Cisco Defense Orchestrator

Contents

Managing network security across today's complex, extended architectures is hard work. In the face of sophisticated adversaries, security controls are needed everywhere: in your data center and private and public clouds, at remote sites, and for your mobile workers.

The increased workload and sheer complexity of overseeing security across heterogenous environments will continue to place greater demands on network operations teams. Organizations need a simplified approach to managing security policies across Cisco® Next-Generation Firewalls (NGFW) and other core security platforms to improve efficiencies and drive consistency while reducing the risk of vulnerabilities.

Figure 1.
Cisco Defense Orchestrator design principles: Simple – efficient – effective management

Cloud-based firewall management

Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms.

Setup is easy, fast, and frictionless, allowing customers to onboard and start managing hundreds of devices within hours. The intuitive user interface and focus on simplicity means that training requirements are minimal, with a learning curve measured in hours rather than days.

Flexibility and scale are attributes of our open API as well as being a cloud technology. Because it's a cloud solution, Cisco Defense Orchestrator does not require further capital expenditures, floor space, or application management, dramatically reducing your operational costs.

It doesn't matter whether your organization has 5 or 5000 devices. Cisco Defense Orchestrator will provide your network operations team with the ability to reduce time spent managing and maintaining security devices, enabling them to focus on what is most important to your core business.

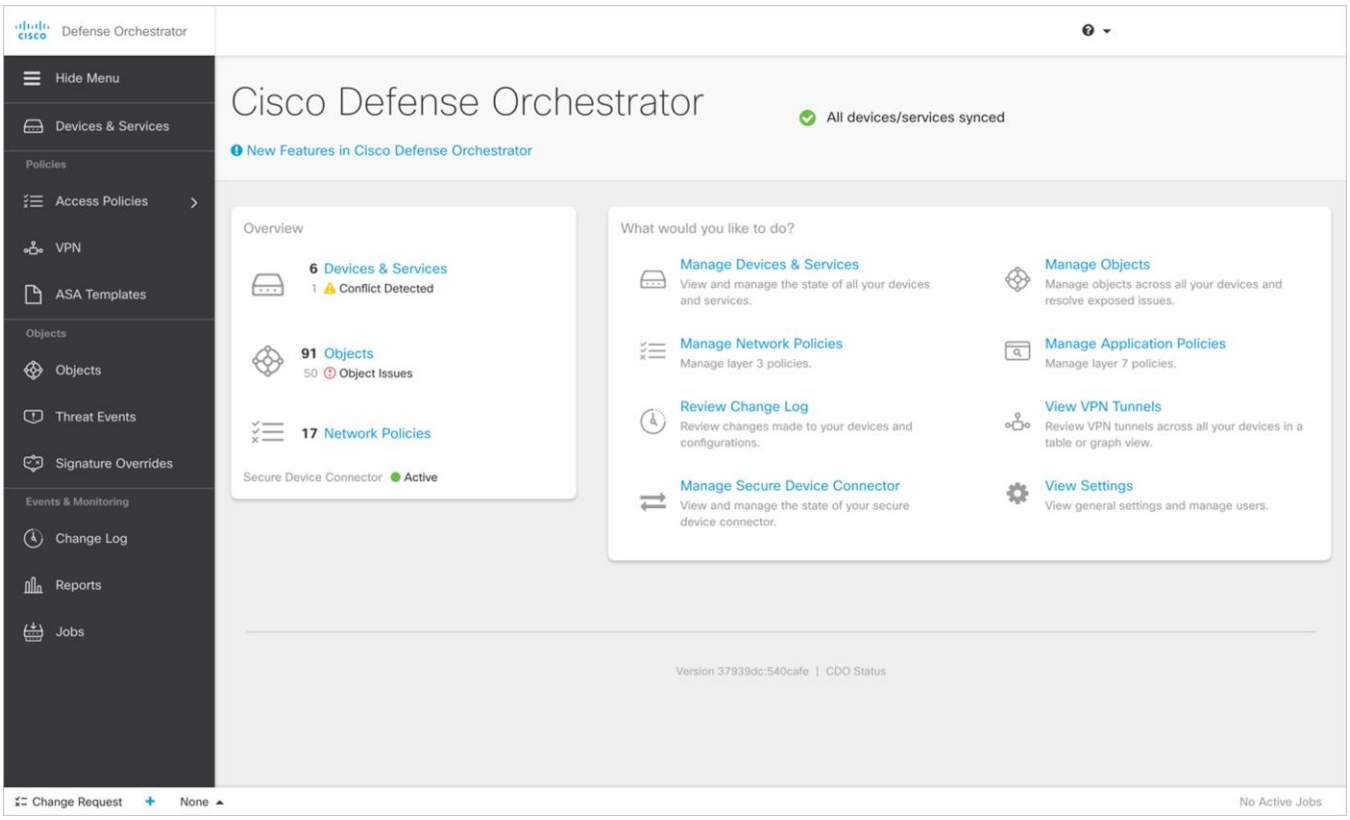

Figure 2.
Intuitive user interface speeds up adoption and decreases training time

Cisco Defense Orchestrator benefits

Staying on top of security is easier than ever. Cisco Defense Orchestrator helps you consistently manage policies and devices across your Cisco and cloud-native security products. It is a cloud-based application that cuts through complexity to save time and keep your organization protected against the latest threats.

- **Simplify management:** Streamline security policy and device management across your extended network.
- **Improve efficiency:** Reduce time spent on repetitive security management tasks by up to 90 percent.
- **Strengthen your security:** Achieve better, more consistent security while reducing complexity.

Cisco Defense Orchestrator features

Cisco Defense Orchestrator strengthens your security posture by aligning policies throughout your organization. Our solution addresses the challenge of staying on top of your policies when adding security tools. This is especially helpful for organizations with geographically dispersed locations as well as hybrid network environments.

The solution eliminates the time-consuming complexity of managing policies across distributed security devices. It helps prevent inconsistencies and gaps in your security.

You can manage from anywhere with a highly secure, always available, highly reliable, and scalable multitenant cloud solution. It frees up capacity for other priorities by strengthening and maintaining security posture in less time and with fewer resources.

Templates for consistent policy design: Using Cisco Defense Orchestrator, you can now create, apply, and manage a consistent policy design across disparate devices from a single place. Our template feature allows you to create a "gold configuration" that can be replicated and customized. Once you are done, you can export and apply your standardized configuration to any new platform.

Optimize your existing platforms: Upon onboarding, Cisco Defense Orchestrator will immediately be able to identify and flag common issues across firewalls that have been in production for years. After assessing and identifying all risks, you will now be able to swiftly remediate issues across all devices in bulk — bringing your devices to a consistent and more secure state. Cisco Defense Orchestrator helps to correct issues such as:

- **Unused objects** are objects that will never be hit and cause issues during troubleshooting as well as add to potentially unwanted questions during audits.
- **Duplicate objects** are often found on a device and associate different names to the same IPs. Removing duplicate objects can improve the overall performance of the appliance.
- **Inconsistent objects** are objects that get represented differently across deployed firewalls. This is typically the most important object issue from a security perspective. For example, if you had an object name "block list" and all devices are supposed to have this object with matching variables or IPs, Cisco Defense Orchestrator will quickly validate this. If the object is not consistent across firewall devices, Cisco Defense Orchestrator will alert you and allow you to resolve the issue in seconds.
- **Shadow rules** are rules that will never be hit due to a preceding rule that will supersede it.

Simplified OS upgrades: Often one of the most time consuming and frustrating challenges that our customers face is maintaining the firewall OS for both features and vulnerabilities. Using Cisco Defense Orchestrator, you can reduce the time it takes to perform Adaptive Security Appliance (ASA) or Cisco Firepower® Threat Defense (FTD) image upgrades by up to 90 percent. We take the guesswork out of planning and enable you to perform the upgrade in bulk across all of your devices at once.

CLI in bulk: In addition to an intuitive web-based UI, we also provide our Command Line Interface (CLI) users with a streamlined user experience as well. Cisco Defense Orchestrator's CLI Tool gives users the ability to perform CLI commands in bulk across many devices at once, including the ability to create user-defined macros or shortcuts for your most common commands.

Audit of changes with change-log: Customers can track changes through our change-log to review what change was made, when, and who performed the change. All changes made in both the Cisco Defense Orchestrator UI and the CLI Tool are captured.

Migration: It is now easier than ever to migrate your environment from Adaptive Security Appliance (ASA) to Cisco Firepower® Threat Defense (FTD), thanks to Cisco Defense Orchestrator's embedded migration wizard. It will even help you improve your configurations in the process.

Cisco Security Analytics and Logging: Improve network visibility so you can quickly detect threats in real time and remediate incidents with confidence at scale. Security Analytics and Logging allows organizations to store firewall logs, but also gain insights from behavioral analytics as well as get actionable security intelligence to help make security teams more efficient.

Management of hybrid environments: Managing a mix of firewalls running the ASA, FTD, and Meraki MX software is now easy, with the ability to share policy elements across platforms.

Management of AWS security groups: Cisco Defense Orchestrator now helps you manage your Amazon Web Services (AWS) Virtual Private Cloud (VPC) security groups. Orchestrate security groups across several VPCs and even AWS accounts, identify problems with objects and rules, and standardize policies between your AWS environment and existing premises-based ASA, FTD, and Meraki MX deployments. You can even visualize VPN tunnels between VPCs and Cisco equipment.

Table 1. Features and benefits

Objective	How we can make it happen
Fast deployment and device onboarding	Cisco Defense Orchestrator accounts are assigned in 24 hours and you can start onboarding devices almost immediately. Devices can be onboarded as just a configuration, single device, or thousands of devices through bulk imports with no associated downtime.
Object and policy analysis for optimization of existing devices	At onboarding, Cisco Defense Orchestrator will uncover areas for optimization and put the user in a position to quickly remediate the problems found. Common issues include duplicate, unused, and inconsistent objects across devices. We can also identify hit rates and shadow rules that will never be hit.
Options for proactive configuration and policy changes	Cisco Defense Orchestrator gives you options for how you can manage your devices centrally. If you prefer, you can deploy directly to the device immediately using the CLI Tool, enabling the use of "bulk" deployments, macros, and/or shortcuts for your most common commands. Next, you can also use the UI to provide a simple way to "stage" changes in the cloud during normal business hours then push these changes out at your next maintenance window.
Security templates	Leveraging an existing "gold configuration," you can design and manage templates for easy, consistent deployment of your new devices.
Simple search	See how policies are enforced across device types by searching for any object name, Access Control List (ACL) name, network, or application policy element.
Change-log	Track changes to the configuration being made within Cisco Defense Orchestrator for accountability, auditing, and troubleshooting purposes.
Out-of-band notifications	Changes made via ASDM or CLI (SSH) will be identified by the Cisco Defense Orchestrator administrator as an Out-Of-Band (OOB) change. The administrator can make the decision to keep this change or revert back to the original configuration.

Objective	How we can make it happen
Backup and rollback of configurations	Cisco Defense Orchestrator backs up the configuration after every change and offers the ability to roll back to the previous good known configuration.
Simple image upgrades	Streamline the approach to performing OS upgrades for faster access to the latest patches and features.
Troubleshoot potential issues	Built into Cisco Defense Orchestrator is the ability to pull live logs and run PacketTracer to help with troubleshooting of your devices.
Integration to third-party applications	Cisco Defense Orchestrator was developed on a REST API, which offers our customers and partners the opportunity to integrate with platforms such as Splunk, ServiceNow, and more.

Platform support matrix: Cisco security devices supported by Cisco Defense Orchestrator

Product	ASA software version	FTD version
ASA 5505, 5510, 5520, 5540, 5550	8.4 and later	N/A
ASAv	8.4 and later	N/A
ASA 5506-X, ASA 5512-X	8.4 and later	N/A
ASA 5508-X, ASA 5516-X	8.4 and later	6.4 and later
ASA 5515-X, 5525-X, 5545-X, 5555-X	8.4 and later	6.4 and later
ASA 5585-10, 5585-20, 5585-40, 5585-60	9.2.2 and later	N/A
ISA 3000	8.4 and later	6.4 and later
Firepower 1010, Firepower 1120, Firepower 1140, Firepower 1150*	9.13.1 and later	6.4 and later
Firepower 2110, Firepower 2120, Firepower 2130, Firepower 2140	8.4 and later	6.4 and later
Firepower 4110, Firepower 4115*, Firepower 4120, Firepower 4125*, Firepower 4140, Firepower 4145*, Firepower 4150	8.4 and later	6.5 and later
Firepower 9300	8.4 and later	6.5 and later
FTDv – KVM / WMWare	N/A	6.4 and later
FTDv – Azure	N/A	6.5 and later
Meraki MX	N/A	N/A

Ordering information

To place an order, visit the Cisco ordering homepage.

Table 2. Cisco Defense Orchestrator for managing Cisco firewalls: Subscription of 1, 3, and 5 years available

Part number	Description
L-FPR1010-P=	Cisco Defense Orchestrator for FPR1010 running ASA or FTD Image
L-FPR1120-P=	Cisco Defense Orchestrator for FPR1120 running ASA or FTD Image
L-FPR1140-P=	Cisco Defense Orchestrator for FPR1140 running ASA or FTD Image
L-FRP1150-P=	Cisco Defense Orchestrator for FPR1150 running ASA or FTD Image
L-ASA5505-P=	Cisco Defense Orchestrator for ASA 5505 running ASA or FTD Image
L-ASA5506-P=	Cisco Defense Orchestrator for ASA 5506 running ASA or FTD Image
L-ASA5506W-P=	Cisco Defense Orchestrator for ASA 5506W running ASA or FTD Image
L-ASA5506H-P=	Cisco Defense Orchestrator for ASA 5506H running ASA or FTD Image
L-ASA5508-P=	Cisco Defense Orchestrator for ASA 5508 running ASA or FTD Image
L-ASA5512-P=	Cisco Defense Orchestrator for ASA 5512 running ASA or FTD Image
L-ASA5515-P=	Cisco Defense Orchestrator for ASA 5515 running ASA or FTD Image
L-ASA5516-P=	Cisco Defense Orchestrator for ASA 5516 running ASA or FTD Image
L-ASA5525-P=	Cisco Defense Orchestrator for ASA 5525 running ASA or FTD Image
L-ASA5545-P=	Cisco Defense Orchestrator for ASA 5545 running ASA or FTD Image
L-ASA5555-P=	Cisco Defense Orchestrator for ASA 5555 running ASA or FTD Image
L-ASA5585-P=	Cisco Defense Orchestrator for ASA 5585 running ASA or FTD Image
L-ASAV-P=	Cisco Defense Orchestrator for Cisco Adaptive Security Virtual Appliance (ASAv) running ASA or FTD Image
L-FPRTD-V-P=	Cisco Defense Orchestrator for virtual FTD running ASA or FTD Image
L-FPR2110-P=	Cisco Defense Orchestrator for FPR 2110 running ASA or FTD Image
L-FPR2120-P=	Cisco Defense Orchestrator for FPR 2120 running ASA or FTD Image
L-FPR2130-P=	Cisco Defense Orchestrator for FPR 2130 running ASA or FTD Image
L-FPR2140-P=	Cisco Defense Orchestrator for FPR 2140 running ASA or FTD Image
L-FPR4110-P=	Cisco Defense Orchestrator for FPR 4110 running ASA or FTD Image

Part number	Description
L-FPR4120-P=	Cisco Defense Orchestrator for FPR 4120 running ASA or FTD Image
L-FPR4140-P=	Cisco Defense Orchestrator for FPR 4140 running ASA or FTD Image
L-FPR4150-P=	Cisco Defense Orchestrator for FPR 4150 running ASA or FTD Image
L-FPR4115-P=	Cisco Defense Orchestrator for Firepower 4115 running ASA or FTD Image
L-FPR4125-P=	Cisco Defense Orchestrator for Firepower 4125 running ASA or FTD Image
L-FPR4145-P=	Cisco Defense Orchestrator for Firepower 4145 running ASA or FTD Image
L-FPR-9K-P=	Cisco Defense Orchestrator for FPR 9300 Series running ASA or FTD Image
L-ISA3000-P=	Cisco Defense Orchestrator for ISA 3000 running ASA or FTD Image
L-MX64-P=	Cisco Defense Orchestrator for Meraki MX64 Platform
L-MX65-P=	Cisco Defense Orchestrator for Meraki MX65 Platform
L-MX67-P=	Cisco Defense Orchestrator for Meraki MX67 Platform
L-MX68-P=	Cisco Defense Orchestrator for Meraki MX68 Platform
L-MX84-P=	Cisco Defense Orchestrator for Meraki MX84 Platform
L-MX100-P=	Cisco Defense Orchestrator for Meraki MX100 Platform
L-MX250-P=	Cisco Defense Orchestrator for Meraki MX250 Platform
L-MX450-P=	Cisco Defense Orchestrator for Meraki MX450 Platform
L-AWS-SG-P=	Cisco Defense Orchestrator for Amazon Web Services VPC Security Group

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

More Information: https://www.cisco.com/go/cdo. Need a demo or proof of value? Contact cdosales@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-736847-08 01/20