What's New for Cisco Defense Orchestrator

First Published: 2021-04-16

Last Modified: 2024-04-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

PART I

New Features in Cisco Defense Orchestrator

CHAPTER 1

New Features in 2024

This chapter describes some of the features that were added to Cisco Defense Orchestrator in 2024.

April 2024

April 25, 2024

Dark Theme in CDO

CDO now offers a Dark theme option for a more customizable user interface look. Click the admin drop-down on the top right corner, navigate to **Settings** > **General Settings** > **User Settings**, and click **Dark** in the **Theme** field. The default theme is the Light theme.

See User Settings for more information.

April 18, 2024

Automatically Synchronize Network Objects to On-Prem Secure Firewall Management Centers

You can now automatically and continuously synchronize your network objects in CDO to On-Prem FMCs managed by CDO. Note that this feature is disabled by default. To enable this feature, navigate to **Tools & Services**, select an On-Prem FMC, and choose **Settings** > **Enable automatic sync of network objects**.

See Discover and Manage On-Prem Firewall Management Center Network Objects for more information.

March 2024

March 07, 2024

Improved CDO Tenant Provisioning

You can now create a CDO tenant using an enhanced, faster provisioning process. You can also create new CDO tenants even if you already have tenants. In addition, if you have an On-Prem Firewall Management Center that is not SecureX-enabled, you can now register it to the Cisco Security Cloud through CDO. If you do not have a CDO account, you can create one during the registration process. See Create a CDO Tenant for more information.

Disable Individual Threat Defense Devices From Sending Event Logs to the Cisco Cloud

You can now disable individual cloud-delivered Firewall Management Center-managed threat defense devices (Version 7.4.1 or later) from sending event logs to the Cisco cloud. This device-level control allows you to temporarily stop threat defense devices from sending event logs sent to the cloud, if required. To specify which threat defense devices are to be disabled from sending event logs to the Cisco cloud, click **Inventory**, select the corresponding threat defense devices, and click **Cloud Events** from the **Device Management** pane.

Simplified Secure Device Connector and Secure Event Connector Installation on Ubuntu

You can now easily deploy Secure Device Connector and Secure Event Connector on Ubuntu server using the GitHub project available on the Cisco DevNet site. For more information, refer to this document and watch this video on YouTube.

February 2024

February 13, 2024

Updates to Cloud-Delivered Firewall Management Center

Cisco Defense Orchestrator released an update to the cloud-delivered Firewall Management Center. Read the Release Notes for Cloud-delivered Firewall Management Center to learn about the many new features included in the update.

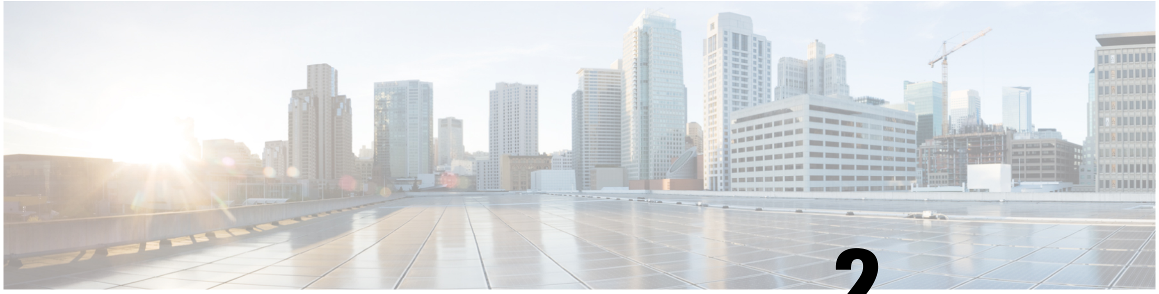
January 2024

January 25, 2024

Updates to Firewall Migration Tool

CDO now hosts an updated version of the Firewall Migration Tool. You can now migrate WebVPN configurations from your Secure Firewall ASA devices to Zero Trust Access Policy configurations on threat defense devices managed by the cloud-delivered Firewall Management Center. You can also migrate SNMP, DHCP, DVTI configurations from ASAs to threat defense devices and ECMP routing configurations when migrating from a multi-context ASA device to a single-instance threat defense device. Read the Cisco Secure Firewall Migration Tool Release Notes to know about the other new features included in the release.

January 25, 2024



CHAPTER 2

Feature Highlights of 2023

This chapter describes some of the features that were added to Cisco Defense Orchestrator in 2023.

December 2023

December 14, 2023

Monitor Additional Event Types for Threat Defense Devices

CDO now supports new firewall event types such as AAA, BotNet, Failover, and SSL VPN for threat defense devices.

Navigate **Analytics** > **Event Logging** and filter from the new list of events available under **FTD Events**. See Event Types in CDO for more information.

December 07, 2023

Manage On-Prem Firewall Management Center Network Objects Using CDO

You can now manage and share network objects from a CDO-managed On-Prem Firewall Management Center to threat defense devices managed by other On-Prem Firewall Management Centers, the cloud-delivered Firewall Management Center, and to CDO-managed ASA and threat defense devices. This helps promote consistency in network object definitions across platforms managed by CDO.

After onboarding an On-Prem Firewall Management Center, navigate **Tools & Services** > **Firewall Management Center**, select the device and choose **Settings**, and enable the **Discover & Manage Network Objects** toggle button.

See Discover and Manage On-Prem Firewall Management Center Network Objects for more information.

November 2023

November 30, 2023

Schedule a Secure Firewall Threat Defense Device Backup in Cloud-delivered Firewall Management Center

Use the cloud-delivered Firewall Management Center to perform scheduled backups of the Secure Firewall Threat Defense devices it manages.

See Schedule Remote Device Backups for more information.

November 14, 2023

Improved Cloud-Delivered Firewall Management Center Provisioning

CDO now provides an enhanced, faster provisioning process for cloud-delivered Firewall Management Center. When you enable the cloud-delivered Firewall Management Center on your tenant, CDO provisions it automatically and notifies you through the CDO notifications center and the applications in which you have configured incoming webhooks. To enable it, navigate **Tools & Services** > **Firewall Management Center** > + > **FMC** > **Enable Cloud-Delivered FMC**.

See Enable Cloud-delivered Firewall Management Center on Your CDO Tenant and Notification Settings for more information.

November 2, 2023

Onboard a Threat Defense Device to an On-Prem Management Center with Low-Touch Provisioning

You can now select an On-Prem Firewall Management Center as the managing platform when you onboard a threat defense device with the low-touch provisioning method. This supports on-prem management for new devices or devices that have not been previously configured or managed. See Onboard a Secure Firewall Threat Defense Device With Low-Touch Provisioning for more information.

October 2023

October 26, 2023

Updates to Firewall Migration Tool

CDO hosts an updated version of the Firewall Migration Tool. Using this, you can merge multiple transparent firewall-mode contexts that are present in your Secure Firewall ASA devices into a transparent-mode instance and migrate them.

In addition, you can migrate the site-to-site and remote access VPN configurations from your Fortinet and Palo Alto Networks firewalls to the threat defense devices managed by Cisco's cloud-delivered Firewall Management Center. See the Secure Firewall Migration Tool Release Notes for more information.

October 19, 2023

Updates to Cloud-Delivered Firewall Management Center

Cisco Defense Orchestrator released an update to the cloud-delivered Firewall Management Center. Read the release notes for cloud-delivered Firewall Management Center to learn about the many new features included in the update. See the Release Notes for Cloud-delivered Firewall Management Center: A Feature of Cisco Defense Orchestratorfor a complete list of the new features.

Migrate Secure Firewall Threat Defense Devices with Site-to-Site VPN Configurations from On-Prem to Cloud-Delivered Firewall Management Center

Site-to-site VPN configurations on Secure Firewall Threat Defense devices are now migrated along with the rest of the configuration when the device is migrated from the on-prem Firewall Management Center to the cloud-delivered Firewall Management Center. See Migrate On-Prem Management Center managed Secure Firewall Threat Defense to Cloud-delivered Firewall Management Center for more information.

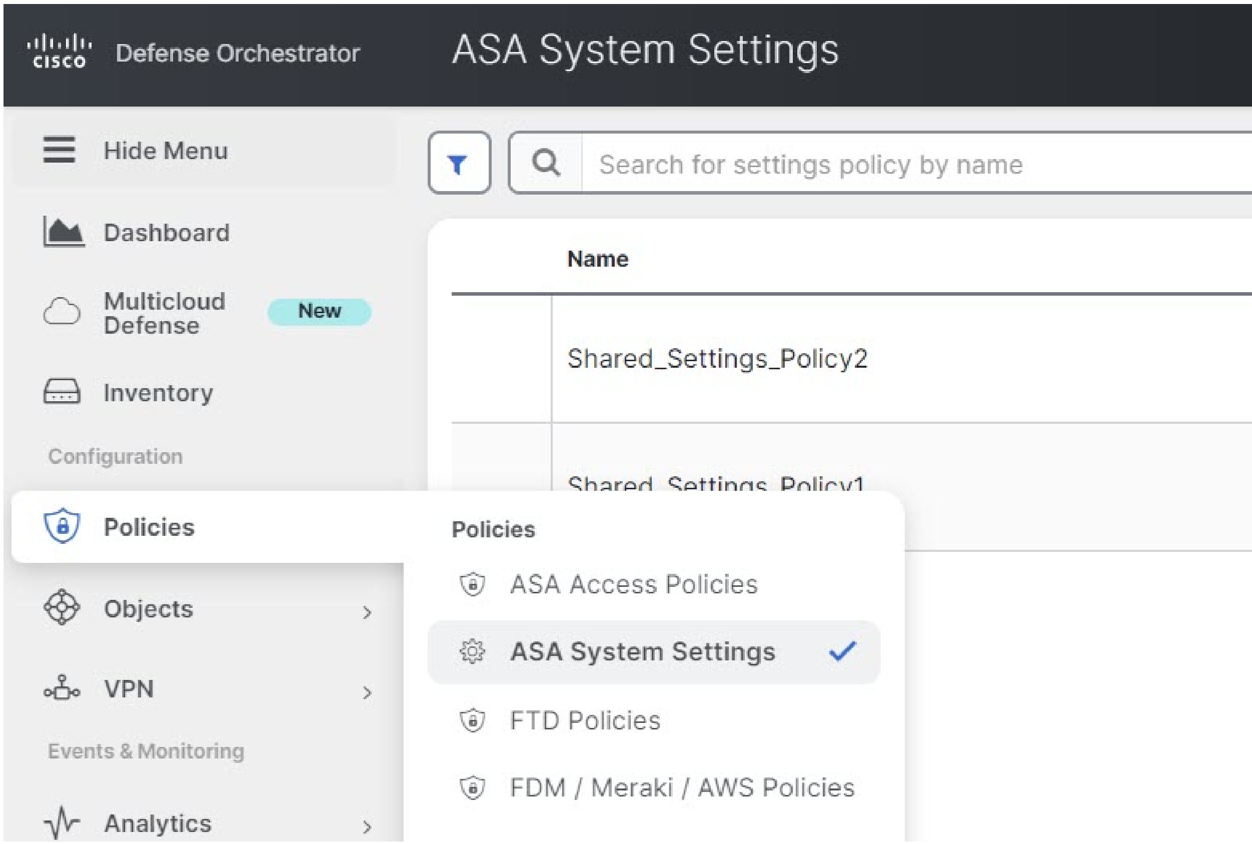
October 12, 2023

ASA System Settings Policy

CDO provides the ability to create a system settings policy to effortlessly manage essential configurations for ASA devices such as domain name services, HTTP, enabling the secure copy server, message logging, and allowing VPN traffic without checking access control lists. You can apply this policy to multiple ASA devices, and any change made to the policy affects all devices using this policy. Additionally, you can individually edit device-specific settings for a single ASA device and override the shared system settings with device-specific values.

See ASA System Settings for more information.

Choose **Policies** > **ASA System Settings**.



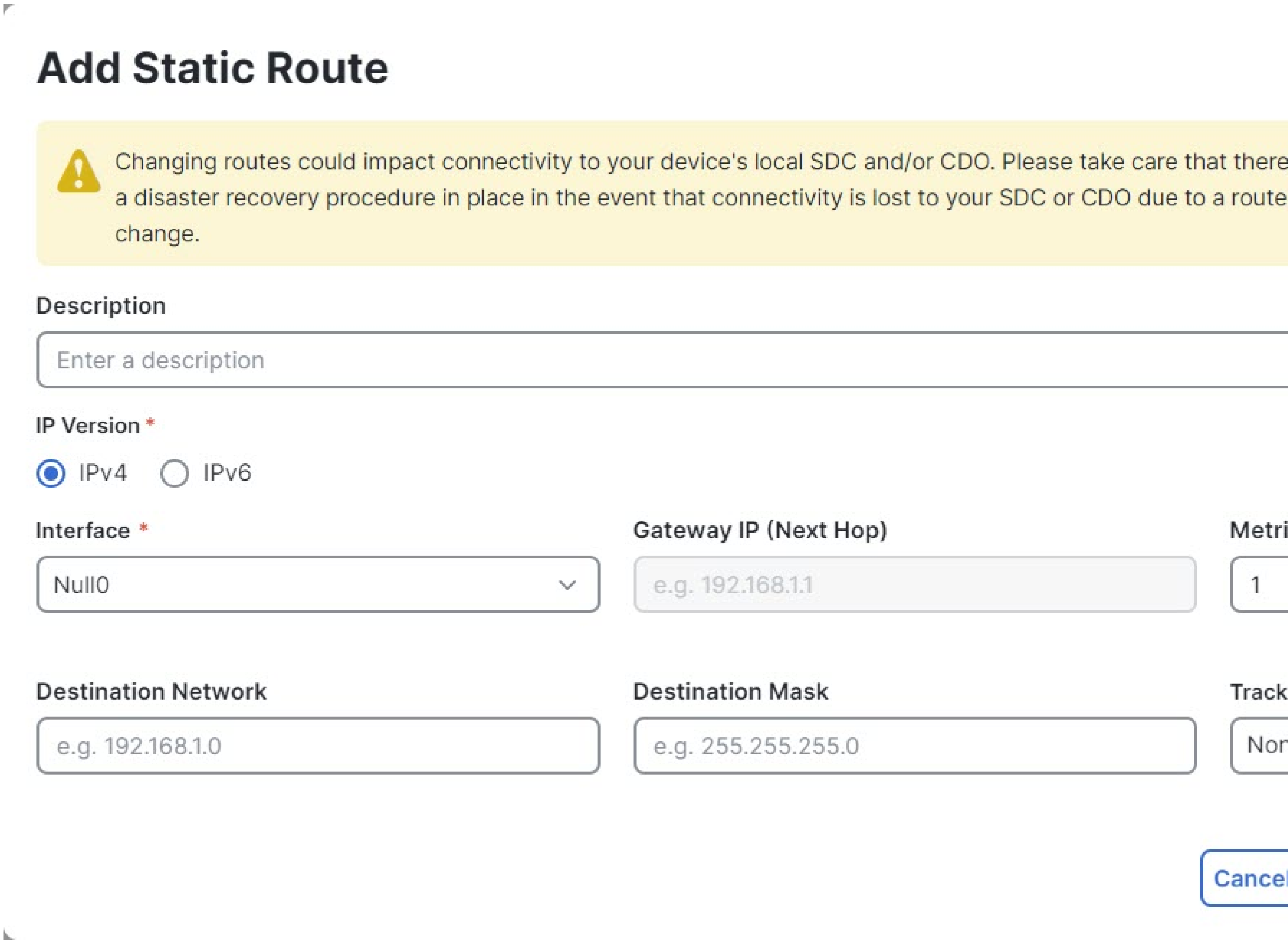
October 05, 2023

CDO Support for ASA Static Routing

You can now use the CDO user interface to configure static routes for the ASA. This feature lets you specify where to send traffic for specific IPv4 or IPv6 destination networks without having to use the CLI.

See ASA Static Routing for more information.

Inventory > **ASA** tab > **Routing**.



Add Static Route

Changing routes could impact connectivity to your device's local SDC and/or CDO. Please take care that there
a disaster recovery procedure in place in the event that connectivity is lost to your SDC or CDO due to a route
change.

Description

Enter a description

IP Version *

● IPv4 ○ IPv6

Interface *

Null0

Gateway IP (Next Hop)

e.g. 192.168.1.1

Metri

1

Destination Network

e.g. 192.168.1.0

Destination Mask

e.g. 255.255.255.0

Track

Non

Manage CDO Using Terraform

You can now use Terraform to automate the management of your CDO infrastructure using Infrastructure as Code (IaC) principles. CDO now provides a Terraform provider and Terraform modules to quickly deploy secure device connectors and secure event connetors. See Terraform for more information.

September 2023

September 14, 2023

Navigation Change for Secure Event Connectors

You can no longer access the Secure Connectors page by expanding the admin menu in the top right. To manage Secure Connectors, navigate to **Tools & Services** > **Secure Connectors**. See Secure Event Connectors for more information.

September 7, 2023

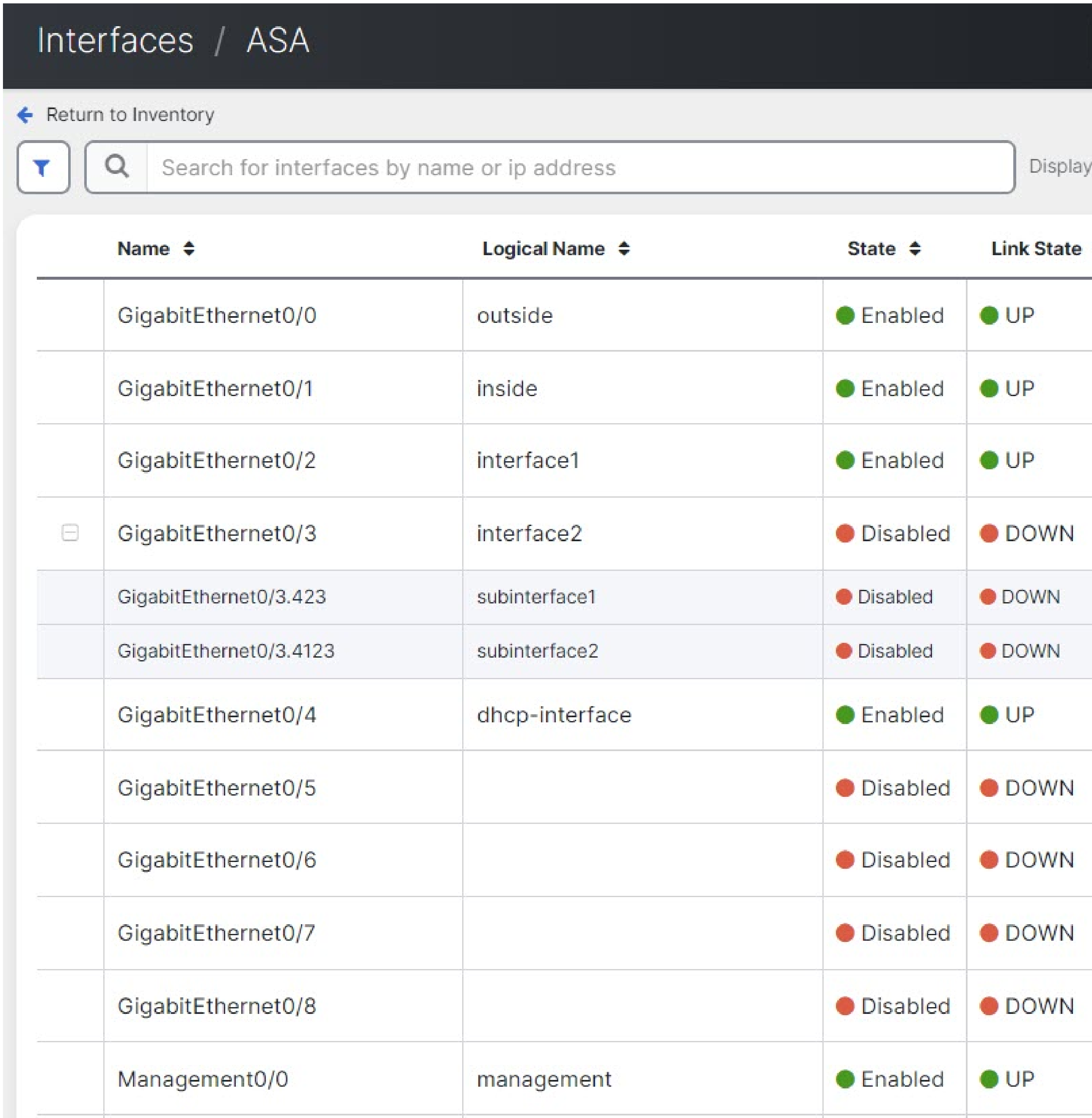
Configure ASA Interfaces using CDO User Interface

You can now configure ASA's physical network interfaces, logical subinterfaces, VLAN, and EtherChannels using a graphical user interface in CDO. You can also view Virtual Tunnel Interfaces that are created during route-based site-to-site VPN.

Note VLAN is only supported for 110 devices.

See Configure ASA Interfaces for more information.

Inventory > **ASA** > **Management** > **Interfaces**.



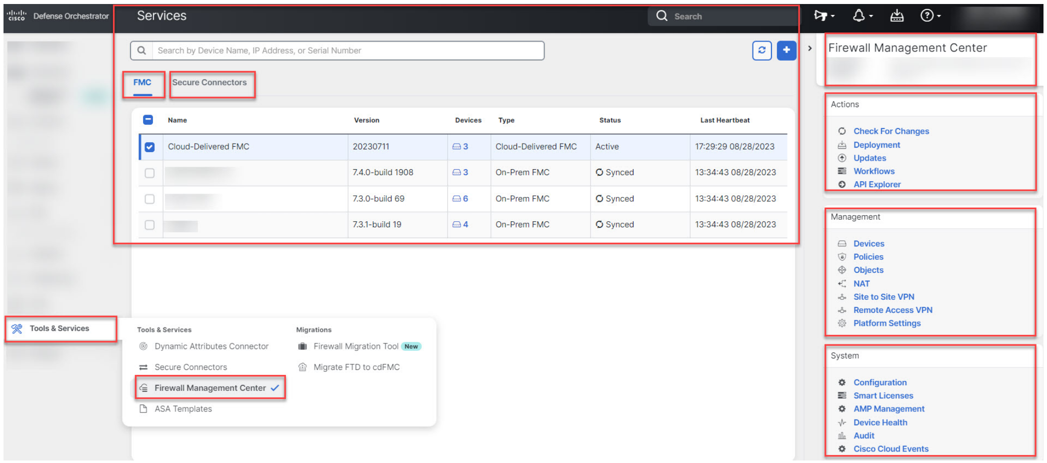
	Name	Logical Name	State	Link State
	GigabitEthernet0/0	outside	● Enabled	● UP
	GigabitEthernet0/1	inside	● Enabled	● UP
	GigabitEthernet0/2	interface1	● Enabled	● UP
⊟	GigabitEthernet0/3	interface2	● Disabled	● DOWN
	GigabitEthernet0/3.423	subinterface1	● Disabled	● DOWN
	GigabitEthernet0/3.4123	subinterface2	● Disabled	● DOWN
	GigabitEthernet0/4	dhcp-interface	● Enabled	● UP
	GigabitEthernet0/5		● Disabled	● DOWN
	GigabitEthernet0/6		● Disabled	● DOWN
	GigabitEthernet0/7		● Disabled	● DOWN
	GigabitEthernet0/8		● Disabled	● DOWN
	Management0/0	management	● Enabled	● UP

August 2023

August 31, 2023

Manage Your Cloud-Delivered FMC, On-Prem FMCs, and Secure Connectors from the Services Page

You can now manage your cloud-delivered Firewall Management Center, On-Prem Firewall Management Centers, and secure connectors from the new **Services** page. Choose **Tools & Services** > **Firewall Management Center** or **Secure Connectors**. Refer View Services Page Information to know more.

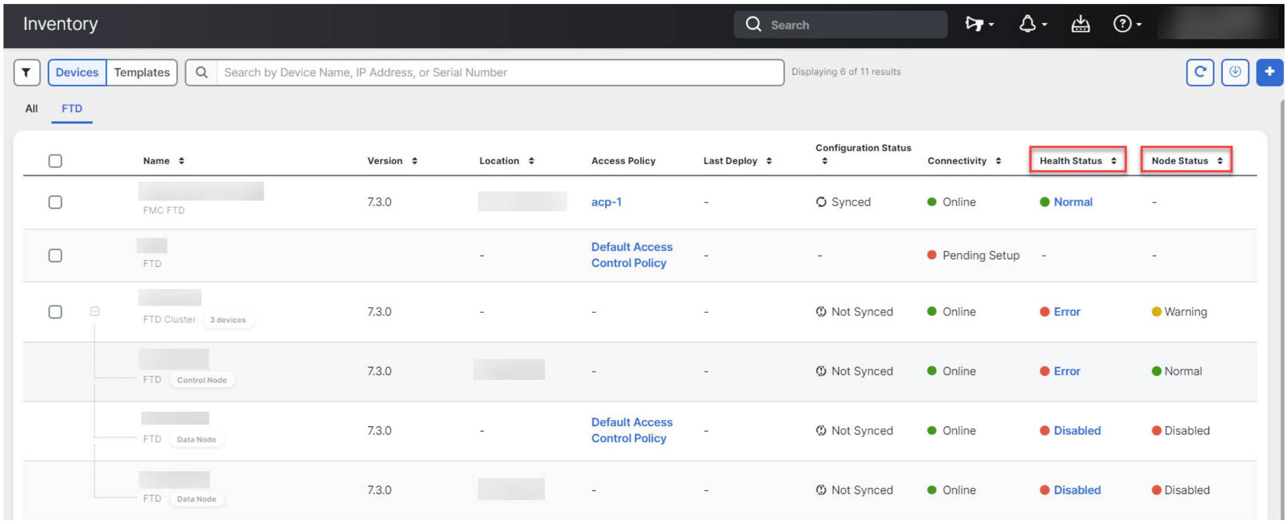


☐	Name	Version	Devices	Type	Status	Last Heartbeat
☑	Cloud-Delivered FMC	20230711	3	Cloud-Delivered FMC	Active	17:29:29 08/28/2023
☐	[redacted]	7.4.0-build 1908	3	On-Prem FMC	Synced	13:34:43 08/28/2023
☐	[redacted]	7.3.0-build 69	6	On-Prem FMC	Synced	13:34:43 08/28/2023
☐	[redacted]	7.3.1-build 19	4	On-Prem FMC	Synced	13:34:43 08/28/2023

August 17, 2023

Know the Health Status of Your Threat Defense Devices

CDO now displays the health and node status for threat defense devices on the Inventory page. For more details about the device health, you can click on the health status of a device to navigate to the device's health monitoring page in the cloud-delivered Firewall Management Center or the On-Prem Firewall Management Center user interface. Note that node status is displayed only for threat defense devices managed by cloud-delivered Firewall Management Center.



Inventory
Search
Devices
Templates
Search by Device Name, IP Address, or Serial Number
Displaying 6 of 11 results
All
FTD

☐	Name	Version	Location	Access Policy	Last Deploy	Configuration Status	Connectivity	Health Status	Node Status
☐	FMC FTD	7.3.0		acp-1	-	Synced	● Online	● Normal	-
☐	FTD		-	Default Access Control Policy	-	-	● Pending Setup	-	-
☐	FTD Cluster 3 devices	7.3.0	-	-	-	Not Synced	● Online	● Error	● Warning
	FTD Control Node	7.3.0		-	-	Not Synced	● Online	● Error	● Normal
	FTD Data Node	7.3.0	-	Default Access Control Policy	-	Not Synced	● Online	● Disabled	● Disabled
	FTD Data Node	7.3.0		-	-	Not Synced	● Online	● Disabled	● Disabled

For more information, see Managing On-Prem FMC with Cisco Defense Orchestrator and Managing Cisco Secure Firewall Threat Defense Devices with Cloud-delivered Firewall Management Center.

August 3, 2023

Updates to Firewall Migration Tool

Cisco Defense Orchestrator now hosts an updated version of the Firewall Migration Tool. You can now merge multiple contexts in your Secure Firewall ASA devices to a routed-mode instance and migrate them to threat defense devices managed by the cloud-delivered Firewall Management Center. In addition, the migration tool now leverages the virtual routing and forwarding (VRF) functionality to replicate the segregated traffic flow observed in a multi-context ASA environment, which will be part of the new merged configuration.

See Migrating Secure Firewall ASA Managed by CDO in *Migrating Firewalls with the Firewall Migration Tool in Cisco Defense Orchestrator* guide for more information.

July 2023

July 20, 2023

EasyDeploy for Virtual Threat Defense Devices Managed by GCP

You can now create a virtual threat defense device and deploy it to a Google Cloud Platform (GCP) project simultaneously. The EasyDeploy method combines the steps required to create a new virtual device and then associating the device with the cloud environment, streamlining the procedure and minimizing the amount of time required for setup.

Note that you **must** have cloud-delivered Firewall Management Center enabled for these onboarding flows. See Deploy a Threat Defense Device to Google Cloud Platform for more information.

July 13, 2023

Open CDO and Cloud-delivered Firewall Management Center Portals on Different Browser Tabs

You can now open CDO and cloud-delivered Firewall Management Center portal pages in different browser tabs and simultaneously work in both CDO and cloud-delivered Firewall Management Center.

See Support to Open CDO and Cloud-delivered Firewall Management Center Applications on Different Tabs for more information.

June 2023

June 29, 2023

Schedule a Background Search in the Event Viewer

You can now run a background search in the Event Viewer on a re-occurring schedule. The schedule supports absolute time (ex May 1 to May 5th) or a sliding window (ex "The last day").

See Schedule a Background Search in the Event Viewer for more information.

Support for New Event Attributes

Now, Security Group, Encrypted Visibility Process Confidence Score, Encrypted Visibility Threat Confidence, Encrypted Visibility Threat Confidence Score, Encrypted Visibility Fingerprint are supported syslog event attributes in CDO's event viewer. When you customize your event logging view you can create a column for any of these newly supported attributes.

June 15, 2023

Migrate Your Firewalls using the Firewall Migration Tool in CDO

You can now migrate configurations from your Secure Firewall ASA devices, FDM-managed threat defense devices, and third-party firewalls such as Check Point, Palo Alto Networks, and Fortinet firewalls to the cloud-delivered Firewall Management Center using the Firewall Migration Tool in Cisco Defense Orchestrator. See Migrating Firewalls with the Firewall Migration Tool in Cisco Defense Orchestrator guide for more information.

June 8, 2023

EasyDeploy for Virtual Threat Defense Devices Managed by AWS and Azure

You can now create a virtual threat defense device and deploy it to an Amazon Web Services (AWS) or Azure environment simultaneously. The easydeploy method combines the steps required to create a new virtual device and then associating the device with the cloud environment, streamlining the procedure and minimizing the amount of time required for setup.

Note that you **must** have cloud-delivered Firewall Management Center enabled for these onboarding flows. See Deploy a Threat Defense Device with AWS and Deploy a Threat Defense Device with an Azure VNet respectively for more information.

June 5, 2023

CDO Introduces the Multicloud Defense Solution

Multicloud Defense Solution specializes in security policy orchestration and protection of cloud network traffic, and cloud applications and workloads. It delivers unified security policies and web protection across multiple cloud types, provides network visibility into your cloud assets, and integrates services like threat intelligence and external logging. It enforces ingress traffic to, and egress traffic from, your cloud account, as well as the "east-west" network traffic within your cloud account.

Multicloud Defense Solution currently supports AWS, Azure, Google Cloud Platform, and Oracle OCI cloud accounts.

See About Multicloud Defense for more information, and Multicloud Defense 90-Day Free Trial to try out the Multicloud Defense Solution.

June 1, 2023

Auto Discovery of On-Prem Secure Firewall Management Centers with SecureXIntegration

CDO now has the ability to onboard all the on-prem management centers associated with the SecureX tenant that is linked to your CDO account. It also onboards the Secure Firewall Threat Defense devices linked to those on-prem management centers. See Auto Onboard an On-Prem Firewall Management Center with SecureX for more information.

April 2023

April 27, 2023

Improved Event Filtering

You can now filter events further with a relative time range. Absolute time range is an explicitly stated time frame. An example of a relative time range is `last 3 days` or `last 3 hours`. This can help target traffic and events that may not necessarily be included in an absolute time range. See Search for Events in the Events Logging Page for more information.

March 2023

March 23, 2023

Background Search for Event Logging

CDO provides you the ability to define a search criteria and search for events in event logs based on any defined search criteria. Using the background search capability, you can perform event log searches in the background, and view the search results once the background search is completed.

Based on the subscription alert and service integrations you have configured, you can be notified once the background search has been completed. Learn more about background searches used with event logging.

January 2023

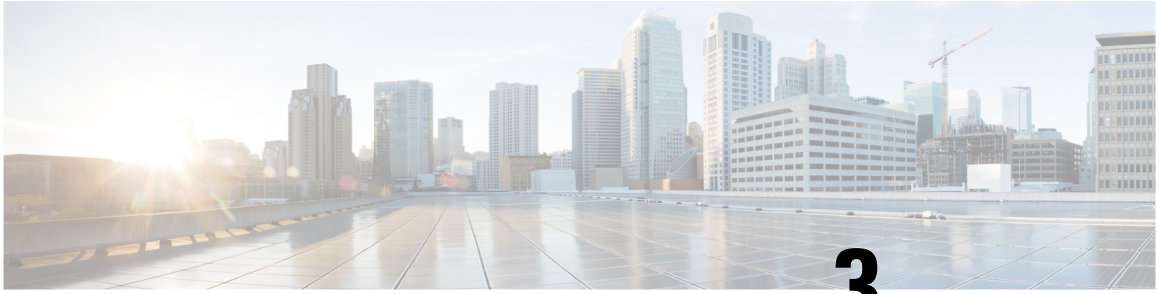
January 18, 2023

Monitor Remote Access VPN Sessions of FTDs

CDO can now monitor Remote Access VPN sessions of FTDs managed using the cloud-delivered Firewall Management Center in CDO.

The RA VPN monitoring page provides the following information:

- A list of active and historical sessions.
- The details of the device and user associated with each session.



CHAPTER 3

Feature Highlights of 2022

This chapter describes some of the features that were added to Cisco Defense Orchestrator in 2022.

December 2022

December 15, 2022

Cisco Defense Orchestrator released an update to the cloud-delivered Firewall Management Center. Read the release notes for cloud-delivered Firewall Management Center to learn about new features included in the update.

December 1, 2022

Route Based Site-to-Site VPN Support for ASA

Using Cisco Defense Orchestrator, you can now create a site-to-site VPN tunnel between peers with Virtual Tunnel Interfaces configured. This supports route based VPN with IPsec profiles attached to the end of each tunnel. Any traffic routed into the IPSec tunnel is encrypted regardless of the source/destination subnet.

VTI-based VPNs can be created between:

- A CDO-managed ASA and any route-based VPN-capable device.
- Two CDO-managed ASAs.

See Site-to-Site Virtual Private Network for more information.

Global Search

The global search feature in CDO allows you to search for and navigate to devices managed by CDO. This feature now supports the search capability for devices that are managed in cloud-delivered Firewall Management Center from the CDO user interface. From the search results, you can navigate to the corresponding pages in cloud-delivered Firewall Management Center.

See Global Search for more information.

October 2022

October 27, 2022

Duo Admin Panel Onboarding and Multi-Factor Authentication Logging

CDO can now onboard the Duo Admin Panel and show the logs as MFA events in the dashboard and tabular forms. You can also export the MFA sessions of one or more devices to a file containing a comma-separated value (.csv).

The Duo Admin Panel records a Multi-Factor Authentication (MFA) log containing information on whether the user's two-factor authentication has passed or failed.

See "Onboard Duo Admin Panel" and "Monitor Multi-Factor Authentication Events" in Cisco Defense Orchestrator Guide for more information.

October 12, 2022

Policy-Based Site-to-Site VPN Wizard for ASA

CDO now allows configuring a policy-based site-to-site VPN tunnel between two peers. This means that any traffic routed into the IPSec tunnel is encrypted regardless of the source/destination subnet.

To configure a policy-based site-to-site VPN, one of the following conditions must be met:

- Both peers are CDO-managed ASAs.
- One of the peers is a CDO-managed ASA and the other is any policy-based VPN capable device.

See Site-to-Site Virtual Private Network for more information.

August 2022

August 4, 2022

CDO Support for FDM-Managed Devices, Version 7.2

CDO now supports version 7.2 for FDM-managed devices. These are the aspects of support CDO provides:

- Onboard a supported physical or virtual FDM-managed devices running version 7.2 to CDO.

- Upgrade FDM-managed devices from versions 6.4+ to version 7.2.
- Support for existing Secure Firewall Threat Defense features.
- Onboard a supported physical or virtual device running version 7.2 to cloud-delivered Firewall Management Center.

Note CDO does not support features introduced in the version 7.2 release.

June 2022

June 30, 2022

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

The Secure Firewall migration tool allows you to migrate Secure Firewall ASA configurations 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. The desktop tool also supports migrations from third-party vendors Check Point, Palo Alto Networks, and Fortinet.

Cisco Secure Firewall Migration Tool Version 3.0 supports migrations to a Secure Firewall Threat Defense device running threat defense software version 7.2. That version of threat defense can be managed by a cloud-delivered Firewall Management Center on CDO. The migration process is part of CDO and does not require any specific license other than the CDO license.

You can download the Secure Firewall Migration Tool from the Software Download page.

CDO provides a wizard to help you migrate the following elements of the ASA's running configuration to the threat defense template:

- Access Control Rules (ACLs)
- Interfaces
- Network Address Translation (NAT) rules
- Network objects and network group objects
- Routes

Once these elements of the ASA running configuration are migrated, you can deploy the configuration to a new threat defense device that is managed by cloud-delivered Firewall Management center on CDO.

For more information, see Migrating ASA Firewall to Cisco Secure Firewall Threat Defense with the Cisco Secure Firewall Migration Tool.

June 9, 2022

Managing Cisco Secure Firewall Threat Defense Devices with Cloud-Delivered Firewall Management Center

Cisco Defense Orchestrator (CDO) is now the platform for the cloud-delivered Firewall Management Center.

The cloud-delivered Firewall Management Center is a software-as-a-service (SaaS) product that manages Secure Firewall Threat Defense devices. It offers many of the same functions as an on-premises Secure Firewall Management Center, it has the same appearance and behavior as an on-premises Secure Firewall Management Center, and uses the same FMC API.

This product is designed for Secure Firewall Management Center customers who want to move from an on-premises version of the Secure Firewall Management Center to a SaaS version.

As a SaaS product, the CDO operations team is responsible for maintaining it. As new features are introduced, the CDO operations team updates CDO and the cloud-delivered Firewall Manager for you.

A migration wizard is available to help you migrate your Secure Firewall Threat Defense devices registered to your on-premises Secure Firewall Management Center to the cloud-delivered Firewall Management Center.

Onboarding Secure Firewall Threat Defense devices is carried out in CDO using familiar processes such as onboarding a device with its serial number or using a CLI command that includes a registration key. Once the device is onboarded, it is visible in both CDO and in the cloud-delivered Firewall Management Center, however, you configure the device in the cloud-delivered Firewall Management Center. Secure Firewall Threat Defense devices running Version 7.2 or later can be onboarded.

The license for cloud-delivered Firewall Management Center is a per-device-managed license and there is no license required for the cloud delivered FMC itself. Existing Secure Firewall Threat Defense devices re-use their existing smart licenses and new Secure Firewall Threat Defense devices provision new smart licenses for each feature implemented on the FTD.

In a remote branch office deployment, the data interface of the threat defense device is used for Cisco Defense Orchestrator management instead of the Management interface on the device. Because most remote branch offices only have a single internet connection, outside CDO access makes centralized management possible. In the case of remote branch deployment, CDO provides high availability support for the threat defense devices that it manages through the data interface.

You can analyze syslog events generated by your onboarded threat defense devices using Security Analytics and Logging (SaaS) or Security Analytics and Logging (On Premises). The SaaS version stores events in the cloud and you view the events in CDO. The on-premises version stores events in an on-premises Secure Network Analytics appliance and analysis is done in the on-premises Secure Firewall Management Center. In both cases, just as with an on-premises FMC today, you can still send logs to a log collector of your choice directly from the sensors.

The FTD dashboard provides you an at-a-glance view of the status, including events data collected and generated by all threat defense devices managed by the cloud-delivered Firewall Management Center. You can use this dashboard to view collective information that is related to the device status and the overall health of the devices in your deployment. The information that the FTD dashboard provides depends on how you license, configure, and deploy the devices in your system. The FTD dashboard displays data for all CDO-managed threat defense devices. However, you can choose to filter device-based data. You can also choose the time range to display for specific time range.

The Cisco Secure Dynamic Attributes Connector enables you to use service tags and categories from various cloud service platforms in cloud-delivered Firewall Management Center access control rules. Network constructs such as IP addresses may be ephemeral in virtual, cloud and container environments due to the dynamic nature of the workloads and the inevitability of IP address overlap. Customers require policy rules to be defined based on non-network constructs such as VM name or security group, so that firewall policy is persistent even when the IP address or VLAN changes.

Proxy sequences of one or more managed devices can be used to communicate with an LDAP, Active Directory, or ISE/ISE-PIC servers. It is necessary only if Cisco Defense Orchestrator(CDO) cannot communicate with your Active Directory or ISE/ISE-PIC server. For example, CDO might be in a public cloud but Active Directory or ISE/ISE-PIC might be in a private cloud.

Although you can use one managed device as a proxy sequence, we strongly recommend you set up two or more so that, in the event one managed device cannot communicate with Active Directory or ISE/ISE-PIC, another managed device can take over.

Any customer can use CDO to manage other device types like, the Secure Firewall ASA, Meraki, Cisco IOS devices, Umbrella, and AWS virtual private clouds. If you use CDO to manage a Secure Firewall Threat Defense device configured for local management with Firepower Device Manager, you can continue to manage them with CDO as well. If you are new to CDO, you can manage Secure Firewall Threat Defense devices with the new cloud-delivered Firewall Management Center and all of the other device types as well.

Learn more about the Firewall Management Center features we support in the cloud-delivered Firewall Management Center.

- Health Monitoring
- Secure Firewall Threat Defense Device Backup/Restore
- Scheduling
- Import/Export
- External Alerting with Alert Responses
- Transparent or Routed Firewall mode
- High Availability for Secure Firewall Threat Defense Devices
- Interfaces
- Network Access Control (NAT)
- Static and Default Routes and other routing configurations
- Object Management and Certificates
- Remote Access VPN and Site to Site VPN configuration
- Access Control policies
- Cisco Secure Dynamic Attributes Connector
- Intrusion and Detection and Prevention policies
- Network Malware and Protection and File Policies
- Encrypted Traffic Handling
- User Identity
- FlexConfig Policies

Onboard an On-Prem management center with SecureX

If you have an on-prem management center that is already associated with your Securex account, you can onboard the management center to CDO through SecureX. Devices onboarded through SecureX experience the same amount of feature support and functionality as a management center onboarded through traditional methods. To onboard a management center to CDO through SecureX, see Onboard an On-Prem FMC with SecureX.

Note Even if your management center account is associated with SecureX, we strongly recommend merging your CDO account with SecureX before you attempt to onboard the management center. See Merge Your CDO and SecureX Accounts for more information.

May 2022

May 12, 2022

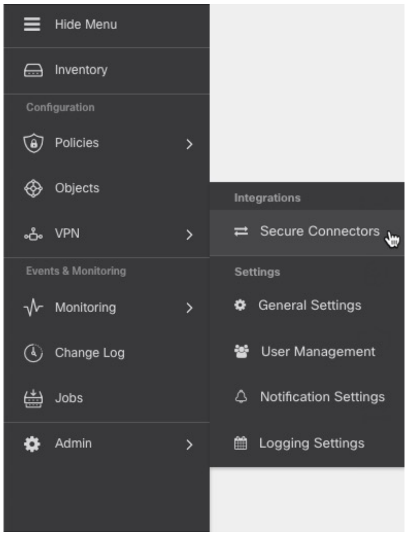
ASA Policy Support for IPv6

ASA access policies and NAT configurations now support rules that use network objects and network groups containing IPv6 addresses. In addition, these rules can also specify ICMP and ICMPv6 protocols. Finally, ASAs now support AnyConnect Connection Profiles containing IPv6 addresses. See ASA Network Policies for more information.

Navigation to the Secure Connectors Page

The Secure Connectors page is accessible from the CDO menu bar. To view the Secure Connectors page, choose **Admin** > **Secure Connectors**.

Figure 1: Secure Connectors Menu



April 2022

April 14, 2022

Monitor AWS VPC tunnels using AWS Transit Gateway

CDO can now monitor AWS VPC tunnels using AWS Transit Gateway. For more information, see Monitor AWS VPC tunnels using AWS Transit Gateway.

April 6, 2022

Global Search

Global search provides an option to search for all onboarded devices and associated objects available within CDO. The search results allow you to navigate to the corresponding device and object pages.

Currently, CDO supports global search for ASA, Firepower Management Center, Secure Firewall Threat Defense, and Meraki devices.

For more information, see "*Global Search*" in the following documents:

- Managing ASA with Cisco Defense Orchestrator
- Managing FMC with Cisco Defense Orchestrator
- Managing FTD with Cisco Defense Orchestrator
- Managing Meraki with Cisco Defense Orchestrator

Support for Cisco Secure Firewall 3100

Cisco Defense Orchestrator supports onboarding ASA and Secure Firewall Threat Defense devices running on new Cisco Secure Firewall 3100 Series devices.

Secure Firewall Threat Defense devices can be onboarded using Low Touch Provisioning or by using a registration key or serial number.

February 2022

February 03, 2022

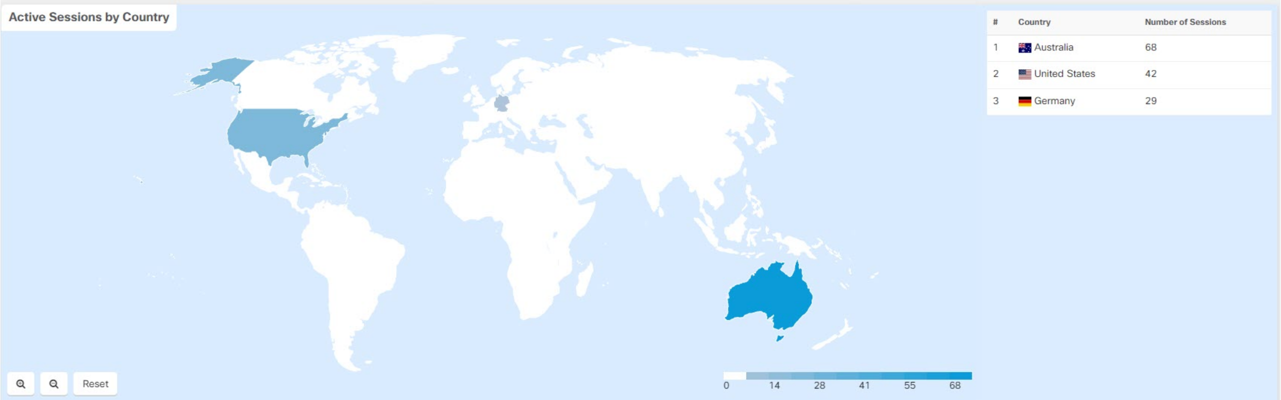
Active Directory (AD) Groups in User Management

For an easier way to manage users in CDO, you can now map your Active Directory (AD) groups in CDO instead of managing individual users. Any user changes, such as a new user(s) addition, removing existing user(s), or changing roles can now be done in Active Directory without changing anything within CDO. CDO now also supports multiple-roles per user with AD. For more information, see the "Active Directory Groups in User Management" section of the **User Management** chapter of you're device's configuration guide.

Improved Charts View for Active Remote Access VPN Sessions

CDO now provides a new and improved charts view for your active RA VPN sessions. In addition to the charts you are already familiar with, CDO now displays a heat map of the location of users connected to your RA VPN headends. This map is available only in the live view.

To view the new charts view, on the RA VPN Monitoring page, click the **Show Charts View** icon appearing at the top-right corner of the screen.



#	Country	Number of Sessions
1	Australia	68
2	United States	42
3	Germany	29

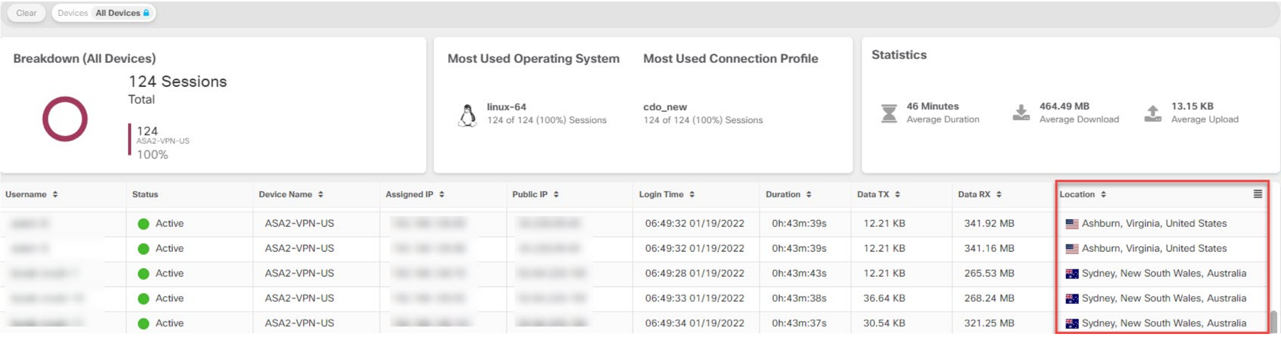
For more information, see "Monitoring Remote Access Virtual Private Network Sessions" in Managing FTD with Cisco Defense Orchestrator or Managing ASA with Cisco Defense Orchestrator depending on your firewall.

January 2022

January 20, 2022

Geolocation Information of Remote Access VPN Users

The remote access VPN monitoring page now shows the location of all users who are connected to the VPN headend. CDO obtains this information by geolocating the public IP addresses of the users. This information is available on live and historical views. On clicking the location in the **User Details** area in the left pane, the precise location of the user is shown on a map.



Breakdown (All Devices)

124 Sessions
Total

124
ASA2-VPN-US
100%

Most Used Operating System
linux-64
124 of 124 (100%) Sessions

Most Used Connection Profile
cdo_new
124 of 124 (100%) Sessions

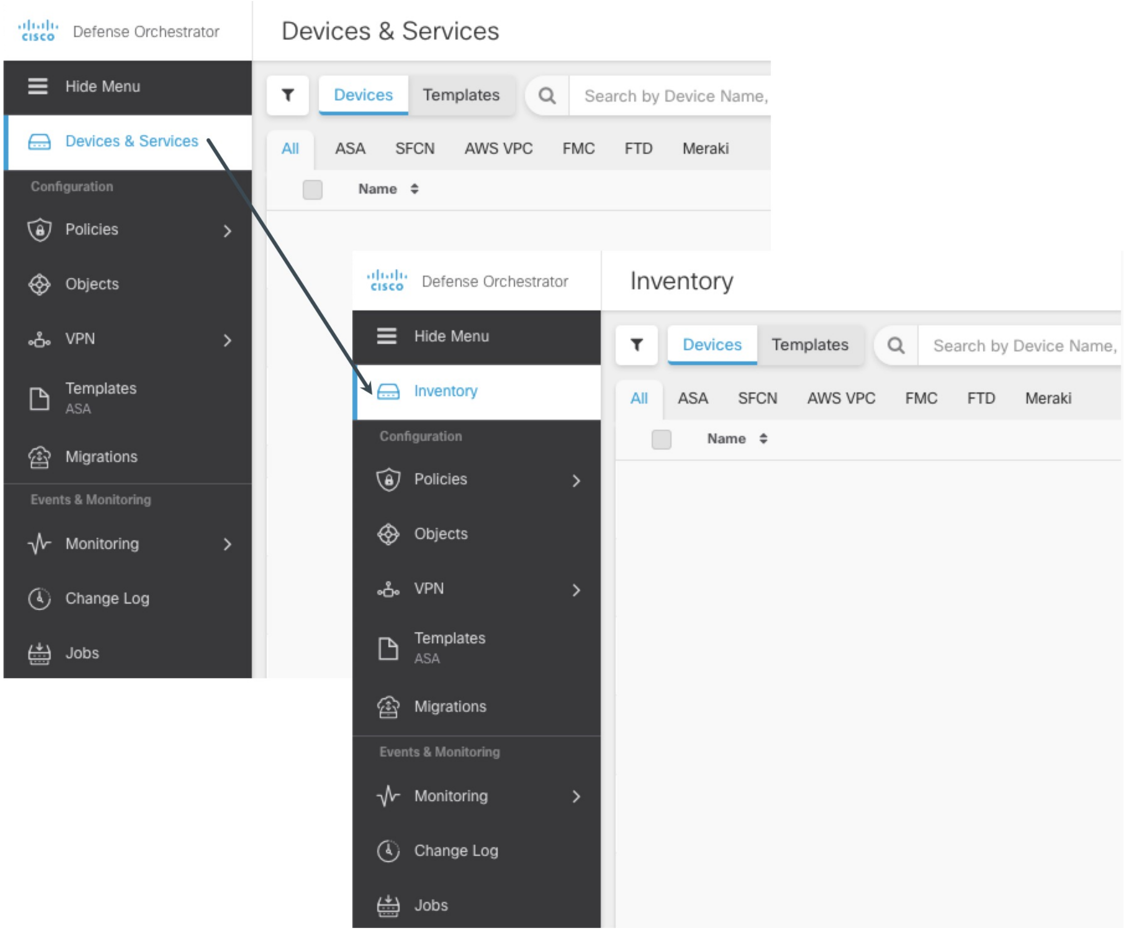
Statistics
46 Minutes Average Duration
464.49 MB Average Download
13.15 KB Average Upload

Username	Status	Device Name	Assigned IP	Public IP	Login Time	Duration	Data TX	Data RX	Location
[redacted]	● Active	ASA2-VPN-US	[redacted]	[redacted]	06:49:32 01/19/2022	0h:43m:39s	12.21 KB	341.92 MB	Ashburn, Virginia, United States
[redacted]	● Active	ASA2-VPN-US	[redacted]	[redacted]	06:49:32 01/19/2022	0h:43m:39s	12.21 KB	341.16 MB	Ashburn, Virginia, United States
[redacted]	● Active	ASA2-VPN-US	[redacted]	[redacted]	06:49:28 01/19/2022	0h:43m:43s	12.21 KB	265.53 MB	Sydney, New South Wales, Australia
[redacted]	● Active	ASA2-VPN-US	[redacted]	[redacted]	06:49:33 01/19/2022	0h:43m:38s	36.64 KB	268.24 MB	Sydney, New South Wales, Australia
[redacted]	● Active	ASA2-VPN-US	[redacted]	[redacted]	06:49:34 01/19/2022	0h:43m:37s	30.54 KB	321.25 MB	Sydney, New South Wales, Australia

Note This information is available to user sessions that are established after the new CDO deployment and will not be available for existing user sessions.

Devices & Services Page Renamed to Inventory

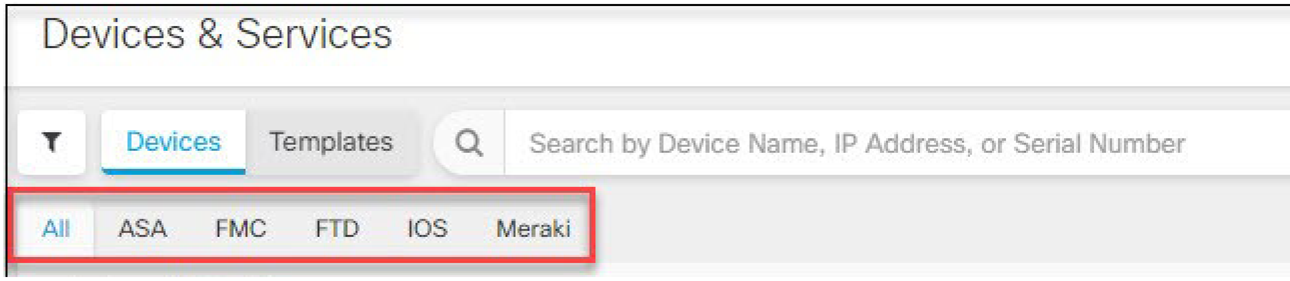
The Devices & Services page has been renamed, "Inventory." The Inventory table lists all the devices and services you manage with CDO. No features were added or removed as a result of the name change.



January 13, 2022

Enhanced Devices & Services Interface

The CDO **Devices & Services** interface now classifies devices and templates based on their type and displays them in the corresponding tabs dedicated to each device type.



Devices & Services

CHAPTER 4

Feature Highlights of 2021

This article describes some of the features that were added to Cisco Defense Orchestrator in 2021.

December 2021

December 9, 2021

CDO Support for Firepower Threat Defense, Version 7.1

CDO now supports Firepower Threat Defense (FTD), version 7.1 devices. These are the aspects of support CDO provides:

- Onboard a supported physical or virtual device running Firepower Threat Defense version 7.1.
- Upgrade from Firepower Threat Defense versions 6.4+ to version 7.1.
- Support for existing Firepower Threat Defense features.

These caveats apply to Firepower Threat Defense, version 7.1 support:

- CDO currently does not support backing up Firepower Threat Defense devices running version 7.1. Support for this functionality is planned for the first maintenance release of Firepower Threat Defense, version 7.1.
- CDO does not support features introduced in the Firepower Threat Defense, version 7.1 release.

For more information about the FTD features CDO currently supports, see *Managing FTD with Cisco Defense Orchestrator*.

New CDO Documentation Platform

Online Help

- Content describing all your devices in a single place.
- Context-sensitivity.
- Content matches found as you search.
- Search results highlighted in a table of contents puts information in a larger context.

Content Maintained on Cisco.com

- Availability on Cisco.com places all your Cisco documentation on one site.
- Device-specific configuration guides makes finding information easier.
- What's New for Cisco Defense Orchestrator continues to describe the latest features available in CDO.

November 2021

November 11, 2021

New SASE Tunnel Functionality

You can now edit SASE tunnels that have been read into or created through the CDO UI. Note that this function only supports tunnels between an Umbrella organization and an ASA peer device that is already onboarded to CDO.

For more information see "Edit a SASE Tunnel" in *Managing an ASA with Cisco Defense Orchestrator* for more information.

October 2021

October 21, 2021

Improved SecureX Integration

For users who have not already linked SecureX with their CDO tenant, CDO now offers a streamlined integration with SecureX. This process allows you to quickly and securely connect your CDO tenant to your SecureX Organization and add a CDO module to the SecureX dashboard with a single click. If you do not have a SecureX Organization, you can create one during this process.

For more information, see "Integrating CDO with SecureX" in *Managing FTD with Cisco Defense Orchestrator*.

Upload an AnyConnect Package from CDO Repository

CDO now supports uploading the AnyConnect package to ASA and FTD devices from the CDO repository.

The Remote Access VPN Configuration wizard presents AnyConnect packages per operating system, which you can select and upload to a device.

For more information, see "Upload an AnyConnect Package from CDO Repository" in *Managing FTD with Cisco Defense Orchestrator* and "Manage AnyConnect Software Packages on ASA Devices" in *Managing ASA with Cisco Defense Orchestrator*.

September 2021

September 16, 2021

CDO Notifications with Service Integrations

CDO notifications now integrate with webhooks. The notifications selected in the Notification Settings page will be sent to the application or service integration of your choice.

For more information, see "Enable Service Integrations for CDO Notifications" in *Managing FTD with Cisco Defense Orchestrator*.

Cisco Secure Firewall Cloud Native Support for Cisco Security Analytics and Logging

Cisco Security Analytics and Logging has been greatly expanded to support logging events from Secure Firewall Cloud Native.

Secure Firewall Cloud Native logging: Security Analytics and Logging (SAL SaaS) now supports logging from any Secure Firewall Cloud Native device. Users can choose to store Secure Firewall Cloud Native events in syslog format, NetFlow Security Event Logs (NSEL) format, or both in the Cisco Cloud and use Cisco Secure Cloud Analytics to analyze them. Customers that want to enable logging analytics will be required to enable NSEL logs to provide the necessary telemetry for the higher-tier SAL licenses.

- Traffic Analysis—Secure Firewall Cloud Native logs can be run through SAL's traffic analysis and observations and alerts can be reviewed by cross-launching Cisco Secure Cloud Analytics from CDO. Cloud Native customers only logging syslog events must switch to NSEL logs to enable traffic analytics.

- Logging Analytics and Detection and Total Network Analytics Detection—Customers acquiring Logging Analytics and Detection and Total Network Analytics Detection licenses can provision and use a Secure Cloud Analytics portal for analysis. Secure Cloud Analytics detections include observations and alerts specifically enabled using firewall logging data, in addition to the other detections available to SAL users as part of Secure Cloud Analytics core capability. Existing Logging and Troubleshooting license holders can test the detection capabilities of higher licenses with no commitment for 30 days.

- Free Trials—You can start a no-commitment 30-day SAL trial for all licenses by filling out this form. This trial requires only a minimal set of on-premises connectors for exporting data to the cloud. You can use this trial to evaluate SAL capabilities, and estimate the data volume required to support production environments, as a precursor to purchasing the appropriate daily volume for SAL licenses. To this end, the SAL trial will not throttle data for most user volumes. In addition, an estimator tool helps you estimate SAL daily volume.

For information, see "Cisco Security Analytics and Logging" in *Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator*.

August 2021

August 26, 2021

CDO and Umbrella Integration

CDO now supports Umbrella integration. You can onboard Umbrella organizations and view, manage, and create SASE tunnels that exist between Umbrella and ASA devices. ASA devices utilize Umbrella's SIG tunnel and inspection which provides centralized management for easy-to-use security.

When you onboard an Umbrella organization, we recommend onboarding the ASA devices associated with that organization as well.

For more information about what Umbrella is and how CDO communicates with it, see *Managing ASA with Cisco Defense Orchestrator*.

August 13, 2021

Duo Configuration Support using LDAP for FTD RA VPN

You can now configure Duo two-factor authentication using LDAP for an FTD Remote Access VPN connection.

Use the Duo LDAP server as the secondary authentication source along with a Microsoft Active Directory (AD) or RADIUS server as the primary authentication source. With Duo LDAP, the secondary authentication validates the primary authentication with a Duo passcode, push notification, phone call, or SMS.

For more information, see "Duo Two-Factor Authentication using LDAP" in *Managing FTD with Cisco Defense Orchestrator*.

July 2021

July 08, 2021

Digital Certificate Management Support for ASA

CDO now manages digital certificates on ASA devices. You can add a digital certificate such as identity certificates and trusted CA certificates as trustpoint objects and install them on one or more managed ASA devices. You can also export an installed identity certificate to duplicate a trustpoint configuration on a different ASA manually.

You can upload or create an identity certificate in the following formats:

- PKCS12 file with a passphrase
- Self-signed certificate

- Certificate Signing Request (CSR) signed by a certificate authority

The Remote Access VPN uses digital certificates for authenticating ASA and AnyConnect clients to establish a secure VPN connection.

For more information, see "ASA Certificate Management" in *Managing ASA with Cisco Defense Orchestrator*.

AnyConnect Module Support for RA VPN ASA and FTD

CDO now supports managing AnyConnect modules on ASA and FTD devices.

Note This feature is supported on FTD running software version 6.7 or later versions.

As part of your RA VPN group policy creation, you can now configure a variety of optional modules to be downloaded and installed when a user downloads the Cisco AnyConnect VPN client. These modules can provide services such as web security, malware protection, off-network roaming protection, and so on.

You can associate each module with a profile containing your custom configurations, created in the AnyConnect Profile Editor and uploaded to the CDO as an AnyConnect File object.

For more information on how to upload the profiles and assign them to group policies, see "Upload RA VPN AnyConnect Client Profile" and "Create New FTD RA VPN Group Policies" in *Managing FTD with Cisco Defense Orchestrator*.

July 01, 2021

Snort 3 Support

CDO now supports the Snort 3 processing engine for FTD devices running Version 6.7 and later. The Snort engine automatically updates new snort rules to keep your device compliant with the latest vulnerabilities. You can perform a standalone upgrade from Snort 2 to Snort 3 or upgrade the device system and the Snort engine simultaneously for an abridged upgrade experience.

For more information, see "Upgrade to Snort 3.0" in *Managing FTD with Cisco Defense Orchestrator*.

Custom Intrusion Prevention System Policy

CDO now supports Snort 3 and customized Intrusion Prevention System (IPS) policies for FTD devices running Version 6.7 and later. The improved Snort 3 processing engine allows you to create and customize IPS policies using rules provided by the Cisco Talos Intelligence Group (Talos). The best practice is to create your own policy based on the provided Talos policy templates and change that if you need to adjust rule actions.

Note Be aware of the differences and limitations when you upgrade to or from Snort 3, as the upgrade may change how your rules are configured.

For more information, see "Custom Firepower Intrusion Prevention System Policy" in *Managing FTD with Cisco Defense Orchestrator*.

June 2021

June 17, 2021

CDO Support for Firepower Threat Defense, Version 7.0

CDO now supports Firepower Threat Defense (FTD), 7.0. You can onboard an FTD device running FTD 7.0, or use CDO to upgrade the device to that version. CDO continues to support existing FTD features in addition to the new Reputation Enforcement on DNS Traffic feature. This feature is an access control policy setting. Enable this option to apply your URL filtering category and reputation rules to DNS lookup requests.

For more information, see "Configuring Access Policy Settings" in *Managing FTD with Cisco Defense Orchestrator*.

CDO has limited support for these features:

- FTDv Tiered License Support—Version 7.0 supports performance-tiered Smart Licensing for FTDv devices based on throughput requirements and RA VPN session limits. CDO does not fully support tiered smart licensing at this time. You can onboard an FTDv device that uses a tiered license but you cannot update the license using CDO. Use the device's Firepower Device Manager to install and manage licenses on the FTDv.

  For more information, see "FTD Licensing" in *Managing FTD with Cisco Defense Orchestrator*.

- Scan Interface Support—If an interface is added to a Firepower device by using the Firepower eXtensible Operating System (FXOS) Chassis Manager, on the Firepower 4100 series or 9300 series devices, you will need to configure that interface on FDM and then have CDO "check for changes" to the device to read in the configuration.

  For more information, see "Synchronizing Interfaces Added to a Firepower Device using FXOS" in *Managing FTD with Cisco Defense Orchestrator*

- Virtual Router Support—VRF routes are not seen in CDO. You can onboard a device with virtual route support but you will not be able to see the virtual route in CDO's static routing page.

  For more information, see "About Virtual Routing and Forwarding" in *Managing FTD with Cisco Defense Orchestrator*

- Equal Cost Multi Path Routing (ECMP)—CDO can onboard a device that uses ECMP and read the configuration but doesn't allow you to modify them. You can create and change the ECMP configuration through FDM and then read it into CDO.

- Rulesets—You cannot apply rulesets to an FTD 7.0 device.

Note For information about the FTD features that CDO currently supports, see Managing FTD with Cisco Defense Orchestrator.

June 10, 2021

Cisco Secure Firewall Cloud Native Support

CDO now supports Cisco Secure Firewall Cloud Native. The Cisco Secure Firewall Cloud Native seamlessly extends Cisco's industry-leading security to a cloud-native form factor (CNFW) using Kubernetes (K8s) orchestration to achieve scalability and manageability. Amazon Elastic Kubernetes Service (Amazon EKS) gives you the flexibility to start, run, and scale Kubernetes applications in the AWS cloud. Amazon EKS helps you provide highly-available and secure clusters and automates key tasks such as patching, node provisioning, and updates.

CDO allows onboarding of this firewall and provides complete firewall management:

- View real-time and historical data from AnyConnect RA VPN sessions.
- Create and manage objects and use them in different policies that handle ingress and egress traffic in your network.
- Recognizes and reconciles changes made to the firewall outside of CDO, using the Kubernetes command-line tool.

For more information, see *Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator*.

You can also read *Cisco Secure Firewall Cloud Native At-a-Glance* for additional information.

Enhanced Remote Access VPN Monitoring

In addition to monitoring the live AnyConnect Remote Access VPN session, CDO now allows monitoring the historical data from AnyConnect Remote Access VPN sessions recorded over the last three months.

You can monitor VPN sessions across all Adaptive Security Appliance (ASA), Firepower Threat Defense (FTD), and Cisco Secure Firewall Cloud Native (SFCN) VPN head-ends in your tenant.

These are some of the salient enhancements made to the current release:

- Displays intuitive graphical visuals to provide at-a-glance views from all active VPN head-ends managed by CDO.
- The live session screen shows the most used operating system and VPN connection profile in the CDO tenant. It also shows the average session duration and data uploaded and downloaded.
- The historical session screen plots a bar graph to show data recorded for all devices in the last 24 hours, 7 days, and 30 days.
- Provides new filtering capabilities to narrow down your search based on criteria such as device type, session length, and upload and download data range.

Open the Remote Access VPN Monitoring screen from the navigation bar by clicking **VPN** > **Remote Access VPN Monitoring**.

New User Role

CDO now provides a new user role, the VPN Sessions Manager user role, that allows specific users the ability to terminate VPN sessions per tenant. Note that terminating VPN sessions is the only action this role allows; users designated with this role are otherwise limited with read-only capabilities.

May 2021

May 27, 2021

Improved Device Notifications in CDO

You can now subscribe to CDO email alerts and view recent notifications within the CDO UI.

Receive email alerts for when a device associated with your tenant experiences a wokflow or event change. Workflow changes include deployments, upgrades, or backups; event changes include devices going online or offline, conflict detection, HA or failover state, and site-to-site VPN connection status.

Note These customizable notifications and alerts are applied to all devices associated with your tenant and are not device-specific.

For more information, see "Notifcations Settings" in *Managing FTD with Cisco Defense Orchestrator*.

March 2021

March 25, 2021

Cisco Security Analytics and Logging Availability in APJC

Cisco Security Analytics and Logging is now available in the Asia (APJC) region through the newly commissioned Tokyo data store. Security Analytics-enabled accounts will have access to the Cisco Secure Cloud Analytics service in Sydney, Austraila for security-related alerting. With this, the Asia region has been brought up to par with capabilities available in the Americas and EU regions.

For more information, see "Cisco Security Analytics and Logging" at *Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator*

March 18, 2021

EtherChannel Interface Support

CDO now supports EtherChannel interface configuration on supported models running Firepower Version 6.5 and later, such as the Firepower 1010, 1120,1140,1150, 2110, 2120, 2130, 2140. EtherChannel is a port link aggregation technology or port-channel architecture that allows the grouping of several physical Ethernet links to create one logical Ethernet link for the purpose of providing links between switches, routers and servers.

Note that the configuration that you apply to the physical ports affects only the LAN port where you apply the configuration.

For more information about device support and configuration limitations, see "Guidelines and Limitations for Firepower Interface Configuration" in *Managing FTD with Cisco Defense Orchestrator*.

March 15, 2021

ASA Remote Access VPN Support

CDO now allows creating Remote Access Virtual Private Network (RA VPN) configuration on Adaptive Security Appliance (ASA) devices to enable remote users to connect to the ASA and securely access the remote network. It also allows managing the RA VPN settings that have already been configured using other ASA management tools, such as the Adaptive Security Defense Manager (ASDM) or Cisco Security Manager (CSM).

AnyConnect is the only client that is supported on endpoint devices for RA VPN connectivity.

CDO supports the following aspects of RA VPN functionality on ASA devices:

- SSL client-based remote access
- IPv4 and IPv6 addressing
- Shared RA VPN configuration across multiple ASA devices

For more information, see "Configuring Remote Access VPN for an ASA" in *Managing ASA with Cisco Defense Orchestrator*.

ASA File Management Support

CDO provides the File Management tool for performing basic file management tasks such as viewing, uploading, or deleting files present on the ASA device's flash (disk0) space. Using this tool, you can upload any files such as the AnyConnect software images, DAP.xml, data.xml, host scan image files to a single or multiple ASA device using URL-based file upload from the remote server.

This tool helps you to upload the newly released AnyConnect image to multiple ASA devices simultaneously.

For more information, see "ASA File Management" in *Managing ASA with Cisco Defense Orchestrator*.

February 2021

February 11, 2021

Multiple Secure Device Connector Support

You can now deploy more than one on-premises Secure Device Connector (SDC) for your tenant. This allows you to manage more devices with CDO and maintain communication performance between CDO, your SDCs, and your managed devices.

You can move managed ASA, AWS VPC, and Meraki MX devices from one SDC to another.

Having multiple SDCs also allows you to use one CDO tenant to manage devices in isolated network segments. Do this by assigning all managed devices in the isolated network segment to a single SDC.

For more information, see "Using Multiple SDCs on a Single CDO Tenant" in *Managing ASA with Cisco Defense Orchestrator*.

January 2021

January 21, 2021

FMC Object Reading

Now when you onboard an FMC to CDO, CDO imports the objects from the FMC-managed FTD devices. Once imported to CDO, the objects are read-only. Though the FMC objects are read-only, CDO allows you to apply a copy of the objects to other devices on your tenant that are not managed by the FMC. The copy is disassociated from the original object so you can edit the copy without changing the value of the object that was imported from the FMC. FMC objects can be used on any device you manage that support that object type.

For more information, see "FMC Objects" in Managing FMC with Cisco Defense Orchestrator

January 14, 2021

Exporting CLI Command Results

You can export the results of CLI commands issued to a standalone device, or several devices, to a comma separated value (.csv) file so you can filter and sort the information in it however you like. You can export the CLI results of a single device, or many devices at once.

For more information, see "Export CLI Command Results" in *Managing FTD with Cisco Defense Orchestrator*.

Configuring Cloud Services for your FTD Devices

Connecting to the Cisco Success Network and configuring which events are sent to the Cisco cloud are features that can be configured on FTD devices running software version 6.6 or higher.

Cisco Success Network

By enabling Cisco Success Network, you are providing usage information and statistics to Cisco to improve the FTD and to make you aware of unused or additional features that will help you maximize the value of Cisco products in your network. When you enable the Cisco Success Network, your device establishes a secure connection to the Cisco Cloud and maintains this secure connection at all times.

For more information, see "Connecting to the Cisco Success Network" in *Managing FTD with Cisco Defense Orchestrator*.

Send Events Directly to Cisco Cloud

You can now specify which types of events you send from your FTD directly to the Cisco cloud. Once stored in the Cisco cloud, you can use cloud applications, such as Cisco Threat Response, to analyze the events and to evaluate threats that the device might have encountered.

For more information, see "Sending Events to the Cisco Cloud" in *Managing FTD with Cisco Defense Orchestrator*.

Web Analytics

Enabling web analytics provides anonymous product usage information to Cisco based on page hits. The information includes pages viewed, the time spent on a page, browser versions, product version, device hostname, and so forth. This information can help Cisco determine feature usage patterns and improve the product. All usage data is anonymous and no sensitive data is transmitted. You can use CDO to configure this feature on all versions of FTD.

For more information, see "Enabling or Disabling Web Analytics" in *Managing FTD with Cisco Defense Orchestrator*.

January 7, 2021

FTD HA Pair Onboarding

CDO has enhanced the process of onboarding an FTD HA pair. Once you onboard one of the HA peers with either the registration token method or the login credentials method, CDO automatically detects that the corresponding peer is not onboarded yet and prompts you to take action. The improvement minimizes the effort required to onboard both devices, shortens how long it takes to onboard the peer device, and reuses any registration keys or smart license tokens you may have used to onboard the first device.

You can onboard either the active or the standby device, and once synced, CDO will always detect that the device is part of an HA pair.

Note We strongly recommend onboarding your FTD devices using the registration key method.

For more information on FTD HA Pair Onboarding, see "Onboard an FTD HA Pair with a Registration Key" or "Onboard an FTD HA Pair using Username Password and IP Address"in *Managing FTD with Cisco Defense Orchestrator*.

CHAPTER 5

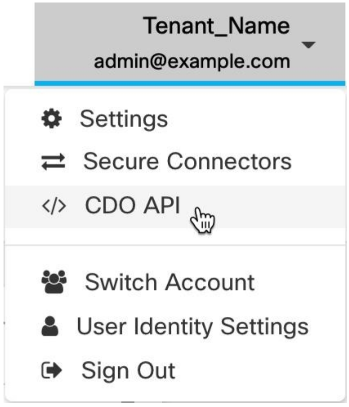
Feature Highlights of 2020

December 2020

December 17, 2020

CDO Public API

CDO has published its public API and provided you with documentation, examples, and a playground to try things out. The goal of our public API is to provide you with a simple and effective way to perform a lot of what you would normally be able to do in the CDO UI, but in code.



To use this API, you will need to know GraphQL. It is very easy to learn, and their official guide (https://graphql.org/learn/) provides a thorough, light read. We chose GraphQL because it is flexible, strongly typed, and auto-documenting.

To find the full schema documentation, simply go to the GraphQL Playground, and click on the docs tab on the right hand side of the page.

You can launch the CDO Public API by selecting it from the user menu.

December 10, 2020

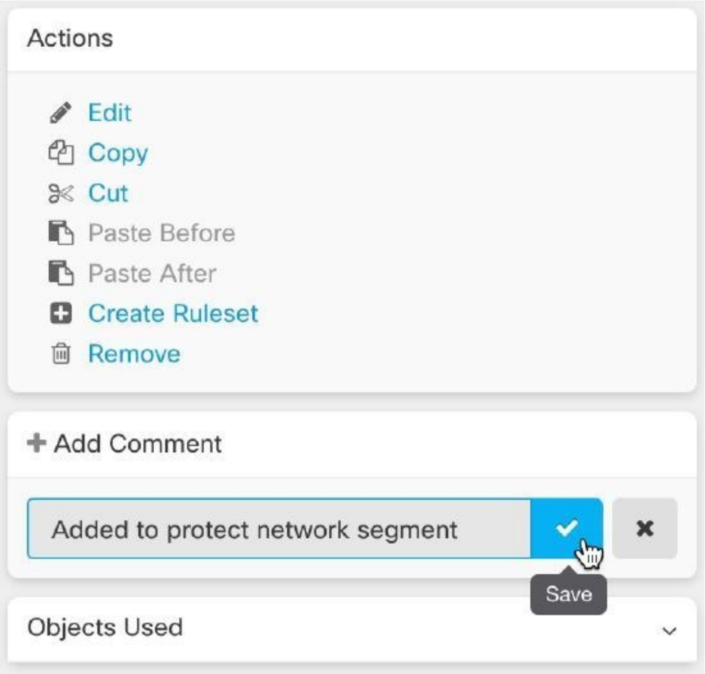
Export FTD Configuration

You can now export the complete configuration of an FTD device as a CDO-readable JSON file. You can import this file as an FTD model (FTD template) on any CDO tenant that you manage.

For more information, see "Export FTD Configuration" in *Managing FTD with Cisco Defense Orchestrator*.

Adding Comments to FTD Rules

You can now add comments to rules in FTD policies and rulesets. Rule comments are only visible in CDO; they are not written to the FTD nor are they visible in FDM.



For more information, see "Adding Comments to Rules in FTD Policies and Rulesets" in *Managing FTD with Cisco Defense Orchestrator*.

November 2020

November 13, 2020

Low Touch Provisioning and Serial Number Onboarding

Low touch provisioning is a feature that allows a new factory-shipped or re-imaged Firepower 1000 or 2100 series device, running FTD software version 6.7 or later, to be plugged in to your network, onboarded to CDO automatically, and then configured remotely. This eliminates many of the manual tasks involved with onboarding the device to CDO. The low touch provisioning process minimizes the need to log in to a physical device. It's intended for remote offices or other locations where your employees are less experienced working with networking devices.

Firepower 1000 and 2100 series devices with factory-installed FTD 6.7 images are expected to be orderable from Cisco at the end of calendar year 2020 or the beginning of calendar year 2021.

It is also possible to onboard a configured Firepower Threat Defense (FTD) version 6.7+ device to FTD 6.7, to CDO using the device's serial number.

See these articles for more information:

- Low Touch Provisioning
- Onboading a FTD 6.7 Device with its Serial Number
- irepower Easy Deployment Guide for Cisco Firepower 1000 or 2100 Firewalls

Assigning Firepower Threat Defense Interfaces to Security Zones

You can now assign an FTD interface to a security zone to further classify and manage traffic. For more information, see "Assign a Firepower Interface to a Security Zone" in *Managing FTD with Cisco Defense Orchestrator*.

November 6, 2020

CDO Support for Firepower Threat Defense, Version 6.6.1 and 6.7

CDO now supports Firepower Threat Defense (FTD), versions 6.6.1 and 6.7. You can onboard a new FTD device running FTD 6.6.1 or 6.7, or use CDO to upgrade to those versions. CDO continues to support existing FTD features and these new FTD 6.7 features:

- Secure Group Tags and SGT Groups
- Active Directory Realm Objects

For more information about the FTD features CDO currently supports, see *Managing FTD with Cisco Defense Orchestrator*.

CDO TLS Server Identity Discovery and TLS 1.3 in Version 6.7

You can now perform URL filtering and application control on traffic encrypted with TLS 1.3, by using information from the server certificate. You do not have decrypt the traffic for this feature to work. For traffic encrypted with TLS 1.3 to match access rules that use application or URL filtering, the system must decrypt the TLS 1.3 certificate. We recommend that you enable **TLS Server Identity Discovery** in the managing UI, whether it is Firepower Device Manager (FDM) or Firepower Management Center (FMC), to ensure encrypted connections are matched to the right access control rule.

For more information, see "TLS Server Identity Discovery in Firepower Threat Defense" in *Managing FTD with Cisco Defense Orchestrator*.

October 2020

October 15, 2020

New User Roles

CDO now provides two additional user roles that divide the responsibilities of editing policies and deploying policies. The new **Edit-Only** role allows users to make configuration changes to devices, but they are not allowed to deploy those changes. The new **Deploy-Only** role allows users to deploy pending configuration changes, but they are not allowed to make configuration changes.

For more information, see "User Roles" in *Managing FMC with Cisco Defense Orchestrator*.

October 2, 2020

FTD API Support

CDO now provides the API tool interface to execute the Representational State Transfer (REST) Application Programming Interface (API) requests for performing advanced actions on an FTD device. Additionally, this interface provides the following features:

- Records a history of already executed API commands.
- Provides system-defined API macros that can be reused.
- Allows creating user-defined API macros using the standard API macros, from a command you have already executed, or another user-defined macro.

For more information about the FTD API tool, see "Using FTD API Tool" in *Managing FTD with Cisco Defense Orchestrator*.

September 2020

September 25, 2020

Multi-Tenant Portal Support

CDO now introduces a Multi-Tenant Portal that provides a consolidated view of devices from tenants across various regions. This view helps you glean information from your tenants in a single-window. You can have the CDO support team create one or more portals based on your requirements.

- Provides the Device Details view that provides the following information:
  - Shows device location, software version, onboarding method, and many more details for each device.
  - Allows you to manage the device on the CDO tenant page that owns that device.
  - Provides a link to sign in to the CDO tenant in a different region and manage that device.
- Exports the portal's information to a comma-separated value (.csv) file to analyze or send it to someone who doesn't have access.
- Allows seamless addition of a new tenant using its API token.
- Allows switching between the portals without signing out from CDO.

For more information, see "Manage Multi-Tenant Portal" in *Managing FTD with Cisco Defense Orchestrator*.

Secure Event Connector Support for Cloud-based Secure Device Connectors

Cisco Security Analytics and Logging (SAL SaaS) customers can now install Secure Event Connectors when their Secure Device Connector is installed in the Cisco cloud. They no longer need to switch to an on-premises Secure Device Connector to configure Cisco Security Analytics and Logging.

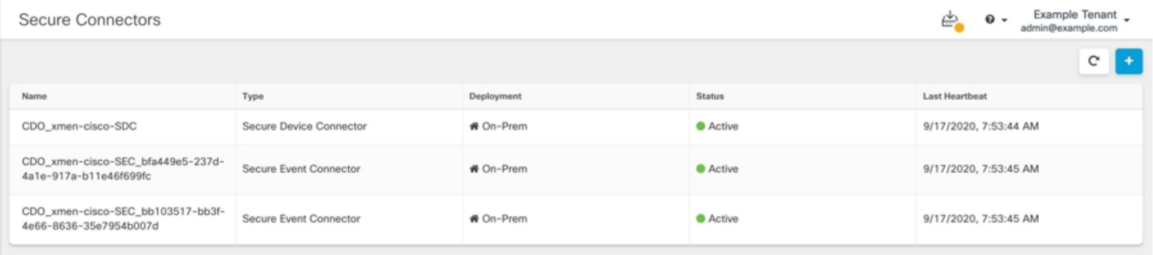
For more information, see the following topics in *Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator*:

- Installing Secure Event Connectors
- Installing SECs, Using CDO Images, on Tenants with Cloud SDCs
- Installing SECs, Using Your VM Image, on Tenants with Cloud SDCs

September 17, 2020

Support for Multiple Secure Event Connectors

The Secure Event Connector (SEC) forwards events from ASAs and FTDs to the Cisco cloud so that you can view them in the Event Logging page and investigate them with Secure Cloud Analytics, depending on your Cisco Security Analytics and Logging (SAL SaaS) licensing. Having more than one SEC allows you to install them in different locations and distribute the work of sending events to the Cisco cloud.



Name	Type	Deployment	Status	Last Heartbeat
CDO_xmen-cisco-SDC	Secure Device Connector	On-Prem	● Active	9/17/2020, 7:53:44 AM
CDO_xmen-cisco-SEC_bfa449e5-237d-4a1e-917a-b11e46f699fc	Secure Event Connector	On-Prem	● Active	9/17/2020, 7:53:45 AM
CDO_xmen-cisco-SEC_bb103517-bb3f-4e66-8636-35e7954b007d	Secure Event Connector	On-Prem	● Active	9/17/2020, 7:53:45 AM

See these articles to learn how to install additional SECs on your tenant:

- Installing Multiple SECs, Using CDO Images, on Tenants with On-Premises SDCs
- Install Multiple SECs Using Your VM Image

For more information, see "Cisco Security Analytics and Logging" in *Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator*.

August 2020

August 20, 2020

Firepower Management Center Support

CDO can now onboard an Firepower Management Center (FMC) running Version 6.4 or later and all of its managed devices. FMC support is limited to onboarding an FMC, viewing the devices it manages, and cross-launching to the FMC UI.

To review how CDO manages an FMC appliance, see *Managing FMC with Cisco Defense Orchestrator*.

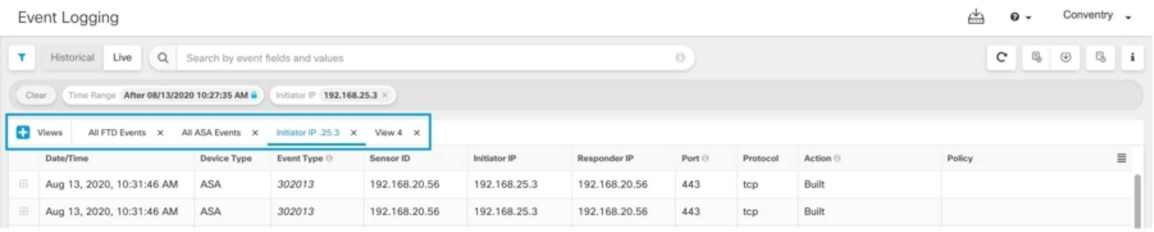
For information on onboarding an FMC, see "Onboard an FMC" in *Managing FMC with Cisco Defense Orchestrator*.

To review supported FMC hardware and software versions, see "Software and Hardware Support by CDO" in *Managing FMC with Cisco Defense Orchestrator*.

Customizable Event Filters

Cisco Security Analytics and Logging (SAL SaaS) customers can create and save customized event filters on the Event Logging page for repeated use.

For more information, see "Customizable Event Filters" in *Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator*.



Date/Time	Device Type	Event Type	Sensor ID	Initiator IP	Responder IP	Port	Protocol	Action	Policy
Aug 13, 2020, 10:31:46 AM	ASA	*302013*	192.168.20.56	192.168.25.3	192.168.20.56	443	tcp	Built	
Aug 13, 2020, 10:31:46 AM	ASA	*302013*	192.168.20.56	192.168.25.3	192.168.20.56	443	tcp	Built	

Improved Search Capabilities in the Event Logging Page

Cisco Security Analytics and Logging (SAL SaaS) customers will now benefit from these improvements to the search capability on the Event Logging page:

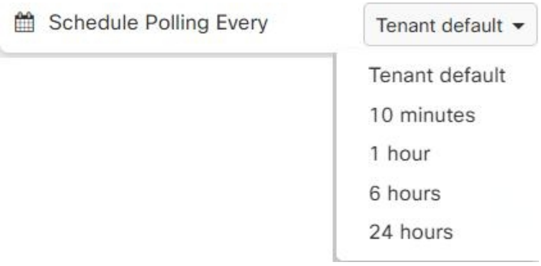
- Click an element attribute to add it to the search field.
- Drag and drop columns on the Event Logging page to view your event information the way you want to.
- New AND NOT and OR NOT search operators in the Event Logging page provide more granular event search capability.

For more information, see "Searching for and Filtering Events in the Event Logging" in *Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator*.

August 13, 2020

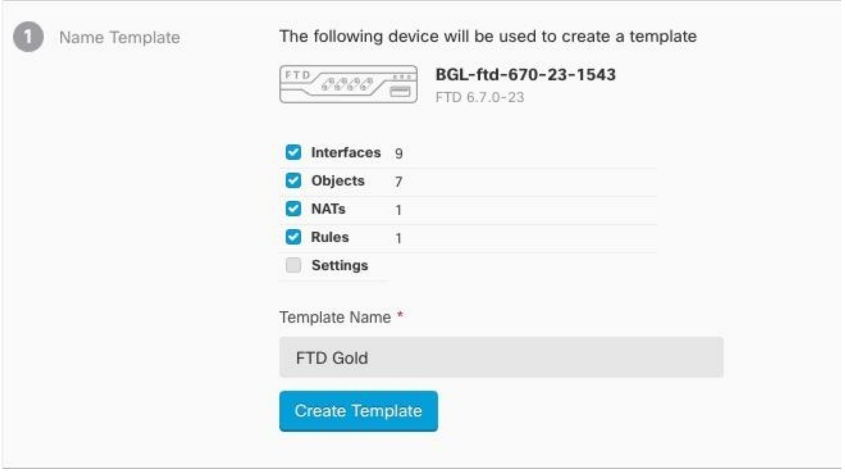
Custom Conflict Detected Polling Interval

You can now configure custom polling intervals by device, regardless of the device type or any previously configured polling intervals. This includes detection for device state or any detected out of band changes. For more information, see "Schedule Polling for Device Changes" in *Managing FTD with Cisco Defense Orchestrator*.



Custom FTD Templates

You can now create a custom FTD template by selecting one or more parts (Access Rules, NAT Rules, Settings, Interfaces, and Objects) of an onboarded FTD device's configuration. Applying a custom template to other FTDs will retain, update, or remove the existing configuration based on the included parts. However, CDO still allows you to select all parts to create a complete template and apply it to other FTDs. For more information, see " FTD Templates" in *Managing FTD with Cisco Defense Orchestrator*.


1 Name Template

The following device will be used to create a template

BGL-ftd-670-23-1543
FTD 6.7.0-23

☑ Interfaces 9
☑ Objects 7
☑ NATs 1
☑ Rules 1
□ Settings

Template Name *

FTD Gold

July 2020

July 30, 2020

Object Overrides

CDO introduces "Object Overrides" that allow you to provide an alternate value for a shared network object, which the system uses for the devices that you specify. It enables you to create a smaller set of shared policies for use across devices without giving up the ability to alter policies when needed for individual devices. Object override makes it possible to create an object that can be overridden on some or all devices that use it in a shared policy or ruleset.

To override an object, see "Object Overrides" in *Managing FTD with Cisco Defense Orchestrator*.

Improved Network Group Wizard

The Network Group editing wizard has been improved to create new network objects instantly and modify the existing ones. It also allows you to add device-specific additional values to devices on which the shared network group is defined.

For more information about the improvements made to Network Group Wizard, see "Create or Edit a Firepower Network Object or Network Group" and Create or Edit ASA Network Objects and Network Groups" in *Managing FTD with Cisco Defense Orchestrator*.

July 9, 2020

Customize the RA VPN and Events Views

You can now customize the tables generated for Remote Access Virtual Private Network (RA VPN), as well as both live and historical event views. Organize and save the tables in the manner that best suits your needs and what is crucial to your portfolio.

For more information related to customization, see the following sections in *Managing FTD with Cisco Defense Orchestrator*:

- Customize the Remote Access VPN Monitoring View
- Viewing Historical Events in CDO

July 2, 2020

SecureX

You can now incorporate CDO into SecureX, which provides a summarization of devices, policy, and applied objects per tenant to strengthen your visibility and automation across your security portfolio. See SecureX for more about how to incorporate CDO and SecureX.

For more information, see the following topics in *Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator*:

- SecureX and CDO
- Connect SecureX in CDO

Cisco Security Analytics and Logging (SAL SaaS) Event Downloads

After filtering ASA and FTD events on the Event Logging page, you can now download your results in a compressed .CSV file.

- The events you add to a downloadable .CSV file are defined by a time range.
- A single .CSV file can accommodate up to approximately 50 GB of compressed information.
- Generation of downloadable files can be done in parallel.
- Once created, the .CSV files are stored in Cisco cloud and downloaded directly from there. These files do not consume any CDO/Secure Cloud Analytics server resources.
- Completed downloadable .CSV files are stored for 7 days and then deleted.

For more information, see "Downloading Events" in *Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator*.

June 2020

June 18, 2020

Firepower Threat Defense Executive Summary Report

You can now generate a custom Executive Summary Report on any or all of your onboarded Firepower Threat Defense (FTD) devices. The report displays a collection of operational statistics such as encrypted traffic, intercepted threats, detected web categories, and more.

For more information, see the following topics in *Managing FTD with Cisco Defense Orchestrator*:

- FTD Executive Summary Report
- Managing Reports

Cisco Security Analytics and Logging Improvements

ASA Syslog and NSEL Events Support

Cisco Security Analytics and Logging has been greatly expanded to support logging events from ASAs.

- **ASA logging**: Security Analytics and Logging (SAL SaaS)) now supports logging from any Cisco ASA Firewall, regardless of how it is managed. Users can choose to send ASA logs in syslog format, NetFlow Security Event Logs (NSEL) format, or both. Customers that want to enable logging analytics will be required to enable NSEL logs to provide the necessary telemetry for the higher-tier SAL licenses.

  In addition to existing FTD logging, this makes CDO the first product in Cisco's Security portfolio to truly aggregate and unify logging for Cisco's entire firewall fleet.

  For more information, see the following topics in *Managing ASA with Cisco Defense Orchestrator*:

  - Cisco Security Analytics and Logging for ASA Devices
  - Implementing Cisco Security Analytics and Logging for ASA Devices

- **Longer-term Storage and Download**: Users can now opt-in to store logs for 1, 2, or 3 years when initially ordering SAL, or as an add-on later. Note that the default retention period of firewall logging remains 90 days. For more information, see "Security Analytics and Logging Event Storage" in *Managing ASA with Cisco Defense Orchestrator*.

- **Traffic Analysis**: Both FTD connection-level logs and ASA (NSEL) logs can be run through SAL's traffic analysis, and observations and alerts can be reviewed by cross-launching to Secure Cloud Analytics using SecureX Sign-On. ASA customers only logging syslog must switch to NSEL logs to enable traffic analytics. Customers acquiring Logging Analytics and Detection and Total Network Analytics and Detection licenses can provision and use a Secure Cloud Analytics portal for analysis at no extra charge. Secure Cloud Analytics detections include observations and alerts specifically enabled using firewall logging data, in addition to the other detections available to SAL users as part of Secure Cloud Analytics' core capability. Existing Logging and Troubleshooting license holders can test the detection capabilities of higher licenses with no commitment for 30 days.

- **Free Trials**: You can start a no-commitment 30-day SAL trial for all licenses by filling out this form. This low-touch trial requires only a minimal set of on-prem connectors for exporting data to the cloud. You can use this trial to evaluate SAL capabilities, and estimate the data volume required to support production environments, as a precursor to purchasing the appropriate daily volume for SAL licenses. To this end, the SAL trial will not throttle data for most user volumes. In addition, an estimator tool helps you estimate SAL daily volume.

Improved Event Monitoring for Security Analytics and Logging

- The Event Logging page in CDO now provides filtering of ASA events by type. You can see all your syslog events or NSEL events separately or together.
- Many ASA syslog events are parsed, providing greater detail about the event. That detail can be used to analyze the event in Secure Cloud Analytics.
- You can customize your view of the Event Logging page by showing only the columns of information you want to see and by hiding the rest.

For more information, see " Filtering Events in the Event Logging" in *Managing ASA with Cisco Defense Orchestrator*.

June 4, 2020

Monitor and Terminate Remote Access VPN Sessions

You can now use CDO to monitor live AnyConnect Remote Access VPN sessions across all Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) VPN head-ends in your tenant. It gathers information on the total number of active VPN sessions, currently connected users and sessions, the volume of data received and transferred.

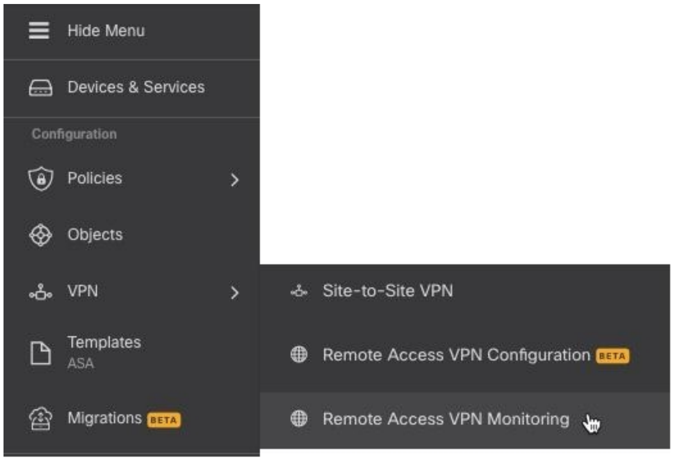
You can view the performance of each RA VPN head-end in your tenant, filter sessions by head-ends, and select the session properties that you want to view in the VPN monitoring table. Also, you can export the RA VPN sessions of one or more devices to a comma-separated value (.csv) file. For more information, see "Export RA VPN Sessions to a CSV File" in *Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator*.

You can terminate all the active RA VPN sessions of a single user on an ASA, and terminate all active RA VPN sessions of all users on an ASA.

For more information, see the following topics:

- Disconnect Active RA VPN Sessions on ASA in *Managing ASA with Cisco Defense Orchestrator*
- Disconnect Active RA VPN Sessions on FTD in *Managing FTD with Cisco Defense Orchestrator*

Open the Remote Access VPN Monitoring screen from the navigation bar by clicking **VPN > Remote Access VPN Monitoring.**



AWS Virtual Private Cloud Management - Free Trial

Try managing your AWS VPC from CDO for free for 90 days. Open the **Inventory** page in CDO and onboard your AWS VPC to get started.

For more information, see "Onboard an AWS VPC" in *Managing AWS with Cisco Defense Orchestrator*.

What's New Tile

The CDO landing page now has a What's New tile to showcase the latest features and when CDO implemented those features. If there is a feature that interests you, click the title of the feature to read the documentation about that specific feature.

May 2020

May 20, 2020

New API Only User

CDO now allows a Super Admin to create an "API Only User" that can be used to generate an API token for authenticating to CDO when making CDO REST API calls. This user account and the corresponding API token continues to function even after the original Super Admin departs your organization.

For more information, see "Create API Only Users" in Managing FTD with Cisco Defense Orchestrator.

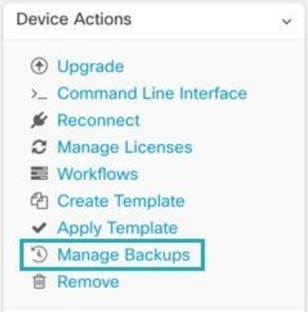
May 7, 2020

Backup Firepower Threat Defense Devices

You can now use CDO to back up a Firepower Threat Defense's (FTD's) system configuration. With CDO you can:

- Backup devices on demand.

- Schedule recurring backups on a cadence from every day to every month, at the time you choose.
- Download backups and use Firepower Device Manager (FDM) to restore them.



For more information, see "Backing Up FTDs" in *Managing FTD with Cisco Defense Orchestrator*.

April 2020

April 16, 2020

CDO Support for Devices Running Firepower Threat Defense 6.6.0

CDO now manages FTD 6.6.0 devices. These are the new aspects of support CDO provides:

- Onboarding a device running Firepower Threat Defense (FTD) 6.6.0.
- Upgrading FTD 6.4.x+ devices to FTD 6.6.0 devices. Devices can be individual FTDs or FTDs configured in a high-availability pair. These caveats apply to upgrade support:
  - Upgrades for Firepower 4100 and Firepower 9300 devices is not currently supported.
  - Customers can upgrade to FTD 6.6.0 using the drop-down in the upgrade page in CDO.
- CDO continuously develops support for FTD features and releases new feature support as it is ready.

For more information, see "Firepower Threat Defense Support Specifics" in *Managing FTD with Cisco Defense Orchestrator*.

April 9, 2020

Firepower Threat Defense Command Line Interface

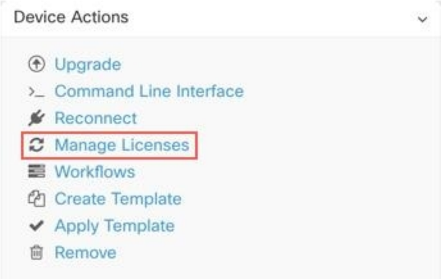
You can now issue CLI requests to your FTD devices directly from CDO.

For more information, see "Using the CDO Command Line Interface" in *Managing FTD with Cisco Defense Orchestrator*.

April 2, 2020

Improved License Management for Firepower Threat Defense Devices

Viewing FTD device license information, enabling and disabling licenses, and refreshing licenses is now all managed from a single button in the Device Actions pane on the **Inventory** page.



March 2020

March 26, 2020

FTD Security Database Updates

CDO allows you to immediately update and, simultaneously, schedule future updates for security databases when you onboard you FTD device. This feature updates the SRU, security intelligence (SI), vulnerability (VDB), and geolocation databases. Note that you can only schedule future updates as part of the onboarding process.

For more information, see "Update FTD Security Databases" in *Managing FTD with Cisco Defense Orchestrator*.

Support for Port Ranges in FTD Service Objects

CDO now supports creating service objects (also referred to as port objects in FTD) that contain a range of port numbers.

For more information, see "Create and Edit Firepower Service Objects" in *Managing FTD with Cisco Defense Orchestrator*.

March 24, 2020

Cisco Secure Sign-on Domain Migration

On Tuesday March 24, 2020, at 5pm Pacific Daylight Savings Time, the official domain for Cisco Security Single Sign-on solution was moved from https://security.cisco.com to https://sign-on.security.cisco.com.

We recommend that you update any saved links and update any password managers, so they are referencing the new URL.

This move will limit your access to CDO for a short period of time, but doesn't limit your ability to perform updates using your local device managers or SSH connections.

If you experience any issues please contact Cisco TAC, who can provide you with technical support.

March 12, 2020

FTD Rulesets

CDO introduces **Rulesets** for Firepower Threat Defense devices. A ruleset is a collection of access control rules that can be shared by multiple FTD devices. Any change made to the rules of a ruleset affects the other FTD devices that use the ruleset. An FTD policy can have both device-specific (local) and shared (rulesets) rules. You can also create rulesets from existing rules in an FTD device.

This feature is currently available for devices running Firepower Threat Defense 6.5 and later releases.

For more information, see "FTD Rulesets" in *Managing FTD with Cisco Defense Orchestrator*.

March 5, 2020

Copy or Move rules within an FTD Policy or to Another FTD Policy

It's now possible to copy or move rules from the policy on one FTD to the policy on another FTD. We have also made it easier to move rules within an FTD policy so you can fine-tune the order in which rules evaluate network traffic.

For more information, see "Copy FTD Access Control Rules" and "Move FTD Access Control Rules" in *Managing FTD with Cisco Defense Orchestrator*.

AnyConnect Software Package Upload to FTD Version 6.5+

You can now use CDO's Remote Access VPN wizard to upload AnyConnect packages from a remote server to a Firepower Threat Defense (FTD) device running FTD 6.5 or later. Ensure that the remote server supports HTTP or HTTPS protocol.

For more information, see "Upload AnyConnect Software Packages to an FTD Device Running FTD Version 6.5 or Later" in *Managing FTD with Cisco Defense Orchestrator*.

March 3, 2020

Terminology Update in CDO's Interface

In order to manage a device, Cisco Defense Orchestrator (CDO) must have a copy of the device's configuration stored in its own database. When CDO "reads" a configuration, it makes a copy of the configuration stored on the device and saves it to CDO's database. We have renamed some interface options to better describe what you are doing when you perform a read action.

This is the new terminology:

- **Check for Changes**. If a device's configuration status is Synced, the Check for Changes link is available. Clicking Check for Changes directs CDO to compare its copy of the device's configuration with the device's copy of the device's configuration. If there is a difference CDO immediately overwrites its copy of the device's configuration with the copy stored on the device.

- **Discard Changes**. If a device's configuration is Not Synced, clicking Discard Changes deletes any changes CDO made to its copy of the device configuration and also overwrites it with a copy of the configuration found on the device.
- **Accept Without Review.**This action overwrites CDO's copy of a device's configuration with the copy of the configuration stored on the device. CDO does not prompt you to confirm the action.

For more information, see "Reading, Discarding, Checking for, and Deploying Configuration Changes" in *Managing FTD with Cisco Defense Orchestrator*.

February 2020

February 6, 2020

Switch Port Mode Support for Firepower 1010

CDO now fully supports the switch port mode feature for the Firepower 1010 device.

For more information on the configuration guidelines and limitations, see "Switch Port Mode Interfaces for an FTD" and "Configure an FTD VLAN for Switch Port Mode" in *Managing FTD with Cisco Defense Orchestrator*.

January 2020

January 22, 2020

Dynamic Peer Support for Site-to-Site Connections

You can now configure a site-to-site VPN tunnel between two peers when one of the peer's VPN interface has a dynamic IP address. This dynamic peer can be a managed FTD device or an Extranet device.

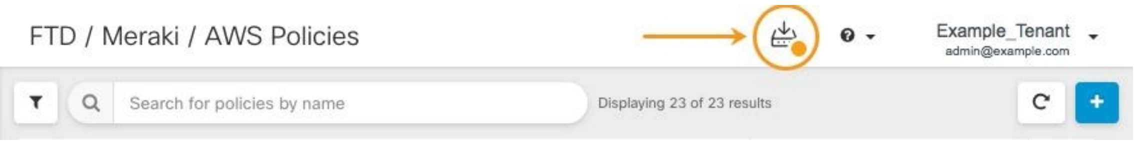
For more information, "Configure Site-to-Site VPN Connections with Dynamically-Addressed Peers" in *Managing FTD with Cisco Defense Orchestrator*.

January 16, 2020

Improved Deployment Experience

CDO has improved its deployment workflow. An additional deployment icon is now visible throughout CDO. You no longer have to return to the **Inventory** page to deploy your configuration changes.

When the deployment icon includes an orange dot it signals that there is at least one configuration change made to at least one of the devices you manage with CDO, that is ready to be deployed.


FTD / Meraki / AWS Policies
Example_Tenant
admin@example.com
Search for policies by name
Displaying 23 of 23 results

For more information, see "Preview and Deploy Configuration Changes for All Devices" in *Managing FTD with Cisco Defense Orchestrator*.

Cancelling Bulk Actions

You can now cancel any active bulk action you have taken on multiple devices. For example, assume you have tried to reconnect four managed devices and three of the devices have successfully reconnected but the fourth device has neither succeeded nor failed to reconnect. You can now go to the **Jobs** page, find the ongoing bulk action and click Cancel to stop the action.

CHAPTER 6

Feature Highlights of 2019

November 2019

November 2019

CDO Support for Devices Running Firepower Threat Defense 6.5.0

CDO now manages FTD 6.5.0 devices. These are the aspects of support CDO provides:

- Onboading a device running Firepower Threat Defense (FTD) 6.5.0.
- Support for additional Firepower series devices such as the Firepower 4100 and Firepower 9300.
- Support for a virtual FTD instance on Microsoft Azure. For a complete list of supported devices, see "Firepower Threat Defense Support Specifics" in Managing FTD with Cisco Defense Orchestrator.
- Devices can be individual FTDs or FTDs configured in a high-availability pair. For more information, see "Firepower Software Upgrade Path" in Managing FTD with Cisco Defense Orchestrator. These caveats apply to upgrade support:
  - Upgrading an HA pair will not be supported for FTDs running 6.5.0 if the device is using a data interface for management.
  - Upgrades on Firepower 4100 and Firepower 9300 devices are not currently supported.
  - Customers will be able to upgrade to FTD 6.5.0 using the drop-down in the upgrade page in CDO. The link that is provided to the device for 6.5 image download will be a HTTP. This may mean that the image download time could be slightly longer than if the download were done over HTTPS. In addition, if outbound HTTP traffic from the FTD is blocked, the image download will fail.

- When FTD 6.5.0 is installed on a Firepower 1010 you can configure interfaces to run as a regular firewall interface or as a Layer 2 hardware switch port. At this time, switch mode support on CDO is read-only. To create or modify an interface for switch port mode, use the FDM console. CDO continues to develop its support for switch port mode on Firepower 1010s and will announce its full support in What's New when it is available.
- When you onboard an FTD 6.5.0 device using a registration token, you can send connection events, file and malware events, and intrusion events directly to the Cisco cloud without using a Secure Event Connector. See "mplementing Cisco Security Analytics and Logging" in Managing FTD with Cisco Defense Orchestrator.
- Continued support for FTD 6.4.x features. CDO is continuously developing support for FTD 6.5 features and will release support as it is ready.

For more information about the FTD features CDO supports, see Managing FTD with Cisco Defense Orchestrator.

IKEv1 Support for Site to Site VPN Connections

CDO now supports creating site-to-site VPN tunnels using Internet Key Exchange version 1 (IKEv1). It helps you to configure site-to-site VPN on legacy firewalls, which does not support Internet Key Exchange version 2 (IKEv2). Internet Key Exchange (IKE) is a key management protocol that is used for authenticating IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

For more information, see "Site-to-Site Virtual Private Network" in Managing FTD with Cisco Defense Orchestrator.

Firepower Threat Defense Template Improvements

CDO now allows you to parameterize some aspects of the FTD template to further customize templates. For more information, see "Configure FTD Templates" in Managing FTD with Cisco Defense Orchestrator.

Smart License Management

You can now manage Cisco Smart Licenses for Firepower Threat Defense devices within CDO. Smart Licensing is conveniently built into our workflows and easily accessible from the CDO interface. You can now perform these Cisco Smart Licensing tasks within CDO:

- Apply a Smart License while onboarding an FTD device using a registration token
- View the licenses applied to a device
- Register the licenses with Cisco Smart Software Manager
- Enable and Disable different license types for your device

For more information, see "Onboard a Firepower Threat Defense Device with a Registration Token" and "Smart-licensing an Onboarded FTD" in Managing FTD with Cisco Defense Orchestrator.

October 2019

October 2019

Amazon Web Services Support

CDO now manages AWS VPC!

Amazon Web Services (AWS) Virtual Private Cloud (VPC) is a commercial cloud computing service that provides users a virtual private cloud associated to your AWS account; this network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

CDO helps you optimize your AWS VPC by identifying problems with objects and rules and gives you ways to fix them. Use CDO to:

- Manage an AWS VPC environment along with your FTD or ASA devices.
- Simultaneously manage all security group rules associated with the AWS VPC.
- Create and customize security group rules with objects that are compatible across other supported platforms, such as FTD and ASA devices.
- View AWS VPC site-to-site VPN connections.

For more information, see *Managing AWS with Cisco Defense Orchestrator*.

Migrate your ASAs to FTD Devices Using CDO

CDO helps you migrate your Adaptive Security Appliance (ASA) to a Firepower Threat Defense (FTD) device. CDO provides a wizard to help you migrate these elements of the ASA's running configuration to an FTD template:

- Interfaces
- Routes
- Access Control Rules (ACLs)
- Network Address Translation (NAT) rules
- Network objects and network group objects
- Service objects and service group objects

Once these elements of the ASA running configuration have been migrated to an FTD template, you can then apply the FTD template to a new FTD device that is managed by CDO. The FTD device adopts the configurations defined in the template, and so, the FTD is now configured with some aspects of the ASA's running configuration.

For more information on the process of migrating an ASA to an FTD using CDO, see "Migrating ASA to FTD Workflow" in *Managing ASA with Cisco Defense Orchestrator*.

Cisco Introduces a New Single Sign-On Solution using Cisco Secure Sign-on and Duo Multi-factor Authentication

CDO adopts this new solution and converts customer tenants to the Cisco Secure Sign-on identity provider (IdP) and Duo Security multi-factor authenticator.

With Cisco Secure Sign-On, you will benefit from:

- **Strong and resilient identity**: Security that meets the highest industry standards, including AICPA SOC 2, CSA-Star, and ISO 27001. It also supports segregated FedRAMP and HIPAA environments for customers.
- **Duo Multi-Factor Authentication (MFA)**: Duo MFA integrated with Cisco Secure Sign-On means adaptive, layered, and simplified authentication. One push notification, one tap, instant access.
- **A single sign-in for seamless workflows**: Enter a single username and password to access all your applications, anywhere, and on any device, while maintaining context through workflows.
- **A customized experience**: Arrange your work apps on your Cisco Secure Sign-On dashboard any way you want. Tabs and a search bar help keep you organized.

Note

- If you sign in to CDO using your own single sign-on identity provider, this transition to Cisco Secure Sign-On and Duo *does not* affect you. You continue to use your own sign-on solution.
- If you are in the middle of a free trial of CDO, this transition *does* affect to you.

For more information, see "Migrating to Cisco Secure Sign-On Identity Provider" in *Managing AWS with Cisco Defense Orchestrator*.

Cisco Security Analytics and Logging Including Integration with Secure Cloud Analytics

Cisco Security Analytics and Logging improves network visibility so you can quickly detect threats in real time and remediate incidents with confidence and at scale.

With Cisco Security Analytics and Logging you can capture connection, intrusion, file, malware, and Security Intelligence events from all of your Firepower Threat Defense (FTD) devices and view them in one place in CDO.

The events are stored in the Cisco cloud and viewable from the Event Logging page in CDO where you can filter and review them to gain a clear understanding of what security rules are triggering in your network. The Logging and Troubleshooting package gives you these capabilities.

With the Firewall Analytics and Monitoring package, the system can apply Secure Cloud Analytics dynamic entity modeling to your FTD events, and use behavioral modeling analytics to generate Secure Cloud Analytics observations and alerts. If you obtain a Total Network Analytics and Monitoring package, the system applies dynamic entity modeling to both your FTD events and your network traffic, and generates observations and alerts. You can cross-launch from CDO to a Secure Cloud Analytics portal provisioned for you, using Cisco Single Sign-On.

For more information, see "Cisco Security Analytics and Logging" in *Managing FTD with Cisco Defense Orchestrator*.

September 2019

September 2019

Onboarding a Firepower Threat Defense Device with a Registration Token

You can now onboard your FTD device using a registration token rather than using an IP address, username and password. This is especially beneficial if your FTD is assigned an IP address using DHCP. If that IP address changes for some reason, your FTD remains connected to CDO. Additionally, your FTD can have an address on your local area network, and as long as it can access the outside network it can be onboarded to CDO using this method.

This method of onboarding is currently available for FTD 6.4 releases and to customers connecting to defenseorchestrator.cisco.com. It is not yet available for customers connecting to defenseorchestrator.cisco.eu.

For more information, see "Onboarding an FTD with a Registration Key" in *Managing FTD with Cisco Defense Orchestrator*.

August 2019

August 2019

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging improves network visibility so you can quickly detect threats in real time and remediate incidents with confidence and at scale.

Remote Access VPN Support for Firepower Threat Defense

Remote Access (RA) VPN allows individuals to establish a secure connection to your network using supported laptop, desktop, and mobile devices. CDO provides an intuitive user interface for you to setup RA VPN on the Firepower Threat Defense (FTD) devices you have onboarded.

AnyConnect is the only client that is supported on endpoint devices for RA VPN connectivity.

CDO supports the following aspects of RA VPN functionality on FTD devices:

- Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) for privacy, authentication, and data integrity
- SSL client-based remote access
- IPv4 and IPv6 addressing
- Shared RA VPN configuration across multiple FTD devices

For more information, see "Remote Access Virtual Private Network" in *Managing FTD with Cisco Defense Orchestrator*.

Firepower Threat Defense High Availability Image Upgrade Support

You can now upgrade FTD HA pairs in CDO. When you upgrade a failover pair, CDO copies the desired upgrade image to both devices for you. CDO temporarily moves the primary device to active mode if it is not already, then upgrades the secondary device. Once the secondary device successfully upgrades, the primary device upgrades. The failover pair upgrades the devices one at a time to minimize network disruption.

To upgrade your failover pairs, see "Upgrade an FTD High Availability Pair" in *Managing FTD with Cisco Defense Orchestrator*.

Site-to-Site VPN for Firepower Threat Defense Devices

Site-to-Site VPN for Firepower Threat Defense devices is now generally available!

CDO allows you to establish secure connections between two sites in different geographic locations. These peers can have any mix of inside and outside IPv4 and IPv6 addresses. Site-to-site tunnels are built using the Internet Protocol Security (IPsec) protocol suite and Internet Key Exchange version 2 (IKEv2). After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel. You can create site-to-site IPsec connections for the following scenarios for devices that are onboarded to CDO:

- Between two managed devices
- Between the managed device and other Cisco peers
- Between the managed device and third-party peers

Firepower Threat Defense High Availability Support

CDO makes high availability (HA) support for Firepower Threat Defense firewalls generally available! You can now onboard an existing HA pair or create an HA pair in CDO. HA configurations make it possible to maintain a secure network in scenarios where a device might be unavailable, such as during an upgrade period or an unexpected device failure; in failover mode, the standby device is already configured to become active, meaning that even if one of the HA devices becomes unavailable, the other device continues to handle traffic.

Most of the features supported for standalone FTD devices also support devices configured for HA. For more information, see "FTD High Availability" in *Managing FTD with Cisco Defense Orchestrator*.

Coming soon... support for FTD HA upgrades. At the moment, if you need to upgrade your HA pair, you must execute the upgrade through the active device's FDM console.

July 2019

July 2019

Time Range Objects for ASA Devices

You can now customize the rules in your network policies with time range objects; these objects let you execute one-time or recurring rules and customize how your network handles traffic.

For more information, see "ASA Time Range Objects" in *Managing ASA with Cisco Defense Orchestrator*.

Firepower Threat Defense Support

CDO makes support for Firepower Threat Defense firewalls generally available!

CDO is designed for firewall administrators who want a simplified management interface and cloud-access to their Firepower Threat Defense devices. Firepower Device Manager (FDM) administrators will notice many similarities between the FDM interface and the CDO interface. We built CDO with the idea of keeping things as consistent as possible between managers.

CDO can now manage Firepower Threat Defense (FTD) devices running FTD version 6.4.0 and later when it is installed on the ASA 5508-x, ASA 5515-x, ASA 5516-x, ASA 5525-x, ASA 5545-x, ASA 5555-x, the FTD 2100 series devices, the FTD 1000 series devices, or virtual FTD devices.

Use CDO to manage these aspects of your physical or virtual Firepower Threat Defense (FTD) device:

- Device management
- Device upgrade
- Interface Management
- Routing
- Security Policies
- Promote policy and configuration consistency
- Change tracking
- Monitoring your network

All CDO FTD PIDs are orderable in CCW, including for the Firepower 1000 series and Virtual FTD. The PIDs are platform specific, but common for ASA and FTD. Please consult our ordering guide in Salesconnect for more details.

For more information about the features we support, see *Managing FTD with Cisco Defense Orchestrator*.

Meraki MX Support

CDO now manages Meraki MX Firewall Policies!

Meraki MX is an enterprise security and software-defined wide-area-network (SD-WAN) next-generation firewall appliance designed for distributed deployments. You can now manage layer 3 network rules on Meraki MX devices using Cisco Defense Orchestrator.

CDO helps you optimize your Meraki environment by identifying problems with objects and policies and gives you ways to fix them. This applies to policies that are associated to both devices and templates.

Use CDO to:

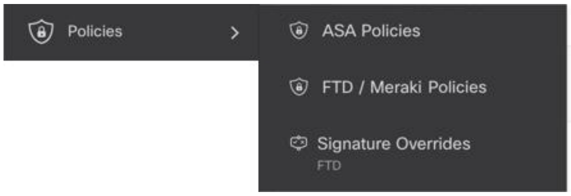
- Simultaneously manage policies on one or more Meraki devices.
- Monitor and manage Meraki policies or templates alongside your FTD and ASA devices in an all-encompassing environment.
- Use a Meraki template to manage multiple networks.
- Customize access rules with objects that are compatible across other supported platforms, such as FTD and ASA devices.

For more information, see *Managing Meraki with Cisco Defense Orchestrator*.

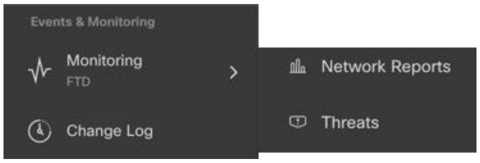
Updated GUI Navigation

Navigating CDO's UI just got easier.

The policy menu in the navigation bar now guides you to policies grouped by device or function. We only expose the menu paths you need to reach the policies that currently exist on your tenant.



All of FTD's monitoring capabilities are grouped in the **Events & Monitoring** area of the navigation bar. The Monitoring menu shows you **Network Reports** and **Threats**.



May 2019

May 2019

Device Connectivity Troubleshooting

This tool allows you to test or troubleshoot connectivity issues between the Secure Device Connector (SDC) and any of your devices. You may want to test this connectivity if your device fails to on-board or if you want to determine, before on-boarding, if CDO can reach your device.

For more information, see "Troubleshoot a Secure Device Connector with the SDC" in *Managing FTD with Cisco Defense Orchestrator*.

April 2019

April 2019

You can Help us Improve the CDO User Experience

We want to know about your CDO user experience and we now have an easy way for you to tell us. We've added a **Provide Feedback** button to our Help menu so you can give us your feedback without leaving the CDO portal. Tell us what you like and what we can improve on.

When you leave us your feedback, tell us your role in your company. Are you in the network operations center, the security operation center, or are you in the I-do-it-all-IT-center? Tell us what task you're trying to complete. Are you trying to edit a security policy or find something in the change log?

Here's how to leave us your feedback:

Step 1 Log in to CDO.

Step 2 Next to your tenant and account name, click the help button and select **Provide Feedback**.

Step 3 Enter your feedback and click **Send Email**. This generates an email to in your local mail server that you must manually send.

A member of our support staff will respond as soon as possible.

February 2019

February 2019

Resolution to Container Privilege Escalation Vulnerability Affecting Secure Device Connector: cisco-sa-20190215-runc

The Cisco Product Security Incident Response Team (PSIRT) published the security advisory **cisco-sa-20190215-runc** which describes a high-severity vulnerability in Docker. Read the entire PSIRT team advisory for a full explanation of the vulnerability.

This vulnerability impacts all CDO customers:

- Customers using CDO's cloud-deployed Secure Device Connector (SDC) do not need to do anything as the remediation steps have already been performed by the CDO Operations Team.
- Customers using an SDC deployed on-premise need to upgrade their SDC host to use the latest Docker version.

For instructions on how to update a CDO-standard SDC host and a custom SDC host, see Container Privilege Escalation Vulnerability Affecting Secure Device Connector: cisco-sa-20190215-runc.

Add Labels when Bulk Onboarding ASA Devices

You can now specify custom device labels when bulk onboarding your ASA devices. For more information, see "Onboard ASAs in Bulk" in *Managing ASA with Cisco Defense Orchestrator*.

Cisco IOS Device Support

Cisco Defense Orchestrator (CDO) allows you to manage Cisco IOS devices. These are the features we support for those devices:

- Onboarding Cisco IOS devices
- View the device configuration

- End policy and configuration changes from device
- Detect out-of-band changes
- Command line interface support
- Individual CLI commands and groups of commands can be turned into editable and reusable macros
- Detect and manage SSH fingerprint changes
- View changes to IOS devices in the Change Log

Schedule Automatic Deployments

After making configuration changes for one or more devices using CDO, you can now schedule the deployment of those changes, to those devices, at a date and time that is convenient for you. For example you can schedule the deployments to occur during your maintenance window or during a time of low network traffic.

For more information, see "Enable the Option to Schedule Automatic Deployments" and "Schedule Automatic Deployments" in *Managing ASA with Cisco Defense Orchestrator*.

Terminology Change: CDO "Deploys" Changes to the Devices it Manages

We updated the terminology we use to describe transferring changes you made on CDO's local copy of a device's configuration to the device itself. We previously used the word "write" to describe that transfer, now we use the word "deploy" to describe that transfer.

As you manage and make changes to a device's configuration with CDO, CDO saves the changes you make to its own copy of the configuration file. Those changes are considered "staged" on CDO until they are "deployed" to the device. Staged configuration changes have no affect on the network traffic running through the device. Only after CDO "deploys" the changes to the device do they have an affect on the traffic running through the device. When CDO deploys changes to the device's configuration, it only overwrites those elements of the configuration that were changed. It does not overwrite the entire configuration file stored on the device.

CHAPTER 7

Feature Highlights of 2018

November 2018

November 22, 2018

Auto-Accept Out-of-Band Changes

You can now make configuration changes directly on your managed devices and set Defense Orchestrator to accept them automatically when it detects them. You will not have to monitor Defense Orchestrator and accept out-of-band changes manually.

For more information, see "Automatically Accept Out-of-Band Changes from your Device" in *Managing ASA with Cisco Defense Orchestrator*.

November 8, 2018

System Objects Filter

The system object filter lets you see the objects in the object table that are most important to you.

Some devices come with pre-defined objects for common services. These system objects are convenient because they are already made for you and you can use them in your rules and policies. There can be many system objects in the objects table. System objects cannot be edited or deleted.

Show System Objects is "off" by default. To display system objects in the object table, check Show System Objects in the filter bar. To hide system objects in the object table, leave Show System Objects unchecked in the filter bar.

For more information, see "Object Filters" in *Managing ASA with Cisco Defense Orchestrator*.

September 2018

September 20, 2018

Improvements to Policy Exports

When you export an ASA policy with a specified time range, the time range object name is now included in the .CSV file. This gives you a better sense of when rules in the policy are active.

Improvements to CLI Handling

Defense Orchestrator no longer trims trailing spaces on ASA CLI commands it executes.

Documentation Updates

ASA change log and "Diff" documentation added to give you a clear understanding of the contents of a change log entry and the "Diff" page. See before-and-after side-by-side comparisons of configuration changes. For more information, see "Change Log" in *Managing ASA with Cisco Defense Orchestrator*.

September 13, 2018

Export Only The Change Log Entries You Are Interested In

Previously you could only export the entire Defense Orchestrator's change log. Now you can apply filter and search criteria to the change log and export only the entries you are interested in.

For more information, see "Exporting the Change Log to a CSV file" in *Managing FTD with Cisco Defense Orchestrator*.

September 6, 2018

New Super Admin Role Can Create New User Records and Change User Roles

Defense Orchestrator added support for the Super Admin role. This new role has all of the permissions of the Admin role and has additional permissions of being able to manage user records. The Defense Orchestrator support team can upgrade your existing Admin accounts to Super Admins. Having a user with a Super Admin role gives you the ability to create and manage additional user records without opening a support ticket.

If your company integrated its SAML Identity Provider (IdP) with Defense Orchestrator, you are now be able to fully manage user access to your Defense Orchestrator account.

If you are a Managed Service Provider with multiple Defense Orchestrator accounts, you are now able to grant and revoke account access for your existing users without opening a support ticket with Defense Orchestrator.

If your company uses Defense Orchestrator's default identity provider (OneLogin), you'll continue to need to open support tickets to create new user accounts but will be able to revoke access to your Defense Orchestrator account without opening a support ticket.

For more information, see "User Management" in *Managing FTD with Cisco Defense Orchestrator*.

August 16, 2018

Improvements to Change Log

When you make a change to an ASA through CDO and the configuration change succeeds, the change log now shows the CLI commands used to make the change.

If you make a change to an ASA through CDO and the configuration change fails, the Change Log shows the CLI commands that failed and surrounds them with asterisks so you can locate them easily.

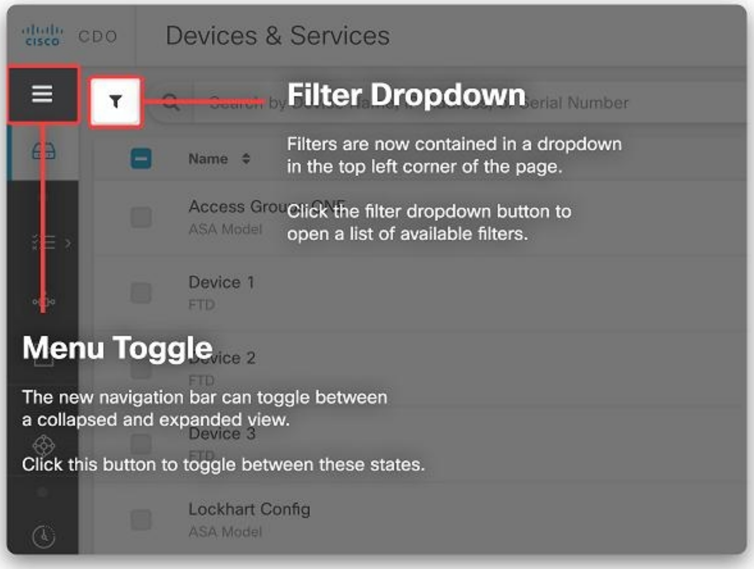
To see the commands that succeeded or failed, open the Change Log for the device on which the change was made, locate the entry for your action and expand it by clicking the + button at the end of the log entry.

July 2018

July 26, 2018

New CDO UI

We redesigned the navigation and filtering to be more intuitive and help you manage your environment more efficiently.



Filter Dropdown

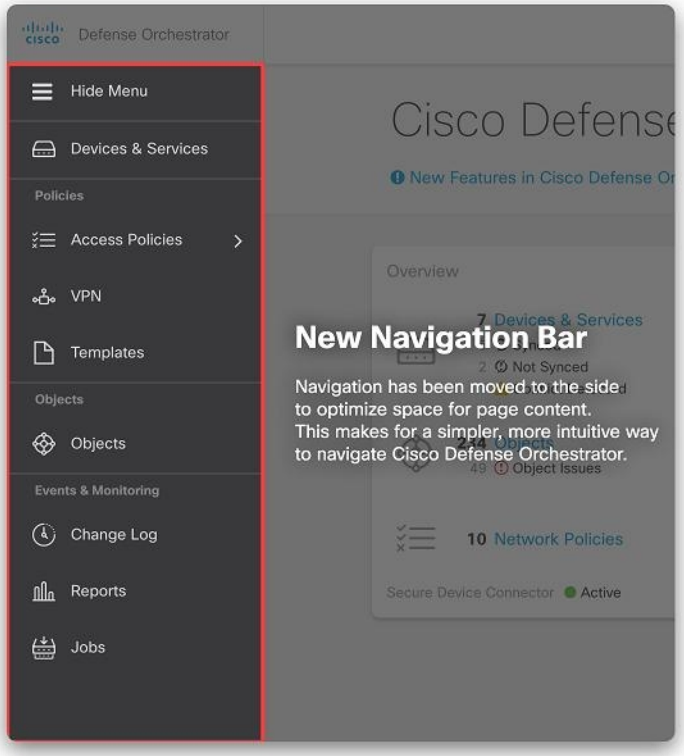
Filters are now contained in a dropdown in the top left corner of the page.

Click the filter dropdown button to open a list of available filters.

Menu Toggle

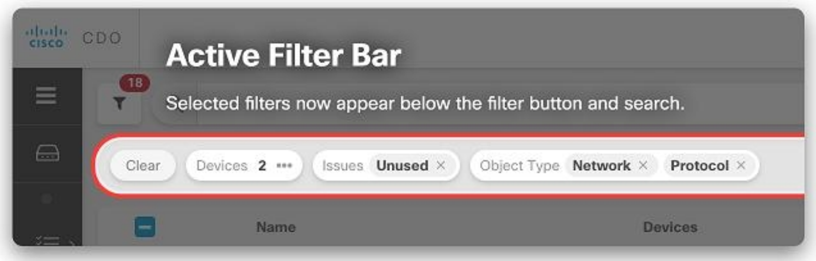
The new navigation bar can toggle between a collapsed and expanded view.

Click this button to toggle between these states.



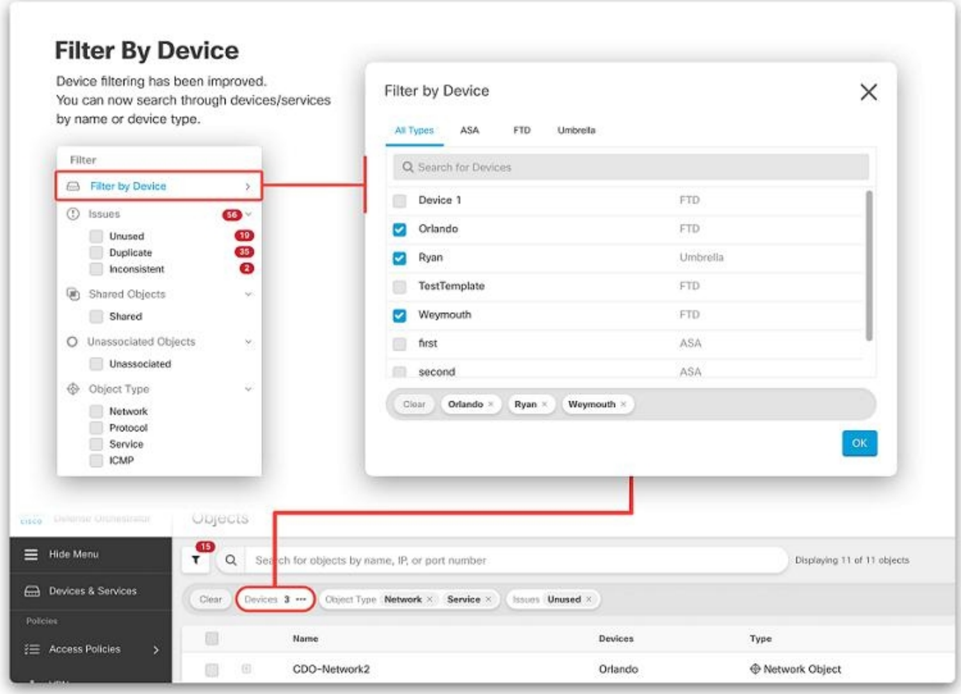
New Navigation Bar

Navigation has been moved to the side to optimize space for page content. This makes for a simpler, more intuitive way to navigate Cisco Defense Orchestrator.



Active Filter Bar

Selected filters now appear below the filter button and search.



Filter By Device

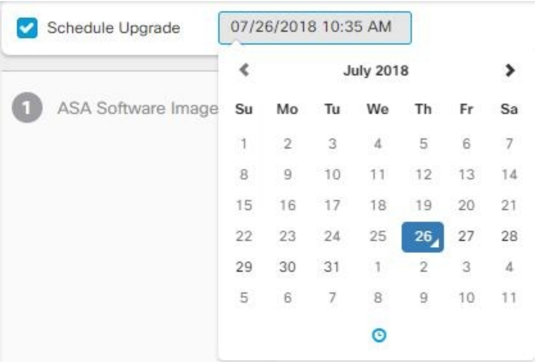
Device filtering has been improved. You can now search through devices/services by name or device type.

□	Device 1	FTD
☑	Orlando	FTD
☑	Ryan	Umbrella
□	TestTemplate	FTD
☑	Weymouth	FTD
□	first	ASA
□	second	ASA

	Name	Devices	Type
□	CDO-Network2	Orlando	Network Object

Schedule Device Upgrade

You can now schedule software upgrades to your devices. On the Device Upgrade page, select the Schedule Upgrade check box, and configure a later date and time. For more information, see "Upgrade Devices and Services" in in *Managing ASA with Cisco Defense Orchestrator*.



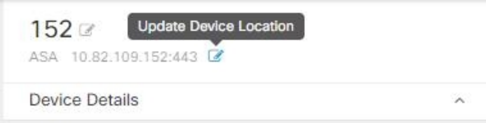
☑ Schedule Upgrade 07/26/2018 10:35 AM

Bulk Update Credentials

You can now update the credentials that CDO uses to connect to your ASA on multiple ASA devices at once. On the **Inventory** page, select multiple ASA devices, and click Update Credentials. For more information, see "Update ASA Connection Credentials" in *Managing ASA with Cisco Defense Orchestrator*.

Update Device Location

You can now update the device location of an onboarded ASA by clicking the edit button next to its IP address.



July 20, 2018

Update Credentials

You can now update the credentials that CDO uses to connect to your ASA. In the process of onboarding an ASA, you entered the username and password CDO must use to connect to the ASA. In the past, if you wanted to change those credentials or change the password, you needed to remove the ASA from CDO and onboard it again with the new credentials. Now you can change the credentials without having to re-onboard the ASA.

For more information, see "Updating ASA Connection Credentials" in *Managing ASA with Cisco Defense Orchestrator*.

July 12, 2018

New ASA Default Rule Behavior

When a new rule is added to an ASA network policy, it is assigned the "Permit" action by default.

Exported Device Lists Include the Tenant Name

When you export the device list of a particular tenant, the name of the tenant is now incorporated in the exported file name.

For more information, see "Export List of Devices and Services" in Managing ASA with Cisco Defense Orchestrator

Bulk Entry of Network Groups

When creating or editing an ASA network object group, you can now add IP addresses in bulk rather than one at a time.

For more information, see "Create or Edit ASA Network Objects and Network Groups" in Managing ASA with Cisco Defense Orchestrator.

May 2018

May 24, 2018

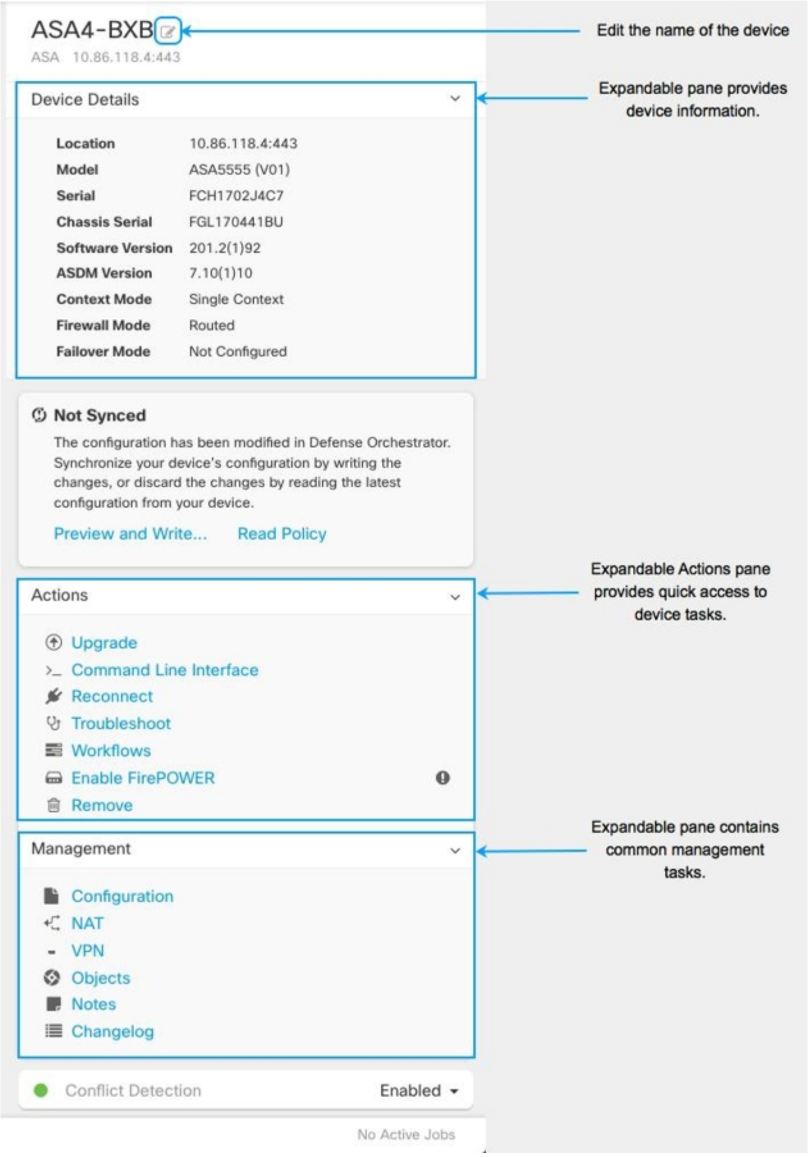
Support for Time-based ASA Network Policies

Time-based ASA Network policies allow access to networks and resources based on time of day. The time of day is defined by a time range object. Time range objects have a start time and an end time and can also be defined as a recurring event. For more information, see "Define a Time Range for a Policy" in *Managing ASA with Cisco Defense Orchestrator*.

May 17, 2018

New Device Details Panel Layout

We reorganized our device details panel to make device information and commonly used command buttons easier to find.



ASA4-BXB

ASA 10.86.118.4:443

Device Details

Location	10.86.118.4:443
Model	ASA5555 (V01)
Serial	FCH1702J4C7
Chassis Serial	FGL170441BU
Software Version	201.2(1)92
ASDM Version	7.10(1)10
Context Mode	Single Context
Firewall Mode	Routed
Failover Mode	Not Configured

Not Synced

The configuration has been modified in Defense Orchestrator. Synchronize your device's configuration by writing the changes, or discard the changes by reading the latest configuration from your device.

Conflict Detection: Enabled

No Active Jobs

Edit the name of the device

Expandable pane provides device information.

Expandable Actions pane provides quick access to device tasks.

Expandable pane contains common management tasks.

Support for ASA Global Access Policies

Now you can create a global access policy for your ASAs using CDO. A global access policy is a network policy applied to all the interfaces on an ASA. It is applied to inbound network traffic.With CDO, you can also copy a global access policy from one ASA to another to maintain consistency across devices. For more information, see " Configure an ASA Global Access Policy" in *Managing ASA with Cisco Defense Orchestrator*.

Network Address Translation Rule Wizard for ASA Devices

There is a new Network Address Translation (NAT) rule wizard to help you create NAT rules on your ASA devices for these use cases:

- Enable Internet Access for Internal Users
- Expose an Internal Server to the Internet

For more information, see "Network Address Translation Rule Wizard" in *Managing ASA with Cisco Defense Orchestrator*.

April 2018

April 26, 2018

New troubleshooting documentation

If Cisco Defense Orchestrator (CDO) and your ASA do not connect after an ASA reboot, it may be because the ASA has fallen back to using an OpenSSL cipher suite that is not supported by CDO's Secure Device Connector. The "ASA Fails to Reconnect to CDO After Reboot" troubleshooting topic tests for that case, provides a list of supported cipher suites, and remediation steps.

April 5, 2018

Access Control Entry (ACE) Limit Calculation

CDO displays the number of access control entries (ACEs) in individual rules, network policies, and the total number running on an ASA. Though there is no hard-coded limit to the number of ACEs that an ASA can process, an ASA's performance will degrade when the number of access control entries becomes too large. For more information, see "Access Control Entries (ACEs)" in *Managing ASA with Cisco Defense Orchestrator*.

March 2018

March 22, 2018

Unsuported Device

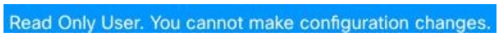
CDO does support the **ASA Service Module** (ASASM) at this time.

March 15, 2018

Read-only Users

We have created a read-only user role. Read-only users can view everything in CDO but they cannot create, update, configure, or delete anything on any page. Neither can they onboard devices.

Read-only users see a blue banner that reads, "Read Only User. You cannot make configuration pages." on every page



Read Only User. You cannot make configuration changes.

and they are identified by their role in the User Management table. For more information, see "User Roles" in *Managing ASA with Cisco Defense Orchestrator*.

Update Connection Credentials

When you onboard a device, you specify a username and password for that device. Cisco Defense Orchestrator connects to the device using those credentials and acts as that user when sending commands to the device. If users or passwords change on the device, you can update the device credentials to reflect those changes.

For more information, see the following topics:

- Updating ASA Connection Credentials—*Managing ASA with Cisco Defense Orchestrator*
- Updating AWS Connection Credentials—*Managing AWS with Cisco Defense Orchestrator*
- Updating Meraki MX Connection Credentials—*Managing Meraki with Cisco Defense Orchestrator*

Improved Network Policy Filtering

You can now filter network policies by hit count without first knowing which ASA the policy runs on. This allows you to find network policies with zero hit counts anywhere in your deployment. For more information, see "Filtering Use Cases" in *Managing ASA with Cisco Defense Orchestrator*.

Export Network Policy Rules

You can export the contents of each Access-Group or Crypto-Map to a .csv file. This .csv displays each Access Control List (ACL) and the data that CDO has for each ACL. For more information, see "Export Network Policy Rules" in *Managing ASA with Cisco Defense Orchestrator*.

March 7, 2018

New CDO Portal

We redesigned the portal to quickly communicate what you need to know, what you need to do, and where you go to do it.

Custom URL Upgrade

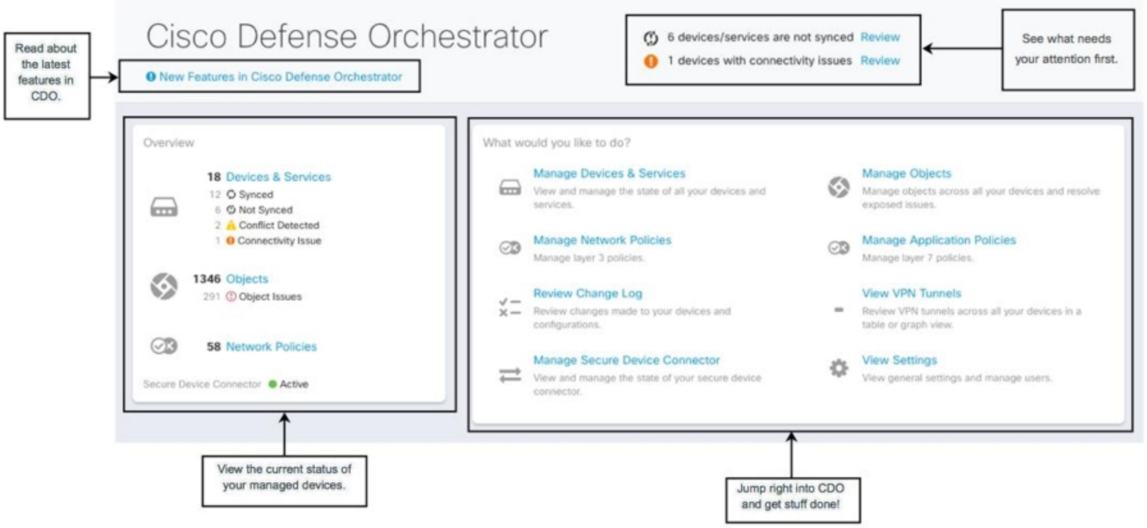
You can now upgrade your ASA device with ASA software and ASDM images you maintain in your own image repository. If your ASA does not have outbound access to the internet or you want an image that is not yet in CDO's image repository, this is the best way to upgrade your ASA. You can retrieve the images from your repository using any of these protocols: FTP, TFTP, HTTP, HTTPS, SCP, and SMB.

For more information, see "Custom URL Upgrade" in *Managing ASA with Cisco Defense Orchestrator*.

Device Notes

Now you can save notes about a specific ASA in a single, plain-text, file without leaving CDO. For more information, see "Device Notes" in *Managing ASA with Cisco Defense Orchestrator*.

February 2018



Read about the latest features in CDO.

See what needs your attention first.

View the current status of your managed devices.

Jump right into CDO and get stuff done!

Cisco Defense Orchestrator

New Features in Cisco Defense Orchestrator

6 devices/services are not synced Review

1 devices with connectivity issues Review

Overview

18 Devices & Services

12 Synced

6 Not Synced

2 Conflict Detected

1 Connectivity Issue

1346 Objects

291 Object Issues

58 Network Policies

Secure Device Connector ● Active

What would you like to do?

Manage Devices & Services

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

Manage Objects

Manage objects across all your devices and resolve exposed issues.

Manage Network Policies

Manage layer 3 policies.

Manage Application Policies

Manage layer 7 policies.

Review Change Log

Review changes made to your devices and configurations.

View VPN Tunnels

Review VPN tunnels across all your devices in a table or graph view.

Manage Secure Device Connector

View and manage the state of your secure device connector.

View Settings

View general settings and manage users.

February 29, 2018

See All the Accounts Associated with your Tenant

You will now be able to see all the users associated with your tenant on the **User Management** screen. This includes any Cisco support engineer temporarily associated with your account to resolve a support ticket.

To view the users associated with your tenant:

1. From the user menu, select **Settings**.
2. Click **User Management**.

Manage Cisco Access to Your Tenant

Cisco support will associate its users with your tenant to resolve support tickets or proactively fix issues that affect more than one customer. However, if you prefer, you can prevent Cisco support from accessing your account by changing your account settings. For more information, see "General Settings" in *Managing FTD with Cisco Defense Orchestrator*.

See All the Accounts Associated with your Tenant

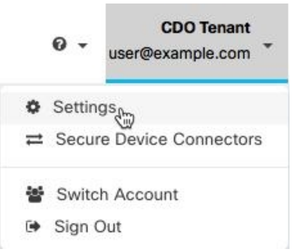
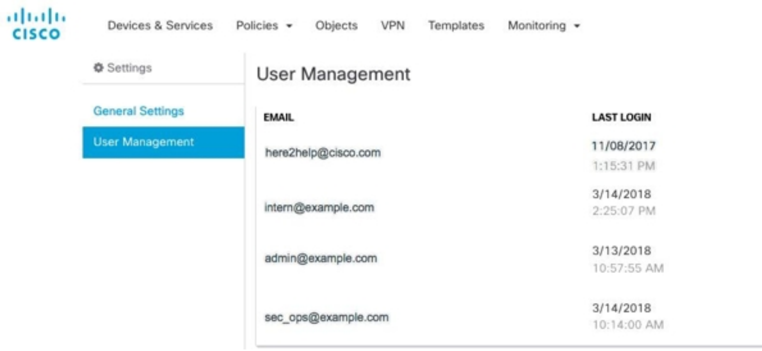
You will now be able to see all the users associated with your tenant on the **User Management** screen. This includes any Cisco support engineer temporarily associated with your account to resolve a support ticket.

To view the users associated with your tenant:

SUMMARY STEPS

1. From the user menu, select **Settings**
2. Click **User Management**

DETAILED STEPS

	Command or Action	Purpose
Step 1	From the user menu, select **Settings**	
Step 2	Click **User Management**	

User Management

EMAIL	LAST LOGIN
here2help@cisco.com	11/08/2017 1:15:31 PM
intern@example.com	3/14/2018 2:25:07 PM
admin@example.com	3/13/2018 10:57:55 AM
sec_ops@example.com	3/14/2018 10:14:00 AM

Manage Cisco Access to Your Tenant

Cisco support will associate its users with your tenant to resolve support tickets or proactively fix issues that affect more than one customer. However, if you prefer, you can prevent Cisco support from accessing your account by changing your account settings. See for more information.

February 15, 2018

Manage ASAs Using CLI Macros

CDO provides a list of complete CLI-based commands and command templates that are ready for you to customize and run on your ASAs. These CLI macros can be run on a single ASA or ASAs in bulk. Do you have a regular monitoring or maintenance task you perform? You can create and store your own CLI-based commands on CDO and reuse them when you need them.

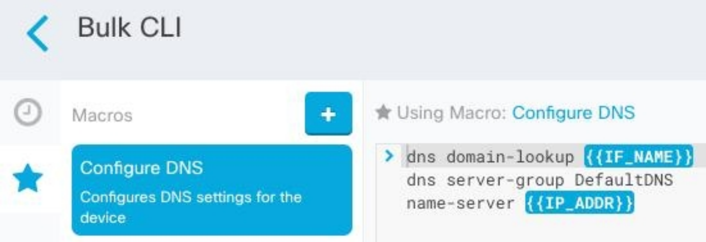
Manage ASAs Using CLI Macros

CDO provides a list of complete CLI-based commands and command templates that are ready for you to customize and run on your ASAs. These CLI macros can be run on a single ASA or ASAs in bulk. Do you have a regular monitoring or maintenance task you perform? You can create and store your own CLI-based commands on CDO and reuse them when you need them.

Here's an example of using a CLI macro to configure a DNS server on your ASAs:

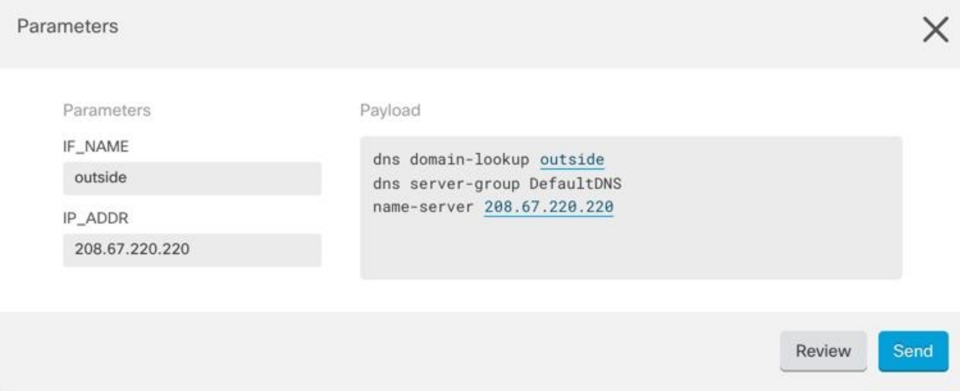
Step 1 Select the devices you need to configure.

Step 2 Select the Configure DNS macro.


Bulk CLI
Macros
+
Configure DNS
Configures DNS settings for the device
Using Macro: Configure DNS

```
dns domain-lookup {{IF_NAME}}
dns server-group DefaultDNS
name-server {{IP_ADDR}}
```

Step 3 Fill in the parameter fields with your information:



IF_NAME: outside

IP_ADDR: 208.67.220.220

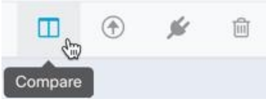
```
dns domain-lookup outside
dns server-group DefaultDNS
name-server 208.67.220.220
```

Step 4 Send it to all of your ASAs.

February 11, 2018

Compare ASA Configurations

You can now easily compare two ASA configurations. Select two ASAs in the **Inventory** page and click the compare button. CDO provides a side-by-side comparison of the devices' configurations. For more information, see "Compare ASA Configurations" in *Managing ASA with Cisco Defense Orchestrator*.



January 2018

January 31, 2018

Use CDO to Mitigate the Risks of Recent Cisco ASA Security Advisory

On January 29, 2018, the Cisco Product Security Incident Response Team (PSIRT) published the security advisory cisco-sa-20180129-asa1 describing an ASA and Firepower security vulnerability. Read our article, Using *CDO to Respond to Cisco ASA Advisory cisco-sa-20180129-asa1* to learn how to find the ASAs in your enterprise that are affected by the advisory and upgrade them to a patched version of ASA.

CDO Allows Long CLI Sequences

If you enter a long list of commands in the command box of the CLI, CDO attempts to break up your command into multiple commands so that they can be run against the ASA API at once. If CDO is unable to determine a proper separation in your command, it will prompt you for a hint. For example:

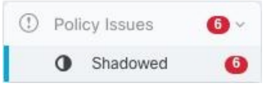
Error: CDO attempted to execute a portion of this command with a length that exceeded 600 characters. You can give a hint to CDO at where a proper command separation point is by breaking up your list of commands with an additional empty line between them.

For more information, see "ASA Command Line Interface" in *Managing ASA with Cisco Defense Orchestrator*.

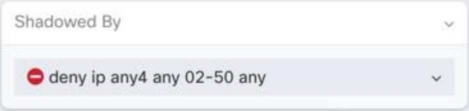
January 18, 2018

Enhancements to Help You Manage Shadow Rule Issues

- The ASA network policy issues filter indicate if there are any shadowed rules in a policy.



- A new badge ⚠ next to a rule in an ASA network policy indicates that it is shadowing another rule in the policy.
- For a shadowed rule, the network policy details pane identifies which rule in the policy is shadowing it.

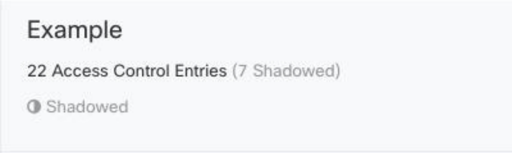

Shadowed By

deny ip any4 any 02-50 any

- New documentation on Resolving Shadow Rule Issues.

CDO Calculates Access Control Entries in your ASA Network Policies

Cisco Defense Orchestrator (CDO) calculates the number of access control entries (ACEs) derived from all the rules in an ASA network policy and displays that total at the top of the network policy details pane. If any of the rules in the network policy are shadowed, it lists that number as well.

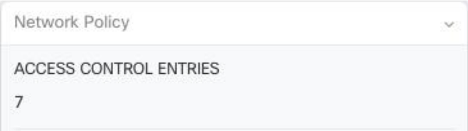


Example

22 Access Control Entries (7 Shadowed)

◑ Shadowed

CDO also displays the number of ACEs derived from a single rule in a network policy and displays that information in the network policy details pane. Here is an example of that listing:



Network Policy

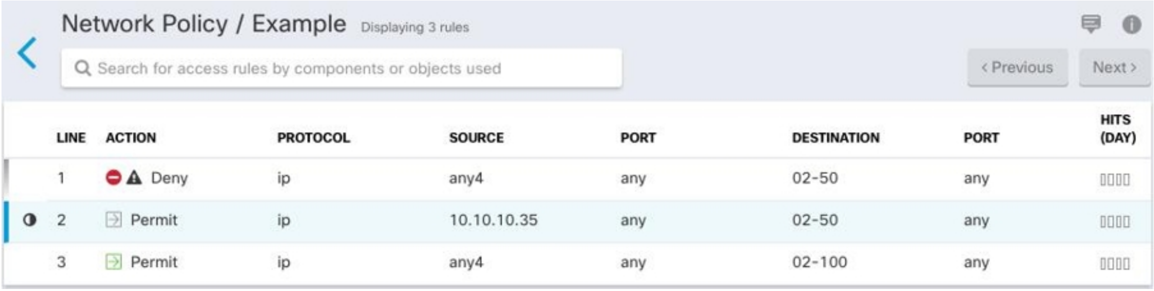
ACCESS CONTROL ENTRIES

7

ASAs have recommended limits on the number of ACEs created on a device. Following those recommendations allows the ASA to process network traffic at an optimal speed. Deleting unused rules or shadowed rules helps keep your ACE count down.

Numbered Lines in Network Policies

CDO numbers rules in network policies for easy reading. Lines are renumbered as you add and delete rules or reorder them in a policy.



Network Policy / Example Displaying 3 rules

Search for access rules by components or objects used

‹ Previous Next ›

	LINE	ACTION	PROTOCOL	SOURCE	PORT	DESTINATION	PORT	HITS (DAY)
	1	⛔ ⚠ Deny	ip	any4	any	02-50	any	▯▯▯▯
◑	2	Permit	ip	10.10.10.35	any	02-50	any	▯▯▯▯
	3	Permit	ip	any4	any	02-100	any	▯▯▯▯

January 4, 2018

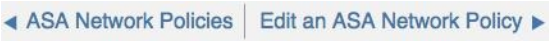
Enhanced ASA Network Policy Management

You can now perform these tasks with your ASA network policies!

- **Copy and paste policies between ASA devices**. Copy a policy from one ASA to another and assign it to a specific interface.
- **Cut and paste rules within policies**. Change the prioritization of rules within a policy by cutting and pasting them in the rule table.
- **Copy and paste rules between policies**. Promote policy consistency by copying a rule from one policy to another. These policies can be on the same device or on different devices.

These enhancements compliment existing functions like creating ASA network policies, activating or deactivating rules in a policy, and logging activity generated by rules in a policy.

For more information, see "Create or Edit ASA Network Objects and Network Groups" and "ASA Network Policies" in *Managing ASA with Cisco Defense Orchestrator* and navigate through the ASA network policy documentation using the topic arrows at the bottom of a page:



CHAPTER 8

Feature Highlights of 2017

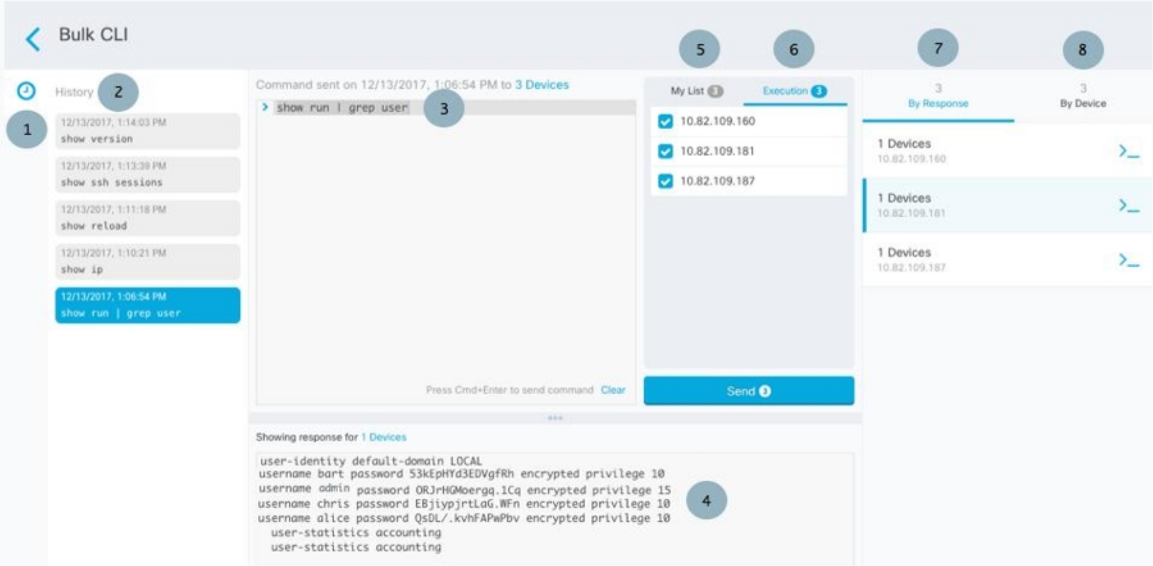
This articles highlights some of the features added to Cisco Defense Orchestrator in 2017.

December 2017

December 14, 2017

Bulk Command Line Interface

Cisco Defense Orchestrator (CDO) promotes consistent configurations across your devices by giving administrators the ability to send one command to multiple devices simultaneously. CDO groups responses to a bulk CLI command by response type and by device type so you can identify which ASAs returned a certain response and which devices were sent a particular command. CDO maintains a historical list of your commands so you can rerun them or modify them. For more information, see "Bulk Command Line Interface" in *Managing ASA with Cisco Defense Orchestrator*.



12/13/2017, 1:14:03 PM
show version

12/13/2017, 1:13:39 PM
show ssh sessions

12/13/2017, 1:11:18 PM
show reload

12/13/2017, 1:10:21 PM
show ip

12/13/2017, 1:06:54 PM
show run | grep user

Command sent on 12/13/2017, 1:06:54 PM to 3 Devices

```
> show run | grep user
```

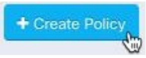
☑ 10.82.109.160
☑ 10.82.109.181
☑ 10.82.109.187

Showing response for 1 Devices

```
user-identity default-domain LOCAL
username bart password 53kEpHYd3EDVgfRh encrypted privilege 10
username admin password ORJrHGMoergq.1Cq encrypted privilege 15
username chris password EBjiypjrtLaG.WFn encrypted privilege 10
username alice password QsDL/.kvhFAPwPbv encrypted privilege 10
  user-statistics accounting
  user-statistics accounting
```

Create ASA Network Policies

Now you can create a network policy for an ASA. You can add rules to the policy, change the order of rules within a policy, activate or deactivate rules within the policy, as well as copy that policy from one ASA to another! See "Create an ASA Network Policy" in *Managing ASA with Cisco Defense Orchestrator* to get started!



November 2017

November 9, 2017

Bulk Operations

Certain CDO configuration tasks can be performed on multiple devices at the same time; they can be done "in bulk." This feature saves you time and promotes consistency among your devices. These are the operations you can perform in bulk and some additional features we've added to compliment them.

Bulk ASA and ASDM Upgrades

You can now use CDO's upgrade wizard to upgrade the ASA and ASDM images on multiple ASAs simultaneously. We make the process easy by performing all the necessary upgrade steps behind the scenes. The wizard guides you through the process of choosing compatible ASA and ASDM software images, installing them, and rebooting the device to complete the upgrade. We secure the upgrade process by validating that the images you choose on CDO are the ones copied to, and installed on, your ASA. For more information, see "Bulk ASA and ASDM Upgrade" in *Managing ASA with Cisco Defense Orchestrator*.

Bulk Read Configurations

If a configuration change is made to a device outside of CDO, the device's configuration stored on CDO and the device's local configuration are no longer the same. In this case, CDO displays a "Conflict detected" message to alert the administrator. The administrator performs a "Read policy" action, which overwrites the configuration on CDO with the configuration stored on the device. The two configurations are now the same, they are "Synced." The bulk read configuration function allows administrators to perform this action on multiple devices at the same time.

Another use for bulk reading configurations is to prevent changes staged on CDO from being written to your devices. By reading the configurations from the device to CDO, you overwrite all staged changes on CDO. This could also be a good way to revert changes you made to your devices' configurations on CDO if you need to. For more information, see "Bulk Read Configuration" in *Managing ASA with Cisco Defense Orchestrator*.

Bulk Reconnecting Devices

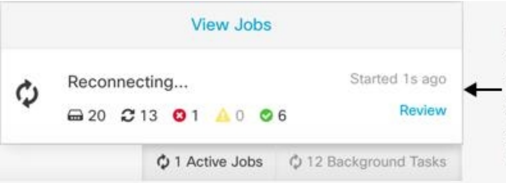
CDO allows an administrator to attempt to reconnect more than one managed device to CDO simultaneously. When a device CDO manages is marked "unreachable," CDO can no longer detect out of band configuration changes or mange the device. Attempting to reconnect the devices is a simple first step in restoring CDO's management of the device. For more information, see "Bulk Reconnecting Devices" in *Managing ASA with Cisco Defense Orchestrator*.

Bulk Enabling and Disabling of Conflict Detection

You can enable or disable conflict detection for multiple devices simultaneously. Enabling conflict detection will alert you to instances where changes have been made to a device outside of CDO. For more information, see "Enabling Conflict Detection" in *Managing ASA with Cisco Defense Orchestrator*.

Jobs Notifications

The notifications tab is located at the bottom right corner of CDO. It displays an active count of ongoing actions in a job.



The notifications tab displays status information about the job. This example shows the bulk action (Reconnect), the number of actions in the job (20), actions being processed (13), number of actions failed (1), number of warnings (0), and number of actions succeeded (6).

Jobs Page

The Jobs page displays information about the status, success, and failure of a bulk operation. Color-coded rows in the jobs table indicate individual actions that have succeeded or failed. For more information, see "Jobs Page" in *Managing ASA with Cisco Defense Orchestrator*.

Reinitiate a Task for a Failed Action

CDO remembers the bulk operation, identifies individual actions that failed, and saves you time by re-running the task on only the failed actions. When reviewing the jobs page, if you find one or more actions in a bulk operation that failed, you can re-run the bulk operation after you have made whatever corrections are necessary. CDO will re-run the job on only the failed actions. For more information, see "Reinitiating a Bulk Operation that Resulted in a Failed Action" in *Managing ASA with Cisco Defense Orchestrator*.

NAT Documentation

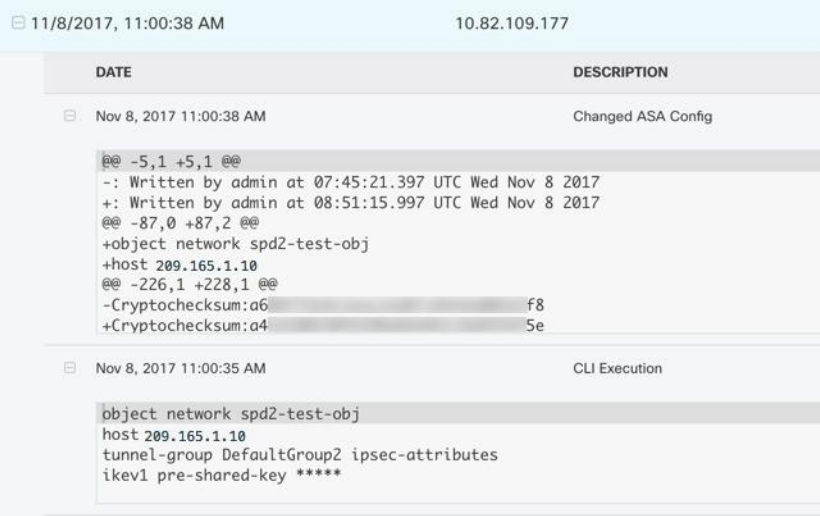
We have documented procedures for these use cases:

- Enable a Server on the Inside Network to Reach the Internet Using a Public IP Address

- Make a server on the inside network available to users on a specific port of a public IP address
- Translate a range of private IP addresses to a range of public IP addresses

CLI Logging

Whenever you use CDO to execute a CLI command on an ASA, the command and the results of the command are now logged in the device's changelog. In the example below, the entry for CLI Execution row shows what commands were sent and the Changed ASA Config row shows what was changed in the configuration file as a result of the commands.



⊟ 11/8/2017, 11:00:38 AM 10.82.109.177

DATE	DESCRIPTION
⊟ Nov 8, 2017 11:00:38 AM	Changed ASA Config

```
@@ -5,1 +5,1 @@
-: Written by admin at 07:45:21.397 UTC Wed Nov 8 2017
+: Written by admin at 08:51:15.997 UTC Wed Nov 8 2017
@@ -87,0 +87,2 @@
+object network spd2-test-obj
+host 209.165.1.10
@@ -226,1 +228,1 @@
-Cryptochecksum:a6[redacted]f8
+Cryptochecksum:a4[redacted]5e
```

DATE	DESCRIPTION
⊟ Nov 8, 2017 11:00:35 AM	CLI Execution

```
object network spd2-test-obj
host 209.165.1.10
tunnel-group DefaultGroup2 ipsec-attributes
ikev1 pre-shared-key *****
```

October 2017

October 19, 2017

Bulk Onboarding of ASAs

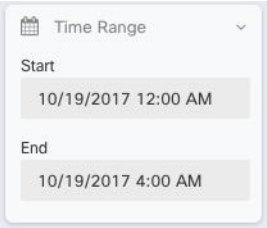
You can now onboard multiple ASAs to CDO in a single batch. For more information, see "Onboard ASAs in Bulk" in *Managing ASA with Cisco Defense Orchestrator*.

Shared Network Policies

Cisco Defense Orchestrator (CDO) finds identical network policies used by multiple ASAs and identifies them on the network policy page. If you have a shared network policy, you can change it once and distribute the change to the other devices that share the policy. This keeps network policies consistent across devices. For more information, see "Shared Network Policies" in *Managing ASA with Cisco Defense Orchestrator*.

Filter Change Logs by Time and Date

You can now filter events in the change log by time and date. Navigate Monitoring > Change Log and find this time and date calendar in the filter bar:



Time Range

Start

10/19/2017 12:00 AM

End

10/19/2017 4:00 AM

October 12, 2017

Packet Tracer

Packet tracer helps you troubleshoot access and policy issues. Packet tracer sends a synthetic packet into the network and evaluates how the saved routing configuration, NAT rules, and policy configurations interact with that packet. For example, if a rule is dropping packets, packet tracer identifies that rule for you and gives you a link to it, so you can evaluate it and edit it. Packet tracer can be used on a live, online, physical or virtual Adaptive Security Appliance (ASA). For more information, see "ASA Packet Tracer" in *Managing ASA with Cisco Defense Orchestrator*.

October 5, 2017

New Screencast!

▶

New screencast demonstrating how you can use CDO to upgrade a single ASA or two ASAs configured as an active/standby failover pair.

September 2017

September 28, 2017

Updated Documentation

- Resolve configuration Conflicts - A troubleshooting topic that describes what to do when you have a device that is "Not Synced" or reports "Conflict Detected."
- Configuration Changes Made to ASAs in Active-Active Failover Mode - Provides important information about making configuration changes to ASA's configured in Failover mode as an Active-Active pair.
- Resolving Certificate Issues - A troubleshooting topic that explores why CDO may reject a certificate and what to do about it.
- Updates to our Frequently Asked Questions page.

September 14, 2017

CDO Service Status Page

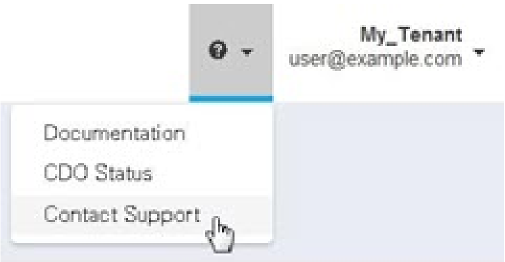
CDO maintains a customer-facing service status page at https://status.defenseorchestrator.com/. The page shows if the CDO service is up and any service interruptions it may have had. You can view up-time information with daily, weekly, or monthly graphs.

On the status page, you can click **Subscribe to Updates** to receive a notification if the CDO service goes down.

CDO Support Page

Customers can now get support through the CDO interface:

- Paying customers should open support cases directly with Cisco's Technical Assistance Center (TAC) by clicking **Support Case Manager** on the new Contact Support page.
- All demo, internal, and trial customers can send email to cdo.support@cisco.com by entering their question in the details request form on the Contact Support page. A member of our support staff will respond as soon as possible.



September 7, 2017

External Links for Devices

You can now create a hyperlink to an external resource and associate it with a device you manage with CDO. You could use this feature to create a convenient link to a search engine, documentation resource, a corporate wiki, or any other URL you choose. You can associate as many external links with a device as you want. You can also associate the same link with multiple devices at the same time.

August 2017

August 17, 2017

New Object Functions

- **Resolving Duplicate, Inconsistent, and Unused Objects**: When resolving object issues, you will have better visibility into network and services objects. You see a consolidated view of all the objects in the group, making it easier to compare object to object. You also have command buttons to resolve object issues by merging, renaming, or ignoring them.

- **New object filtering:** More precise search capabilities to find the objects you are looking for.

August 10, 2017

Upgrades to ASAs configured as an Active/Standby Failover Pair

CDO has extended the functionality of the upgrade wizard to include upgrading ASAs configured as an active/standby failover pair. You use the same wizard functionality as you did for upgrading individual ASAs but now you can upgrade an active/standby failover pair. For more information about this feature, see "Upgrading ASA and ASDM Images in an Active-Standby Pair" in *Managing ASA with Cisco Defense Orchestrator*.

August 3, 2017

Upgrades to Individual ASAs in Single Context or Multi-Context Mode

CDO now provides a wizard that allows you to upgrade the ASA and ASDM images installed on an individual ASA in single or context or multi-context mode. We make the process easy by performing all the necessary upgrade steps behind the scenes. The wizard guides you through the process of choosing compatible ASA Software and ASDM images, installing them, and rebooting the device to complete the upgrade. We secure the upgrade process by validating that the images you chose on CDO are the ones copied to, and installed on, your ASA.

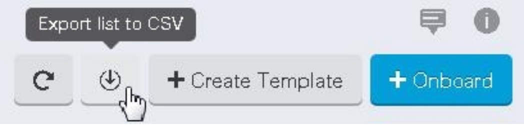
Click in the details pane of the **Inventory** page to start your upgrade. For more information, see "Upgrading ASA and ASDM Images" in *Managing ASA with Cisco Defense Orchestrator*.

June 2017

June 20, 2017

Export List of Devicses and Services

You can now export a list of the devices and services on the **Inventory**page to a comma-separated value (.csv) file. From there, you can open the file in a spreadsheet application such as Microsoft Excel to sort and filter the items in your list.

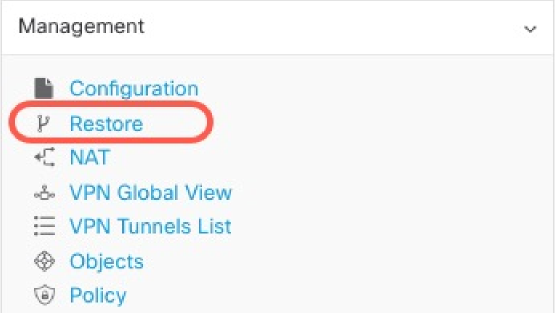


For more information, see "Exporting the Change Log to a CSV File" in Managing FTD with Cisco Defense Orchestrator".

June 13, 2017

ASA Configuration Restore

You can now return an ASA to one of its previously saved configurations. This is a convenient way to remove a configuration change that had unexpected or undesired results. Choose the ASA configuration you want to restore, CDO shows you a comparison of that configuration and the last configuration saved to memory, and if you are satisfied that you are restoring the desired configuration you can restore it.



For more information, see "Restoring ASA Configurations" in *Managing ASA with Cisco Defense Orchestrator*.

May 2017

May 3, 2017

Change Request Management.

You can now associate a change request and its business justification, opened in a separate ticketing system, with an event in the Change Log. Change request management allows you to create a change request in CDO, identify it with a unique name, enter a description of the change, and associate the change request with change log events. You can later search the Change Log for the change request name.

For more information, see "Change Request Management" in *Managing FTD with Cisco Defense Orchestrator*.

April 2017

Improved search: The Inventory page search bar now supports partial matches, making easier to find the device or service you want.

VPN: Various usability improvements.

February 2017

Cisco Defense Orchestrator New EMEA Site

Application Visibility Control (AVC) Identity Profile Support

January 2017

Read only IPSec VPN Tunnel Management

Cisco Defense Orchestrator now supports parsing and processing of IPsec Site-to-Site VPN ASA device configurations. A network-based VPN tunnel diagram is available and provides a complete view of all tunnels connected to a single peer, its tunnel details including the access policies, key exchange encryption, and its connectivity status. CDO also provides a complete view of all tunnels available in the configuration of an organization's onboarded ASA devices. CDO's new VPN management capabilities provides organization and network operations engineers to:

- Visualize their entire VPN tunnels both on a per device basis as well as across all devices
- Easily identify tunnel misconfiguration by using the tunnel connectivity state and at a glance view of its access policy and cryptomap encryption

VPNs are secure but must be configured properly to ensure stable and secure communication. CDO can help by enabling users an organizational view of their VPN configurations to facilitate the reduction of bloated and outdated policies.

Network and Service Single Object Support

In addition to Object Group support available today, Cisco Defense Orchestrator now enables creation of a single object of both network and service type during Access Rule modification, or directly from the Objects page.

CHAPTER 9

Feature Highlights of 2016

This article describes some of the features that were added to Cisco Defense Orchestrator in 2016

December 2016

December 22, 2016

NAT Policy Management

Cisco Defense Orchestrator now supports reading, editing, searching, and creating NAT policies via an easy to use navigation wizard and advanced interface-based diagram, to show a full list of NAT policies (and their order) defined on an ASA device.

December 15, 2016

Obsolete Names (Objects) conversion

Your device's configuration contains legacy (obsolete) names ? Cisco Defense Orchestrator now enables, during objects issues resolution, to investigate across objects, object groups and now names to provide consistency across all objects used in policy and to assist with the conversion of names into object.

November 2016

November 18, 2016

Fully Shadowed Rules Support

You can now filter and identify superfluous network policies that will never handle traffic intended, as all traffic is handled by a rule(s) up in rule set order. Upon making a change to network policies, CDO will alert in case rule edited or added is shadowed by a different rule.

November 8, 2016

On-Prem Secure Device Connector

Cisco Defense Orchestrator enables direct communication between CDO and supported devices and services. This communication is enabled by CDO Secure Device Connector (SDC) acting as proxy between remote location and CDO cloud services. This service is available now in two deployment models as follows:

On-Prem Secure Device Connector – On-prem Secure Device Connector is a pre-configured virtual appliance dedicated to the requested account.

Cloud Secure Device Connector – All cloud Secure Device Connectors are provisioned automatically and managed by Cisco Defense Orchestrator team.

September 2016

September 29, 2016

Change Log

Continuous capture of both application (layer7) and network (layer3) policy changes performed via Cisco Defense Orchestrator within a single view across on-boarded devices and services. New Change Log lists at-a-glance view of most recent changes, while further revisions can be sorted and filters by device, change status, user and more. New Change Log functionality enables organizations to:

- Before and after inline incremental view (diff) of a network and application policy change (new, edited, and deleted rule; on-boarded or deleted devices and services, and more)
- Detection of policy change conflicts (occurring outside of Cisco Defense Orchestrator) and overwriting to/from a device or service
- Be able to answer Who, What, and When during an incident investigation or troubleshooting
- Export to a common format or 3rd party monitoring systems

Note Devices and services currently managed by Cisco Defense Orchestrator will initiate change log event collection only after first deploy or read. For more information, see "Secure Logging Analytics for FTD Devices" in *Managing FTD with Cisco Defense Orchestrator*.

Hit Rates. Cisco Defense Orchestrator now enable network operations users to evaluate policy rules outcome, on top of secure and scalable orchestration of policies, providing simple visualization for more accurate policy analysis and immediate actionable pivot to root cause, all in a single pane from the cloud. New Hit Rates functionality enable organizations to:

- Eliminate obsolete and never matched policy rules increasing security posture
- Optimize Firewall performance by instantly identifying bottlenecks as well as correct and efficient prioritization is enforced (most triggered policy rule prioritized higher)
- Maintain Hit Rates history information even upon device or policy rule reset for configured data retention (1 year)
- Strengthen validation on suspected shadow and unused rules based on actionable information. Removing doubt about update or delete of those
- Visualize policy rules usage in context to entire policy, leveraging pre-defined time intervals (day, week, month, year) and scale of actual hits (zero, >100, >100k, etc.), to evaluate impact on packets traversing the network

September 23, 2016

User interface redesign: Change to Light Theme

Redesign Cisco Defense Orchestrator user experience with a light brand new user experience theme making it more intuitive, self-explanatory, and Cisco style aligned. Try it out!

Multiple Objects Support

Cisco Defense Orchestrator object management now enables inline editing of object and object group value(s) as well as referencing multiple objects in a single access list parameter; automatically assigning to a user-defined object group (without the need for dm_inline_* object creation).

Approve or Reject Out-of-Band Policy Modifications

Enhanced policy orchestration enforcement by not only identifying a remote change performed or what the change was (on a device or service), but the ability to approve or reject identified out-of-band changes in real-time.

August 2016

August 18, 2016

Delegated Admin Support

Delegated Admin Support. Cisco Defense Orchestrator enable managing more than a single account (tenant) per user for easier and faster pivot between assigned accounts, while maintaining account security and complete data separation between accounts (tenants).

Import & Export of Pre-Defined Templates

Enable Import Pre-defined Templates. Leverage pre-defined device configuration templates, either available in your organization or from a third-party, to enable the scalable orchestration of onboarding all devices and services in your organization.

Devices and Services Connection Status Management

Device Connection Status Evaluation. New "*Reconnect*" button added to enable continuous monitoring of devices and services availability state, and alert for any change or actions need to be taken automatically or on-demand (e.g. update device credentials, renew device certificate).

August 11, 2016

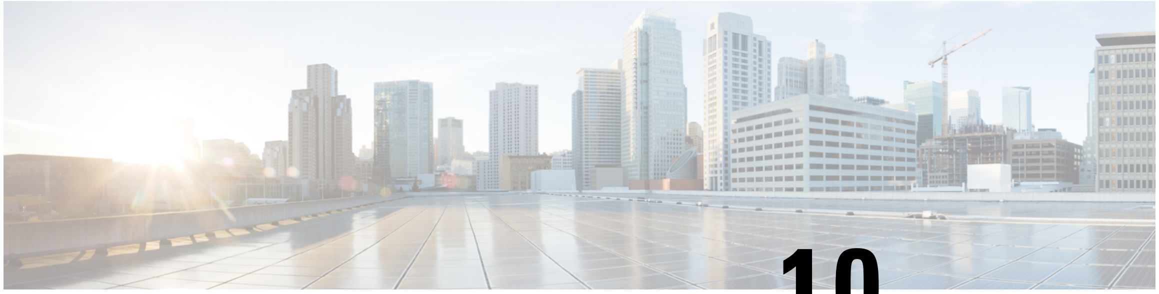
Enhanced Template Management

Manage Template Enhancements. When creating new or updating an existing device template configuration file, a Cisco Defense Orchestrator user can now easily search across a device configuration file and assign multiple values to new or existing parameters, for use across account's devices.

. For further information on creating and managing template, see "Templates" in Managing FTD with Cisco Defense Orchestrator.

PART II

New Features in Cloud-Delivered Firewall Management Center



CHAPTER 10

New Features in Cloud-delivered Firewall Management Center 2024

April 2, 2024

This release introduces stability, hardening, and performance enhancements.

February 13, 2024

New Features

Table 1: New Features: Version 20240203

Feature	Min. Threat Defense	Details
Platform		
Threat defense Version 7.4.1 support.	7.4.1	You can now manage threat defense devices running Version 7.4.1.
Network modules for the Secure Firewall 3130 and 3140.	7.4.1	The Secure Firewall 3130 and 3140 now support these network modules: • 2-port 100G QSFP+ network module (FPR3K-XNM-2X100G) See: Cisco Secure Firewall 3110, 3120, 3130, and 3140 Hardware Installation Guide

Feature	Min. Threat Defense	Details
Optical transceivers for Firepower 9300 network modules.	7.4.1	The Firepower 9300 now supports these optical transceivers: • QSFP-40/100-SRBD • QSFP-100G-SR1.2 • QSFP-100G-SM-SR On these network modules: • FPR9K-NM-4X100G • FPR9K-NM-2X100G • FPR9K-DNM-2X100G See: Cisco Firepower 9300 Hardware Installation Guide
Performance profile support for the Secure Firewall 3100.	7.4.1	The performance profile settings available in the platform settings policy now apply to the Secure Firewall 3100. Previously, this feature was supported on the Firepower 4100/9300, the Secure Firewall 4200, and on threat defense virtual. See: Configure the Performance Profile
NAT		
Create network groups while editing NAT rules.	Any	You can now create network groups in addition to network objects while editing a NAT rule. See: Customizing NAT Rules for Multiple Devices
Device Management		
Device management services supported on user-defined VRF interfaces.	Any	Device management services configured in the threat defense platform settings (NetFlow, SSH access, SNMP hosts, syslog servers) are now supported on user-defined Virtual Routing and Forwarding (VRF) interfaces. Platform restrictions: Not supported with container instances or clustered devices. See Platform Settings
SD-WAN		
SD-WAN Summary dashboard	7.4.1	The WAN Summary dashboard provides a snapshot of your WAN devices and their interfaces. It provides insight into your WAN network and information about device health, interface connectivity, application throughput, and VPN connectivity. You can monitor the WAN links and take proactive and prompt recovery measures. In addition, you can also monitor the WAN interface application performance using the **Application Monitoring** tab. New/modified screens: **Analysis** > **SD-WAN Summary** See: SD-WAN Summary Dashboard
Access Control: Identity		

Feature	Min. Threat Defense	Details
Captive portal support for multiple Active Directory realms (realm sequences).	7.4.1	**Upgrade impact. Update custom authentication forms.** You can configure active authentication for either an LDAP realm; or a Microsoft Active Directory realm or a realm sequence. In addition, you can configure a passive authentication rule to fall back to active authentication using either a realm or a realm sequence. You can optionally share sessions between managed devices that share the same identity policy in access control rules. In addition, you have the option to require users to authenticate again when they access the system using a different managed device than they accessed previously. If you use the HTTP Response Page authentication type, after you upgrade threat defense, you must add **`<select name="realm" id="realm"></select>`** to your custom authentication form. This allows the user to choose between realms. Restrictions: Not supported with Microsoft Azure Active Directory. New/modified screens: • **Policies** > **Identity** > **(edit policy)** > **Active Authentication** > **Share active authentication sessions across firewalls** • **Identity policy** > **(edit)** > **Add Rule** > **Passive Authentication** > **Realms & Settings** > **Use active authentication if passive or VPN identity cannot be established** • **Identity policy** > **(edit)** > **Add Rule** > **Active Authentication** > **Realms & Settings** > **Use active authentication if passive or VPN identity cannot be established** See: How to Configure the Captive Portal for User Control
Share captive portal active authentication sessions across firewalls.	7.4.1	Determines whether or not users are required to authenticate when their authentication session is sent to a different managed device than one they previously connected to. If your organization requires users to authenticate every time they change locations or sites, you should *disable* this option. • (Default.) Enable to allow users to authenticate with any managed device associated with the active authentication identity rule. • Disable to require the user to authenticate with a different managed device, even if they have already authenticated with another managed device to which the active authentication rule is deployed. New/modified screens: **Policies** > **Identity** > **(edit policy)** > **Active Authentication** > **Share active authentication sessions across firewalls** See: How to Configure the Captive Portal for User Control
Deployment and Policy Management		

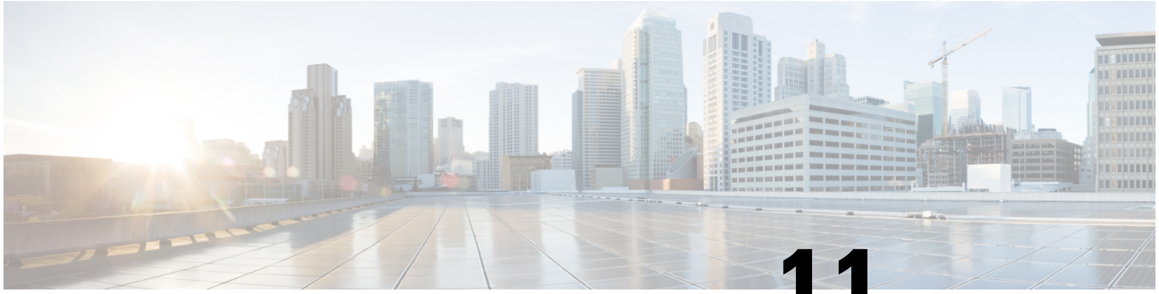
Feature	Min. Threat Defense	Details
View and generate reports on configuration changes since your last deployment.	Any	You can generate, view, and download (as a zip file) the following reports on configuration changes since your last deployment: • A policy changes report for each device that previews the additions, changes, or deletions in the policy, or the objects that are to be deployed on the device. • A consolidated report that categorizes each device based on the status of policy changes report generation. This is especially useful after you upgrade threat defense devices, so that you can see the changes made by the upgrade before you deploy. New/modified screens: **Deploy** > **Advanced Deploy**. See: Download Policy Changes Report for Multiple Devices
Suggested release notifications.	Any	The management center now notifies you when a new suggested release is available. If you don't want to upgrade right now, you can have the system remind you later, or defer reminders until the next suggested release. The new upgrade page also indicates suggested releases. See: Cisco Secure Firewall Management Center New Features by Release
Enable revert from the threat defense upgrade wizard.	Any	You can now enable revert from the threat defense upgrade wizard. Other version restrictions: You must be upgrading threat defense to Version 7.2+. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center
View detailed upgrade status from the threat defense upgrade wizard.	Any	The final page of the threat defense upgrade wizard now allows you to monitor upgrade progress. This is in addition to the existing monitoring capability on the Upgrade tab on the Device Management page, and on the Message Center. Note that as long as you have not started a new upgrade flow, **Devices** > **Threat Defense Upgrade** brings you back to this final wizard page, where you can view the detailed status for the current (or most recently complete) device upgrade. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center
Firmware upgrades included in FXOS upgrades.	Any	**Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.** For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1 now include firmware upgrades. If any firmware component on the device is older than the one included in the FXOS bundle, the FXOS upgrade also updates the firmware. If the firmware is upgraded, the device reboots twice—once for FXOS and once for the firmware. Just as with software and operating system upgrades, do not make or deploy configuration changes during firmware upgrade. Even if the system appears inactive, do not manually reboot or shut down during firmware upgrade. See: Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide
Upgrade		

Feature	Min. Threat Defense	Details
Improved upgrade starting page and package management.	Any	A new upgrade page makes it easier to choose, download, manage, and apply upgrades to your entire deployment. The page lists all upgrade packages that apply to your current deployment, with suggested releases specially marked. You can easily choose and direct-download packages from Cisco, as well as manually upload and delete packages. Patches are not listed unless you have at least one appliance at the appropriate maintenance release (or you manually uploaded the patch). You must manually upload hotfixes. New/modified screens: • **System** (⚙) > **Product Upgrades** is now where you upgrade devices, as well as manage upgrade packages. • **System** (⚙) > **Content Updates** is now where you update intrusion rules, the VDB, and the GeoDB. • **Devices** > **Threat Defense Upgrade** takes you directly to the threat defense upgrade wizard. Deprecated screens/options: • **System** (⚙) > **Updates** is deprecated. All threat defense upgrades now use the wizard. • The **Add Upgrade Package** button on the threat defense upgrade wizard has been replaced by a **Manage Upgrade Packages** link to the new upgrade page. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center
Administration		
Updated internet access requirements for direct-downloading software upgrades.	Any	The management center has changed its direct-download location for software upgrade packages from sourcefire.com to amazonaws.com. See: Internet Access Requirements
Scheduled tasks download patches and VDB updates only.	Any	The **Download Latest Update** scheduled task no longer downloads maintenance releases; now it only downloads the latest applicable patches and VDB updates. To direct-download maintenance (and major) releases to the management center, use **System** (⚙) > **Product Upgrades**. See: Software Update Automation
Smaller VDB for lower memory Snort 2 devices.	Any with Snort 2	For VDB 363+, the system now installs a smaller VDB (also called *VDB lite*) on lower memory devices running Snort 2. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Lower memory devices: ASA-5508-X and ASA 5516-X See: Update the Vulnerability Database

Deprecated Features

Table 2: Deprecated Features: Version 20240203

Feature	Deprecated in Threat Defense	Details
Deprecated: DHCP relay trusted interfaces with FlexConfig.	Any	You can now use the management center web interface to configure interfaces as trusted interfaces to preserve DHCP Option 82. If you do this, these settings override any existing FlexConfigs, although you should remove them. See: Configure the DHCP Relay Agent
Deprecated: Merging downloadable access control list with a Cisco attribute-value pair ACL for RADIUS identity sources with FlexConfig.	Any	This feature is now supported in the management center web interface.
Deprecated: `frequent drain of events` health alerts.	7.4.1	The Disk Usage health module no longer alerts with `frequent drain of events`. You may continue to see these alerts until you either deploy health policies to managed devices (stops the display of alerts) or upgrade devices to Version 7.4.1+ (stops the sending of alerts). See: Disk Usage and Drain of Events Health Monitor Alerts



CHAPTER 11

New Features in Cloud-delivered Firewall Management Center 2023

November 30, 2023

Table 3: New Features: Version 20231117

Feature	Min. Threat Defense	Details
Administration		
Schedule a Secure Firewall Threat Defense Device Backup in Cloud-delivered Firewall Management Center	Any	Use the cloud-delivered Firewall Management Center to perform scheduled backups of the Secure Firewall Threat Defense devices it manages. See Schedule Remote Device Backups for more information.

October 19, 2023

Table 4: New Features: Version 20230929

Feature	Min. Threat Defense	Details
Platform		
Threat defense Version 7.4.0 support.	7.4.0	You can now manage threat defense devices running Version 7.4.0. Version 7.4.0 is available *only* on the Secure Firewall 4200. You must use a Secure Firewall 4200 for features that require Version 7.4.0. Support for all other platforms resumes in Version 7.4.1.
Secure Firewall 4200.	7.4.0	You can now manage the Secure Firewall 4215, 4225, and 4245 with cloud-delivered Firewall Management Center. These devices support the following new network modules: • 2-port 100G QSFP+ network module (FPR4K-XNM-2X100G) • 4-port 200G QSFP+ network module (FPR4K-XNM-4X200G) See: Cisco Secure Firewall 4215, 4225, and 4245 Hardware Installation Guide
Performance profile support for the Secure Firewall 4200.	7.4.0	The performance profile settings available in the platform settings policy now apply to the Secure Firewall 4200. Previously, this feature was supported only on the Firepower 4100/9300 and on threat defense virtual. See: Configure the Performance Profile
Numbering convention for cloud-delivered Firewall Management system.	Any	The cloud-delivered Firewall Management system is a feature of CDO. For the purposes of troubleshooting, we identify the version number of the cloud-delivered Firewall Management Center on the FMC Services page. See: View Services Page Information.
Platform Migration		
Migrate from Firepower 1000/2100 to Secure Firewall 3100.	Any	You can now easily migrate configurations from the Firepower 1000/2100 to the Secure Firewall 3100. New/modified screens: **Devices** > **Device Management** > **Migrate** Platform restrictions: Migration not supported from the Firepower 1010 or 1010E. See: Migrate the Configuration to a new Model.

Feature	Min. Threat Defense	Details
Migrate devices from Firepower Management Center 1000/2500/4500 to cloud-delivered Firewall Management Center.	Any	

Feature	Min. Threat Defense	Details
		You can migrate devices from Firepower Management Center 1000/2500/4500 to cloud-delivered Firewall Management Center. To migrate devices, you must *temporarily* upgrade the on-prem management center from Version 7.0.3 (7.0.5 recommended) to Version 7.4.0. This temporary upgrade is required because Version 7.0 management centers do not support device migration to the cloud. Additionally, only standalone and high availability threat defense devices running Version 7.0.3+ (7.0.5 recommended) are eligible for migration. Cluster migration is not supported at this time. **Important** Version 7.4.0 is only supported on the 1000/2500/4500 during the migration process. You should minimize the time between management center upgrade and device migration. To summarize the migration process: **1.** Prepare for upgrade and migration. Read, understand, and meet all the prerequisites outlined in the release notes, upgrade guides, and migration guide. Before you upgrade, it is especially important that the on-prem management center is "ready to go," that is, managing only the devices you want to migrate, configuration impact assessed (such as VPN impact), freshly deployed, fully backed up, all appliances in good health, and so on. You should also provision, license, and prepare the cloud tenant. This must include a strategy for security event logging; you cannot retain the on-prem management center for analytics because it will be running an unsupported version. **2.** Upgrade the on-prem management center and all its managed devices to at least Version 7.0.3 (Version 7.0.5 recommended). If you are already running the minimum version, you can skip this step. **3.** Upgrade the on-prem management center to Version 7.4.0. Unzip (but do not untar) the upgrade package before uploading it to the management center. Download from: Special Release. **4.** Onboard the on-prem management center to CDO. **5.** Migrate all devices from the on-prem management center to the cloud-delivered Firewall Management Center as described in the migration guide. When you select devices to migrate, make sure you choose **Delete FTD from On-Prem FMC**. Note that the device is not fully deleted unless you commit the changes or 14 days pass. **6.** Verify migration success. If the migration does not function to your expectations, you have 14 days to switch back or it is committed automatically. However, note that Version 7.4.0 is unsupported for general operations. To return the on-prem management center to a supported version you must remove the re-migrated devices, re image back to Version 7.0.x, restore from backup, and reregister the devices.

Feature	Min. Threat Defense	Details
		See: • Cisco Secure Firewall Threat Defense Release Notes • Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 • Migrate On-Prem Management Center Managed Secure Firewall Threat Defense to Cloud-delivered Firewall Management Center If you have questions or need assistance at any point in the migration process, contact Cisco TAC.
S2S VPN support in FTD to cloud migration. Migrate threat defense devices with VPN policies from on-prem to cloud-delivered Firewall Management Center.	7.0.3-7.0.x 7.2 or later	Site-to-site VPN configurations on Secure Firewall Threat Defense devices are now migrated along with the rest of the configuration when the device is migrated from the on-prem Firewall Management Center to the cloud-delivered Firewall Management Center. See: Migrate On-Prem Management Center managed Secure Firewall Threat Defense to Cloud-delivered Firewall Management Center
Interfaces		

Feature	Min. Threat Defense	Details
Merged management and diagnostic interfaces.	7.4.0	**Upgrade impact. Merge interfaces after upgrade.** For new devices using 7.4 and later, you cannot use the legacy diagnostic interface. Only the merged management interface is available. If you upgraded to 7.4 or later and: • You did not have any configuration for the diagnostic interface, then the interfaces will merge automatically. • You have configuration for the diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate diagnostic interface. Note that support for the diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including Management) in the configuration. For platform settings, this means: • You can no longer enable HTTP, ICMP, or SMTP for diagnostic. • For SNMP, you can allow hosts on management instead of diagnostic. • For Syslog servers, you can reach them on management instead of diagnostic. • If Platform Settings for syslog servers or SNMP hosts specify the diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices. • DNS lookups no longer fall back to the management-only routing table if you do not specify interfaces. New/modified screens: **Devices** > **Device Management** > **Interfaces** New/modified commands: **show management-interface convergence** See: Merge the Management and Diagnostic Interfaces
VXLAN VTEP IPv6 support.	7.4.0	You can now specify an IPv6 address for the VXLAN VTEP interface. IPv6 is not supported for the threat defense virtual cluster control link or for Geneve encapsulation. New/modified screens: • **Devices** > **Device Management** > **Edit Device** > **VTEP** > **Add VTEP** • **Devices** > **Device Management** > **Edit Devices** > **Interfaces** > **Add Interfaces** > **VNI Interface** See: Configure Geneve Interfaces

Feature	Min. Threat Defense	Details
Loopback interface support for BGP and management traffic.	7.4.0	You can now use loopback interfaces for AAA, BGP, DNS, HTTP, ICMP, IPsec flow offload, NetFlow, SNMP, SSH, and syslog. New/modified screens: **Devices** > **Device Management** > Edit device > **Interfaces** > **Add Interfaces** > **Loopback Interface** See: Configure Loopback Interfaces
Loopback and management type interface group objects.	7.4.0	You can create interface group objects with only management-only or loopback interfaces. You can use these groups for management features such as DNS servers, HTTP access, or SSH. Loopback groups are available for any feature that can utilize loopback interfaces. However, it's important to note that DNS does not support management interfaces. New/modified screens: **Objects** > **Object Management** > **Interface** > **Add** > **Interface Group** See: Interface
High Availability/Scalability		
Reduced "false failovers" for threat defense high availability.	7.4.0	Other version restrictions: Not supported with threat defense Version 7.3.x. See: Heartbeat Module Redundancy
SD-WAN		
Policy-based routing using HTTP path monitoring.	7.2.0	Policy-based routing (PBR) can now use the performance metrics (RTT, jitter, packet-lost, and MOS) collected by path monitoring through HTTP client on the application domain rather than the metrics on a specific destination IP. HTTP-based application monitoring option is enabled by default for the interface. You can configure a PBR policy with match ACL having the monitored applications and interface ordering for path determination. New/modified screens: **Devices** > **Device Management** > Edit device > Edit interface > **Path Monitoring** > **Enable HTTP based Application Monitoring** check box. Platform restrictions: Not supported for clustered devices. See: Configure Path Monitoring Settings
Policy-based routing with user identity and SGTs.	7.4.0	You can now classify the network traffic based on users and user groups, and SGTs in PBR policies. You can select the identity and SGT objects while defining the extended ACLs for the PBR policies. New/modified screens: **Objects** > **Object Management** > **Access List** > **Extended** > Add/Edit Extended Access List > Add/Edit Extended Access List Entry > **Users** and **Security Group Tag** See: Configure Extended ACL Objects
VPN		

Feature	Min. Threat Defense	Details
IPsec flow offload on the VTI loopback interface for the Secure Firewall 4200.	7.4.0	On the Secure Firewall 4200, qualifying IPsec connections through the VTI loopback interface are offloaded by default. Previously, this feature was supported for physical interfaces on the Secure Firewall 3100. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command. Other requirements: FPGA firmware 6.2+ See: IPSec Flow Offload
Crypto debugging enhancements for the Secure Firewall 4200.	7.4.0	We made the following enhancements to crypto debugging: • The crypto archive is now available in text and binary formats. • Additional SSL counters are available for debugging. • Remove stuck encrypt rules from the ASP table without rebooting the device. New/modified CLI commands: **show counters** See: Troubleshooting Using Crypto Archives
VPN: Remote Access		
Customize Secure Client messages, icons, images, and connect/disconnect scripts.	7.2.0	You can now customize Secure Client and deploy these customizations to the VPN headend. The following are the supported Secure Client customizations: • GUI text and messages • Icons and images • Scripts • Binaries • Customized Installer Transforms • Localized Installer Transforms Threat defense distributes these customizations to the endpoint when an end user connects from the Secure Client. New/modified screens: • **Objects** > **Object Management** > **VPN** > **Secure Client Customization** • **Devices** > **Remote Access** > Edit VPN policy > **Advanced** > **Secure Client Customization** See: Customize Secure Client
VPN: Site to Site		

Feature	Min. Threat Defense	Details
Easily exempt site-to-site VPN traffic from NAT translation.	Any	We now make it easier to exempt site-to-site VPN traffic from NAT translation. New/modified screens: • Enable NAT exemptions for an endpoint: **Devices** > **VPN** > **Site To Site** > **Add/Edit Site to Site VPN** > **Add/Edit Endpoint** > **Exempt VPN traffic from network address translation** • View NAT exempt rules for devices that do not have a NAT policy: **Devices** > **NAT** > **NAT Exemptions** • View NAT exempt rules for a single device: **Devices** > **NAT** > **Threat Defense NAT Policy** > **NAT Exemptions** See: NAT Exemption
Easily view IKE and IPsec session details for VPN nodes.	Any	You can view the IKE and IPsec session details of VPN nodes in a user-friendly format in the Site-to-Site VPN dashboard. New/modified screens: **Overview** > **Site to Site VPN** > Under the Tunnel Status widget, hover over a topology, click **View**, and then click the **CLI Details** tab. See: Monitoring the Site-to-Site VPNs
Access Control: Threat Detection and Application Identification		
Sensitive data detection and masking.	7.4.0 with Snort 3	**Upgrade impact. New rules in default policies take effect.** Sensitive data such as social security numbers, credit card numbers, emails, and so on may be leaked onto the internet, intentionally or accidentally. Sensitive data detection is used to detect and generate events on possible sensitive data leakage and generates events only if there is a transfer of significant amount of Personally Identifiable Information (PII) data. Sensitive data detection can mask PII in the output of events, using built-in patterns. Disabling data masking is not supported. See: Custom Rules in Snort 3

Feature	Min. Threat Defense	Details
Clientless zero-trust access.	7.4.0 with Snort 3	We introduced Zero Trust Access that allows you to authenticate and authorize access to protected web based resources, applications, or data from inside (on-premises) or outside (remote) the network using an external SAML Identity Provider (IdP) policy. The configuration consists of a Zero Trust Application Policy (ZTAP), Application Group, and Applications. New/modified screens: • **Policies** > **Zero Trust Application** • **Analysis** > **Connections** > **Events** • **Overview** > **Dashboard** > **Zero Trust** New/modified CLI commands: • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics** See: Zero Trust Access.
Routing		
Configure graceful restart for BGP on IPv6 networks.	7.3.0	You can now configure BGP graceful restart for IPv6 networks on managed devices version 7.3 and later. New/modified screens: **Devices** > **Device Management** > Edit device > **Routing** > **BGP** > **IPv6** > **Neighbor** > Add/Edit Neighbor. See: Configure BGP Neighbor Settings
Virtual routing with dynamic VTI.	7.4.0	You can now configure a virtual router with a dynamic VTI for a route-based site-to-site VPN. New/modified screens: **Devices** > **Device Management** > Edit Device > **Routing** > **Virtual Router Properties** > Dynamic VTI interfaces under **Available Interfaces** Platform restrictions: Supported only on native mode standalone or high availability devices. Not supported for container instances or clustered devices. See: About Virtual Routers and Dynamic VTI
Access Control: Threat Detection and Application Identification		

Feature	Min. Threat Defense	Details
Encrypted visibility engine enhancements.	7.4.0 with Snort 3	Encrypted Visibility Engine (EVE) can now: • Block malicious communications in encrypted traffic based on threat score. • Determine client applications based on EVE-detected processes. • Reassemble fragmented Client Hello packets for detection purposes. New/modified screens: Use the access control policy's advanced settings to enable EVE and configure these settings. See: Encrypted Visibility Engine
Exempt specific networks and ports from bypassing or throttling elephant flows.	7.4.0 with Snort 3	You can now exempt specific networks and ports from bypassing or throttling elephant flows. New/modified screens: • When you configure elephant flow detection in the access control policy's advanced settings, if you enable the **Elephant Flow Remediation** option, you can now click **Add Rule** and specify traffic that you want to exempt from bypass or throttling. • When the system detects an elephant flow that is exempted from bypass or throttling, it generates a mid-flow connection event with the reason **Elephant Flow Exempted**. Platform restrictions: Not supported on the Firepower 2100 series. See: Elephant Flow Detection
Improved JavaScript inspection.	7.4.0 with Snort 3	We improved JavaScript inspection, which is done by normalizing the JavaScript and matching rules against the normalized content. See: HTTP Inspect Inspector and Cisco Secure Firewall Management Center Snort 3 Configuration Guide
Access Control: Identity		
Cisco Secure Dynamic Attributes Connector on the management center.	Any	You can now configure the Cisco Secure Dynamic Attributes Connector on the management center. Previously, it was only available as a standalone application. See: Cisco Secure Dynamic Attributes Connector
Event Logging and Analysis		
Configure threat defense devices as NetFlow exporters from the management center web interface.	Any	NetFlow is a Cisco application that provides statistics on packets flows. You can now use the management center web interface to configure threat defense devices as NetFlow exporters. If you have an existing NetFlow FlexConfig and redo your configurations in the web interface, you cannot deploy until you remove the deprecated FlexConfigs. New/modified screens: **Devices** > **Platform Settings** > **Threat Defense Settings Policy** > **NetFlow** See: Configure NetFlow
Health Monitoring		

Feature	Min. Threat Defense	Details
New asp drop metrics.	7.4.0	You can add over 600 new asp (accelerated security path) drop metrics to a new or existing device health dashboard. Make sure you choose the **ASP Drops** metric group. New/modified screens: **System** (⚙) > **Health** > **Monitor** > **Device** See: show asp drop Command Usage
Administration		
Support for IPv6 URLs when checking certificate revocation.	7.4.0	Previously, threat defense supported only IPv4 OCSP URLs. Now, threat defense supports both IPv4 and IPv6 OCSP URLs. See: Certificate Enrollment Object Revocation Options
Store threat defense backup files in a secure remote location.	Any	When you back up a device, the cloud-delivered Firewall Management Center stores the backup files in its secure cloud storage. See: Backup/Restore
Usability, Performance, and Troubleshooting		
Usability enhancements.	Any	You can now: • Manage Smart Licensing for threat defense clusters from **System** (⚙) > **Smart Licenses**. Previously, you had to use the Device Management page. See: Licenses for Clustering • Download a report of Message Center notifications. In the Message Center, click the new **Download Report** icon, next to the **Show Notifications** slider. See: Managing System Messages. • Download a report of all registered devices. On **Devices** > **Device Management**, click the new **Download Device List Report** link, at the top right of the page. See: Download the Managed Device List. • Easily create custom health monitoring dashboards, and easily edit existing dashboards. See: Correlating Device Metrics
Specify the direction of traffic to be captured with packet capture for the Secure Firewall 4200.	7.4.0	On the Secure Firewall 4200, you can use a new **direction** keyword with the **capture** command. New/modified CLI commands: **capture***capture_name***switchinterface***interface_name* [**direction** { **both** | **egress** | **ingress** }] See: Cisco Secure Firewall Threat Defense Command Reference
Management Center REST API		

Feature	Min. Threat Defense	Details
Cloud-delivered Firewall Management Center REST API.	Feature dependent	For information on changes to the management center REST API, see What's New in the API quick start guide.

Table 5: Deprecated Features: Version 20230929

Feature	Deprecated in Threat Defense	Details
Deprecated: NetFlow with FlexConfig.	Any	You can now configure threat defense devices as NetFlow exporters from the management center web interface. If you do this, you cannot deploy until you remove any deprecated FlexConfigs. See: Configure NetFlow
Deprecated: `high unmanaged disk usage` alerts.	7.0.6 7.2.4 7.4.0	The Disk Usage health module no longer alerts with `high unmanaged disk usage`. You may continue to see these alerts until you either deploy health policies to managed devices (stops the display of alerts), or upgrade the devices to Version 7.0.6, 7.2.4, or 7.4 (stops the sending of alerts). For information on the remaining Disk Usage alerts, see Disk Usage and Drain of Events Health Monitor Alerts.

August 3, 2023

Table 6: New Features: August 3, 2023

Feature	Description
Updates to Firewall Migration Tool	Cisco Defense Orchestrator now hosts an updated version of the Firewall Migration Tool. You can now merge multiple contexts in your Secure Firewall ASA devices to a routed-mode instance and migrate them to threat defense devices managed by the cloud-delivered Firewall Management Center. In addition, the migration tool now leverages the virtual routing and forwarding (VRF) functionality to replicate the segregated traffic flow observed in a multi-context ASA environment, which will be part of the new merged configuration. See Migrating Secure Firewall ASA Managed by CDO in *Migrating Firewalls with the Firewall Migration Tool in Cisco Defense Orchestrator* guide for more information.

July 20, 2023

Table 7: New Features: July 20, 2023

Feature	Description
EasyDeploy for Virtual Threat Defense Devices Managed by GCP	You can now create a virtual threat defense device and deploy it to a Google Cloud Platform (GCP) project simultaneously. The EasyDeploy method combines the steps required to create a new virtual device and then associating the device with the cloud environment, streamlining the procedure and minimizing the amount of time required for setup. Note that you **must** have cloud-delivered Firewall Management Center enabled for these onboarding flows. See Deploy a Threat Defense Device to Google Cloud Platform for more information. Minimum threat defense: • 7.0.3 and later 7.0.x versions • 7.2 and later versions

June 8, 2023

Table 8: New Features: June 8, 2023

Feature	Description
EasyDeploy for Secure Firewall Threat Defense with AWS or Azure	You can now create and deploy a Secure Firewall Threat Defense device with either an AWS or Azure environment simultaneously. Onboard the device with CDO and manage the environment in cloud-delivered Firewall Management Center. See Deploy a Threat Defense Device with AWS and Deploy a Threat Defense Device with an Azure VNet respectively for more information. Minimum threat defense: • 7.0.3 and later 7.0.x versions • 7.2 and later versions

May 25, 2023

Table 9: New Features: May 25, 2023

Feature	Description
Threat defense Version 7.3.1 support.	You can now manage threat defense devices running Version 7.3.1.

Feature	Description
Firepower 1010E.	You can now manage the Firepower 1010E, which does not support power over Ethernet (PoE), with cloud-delivered Firewall Management Center. Minimum threat defense: 7.2.3

March 9, 2023

This release introduces stability, hardening, and performance enhancements.

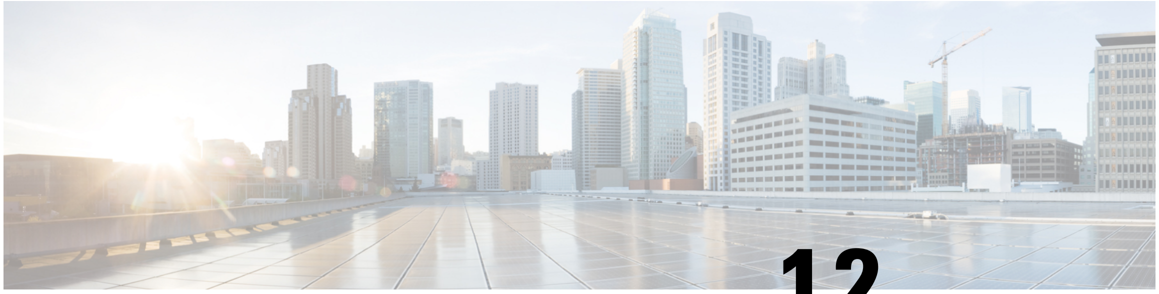
February 16, 2023

This release introduces stability, hardening, and performance enhancements.

January 18, 2023

Table 10: New Features: January 18, 2023

Feature	Description
Remote Access VPN	
Monitor remote access VPN sessions in CDO.	You can now use CDO to monitor RA VPN sessions on threat defense devices managed by the cloud-delivered Firewall Management Center. You can see a a list of active and historical sessions, as well as the details of the device and user associated with each session. Supported threat defense versions: • 7.0.3 and later 7.0.x versions • 7.2 and later versions For more information, see Monitor Remote Access VPN Sessions in the configuration guide.



CHAPTER 12

New Features in Cloud-delivered Firewall Management Center 2022

December 13, 2022

Table 11: New Features: December 13, 2022

Feature	Description
Onboarding to CDO and Threat Defense Upgrades	
Additional Device Support and Onboarding	You can now onboard clustered devices, AWS VPC environments, and Azure VNET environments to cloud-delivered Firewall Management Center. Onboarding these devices currently requires login credentials. Clustered devices must be already formed in their designated managing platform. See the following topics at https://docs.defenseorchestrator.com for more information: • Onboard a Cluster • Onboard a Device Associated with an AWS VPC. • Onboard an Azure VNet Environment

Feature	Description
Unattended Threat Defense Upgrade	The threat defense upgrade wizard now supports unattended upgrades, using a new Unattended Mode menu. You just need to select the target version and the devices you want to upgrade, specify a few upgrade options, and step away. You can even log out or close the browser. With an unattended upgrade, the system automatically copies needed upgrade packages to devices, performs compatibility and readiness checks, and begins the upgrade. Just as happens when you manually step through the wizard, any devices that do not "pass" a stage in the upgrade (for example, failing checks) are not included in the next stage. After the upgrade completes, you pick up with the verification and post-upgrade tasks. You can pause and restart unattended mode during the copy and checks phases. However, pausing unattended mode does not stop tasks in progress. Copies and checks that have started will run to completion. Similarly, you cannot cancel an upgrade in progress by stopping unattended mode; to cancel an upgrade, use the Upgrade Status pop-up, accessible from the Upgrade tab on Device Management page, and from the Message Center. See *Upgrade Threat Defense* in the Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center.
Auto-upgrade to Snort 3	When you upgrade threat defense to Version 7.3+, you can no longer disable the Upgrade Snort 2 to Snort 3 option. After the software upgrade, all eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. Although you can switch individual devices back, Snort 2 will be deprecated in a future release and we strongly recommend you stop using it now. For devices that are ineligible for auto-upgrade because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For migration assistance, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide.
CDO-managed Secure Firewall Threat Defense Devices on Firepower 4100/9300	The Firepower 4100/9300 is a flexible security platform on which you can install one or more logical devices. Before you can add the threat defense to the management center, you must configure chassis interfaces, add a logical device, and assign interfaces to the device on the Firepower 4100/9300 chassis using the Secure Firewall chassis manager or the FXOS CLI. You can now create a CDO-managed, standalone logical threat defense device on the Firepower 4100/9300, by configuring CDO as the manager when creating the device. See *Configure Logical Devices* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator
Interfaces	

Feature	Description
IPv6 DHCP Enhancements	The Dynamic Host Configuration Protocol (DHCP) provides network configuration parameters, such as IP addresses, to DHCP clients. The threat defense device can provide a DHCP server to DHCP clients attached to threat defense device interfaces. The DHCP server provides network configuration parameters directly to DHCP clients. The cloud-delivered Firewall Management Center now supports the following IPv6 addressing features for Secure Firewall Threat Defense devices: • DHCPv6 Address Client: Threat defense obtains an IPv6 global address and optional default route from the DHCPv6 server. • DHCPv6 Prefix Delegation Client: Threat defense obtains delegated prefix(es) from a DHCPv6 server. It can then use these prefixes to configure other threat defense interface addresses so that StateLess Address Auto Configuration (SLAAC) clients can auto-configure IPv6 addresses on the same network. • BGP router advertisement for delegated prefixes. • DHCPv6 Stateless Server: Threat defense provides other information such as the domain name to SLAAC clients when they send Information Request (IR) packets to threat defense. Threat defense only accepts IR packets and does not assign addresses to the clients. See *Configure IPv6 Addressing* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator for more information.
Support for Loopback Interface	A loopback interface is a software interface that emulates a physical interface. It is reachable through multiple physical interfaces with IPv4 and IPv6 addresses. You can configure a loopback interface for the redundancy of static and dynamic VTI VPN tunnels. See *Regular Firewall Interfaces* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.
Paired Proxy VXLAN for the Threat Defense Virtual for the Azure Gateway Load Balancer	You can configure a paired proxy mode VXLAN interface for the threat defense virtual in Azure for use with the Azure Gateway Load Balancer (GWLB). The threat defense virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy. See *Clustering for Threat Defense Virtual in a Public Cloud* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator to learn more.

Feature	Description
Redundant Manager Access Data Interface	You can now configure a secondary data interface to take over the management functions if the primary interface goes down, when using a data interface for manager access. The device uses SLA monitoring to track the viability of the static routes and an equal-cost multi-path (ECMP) zone that contains both interfaces so management traffic can use both interfaces. See *Configure a Redundant Manager Access Data Interface* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator for more information.
Remote Access VPN	
TLS 1.3 in Remote Access VPN	You can now use TLS 1.3 to encrypt remote access VPN connections. Use threat defense platform settings to specify that the device must use TLS 1.3 protocol when acting as a remote access VPN server. See *Platform Settings* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.
Site to Site VPN	
Support for Dynamic Virtual Tunnel Interface	You can create a dynamic VTI and use it to configure a route-based site-to-site VPN in a hub and spoke topology. Previously, you could use only a static VTI to configure a route-based site-to-site VPN in a hub and spoke topology. Dynamic VTI eases the configuration of peers for large enterprise hub and spoke deployments. A single dynamic VTI can replace several static VTI configurations on the hub. You can add new spokes to a hub without changing the hub configuration. See *Site-to-Site VPNs for Secure Firewall Threat Defense* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator
Routing	
Support for Bidirectional Forwarding Detection	Cloud-delivered Firewall Management Center now supports Bidirectional Forwarding Detection (BFD) configuration on Secure Firewall Threat Defense devices. BFD operates in a unicast, point-to-point mode on top of any data protocol being forwarded between two systems. However, in threat defense, BFD is supported on BGP protocols only. BFD configuration on the device includes creating templates and policies and enabling BFD support in the BGP neighbor settings. See *Bidirectional Forwarding Detection Routing* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator for more information.

Feature	Description
EIGRP (IPv4) routing support on Virtual Tunnel Interface	EIGRP (IPv4) routing is now supported on the Virtual Tunnel Interface. You can now use EIGRP (IPv4) protocol to share routing information and to route traffic flow over a VTI-based VPN tunnel between peers. See *Additional Configurations for VTI* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.
Virtual Tunnel Interface (VTI) Support for OSPF	The IPv4 or IPv6 OSPF can be configured on the VTI interface of a threat defense device. You can use OSPF to share routing information and route traffic through a VTI-based VPN tunnel between the devices. See *Site-to-Site VPNs for Secure Firewall Threat Defense* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.
Access Control and Threat Detection	
Decryption Policy	Feature renamed from *SSL policy* to *decryption policy* to better reflect what it does. We now enable you to configure a decryption policy with one or more **Decrypt - Resign** or **Decrypt - Known Key** rules at the same time. Get started by going to **Policies** > **Access Control** > **Decryption**. The Create Decryption Policy dialog box now has two tab pages: **Outbound Connections** and **Inbound Connections**. Use the **Outbound Connections** tab page to configure one or more decryption rules with a **Decrypt - Resign** rule action. (You can either upload or generate certificate authorities at the same time). Each combination of a CA with networks and ports results in one decryption rule. Use the Inbound Connections tab page to configure one or more decryption rules with a Decrypt - Known Key rule action. (You can upload your server's certificate at the same time.) Each combination of a server certificate with networks and ports results in one decryption rule.
Health Monitoring	
Cloud-delivered Firewall Management Center Deployment Notifications on CDO	CDO now notifies you about the status of deployments that are performed on the cloud-delivered Firewall Management Center. The notification messages include information on whether the deployment has succeeded, failed, or is in progress, the time and date of the deployment, and a link to the deployment history page of the cloud-delivered Firewall Management Center. See *Notifications* in Managing FDM Devices with Cisco Defense Orchestrator for more information.

Feature	Description
Cluster Health Monitor Settings	You can now edit cluster health monitor settings in the cloud-delivered Firewall Management Center web interface. If you configure these settings with the FlexConfig in a previous version, the system allows you to deploy, but also warns you to redo the configuration because the FlexConfig settings take precedence. See *Edit Cluster Health Monitor Settings* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator to learn more.
Improved Health Monitoring for Device Clusters	You can now use the health monitor for each cluster to view overall cluster status, load distribution metrics, performance metrics, cluster control link (CCL) and data throughput, and so on. See *Cluster Health Monitor* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator to learn more.
New Health Monitoring Alerts	The cloud-delivered Firewall Management Center now provides new health modules to monitor the temperature and power supply on a Firepower 4100/9300 chassis. Using the new Environment Status and Power Supply health modules, you can create a custom health dashboard and set threshold values for temperature and power supply on your physical appliance. See *Health Monitor Alerts* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator to learn more.
Licensing	
Carrier License	Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. The cloud-delivered Firewall Management Center now supports Carrier license, in addition to the existing smart licenses. The Carrier license allows GTP/GPRS, Diameter, SCTP, and M3UA inspection configurations. See *Licenses* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.
Usability, Performance, and Troubleshooting	

Feature	Description
Core Allocation Performance Profiles	The CPU cores on the Secure Firewall Threat Defense device are assigned to two of the main system processes: Lina and Snort. Lina handles VPN connections, routing, and other basic layer 3/4 processing. Snort provides advanced inspection, including intrusion and malware prevention, URL filtering, application filtering, and other features that require deep packet inspection. You can now adjust the percentage of system cores assigned to the data plane and Snort to adjust system performance, using the performance profiles. Based on your relative use of VPN and intrusion policies, you can choose a desired performance profile. See *Configure the Performance Profile* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator for more information.
Identity	
Proxy Sequence	A *proxy sequence* is one or more managed devices that can be used to communicate with an LDAP, Active Directory, or ISE/ISE-PIC server. It is necessary only if Cisco Defense Orchestrator (CDO) cannot communicate with your Active Directory or ISE/ISE-PIC server. (For example, CDO might be in a public cloud but Active Directory or ISE/ISE-PIC might be in a private cloud.) Although you can use one managed device as a proxy sequence, we strongly recommend you set up two or more so that, in the event one managed device cannot communicate with Active Directory or ISE/ISE-PIC, another managed device can take over. Create a proxy sequence by going to **Integration** > **Other Integrations** > **Realms** > **Proxy Sequence**.

October 20, 2022

Support for Configuring Next-Hop IP Addresses in a Policy-based Route Map

Policy-Based Routing (PBR) helps route network traffic for specified applications based on your priorities, such as source port, destination address, destination port, protocol, applications, or a combination of these objects, rather than by destination network criteria. For example, you can use PBR to route your high-priority network traffic over a high-bandwidth, expensive link and your lower priority network traffic over a lower bandwidth, lower cost link.

The cloud-delivered Firewall Management Center now supports defining next-hop IP addresses when creating a policy-based route map. See *About Policy Based Routing* and *Configure Policy-Based Routing Policy* in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator for more information.

URL Filtering Enhancements

URL filtering lets you control access to websites that the users on your network can use. You can filter websites based on category and reputation, for which your device needs a URL-filtering license, or manually by specifying URLs. The category and reputation-based filtering—the quicker and smarter way to filter URLs—uses Cisco's up-to-date threat intelligence information and is highly recommended.

The cloud-delivered Firewall Management Center can now query for up-to-date URL category and reputation information directly from the Cisco Talos cloud instead of using the local database information. The local database gets updated every 24 to 48 hours. See *URL Filtering Options* in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator for detailed information.

Umbrella Tunnel Integration with Secure Firewall Threat Defense using Cloud-delivered Firewall Management Center

You can now automatically deploy IPsec IKEv2 tunnels to Umbrella from a threat defense device using cloud-delivered Firewall Management Center. This tunnel forwards all internet-bound traffic to the Umbrella Secure Internet Gateway (SIG) for inspection and filtering. Create a SASE topology, a new type of static VTI-based site-to-site VPN topology, using a simple wizard to configure and deploy the Umbrella tunnels.

See *About Umbrella SASE Topology* in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator for more information.

Support for Remote Access VPN Policy in FTD to Cloud Migration

CDO now imports the remote access VPN policy during the migration of the FTD to cloud.

See *Migrate FTD to Cloud* in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator for more information.

Migrate Flex Configured Routing Policies

Cloud-delivered Firewall Management Center now supports the migration of Flex configured ECMP, VxLAN, and EIGRP policies using the Migration Config option in the user interface.

See *Migrating FlexConfig Policies* in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator for more information.

Smart Licensing Standardization

The license names used by cloud-delivered Firewall Management Center have been changed.

Table 12: Smart License Name Changes

Old Name	is now	New Name
Base	is now	Essentials
Threat	is now	IPS
Malware	is now	Malware Defense
RA VPN/AnyConnect License	is now	Cisco Secure Client
AnyConnect Plus	is now	Secure Client Advantage

Old Name	is now	New Name
AnyConnect Apex	is now	Secure Client Premier
AnyConnect Apex and Plus	is now	Secure Client Premier and Advantage
AnyConnect VPN Only	is now	Secure Client VPN Only

See *License Types and Restrictions* in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator for more information.

June 9, 2022

Cisco Defense Orchestrator (CDO) is now the platform for the cloud-delivered Firewall Management Center.

The cloud-delivered Firewall Management Center is a software-as-a-service (SaaS) product that manages Secure Firewall Threat Defense devices. It offers many of the same functions as an on-premises Secure Firewall Management Center, it has the same appearance and behavior as an on-premises Secure Firewall Management Center, and uses the same FMC API.

This product is designed for Secure Firewall Management Center customers who want to move from an on-premises version of the Secure Firewall Management Center to a SaaS version.

As a SaaS product, the CDO operations team is responsible for maintaining it. As new features are introduced, the CDO operations team updates CDO and the cloud-delivered Firewall Manager for you.

A migration wizard is available to help you migrate your Secure Firewall Threat Defense devices registered to your on-premises Secure Firewall Management Center to the cloud-delivered Firewall Management Center.

Onboarding Secure Firewall Threat Defense devices is carried out in CDO using familiar processes such as onboarding a device with its serial number or using a CLI command that includes a registration key. Once the device is onboarded, it is visible in both CDO and in the cloud-delivered Firewall Management Center, however, you configure the device in the cloud-delivered Firewall Management Center. Secure Firewall Threat Defense devices running Version 7.2 or later can be onboarded.

The license for cloud-delivered Firewall Management Center is a per-device-managed license and there is no license required for the cloud delivered FMC itself. Existing Secure Firewall Threat Defense devices re-use their existing smart licenses and new Secure Firewall Threat Defense devices provision new smart licenses for each feature implemented on the FTD.

In a remote branch office deployment, the data interface of the threat defense device is used for Cisco Defense Orchestrator management instead of the Management interface on the device. Because most remote branch offices only have a single internet connection, outside CDO access makes centralized management possible. In the case of remote branch deployment, CDO provides high availability support for the threat defense devices that it manages through the data interface.

You can analyze syslog events generated by your onboarded threat defense devices using Security Analytics and Logging (SaaS) or Security Analytics and Logging (On Premises). The SaaS version stores events in the cloud and you view the events in CDO. The on-premises version stores events in an on-premises Secure Network Analytics appliance and analysis is done in the on-premises Secure Firewall Management Center. In both cases, just as with an on-premises FMC today, you can still send logs to a log collector of your choice directly from the sensors.

The FTD dashboard provides you an at-a-glance view of the status, including events data collected and generated by all threat defense devices managed by the cloud-delivered Firewall Management Center. You can use this dashboard to view collective information that is related to the device status and the overall health of the devices in your deployment. The information that the FTD dashboard provides depends on how you license, configure, and deploy the devices in your system. The FTD dashboard displays data for all CDO-managed threat defense devices. However, you can choose to filter device-based data. You can also choose the time range to display for specific time range.

The Cisco Secure Dynamic Attributes Connector enables you to use service tags and categories from various cloud service platforms in cloud-delivered Firewall Management Center access control rules. Network constructs such as IP addresses may be ephemeral in virtual, cloud and container environments due to the dynamic nature of the workloads and the inevitability of IP address overlap. Customers require policy rules to be defined based on non-network constructs such as VM name or security group, so that firewall policy is persistent even when the IP address or VLAN changes.

Proxy sequences of one or more managed devices can be used to communicate with an LDAP, Active Directory, or ISE/ISE-PIC servers. It is necessary only if Cisco Defense Orchestrator(CDO) cannot communicate with your Active Directory or ISE/ISE-PIC server. For example, CDO might be in a public cloud but Active Directory or ISE/ISE-PIC might be in a private cloud.

Although you can use one managed device as a proxy sequence, we strongly recommend you set up two or more so that, in the event one managed device cannot communicate with Active Directory or ISE/ISE-PIC, another managed device can take over.

Any customer can use CDO to manage other device types like, the Secure Firewall ASA, Meraki, Cisco IOS devices, Umbrella, and AWS virtual private clouds. If you use CDO to manage a Secure Firewall Threat Defense device configured for local management with Firepower Device Manager, you can continue to manage them with CDO as well. If you are new to CDO, you can manage Secure Firewall Threat Defense devices with the new cloud-delivered Firewall Management Center and all of the other device types as well.

Learn more about the Firewall Management Center features we support in the cloud-delivered Firewall Management Center.

- Health Monitoring
- Secure Firewall Threat Defense Device Backup/Restore
- Scheduling
- Import/Export
- External Alerting with Alert Responses
- Transparent or Routed Firewall mode
- High Availability for Secure Firewall Threat Defense Devices
- Interfaces
- Network Access Control (NAT)
- Static and Default Routes and other routing configurations
- Object Management and Certificates
- Remote Access VPN and Site to Site VPN configuration
- Access Control policies
- Cisco Secure Dynamic Attributes Connector
- Intrusion and Detection and Prevention policies

- Network Malware and Protection and File Policies
- Encrypted Traffic Handling
- User Identity
- FlexConfig Policies