The bridge to possible

Cloud-delivered Firewall Management Center

BRKSEC-2318

Adam Bragg, Product Owner
Cloud and Network Security

FMC learns to fly

Your Speaker

CISCO DEFENSE ORCHESTRATOR

- From New Hampshire in the United States
- adam.bragg@cisco.com
- With Cisco since April 1, 2015
- Product Owner for Cisco Defense Orchestrator (CDO)
- Works with customers to ensure that CDO is delivering value for them.
- Enjoys traveling (27 countries, 5 continents so far) and most sports. Butler and chauffeur to his two children.

Content Creator Shout Out

- Namit Agarwal – Technical Marketing Engineer Leader

namiagar@cisco.com

- Aaron Hackney – Technical Product Owner

aahackne@cisco.com

Cisco Webex App

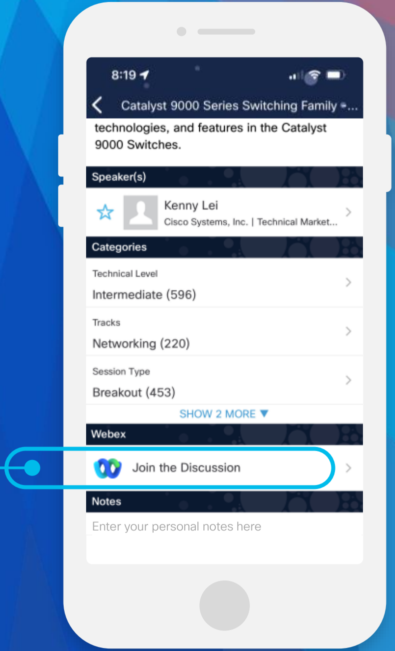
Questions?

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.



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2318

Session Objective

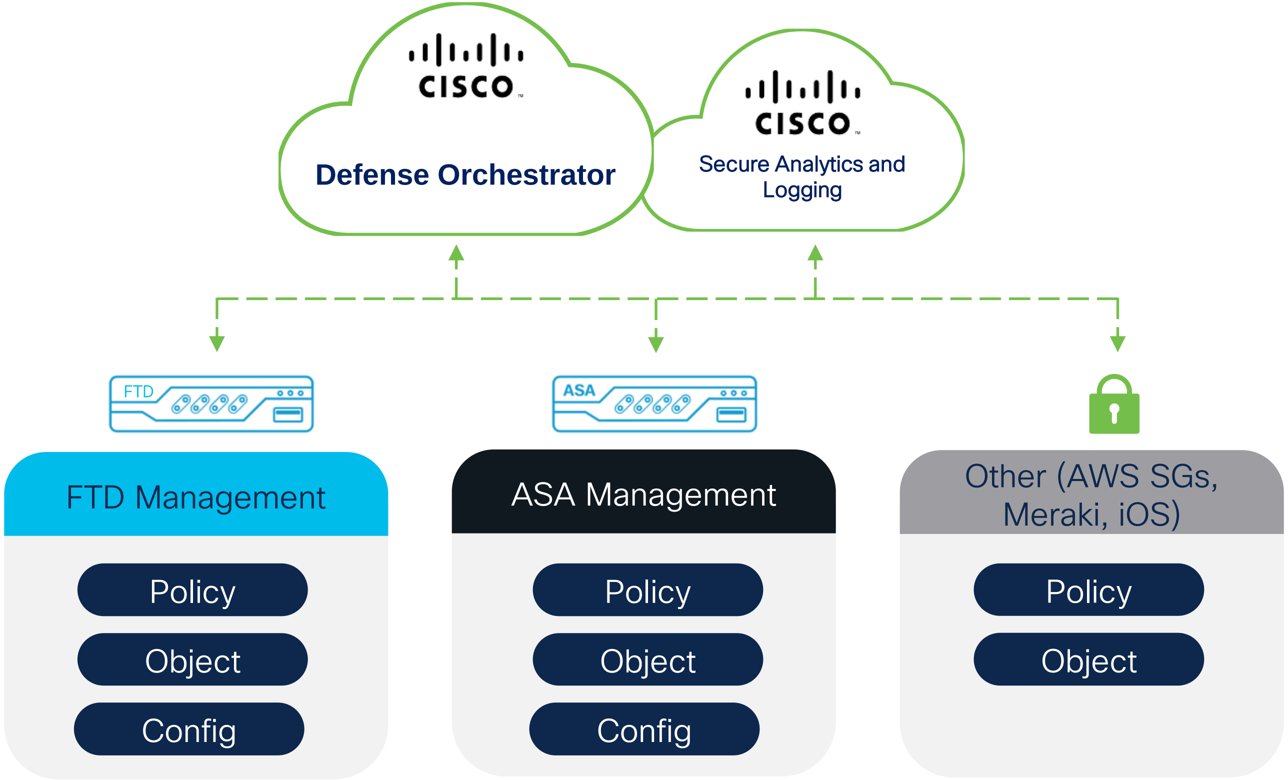
- Target Audience – Security Professionals familiar with Cisco Secure Firewall
- Learn about management options for Cisco Secure Firewall
- Understand the cloud-delivered Firewall Management Center
- Assist in the organization’s cloud adoption journey
- Make it easier to manage Firewalls with lower OpEx
- Provide simpler management experience of edge firewalls

Agenda

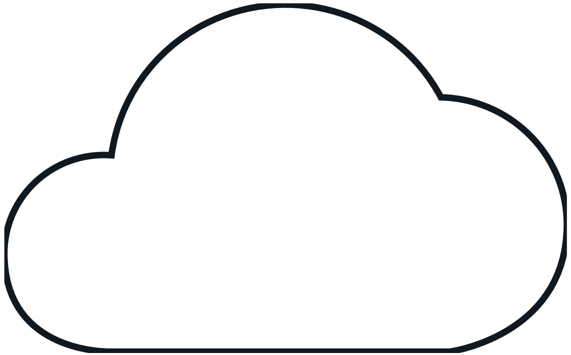
- Background and Vision
- Product Overview
- Key Use Cases
- Eventing and Analytics Capabilities
- Integrations
- Next steps
- Cheatsheets

Background and Vision

Cisco Defense Orchestrator



Cisco Secure gave FMC wings



via CDO

cisco SECURE

Firewall Management Center

Cloud-delivered Firewall Management Center

The SaaS **Firewall Management Center** with policy config and cloud analytics and logging

Same look and feel, no learning curve for existing users

Easy brownfield migration
Supports up to 1000 firewalls

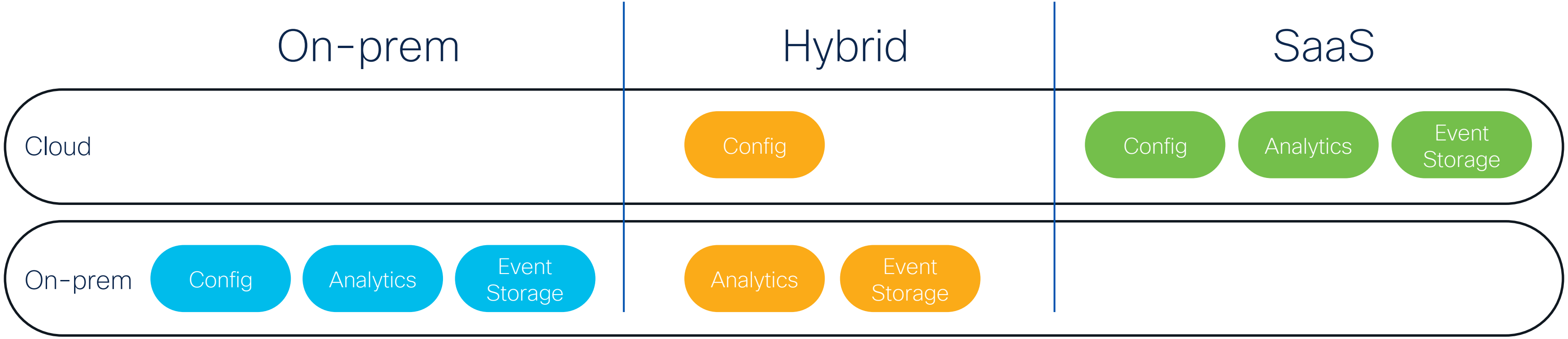
Full SaaS
No HW to refresh, no rack space, no utility bill

Cisco ensures uptime, patching, and updates.
SOC2!

Secure Firewall

Physical Hardware, Virtual Platforms, and Cloud Platforms!

Flexibility of Management Consumption



	On-prem	Hybrid	SaaS
Cloud		Config	Config Analytics Event Storage
On-prem	Config Analytics Event Storage	Analytics Event Storage	

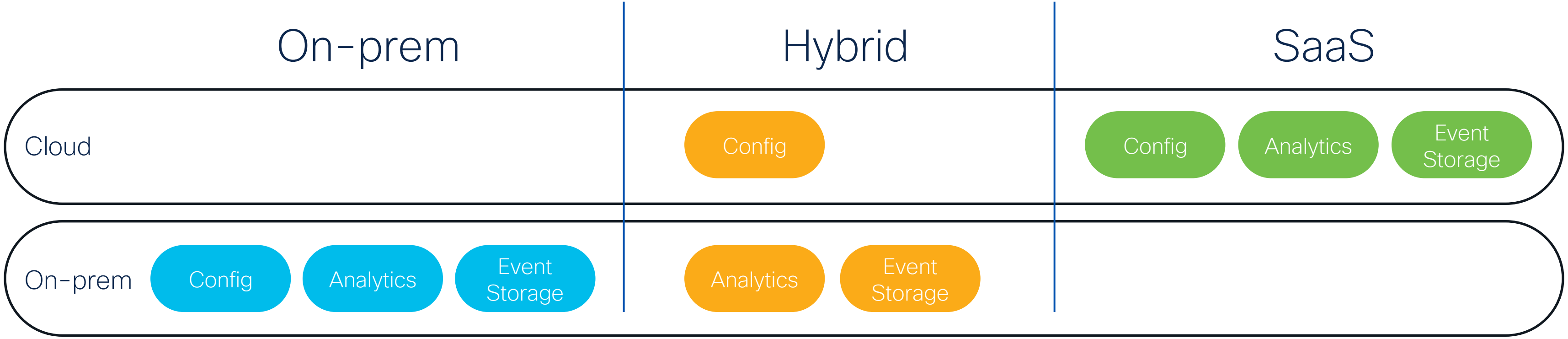
- Driven by security concerns or regulatory compliance
- Government, financials

- Sensitivities around customer data
- Retail, financials

- Cloud-first approach
- Technology, startups

Increasing customer cloud acceptance

Flexibility of Management Consumption



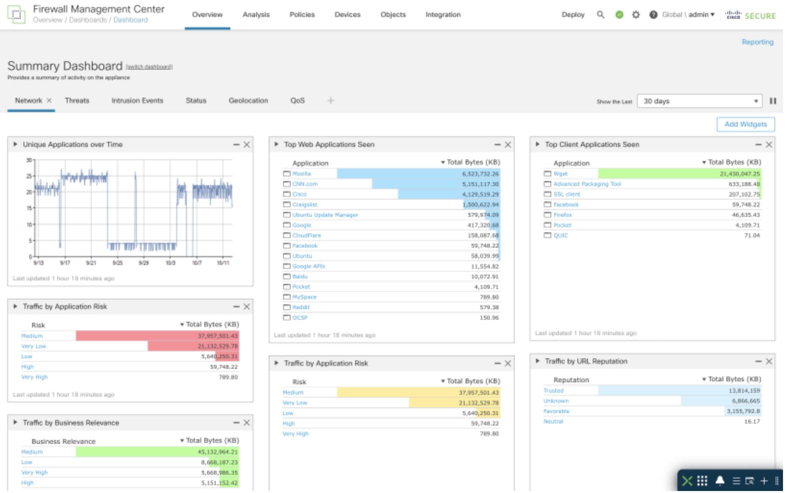
	On-prem	Hybrid	SaaS
Cloud		Config	Config Analytics Event Storage
On-prem	Config Analytics Event Storage	Analytics Event Storage	

It is really All About Your USE CASE!!

Increasing customer cloud acceptance

Firewall Management Center Options

Flexibility of cloud or on-premises options



Summary Dashboard (switch dashboard)

Provides a summary of activity on the appliance

Show the Last: 30 days

Unique Applications over Time

Last updated 1 hour 19 minutes ago

Traffic by Application Risk

Risk	▾ Total Bytes (KB)
Medium	37,957,501.43
Very Low	21,132,529.78
Low	5,640,250.31
High	59,748.22
Very High	789.80

Last updated 1 hour 18 minutes ago

Traffic by Business Relevance

Business Relevance	▾ Total Bytes (KB)
Medium	45,132,964.21
Low	8,668,187.23
Very High	5,668,986.35
High	5,151,152.42

Top Web Applications Seen

Application	▾ Total Bytes (KB)
□ Mozilla	6,523,732.26
□ CNN.com	5,151,117.30
□ Cisco	4,129,519.29
□ Craigslist	1,500,622.94
□ Ubuntu Update Manager	579,974.09
□ Google	417,320.68
□ CloudFlare	158,087.68
□ Facebook	59,748.22
□ Ubuntu	58,039.99
□ Google APIs	11,554.82
□ Baidu	10,072.91
□ Pocket	4,109.71
□ MySpace	789.80
□ Reddit	579.38
□ OCSP	150.96

Last updated 1 hour 18 minutes ago

Traffic by Application Risk

Risk	▾ Total Bytes (KB)
Medium	37,957,501.43
Very Low	21,132,529.78
Low	5,640,250.31
High	59,748.22
Very High	789.80

Top Client Applications Seen

Application	▾ Total Bytes (KB)
□ Wget	21,430,047.25
□ Advanced Packaging Tool	633,188.40
□ SSL client	207,102.75
□ Facebook	59,748.22
□ Firefox	46,635.43
□ Pocket	4,109.71
□ QUIC	71.04

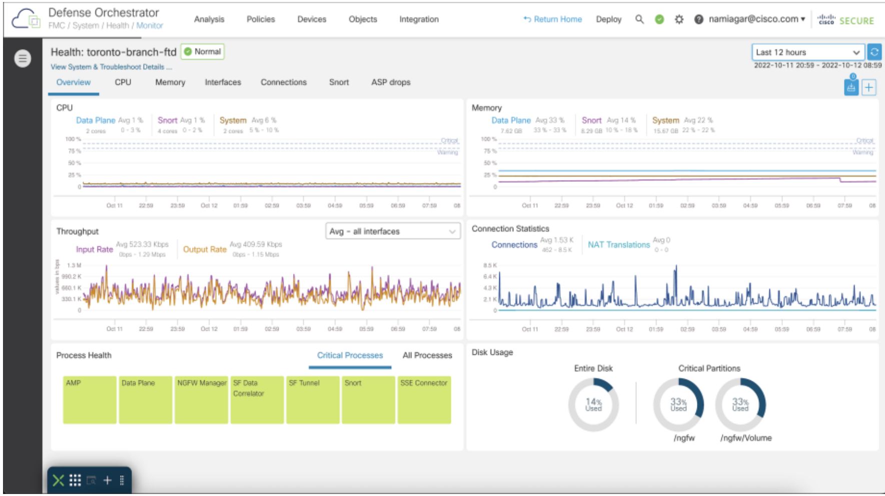
Last updated 1 hour 18 minutes ago

Traffic by URL Reputation

Reputation	▾ Total Bytes (KB)
Trusted	13,814,159
Unknown	6,866,665
Favorable	3,155,792.8
Neutral	16.17

Virtual or Hardware

Firewall Management Center



Health: toronto-branch-ftd ✓ Normal

View System & Troubleshoot Details ...

Last 12 hours

2022-10-11 20:59 - 2022-10-12 08:59

CPU

Data Plane Avg 1 % (2 cores, 0 - 3 %) | Snort Avg 1 % (4 cores, 0 - 2 %) | System Avg 6 % (2 cores, 5 % - 10 %)

Memory

Data Plane Avg 33 % (7.62 GB, 33 % - 33 %) | Snort Avg 14 % (8.29 GB, 10 % - 18 %) | System Avg 22 % (15.67 GB, 22 % - 22 %)

Throughput

Avg - all interfaces

Input Rate Avg 523.33 Kbps (0bps - 1.29 Mbps) | Output Rate Avg 409.59 Kbps (0bps - 1.15 Mbps)

Connection Statistics

Connections Avg 1.53 K (462 - 8.5 K) | NAT Translations Avg 0 (0 - 0)

Process Health

AMP | Data Plane | NGFW Manager | SF Data Correlator | SF Tunnel | Snort | SSE Connector

Disk Usage

Entire Disk: 14% Used

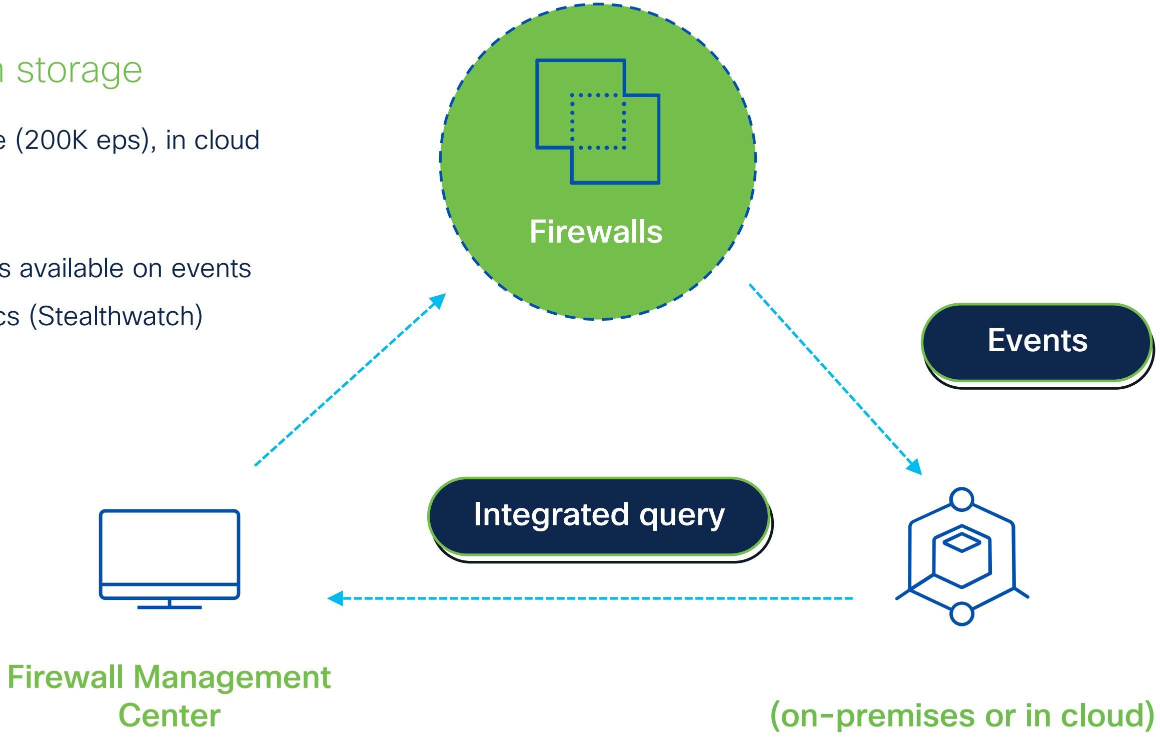
Critical Partitions: /ngfw 33% Used; /ngfw/Volume 33% Used

Cloud-delivered

Scalable Event Aggregation On-Premises and In Cloud

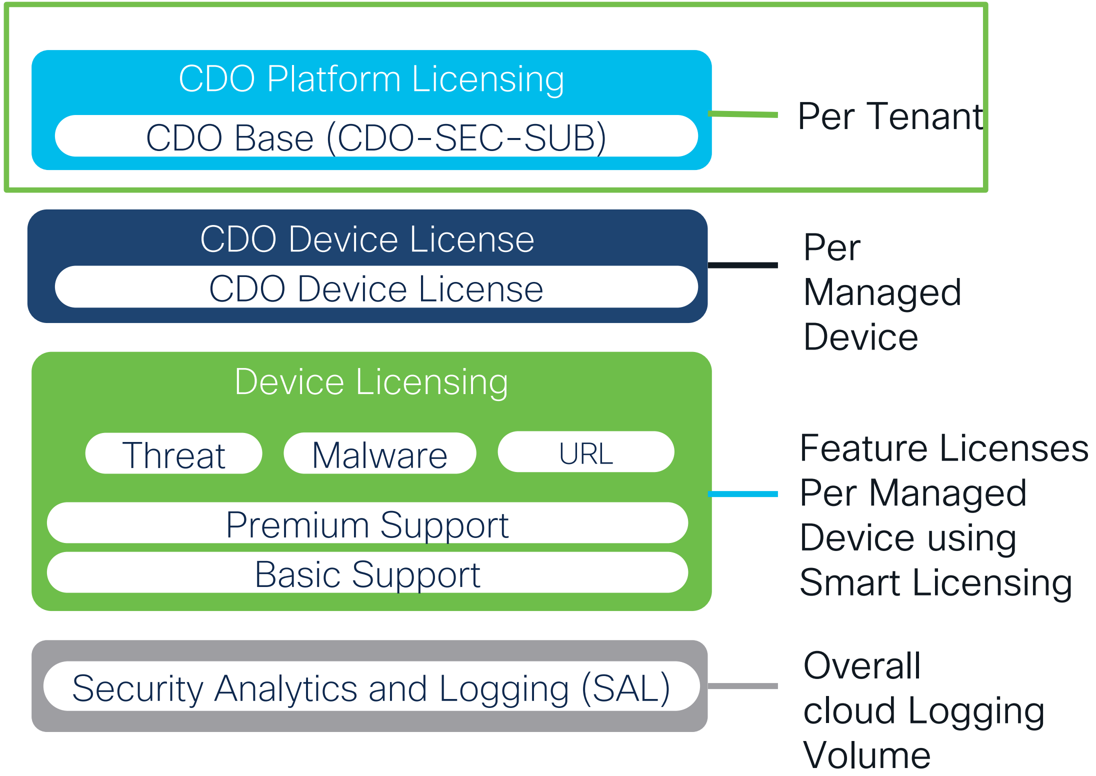
High event scale with long term storage

- External event storage at a massive scale (200K eps), in cloud or on-premise
- Single unified event interface
- ML-powered behavioral and flow analysis available on events
- Based on Secure Cloud/Network Analytics (Stealthwatch) technology



REFERENCE

Licensing & Orderability Example



CDO Platform Licensing

CDO Base (CDO-SEC-SUB)

Per Tenant

CDO Device License

CDO Device License

Per Managed Device

Device Licensing

Threat

Malware

URL

Premium Support

Basic Support

Feature Licenses Per Managed Device using Smart Licensing

Security Analytics and Logging (SAL)

Overall cloud Logging Volume

CDO Ordering Guide

SAL Ordering Guide

Product Overview

What Happens Where?

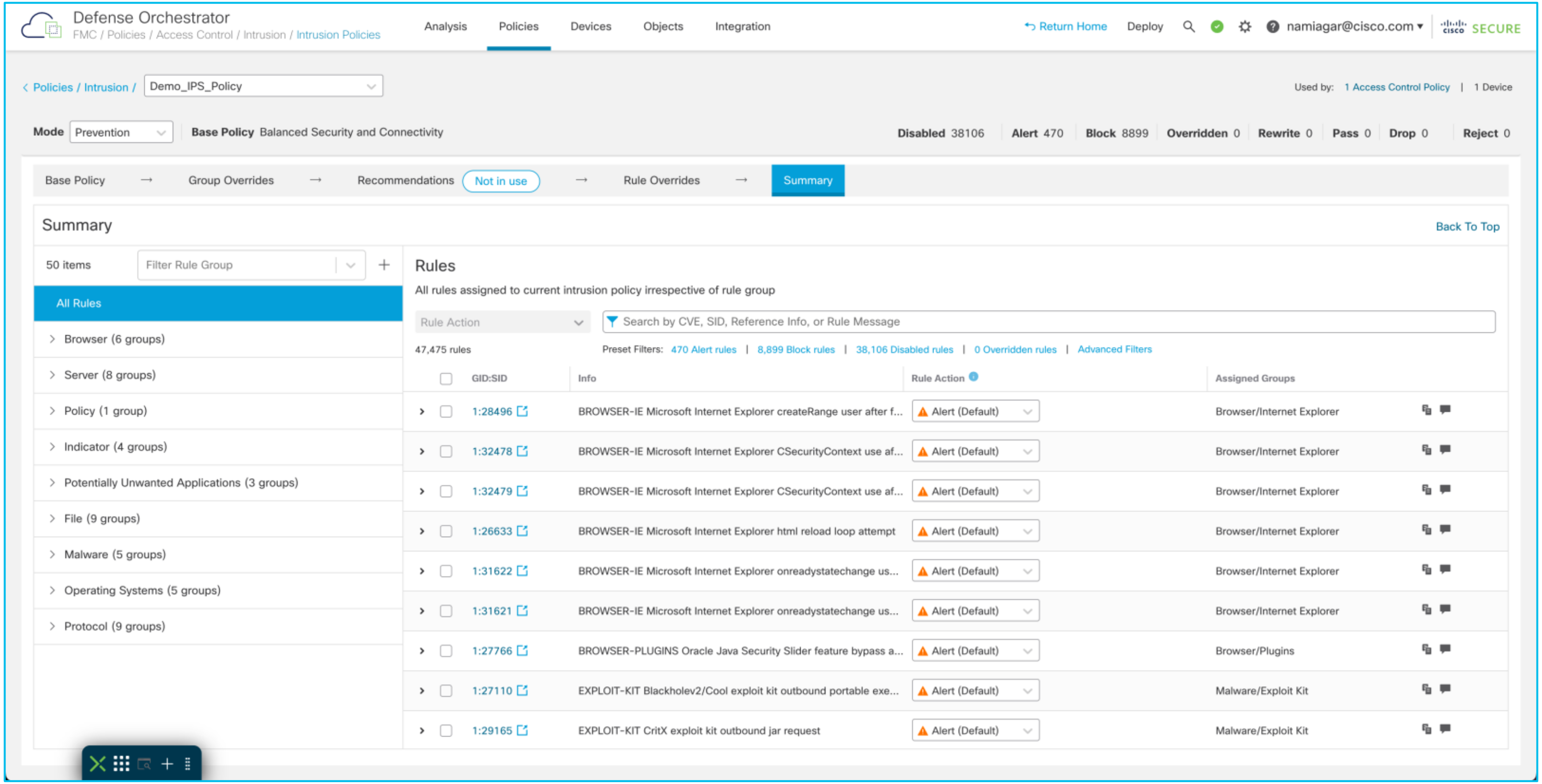
In CDO

- Device Onboarding
- Device Migration
- Event Viewing
- Analytics
- Dynamic Attribute Connector
- User Management
- Network Objects (you can share!)
- Device Inventory

In cdFMC

- Security Policy Management
- NAT and FTD Platform Settings
- VPN Management
- Smart Licensing
- Troubleshooting Tools
- Integrations
- Network Objects
- Device Inventory

Familiar User Experience



Defense Orchestrator
FMC / Policies / Access Control / Intrusion / Intrusion Policies

< Policies / Intrusion / Demo_IPS_Policy

Used by: 1 Access Control Policy | 1 Device

Mode Prevention **Base Policy** Balanced Security and Connectivity

Disabled 38106 **Alert** 470 **Block** 8899 **Overridden** 0 **Rewrite** 0 **Pass** 0 **Drop** 0 **Reject** 0

Base Policy → Group Overrides → Recommendations Not in use → Rule Overrides → Summary

Summary

Back To Top

50 items Filter Rule Group

- All Rules
- Browser (6 groups)
- Server (8 groups)
- Policy (1 group)
- Indicator (4 groups)
- Potentially Unwanted Applications (3 groups)
- File (9 groups)
- Malware (5 groups)
- Operating Systems (5 groups)
- Protocol (9 groups)

Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action Search by CVE, SID, Reference Info, or Rule Message

47,475 rules

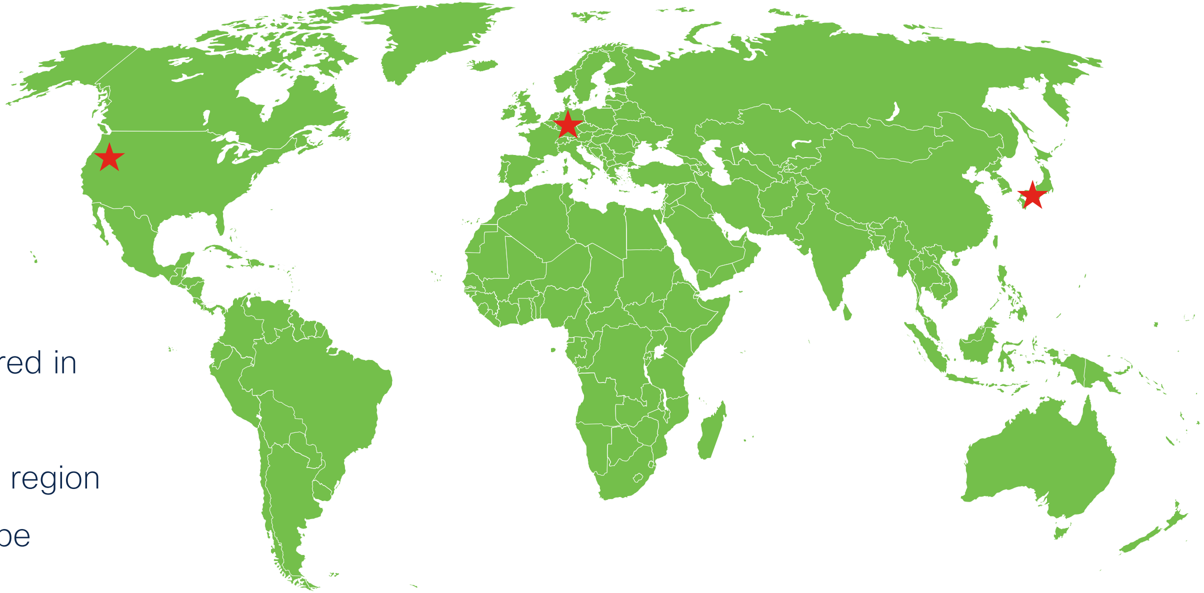
Preset Filters: 470 Alert rules | 8,899 Block rules | 38,106 Disabled rules | 0 Overridden rules | Advanced Filters

GID:SID	Info	Rule Action	Assigned Groups
1:28496	BROWSER-IE Microsoft Internet Explorer createRange user after f...	Alert (Default)	Browser/Internet Explorer
1:32478	BROWSER-IE Microsoft Internet Explorer CSecurityContext use af...	Alert (Default)	Browser/Internet Explorer
1:32479	BROWSER-IE Microsoft Internet Explorer CSecurityContext use af...	Alert (Default)	Browser/Internet Explorer
1:26633	BROWSER-IE Microsoft Internet Explorer html reload loop attempt	Alert (Default)	Browser/Internet Explorer
1:31622	BROWSER-IE Microsoft Internet Explorer onreadystatechange us...	Alert (Default)	Browser/Internet Explorer
1:31621	BROWSER-IE Microsoft Internet Explorer onreadystatechange us...	Alert (Default)	Browser/Internet Explorer
1:27766	BROWSER-PLUGINS Oracle Java Security Slider feature bypass a...	Alert (Default)	Browser/Plugins
1:27110	EXPLOIT-KIT Blackholev2/Cool exploit kit outbound portable exe...	Alert (Default)	Malware/Exploit Kit
1:29165	EXPLOIT-KIT CritX exploit kit outbound jar request	Alert (Default)	Malware/Exploit Kit

Globally available

Where is cdFMC available?

- AWS – US West (Oregon)
- AWS – EU Central (Frankfurt)
- AWS – APJ (Tokyo)



Each Region is Siloed

- No data from one region is copied/stored in another region
- High Availability/Disaster Recovery per region
- Adhere to GDPR requirements in Europe

Demo: Introduction

Key Principles

REFERENCE

New device onboarding supported with 7.0.3 and 7.2 Secure Firewall release

Migrating from on-prem FMC requires on-prem FMC to be upgraded to 7.2 release

Available with CDO Multi-tenancy

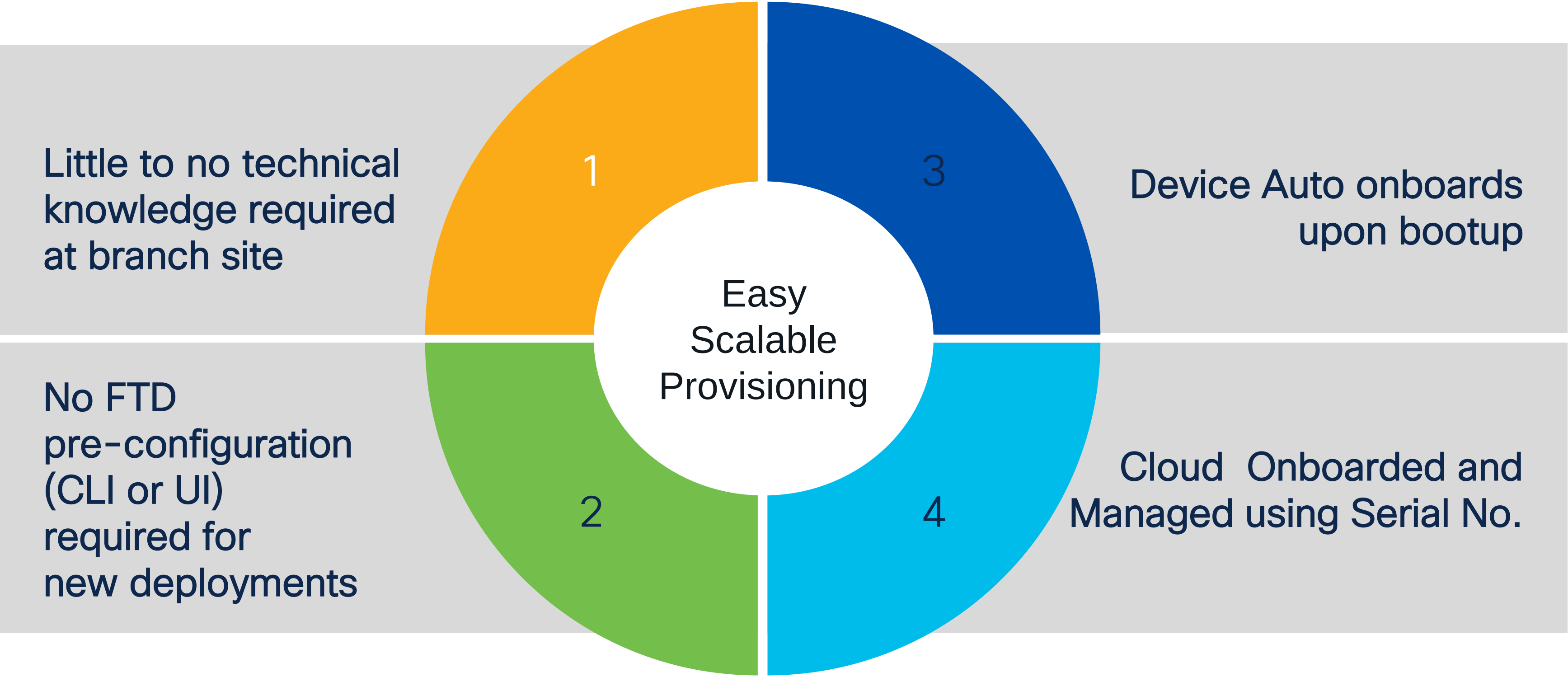
SAML 2.0 compliant idP login with MFA support

Cisco Secure Single Sign-on provided by default

FTD initiated management tunnel for cloud-delivered management and event storage

New Device Onboarding

Cloud Assisted Low Touch Provisioning for Physical Devices



1 Little to no technical knowledge required at branch site

2 No FTD pre-configuration (CLI or UI) required for new deployments

3 Device Auto onboards upon bootup

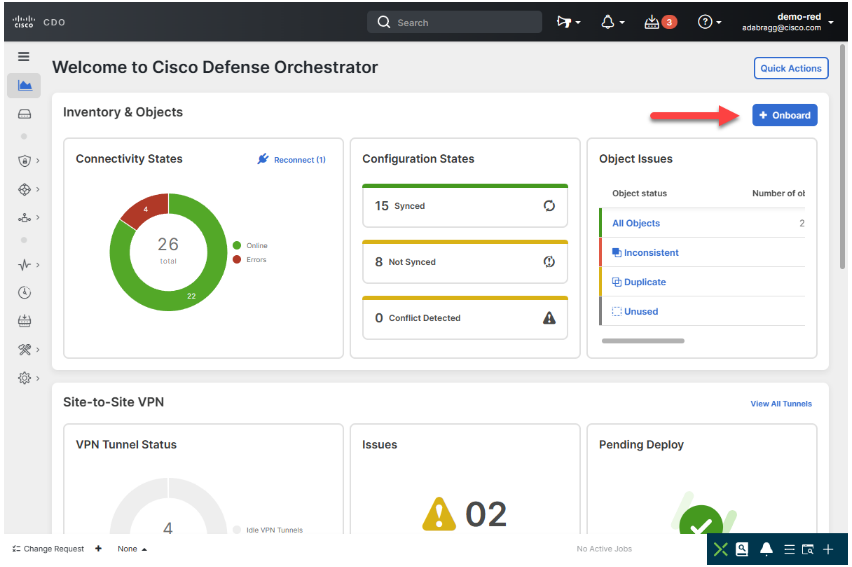
4 Cloud Onboarded and Managed using Serial No.

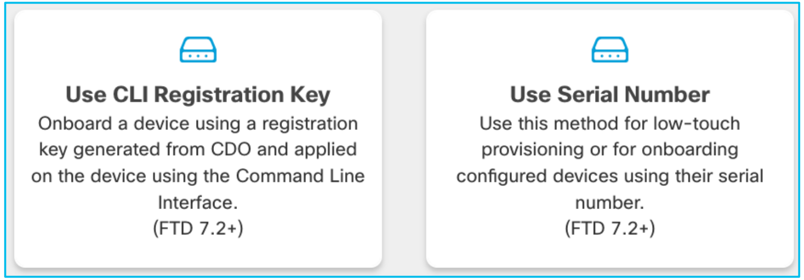
Easy Scalable Provisioning

Simple Onboarding Experience

Registration Key based Onboarding

Low Touch Provisioning using S/N



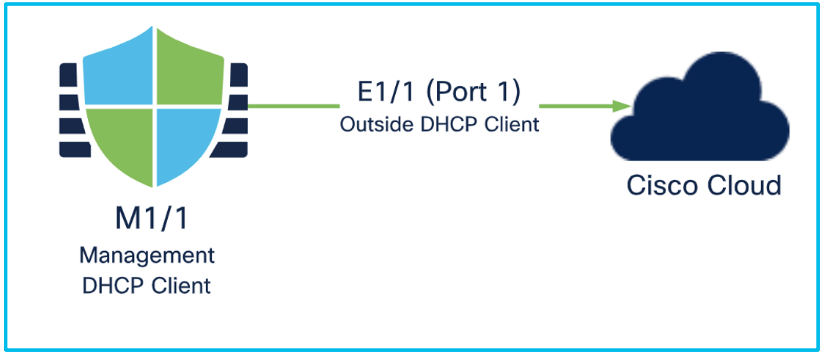


Use CLI Registration Key

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

Use Serial Number

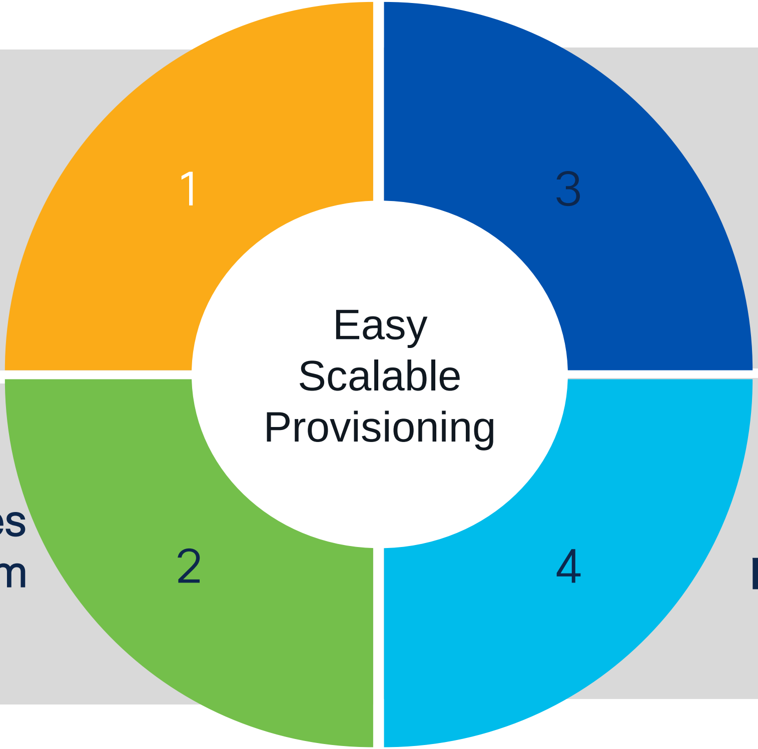
Use this method for low-touch provisioning or for onboarding configured devices using their serial number.
(FTD 7.2+)



Demo: Easy Branch Provisioning with cloud-delivered FMC

CDO Orchestrated Provisioning for Public Cloud Devices

June 2023!!



Easy
Scalable
Provisioning

Little to no technical knowledge required about public cloud provisioning

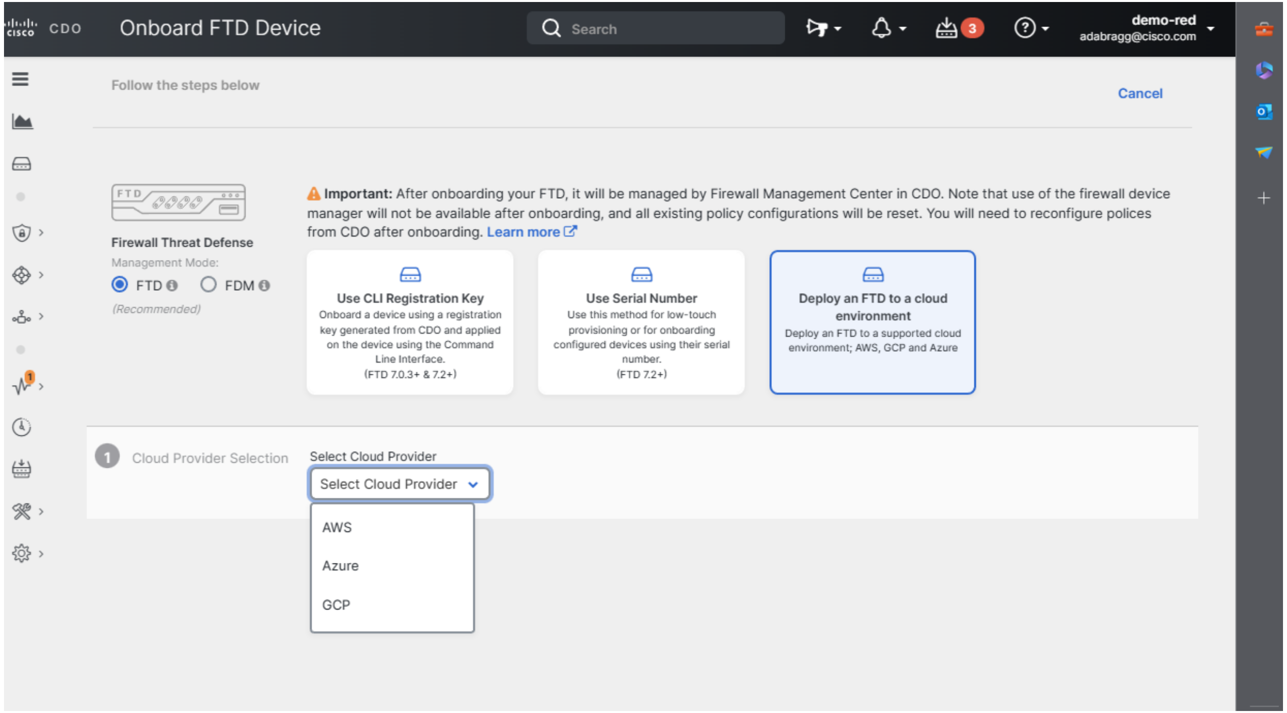
Microsoft Azure
Amazon Web Services
Google Cloud Platform

Deploys directly to your cloud instances inside a CDO created security container

Device Auto onboards upon bootup with pre-configured policies

Simple Public Cloud Onboarding Experience

1. One time user and permissions configuration in the cloud (CDO provides the script/template)
2. CDO provisions the FTD into your cloud
3. CDO auto onboards the FTD
4. CDO auto deploys policy and license



Onboard FTD Device

Follow the steps below

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 polices 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

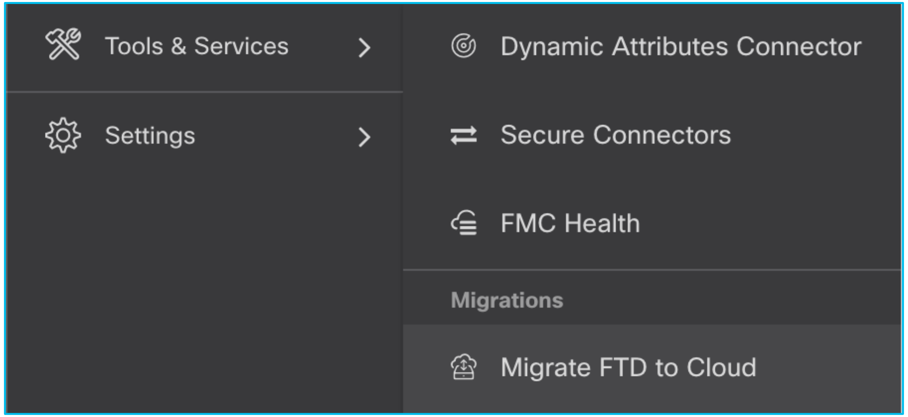
Select Cloud Provider

Select Cloud Provider

- AWS
- Azure
- GCP

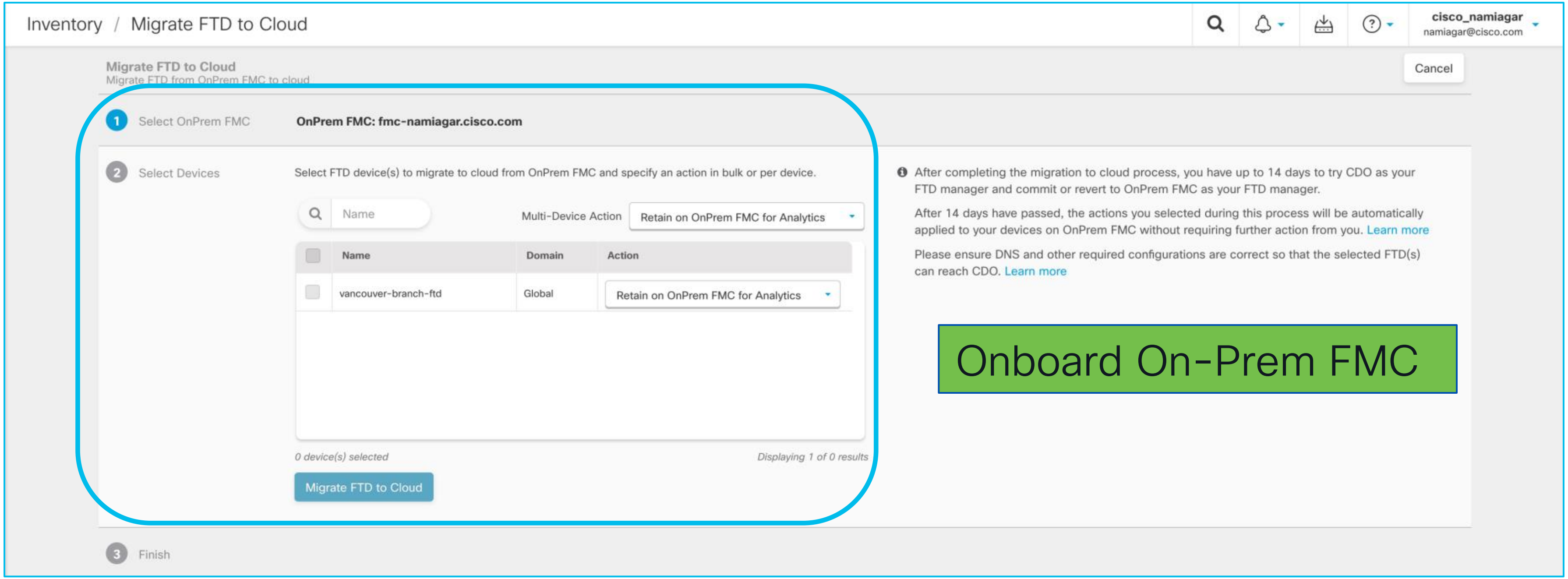
Migrate FTD Management to Cloud

Moving from your FMC to Cloud Delivered FMC is easy!



- CDO Discovers your existing FTD’s
- CDO Guides you through the process
- CDO Error checks to make sure the FTD is suitable to migrate
- Report that you can export to confirm the migration
- Rollback allowed for 14 days if you choose to move back to managing the device on your own FMC
- Fully supported by the Technical Assistance Center (TAC)

Easily migrate to Cloud-delivered management (Contd.)



Inventory / Migrate FTD to Cloud

cisco_namiagar
namiagar@cisco.com

Migrate FTD to Cloud
Migrate FTD from OnPrem FMC to cloud

Cancel

1 Select OnPrem FMC — **OnPrem FMC: fmc-namiagar.cisco.com**

2 Select Devices

Select FTD device(s) to migrate to cloud from OnPrem FMC and specify an action in bulk or per device.

Name

Multi-Device Action: Retain on OnPrem FMC for Analytics

☐	Name	Domain	Action
☐	vancouver-branch-ftd	Global	Retain on OnPrem FMC for Analytics

0 device(s) selected

Displaying 1 of 0 results

Migrate FTD to Cloud

After completing the migration to cloud process, you have up to 14 days to try CDO as your FTD manager and commit or revert to OnPrem FMC as your FTD manager.

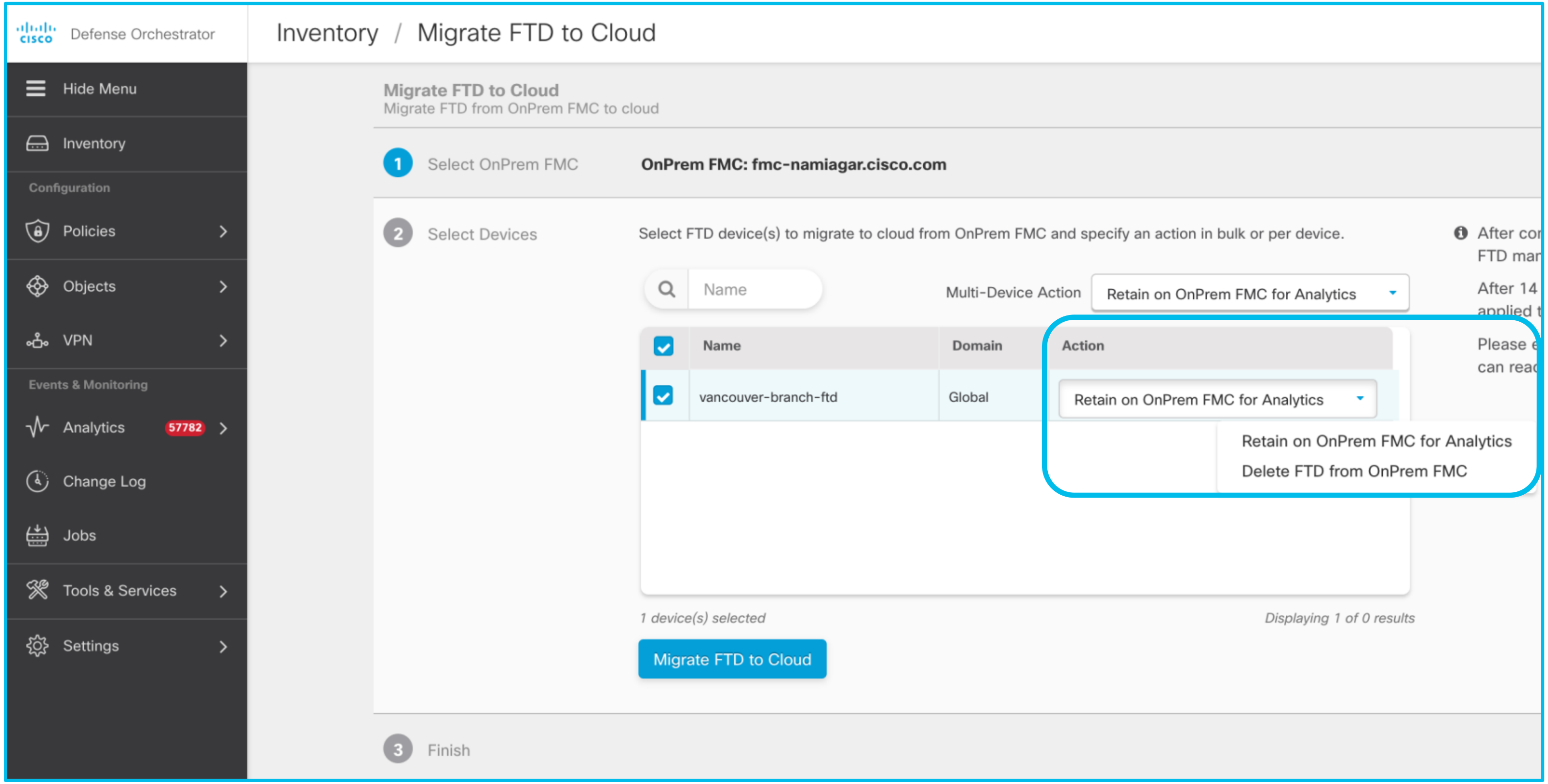
After 14 days have passed, the actions you selected during this process will be automatically applied to your devices on OnPrem FMC without requiring further action from you. Learn more

Please ensure DNS and other required configurations are correct so that the selected FTD(s) can reach CDO. Learn more

3 Finish

Onboard On-Prem FMC

Logging and Analytics – On Prem/Cloud



Inventory / Migrate FTD to Cloud

Migrate FTD to Cloud
Migrate FTD from OnPrem FMC to cloud

1 Select OnPrem FMC — **OnPrem FMC: fmc-namiagar.cisco.com**

2 Select Devices — Select FTD device(s) to migrate to cloud from OnPrem FMC and specify an action in bulk or per device.

After cor
FTD mar
After 14
applied t
Please e
can read

Name

Multi-Device Action: Retain on OnPrem FMC for Analytics

☑	Name	Domain	Action
☑	vancouver-branch-ftd	Global	Retain on OnPrem FMC for Analytics

- Retain on OnPrem FMC for Analytics
- Delete FTD from OnPrem FMC

1 device(s) selected

Displaying 1 of 0 results

Migrate FTD to Cloud

3 Finish

Demo: Migrate Firewall Management to cloud-delivered FMC

Migrate from ASA, FDM, & 3rd party Firewalls

REFERENCE

Firewall Migration Tool – Hosted in CDO!!

Migration to cloud-Delivered Firewall Management Center

Configuration Optimization

- Identify redundant and shadowed rules and provide users with the following rule options: remove, migrate disabled or migrate fully
- Comprehensive reporting on configuration optimization for access rules and objects
- Streamlining object optimizations: removing un-referenced objects, re-using existing objects and resolving inconsistent objects

FDM to FMC migrations

- Consolidation
- Device Refresh

ASA to FTD migration enhancements

- **Remote Access VPN:** now GA, AnyConnect custom attributes and VPN load balancing
- **Routing:** Equal Cost Multi-Path (ECMP), Policy Based Routing (PBR)
- **Release/Device Validation:** Validated support for release 7.3 and FPR3105
- **Hardening**

internal

FMT in Numbers

47K+
Total Downloads

9K & 5k
Direct Customers
Partners

93%+
Device Migration Success Rate

45
Migration Tool Net Promoter Score

Firewall Migration Tool – More Awesomeness

http://cisco.com/go/fmt

Key Features

- RA VPN
- S2S VPN*
- Multi-Context to Multi-Instance*
- Enablement of L7 Firewalling capabilities
- Selective migration of ACL, NAT, object reuse
- Pre- & post-migration reports

Core FW capabilities

- Network, Service & FQDN objects and groups
- Access rules, CSM object grouping
- NAT, Static routes, IPv6, wildcard mask*
- Physical interface, port channels
- Bridge groups (transparent only)

Supported Source Configuration

Migration to FMC managed FTD

- ASA | Check Point | PAN | Fortinet | FP services

Migration to CDO/FDM managed FTD

- ASA

Value-add during migration

- Configuration optimization
  - ID & remove shadow/redundant ACLs
  - Selective migration of ACL, NAT, etc.
  - Re-use objects, identify ACL count
- Enablement of L7 Firewalling capabilities
- Pre- & post-migration reports

Supported FW capabilities

- Network, Service & FQDN objects and groups
- Access rules, CSM object grouping, NAT
- Static routes, BGP, EIGRP, ECMP, PBR
- IPv6, wildcard mask*
- Physical interface, port channels
- S2S VPN*, RA VPN*

Supported Sources & Targets

Migration to on-prem / virtual FMC

- ASA | Check Point | Fortinet | PAN | FDM

Migration to cloud-delivered FMC

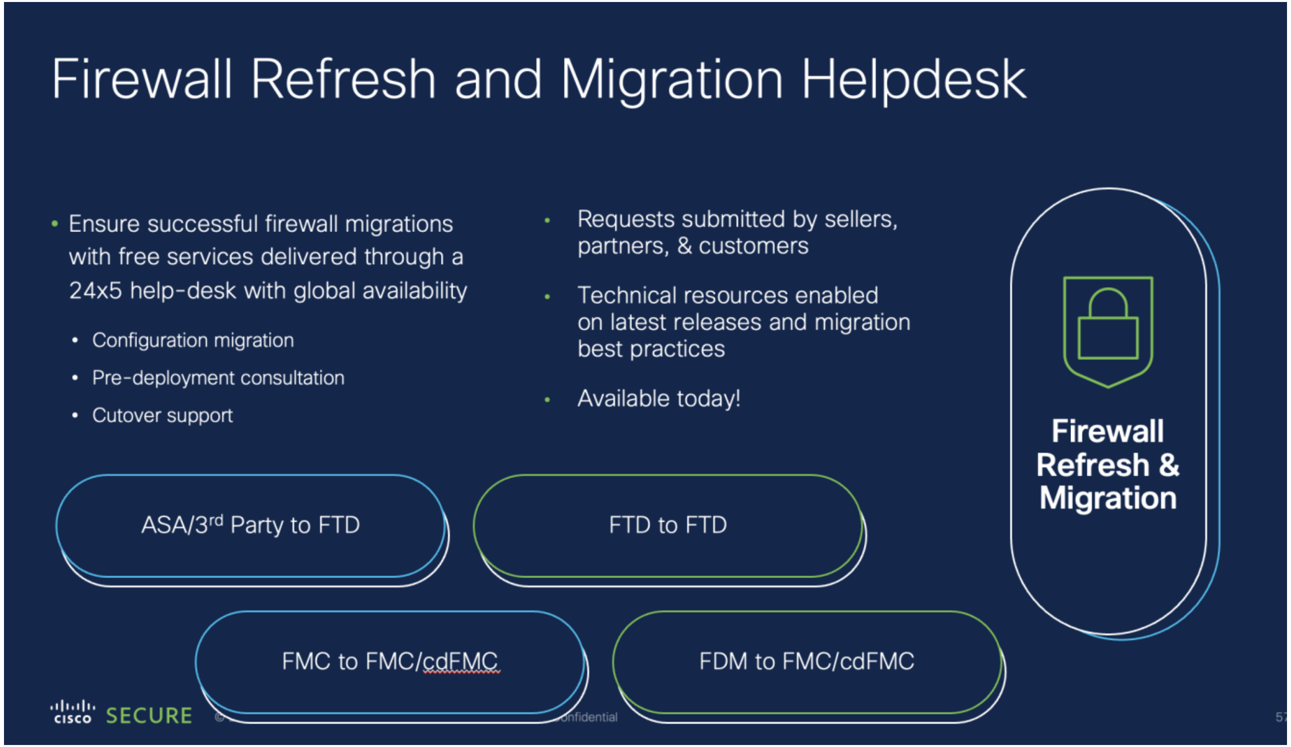
- ASA | Check Point | Fortinet | PAN | FDM

*supported from ASA/FDM only

internal

REFERENCE

Migration Assistance Services



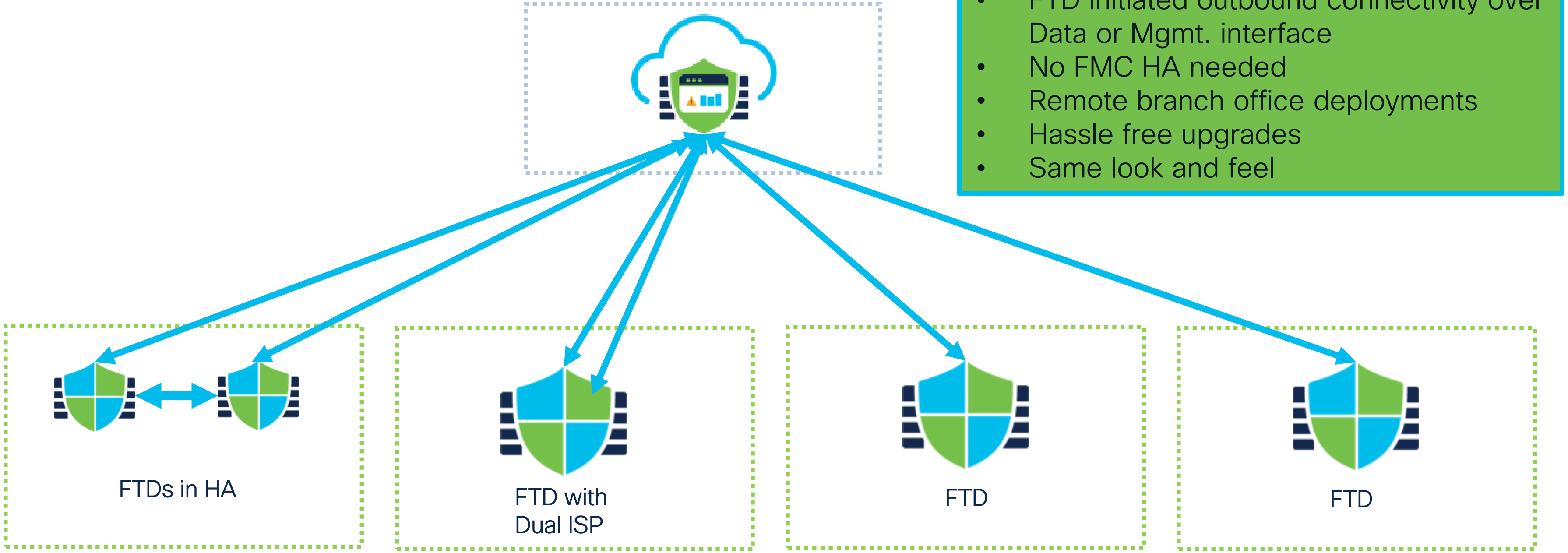
Firewall Refresh and Migration Helpdesk

- Ensure successful firewall migrations with free services delivered through a 24x5 help-desk with global availability
  - Configuration migration
  - Pre-deployment consultation
  - Cutover support

- Requests submitted by sellers, partners, & customers
- Technical resources enabled on latest releases and migration best practices
- Available today!

Branch Management

Managing FTDs in Multiple locations



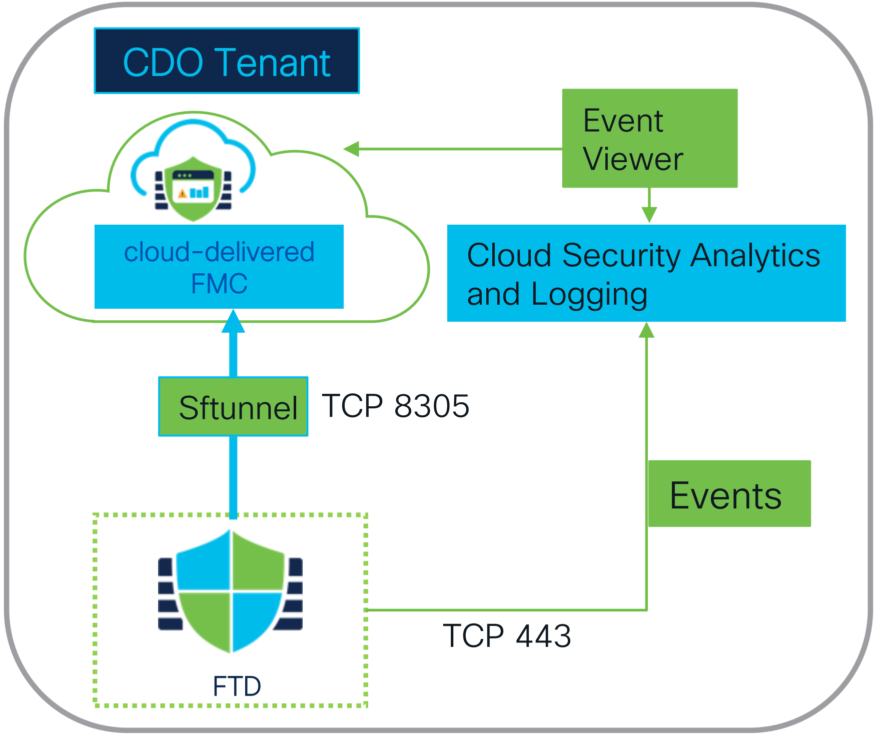
- FTD initiated outbound connectivity over Data or Mgmt. interface
- No FMC HA needed
- Remote branch office deployments
- Hassle free upgrades
- Same look and feel

Great for firewalls having DHCP assigned IPs and Branch deployments

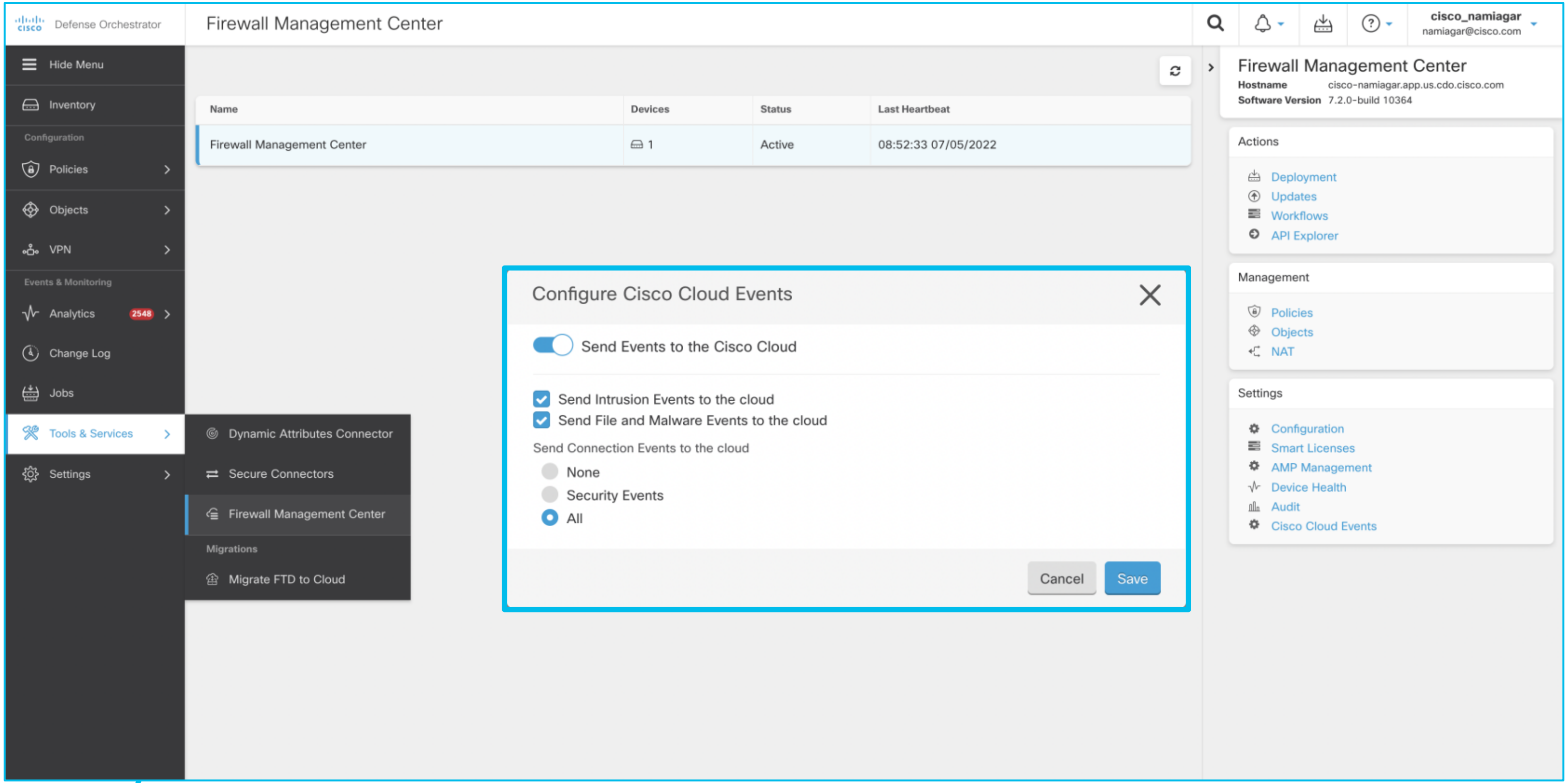
Events and Analytics in the Cloud

Events and Analytics in the cloud

- FTD sends events to the cloud
  - Needs outbound TLS connectivity
- FTD Dashboard with summary data and cross launches into the event viewer with filters
- Unified CDO Event viewer
  - all FTD events and ASA logs
  - Requires SAL subscription (more info in ordering guide)



How to enable Cloud Events



Name	Devices	Status	Last Heartbeat
Firewall Management Center	1	Active	08:52:33 07/05/2022

Firewall Management Center
Hostname cisco-namiagar.app.us.cdo.cisco.com
Software Version 7.2.0-build 10364

Configure Cisco Cloud Events

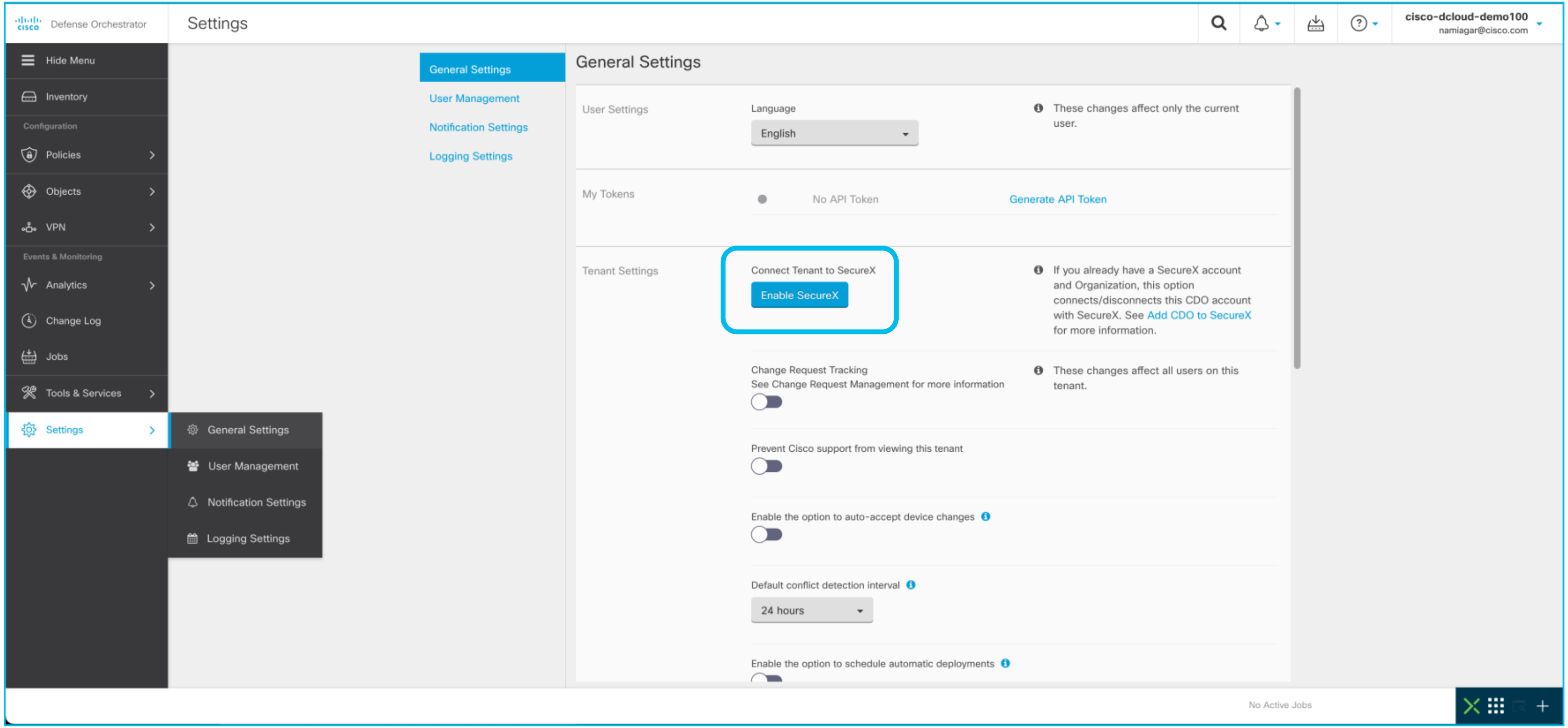
Send Events to the Cisco Cloud (on)

☑ Send Intrusion Events to the cloud
☑ Send File and Malware Events to the cloud

Send Connection Events to the cloud
○ None
○ Security Events
● All

Cancel Save

How to enable SecureX



General Settings

User Settings

Language: English

These changes affect only the current user.

My Tokens

No API Token

Generate API Token

Tenant Settings

Connect Tenant to SecureX

Enable SecureX

If you already have a SecureX account and Organization, this option connects/disconnects this CDO account with SecureX. See Add CDO to SecureX for more information.

Change Request Tracking
See Change Request Management for more information

These changes affect all users on this tenant.

Prevent Cisco support from viewing this tenant

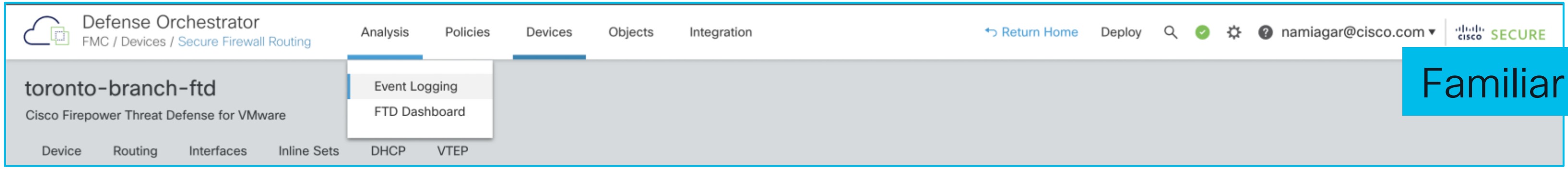
Enable the option to auto-accept device changes

Default conflict detection interval: 24 hours

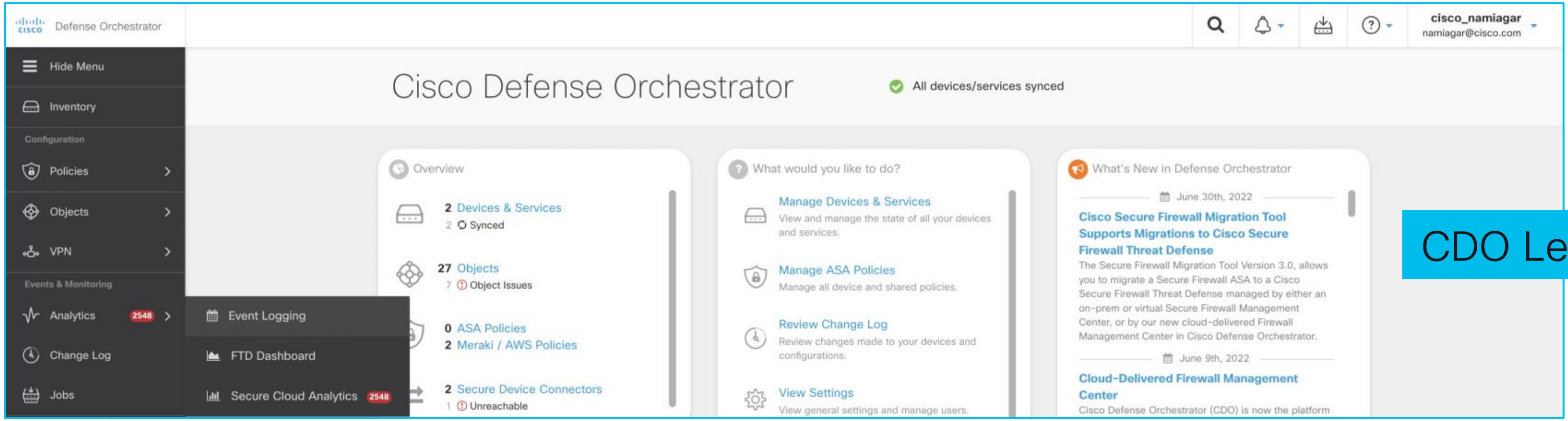
Enable the option to schedule automatic deployments

Event and Analytics in the cloud – How do I launch

Flexible launch options depending on user context



Familiar FMC UI



View and manage the state of all your devices and services.

Manage all device and shared policies.

Review changes made to your devices and configurations.

View general settings and manage users.

Cisco Secure Firewall Migration Tool Supports Migrations to Cisco Secure Firewall Threat Defense

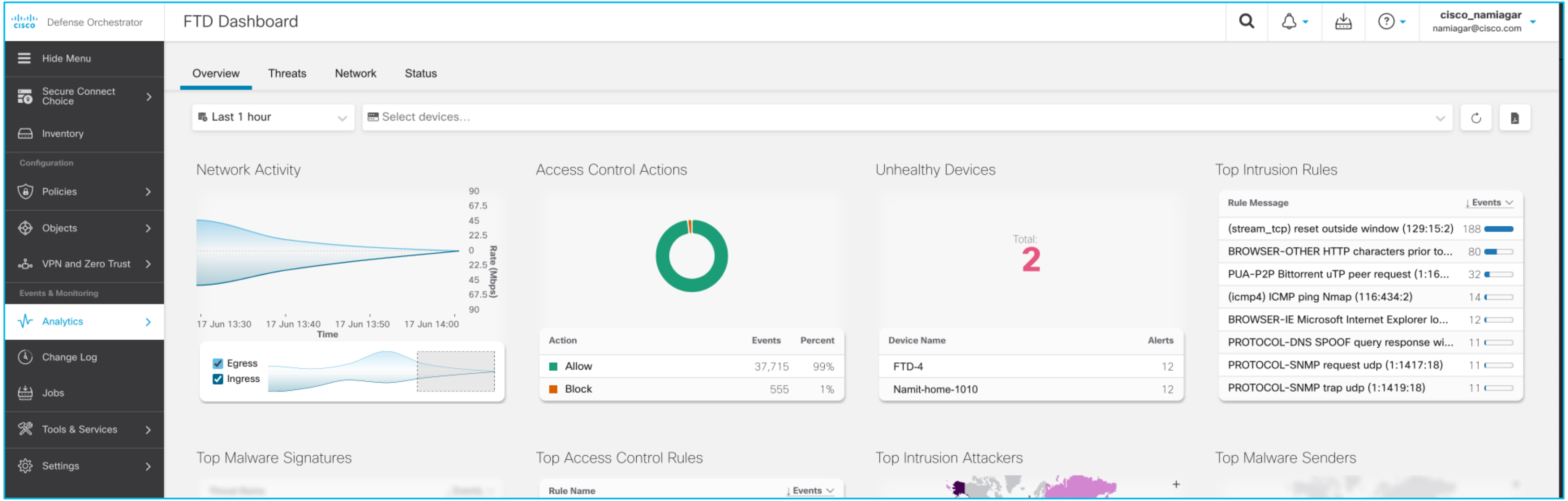
The Secure Firewall Migration Tool Version 3.0, allows you to migrate a Secure Firewall ASA to a Cisco Secure Firewall Threat Defense managed by either an on-prem or virtual Secure Firewall Management Center, or by our new cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.

Cloud-Delivered Firewall Management Center

Cisco Defense Orchestrator (CDO) is now the platform

CDO Left ribbon

New cloud-delivered FTD Dashboard



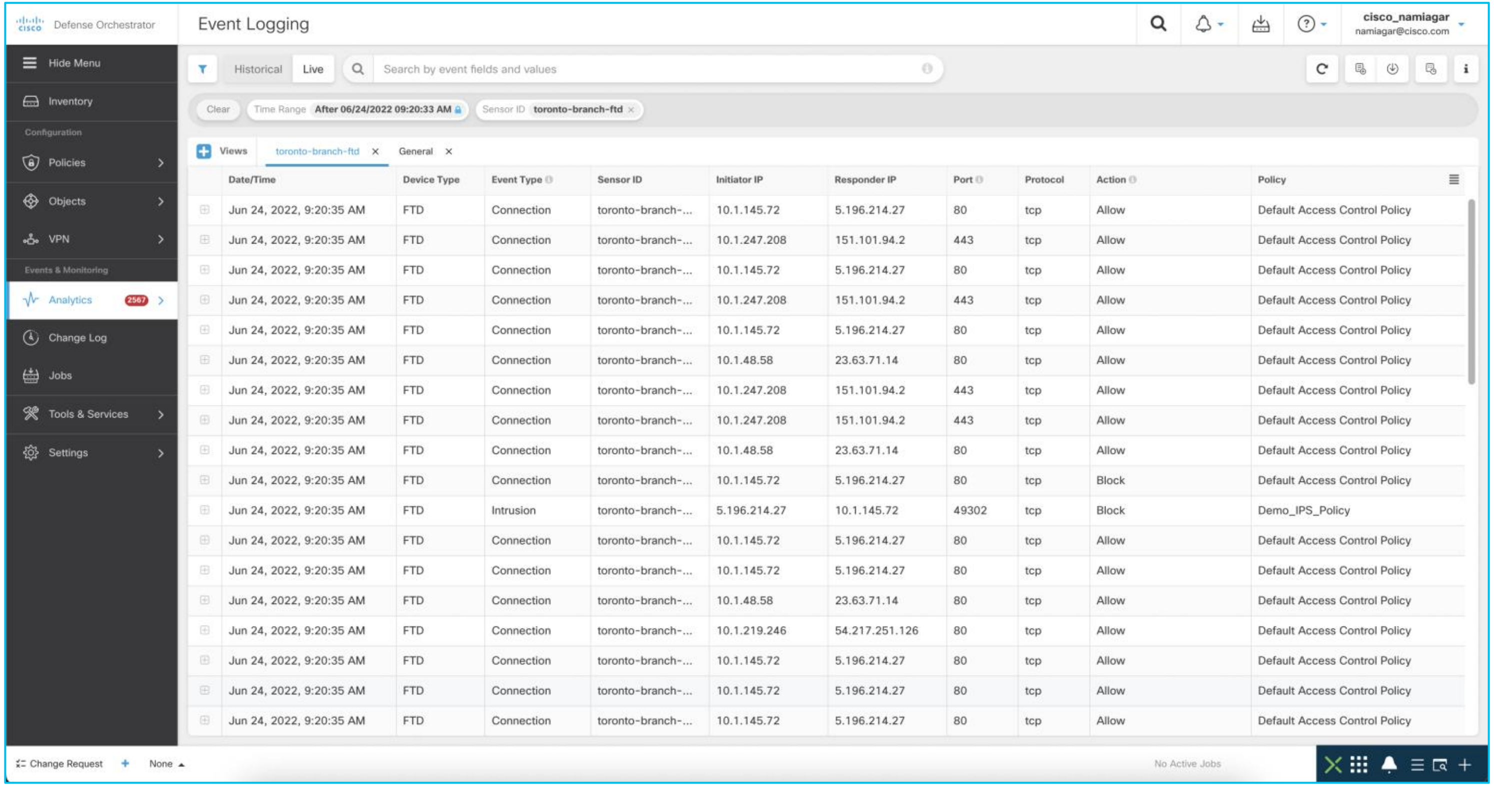
Action	Events	Percent
🟩 Allow	37,715	99%
🟧 Block	555	1%

Device Name	Alerts
FTD-4	12
Namit-home-1010	12

Rule Message	↓Events
(stream_tcp) reset outside window (129:15:2)	188
BROWSER-OTHER HTTP characters prior to...	80
PUA-P2P Bittorrent uTP peer request (1:16...	32
(icmp4) ICMP ping Nmap (116:434:2)	14
BROWSER-IE Microsoft Internet Explorer lo...	12
PROTOCOL-DNS SPOOF query response wi...	11
PROTOCOL-SNMP request udp (1:1417:18)	11
PROTOCOL-SNMP trap udp (1:1419:18)	11

Rule Name	↓Events

CDO Event Viewer



Event Logging

Time Range After 06/24/2022 09:20:33 AM

Sensor ID toronto-branch-ftd

toronto-branch-ftd

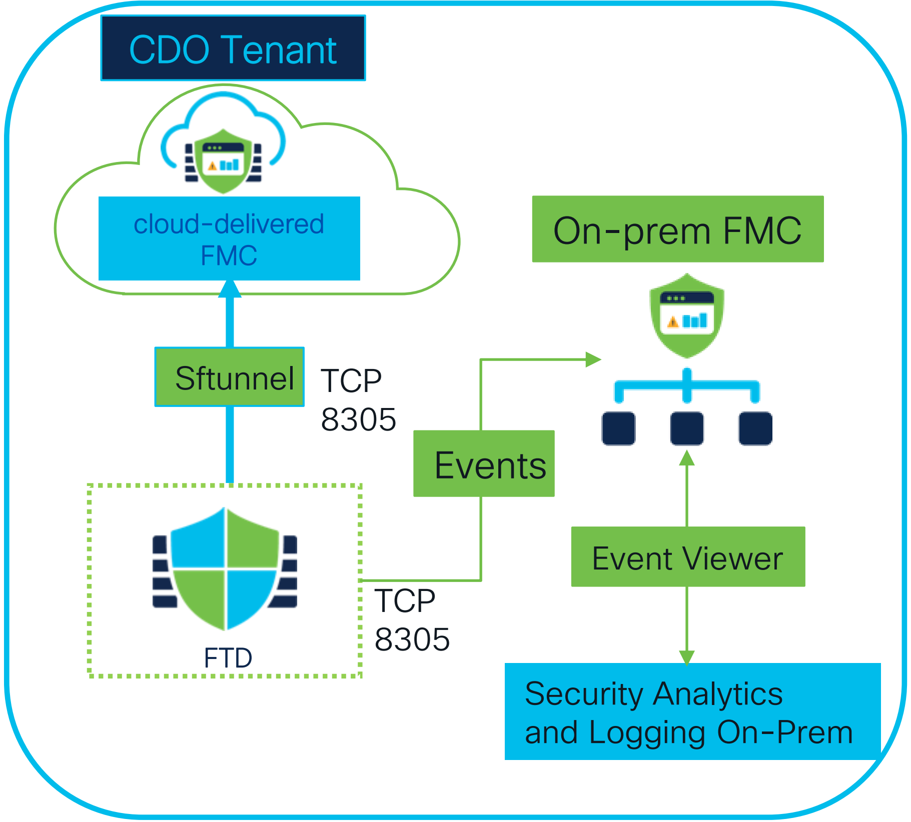
Date/Time	Device Type	Event Type	Sensor ID	Initiator IP	Responder IP	Port	Protocol	Action	Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.145.72	5.196.214.27	80	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.247.208	151.101.94.2	443	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.145.72	5.196.214.27	80	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.247.208	151.101.94.2	443	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.145.72	5.196.214.27	80	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.48.58	23.63.71.14	80	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.247.208	151.101.94.2	443	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.247.208	151.101.94.2	443	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.48.58	23.63.71.14	80	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.145.72	5.196.214.27	80	tcp	Block	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Intrusion	toronto-branch-...	5.196.214.27	10.1.145.72	49302	tcp	Block	Demo_IPS_Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.145.72	5.196.214.27	80	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.145.72	5.196.214.27	80	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.48.58	23.63.71.14	80	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.219.246	54.217.251.126	80	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.145.72	5.196.214.27	80	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.145.72	5.196.214.27	80	tcp	Allow	Default Access Control Policy
Jun 24, 2022, 9:20:35 AM	FTD	Connection	toronto-branch-...	10.1.145.72	5.196.214.27	80	tcp	Allow	Default Access Control Policy

Demo: Cloud Eventing and Analytics

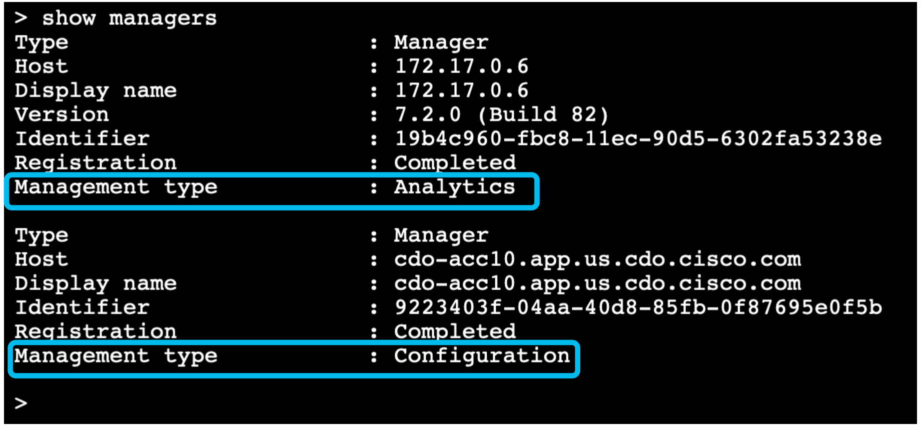
Events and Analytics On-prem

Events and Analytics on-prem

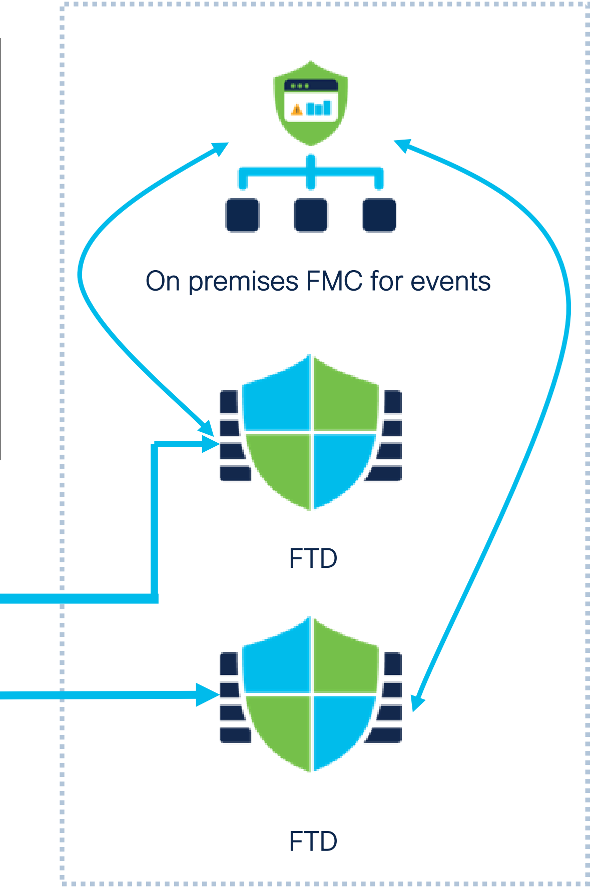
- FTD sends events to the on-prem FMC
  - Needs outbound TLS connectivity
- Familiar dashboard in the On-prem FMC
- Events are viewed in the on-prem FMC Event viewer
- Additional Log retention available through the SAL on-prem integration

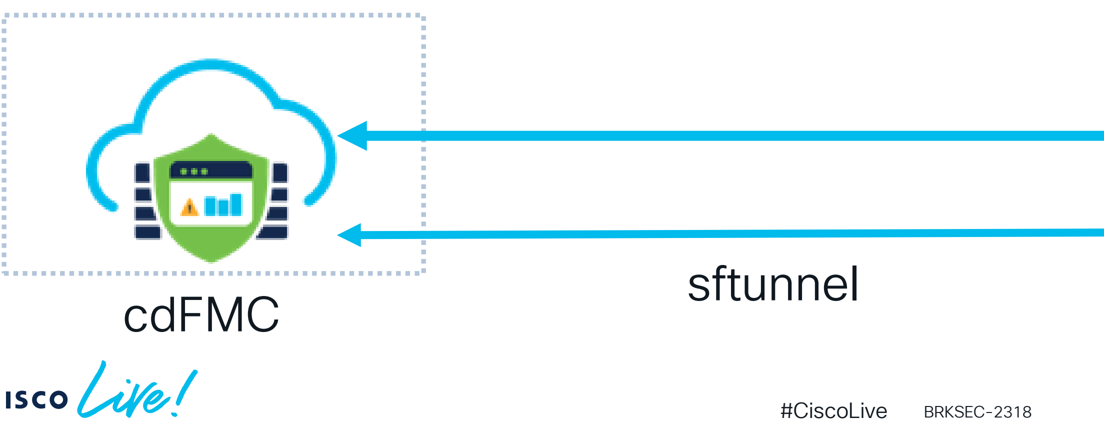


Managing FTDs with on-prem FMC for events

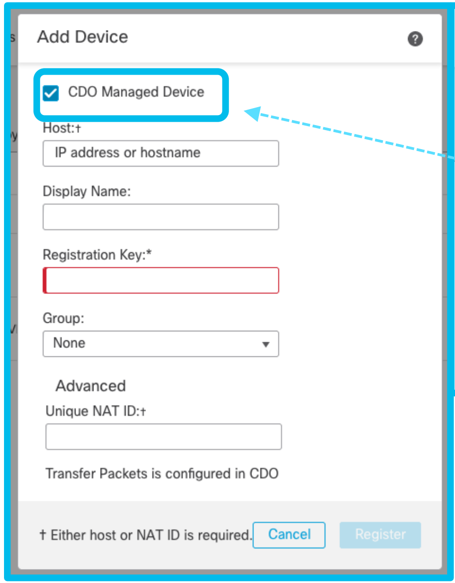


```
> show managers
Type                      : Manager
Host                      : 172.17.0.6
Display name              : 172.17.0.6
Version                   : 7.2.0 (Build 82)
Identifier                : 19b4c960-fbc8-11ec-90d5-6302fa53238e
Registration              : Completed
Management type           : Analytics

Type                      : Manager
Host                      : cdo-acc10.app.us.cdo.cisco.com
Display name              : cdo-acc10.app.us.cdo.cisco.com
Identifier                : 9223403f-04aa-40d8-85fb-0f87695e0f5b
Registration              : Completed
Management type           : Configuration

>
```





Managing FTDs with on-prem FMC for events



Add Device

☑ CDO Managed Device

Host:†

IP address or hostname

Display Name:

Registration Key:*

Group:

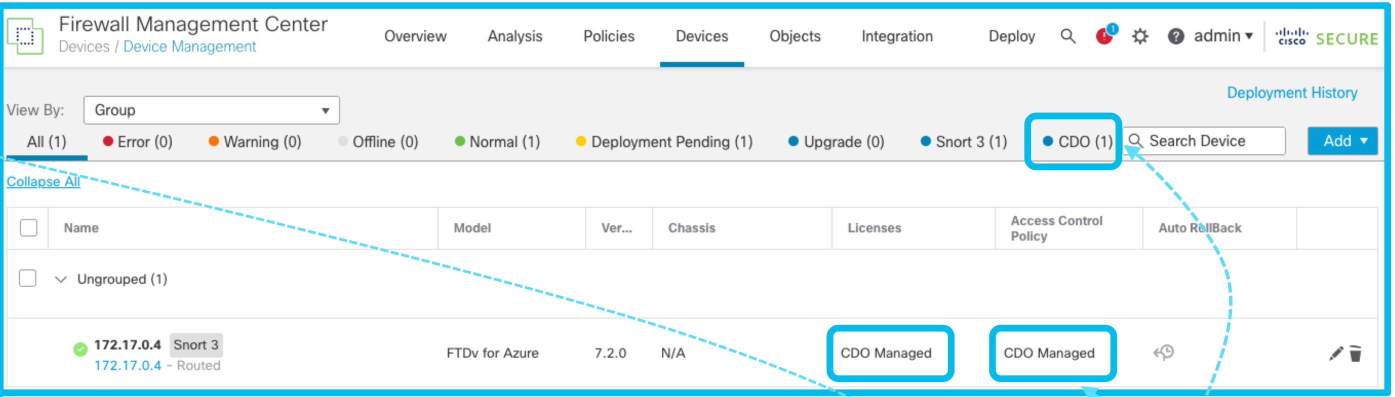
None ▾

Advanced

Unique NAT ID:†

Transfer Packets is configured in CDO

† Either host or NAT ID is required. Cancel Register



Firewall Management Center

Devices / Device Management

Overview Analysis Policies Devices Objects Integration Deploy admin ▾ SECURE

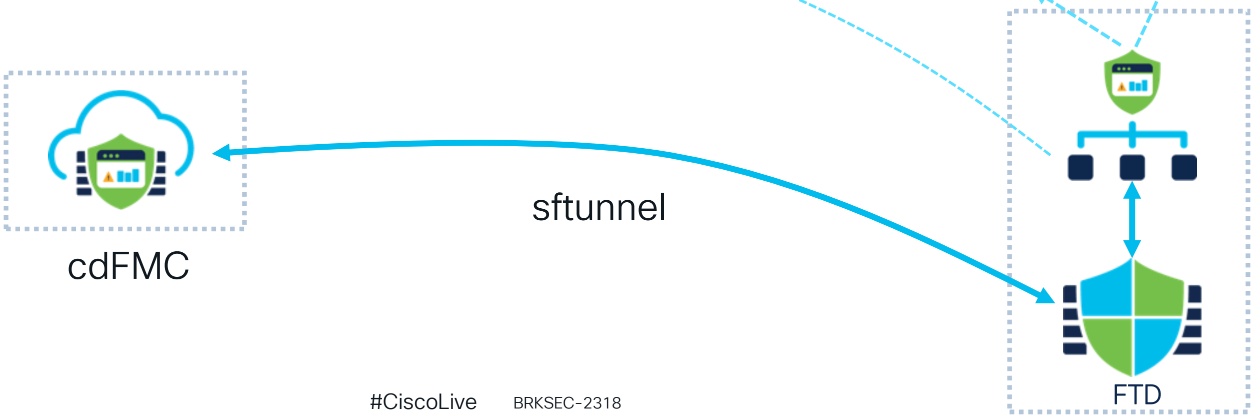
Deployment History

View By: Group ▾

All (1) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (1) ● Deployment Pending (1) ● Upgrade (0) ● Snort 3 (1) ● CDO (1) Search Device Add ▾

Collapse All

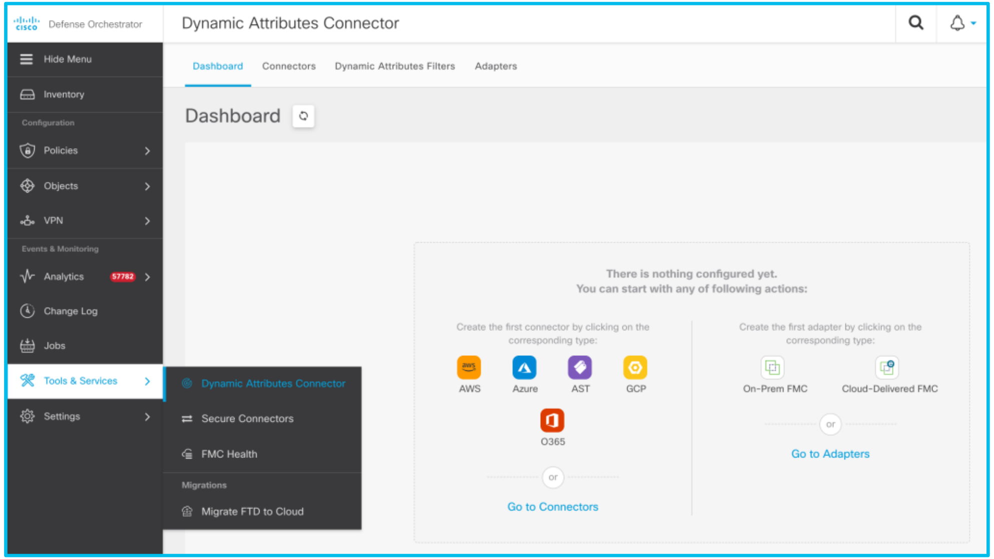
□	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack
□	⌄ Ungrouped (1)						
	172.17.0.4 Snort 3 172.17.0.4 - Routed	FTDv for Azure	7.2.0	N/A	CDO Managed	CDO Managed	



Identity

Cloud Delivered Dynamic Attributes Connector

- Update policy in real time using attributes from dynamically changing cloud environments
- Monitoring Dashboard
- Multi-tenant support
- Support for On-Prem and Cloud Delivered FMC

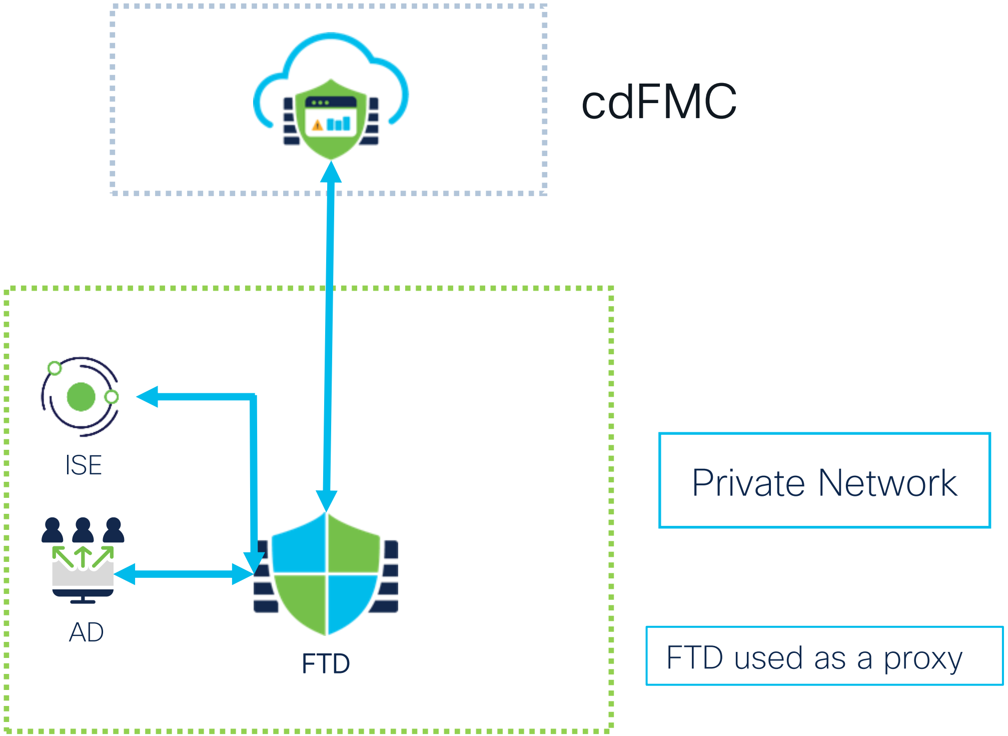


There is nothing configured yet.
You can start with any of following actions:

Create the first connector by clicking on the corresponding type:

Create the first adapter by clicking on the corresponding type:

Connectivity Flow for AD/ISE



Private Network

FTD used as a proxy

Demo: Identity

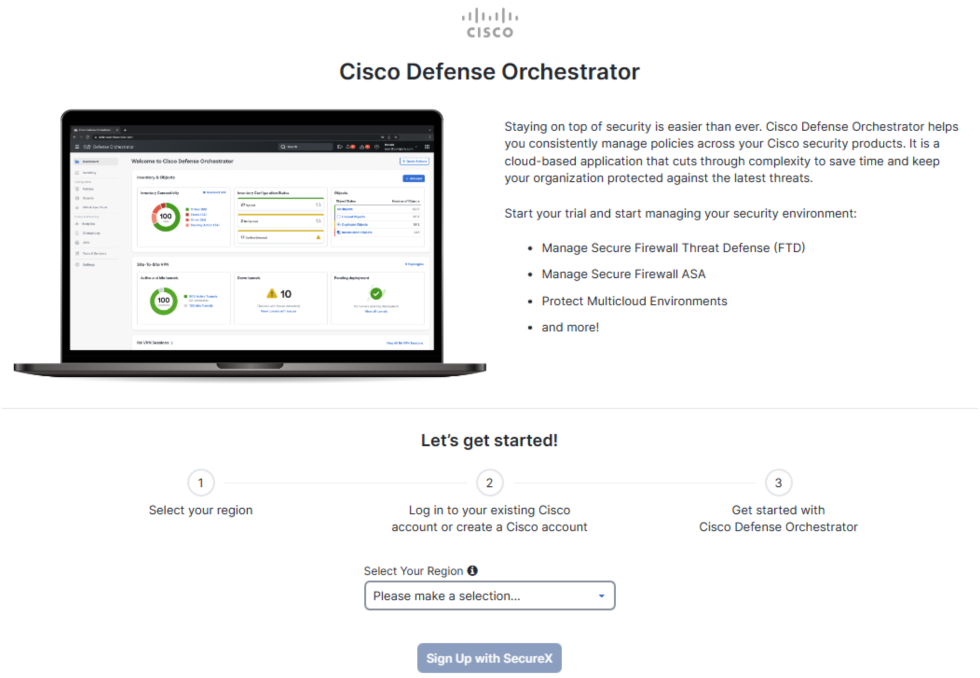
What next ?

Remember

- FMC now available as a cloud-delivered option
- The same look and feel
- Easy Migration from privately managed FMCs and FDM
- Flexible Management Options
- Faster Feature cadence in cloud-delivered offering
- Consolidate Firewall Management
- Multi-cloud deployments

Get up and running with CDO and cdFMC

https://getcdo.com



Cisco Defense Orchestrator

Staying on top of security is easier than ever. Cisco Defense Orchestrator helps you consistently manage policies across your Cisco security products. It is a cloud-based application that cuts through complexity to save time and keep your organization protected against the latest threats.

Start your trial and start managing your security environment:

- Manage Secure Firewall Threat Defense (FTD)
- Manage Secure Firewall ASA
- Protect Multicloud Environments
- and more!

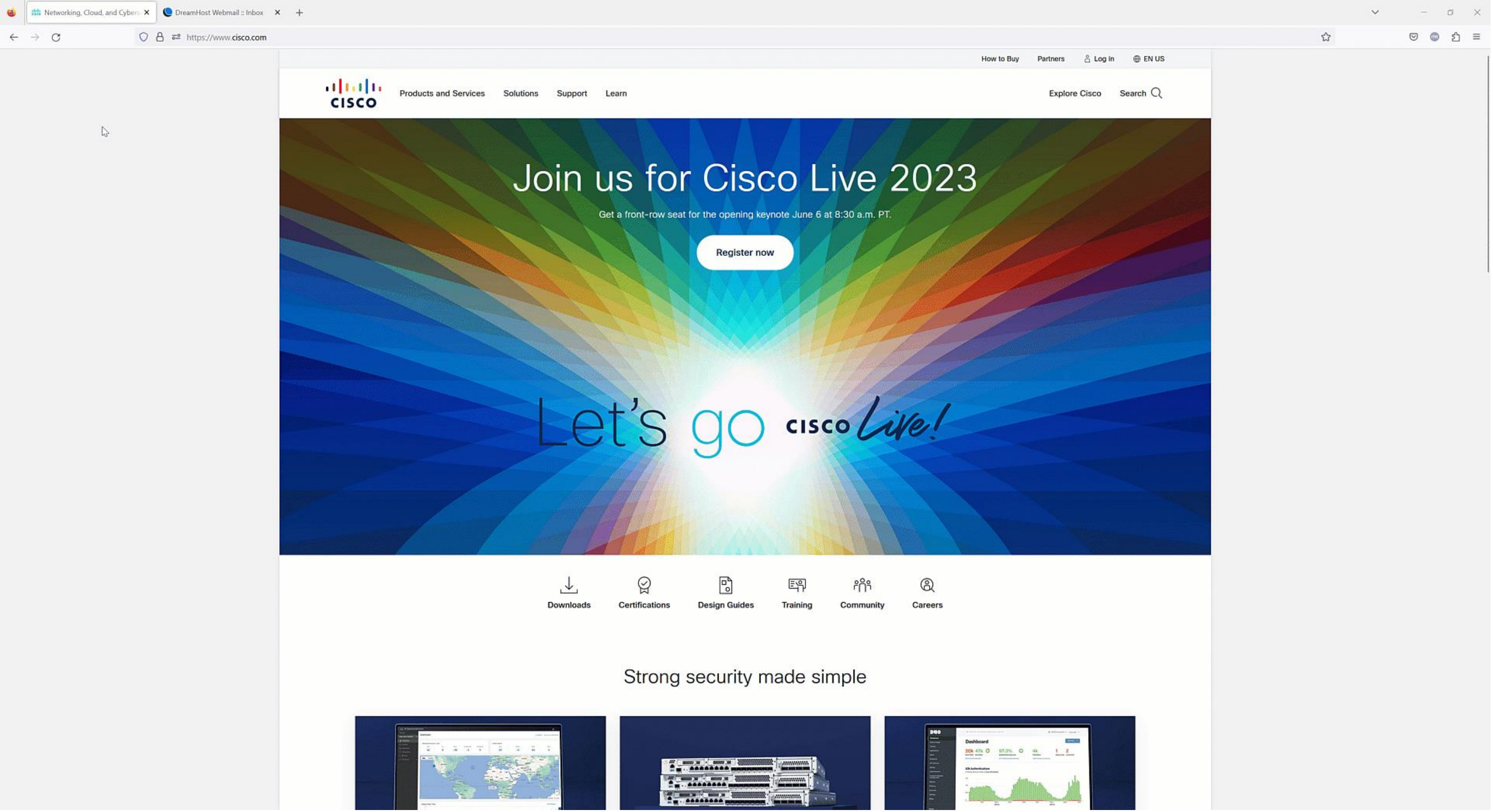
Let's get started!

1. Select your region
2. Log in to your existing Cisco account or create a Cisco account
3. Get started with Cisco Defense Orchestrator

Select Your Region

Please make a selection...

Workflow Demo for a Greenfield Customer



Join us for Cisco Live 2023

Get a front-row seat for the opening keynote June 6 at 8:30 a.m. PT.

Strong security made simple

CISCO SECURE

UX Research

Participate in UX research after Cisco Live 2023 Las Vegas!

Sign up today: cs.co/SecurePanel

cisco Live!

Learn about a new CDO integration called Cisco Multicloud Defense!

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

Thursday, Jun 89:30 AM - 10:30 AM PDT
Level 3, Palm D

Resources – Docs

REFERENCE

- Documentation
  - https://docs.defenseorchestrator.com/
  - https://www.cisco.com/c/en/us/td/docs/security/cdo/cloud-delivered-firewall-management-center-in-cdo/managing-firewall-threat-defense-services-with-cisco-defense-orchestrator.html
- Track cloud-delivered FMC features
  - https://www.cisco.com/c/en/us/td/docs/security/cdo/whats-new-for-cisco-defense-orchestrator/feature-highlights-of-2023.html
- Service Level Objective doc
  - https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/cisco-defense-orchestrator.pdf
- Datasheet
  - https://www.cisco.com/c/en/us/products/collateral/security/defense-orchestrator/datasheet-c78-736847.html
- Instant Demo
  - https://getCDO.com << End Customers
  - https://tryCDO.com << Partners/Service Provider

REFERENCE

Resources – Videos

- Cisco Secure Firewall Channel
  - This channel is managed by the Cisco Secure Technical Marketing Engineering Team. It is awesome content.
  - https://www.youtube.com/@CiscoNetSec

- Full Send Fridays
  - This channel is managed by Nic Conroy, Cisco Technical Solutions Architect. Nic features weekly quick hits of features of the Secure Firewall (including management!)
  - https://www.youtube.com/@fullsendNic

Cloud Delivered FMC (cdFMC) Cheat Sheet

REFERENCE

- cdFMC Supports Cisco Secure Firewall (FTD) that are running version 7.0.3+ and 7.2+ (7.1 is not supported)
- In order to move an FTD being managed by your FMC to cdFMC, ***your FMC*** needs to be running version 7.2+
- The FTD that is being managed by CDO needs to be able to reach the Internet outbound on TCP 8305. *Not allowing this communication is the number one reason that FTD onboarding failures happen*. Start your troubleshooting with verifying this traffic.
- TCP 8305 is used by the SFTunnel, which is the protocol by which the FTD and FMC communicate with one another
- FTD's can be managed via their Outside Interface
- Ping system x.x.x.x instead of ping x.x.x.x
- Events from the FTD can be sent directly to the Cisco Cloud (this is called SAL – Security Analytics and Logging. These events are sent via TCP 443
- Events from the FTD can also be sent to an FMC that is in your control (on Prem FMC).
- Events can still also be sent to some other destination as well via syslog. You have options!
- Active Directory/Realms/ISE Communications all flow throw one of the FTD's that is in your network, so policies with Identity are still 100% feasible with cdFMC
- Network Objects can be shared between your FTD's, ASA, & Meraki MX Devices via CDO
- Low Touch Provisioning and Easy Provisioning to the public clouds are all workflows that start with Onboard → FTD. Use them and save time.

Cloud Delivered FMC (cdFMC) Cheat Sheet (2 of 3)

REFERENCE

Troubleshooting Connectivity Issues from FTD to cdFMC

```
> ping system cisco.com

> system support diagnostic-cli

> en (no password, just hit enter)

FPR1150# capture cap1 interface outside real-time match tcp any any eq 8305

Warning: using this option with a slow console connection may result in an excessive amount of non-displayed packets due to performance limitations.

Use ctrl-c to terminate real-time capture

   1: 19:04:26.021727       72.178.118.98.50257 > 35.93.117.27.8305: P 3941217117:3941217147(30) ack 1513720207 win 8680 <nop,nop,timestamp 
3092606231 573335002>
```

REFERENCE

Cloud Delivered FMC (cdFMC) Cheat Sheet (3 of 4)

Troubleshooting Connectivity Issues from FTD to cdFMC

```
> show network

===============[ System Information ]===============

Hostname                  : FPR1150.hacksbrain.com

Domains                   : hacksbrain.com

DNS Servers               : 208.67.222.222

                            208.67.220.220

DNS from router           : disabled

Management port           : 8305

IPv4 Default route

  Gateway                 : data-interfaces
```

REFERENCE

Cloud Delivered FMC (cdFMC) Cheat Sheet (4 of 4)

Troubleshooting Connectivity Issues from FTD to cdFMC

```
----------------------[ IPv4 ]----------------------

Configuration         : Manual

Address              : 192.168.30.2

Netmask              : 255.255.255.0

Gateway              : 169.254.1.1
```

When using data-interface as the default gateway, 169.254.1.1 is normal and expected. This routes the management-plane to the data-plane.

Troubleshooting SFTunnel Errors

```
> expert

> admin@FPR1150:~$ sudo tail -f /ngfw/var/log/messages
```

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)!

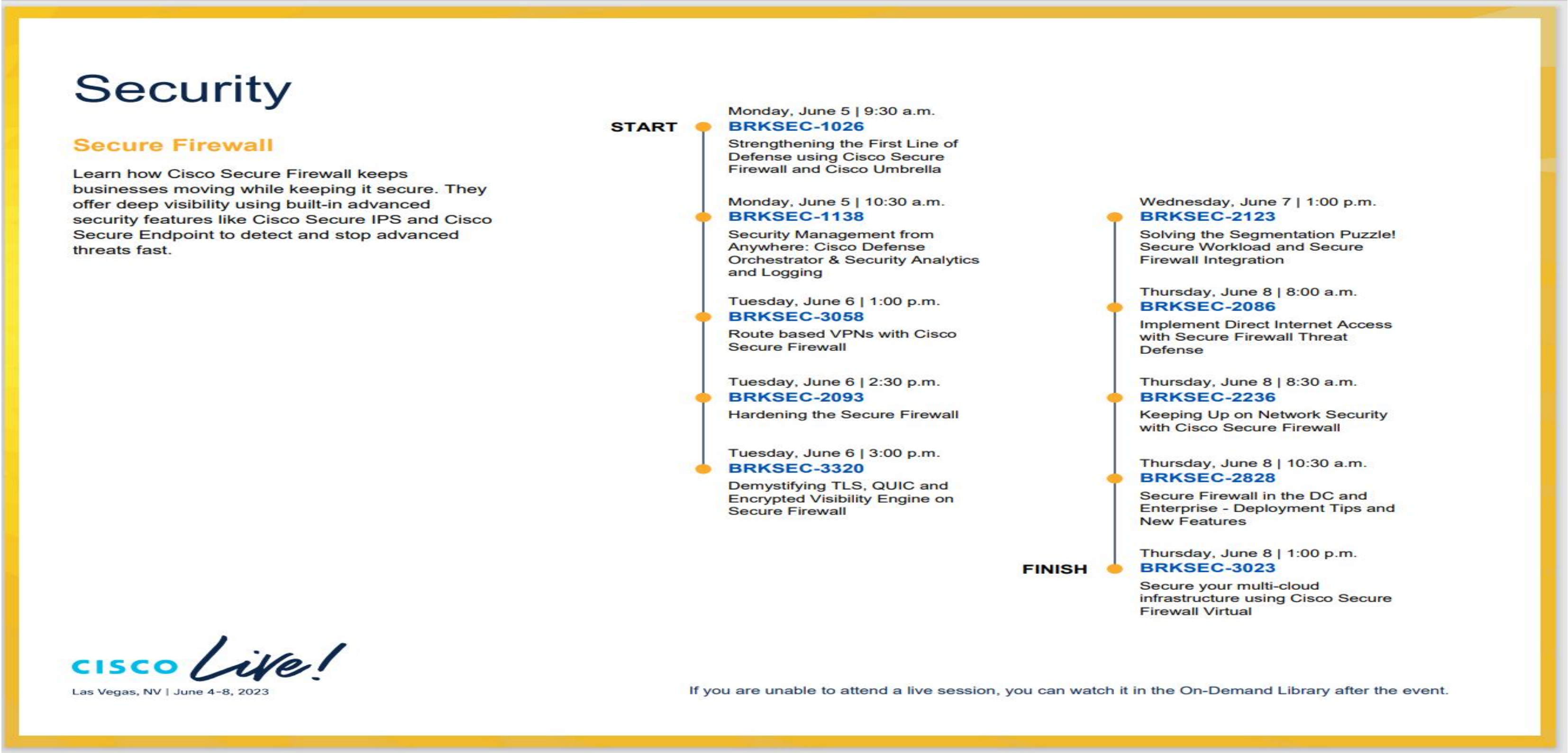
Attendees will also earn 100 points in the **Cisco Challenge** for every survey completed.

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 any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

Learning Map



Security

Secure Firewall

Learn how Cisco Secure Firewall keeps businesses moving while keeping it secure. They offer deep visibility using built-in advanced security features like Cisco Secure IPS and Cisco Secure Endpoint to detect and stop advanced threats fast.

START

Monday, June 5 | 9:30 a.m.
BRKSEC-1026
Strengthening the First Line of Defense using Cisco Secure Firewall and Cisco Umbrella

Monday, June 5 | 10:30 a.m.
BRKSEC-1138
Security Management from Anywhere: Cisco Defense Orchestrator & Security Analytics and Logging

Tuesday, June 6 | 1:00 p.m.
BRKSEC-3058
Route based VPNs with Cisco Secure Firewall

Tuesday, June 6 | 2:30 p.m.
BRKSEC-2093
Hardening the Secure Firewall

Tuesday, June 6 | 3:00 p.m.
BRKSEC-3320
Demystifying TLS, QUIC and Encrypted Visibility Engine on Secure Firewall

Wednesday, June 7 | 1:00 p.m.
BRKSEC-2123
Solving the Segmentation Puzzle! Secure Workload and Secure Firewall Integration

Thursday, June 8 | 8:00 a.m.
BRKSEC-2086
Implement Direct Internet Access with Secure Firewall Threat Defense

Thursday, June 8 | 8:30 a.m.
BRKSEC-2236
Keeping Up on Network Security with Cisco Secure Firewall

Thursday, June 8 | 10:30 a.m.
BRKSEC-2828
Secure Firewall in the DC and Enterprise - Deployment Tips and New Features

FINISH

Thursday, June 8 | 1:00 p.m.
BRKSEC-3023
Secure your multi-cloud infrastructure using Cisco Secure Firewall Virtual

CISCO Live!
Las Vegas, NV | June 4-8, 2023

If you are unable to attend a live session, you can watch it in the On-Demand Library after the event.

“The one who knows all the answers has not been asked all the questions.”

- Confucius

Q&A

The bridge to possible

Thank you

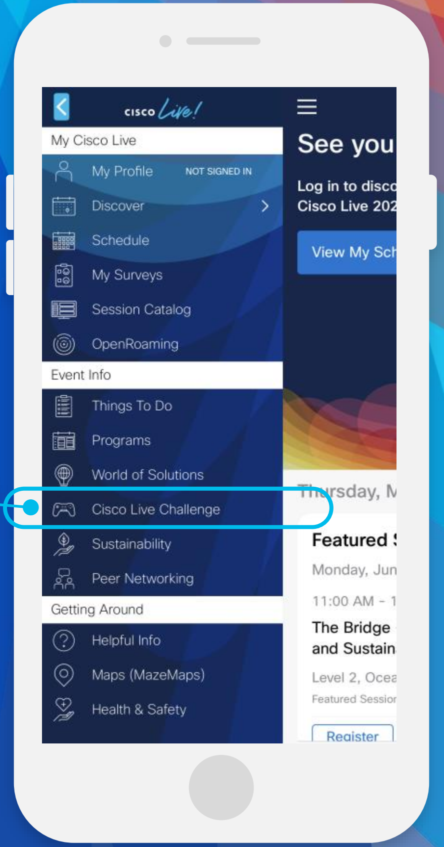
Cisco Live **Challenge**

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:



cisco Live!

cisco Live!

Let's go

#CiscoLive