Cisco Defense Orchestrator (CDO)

Cisco Partner
https://cs.co/1page

Cisco Defense Orchestrator (CDO) is a cloud-based SaaS multi-device manager that facilitates management of security policies in highly distributed environments to achieve consistent policy implementation. CDO helps you optimize your security policies by identifying inconsistencies with them and by giving you tools to fix them.

Benefits:

Simplify: Streamline security policy and device management across extended network.
Improve efficiency: Reduce time spent on repetitive management tasks by up to 90%.
Strengthen security: Achieve better and consistent security while reducing complexity.
Resiliency: Robust data centers across multiple regions ensure high uptime.

Features:

Unify security policy and objects: Manage security policy consistently across the Cisco firewall portfolio - including Secure Firewall with FTD and ASA software, Umbrella and Meraki - as well as Amazon Web Services (AWS).

Optimize configurations: Analyze policies and objects across security devices to identify errors and inconsistencies. Correct them in seconds to improve your security posture and device performance.

Deploy devices faster: Drive consistency and efficiency by leveraging templates for new deployments. Efficiency with low-touch provisioning for faster deployments.

Simplify upgrades: Conduct ASA and FTD software upgrades within minimal clicks.

Track every change: Every change made over time is continuously documented and viewable in the change log. Roll back to a last-known good configuration at any time.

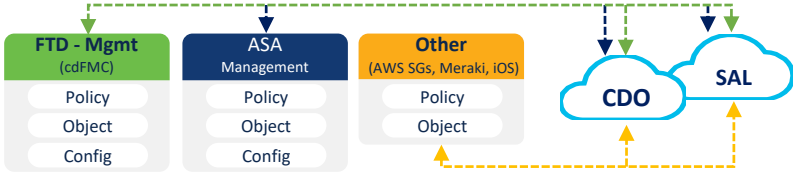
End-to-end visibility: Leverages Cisco Security Analytics and Logging (SAL) to provide high-fidelity alerts on threats such as C&C attacks, ransomware, DDoS attacks, Cryptomining, known malware, and insider threats.

Optimize operational efficiency: Integration with other Cisco Secure solutions provides additional automation while reducing risk.

Unified event viewer: ASA and FTD logs are available in a single pane of glass.

Cloud Delivered FMC (cdFMC): CDO platform offering to manage Secure Firewalls. cdFMC offers the same look, functionality, and workflow as on-premises and virtual versions of the Firewall Management Center. Compare each with the feature matrix.

Monitor Remote Access VPN: Monitor Remote Access VPN sessions for both ASA and FTD natively in CDO.



Solutions:

[1] xxxx denotes Firepower model no.

CDO centrally manages elements of policy and configuration across:

- Secure Firewall on-prem and virtual
- Cisco Secure Firewall Cloud Native (SFCN)
- Cisco Adaptive Security Appliance (ASA) 5500-X Series and virtual (ASAv)
- Virtual - Private Cloud (KVM, VMWare)
- Virtual - Public Cloud (AWS, Azure, Hyperflex, Nutanix)
- Meraki MX Series
- Cisco Umbrella
- Cisco IOS devices
- Amazon Web Services (AWS) security groups
- Devices administered using an SSH connection
- Multicloud Defense
- Hypershield

Licensing:

- CDO Base License: **CDO-SEC-SUB** (needed for each CDO tenant)
- CDO Device License: (e.g., *L-FPR**xxxx**-P-3Y*) per managed device [1]
- Security Analytics and Logging (SAL) On-prem: **SAL-OP-LT-1GB**
- Combined CDO Device License + SAL SKU: **CDO-ML-xxxx-LIC** [1]
- No license required for HA standby device

FAQs:

Q: Are there any scale limitations for device management?
A: CDO's cloud architecture allows it to scale to thousands of devices.

Q: When is a device Synced with Cisco Defense Orchestrator (CDO)?
A: Configuration can be pushed from CDO or pulled from a device with full conflict and out of band change detection.

Q: How can I connect a device which does not have a public IP address?
A: You can leverage CDO Secure Device Connector (SDC) which can be deployed within your network and doesn't need any outside port opened.

Resources:

CDO Ordering Guide
SAL Ordering Guide
CDO Data Sheet
What's new in CDO
CDO On-line Help
CDO Console Access
Multi-Tenant Portal
FAQ's
CDO Status
CDO Account (partner & PoV's)
Public page

Example SKU: ***CDO-SEC-SUB***

EXPIRED