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:

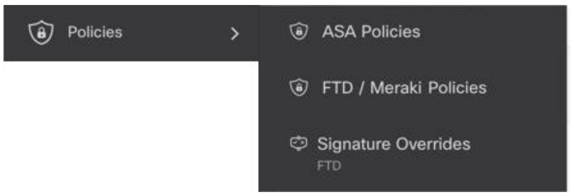
- Simultaneously manage policies on one or more Meraki devices.
- Monitor and manage Meraki policies or templates alongside your FTD and ASA devices in an all-encompassing environment.
- Use a Meraki template to manage multiple networks.
- Customize access rules with objects that are compatible across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

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

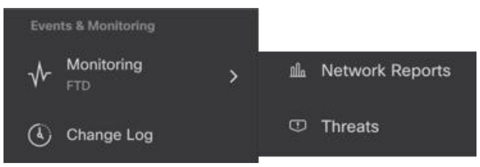
Updated GUI Navigation

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.