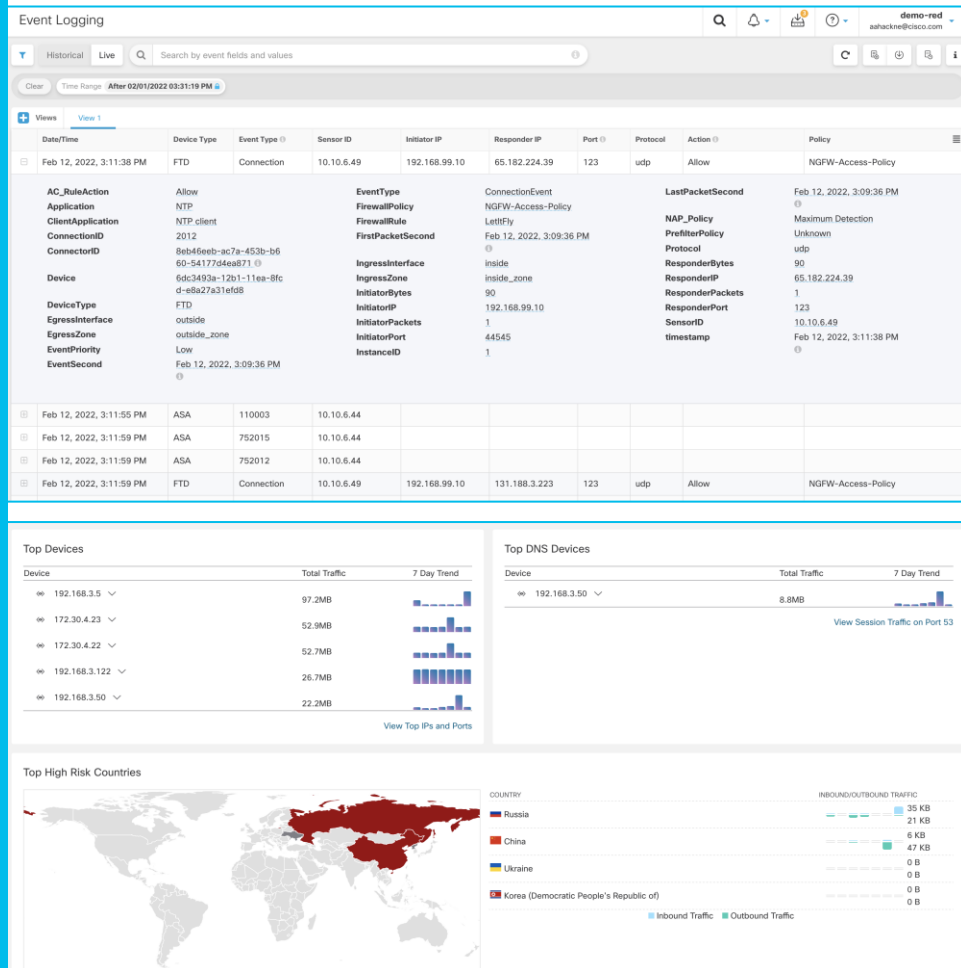
Security Analytics and Logging

Unified views:

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

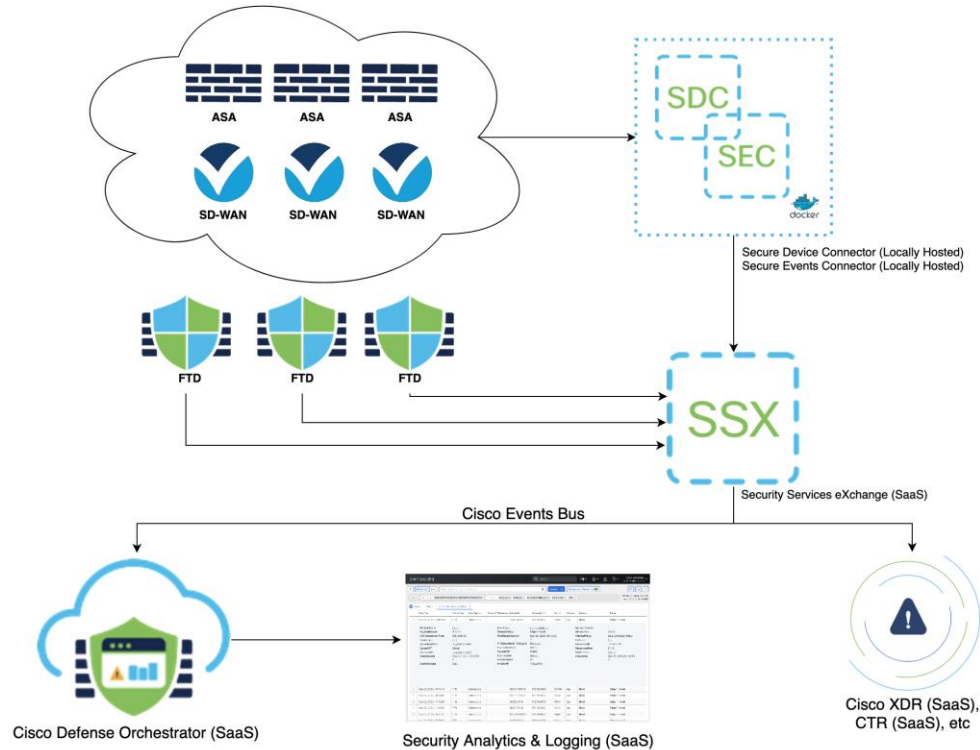
SCALE

CISCO *Live!*



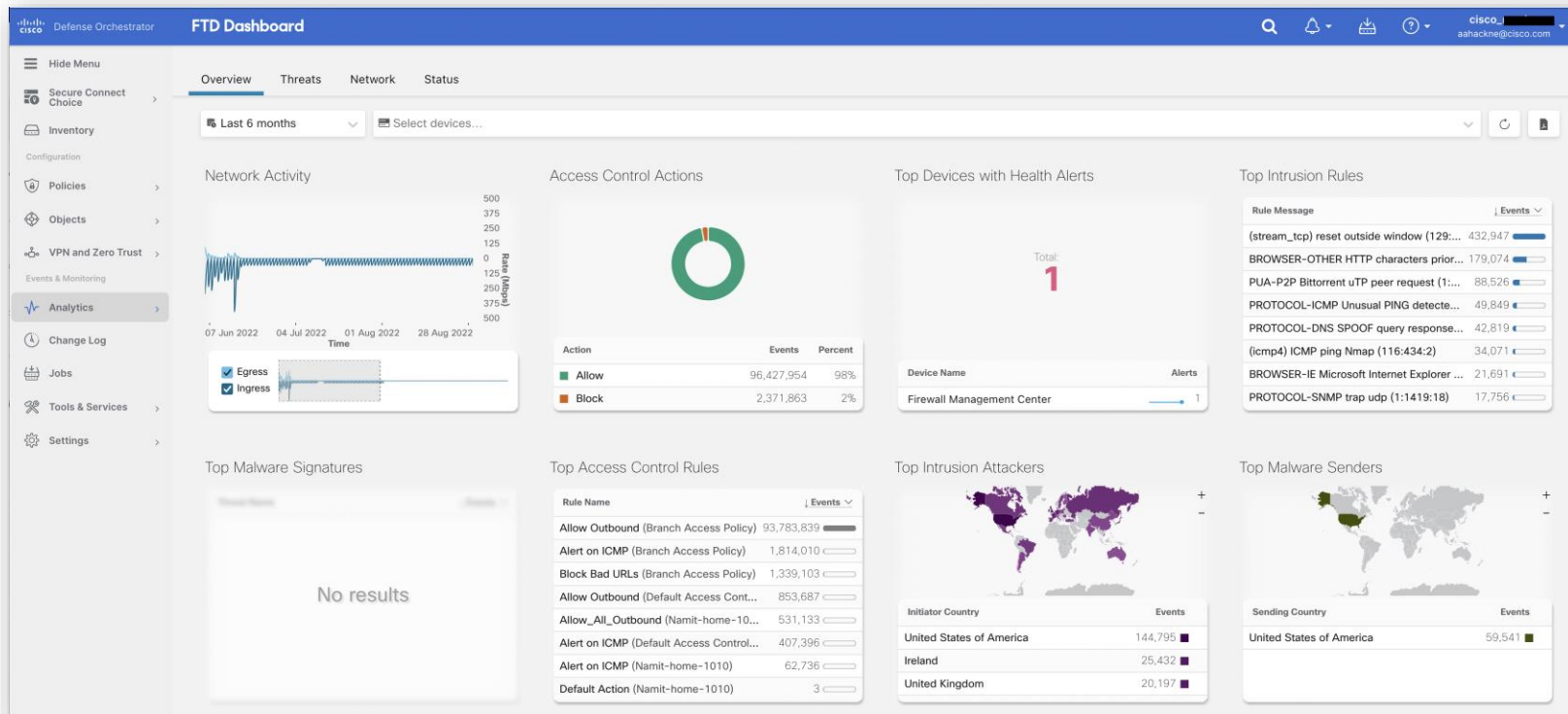
Security Analytics and Logging

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-backtoham.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

Event Logging

Search

Historical Live

Search by event fields and values

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

FTD Events Intrusion Malware Security Intelligence

Search Background Searches 21

Search in Background

Run in the background and be notified later when the results are ready.

+ Views View 1

	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

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

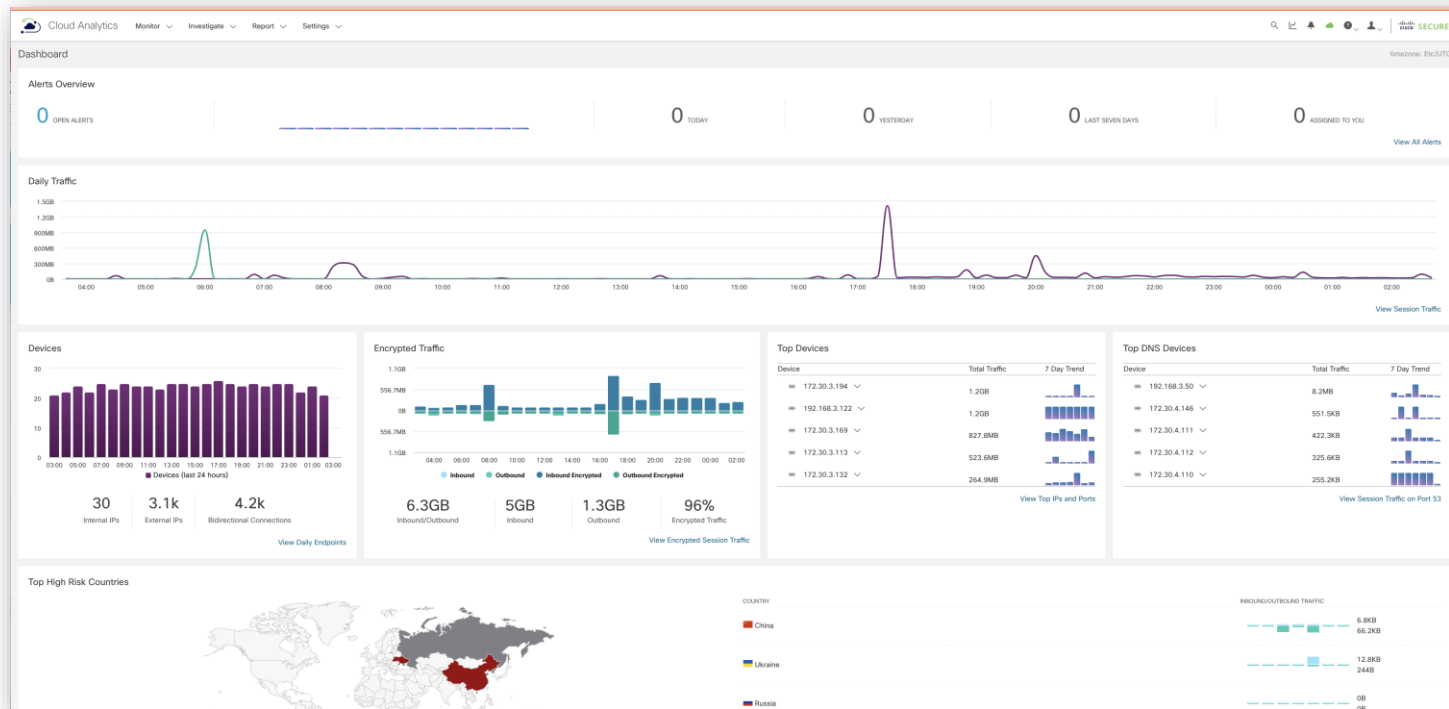
Time (UTC+00:00) 03 : 00

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

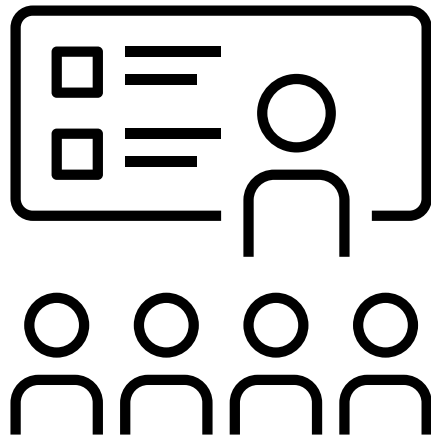
What's coming for Security Analytics and Logging*

- 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 Terraform Provider

CDO terraform provider available through the Terraform Registry
<https://registry.terraform.io/providers/CiscoDevNet/cdo/latest>



The screenshot shows the Terraform Registry interface. At the top, there's a purple header with the Terraform logo and a search bar. Below the header, a breadcrumb trail reads 'Providers / CiscoDevNet / cdo / Version 1.0.1', with a 'Latest Version' button. The main content area features the 'cdo' provider name with a small icon, a 'Partner' badge, and the text 'by: CiscoDevNet'. Below this is a 'Cloud Automation' tag. At the bottom, there are three sections: 'VERSION 1.0.1', 'PUBLISHED a day ago', and 'SOURCE CODE' with a link to 'CiscoDevNet/terraform-provider-cdo'.

cdo

Cloud Automation

VERSION 1.0.1

PUBLISHED a day ago

SOURCE CODE [CiscoDevNet/terraform-provider-cdo](#)

CDO Ansible Collection

CDO Ansible collection available through Ansible-Galaxy

<https://galaxy.ansible.com/ui/repo/published/cisco/cdo>



The screenshot shows the Ansible Galaxy web interface. On the left is a dark sidebar with navigation links: 'Ansible Galaxy', 'Search', 'Collections' (with a dropdown arrow), 'Namespaces', 'Roles' (with a right arrow), 'Documentation' (with an external link icon), and 'Terms of Use' (with an external link icon). The main content area has a dark header with a hamburger menu icon and the 'GALAXY' logo. Below the header is a message: 'Thanks for trying out the new and improved Galaxy, please share your feedback on forum.ansible.com.' The breadcrumb trail is 'Namespaces > cisco > cdo'. The collection name 'cdo' is displayed prominently. Below it, the version '1.1.7 updated 8 days ago (latest)' is shown, along with a dropdown menu and the text 'Last updated 8 days ago'. There are five tabs: 'Install' (active), 'Documentation', 'Contents', 'Import log', and 'Dependencies'. The 'Install' tab contains the heading 'Install' and the description 'A collection for automating Cisco Defense Orchestrator'. Below this is a row of tags: 'cdo', 'defense', 'cdfmc', 'ios', 'fmc', 'ftd', 'firepower', 'security', 'cisco', 'asa', and 'orchestrator'. The 'Installation' section shows the command 'ansible-galaxy collection install cisco.cdo' in a light gray box. Below the command is a note: 'Note: Installing collections with ansible-galaxy is only supported in ansible-core>=2.13.9'. At the bottom, there is a 'Download' section with a blue download icon and the text 'Download tarball'.

CDO API

A **NEW** customer API is coming! (March/April 2024*)
Both fully documented and DevNet community supported



asa-device-controller

POST /v1/inventory/devices/asas Onboard a ASA device in the CDO tenant.

transactions-controller

GET /v1/transactions/{transactionUid} Get information of an in-progress CDO transaction.

regions-controller

GET /v1/regions Fetch a list of CDO regions.

template-device-controller

GET /v1/inventory/templates Fetch a list of template devices in the CDO tenant.

GET /v1/inventory/templates/{templateDeviceUid} Fetch a template device by UID in the CDO tenant.

device-cloud-services-controller

GET /v1/inventory/services Fetch a list of Cloud Services in the CDO tenant.

GET /v1/inventory/services/{cloudServiceUid} Fetch a Cloud Service by UID in the CDO tenant.

* Subject to change

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 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

					No API Token
				12/1/2022 5:44:08 AM	No API Token

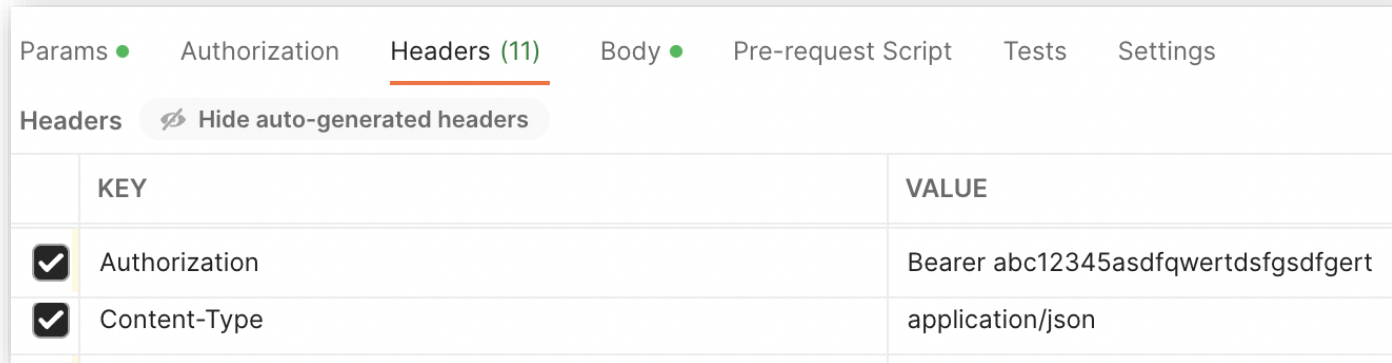
*Disclaimer: API is not fully supported (YET!) today but nothing is stopping your careful use of it.

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:



The screenshot shows the Postman interface with the 'Headers' tab selected. The 'Headers' section is expanded, showing a table with two headers: 'KEY' and 'VALUE'. Two headers are listed: 'Authorization' with a value of 'Bearer abc12345asdfqwertdsfgsdfgert' and 'Content-Type' with a value of 'application/json'. Both headers have a checked checkbox in the first column.

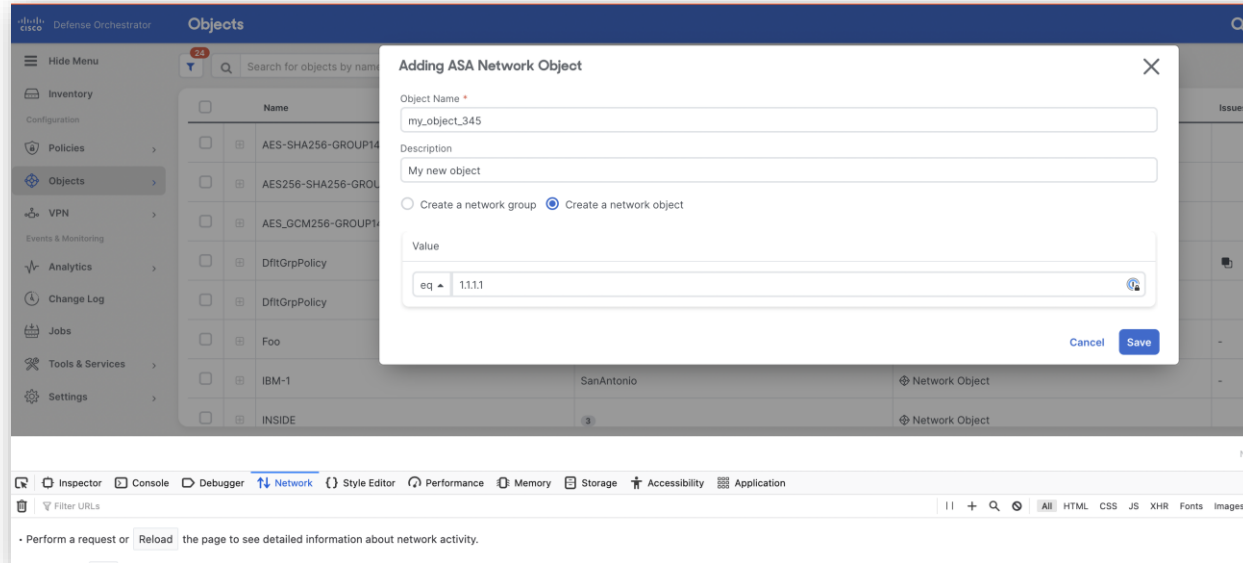
	KEY	VALUE
☒	Authorization	Bearer abc12345asdfqwertdsfgsdfgert
☒	Content-Type	application/json

cURL Example: `curl --header 'Content-Type: application/json' --header 'Authorization: Bearer abc12345asdfqwertdsfgsdfgert'`

CDO API

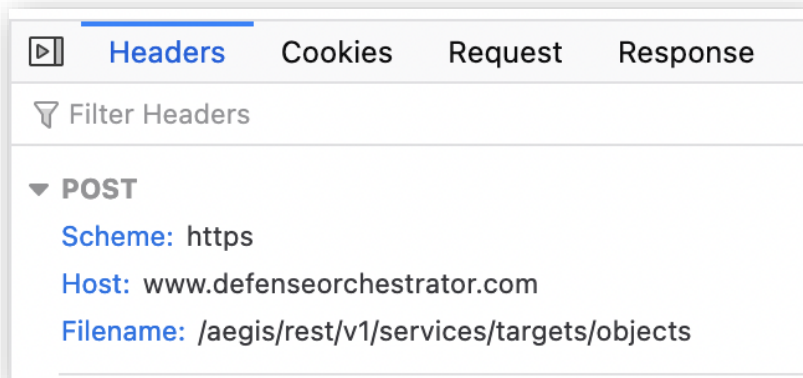
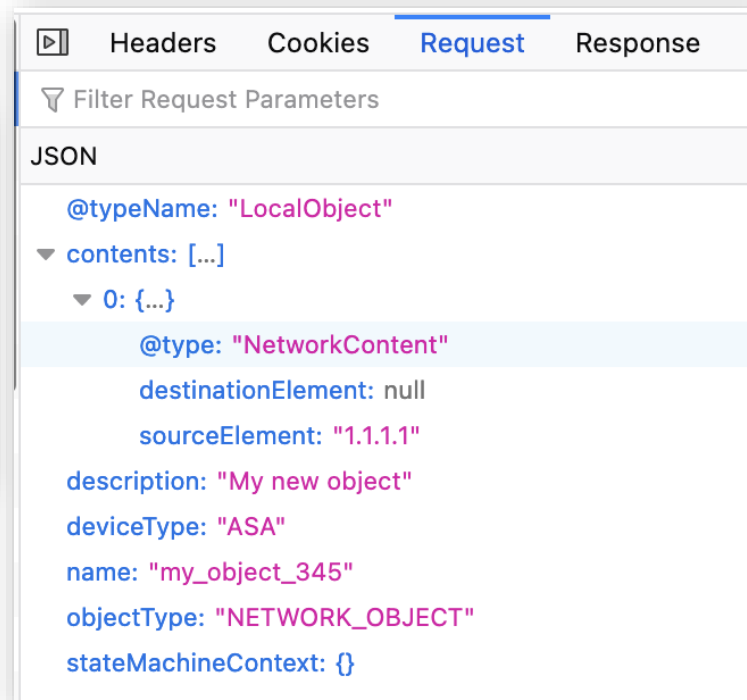
Step 3: How does the CDO UI do it?

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?



Automating CDO using Terraform and Ansible



EXPLORER

FULL CONFERENCE

IT LEADERSHIP

Automate Cisco Defense Orchestrator (cdFMC/FTD, ASA, and IOS) with Ansible (Workshop) [DEVWKS-1730]

Aaron Hackney, Technical Product Owner, Cisco

Full

Friday, Dec 8 | 9:15 AM - 10:00 AM AEDT | DevNet Workshop 1



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>

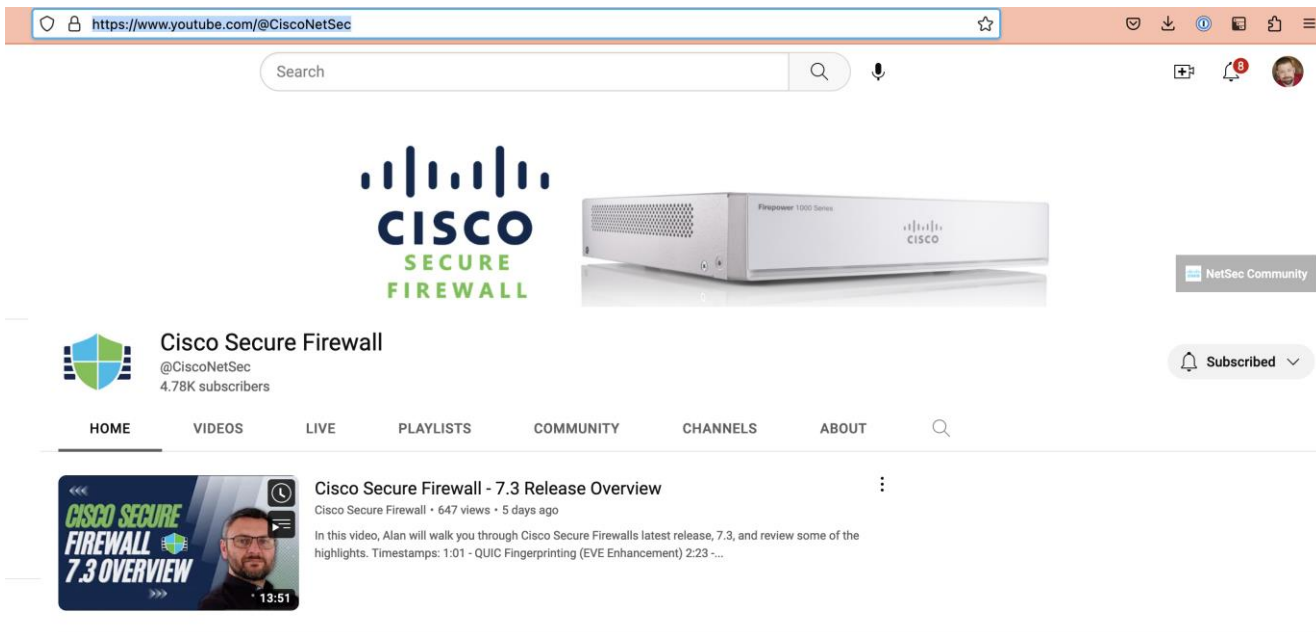
Or go to <https://getcdo.com>

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 links for HOME, VIDEOS, LIVE, PLAYLISTS, COMMUNITY, CHANNELS, and ABOUT. The first video in the list is "Cisco Secure Firewall - 7.3 Release Overview", which has 647 views and was posted 5 days ago. 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 - ...".



Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert 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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC