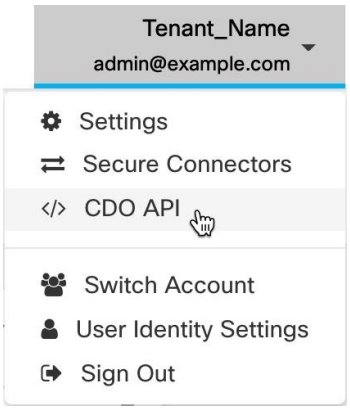
Feature Highlights of 2020

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

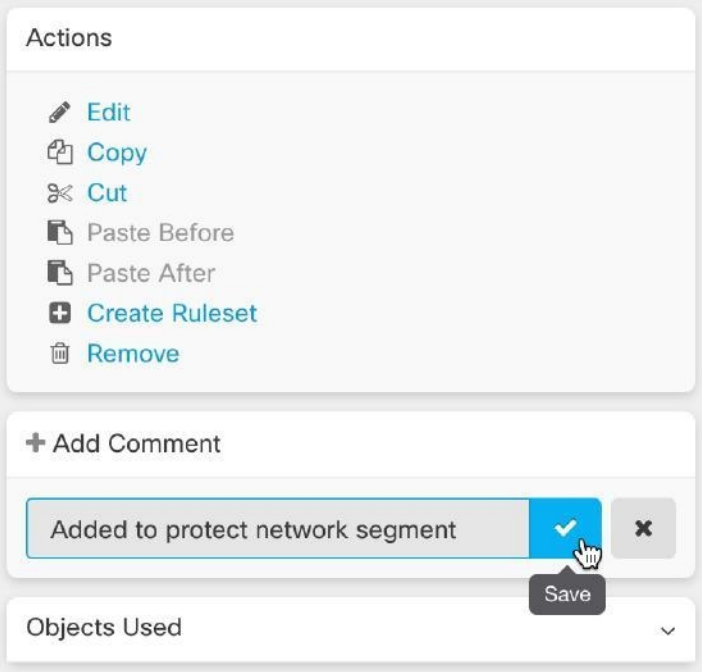
Export FTD Configuration

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.

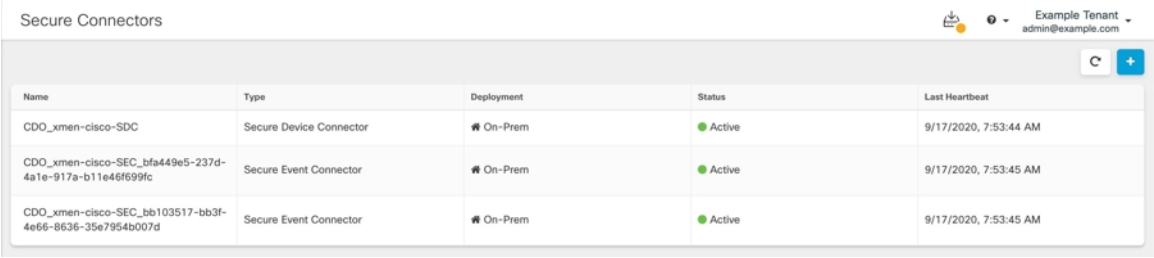
For more information, see the following topics in *Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator*:

- 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.



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*.

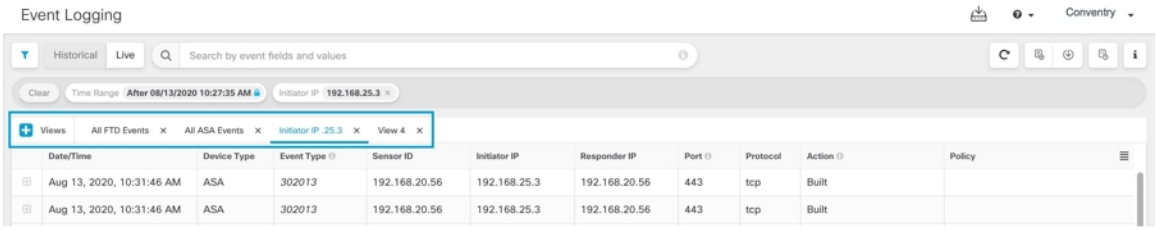
For information on onboarding an FMC, see "Onboard an FMC" in *Managing FMC with Cisco Defense Orchestrator*.

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*.



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*.

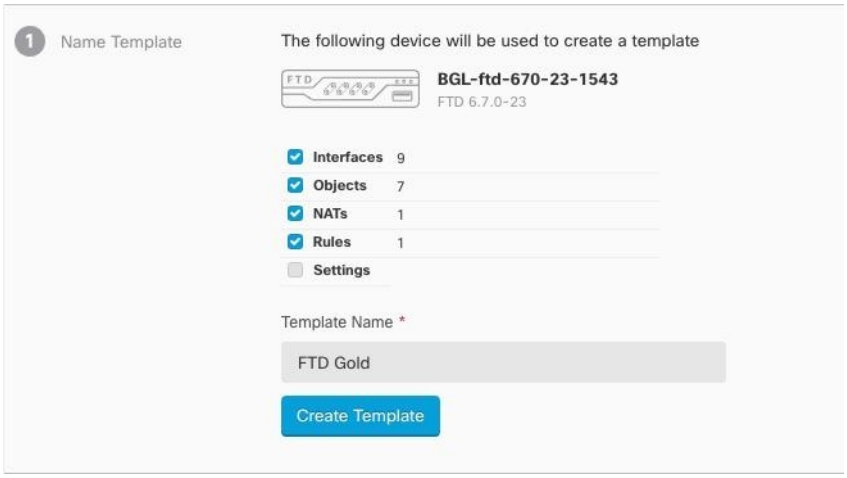
August 13, 2020

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*.



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.

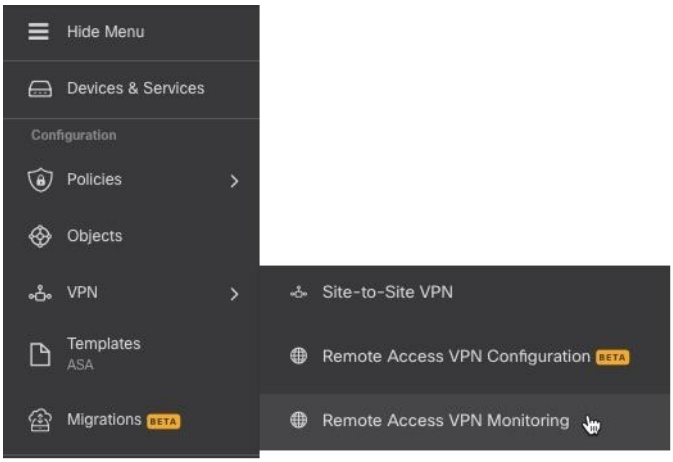
You can view the performance of each RA VPN head-end in your tenant, filter sessions by head-ends, and select the session properties that you want to view in the VPN monitoring table. Also, you can export the RA VPN sessions of one or more devices to a comma-separated value (.csv) file. For more information, 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.

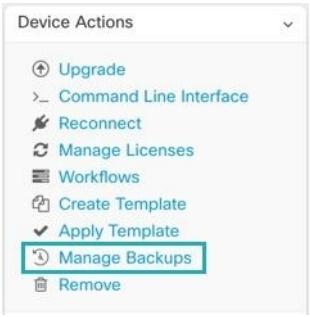
May 7, 2020

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

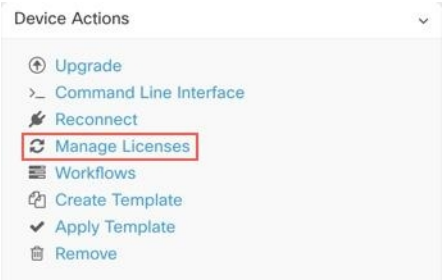
You can now issue CLI requests to your FTD devices directly from CDO.

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.

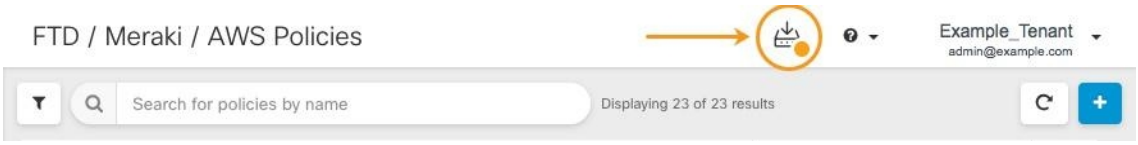
For more information, "Configure Site-to-Site VPN Connections with Dynamically-Addressed Peers" in *Managing FTD with Cisco Defense Orchestrator*.

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.



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.