Managing FDM-Managed Devices with Cisco Defense Orchestrator

Managing FDM-Managed Devices with Cisco Defense Orchestrator

Important Secure Firewall device manager (FDM) support and functionality is only available upon request. If you do not already have Firewall device manager support enabled on your tenant you cannot manage or deploy to FDM-managed devices. Send a request to the support team to enable this platform.

Cisco Defense Orchestrator provides a simplified management interface and cloud-access to your Secure Firewall device manager devices. FDM-managed administrators will notice many similarities between the device interface and the CDO interface. We built CDO with the idea of keeping things as consistent as possible between managers.

Use CDO to manage these aspects of your physical or virtual FDM-managed device:

- Onboarding FDM-Managed Device
- Device Management
- Device Upgrade
- ASA to Threat Defense Migration
- Interface Management
- Routing
- High Availability
- Security Policies
- Promote Policy and Configuration Consistency
- Site-to-Site VPN

- Remote Access VPN
- Monitoring Your Network
- Cisco Security Analytics and Logging

Software and Hardware Support

CDO supports version 6.4 and later, which can be installed on a number of different devices or virtual machines. See FDM-Managed Support Specifics for more information.

Managing Smart Licenses

You can use Cisco Smart Licenses to license the FDM-managed devices during onboarding or after onboarding the devices to CDO. Smart Licensing is conveniently built into our workflows and easily accessible from the CDO interface. For more information, see Applying or Updating a Smart License.

Note If the device you want to onboard is running software version 6.4 or 6.5, and is already smart-licensed, the device is likely to be registered with Cisco Smart Software Manager. **You must unregister the device from Cisco Smart Software Manager before you onboard it to CDO with a registration Key.** When you unregister, the license and all optional licenses associated with the device, are freed in your virtual account.

If the device you want to onboard is running software version 6.6 and later and is already registered with the Cisco cloud, **you must unregister the device from Cisco Cloud Services before you onboard it to CDO with a registration key.**

CDO User Interfaces

CDO GUI and CLI Interfaces

CDO is a web-based management product that provides you with both a graphic user interface (GUI) and a command line interface (CLI) to manage your devices one at a time or many at once.

With the CLI interface, you can send commands to your FDM-managed devices directly from CDO. Use CLI macros to save and run commonly used commands. See Command Line Interface Documentation and CDO Command Line Interface for more information.

API Support

CDO provides the API tool interface that can perform advanced actions on an FDM-managed device using the device's REST API. 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 API tool, see Using the API Tool.

Onboarding FDM-Managed Devices

Before you onboard an FDM-managed device, review the general device requirements and onboarding prerequisites.

The best practice is to onboard FDM-managed devices with a registration token. See Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key for more information.

You can use these additional methods to onboard an FDM-managed device to CDO as well:

- Onboard an FDM-Managed Device Using Username, Password, and IP Address
- Onboard a Configured FDM-Managed Device using the Device's Serial Number
- Workflow and Prerequisites to Onboard the FDM-Managed Device Using Low-Touch Provisioning

Device Management

Use CDO to upgrade software, configure high availability, configure device settings and network resources for your FDM-managed devices.

- **System Settings**. Once you have licensed your FDM-managed device and onboarded it, you can manage your FDM-managed device settings entirely from CDO. You will be able to configure management access protocols, logging settings, DHCP and DNS server interaction, the device's hostname, the time server it uses, and URL filtering preferences.
- **Security Database Updates**. Keep your device up to date and compliant with current security database updates with a recurring task to check and update your device when necessary.
- **High Availability**. Manage HA configuration and operations with the FDM-Managed High Availability Page.

Device Upgrade

Perform immediate upgrades to your FDM-managed devices, or schedule them, using one of following methods:

- Upgrade a single FDM-managed device.
- Upgrade multiple FDM-managed devices.
- Upgrade an FDM-managed HA pair.

ASA to Threat Defense Migration

CDO helps you migrate your Adaptive Security Appliance (ASA) to an FDM-managed device. CDO provides a wizard to help you migrate these elements of the ASA's running configuration to an Firewall device manager template:

This migration is supported for the following elements:

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

- Routes
- Service objects and service group objects
- Site-to-site VPN

See Migrating an ASA Configuration to an FDM Template for more information.

Interface Management

You can use CDO to configure and edit data interfaces or the management/diagnostic interface on an FDM-managed device.

Routing

Routing is the act of moving information across a network from a source to a destination. Routing involves two basic activities: determining optimal routing paths and transporting packets through a network. Use CDO to configure these aspects of routing:

- **Configuring Static Routes and Default Routes**. Using CDO, you can define a default route, and other static routes, for your FDM-managed devices.
- **Bridge Group Support**. A bridge group is a virtual interface that groups one or more interfaces. The main reason to group interfaces is to create a group of switched interfaces. Using CDO you can configure and edit bridge groups on your device.
- **NAT (Network Address Translation)**. NAT rules help route your traffic from your inside (private) network to the Internet. NAT rules also play a security role by keeping internal IP addresses hidden from the world outside your network. You can create and edit NAT rules for your device using CDO. See Network Address Translation for more information.

Security Policies

Security policies examine network traffic with the ultimate goal of either allowing network traffic to reach or prevent network traffic from reaching its intended destination. Use CDO to manage all the components of the device's security policies:

- **Copy and paste rules**. Make sharing rules across policies easy by copying and pasting rules from policy to another. See Copy FDM Access Control Rules for more information.
- **SSL Decryption Policy**. Some protocols, such as HTTPS, use Secure Sockets Layer (SSL) or its follow-on version, Transport Layer Security (TLS), to encrypt traffic for secure transmissions. Because the system cannot inspect encrypted connections, you must apply SSL decryption policy to decrypt them if you want to apply access rules that consider higher-layer traffic characteristics to make access decisions. See FDM-Managed Device SSL Decryption Policy for more information.
- **Identity Policy**. Use identity policies to collect user identity information from connections. You can then view usage based on user identity in the dashboards, and configure access control based on user or user group.
- **Security Intelligence Policy**. The Security Intelligence policy gives you an early opportunity to drop unwanted traffic based on source/destination IP address or destination URL. The system drops the traffic on the blocked list before evaluating it with the access control policy, thus reducing the amount of system resources used.

- **Access Control Policy**. The access control policy controls access to network resources by evaluating network traffic against access control rules. Secure Firewall Device Manager compares the criteria of the access control rules, in the order they appear in the access control policy, to the network traffic. When all the traffic conditions in an access control rule are matched, Secure Firewall Device Manager takes the action defined by the rule. You can configure all aspects of access control policy using CDO.
- TLS 1.3 Security Identity Discovery. Introduced in version 6.7, this feature allows you to perform URL filtering and application control on traffic encrypted with TLS 1.3. See TLS Server Identity Discovery in Firepower Threat Defense for more information.
- **Intrusion Policy**. Cisco delivers several intrusion policies with the Firepower system. These policies are designed by the Cisco Talos Security Intelligence and Research Group, who set the intrusion and preprocessor rule states and advanced settings. Intrusion policies are aspects of access control rules. See Intrusion Policy Settings in an FDM Access Control Rule for more information.

Note Snort 3 is available for FDM-managed devices running version 6.7 and later. Please note that you can toggle between Snort 2 and Snort 3 at will, but risk incompatible configurations. For more information about Snort 3, supported devices and software, and any limitations see Upgrade to Snort 3.0.

- **Threat Events**. A threat event is a report of traffic that has been dropped, or that has generated an alert, after matching one of Cisco Talos's intrusion policies. In most cases, there's no need to tune IPS rules. If necessary, you have the option to override how an event is handled by changing the matching rule action in CDO. CDO supports IPS rule tuning on all versions of versions 6.4 and 6.6.1. CDO does not support IPS rule tuning on any version 6.5, any 6.6 version other than 6.6.1, or any 6.7 version.
- **NAT (Network Address Translation)**. NAT rules help route your traffic from your inside (private) network to the Internet. NAT rules also play a security role by keeping internal IP addresses hidden from the world outside your network. You can create and edit NAT rules for your Firepower Threat Defense using CDO.

Promote Policy and Configuration Consistency

Object Management

An object is a container of information that you can use in one or more security policies. Objects make it easy to maintain policy consistency because you can modify an object and that change affects all the other policies that use that object. Without objects, you would need to modify all the policies, individually, that require the same change.

Use CDO to create and manage these object types:

- Active Directory Realm
- AnyConnect Client Profile
- Application Filter
- Certificate
- DNS Group

- Geolocation
- Identity Source
- IKEv1 Policy
- IKEv1 IPsec Proposal
- IKEv2 Policy
- IKEv2 IPsec Proposal
- Network
- RA VPN Group Policy
- Security zone
- Service
- Security Group Tags
- Syslog Server
- URL

Resolve Object Issues

CDO calls an object used on multiple devices a "shared object" and identifies them in the Objects page with this badge ⧉. Sometimes a shared object develops some "issue" and is no longer perfectly shared across multiple policies or devices. CDO makes it easy to Resolve Duplicate Object Issues, Resolve Unused Object Issues, and Resolve Inconsistent Object Issues to manage your devices as well as your repository of objects.

Templates

A Secure Firewall Device Manager template is a complete copy of an onboarded FDM-managed device's configuration. You can then modify that template and use it to configure other FDM-managed devices you manage. Secure Firewall Device Manager templates promote policy consistency between devices. See FDM Templates for more information.

High Availability

CDO makes it easy to configure and manage a high availability pair of FDM-managed devices. You can 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.

You can upgrade FDM-managed HA pairs in CDO. See Upgrade an FDM-Managed High Availability Pair for more information.

Configuring Virtual Private Networks

Site-to-Site VPN

A virtual private network (VPN) consists of multiple remote peers transmitting private data securely to one another over an unsecured network, thusly connecting network to network. CDO uses tunnels to encapsulate data packets within normal IP packets for forwarding over IP-based networks, using encryption to ensure privacy and authentication to ensure data integrity. See Site-to-Site VPN for more information.

For additional information about Virtual Private Networks, refer to the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

Remote Access VPN

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 FDM-managed devices. AnyConnect is the only client that is supported on endpoint devices for RA VPN connectivity to FDM-managed devices.

CDO supports the following aspects of RA VPN functionality on FDM-managed 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 FDM-managed devices

See RA VPN for more information. For additional information about Virtual Private Networks, refer to the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

Monitoring Your Network

CDO provides reports summarizing the impact of your security policies and methods of viewing notable events triggered by those security policies. CDO also logs the changes you make to your devices and provides you with a way to label those changes so you can associate the work you do in CDO with a help ticket or other operational request.

Executive Summary Report

Executive summary reports display a collection of operational statistics such as encrypted traffic, intercepted threats, detected web categories, and more. Data in the reports is generated when network traffic triggers an access rule or policy on an FDM-managed device. We recommend enabling malware and licenses, as well as enabling file logging for access rules, to allow a device to generate the events that are reflected in the reports.

Read FDM-Managed Device Executive Summary Report for more information about what the report offers and how you can use it to improve your network infrastructure. To create and manage your reports, see Managing Reports.

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging allows you to capture connection, intrusion, file, malware, and Security Intelligence events from all of your FDM-managed 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 FDM-managed device 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 FDM-managed device 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. See Cisco Security Analytics and Logging for more information.

Change Log

The Manage Change Logs in CDO continuously captures configuration changes as they are made in CDO. This single view includes changes across all supported devices and services. These are some of the features of the change log:

- Side-by-side comparison of changes made to device configuration
- Plain-English labels for all change log entries.
- Records on-boarding and removal of devices.
- Detection of policy change conflicts occurring outside of CDO.
- Answers who, what, and when during an incident investigation or troubleshooting.
- The full change log, or only a portion, can be downloaded as a CSV file.

Change Request Management

Change request management allows you to associate a change request and its business justification, opened in a third-party ticketing system, with an event in the Change Log. Use change request management 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.