

# Cisco Defense Orchestrator

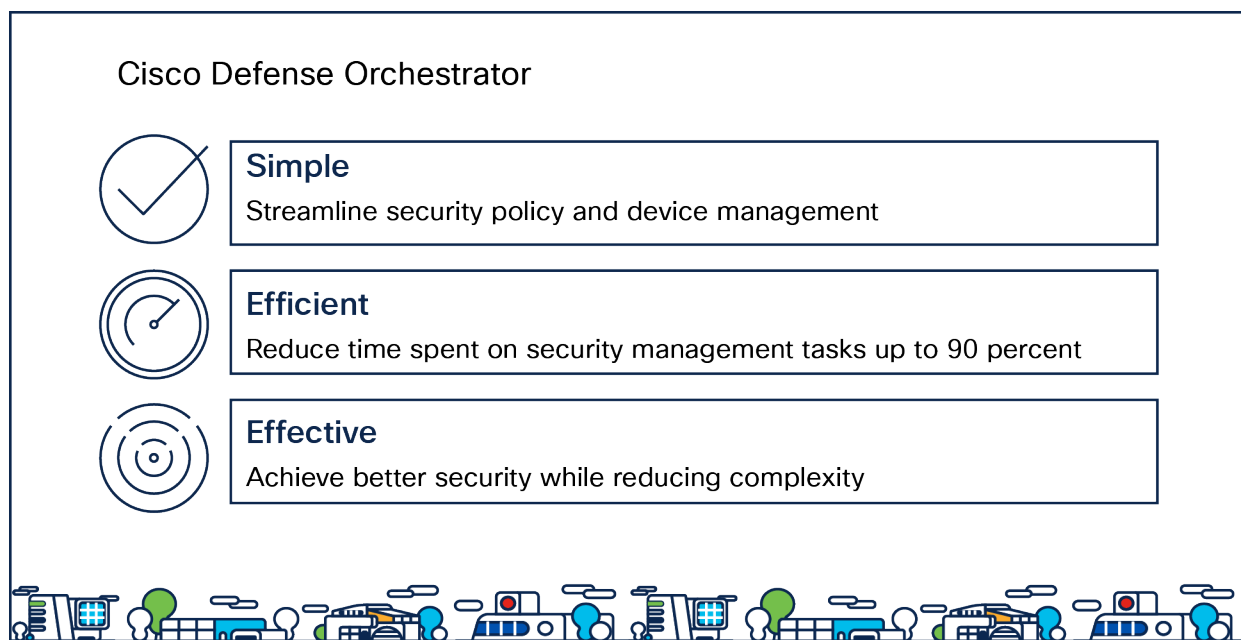
---

# Contents

Cloud-based Firewall Management	3
Cisco Defense Orchestrator benefits	4
Cisco Defense Orchestrator features	5
Cisco platform integration: Native integration to other key Cisco applications	8
Platform support matrix: Cisco security devices supported by Cisco Defense Orchestrator	9
Ordering information	10
Cisco Capital	16
For more information	16

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 heterogeneous environments will continue to place greater demands on network operations teams. Organizations need a simplified approach to managing security policies across Cisco® firewalls to improve efficiencies, drive consistency, and reduce risk.



**Figure 1.** Cisco Defense Orchestrator design principles: simple, efficient, and 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.

Cisco Defense Orchestrator centrally manages elements of policy and configuration across:

- Cisco Multicloud Defense
- Cisco Secure Firewall ASA, both on-premises and virtual
- Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual
- Cisco Meraki™ MX
- Cisco IOS devices
- AWS security groups

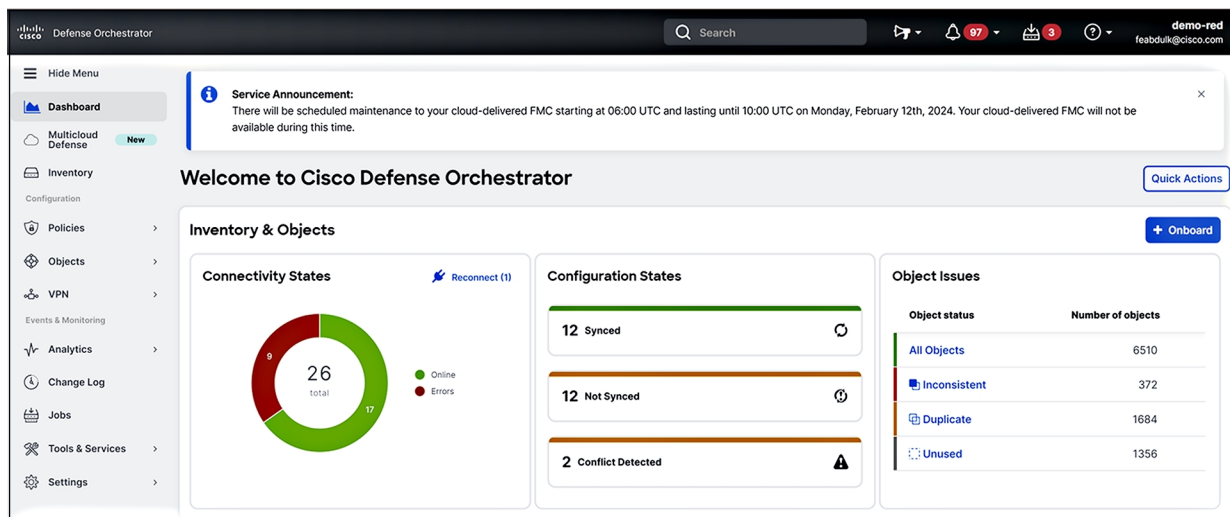
Cisco Defense Orchestrator also incorporates the cloud-delivered version of Firewall Management Center (FMC), providing a fully unified experience between on-premises and cloud-based firewall management. This expands management of policy and configuration to:

- Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual
- Cisco Secure IPS (formerly Firepower NGIPS)
- Cisco Firewall Threat Defense for ISR

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-based solution, Cisco Defense Orchestrator does not require capital expenditures, rack space, or manual patching and upgrading, dramatically reducing your operational costs.

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



**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.
- **Resiliency:** Robust data centers across multiple regions ensure high uptime.

---

## 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.

**Optimization for 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 the following issues:

- **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 preceding rules that supersede them.

**Simplified firewall 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 Cisco ASA or Cisco 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 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.

**ASA-to-FTD transition:** It is now easier than ever to migrate your environment from ASA to Cisco Threat Defense (FTD), thanks to Cisco Defense Orchestrator’s embedded migration wizard. Manage both ASA and FTD from a single UI, enabling you to transition to NGFW in your own timeline!

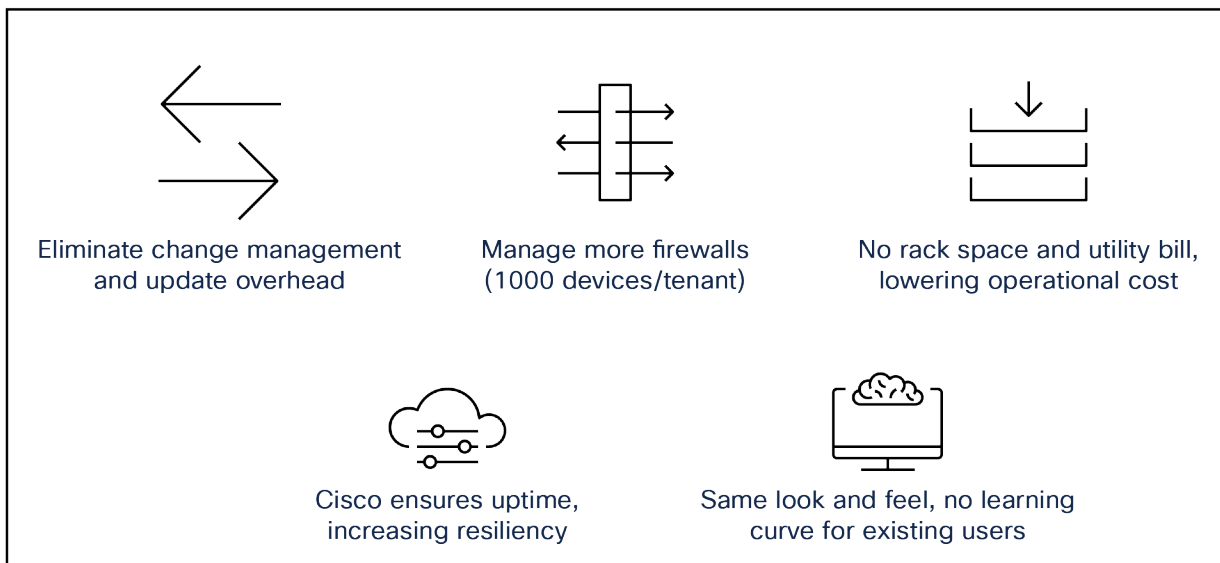
**Management of hybrid environments (ASA, FTD and Multicloud Defense):** Enable secure hybrid connectivity between on-premises and cloud environment and ensure consistent policy outcomes through object sharing, thereby streamlining operations, and extending security across hybrid, multi-cloud environments.

**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.

**Remote-access VPN monitoring and management:** Visibility across remote user sessions and head-end devices with a historical view over 90 days for capacity planning. Extend visibility of user traffic by leveraging Cisco Security Analytics and Logging.

**Cloud-delivered version of Firewall Management Center:** Offers the same look –and feel as on-premises and virtual versions of Firewall Management Center, with:

- **Comprehensive visibility and policy control:** Provides exceptional visibility into what is running in your network and cloud so you can see what needs to be protected. Using this visibility, you can create and manage firewall rules and control thousands of web and custom applications used in your environment.
- **Automated security for dynamic defense:** Continually monitors how your network is changing, streamlining operations, and improving your security so you can focus on the threats that matter.



**Figure 3.** Benefits of cloud-delivered Firewall Management Center via CDO.

For more information, visit the [Cisco Secure Firewall Management Center \(formerly Firepower Management Center\) Data Sheet](#).

For more information on Multicloud Defense, visit [Cisco Multicloud Defense](#).

**Table 1.** Features and benefits

Objective	How we can make it happen
<b>Fast deployment and device onboarding</b>	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Low-touch provisioning streamlines large-scale remote deployments. Available for Firepower 1000 Series and 2000 Series running FTD version 7.0.3 and later (excluding 7.1).</li> </ul>
<b>Object and policy analysis for optimization of existing devices</b>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
<b>Options for proactive configuration and policy changes</b>	<ul style="list-style-type: none"> <li>• 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 and then push these changes out at your next maintenance window.</li> </ul>
<b>Security templates</b>	<ul style="list-style-type: none"> <li>• Leveraging an existing “gold configuration,” you can design and manage templates for easy, consistent deployment of your new devices.</li> </ul>
<b>Simple search</b>	<ul style="list-style-type: none"> <li>• See how policies are enforced across device types by searching for any object name, Access Control List (ACL) name, network, or application policy element.</li> </ul>
<b>ASA-to-FTD transition</b>	<ul style="list-style-type: none"> <li>• <b>Migrate your environment from ASA to Cisco Threat Defense (FTD) using Cisco Defense Orchestrator’s embedded migration wizard.</b></li> </ul>
<b>Change log</b>	<ul style="list-style-type: none"> <li>• Track changes to the configuration being made within Cisco Defense Orchestrator for accountability, auditing, and troubleshooting purposes.</li> </ul>
<b>Out-of-band notifications</b>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
<b>Backup and rollback of configurations</b>	<ul style="list-style-type: none"> <li>• Cisco Defense Orchestrator backs up the configuration after every change and offers the ability to roll back to previous configurations.</li> </ul>
<b>Simple image upgrades</b>	<ul style="list-style-type: none"> <li>• Streamline the approach to performing OS upgrades for faster access to the latest patches and features.</li> </ul>
<b>Troubleshooting of potential issues</b>	<ul style="list-style-type: none"> <li>• Built into Cisco Defense Orchestrator is the ability to pull live logs and run PacketTracer to help with troubleshooting of your devices.</li> </ul>
<b>Integration to third-party applications</b>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>

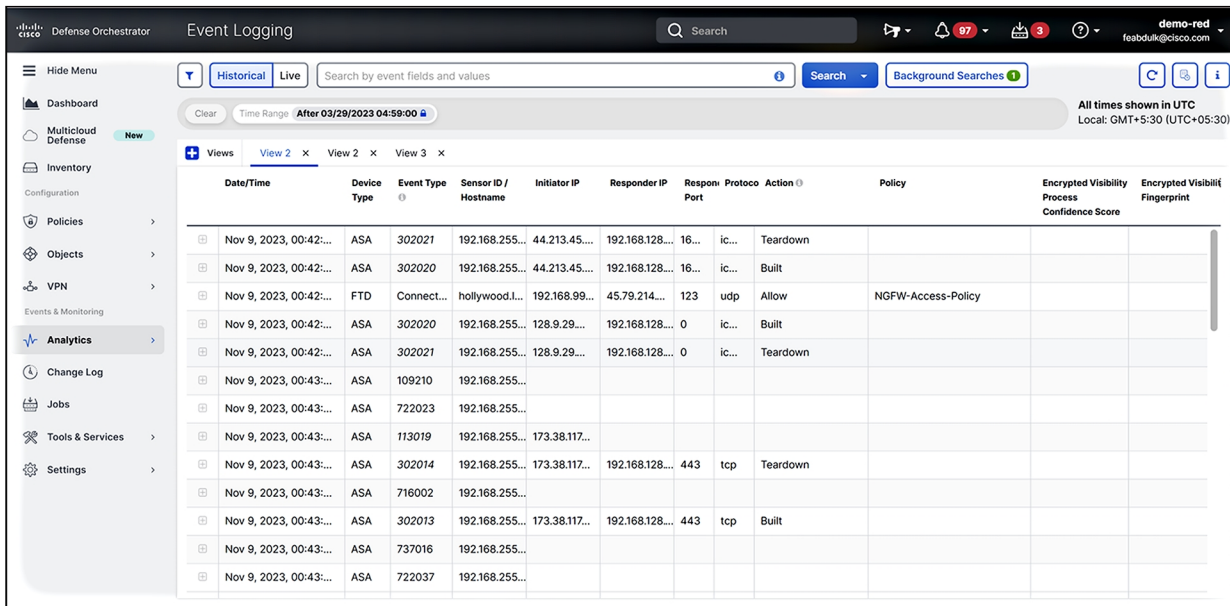
# Cisco platform integration: Native integration to other key Cisco applications

## Cisco Security Analytics and Logging (SAL) SaaS Overview

A cloud-delivered, Software-as-a-Service (SaaS) offering with a cloud-native data store, referred to as SAL (SaaS)

**SAL (SaaS)** is a full-feature offering providing cloud-based and cloud-delivered log management for Next-Generation Firewalls (NGFWs) running Cisco Firepower® Threat Defense (FTD) software, as well as devices running the Adaptive Security Appliance (ASA) software, independent of their management platform. SAL (SaaS) enables event viewing via APIs in Cisco Defense Orchestrator (CDO) for firewall event logs.

**Cisco Security Logging and Troubleshooting:** Allows organizations to store firewall logs in the cloud and present visually in Cisco Defense Orchestrator’s event viewer. Correlate historical and/or live events from your firewall platforms for troubleshooting.



The screenshot shows the Cisco Defense Orchestrator (CDO) Event Logging interface. The interface includes a search bar, a time range filter set to 'After 03/29/2023 04:59:00', and a table of events. The table has columns for Date/Time, Device Type, Event Type, Sensor ID / Hostname, Initiator IP, Responder IP, Respon. Port, Protocol, Action, Policy, Encrypted Visibility Process Confidence Score, and Encrypted Visibility Fingerprint. The table contains 12 rows of event data.

Date/Time	Device Type	Event Type	Sensor ID / Hostname	Initiator IP	Responder IP	Respon. Port	Protocol	Action	Policy	Encrypted Visibility Process Confidence Score	Encrypted Visibility Fingerprint
Nov 9, 2023, 00:42:...	ASA	302021	192.168.255...	44.213.45...	192.168.128...	16...	ic...	Teardown			
Nov 9, 2023, 00:42:...	ASA	302020	192.168.255...	44.213.45...	192.168.128...	16...	ic...	Built			
Nov 9, 2023, 00:42:...	FTD	Connect...	hollywood.l...	192.168.99...	45.79.214...	123	udp	Allow	NGFW-Access-Policy		
Nov 9, 2023, 00:42:...	ASA	302020	192.168.255...	128.9.29...	192.168.128...	0	ic...	Built			
Nov 9, 2023, 00:42:...	ASA	302021	192.168.255...	128.9.29...	192.168.128...	0	ic...	Teardown			
Nov 9, 2023, 00:43:...	ASA	109210	192.168.255...								
Nov 9, 2023, 00:43:...	ASA	722023	192.168.255...								
Nov 9, 2023, 00:43:...	ASA	113019	192.168.255...	173.38.117...							
Nov 9, 2023, 00:43:...	ASA	302014	192.168.255...	173.38.117...	192.168.128...	443	tcp	Teardown			
Nov 9, 2023, 00:43:...	ASA	716002	192.168.255...								
Nov 9, 2023, 00:43:...	ASA	302013	192.168.255...	173.38.117...	192.168.128...	443	tcp	Built			
Nov 9, 2023, 00:43:...	ASA	737016	192.168.255...								
Nov 9, 2023, 00:43:...	ASA	722037	192.168.255...								

**Figure 4.** Integrated cloud-based live logging to extend troubleshooting capabilities and provide historical visibility for audit purposes.

## Required components and setup to run Cisco Security Analytics and Logging (SaaS):

**Secure Event Connector:** To capture Firewall Event Logs from cloud deployments, a Secure Event Connector (SEC) is needed. The SEC is a containerized application that can be installed on an on-premises or cloud Secure Device Connector (SDC), or even be set up to run in standalone mode. It receives events from Firepower Threat Defense (FTD) devices and Adaptive Security Appliance (ASA) devices and forwards them to Cisco SAL in the cloud. Installation instructions can be found here. While SEC remains the most scalable route to send logs to SAL (SaaS), firewall devices running Cisco Firepower version 6.5 or later can send event logs directly to SAL Cloud, without the need for an SEC. This capability has been found to reliably support sustained peak rates of up to 8,500 events per second (eps) per firewall device. The Cisco Firewall Management Center (FMC) version 7.0 supports this direct- to-cloud route of devices under its management through its “Integrations” settings.



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

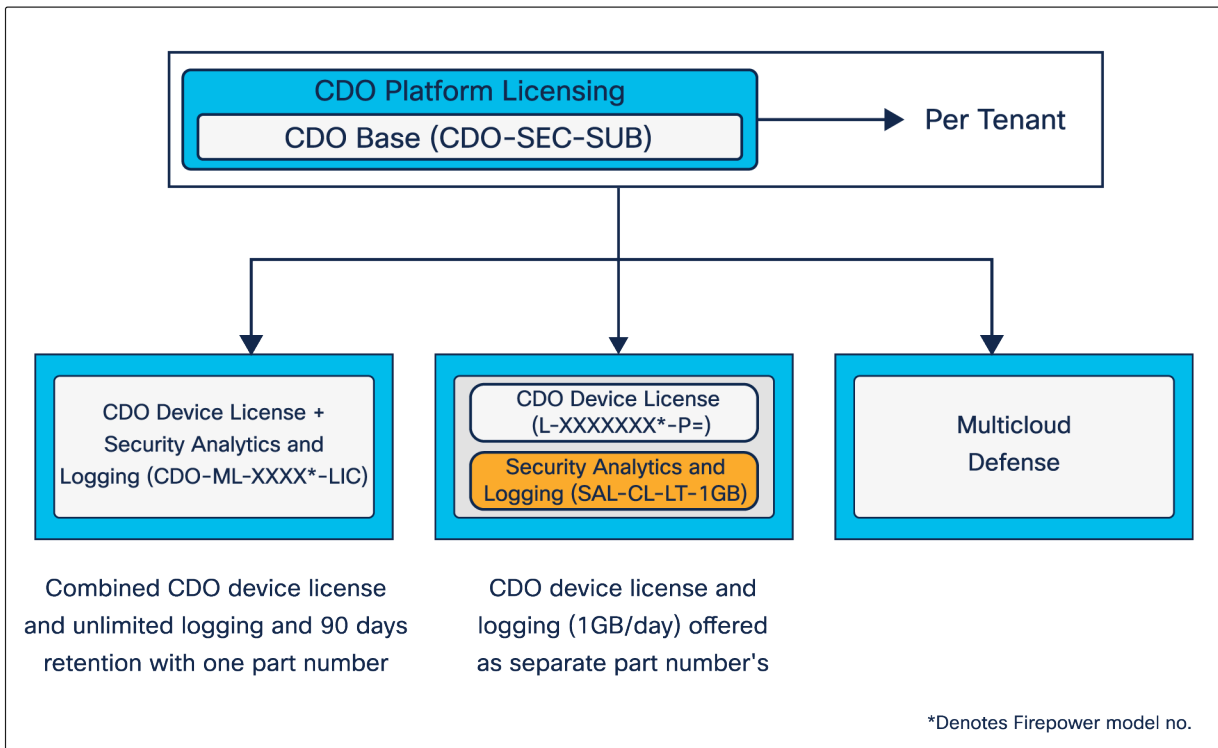
**Table 2.** Cisco security devices supported by Cisco Defense Orchestrator

Product	ASA software version	FTD version
ASAv	8.4 and later	N/A
ASA 5506-X, ASA 5512-X	8.4 and later	N/A
ASA 5525-X, 5545-X, 5555-X	8.4 and later	N/A
ASA 5585-10, 5585-20, 5585-40, 5585-60	8.4 and later	N/A
ISA 3000	8.4 and later	7.0.3 and later (excluding 7.1)
Firepower 1010, Firepower 1120, Firepower 1140, Firepower 1150	9.8 and later	7.0.3 and later (excluding 7.1)
Firepower 2110, Firepower 2120, Firepower 2130, Firepower 2140	9.8 and later	7.0.3 and later (excluding 7.1)
Firepower 3105, Firepower 3110, Firepower 3120, Firepower 3130, Firepower 3140	9.17.1 for 3100, 3120, 3130 and 3140, 9.19.1 for 3105 and later	7.1 and later
Firepower 4112, Firepower 4115, Firepower 4125, Firepower 4145,	9.4 and later	7.0.3 and later (excluding 7.1)
Firepower 4215, Firepower 4225, Firepower 4245	9.20 and later	7.4 and later
Firepower 9300	9.4 and later	7.0.3 and later (excluding 7.1)
FTDv: KVM, VMware, Azure	NA	7.0.3 and later (excluding 7.1)
Meraki MX	NA	NA
Cisco IOS (SSH): Limited to CLI Tool and Change Log Only	NA	NA

## Ordering information

Cisco Defense Orchestrator requires a base subscription for tenant entitlement that covers ASA, FTD and Multicloud Defense. For Firewall customers, there will be per-device license subscription for device management entitlement. Cisco Defense Orchestrator Device License Subscription with Unlimited Logging subscription is available separately. Subscriptions of one, three, and five years are available.

For Multicloud Defense, the product licensing is based on the consumed amount of aggregated gateway hours across all the cloud environments. The product has two tiers available, namely, Advantage and Premier. Firewall device licenses, such as Threat, Malware, URL filtering, and support, should be purchased separately. Security Logging and Analytics can also be added for logging and troubleshooting use cases.



**Figure 5.**  
Cisco Defense Orchestrator licensing structure

\*denotes the firepower model. For example, if you are ordering 10 Cisco FPR1010 devices and want to manage these devices from CDO with unlimited logging and 90 days retention, the part number will be CDO-ML-FP1010-LIC along with CDO-SEC-SUB (tenant entitlement). Another example, if you are ordering 10 Cisco FPR3110 devices and want to manage these devices from CDO with separate logging (1GB/day), there will be 2 part numbers - L-FPR3110-P= & SAL-CL-LT-1GB along with CDO-SEC-SUB (tenant entitlement). Relevant subscription term to be chosen.

[Refer to Guidelines for Quoting Cisco Defense Orchestrator Products Ordering Guide](#) for more information on ordering Cisco Defense Orchestrator. To place an order, [visit the Cisco ordering homepage](#).

**Table 3.** Cisco Defense Orchestrator XaaS license for tenant entitlement

Part number	Description
CDO-SEC-SUB	Cisco Defense Orchestrator XaaS Subscription

**Table 4.** Cisco Defense Orchestrator Base License Subscription tenant entitlement: subscription of 1, 3, and 5 years available

Part number	Description
CDO-BASE-LIC	Cisco Defense Orchestrator Base License Subscription

**Table 5.** SAL Saas logging and troubleshooting XaaS license for logging entitlement

Part number	Description
SAL-SUB	SAL XaaS Subscription

**Table 6.** 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-FPR1150-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-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)
L-FPRTD-V-P=	Cisco Defense Orchestrator for Virtual FTD (FTDv5/10/20/30/50/100)

Part number	Description
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-FPR3105-P=	Cisco Defense Orchestrator for FPR 3105 running ASA or FTD Image
L-FPR3110-P=	Cisco Defense Orchestrator for FPR 3110 running ASA or FTD Image
L-FPR3120-P=	Cisco Defense Orchestrator for FPR 3120 running ASA or FTD Image
L-FPR3130-P=	Cisco Defense Orchestrator for FPR 3130 running ASA or FTD Image
L-FPR3140-P=	Cisco Defense Orchestrator for FPR 3140 running ASA or FTD Image
L-FPR4112-P=	Cisco Defense Orchestrator for FPR 4112 running ASA or FTD Image
L-FPR4115-P=	Cisco Defense Orchestrator for FPR 4115 running ASA or FTD Image
L-FPR4125-P=	Cisco Defense Orchestrator for FPR 4125 running ASA or FTD Image
L-FPR4145-P=	Cisco Defense Orchestrator for FPR 4145 running ASA or FTD Image
L-FPR4215-P=	Cisco Defense Orchestrator for FPR 4215 running ASA or FTD Image
L-FPR4225-P=	Cisco Defense Orchestrator for FPR 4225 running ASA or FTD Image
L-FPR4245-P=	Cisco Defense Orchestrator for FPR 4245 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-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=	Cisco Defense Orchestrator for Amazon Web Services VPC Security Group

**Table 7.** Cisco Defense Orchestrator for managing Cisco firewalls with unlimited logging and 90 days retention: subscription of 1, 3, and 5 years available.

Part number	Description
CDO-ML-FP1010-LIC	Cisco Defense Orchestrator for FPR1010 ASA or FTD Image
CDO-ML-FP1010E-LIC	Cisco Defense Orchestrator for FPR1010E ASA or FTD Image
CDO-ML-FP1120-LIC	Cisco Defense Orchestrator for FPR1120 ASA or FTD Image
CDO-ML-FP1140-LIC	Cisco Defense Orchestrator for FPR1140 ASA or FTD Image
CDO-ML-FP1150-LIC	Cisco Defense Orchestrator for FPR1150 ASA or FTD Image
CDO-ML-FP2110-LIC	Cisco Defense Orchestrator for FPR2110 ASA or FTD Image
CDO-ML-FP2120-LIC	Cisco Defense Orchestrator for FPR2120 ASA or FTD Image
CDO-ML-FP2130-LIC	Cisco Defense Orchestrator for FPR2130 ASA or FTD Image
CDO-ML-FP2140-LIC	Cisco Defense Orchestrator for FPR2140 ASA or FTD Image
CDO-ML-FP3105-LIC	Cisco Defense Orchestrator for FPR3105 ASA or FTD Image
CDO-ML-FP3110-LIC	Cisco Defense Orchestrator for FPR3110 ASA or FTD Image
CDO-ML-FP3120-LIC	Cisco Defense Orchestrator for FPR3120 ASA or FTD Image
CDO-ML-FP3130-LIC	Cisco Defense Orchestrator for FPR3130 ASA or FTD Image
CDO-ML-FP3140-LIC	Cisco Defense Orchestrator for FPR3140 ASA or FTD Image
CDO-ML-FP4112-LIC	Cisco Defense Orchestrator for FPR4112 ASA or FTD Image
CDO-ML-FP4115-LIC	Cisco Defense Orchestrator for FPR4115 ASA or FTD Image
CDO-ML-FP4125-LIC	Cisco Defense Orchestrator for FPR4125 ASA or FTD Image
CDO-ML-FP4145-LIC	Cisco Defense Orchestrator for FPR4145 ASA or FTD Image
CDO-ML-FP4215-LIC	Cisco Defense Orchestrator for FPR4215 ASA or FTD Image
CDO-ML-FP4225-LIC	Cisco Defense Orchestrator for FPR4225 ASA or FTD Image
CDO-ML-FP4245-LIC	Cisco Defense Orchestrator for FPR4245 ASA or FTD Image
CDO-ML-F9K-S40-LIC	Cisco Defense Orchestrator for FPR9K-SM40 ASA or FTD Image
CDO-ML-F9K-S48-LIC	Cisco Defense Orchestrator for FPR9K-SM48 ASA or FTD Image
CDO-ML-F9K-S56-LIC	Cisco Defense Orchestrator for FPR9K-SM56 ASA or FTD Image
CDO-ML-FTDV5-LIC	Cisco Defense Orchestrator -FTDV Base Lic,100Mbps
CDO-ML-FTDV10-LIC	Cisco Defense Orchestrator -FTDV Base Lic, 1Gbps

Part number	Description
CDO-ML-FTDV20-LIC	Cisco Defense Orchestrator -FTDV Base Lic, 3Gbps
CDO-ML-FTDV30-LIC	Cisco Defense Orchestrator -FTDV Base Lic, 5Gbps
CDO-ML-FTDV50-LIC	Cisco Defense Orchestrator -FTDV Base Lic, 10Gbps
CDO-ML-FTDV100-LIC	Cisco Defense Orchestrator -FTDV Base Lic, 16Gbps

**Table 8.** Cisco Logging and Troubleshooting with subscription of 1, 3, and 5 years available

Part number	Description
SAL-CL-LT-1GB	License Logging and Troubleshooting for 1GB/day
SAL-CL-LT-OVRG	Usage-based overage PID for License Logging and Troubleshooting, not charged at time of placing order but is used to calculate overage charges if entitlement is exceeded.
SEC-LOG-CL	Cloud logging with 90 days storage -GB/day
SAL-CL-1GB-(1/2/3)Y-EXTN*	1/2/3 year of logs retention (up from default of 90 days).
SEC-CL-DR-(1/2/3)Y*	Data Retention extensions, which extend log retention to 1, 2, or 3 years in the cloud.
SAL-CL-LT-1GB	License Logging and Troubleshooting for 1GB/day

\*Log retention period can optionally be extended to 1, 2, or 3 years

### Security Buying Programs

The offer leverages the Security Choice Enterprise Agreement buying program with the following PIDs: The mapping for Choice EA PIDs to CDO, SAL (SaaS) a-la-carte PIDs.

**Table 9.**

EA 2.0 ATO	EA 2.0 Billing PID	EA 3.0 ATO	EA 3.0 Billing PID	A-la-carte Fulfillment PID
E2F-SEC-CDO	E2SF-O-CDO5508P	E3-SEC-CDO	E3S-CDO5508P	L-ASA5508-P=
E2F-SEC-CDO	E2SF-O-CDO5516P	E3-SEC-CDO	E3S-CDO5516P	L-ASA5516-P=
E2F-SEC-CDO	E2SF-O-CDO5525P	E3-SEC-CDO	E3S-CDO5525P	L-ASA5525-P=
E2F-SEC-CDO	E2SF-O-CDO5545P	E3-SEC-CDO	E3S-CDO5545P	L-ASA5545-P=
E2F-SEC-CDO	E2SF-O-CDO5555P	E3-SEC-CDO	E3S-CDO5555P	L-ASA5555-P=
E2F-SEC-CDO	E2SF-O-CDO-BASE	E3-SEC-CDO	E3S-O-CDO-BASE	CDO-BASE-LIC
E2F-SEC-CDO	E2SF-O-CDOFPR9K	E3-SEC-CDO	E3S-CDOFPR9K	L-FPR-9K-P=
E2F-SEC-CDO	E2SF-O-FPR1010-P	E3-SEC-CDO	E3S-CDOFPR1010-P	L-FPR1010-P=
E2F-SEC-CDO	E2SF-O-FPR1120-P	E3-SEC-CDO	E3S-CDOFPR1120-P	L-FPR1120-P=

EA 2.0 ATO	EA 2.0 Billing PID	EA 3.0 ATO	EA 3.0 Billing PID	A-la-carte Fulfillment PID
E2F-SEC-CDO	E2SF-O-FPR1140-P	E3-SEC-CDO	E3S-CDOFPR1140-P	L-FPR1140-P=
E2F-SEC-CDO	E2SF-O-FPR1150-P	E3-SEC-CDO	E3S-CDOFPR1150-P	L-FPR1150-P=
E2F-SEC-CDO	E2SF-O-FPR2110-P	E3-SEC-CDO	E3S-CDOFPR2110-P	L-FPR2110-P=
E2F-SEC-CDO	E2SF-O-FPR2120-P	E3-SEC-CDO	E3S-CDOFPR2120-P	L-FPR2120-P=
E2F-SEC-CDO	E2SF-O-FPR2130-P	E3-SEC-CDO	E3S-CDOFPR2130-P	L-FPR2130-P=
E2F-SEC-CDO	E2SF-O-FPR2140-P	E3-SEC-CDO	E3S-CDOFPR2140-P	L-FPR2140-P=
E2F-SEC-CDO	E2SF-O-FPR3110-P	E3-SEC-CDO	E3S-CDOFPR3110-P	L-FPR3110-P=
E2F-SEC-CDO	E2SF-O-FPR3120-P	E3-SEC-CDO	E3S-CDOFPR3120-P	L-FPR3120-P=
E2F-SEC-CDO	E2SF-O-FPR3130-P	E3-SEC-CDO	E3S-CDOFPR3130-P	L-FPR3130-P=
E2F-SEC-CDO	E2SF-O-FPR3140-P	E3-SEC-CDO	E3S-CDOFPR3140-P	L-FPR3140-P=
E2F-SEC-CDO	E2SF-O-FPR4110-P	E3-SEC-CDO	E3S-CDOFPR4110-P	L-FPR4110-P=
E2F-SEC-CDO	E2SF-O-FPR4112-P	E3-SEC-CDO	E3S-CDOFPR4112-P	L-FPR4112-P=
E2F-SEC-CDO	E2SF-O-FPR4115-P	E3-SEC-CDO	E3S-CDOFPR4115-P	L-FPR4115-P=
E2F-SEC-CDO	E2SF-O-FPR4120-P	E3-SEC-CDO	E3S-CDOFPR4120-P	L-FPR4120-P=
E2F-SEC-CDO	E2SF-O-FPR4125-P	E3-SEC-CDO	E3S-CDOFPR4125-P	L-FPR4125-P=
E2F-SEC-CDO	E2SF-O-FPR4140-P	E3-SEC-CDO	E3S-CDOFPR4140-P	L-FPR4140-P=
E2F-SEC-CDO	E2SF-O-FPR4145-P	E3-SEC-CDO	E3S-CDOFPR4145-P	L-FPR4145-P=
E2F-SEC-CDO	E2SF-O-FPR4150-P	E3-SEC-CDO	E3S-CDOFPR4150-P	L-FPR4150-P=
E2F-SEC-SAL-ESS	E2SF-S-SALE-EXT-1Y	E3-SEC-SAL-LT	E3S-SALLT-STG-1Y	SAL-CL-1GB-1Y-EXTN
E2F-SEC-SAL-ESS	E2SF-S-SALE-EXT-2Y	E3-SEC-SAL-LT	E3S-SALLT-STG-2Y	SAL-CL-1GB-2Y-EXTN
E2F-SEC-SAL-ESS	E2SF-S-SALE-EXT-3Y	E3-SEC-SAL-LT	E3S-SALLT-STG-3Y	SAL-CL-1GB-3Y-EXTN
E2F-SEC-SAL-ESS	E2SF-S-SAL-ESS	E3-SEC-SAL-LT	E3S-SAL-LT	SAL-CL-LT-1GB

---

## 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

**Cisco Defense Orchestrator**, [learn more](#).

**Firewall Management Center**, [learn more](#).

**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>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)