

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Simplify Firewall Management

Cisco Security Cloud Control

Anshul Kaushik, Technical Solutions Architect
Distinguished Speaker

BRKSEC-2112

CISCO *Live!*

#CiscoLiveAPJC

Your Speaker

Anshul Kaushik

- ankaushi@cisco.com
- CCIE Security #23790
- 21 Years in Industry, 19 with Cisco
- TAC – Presales – Channels
- Drive end to end Security Enablement
- Lives in Melbourne and like outdoors

cisco *Live!*



Cisco Webex App

Questions?

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

How

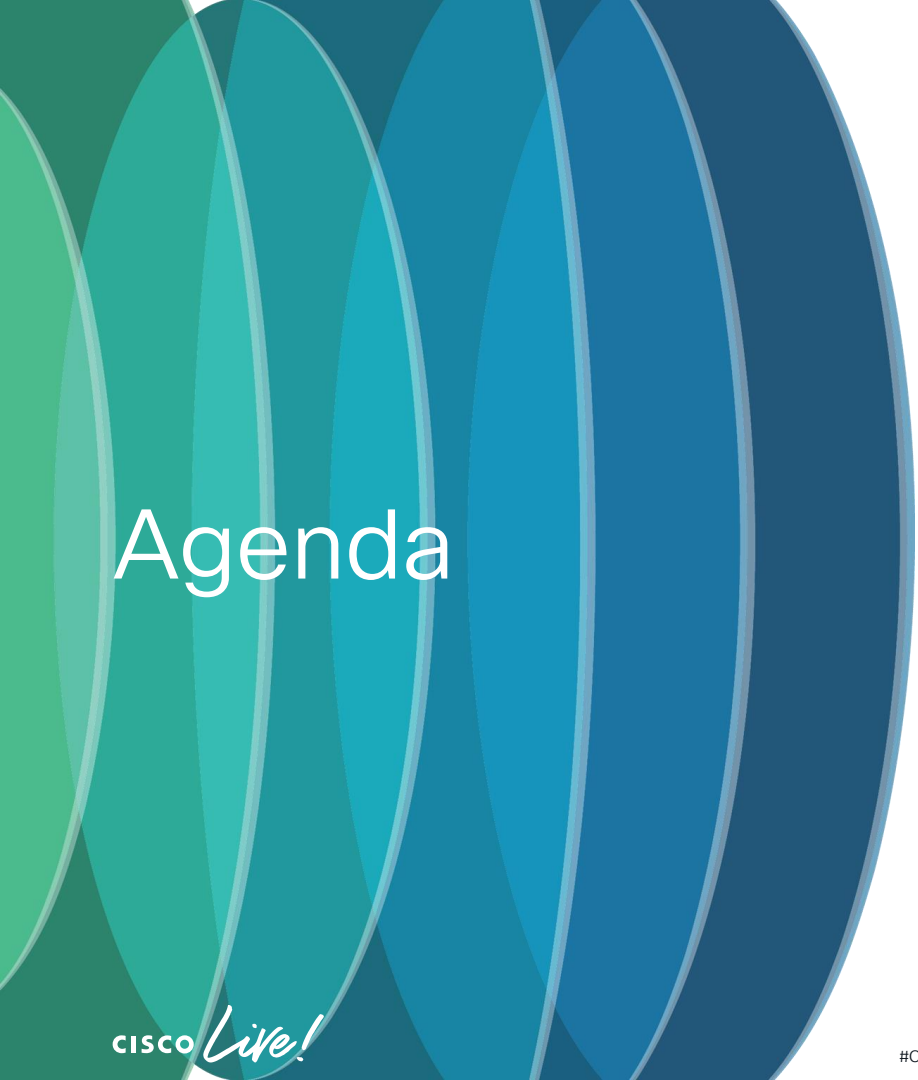
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2112>





Agenda

- Security Challenges in Today's Organizations
- Cisco Security Cloud Control Overview & Demo
- cdFMC and FTD Management & Demo
- ASA Management & Demo
- DevOps
- Key Takeaways and Resources



Configuration and monitoring are common culprits

MONITORING

Overloaded
sensor

dropping packets at peak

Poor visibility into
past events

preventing threat investigation

Fragmented device
tracking

slowing response to outages

CONFIGURATION

Misordered
firewall rule

lost in 10s of thousands

Disabled
security feature

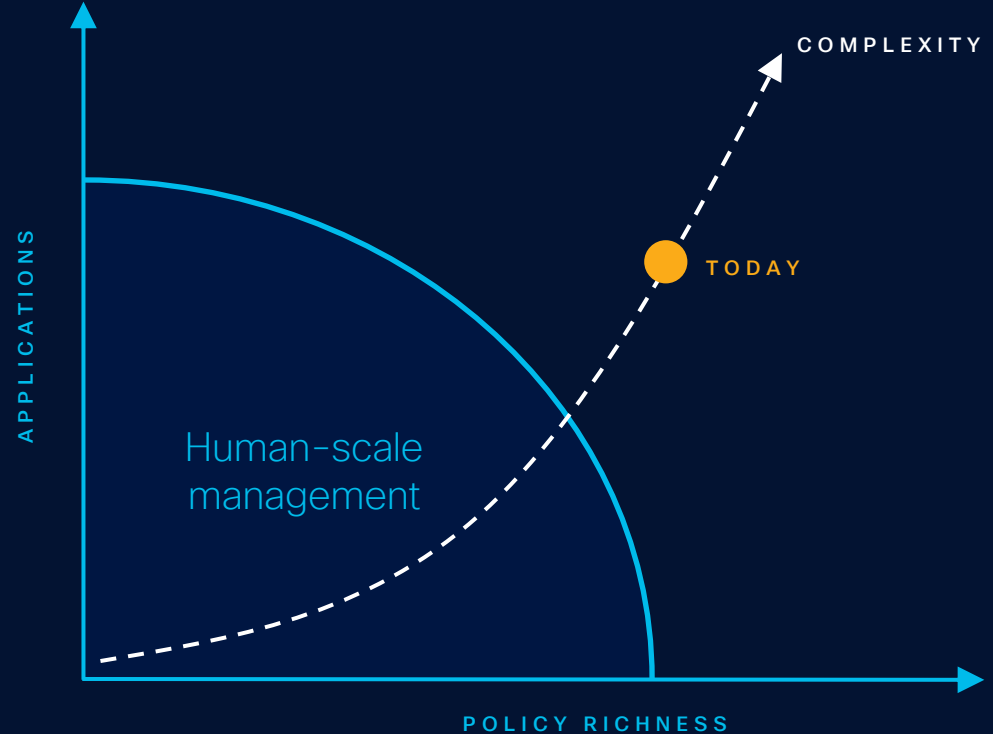
discovered in retrospect

Steep learning
curves for IT teams

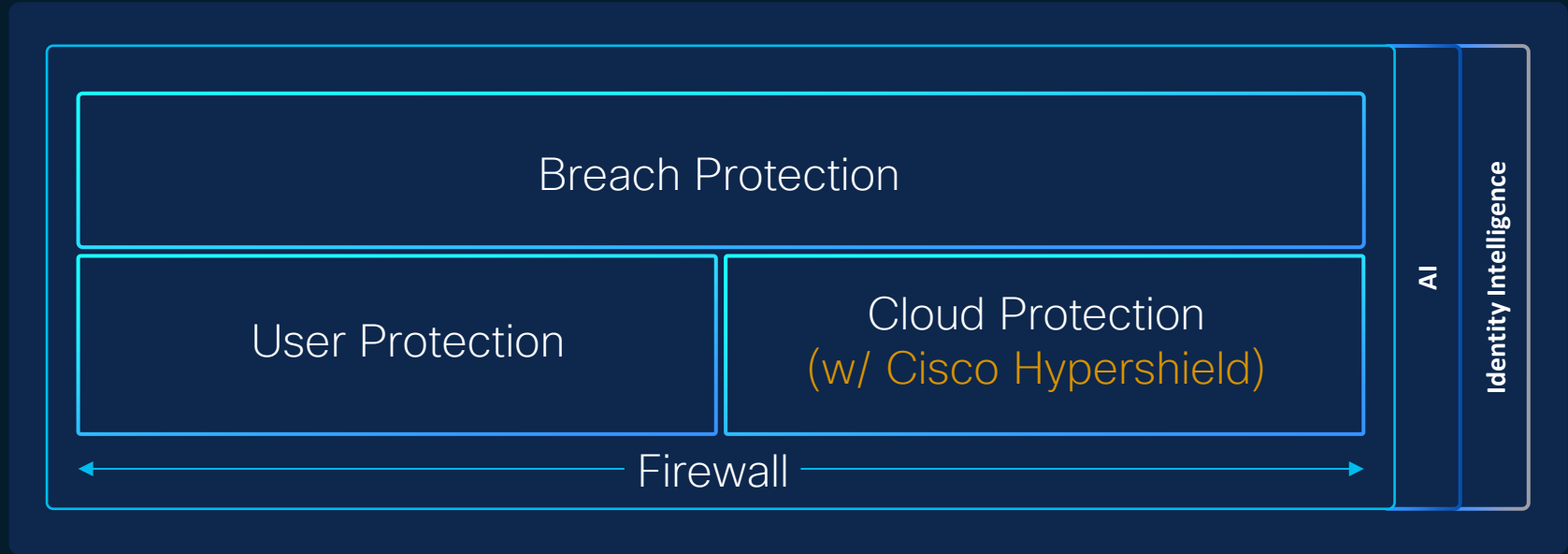
when transitioning to cloud

ROOT CAUSE

Complexity has exceeded human scale

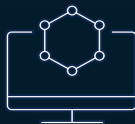


Security Cloud Control: Simplifying management for the Cisco Security Cloud



Cisco Security Cloud Control

Empower your security teams by expanding firewall management capabilities to the cloud



Simplify operations

Centralize visibility and management of devices and policies

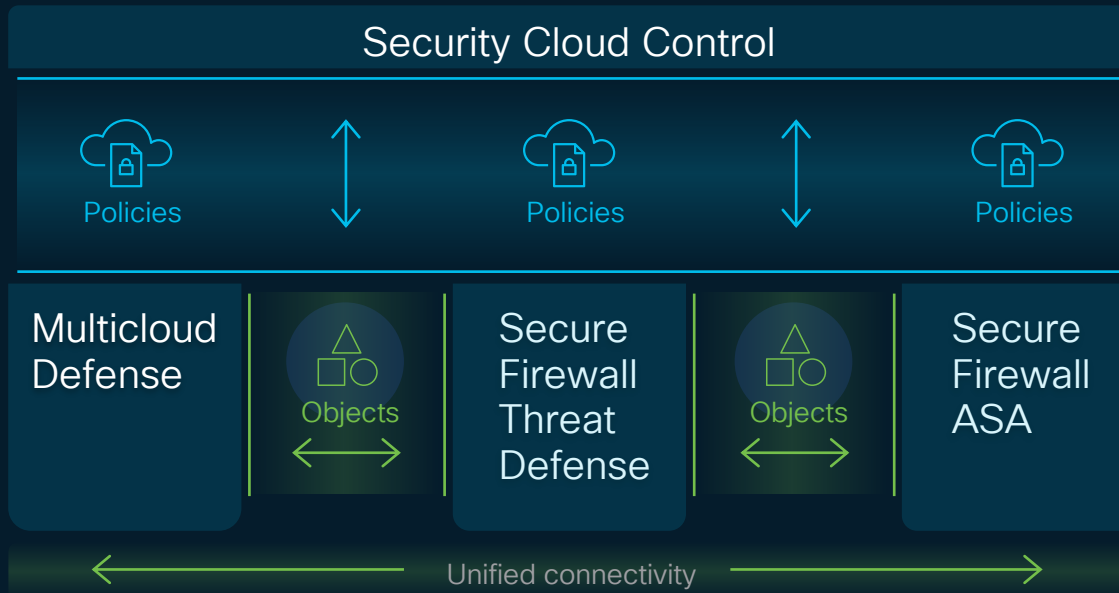
Enhance security

Leverage AI to strengthen protection and prevent downtime

Improve productivity

Minimize dependence on tribal knowledge and manual work

Streamline policy and device control



Centralize coordination of all ASA and FTD form factors eliminating complexity across diverse environments

Ensure consistent security policies and compliance reducing misconfigurations

Automate object updates saving time for strategic initiatives

Retain on-premises FMC or manage firewalls directly from Security Cloud Control allowing you to migrate to the cloud at your own pace

Simplify operations

Gain end-to-end visibility from a single screen



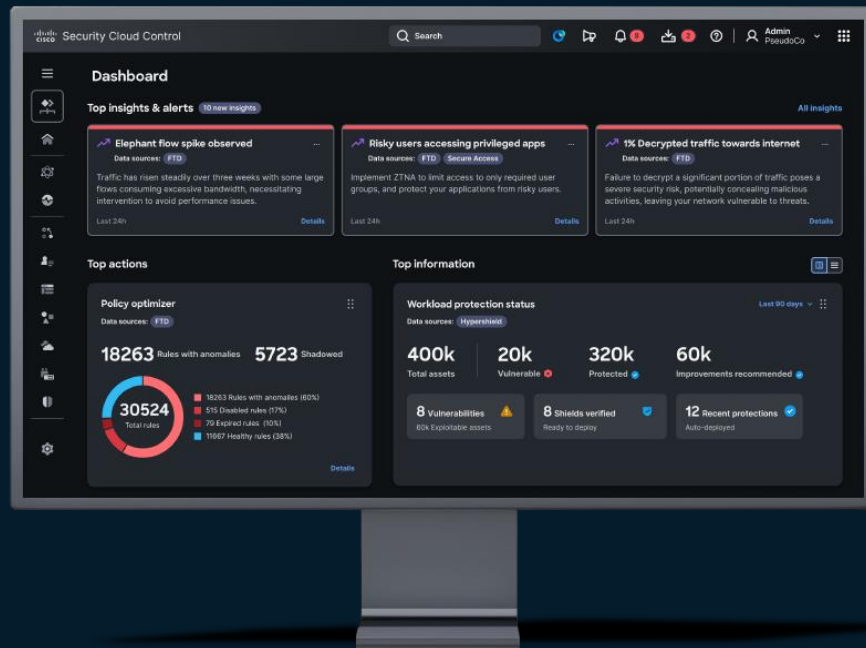
Access comprehensive insights across all firewall and security deployments



Enable prompt issue resolution through a live view of network traffic and security events



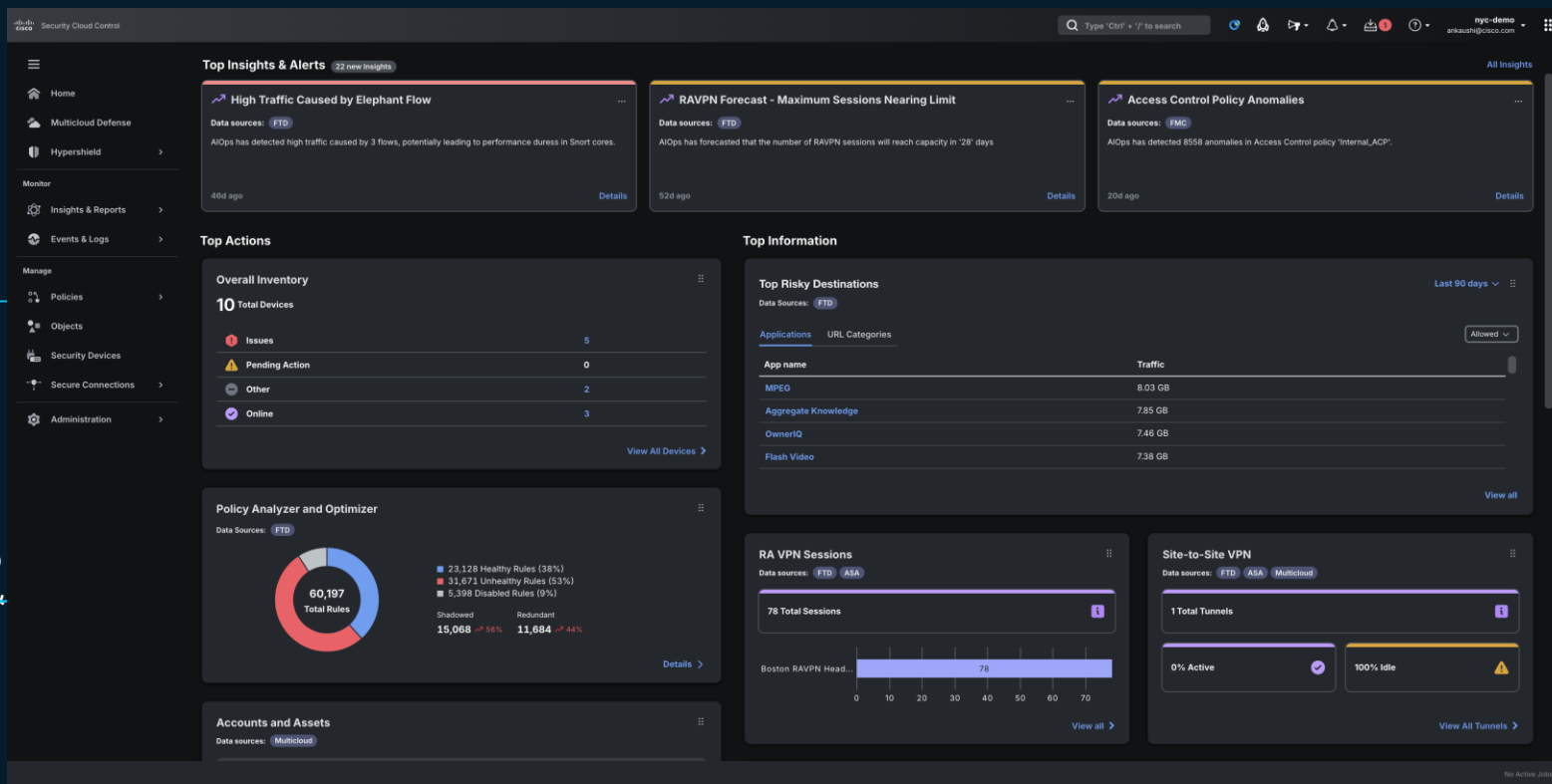
Empower informed decisions with operational insights from network data



Simplify operations

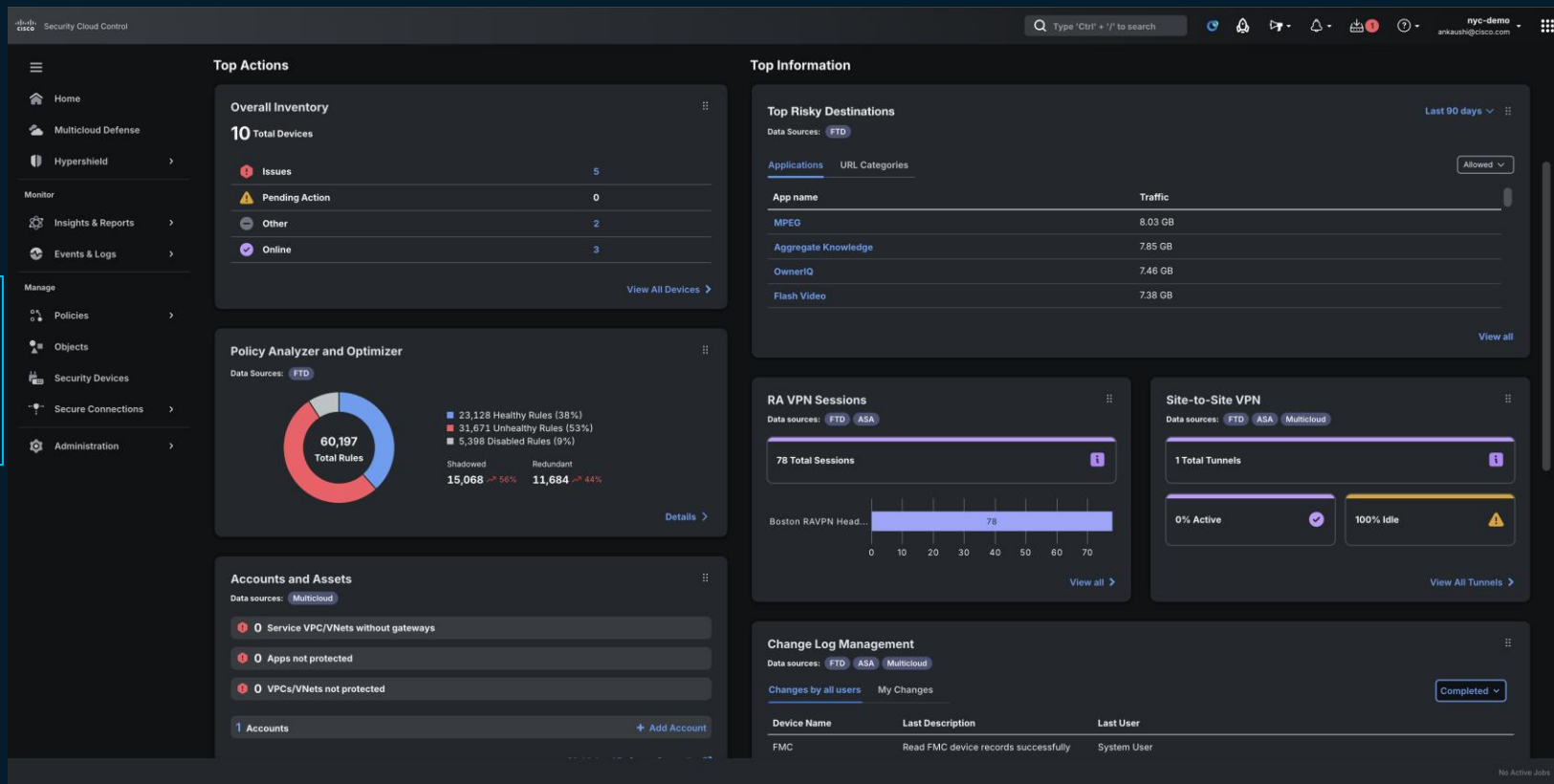
Surface top insights and alerts that needs immediate attention for security and improved network performance.

Present key items with recommended actions to improve policy hygiene & overall security posture

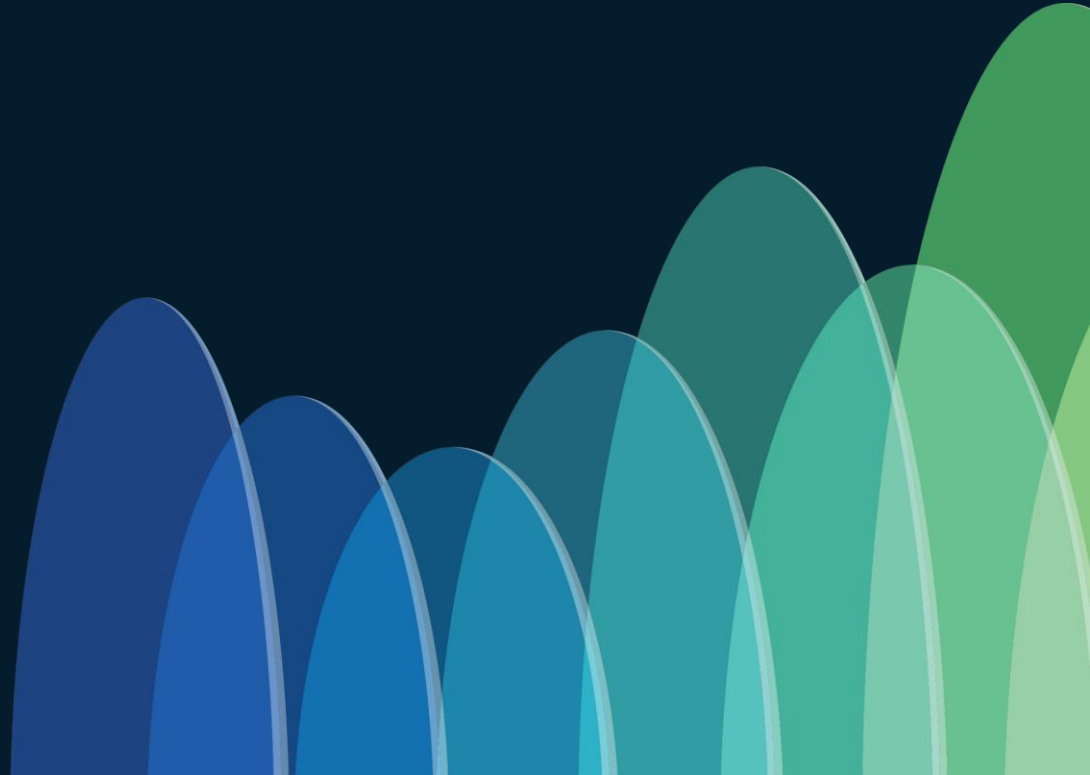


Simplify operations

Centralized view of all the changes across Firewalls, VPN, Multicloud Defense.



Security Cloud Control Demo



Enhance security

Optimize policies tailored to your environment



Policy analyzer
and optimizer



Minimize misconfigurations
and downtime



Speed up policy deployment
and updates



Address issues such as overlapping,
hidden, or overly broad rules



Improve firewall performance



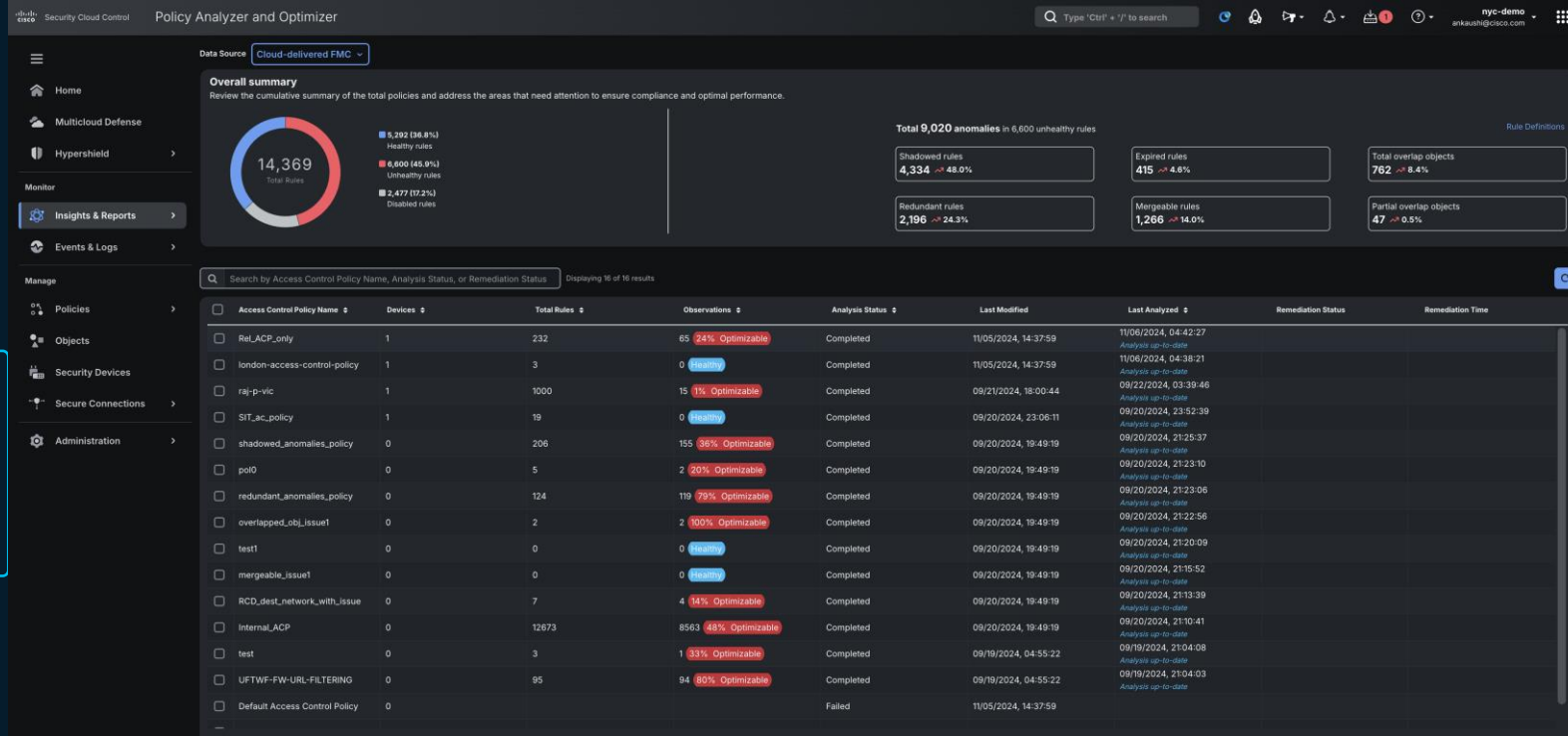
Aid collaboration with the
AI Assistant



Improve overall security
posture

Enhance security

Surface anomalies in rules to guide users to attend to stale rules and other policy hygiene issues that might be oversights

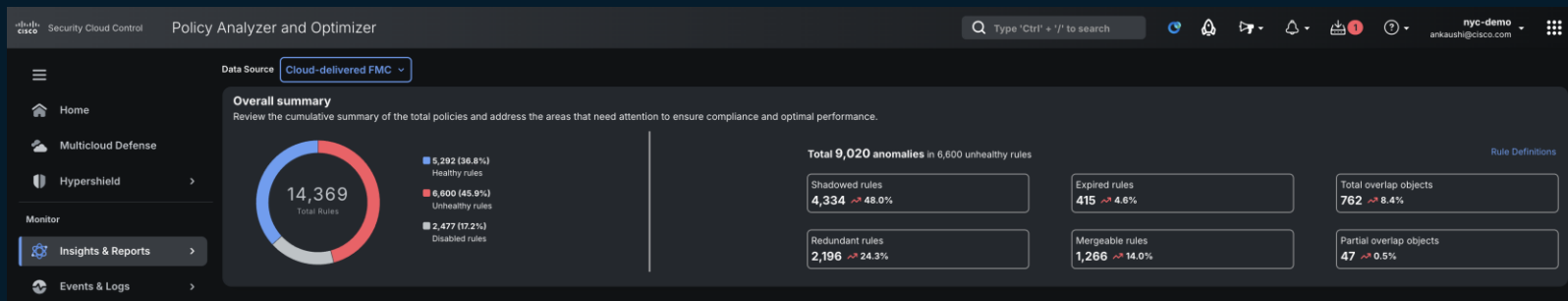


Enhance security

81%

Config anomalies
detected in a real
customer deployment

Misconfigurations
lead to breaches.



Policy Analyzer and Optimizer Demo

Home

Multicloud Defense

Hypershield

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Security Devices

Secure Connections

Administration

Top Insights & Alerts

22 new Insights

High Traffic Caused by Elephant Flow

Data sources: FTD

AIops has detected high traffic caused by 3 flows, potentially leading to performance duress in Snort cores.

Last 17h

Details

RAVPN Forecast - Maximum Sessions Nearing Limit

Data sources: FTD

AIops has forecasted that the number of RAVPN sessions will reach capacity in '31' days

Last 24h

Details

Access Control Policy Anomalies

Data sources: FMC

AIops has detected 8558 anomalies in Access Control policy 'Internal_ACP'.

23d ago

Details

Top Actions

Policy Analyzer and Optimizer

Data Sources: FTD

59,965 Total Rules

23,001 Healthy Rules (38%)

31,606 Unhealthy Rules (53%)

5,358 Disabled Rules (9%)

Shadowed 15,068 ↗ 56%

Redundant 11,627 ↗ 44%

Details

AIOPs Insights Summary

Top Information

Top Risky Destinations

Data Sources: FTD

Last 90 days

Applications

URL Categories

Allowed

App name	Traffic
MPEG	8.03 GB
Aggregate Knowledge	7.85 GB
OwnerIQ	7.46 GB
Flash Video	7.38 GB

View all

Customize

All Insights

Improve Productivity

Expedite workflows using a conversational interface

Assist



Policy configuration

Augment



Troubleshooting

Automate



Policy Lifecycle Management

Cisco AI Assistant

You

Allow Lee access to Facebook but only from office source zone

AI Assistant

11:05 am PST

Here is your rule recommendation, This rule will be added in policy 'Test_1' in the category, 'Geo_Controls'.

Rule Name	Action	Source zone	Destination zone
Rule_Test_1	Allow	Office	guest_zone

>

AI Assistant

11:05 am

✔ 'Rule_Test_1' is successfully created in policy 'Test_1'.

Congratulations, your rule named, 'Rule_Test_1' is successfully created in policy 'Test_1'. The rule is created in a **disabled state** as of now. You can enable it from your 'Test_1' policy detail page.

[Go to policy detail page](#)

>

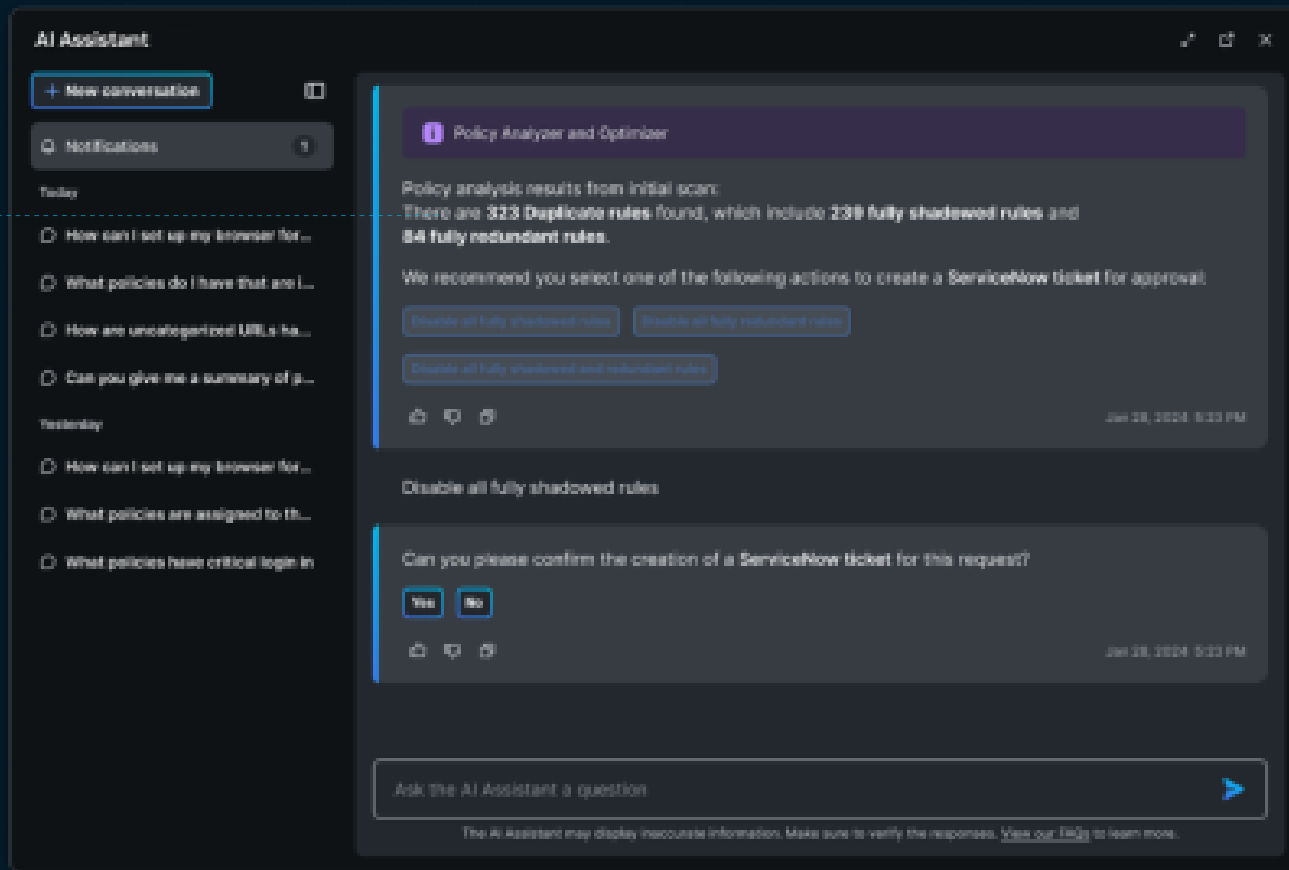
Ask the AI Assistant a question

>

The AI Assistant may display inaccurate information. Make sure to verify the responses. [View our FAQs](#) to learn more.

Improve Productivity

Users will be notified through AI assistant and could kick off remediation workflow through the conversational interface.



Improve Productivity

AI Assistant Beta

+ New conversation

Notifications 1

Today

How can I set up my browser for...

What policies do I have that are L...

How are uncategorized URLs ha...

Can you give me a summary of p...

Yesterday

How can I set up my browser for...

What policies are assigned to th...

What policies have critical login...

Policy Analyzer and Optimizer

Policy analysis results from initial scan:
There are **323 Duplicate rules** found, which include **238 fully shadowed rules** and **84 fully redundant rules**.

We recommend you select one of the following actions to create a ServiceNow ticket for approval:

Disable all fully shadowed rules

Disable all fully redundant rules

Disable all fully shadowed and redundant rules

👍

👎

🗑️

Jun 28, 2024 5:23 PM

Disable all fully shadowed rules

Can you please confirm the creation of a ServiceNow ticket for this request?

Yes

No

👍

👎

🗑️

Jun 28, 2024 5:23 PM

Ask the AI Assistant a question

➡

The AI Assistant may display inaccurate information. Make sure to verify the responses. [View our FAQs](#) to learn more.

CISCO *Live!*

#CiscoLiveAPJC

BRKSEC-2112

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public Cisco24 Confidential

Improve Productivity

Create firewall rule in conversational language.

Rule recommendation will be analyzed against existing rules to avoid rule shadowing, duplicating rules and other unintended scenario.

Cisco AI Assistant

You

Allow Lee access to Facebook but only from office source zone

AI Assistant

11:05 am PST

Here is your rule recommendation, This rule will be added in policy '**Test_1**' in the category, '**Geo_Controls**'.

Rule Name	Action	Source zone	Destination zone
Rule_Test_1	Allow	Office	guest_zone

>

AI Assistant

'Rule_Test_1' is successfully created in policy 'Test_1'.

11:05 am

Congratulations, your rule named, '**Rule_Test_1**' is successfully created in policy '**Test_1**'. The rule is created in a **disabled state** as of now. You can enable it from your '**Test_1**' policy detail page.

[Go to policy detail page](#)

>

Ask the AI Assistant a question

The AI Assistant may display inaccurate information. Make sure to verify the responses. [View our FAQs](#) to learn more.

AI Demo

 Security Cloud Control

Q

Type 'Ctrl' + '/' to search

 87 2

starks-team
ankaushi@cisco.com



Home

Multicloud Defense

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Security Devices

Secure Connections

Administration

Overall Inventory

23 Total Devices

Issues

Pending Action

Other

Online

2

1

0

20

View All Devices

Accounts and Assets

Data sources: Multicloud

0 Service VPC/VNets without gateways

0 Apps not protected

0 VPCs/VNets not protected

0 Accounts

Add Account

Multicloud Defense Controller

Configuration States

13 Not Synced

2 Conflict Detected

9 Synced

Change Log Management

No Active Jobs

Improve productivity

Boost productivity with actionable intelligence

- Discover patterns in security events using predictive analytics
- Improve security posture with AI-guided best practices
- Reduce mean time to resolution with risk-based prioritization
- Get the most out of security spending by leveraging the feature utilization overview



AIOps – Use Cases Demo

 Security Cloud Control

Q

Type 'Ctrl' + '/' to search



nyc-demo
ankaushi@cisco.com



Home

Multicloud Defense

Hypershield

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Security Devices

Secure Connections

Administration

Customize

All Insights

Top Insights & Alerts22 new Insights

High Traffic Caused by Elephant Flow

Data sources: FTD

AIOps has detected high traffic caused by 3 flows, potentially leading to performance duress in Snort cores.

Last 17h

Details

RAVPN Forecast - Maximum Sessions Nearing Limit

Data sources: FTD

AIOps has forecasted that the number of RAVPN sessions will reach capacity in '31' days

Last 24h

Details

Access Control Policy Anomalies

Data sources: FMC

AIOps has detected 8558 anomalies in Access Control policy 'InternalLACP'.

23d ago

Details

Top Actions

Policy Analyzer and Optimizer

Data Sources: FTD

59,965
Total Rules

23,001 Healthy Rules (38%)

31,606 Unhealthy Rules (53%)

5,358 Disabled Rules (9%)

Shadowed
15,068 ↗ 56%

Redundant
11,627 ↗ 44%

Details

AIOPS Insights Summary

Top Information

Top Risky Destinations

Data Sources: FTD

Applications

URL Categories

Allowed

App name	Traffic
MPEG	8.03 GB
Aggregate Knowledge	7.85 GB
OwnerIQ	7.46 GB
Flash Video	7.38 GB

View all

No Active Jobs

CISCO Live!

#CiscoLiveAPJC

BRKSEC-2112

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cloud Delivered Firewall Management Center

Cloud Delivered FMC (cdFMC)



- Not just a lift-and-shift VM – “Cloudified”
- Monolithic backend systems evolved to cloud-native technologies
- Economy of SCALE: Manage 1000 FTDs from a single cdFMC
- No FMC maintenances to perform – Complete SaaS by Cisco
- Physical or virtual FTDs
- Newest features delivered every 4-6 weeks!



Cloud Delivered FMC (cdFMC)

The screenshot displays the Cisco Security Cloud Control interface. The left sidebar contains navigation options: Home, Multicloud Defense, Hypershield, Monitor (Insights & Reports, Events & Logs), Manage (Policies, Objects, Security Devices, Secure Connections), and Administration. The Administration menu is expanded, showing options like General Settings, User Management, Notification Settings, Log Settings, Integrations, Secure Connectors, Firewall Management Center (selected), Multicloud Defense Management, Dynamic Attributes Connector, Migration, Firewall Migration Tool, and Migrate FTD to cdFMC.

The main content area shows the 'Cloud-Delivered FMC' configuration page. It includes a search bar, a table of FMC instances, and a right-hand sidebar with sections for Actions, Management, and System.

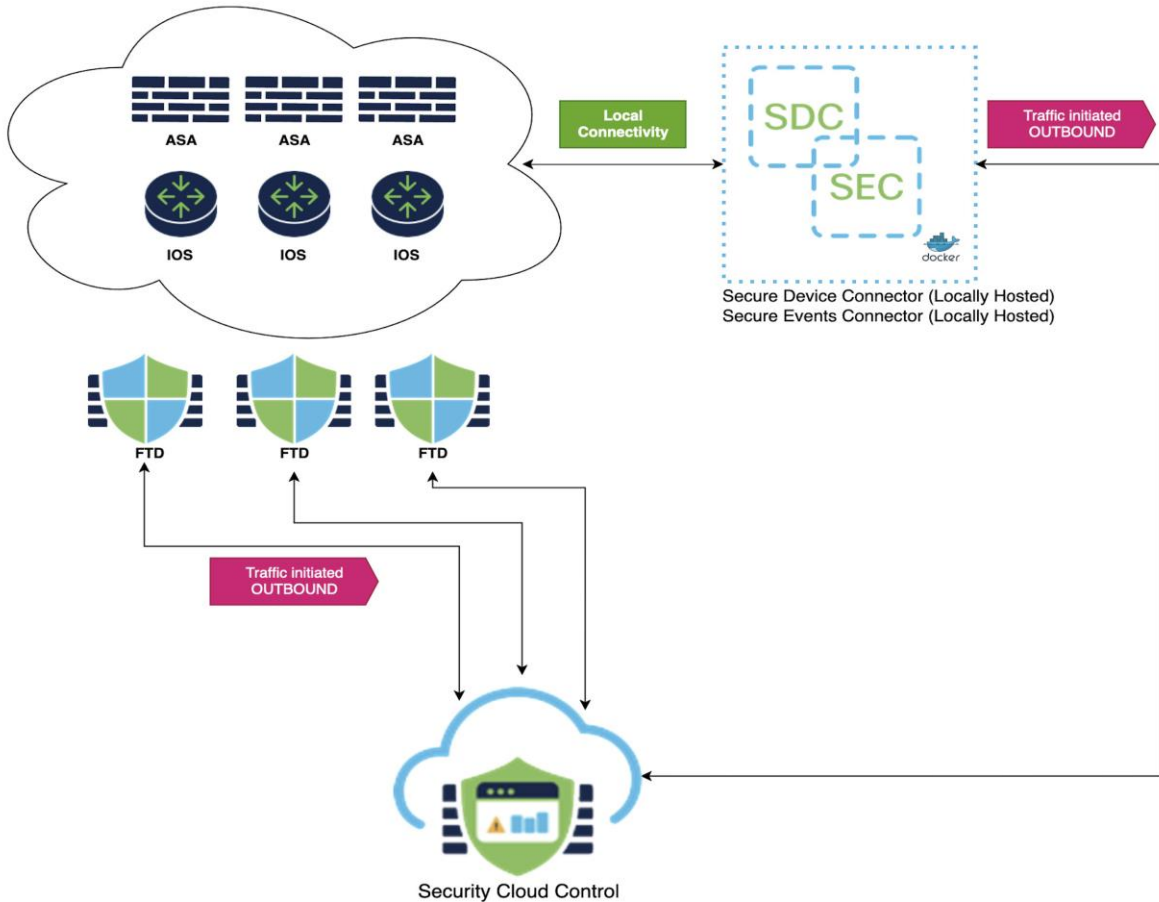
Version	Devices	Type	Status	Last Heartbeat
20240808	5	Cloud-Delivered FMC	Active	11/06/2024, 13:02:27
7.6.0-build 51	1	On-Prem FMC	Unreachable	-

The right-hand sidebar contains the following sections:

- Cloud-Delivered FMC**
 - Hostname: nyc-demo.app.staging.cdo.cisco.com
 - Version: 20240808
- Actions**
 - Check For Changes
 - Deployment
 - Updates
 - Workflows
 - API Explorer
 - Unified Events
- Management**
 - Devices
 - Policies
 - Objects
 - NAT
 - Site to Site VPN
 - Remote Access VPN
 - Platform Settings
- System**
 - Configuration
 - Smart Licenses
 - AMP Management
 - Device Health
 - Audit
 - Cisco Cloud Events

At the bottom right, it states "No Active Jobs".

Security Cloud Control-cdFMC Architecture



cdFMC AI Assistant

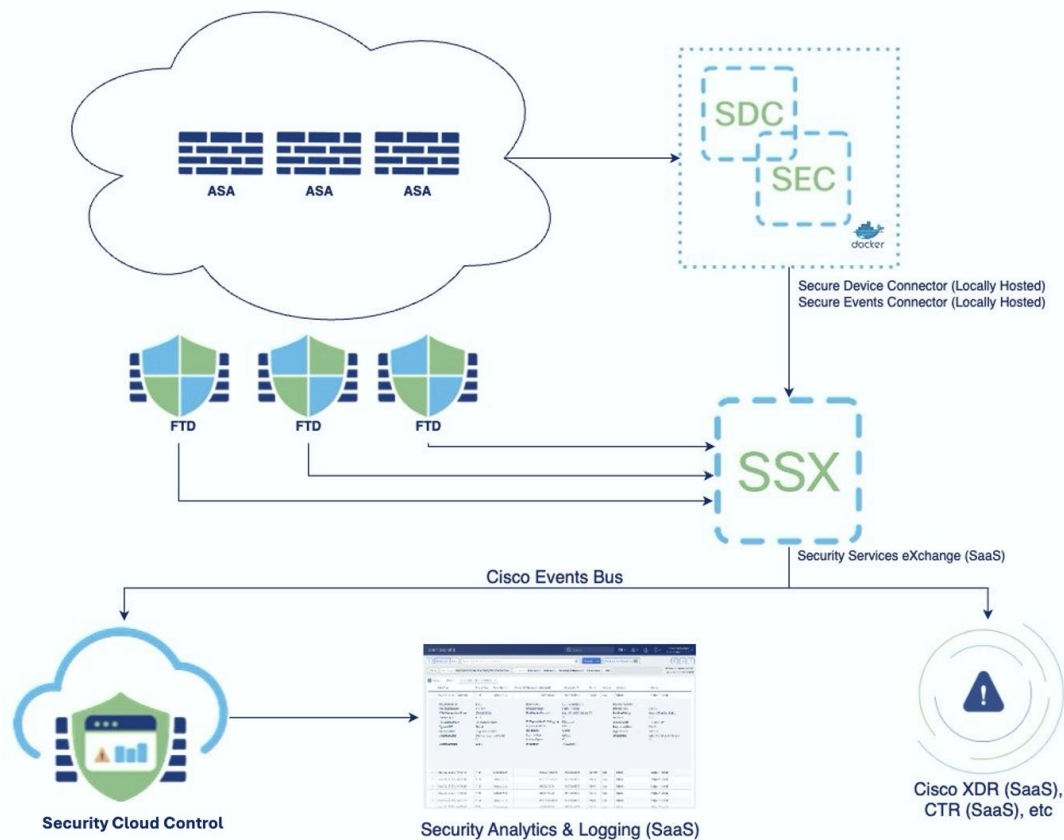
The screenshot displays the Cisco Defense Orchestrator (cdFMC) AI Assistant interface. The top navigation bar includes tabs for Analysis, Policies, Devices (selected), Objects, and Integration. The user is logged in as ankaushi@ciseco.com. The main content area is divided into three sections:

- Left Sidebar:** A list of devices grouped under 'All (5)'. The devices are: London (Snort 3, N/A - Routed), vFTD-36 (Snort 3, N/A - Routed), vFTD-40 (Snort 3, N/A - Routed), vFTD-47 (Snort 3, N/A - Routed), and vFTD-50 (Snort 3, N/A - Routed).
- Central AI Assistant Window:** A chat window titled 'AI Assistant' with a blue circular logo. It asks 'How can I help today?' and provides suggestions for questions: 'What is Hypershield?', 'What is a compensating control?', 'What is the PARC policy language?', and 'What is a CVE?'. There is a text input field at the bottom labeled 'Ask the AI Assistant a question'.
- Right Panel:** A section for device management with a 'Search Device' field, an 'Add' button, and a 'Download Device List Report' link. Below this is a table with columns for 'Policy', 'Auto RollBack', and 'Control-policy'.

Cloud Delivered FMC (cdFMC)

- API Explorer and FMC API Available via SCC Public API
- Code based on OnPrem FMC
- Cisco SaaS manages the FMC freeing you to focus on Policies
- cdFMC is included with every SCC tenant
- cdFMC is not in the flow of Analytics
- Analytics handled by SCC Cloud Events and XDR

Logging Architecture



Unified Event Viewer in cdFMC

Home

Search...

9,406 591 0 3 0 10,000 events

2024-06-05 15:37:02 EDT
2024-06-21 16:37:02 EDT 2w 2d

Ref

Analysis

Policies

Devices

Objects

Integration

Time	Event Type	Reason	Source IP	Destination IP	Action	Source Port / ICMP Type
2024-06-13 05:34:33	Connection		10.10.1.102	3.235.189.115	Allow	52769 / tcp
2024-06-13 05:34:33	Connection		10.10.90.111	3.82.76.181	Fastpath	35764 / tcp
2024-06-13 05:34:33	Security-Related Conn	Encrypted Visibility Block	10.10.1.25	52.20.182.36	Block	35783 / tcp
2024-06-13 05:34:33	Connection		10.10.90.111	18.154.185.109	Fastpath	49730 / tcp
2024-06-13 05:34:29	Connection		10.10.90.30	3.162.174.10	Fastpath	58446 / tcp
2024-06-13 05:34:29	Connection		10.10.90.30	3.162.174.36	Fastpath	47976 / tcp
2024-06-13 05:34:28	Connection		10.10.15.82	18.154.108.89	Allow	46350 / tcp
2024-06-13 05:34:27	Connection		10.10.1.39	8.8.4.4	Allow	8 (Echo Request)
2024-06-13 05:34:27	Connection		10.10.1.104	1.1.1.1	Allow	8 (Echo Request)
2024-06-13 05:34:26	Connection		10.10.1.26	44.234.123.138	Allow	48198 / tcp
2024-06-13 05:34:23	Security-Related Conn	Encrypted Visibility Block	10.10.1.104	172.64.151.218	Block	60524 / tcp
2024-06-13 05:34:23	Connection		10.10.255.1	1.1.1.0	Allow	8 (Echo Request)
2024-06-13 05:34:23	Security-Related Conn	Encrypted Visibility Block	10.10.1.104	104.18.36.38	Block	60525 / tcp
2024-06-13 05:34:23	Connection		10.10.1.104	1.1.1.1	Allow	8 (Echo Request)
2024-06-13 05:34:22	Connection		10.10.15.64	52.202.2.34	Allow	51618 / tcp
2024-06-13 05:34:22	Connection		10.10.1.39	8.8.4.4	Allow	8 (Echo Request)
2024-06-13 05:34:21	Security-Related Conn	Encrypted Visibility Block	10.10.1.104	172.64.151.218	Block	60523 / tcp
2024-06-13 05:34:21	Connection		10.10.15.64	52.202.2.34	Allow	51616 / tcp
2024-06-13 05:34:21	Connection		10.10.15.64	52.202.2.34	Allow	51614 / tcp
2024-06-13 05:34:21	Connection		10.10.1.26	44.234.123.157	Allow	48004 / tcp
2024-06-13 05:34:19	Security-Related Conn	Encrypted Visibility Block	10.10.1.104	104.21.67.201	Block	60522 / tcp

Event Details

Filter columns

Access Control Policy KC-Access-Policy

Device KC-1210-FTD-1

General Information

Last Packet 2024-06-13 05:34:33

Source User Not Found

Network Analysis Policy KC-NAP-Policy

Prefilter Policy KC-P

Detection Rule

Source IP 10.10.90.111

Destination IP 3.82.76.181

COMING SOON!

FTD Policy Analyzer and Optimizer

Security Cloud Control Policy Analyzer and Optimizer

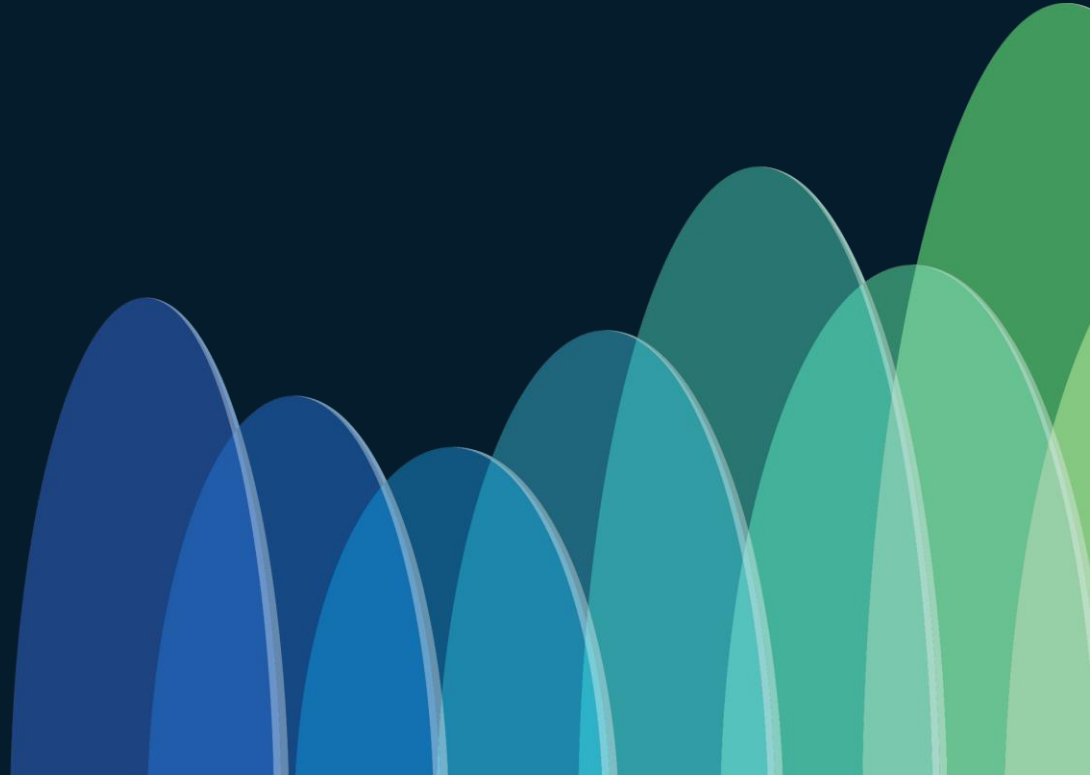
Search by Access Control Policy Name, Analysis Status, or Remediation Status

Displaying 16 of 16 results

☐	Access Control Policy Name	Devices	Total Rules	Observations	Analysis Status	Last Modified	Last Analyzed	Remediation Status	Remediation Time
☐	Access Policy Branch	1	4	1 25% Optimizable	Completed	11/08/2024, 14:37:56	11/10/2024, 04:41:06 Analysis up-to-date		
☐	Default Access Contr	0	0	0 Healthy	Completed	11/08/2024, 14:37:56	11/09/2024, 04:38:56 Analysis up-to-date		
☐	london-access-contr	1	3	0 Healthy	Completed	11/08/2024, 14:37:56	11/09/2024, 04:38:18 Analysis up-to-date		
☐	raj-p-vic	1	1000	15 1% Optimizable	Completed	09/21/2024, 18:00:44	09/22/2024, 03:39:4 Analysis up-to-date		
☐	SIT_ac_policy	1	19	0 Healthy	Completed	09/20/2024, 23:06:1	09/20/2024, 23:52:3 Analysis up-to-date		
☐	shadowed_anomalies	0	206	155 36% Optimizable	Completed	09/20/2024, 19:49:16	09/20/2024, 21:25:3 Analysis up-to-date		
☐	pol0	0	5	2 20% Optimizable	Completed	09/20/2024, 19:49:16	09/20/2024, 21:23:10 Analysis up-to-date		
☐	redundant_anomalies	0	124	119 79% Optimizable	Completed	09/20/2024, 19:49:16	09/20/2024, 21:23:01 Analysis up-to-date		
☐	overlapped_obj_issu	0	2	2 100% Optimizable	Completed	09/20/2024, 19:49:16	09/20/2024, 21:22:51 Analysis up-to-date		
☐	test1	0	0	0 Healthy	Completed	09/20/2024, 19:49:16	09/20/2024, 21:20:01 Analysis up-to-date		
☐	mergeable_issue1	0	0	0 Healthy	Completed	09/20/2024, 19:49:16	09/20/2024, 21:15:52 Analysis up-to-date		
☐	RED_def_network	0	7	4 57% Optimizable	Completed	09/20/2024, 19:49:16	09/20/2024, 21:13:36 Analysis up-to-date		

No Active Jobs

Demo of cdFMC and FTD management



Top Insights & Alerts

1 new Insights

 **Access Control Policy Anomalies**

Data sources: **FMC**

AIOps has detected 1 anomalies in Access Control policy 'FP1010Policy'.

Last 8h

Details

Top Actions

Policy Analyzer and Optimizer

Data Sources: **FTD**

■ 19 Healthy Rules (90%)

■ 1 Unhealthy Rules (5%)

■ 1 Disabled Rules (5%)

Shadowed 0 0%

Redundant 1 100%

Details

Top Information

Overall Inventory

25 Total Devices

Issues	8
Pending Action	1
Other	3
Online	13

Accounts and Assets

Data sources: **Multicloud**

0 Service VPC/VNets without gateways

68 Apps not protected

60 VPCs/VNets not protected

1 Accounts

+ Add Account

ASA Management

ASA Management

Objects and Policy Management

The screenshot displays the Cisco Security Cloud Control interface for managing network objects. The left sidebar contains navigation options: Home, Multicloud Defense, Hypershield, Monitor (Insights & Reports, Events & Logs), and Manage (Policies, Objects, Security Devices, Secure Connections, Administration). The 'Objects' section is currently selected.

The main panel shows a table of 50 objects (out of 18017 total). The table has columns for Name, Devices, Type, and Issues. The object '1.1.1.0' is selected, and its details are shown on the right sidebar.

Name	Devices	Type	Issues
02-100	toms-asa	Network Object	
1-128.0.1.0_24	toms-asa	Network Object	
1-26.0.1.0_24	toms-asa	Network Object	
1.1.1.0		Network Object	
1.1.1.2/32	Edd Template	Network Group	
10.0.0.0	toms-asa	Network Object	
10.0.0.0-8	toms-asa	Network Object	
10.0.0.0M8		Network Object	
10.0.0.0_8		Network Object	
10.0.103.100		Network Object	
10.0.103.49		Network Object	
10.0.103.85		Network Object	
10.0.103.81		Network Object	

The right sidebar for the selected object '1.1.1.0' shows the following details:

- Object Type:** Network Object
- Actions:** Edit, Remove
- Details:** 1.1.1.0
- Relationships:** Cloud-delivered FMC, chander-test-net
- Label Groups and Labels:** Add Labels, Add label groups and labels

No Active Jobs

ASA Management

Policy Based and VTI/Route-Based VPN Wizards

Security Cloud Control Create Site-to-Site VPN

Search: Type 'Ctrl' + '/' to search

Navigation:

- Home
- Multicloud Defense
- Hypershield
- Monitor
 - Insights & Reports
 - Events & Logs
- Manage
 - Policies
 - Objects
 - Security Devices
 - Secure Connections**
 - Administration

Follow the steps below

- 1 Peer Devices**
 - Configuration Name ***
Enter a name for the Site-to-Site VPN Configuration
 - ☒ Route Based ☐ Policy Based ⓘ
 - Peer 1**
 - Device ***
Select Device
 - VPN Access Interface ***
None
 - Peer 2**
 - ☐ Extranet ⓘ
 - Device ***
Select Device
 - VPN Access Interface ***
None
 - Next**
- 2 IKE Settings**
- 3 IPSec Settings**
- 4 Finish**

Cancel

No Active Jobs

ASA Management

ASA Bulk CLI and Macros

The screenshot displays the Cisco Security Cloud Control Bulk CLI interface. The top navigation bar includes the Cisco logo, 'Security Cloud Control', a breadcrumb for 'Bulk CLI', a search bar, and user information for 'demo-red' (ankaushi@cisco.com). The left sidebar contains a menu with categories: Home, Multicloud Defense, Hypershield, Monitor (Insights & Reports, Events & Logs), and Manage (Policies, Objects, Security Devices, Secure Connections, Administration). The main content area is titled 'Macros' and features a list of predefined macros on the left, such as 'ASA ASA_Golden_Te...', 'ASA Get Serial Numb...', 'ASA Cat File to Console', 'ASA Add Static Route', 'ASA Daily Tasks', 'ASA show version full', 'ASA Clear all connect...', 'ASA show version', 'ASA GoogleDNS', 'ASA Device Cert Check', and 'ASA License Review'. The central pane shows a command editor with 'interface outside' and 'shut' entered. The right pane, titled 'My List', shows a list of devices with checkboxes: Clarksville (10.10.6.42:8443), Dayton (10.10.6.44:8443), Richmond (10.10.6.47:443), and u73c0ip05-ftd-1010-2 (10.84.31.163:443). A 'Send' button is at the bottom right. The bottom status bar shows 'Change Request' and 'None'.

ASA Management

Scheduled ASA Upgrades

The screenshot shows the Cisco Security Cloud Control interface for managing ASA devices. The top navigation bar includes the Cisco logo, 'Security Cloud Control', and the current page 'Device Upgrade / ASA: Boston RAVPN Headend'. A search bar and various utility icons are also present.

The left sidebar contains navigation options: Home, Multicloud Defense, Hypershield, Monitor (Insights & Reports, Events & Logs), and Manage (Policies, Objects, Security Devices, Secure Connections, Administration).

The main content area displays device details for 'Boston RAVPN Headend':

- Device: Boston RAVPN Headend
- Model: ASAv (V01)
- Location: vpn-mgmt.shared.labs.cdo.cisco.com:443
- Failover Mode: Not Configured
- Devices: 1
- Disk Size: 798 GB
- Disk Usage: 256.27 MB

Below the device details, there is a 'Schedule Upgrade' button and a 'Select date and time' dropdown. The main content area is divided into three sections:

- ASA Software Image**: Shows the current image '9.20(2.10)'. There is a 'Skip Upgrade' checkbox and an 'Image Source' section with options 'Use SCC Image Repository' (selected) and 'Specify Image URL'. A 'Continue' button is present. A 'Software Image' dropdown menu is open, showing 'Select an Image' and '9.20(3.7) 154.46 MB'. A note states: 'Select the ASA software image you want to upgrade to. Only compatible versions of ASA and ASDM are shown.' Another note states: 'DNS must be properly configured on the device before attempting the upgrade. Please reference [Configure DNS on ASA](#) for details.' A final note states: 'If you check "Skip Upgrade," the ASA software image on your device will not be changed. You may still upgrade ASDM.'
- ASDM Software Image**: Shows the current image '7.10(1)' with a right arrow.
- Perform Upgrade**: A button to initiate the upgrade process.

The bottom right corner of the interface indicates 'No Active Jobs'.

ASA Management

Detailed Changelogs and Diff Views Available

The screenshot displays the 'Change Log' section of the Cisco Security Cloud Control interface. The interface features a dark theme with a sidebar on the left containing navigation links: Home, Multicloud Defense, Hypershield, Monitor, Insights & Reports, Events & Logs, Manage, Policies, Objects, Security Devices, Secure Connections, and Administration. The main content area shows a table of events with columns for Last Updated, Device Name, Last Description, and Last User. Each event entry includes a date and time, a status icon, and a 'Diff' link. A search bar at the top right allows for filtering events. The bottom status bar indicates 'No Active Jobs'.

Last Updated	Device Name	Last Description	Last User
Nov 6, 2024 1:18:14 PM	Clarksville	Conflict Detected	System User
Nov 6, 2024 1:18:14 PM		Conflict Detected	System User
Nov 6, 2024 1:17:06 PM	Clarksville	Changes written successfully	System User
Nov 6, 2024 1:17:06 PM		Changes written successfully	System User
Nov 5, 2024 1:18:14 PM		Conflict Detected	System User
Nov 6, 2024 1:12:27 PM	Cloud-delivered FMC	Read FMC device records successfully	System User
Nov 6, 2024 1:12:27 PM		Read FMC device records successfully	System User

ASA Management

Troubleshooting Tools From SCC – No CLI required

The screenshot displays the Cisco Security Cloud Control (SCC) interface for ASA management. The top navigation bar shows the Cisco logo, "Security Cloud Control", and the breadcrumb "ASA: Boston RAVPN Headend / Troubleshoot". A search bar is present with the placeholder "Type 'Ctrl' + '/' to search". The right side of the header contains various icons and the user profile "nyc-demo" with email "ankaushi@cisco.com".

The left sidebar contains a menu with the following sections:

- Home
- Multicloud Defense
- Hypershield
- Monitor
 - Insights & Reports
 - Events & Logs
- Manage
 - Policies
 - Objects
 - Security Devices
 - Secure Connections
 - Administration

The main content area is divided into two panels. The left panel, titled "Clear", contains the following controls:

- Run Packet Tracer** button
- View Real-Time Log** button
- Interface** dropdown menu (currently set to "inside")
- Packet Type** section with radio buttons for TCP (selected), UDP, ICMP, and IP
- Source** section with an "IP Address" dropdown and an "Enter Source" text input
- Port** section with an "Enter Source Port" dropdown
- Destination** section with an "IP Address" dropdown and an "Enter Destination" text input
- Port** section with an "Enter Destination Port" dropdown
- SGT Number (0-65535)** text input

The right panel, titled "PACKET TRACER OUTPUT", contains the following text:

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

Below this, the "REAL-TIME LOG OUTPUT" section is visible, showing "No Active Jobs".

ASA Object and Policy Management

Security Cloud Control < ASA Access Policies / inside_access_in / Access Control Entries

Search for access rules by components or objects used

Displaying 18 rules

Line	Action	Protocol	Source	Port	Destination	Port	Hits (Day)
1	Deny	ip	any	any	EmergencyBlock	any	0000
2	Permit	udp	any	any	Umbrella	UmbrellaUDP	0000
3	Permit	tcp	any	any	Umbrella	UmbrellaPorts	0000
4	Permit	ip	any	any	O365	any	0000
5	Permit	ip	any	any	ActiveDirectoryServers	any	0000
6	Permit	ip	AlarmSystemPanel	any	AlarmCompany	any	0000
7	Permit	ip	any	any	Duluth-Remote-Netwrok	any	0000
8	Permit	tcp	web-proxy-servers	any	any	www	0000
9	Permit	tcp	PrinterAndScanner	SuperWoopleApplication	any	any	0000
10	Permit	ip	Backend-Servers	any	any	any	0000
11	Permit	ip	MySpecialServer	any	any	any	0000
12	Permit	tcp	web-proxy-servers	any	any	https	0000
13	Permit	tcp	any	any	any	https	0000
14	Permit	ip	10.56.56.123	any	any	any	0000
15	Deny	ip	10.56.56.0/24	any	any	any	0000
16	Permit	ip	newobjectest	any	any	any	0000
17	Permit	icmp	any	-	any	-	0000

inside_access_in

55 Access Control Entries (1 Shadowed)

Shadowed

Edit Policy

Troubleshoot

Network Policy

Access Control Entries

1

Logging

Default

Time Range

Select Time Range

Remarks

Add a remark for this rule...

Devices

toms-asa

Hits

No Active Jobs

ASA Object and Policy Management

The screenshot displays the Cisco ASA configuration interface. On the left is a navigation sidebar with sections: Home, Multicloud Defense, Hypershield, Monitor (Insights & Reports, Events & Logs), Manage (Policies, Objects, Security Devices, Secure Connections, Administration), and a status bar at the bottom showing 'Change Request' and 'None'. The main content area is titled 'DNS' with the subtitle 'Configure servers'. A 'Parent Policy' dropdown at the top shows 'e267eb64-87fe-4e76-9556-b4d7d76b0f31_SETTINGS_POLICY_SHARED'. A modal dialog box titled 'Apply Setting Policy to Device' is open, featuring a 'Policies' section with a search bar (containing 'Search for policy' and '2 results') and a table with two rows: 'Gold-Standard' and 'e267eb64-87fe-4e76-9556-b4d7d76b0f31_SETTINGS_POLICY_SHARED'. The 'e267eb64...' row is selected. Below the table is a 'Clear Selection' link and 'Cancel' and 'Apply' buttons. In the background, the 'DNS' configuration page shows a table with columns 'Name', 'Type', and 'Actions', and a 'Reset' button at the bottom right.

ASA Management

Management

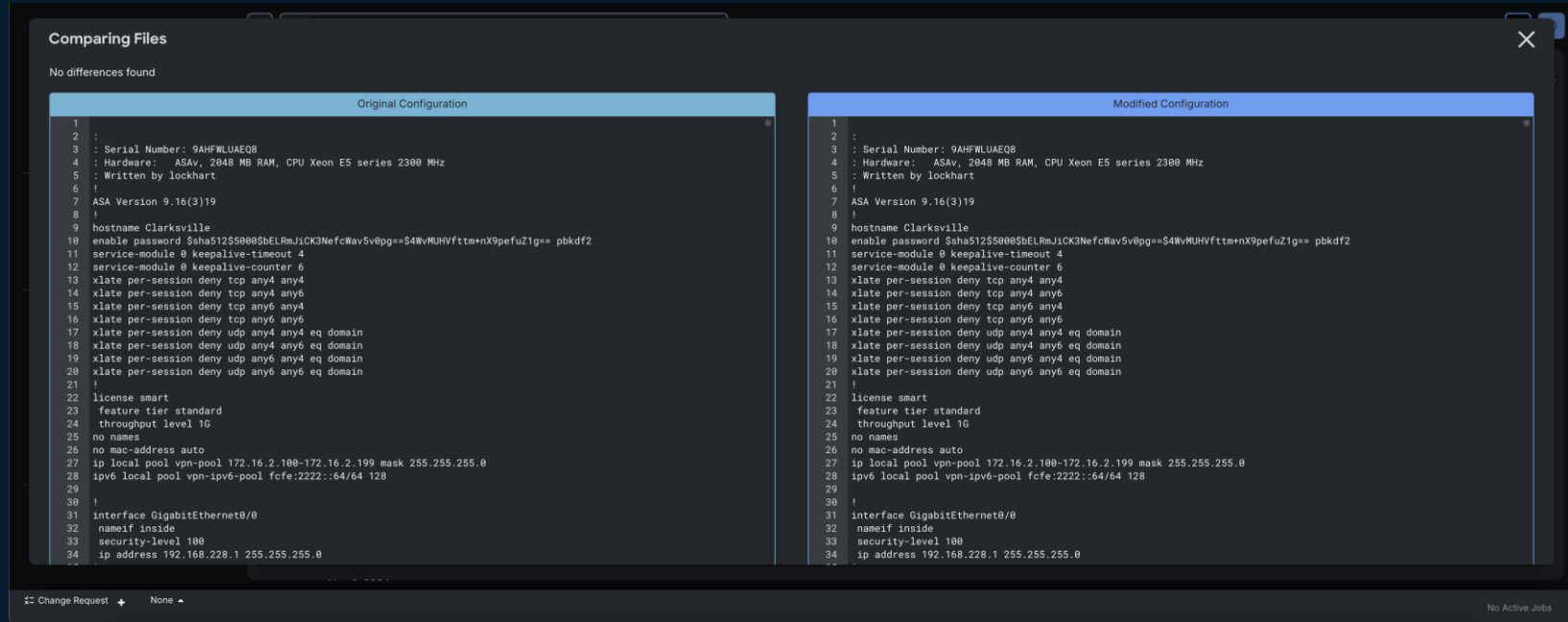
-  Configuration
-  Restore
-  NAT
-  VPN Tunnels List
-  Objects
-  Policy
-  File Management
-  Settings
-  Interfaces
-  Trustpoints
-  Routing
-  Notes
-  Changelog

Lots more functionality including:

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

Change control and visibility

ASA configuration changes



Centralized Cloud ASA Events

The screenshot displays the Cisco Security Cloud Control Event Logging interface. The top navigation bar includes the Cisco logo, 'Security Cloud Control', and 'Event Logging'. A search bar is present with the placeholder text 'Type Ctrl + F to search'. The interface is divided into a left sidebar with navigation options (Home, Multicloud Defense, Hypershield, Monitor, Insights & Reports, Events & Logs, Manage) and a main content area. The main content area shows a list of events, with the first event selected and its details expanded. The event details are organized into two columns: 'Device Type' and 'Event Type'. The 'Device Type' column lists fields like Action, ConnectionID, ConnectorID, DeviceType, Direction, EgressInterface, EventGroup, EventGroupDefinition, EventName, and Message. The 'Event Type' column lists fields like IngressInterface, InitiatorIP, InitiatorPort, MappedInitiatorIP, MappedInitiatorPort, MappedResponderIP, MappedResponderPort, Protocol, ResponderIP, ResponderPort, SensorID, Severity, SyslogTimestamp, and timestamp. The event details are as follows:

Field	Value
Action	Built
ConnectionID	23963
ConnectorID	b8d34396-36c8-4ba8-905c-4d74eb0f5f73
DeviceType	ASA
Direction	outbound
EgressInterface	inside
EventGroup	session
EventGroupDefinition	User Session
EventName	Built UDP
Message	ASA-6-302015: Built outbound UDP connection 23963 for inside:192.168.129.1/67 (192.168.129.1/67) to identity:192.168.129.87/68 (192.168.129.87/68)
IngressInterface	identity
InitiatorIP	192.168.129.87
InitiatorPort	68
MappedInitiatorIP	192.168.129.87
MappedInitiatorPort	68
MappedResponderIP	192.168.129.1
MappedResponderPort	67
Protocol	udp
ResponderIP	192.168.129.1
ResponderPort	67
SensorID	192.168.255.206
Severity	Informational
SyslogTimestamp	2024-08-08 00:42:43.968987 +0000 UTC
timestamp	Aug 8, 2024, 11:42:44

The bottom of the interface shows a 'Change Request' button and a 'None' status indicator.

Live demo of common ASA tasks

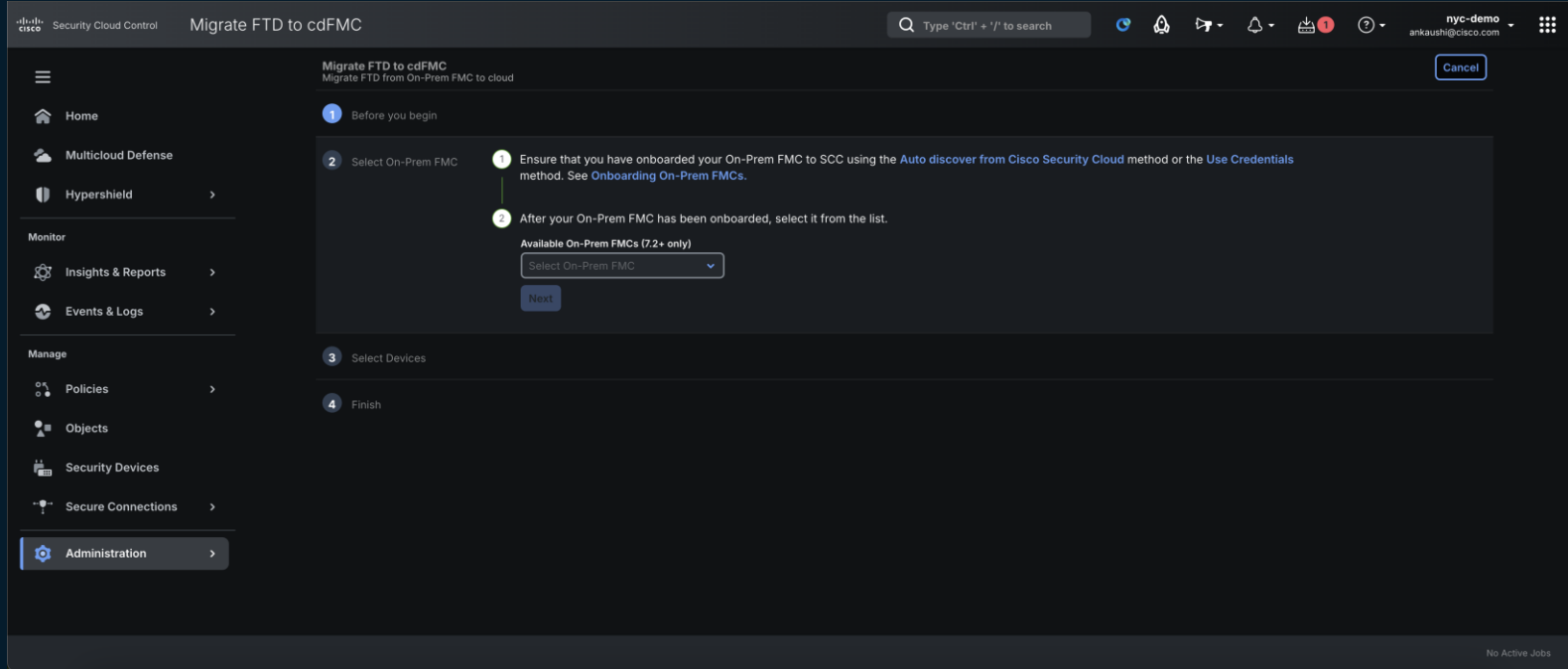
Demo of common ASA tasks

100% Idle

Advanced Tooling & Features

Security Cloud Control Simplifies Advanced Tooling

Migrate FTD from On-Prem FMC to cdFMC



Security Cloud Control Simplifies Advanced Tooling

Firewall Migration Tool (FMT)

- ASA → cdFMC/FTD
- FDM → cdFMC/FTD
- PAN → cdFMC/FTD
- Fortinet → cdFMC/FTD

The screenshot displays the Cisco Security Cloud Control Firewall Migration Tool (FMT) interface. The top panel shows the 'About Firewall Migration Tool' page, which explains that the tool converts configurations from Cisco Adaptive Security Appliances (ASA) or Firewall Device Manager (FDM) to Cisco Secure Firewall Multicloud Defense (cdFMC). The bottom panel shows the 'Services' page with a table of FMCs. The 'Cloud-Delivered FMC' is selected, and an 'Initialize Migration' dialog box is open, prompting the user to name the migration.

Name	Version	Devices	Type	Status	Last Heartbeat
☒ Cloud-Delivered FMC	20240808	5	Cloud-Delivered FMC	Active	11/06/2024, 15:03:31
☐ firepower_10.10.18.139	7.6.0-build 51	1	On-Prem FMC	Unreachable	-

Initialize Migration

To initialize the migration process, name this migration and click OK. SCC will notify you when the migration tool is ready for use. When ready, select this named migration and launch the tool.

Name *

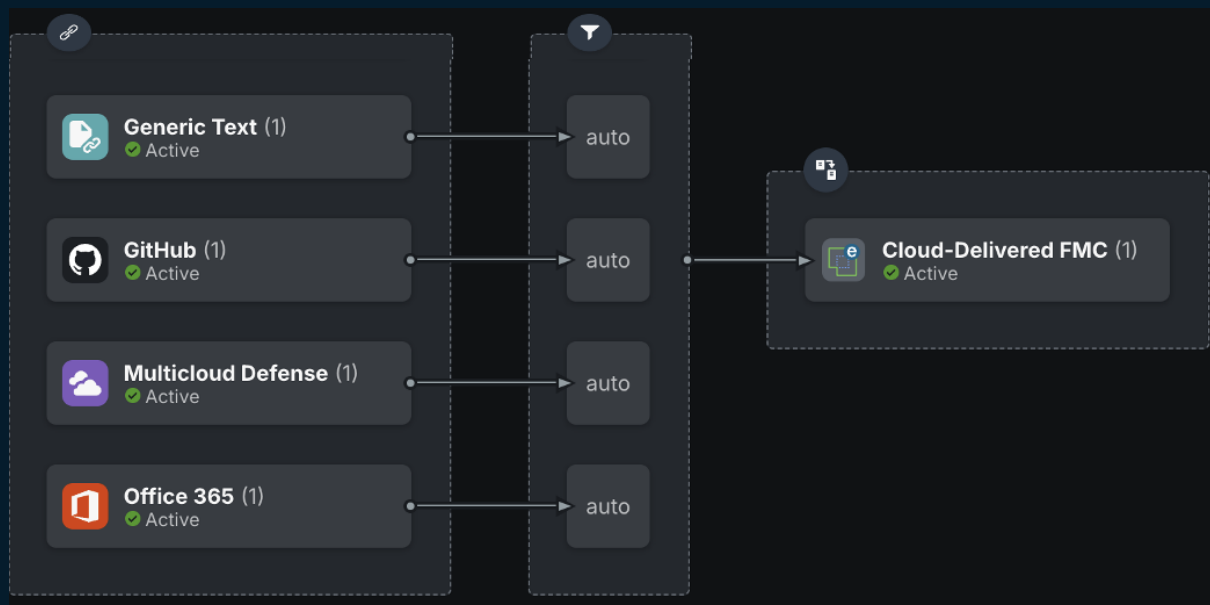
major-tips-admin

This is an auto-generated name. You can change it if you wish.

Cancel OK

Security Cloud Control Simplifies Advanced Tooling

Cisco Secure Dynamic Attributes Connector (CSDAC)



Security Cloud Control Simplifies Fleet Management

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

The screenshot displays the Cisco Security Cloud Control interface. The main section shows a table of security devices with columns for Name, Configuration Status, and Connectivity. The devices listed include 'toms-asa', 'London', 'Boston RAVPN Headend', 'vFTD-36', 'vFTD-40', 'vFTD-50', 'vFTD-47', 'ninja1-ftd', 'Edd Template', and 'firecower'. The 'Boston RAVPN Headend' device is highlighted, and its details are shown on the right side of the interface. The details include Location, Model, Serial, Chassis Serial, Software Version, ASDM Version, Context Mode, Firewall Mode, Uptime, and Failover Mode. The interface also includes a sidebar with navigation options like Home, Multicloud Defense, Hypershield, Monitor, Insights & Reports, Events & Logs, Manage, Policies, Objects, Security Devices, Secure Connections, and Administration.

Name	Configuration Status	Connectivity
toms-asa ASA	Conflict Detected	Online
London FTD	Not Synced	Online
Boston RAVPN Headend ASA	Synced	Online
vFTD-36 FTD	Not Synced	Offline
vFTD-40 FTD	Not Synced	Offline
vFTD-50 FTD	Not Synced	Offline
vFTD-47 FTD	Not Synced	Offline
ninja1-ftd FTD	-	Unreachable
Edd Template Meraki MX Template	Synced	-
firecower 10.10.18.139 10.10.18.140	-	-

Boston RAVPN Headend Details:

- Location: vpn-
- Model: ASA v90
- Serial: BANAH81SMEF
- Chassis Serial: BANAH81SMEF
- Software Version: 9.20(2)10
- ASDM Version: 7.9(1)
- Context Mode: Single Context
- Firewall Mode: Routed
- Uptime: 187 Days 11 Hours
- Failover Mode: Not Configured

Security Cloud Control Simplifies Fleet Management

Notifications via email or webhooks

The screenshot shows the Cisco Security Cloud Control interface. The top navigation bar includes the Cisco logo, 'Security Cloud Control', and 'Preferences'. A search bar is present with the text 'Type \'Ctrl\' + \'/\' to search'. The left sidebar contains a menu with categories: Home, Multicloud Defense, Hypershield, Monitor, and Manage. The main content area is titled 'Notification Preferences' and includes a sub-header 'Notifications are deleted after 30 days.' The settings are organized into three columns: 'Notify Me in SCC When', 'Device Workflows', and 'Device Events'. The 'Device Workflows' column has a 'Save' button. At the bottom, there is an 'Email Alerts' section with a toggle switch and a checkbox for 'Use SCC notification settings above'. The bottom status bar shows 'Change Request' and 'None' on the left, and 'No Active Jobs' on the right.

Notification Preferences
Notifications are deleted after 30 days.

Notify Me in SCC When

Device Workflows

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

Device Events

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

Background Log Search

- ☐ All background log search events
 - ☐ Search started
 - ☐ Search completed
 - ☐ Search failed

Email Alerts

Subscribe to receive email alerts

☒ Use SCC notification settings above

IOS Bulk CLI Access & Config Visibility

The screenshot displays the Cisco Security Cloud Control Bulk CLI interface. The top navigation bar includes the Cisco logo, "Security Cloud Control", a back arrow, "Bulk CLI", a search bar with the placeholder "Type 'Ctrl' + '/' to search", and user information for "demo-red" (ankaush@cisico.com). The left sidebar contains a menu with sections: Home, Multicloud Defense, Hypershield, Monitor (Insights & Reports, Events & Logs), and Manage (Policies, Objects, Security Devices, Secure Connections, Administration). The main content area is titled "Macros" and shows a list of macros: "IOS Show Routes" (Shows the IP routing table), "IOS Create VLAN" (Create a VLAN on the device), "IOS Check For VLAN" (See if a VLAN is Defined), "IOS Commit Change" (Copy running config to startup config), "IOS Find a MAC" (Finds a MAC address in the MAC table), and "IOS Find an IP" (Finds an IP address in the ARP table). The "IOS Show Routes" macro is selected, and the command "sh ip route" is entered in the command field. The command was sent on 11/9/2024 at 4:57:50 PM. The execution status shows "2" devices selected: Worcester and Fitchburg. The response for 1 device is shown, displaying the IP routing table output for the selected device.

Command sent on 11/9/2024, 4:57:50 PM

sh ip route

Press Cmd+Enter to send command Clear

Send

Showing response for 1 Devices

```
# terminal length 0

# sh ip route
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
       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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 10.10.6.33 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 10.10.6.33, GigabitEthernet1
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C     10.10.6.0/26 is directly connected, GigabitEthernet1
L     10.10.6.51/32 is directly connected, GigabitEthernet1
```

No Active Jobs

ASA and FTD RAVPN Monitoring

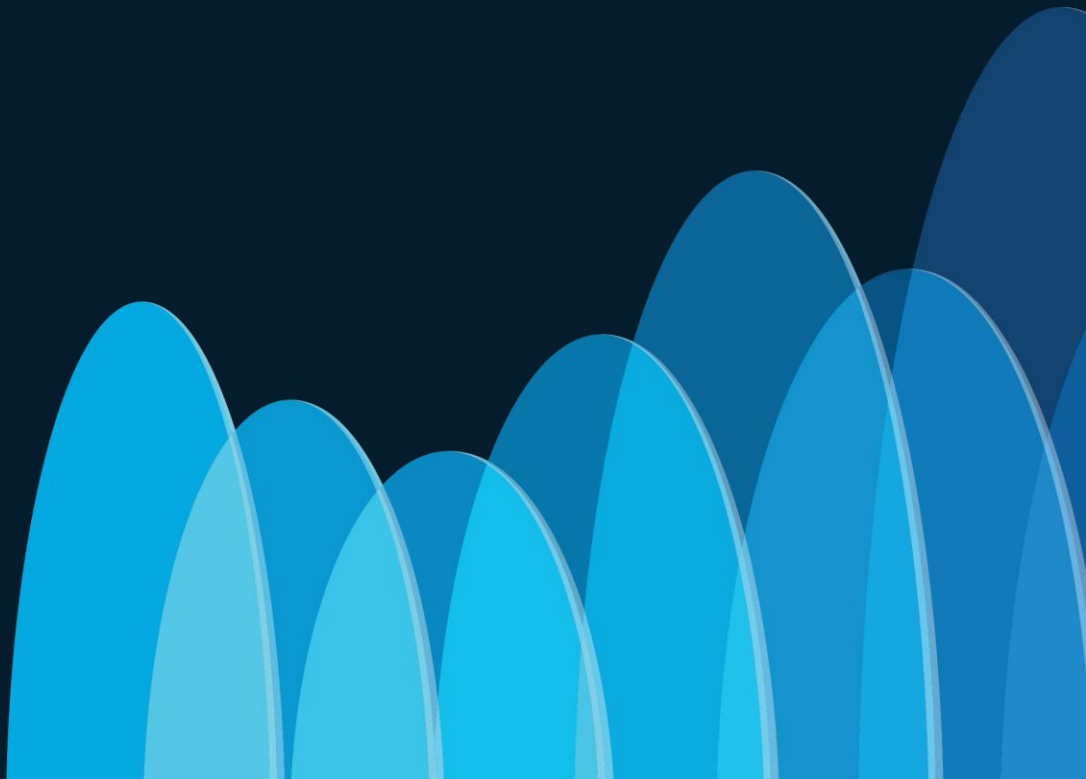
The screenshot displays the Cisco Security Cloud Control Remote Access Monitoring interface. The top navigation bar includes the Cisco logo, "Security Cloud Control", and "Remote Access Monitoring". A search bar is present with the placeholder text "Type 'Ctrl' + '/' to search". The interface is divided into a left sidebar with navigation options (Home, Multicloud Defense, Hypershield, Monitor, Insights & Reports, Events & Logs, Manage, Policies, Objects, Security Devices, Secure Connections, Administration) and a main content area. The main content area shows a table of active RAVPN sessions with columns for Username, Device Name, Assigned IP (v4), Assigned IP (v6), Public IP, Login Time, Duration, Data TX, Data RX, and Location. The table lists 18 sessions for users aaron.ramsdale, arsene.wenger, ben.white, bukayo.saka, cedric, and david.raya. The right sidebar displays user details for aaron.ramsdale, including Location (Ashburn, Virginia, United States), Connection Profile (ravpn-connection-profile), Group Policy (custom-ravpn-group-policy), Assigned IP (v4) (172.16.0.12), Assigned IP (v6) (34.228.89.40), Data Transmitted (11.64 KB), and Idle Timeout Left (60 Minutes). Below this, the Device Details section shows Device Name (Boston RAVPN Headend) and Security Type (ASA). The Actions section includes buttons for "Terminate session" and "Terminate all sessions on this device".

Username	Device Name	Assigned IP (v4)	Assigned IP (v6)	Public IP	Login Time	Duration	Data TX	Data RX	Location
aaron.ramsdale	Boston RAVPN H	172.16.0.12		34.228.89.40	18:00:09 11/06/21	1h:12m:9s	11.64 KB	-	Ashburn, Virginia, United States
aaron.ramsdale	Boston RAVPN H	172.16.0.212		34.228.89.40	18:20:08 11/06/21	0h:52m:10s	20.92 KB	-	Ashburn, Virginia, United States
aaron.ramsdale	Boston RAVPN H	172.16.0.218		34.228.89.40	19:00:09 11/06/21	0h:12m:9s	9.79 KB	-	Ashburn, Virginia, United States
arsene.wenger	Boston RAVPN H	172.16.0.220		34.228.89.40	18:00:19 11/06/21	1h:11m:59s	11.65 KB	-	Ashburn, Virginia, United States
arsene.wenger	Boston RAVPN H	172.16.0.246		34.228.89.40	19:00:20 11/06/21	0h:11m:58s	7.93 KB	-	Ashburn, Virginia, United States
arsene.wenger	Boston RAVPN H	172.16.0.214		34.228.89.40	18:20:19 11/06/21	0h:51m:59s	20.92 KB	-	Ashburn, Virginia, United States
ben.white	Boston RAVPN H	172.16.0.225		34.228.89.40	19:00:11 11/06/20	0h:12m:7s	9.79 KB	-	Ashburn, Virginia, United States
ben.white	Boston RAVPN H	172.16.0.85		34.228.89.40	18:00:11 11/06/20	1h:12m:7s	11.64 KB	-	Ashburn, Virginia, United States
ben.white	Boston RAVPN H	172.16.0.108		34.228.89.40	18:20:10 11/06/20	0h:52m:8s	20.92 KB	-	Ashburn, Virginia, United States
bukayo.saka	Boston RAVPN H	172.16.0.199		34.228.89.40	18:00:16 11/06/20	1h:12m:2s	11.65 KB	-	Ashburn, Virginia, United States
bukayo.saka	Boston RAVPN H	172.16.0.239		34.228.89.40	19:00:17 11/06/20	0h:12m:1s	9.79 KB	-	Ashburn, Virginia, United States
bukayo.saka	Boston RAVPN H	172.16.0.207		34.228.89.40	18:20:16 11/06/20	0h:52m:2s	20.92 KB	-	Ashburn, Virginia, United States
cedric	Boston RAVPN H	172.16.0.112		34.228.89.40	18:20:12 11/06/20	0h:52m:6s	20.92 KB	-	Ashburn, Virginia, United States
cedric	Boston RAVPN H	172.16.0.150		34.228.89.40	18:00:12 11/06/20	1h:12m:6s	11.65 KB	-	Ashburn, Virginia, United States
cedric	Boston RAVPN H	172.16.0.229		34.228.89.40	19:00:12 11/06/20	0h:12m:8s	9.79 KB	-	Ashburn, Virginia, United States
david.raya	Boston RAVPN H	172.16.0.55		34.228.89.40	18:00:09 11/06/21	1h:12m:9s	11.64 KB	-	Ashburn, Virginia, United States
david.raya	Boston RAVPN H	172.16.0.56		34.228.89.40	18:20:09 11/06/21	0h:52m:9s	20.9 KB	-	Ashburn, Virginia, United States

Right Sidebar Details for aaron.ramsdale:

- User Details**
 - Location: Ashburn, Virginia, United States
 - Connection Profile: ravpn-connection-profile
 - Group Policy: custom-ravpn-group-policy
 - Assigned IP (v4): 172.16.0.12
 - Assigned IP (v6): 34.228.89.40
 - Data Transmitted: 11.64 KB
 - Idle Timeout Left: 60 Minutes
- Device Details**
 - Device Name: Boston RAVPN Headend
 - Device Type: ASA
 - Security Group Tag: none
- Actions**
 - Terminate session
 - Terminate all sessions on this device

Devops



Security Cloud Control API

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

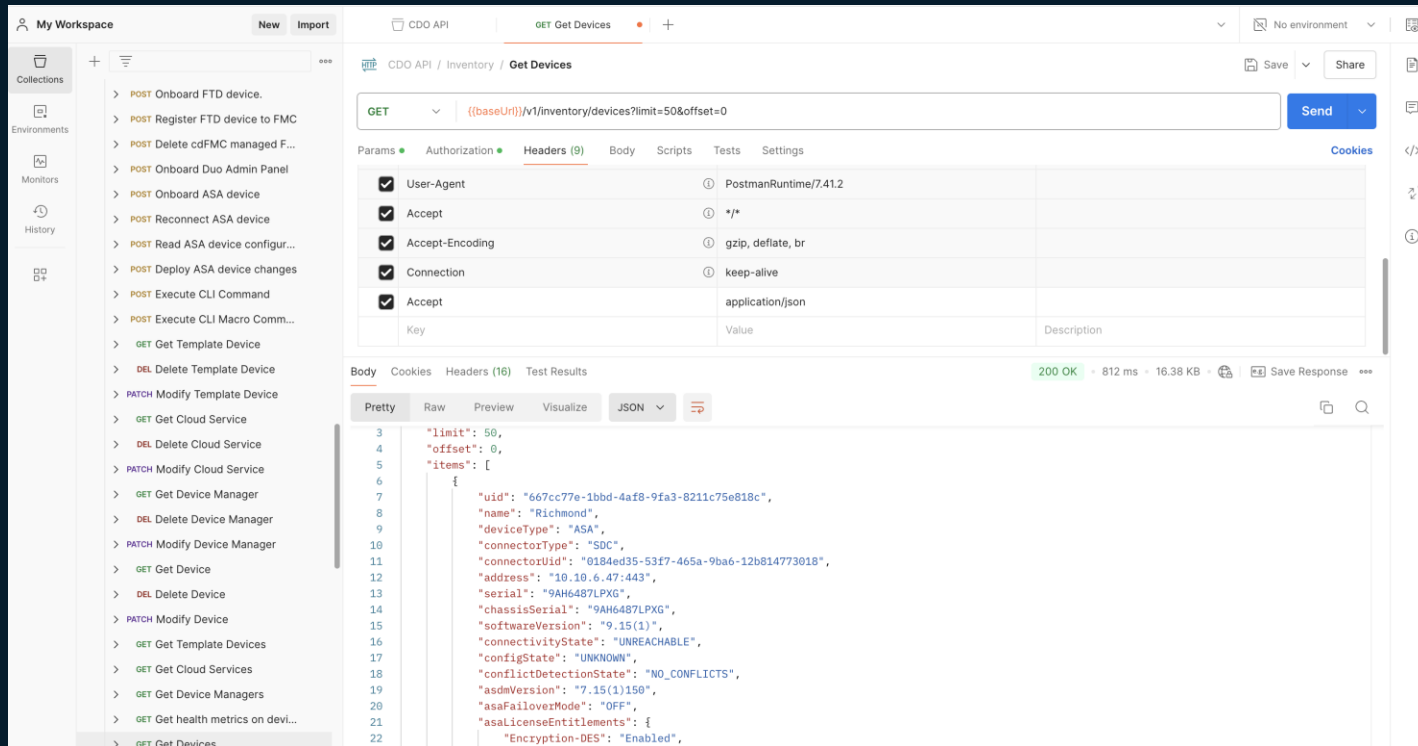
Cancel OK

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

- Public REST API
- Simple Bearer token authorization
- Single endpoint for both Security Cloud Control and cdFMC API calls

<https://developer.cisco.com/docs/cisco-security-cloud-control/>

Security Cloud Control Postman Collection



<https://developer.cisco.com/docs/cisco-security-cloud-control/postman-collection/>

Security Cloud Control SDK (Python)

cdo-sdk-python 1.2.97

✓ Latest version

Released: about 7 hours ago

`pip install cdo-sdk-python`

CDO API

Navigation

- Project description
- Release history
- Download files

Verified details (What is this?)

These details have been verified by PyPI

Maintainers

 cdo.ops

 talhaz114

Project description

Cisco Defense Orchestrator (CDO) Python SDK

The CDO Python SDK facilitates automated interaction with the Cisco Defense Orchestrator (CDO) API, enabling developers to integrate Cisco's cloud-based security policy and device management into Python applications.

For more information and detailed documentation, visit the [CDO Python SDK documentation](#).

Read more about CDO [here](#).

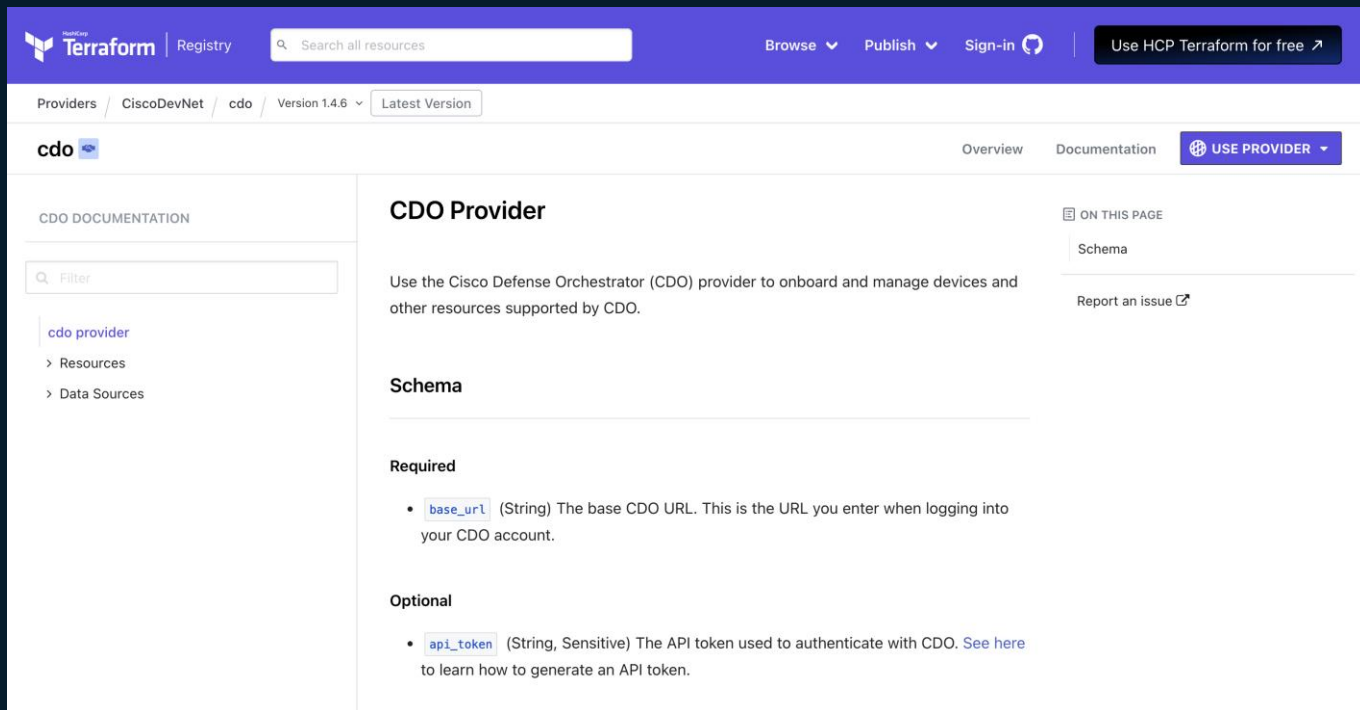
Installation

Install the CDO Python SDK package with the following command:

```
pip install cdo-sdk-python
```

<https://pypi.org/project/cdo-sdk-python/>

Security Cloud Control Terraform Provider



The screenshot shows the Terraform Registry page for the CiscoDevNet cdo provider. The page has a purple header with the Terraform logo, a search bar, and navigation links for Browse, Publish, and Sign-in. Below the header, the breadcrumb trail is Providers / CiscoDevNet / cdo / Version 1.4.6, with a button for the Latest Version. The main content area is titled 'cdo' and includes tabs for Overview and Documentation. A 'USE PROVIDER' button is visible. The left sidebar contains a search bar and a list of links: cdo provider, Resources, and Data Sources. The main content area is titled 'CDO Provider' and includes a description: 'Use the Cisco Defense Orchestrator (CDO) provider to onboard and manage devices and other resources supported by CDO.' Below this is a 'Schema' section with 'Required' and 'Optional' fields. The 'Required' field is 'base_url' (String) with a description: 'The base CDO URL. This is the URL you enter when logging into your CDO account.' The 'Optional' field is 'api_token' (String, Sensitive) with a description: 'The API token used to authenticate with CDO. See here to learn how to generate an API token.'

CDO Provider

Use the Cisco Defense Orchestrator (CDO) provider to onboard and manage devices and other resources supported by CDO.

Schema

Required

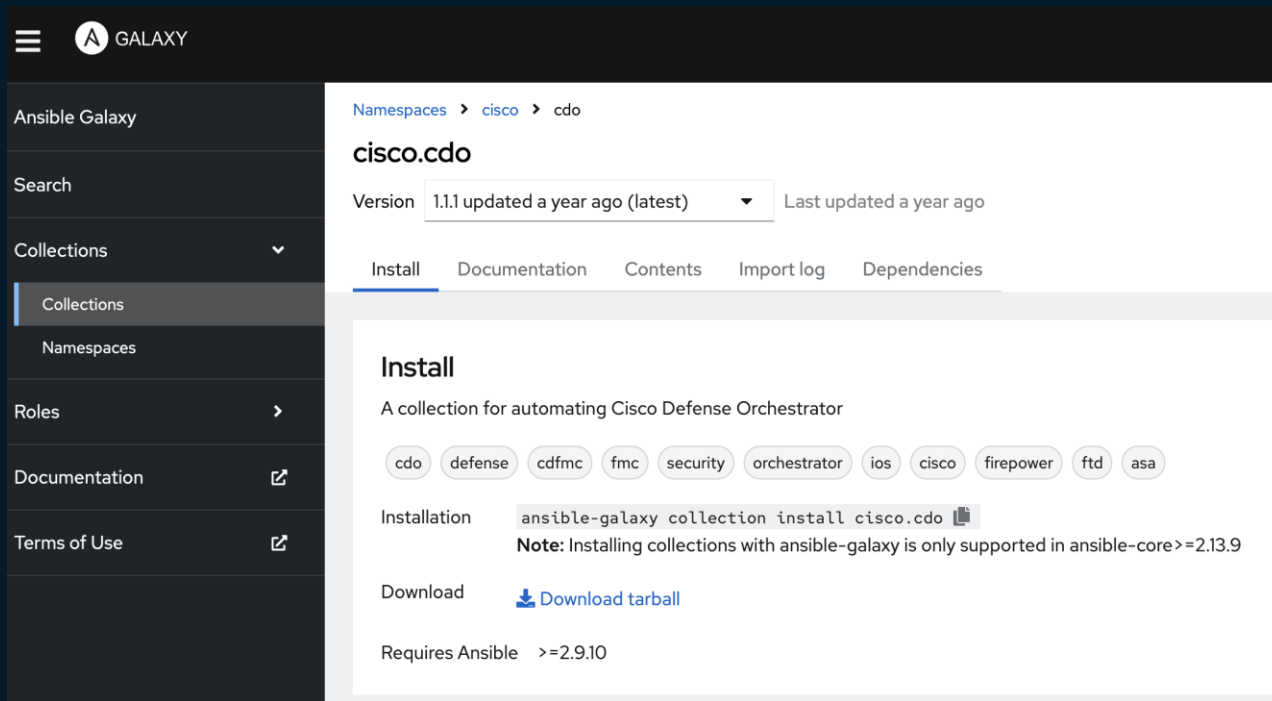
- `base_url` (String) The base CDO URL. This is the URL you enter when logging into your CDO account.

Optional

- `api_token` (String, Sensitive) The API token used to authenticate with CDO. [See here](#) to learn how to generate an API token.

<https://registry.terraform.io/providers/CiscoDevNet/cdo/latest/docs>

Security Cloud Control Ansible Collection (Under development)



The screenshot shows the Ansible Galaxy interface. On the left is a dark sidebar with navigation links: Ansible Galaxy, Search, Collections (selected), Namespaces, Roles, Documentation, and Terms of Use. The main content area is titled 'Namespaces > cisco > cdo' and 'cisco.cdo'. It shows the version '1.1.1 updated a year ago (latest)' and 'Last updated a year ago'. Below this are tabs for 'Install', 'Documentation', 'Contents', 'Import log', and 'Dependencies'. The 'Install' tab is active, displaying the title 'Install' and the description 'A collection for automating Cisco Defense Orchestrator'. Below the description are tags: cdo, defense, cdfmc, fmc, security, orchestrator, ios, cisco, firepower, ftd, and asa. The 'Installation' section shows the command 'ansible-galaxy collection install cisco.cdo' and a note: 'Note: Installing collections with ansible-galaxy is only supported in ansible-core >=2.13.9'. The 'Download' section has a 'Download tarball' link. The 'Requires Ansible' section shows '>=2.9.10'.

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

Security Cloud Control Devnet Learning Labs

The screenshot shows the Cisco DevNet Learning Labs interface. The top navigation bar includes the Cisco DevNet logo and 'Learning Labs Center'. The main title is 'Automating Cisco Defense Orchestrator using Terraform', with a duration of '120 mins'. The content area is divided into two columns. The left column contains text instructions for setting up the Terraform environment, including adding AWS credentials. The right column features a file explorer showing a directory structure with files like 'buildcheck.txt', 'Caddyfile', 'conf.sh', 'requirements.txt', '.bash_logout', '.bashrc', and '.profile'. Below the file explorer is a terminal window with the prompt 'developer:src >'.

cisco DevNet | Learning Labs Center

Automating Cisco Defense Orchestrator using Terraform

120 mins

This section explains how you can set up the Terraform environment by adding the required input variables to the `terraform.tfvars` file.

Add your AWS credentials to the environment

This Lab creates resources in your AWS environment. We use the [Terraform AWS Provider](#), which expects AWS credentials. There are multiple ways in which we can provide credentials to configure the provider (see the [provider docs](#)); in this section, we describe how to set the credentials in environment variables.

As a first step, you must [create an IAM account](#) in your AWS account.

Set the following two environment variables:

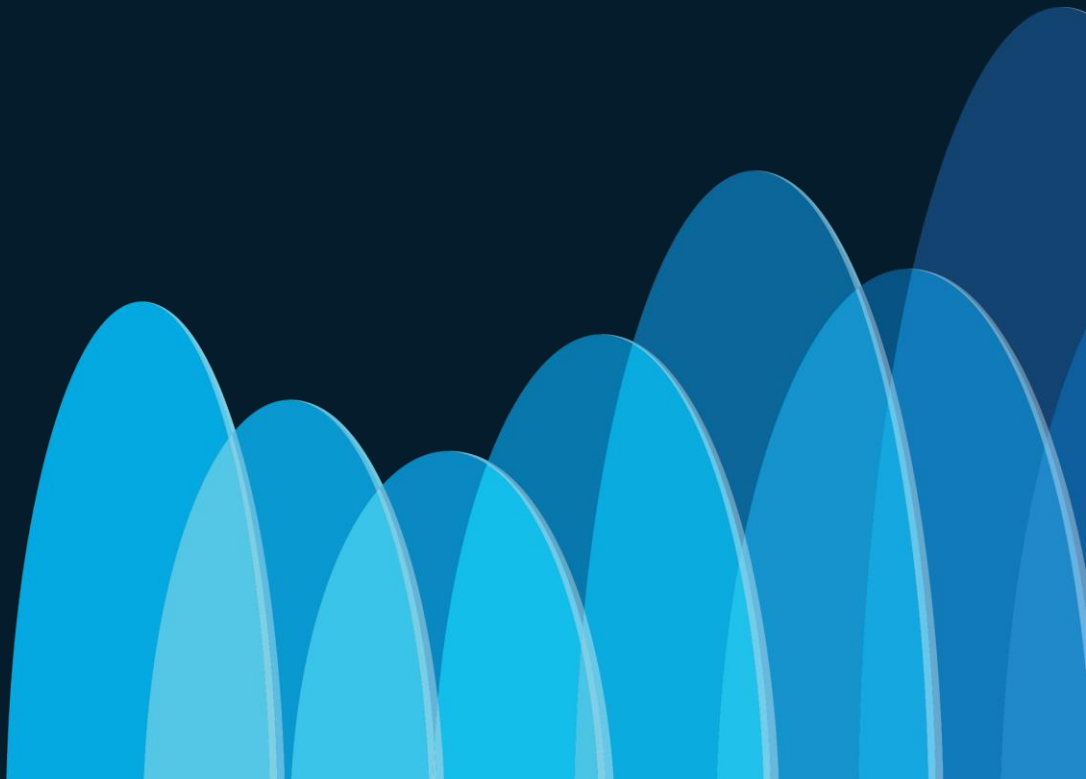
- `AWS_ACCESS_KEY_ID` : Specifies an AWS access key that is associated with an IAM account.
- `AWS_SECRET_ACCESS_KEY` : Specifies the secret key that is associated with the access key. This is essentially the "password" for the access key.

Run the following commands on the in-browser terminal:

```
export AWS_ACCESS_KEY_ID=<your-aws-access-key>
export AWS_SECRET_ACCESS_KEY=<your-aws-secret-access-key>
```

Optional: Using temporary AWS credentials for extra

Wrap-Up



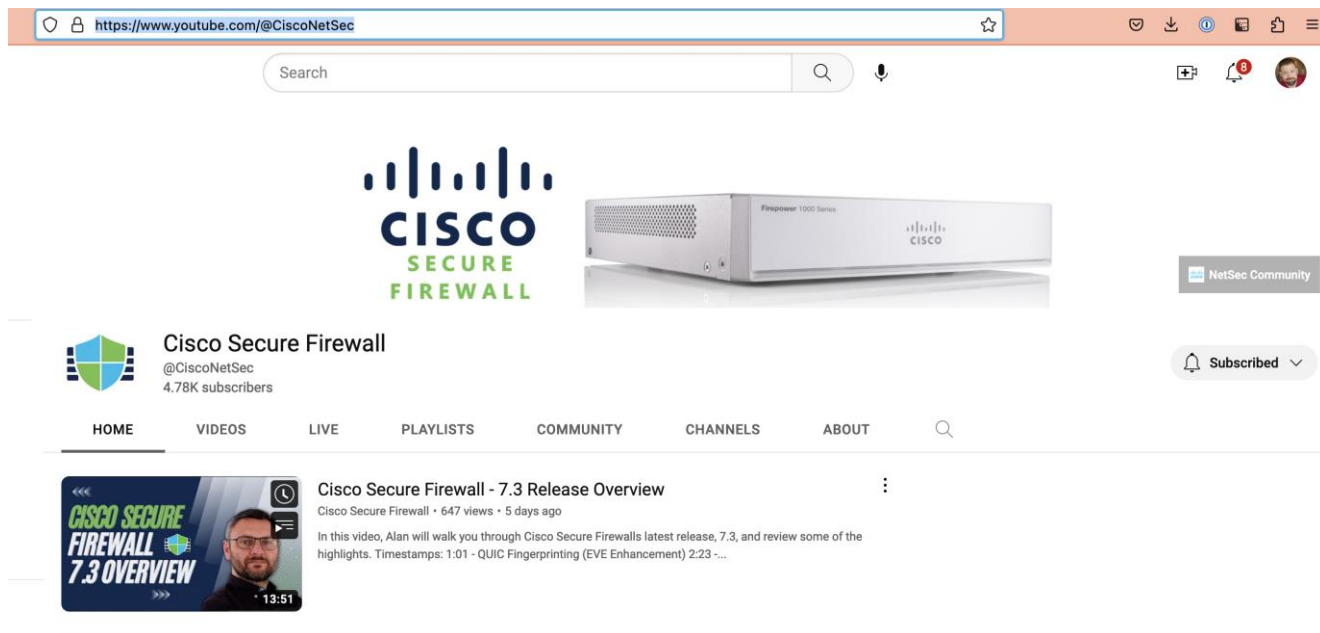
Key Takeaways

- Centralized, Cloud-Managed Security Solution
- Better Operational Efficiency and Scalability using AI Assistant
- Enhanced Security Posture with Simplified Management
- Data-Driven Insights and Continuous Improvement leveraging AIOps
- Automated Updates and Rapid Feature Deployment

Cisco Secure Firewall YouTube Channel

[Cisco Secure Firewall YouTube Channel](#)

[Security Cloud Control Playlist on Cisco Secure Firewall YouTube Channel](#)



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 Cisco Firepower 1000 Series firewall unit. The channel name is "Cisco Secure Firewall" with the handle "@CiscoNetSec" and 4.78K subscribers. A "Subscribed" button is visible. The navigation menu includes Home, Videos, Live, Playlists, Community, Channels, and About. The featured video is "Cisco Secure Firewall - 7.3 Release Overview" by Cisco Secure Firewall, with 647 views and 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 -...".

FULL CONFERENCE

IT LEADERSHIP

FULL CONFERENCE PLUS

Cisco Hypershield: a New Era of AI-Native Security for Data Centers and Cloud [BRKSEC-1501]



Schedule

Wednesday, Nov 13 | 4:15 PM - 5:45 PM AEDT | Room 207

Aamer Akhter, Sr. Director, Product Management, Cisco



FULL CONFERENCE

IT LEADERSHIP

FULL CONFERENCE PLUS

Intelligent Security for the Hybrid Cloud and Multi-cloud [BRKSEC-2581]



Schedule

Wednesday, Nov 13 | 1:00 PM - 2:30 PM AEDT | Room 212

Eric Kostlan, Technical Marketing Engineer, Cisco



Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education

- Visit the Cisco Stand 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

Contact me at: **Insert preferred comms method**



Thank you



#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC