Feature Highlights of 2022

This chapter describes some of the features that were added to Cisco Defense Orchestrator in 2022.

December 2022

December 15, 2022

Cisco Defense Orchestrator released an update to the cloud-delivered Firewall Management Center. Read the release notes for cloud-delivered Firewall Management Center to learn about new features included in the update.

December 1, 2022

Route Based Site-to-Site VPN Support for ASA

Using Cisco Defense Orchestrator, you can now create a site-to-site VPN tunnel between peers with Virtual Tunnel Interfaces configured. This supports route based VPN with IPsec profiles attached to the end of each tunnel. Any traffic routed into the IPSec tunnel is encrypted regardless of the source/destination subnet.

VTI-based VPNs can be created between:

- A CDO-managed ASA and any route-based VPN-capable device.
- Two CDO-managed ASAs.

See Site-to-Site Virtual Private Network for more information.

Global Search

The global search feature in CDO allows you to search for and navigate to devices managed by CDO. This feature now supports the search capability for devices that are managed in cloud-delivered Firewall Management Center from the CDO user interface. From the search results, you can navigate to the corresponding pages in cloud-delivered Firewall Management Center.

See Global Search for more information.

October 2022

October 27, 2022

Duo Admin Panel Onboarding and Multi-Factor Authentication Logging

CDO can now onboard the Duo Admin Panel and show the logs as MFA events in the dashboard and tabular forms. You can also export the MFA sessions of one or more devices to a file containing a comma-separated value (.csv).

The Duo Admin Panel records a Multi-Factor Authentication (MFA) log containing information on whether the user's two-factor authentication has passed or failed.

See "Onboard Duo Admin Panel" and "Monitor Multi-Factor Authentication Events" in Cisco Defense Orchestrator Guide for more information.

October 12, 2022

Policy-Based Site-to-Site VPN Wizard for ASA

CDO now allows configuring a policy-based site-to-site VPN tunnel between two peers. This means that any traffic routed into the IPSec tunnel is encrypted regardless of the source/destination subnet.

To configure a policy-based site-to-site VPN, one of the following conditions must be met:

- Both peers are CDO-managed ASAs.
- One of the peers is a CDO-managed ASA and the other is any policy-based VPN capable device.

See Site-to-Site Virtual Private Network for more information.

August 2022

August 4, 2022

CDO Support for FDM-Managed Devices, Version 7.2

CDO now supports version 7.2 for FDM-managed devices. These are the aspects of support CDO provides:

- Onboard a supported physical or virtual FDM-managed devices running version 7.2 to CDO.

- Upgrade FDM-managed devices from versions 6.4+ to version 7.2.
- Support for existing Secure Firewall Threat Defense features.
- Onboard a supported physical or virtual device running version 7.2 to cloud-delivered Firewall Management Center.

Note CDO does not support features introduced in the version 7.2 release.

June 2022

June 30, 2022

Cisco Secure Firewall Migration Tool Supports Migrations to Cisco Secure Firewall Threat Defense

The Secure Firewall migration tool allows you to migrate Secure Firewall ASA configurations to a Cisco Secure Firewall Threat Defense managed by either an on-prem or virtual Secure Firewall Management Center, or by our new cloud-delivered Firewall Management Center in Cisco Defense Orchestrator. The desktop tool also supports migrations from third-party vendors Check Point, Palo Alto Networks, and Fortinet.

Cisco Secure Firewall Migration Tool Version 3.0 supports migrations to a Secure Firewall Threat Defense device running threat defense software version 7.2. That version of threat defense can be managed by a cloud-delivered Firewall Management Center on CDO. The migration process is part of CDO and does not require any specific license other than the CDO license.

You can download the Secure Firewall Migration Tool from the Software Download page.

CDO provides a wizard to help you migrate the following elements of the ASA's running configuration to the threat defense template:

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

Once these elements of the ASA running configuration are migrated, you can deploy the configuration to a new threat defense device that is managed by cloud-delivered Firewall Management center on CDO.

For more information, see Migrating ASA Firewall to Cisco Secure Firewall Threat Defense with the Cisco Secure Firewall Migration Tool.

June 9, 2022

Managing Cisco Secure Firewall Threat Defense Devices with Cloud-Delivered Firewall Management Center

Cisco Defense Orchestrator (CDO) is now the platform for the cloud-delivered Firewall Management Center.

The cloud-delivered Firewall Management Center is a software-as-a-service (SaaS) product that manages Secure Firewall Threat Defense devices. It offers many of the same functions as an on-premises Secure Firewall Management Center, it has the same appearance and behavior as an on-premises Secure Firewall Management Center, and uses the same FMC API.

This product is designed for Secure Firewall Management Center customers who want to move from an on-premises version of the Secure Firewall Management Center to a SaaS version.

As a SaaS product, the CDO operations team is responsible for maintaining it. As new features are introduced, the CDO operations team updates CDO and the cloud-delivered Firewall Manager for you.

A migration wizard is available to help you migrate your Secure Firewall Threat Defense devices registered to your on-premises Secure Firewall Management Center to the cloud-delivered Firewall Management Center.

Onboarding Secure Firewall Threat Defense devices is carried out in CDO using familiar processes such as onboarding a device with its serial number or using a CLI command that includes a registration key. Once the device is onboarded, it is visible in both CDO and in the cloud-delivered Firewall Management Center, however, you configure the device in the cloud-delivered Firewall Management Center. Secure Firewall Threat Defense devices running Version 7.2 or later can be onboarded.

The license for cloud-delivered Firewall Management Center is a per-device-managed license and there is no license required for the cloud delivered FMC itself. Existing Secure Firewall Threat Defense devices re-use their existing smart licenses and new Secure Firewall Threat Defense devices provision new smart licenses for each feature implemented on the FTD.

In a remote branch office deployment, the data interface of the threat defense device is used for Cisco Defense Orchestrator management instead of the Management interface on the device. Because most remote branch offices only have a single internet connection, outside CDO access makes centralized management possible. In the case of remote branch deployment, CDO provides high availability support for the threat defense devices that it manages through the data interface.

You can analyze syslog events generated by your onboarded threat defense devices using Security Analytics and Logging (SaaS) or Security Analytics and Logging (On Premises). The SaaS version stores events in the cloud and you view the events in CDO. The on-premises version stores events in an on-premises Secure Network Analytics appliance and analysis is done in the on-premises Secure Firewall Management Center. In both cases, just as with an on-premises FMC today, you can still send logs to a log collector of your choice directly from the sensors.

The FTD dashboard provides you an at-a-glance view of the status, including events data collected and generated by all threat defense devices managed by the cloud-delivered Firewall Management Center. You can use this dashboard to view collective information that is related to the device status and the overall health of the devices in your deployment. The information that the FTD dashboard provides depends on how you license, configure, and deploy the devices in your system. The FTD dashboard displays data for all CDO-managed threat defense devices. However, you can choose to filter device-based data. You can also choose the time range to display for specific time range.

The Cisco Secure Dynamic Attributes Connector enables you to use service tags and categories from various cloud service platforms in cloud-delivered Firewall Management Center access control rules. Network constructs such as IP addresses may be ephemeral in virtual, cloud and container environments due to the dynamic nature of the workloads and the inevitability of IP address overlap. Customers require policy rules

to be defined based on non-network constructs such as VM name or security group, so that firewall policy is persistent even when the IP address or VLAN changes.

Proxy sequences of one or more managed devices can be used to communicate with an LDAP, Active Directory, or ISE/ISE-PIC servers. It is necessary only if Cisco Defense Orchestrator(CDO) cannot communicate with your Active Directory or ISE/ISE-PIC server. For example, CDO might be in a public cloud but Active Directory or ISE/ISE-PIC might be in a private cloud.

Although you can use one managed device as a proxy sequence, we strongly recommend you set up two or more so that, in the event one managed device cannot communicate with Active Directory or ISE/ISE-PIC, another managed device can take over.

Any customer can use CDO to manage other device types like, the Secure Firewall ASA, Meraki, Cisco IOS devices, Umbrella, and AWS virtual private clouds. If you use CDO to manage a Secure Firewall Threat Defense device configured for local management with Firepower Device Manager, you can continue to manage them with CDO as well. If you are new to CDO, you can manage Secure Firewall Threat Defense devices with the new cloud-delivered Firewall Management Center and all of the other device types as well.

Learn more about the Firewall Management Center features we support in the cloud-delivered Firewall Management Center.

- Health Monitoring
- Secure Firewall Threat Defense Device Backup/Restore
- Scheduling
- Import/Export
- External Alerting with Alert Responses
- Transparent or Routed Firewall mode
- High Availability for Secure Firewall Threat Defense Devices
- Interfaces
- Network Access Control (NAT)
- Static and Default Routes and other routing configurations
- Object Management and Certificates
- Remote Access VPN and Site to Site VPN configuration
- Access Control policies
- Cisco Secure Dynamic Attributes Connector
- Intrusion and Detection and Prevention policies
- Network Malware and Protection and File Policies
- Encrypted Traffic Handling
- User Identity
- FlexConfig Policies

Onboard an On-Prem management center with SecureX

If you have an on-prem management center that is already associated with your Securex account, you can onboard the management center to CDO through SecureX. Devices onboarded through SecureX experience the same amount of feature support and functionality as a management center onboarded through traditional methods. To onboard a management center to CDO through SecureX, see Onboard an On-Prem FMC with SecureX.

Note Even if your management center account is associated with SecureX, we strongly recommend merging your CDO account with SecureX before you attempt to onboard the management center. See Merge Your CDO and SecureX Accounts for more information.

May 2022

May 12, 2022

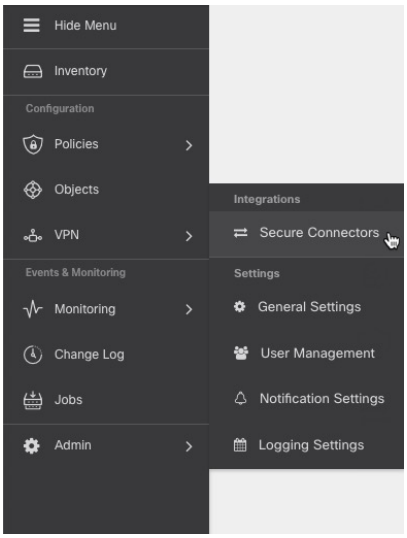
ASA Policy Support for IPv6

ASA access policies and NAT configurations now support rules that use network objects and network groups containing IPv6 addresses. In addition, these rules can also specify ICMP and ICMPv6 protocols. Finally, ASAs now support AnyConnect Connection Profiles containing IPv6 addresses. See ASA Network Policies for more information.

Navigation to the Secure Connectors Page

The Secure Connectors page is accessible from the CDO menu bar. To view the Secure Connectors page, choose **Admin** > **Secure Connectors**.

Figure 1: Secure Connectors Menu



April 2022

April 14, 2022

Monitor AWS VPC tunnels using AWS Transit Gateway

CDO can now monitor AWS VPC tunnels using AWS Transit Gateway. For more information, see Monitor AWS VPC tunnels using AWS Transit Gateway.

April 6, 2022

Global Search

Global search provides an option to search for all onboarded devices and associated objects available within CDO. The search results allow you to navigate to the corresponding device and object pages.

Currently, CDO supports global search for ASA, Firepower Management Center, Secure Firewall Threat Defense, and Meraki devices.

For more information, see "*Global Search*" in the following documents:

- Managing ASA with Cisco Defense Orchestrator
- Managing FMC with Cisco Defense Orchestrator
- Managing FTD with Cisco Defense Orchestrator
- Managing Meraki with Cisco Defense Orchestrator

Support for Cisco Secure Firewall 3100

Cisco Defense Orchestrator supports onboarding ASA and Secure Firewall Threat Defense devices running on new Cisco Secure Firewall 3100 Series devices.

Secure Firewall Threat Defense devices can be onboarded using Low Touch Provisioning or by using a registration key or serial number.

February 2022

February 03, 2022

Active Directory (AD) Groups in User Management

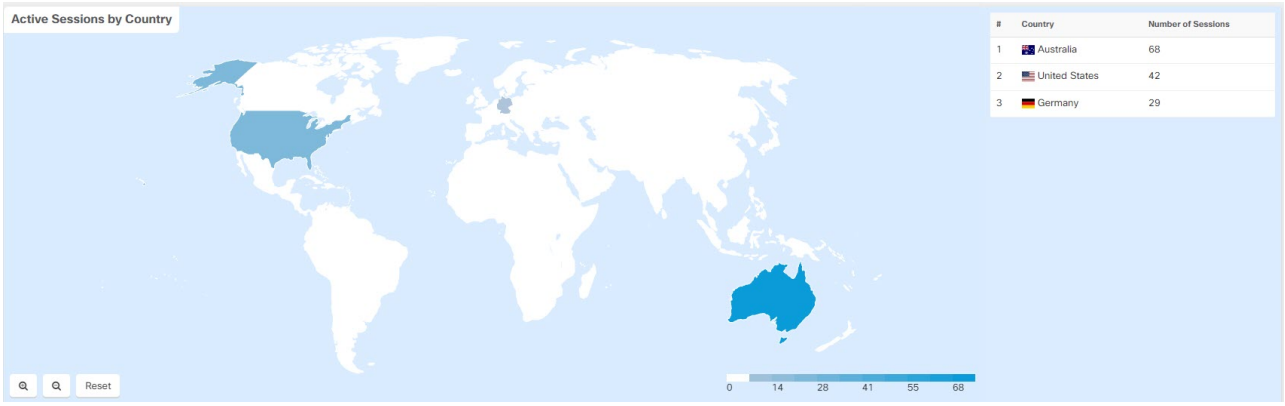
For an easier way to manage users in CDO, you can now map your Active Directory (AD) groups in CDO instead of managing individual users. Any user changes, such as a new user(s) addition, removing existing user(s), or changing roles can now be done in Active Directory without changing anything within CDO. CDO

now also supports multiple-roles per user with AD. For more information, see the "Active Directory Groups in User Management" section of the **User Management** chapter of you're device's configuration guide.

Improved Charts View for Active Remote Access VPN Sessions

CDO now provides a new and improved charts view for your active RA VPN sessions. In addition to the charts you are already familiar with, CDO now displays a heat map of the location of users connected to your RA VPN headends. This map is available only in the live view.

To view the new charts view, on the RA VPN Monitoring page, click the **Show Charts View** icon appearing at the top-right corner of the screen.



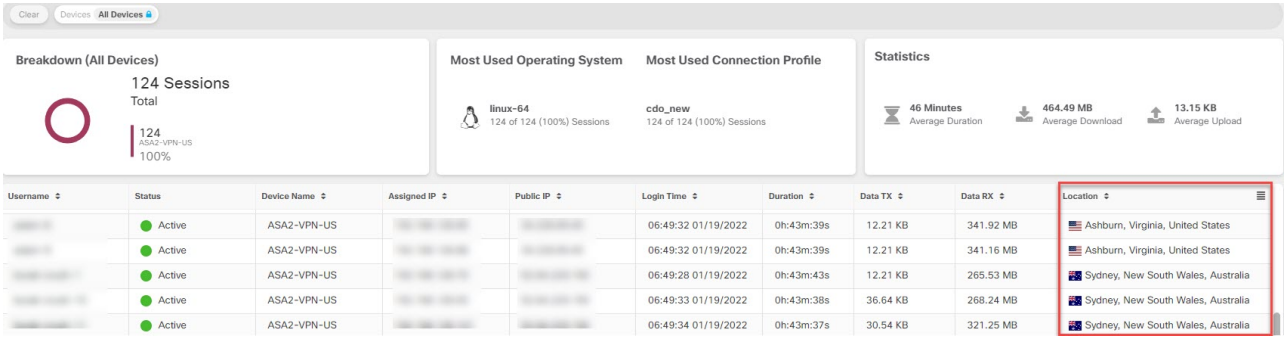
For more information, see "Monitoring Remote Access Virtual Private Network Sessions" in Managing FTD with Cisco Defense Orchestrator or Managing ASA with Cisco Defense Orchestrator depending on your firewall.

January 2022

January 20, 2022

Geolocation Information of Remote Access VPN Users

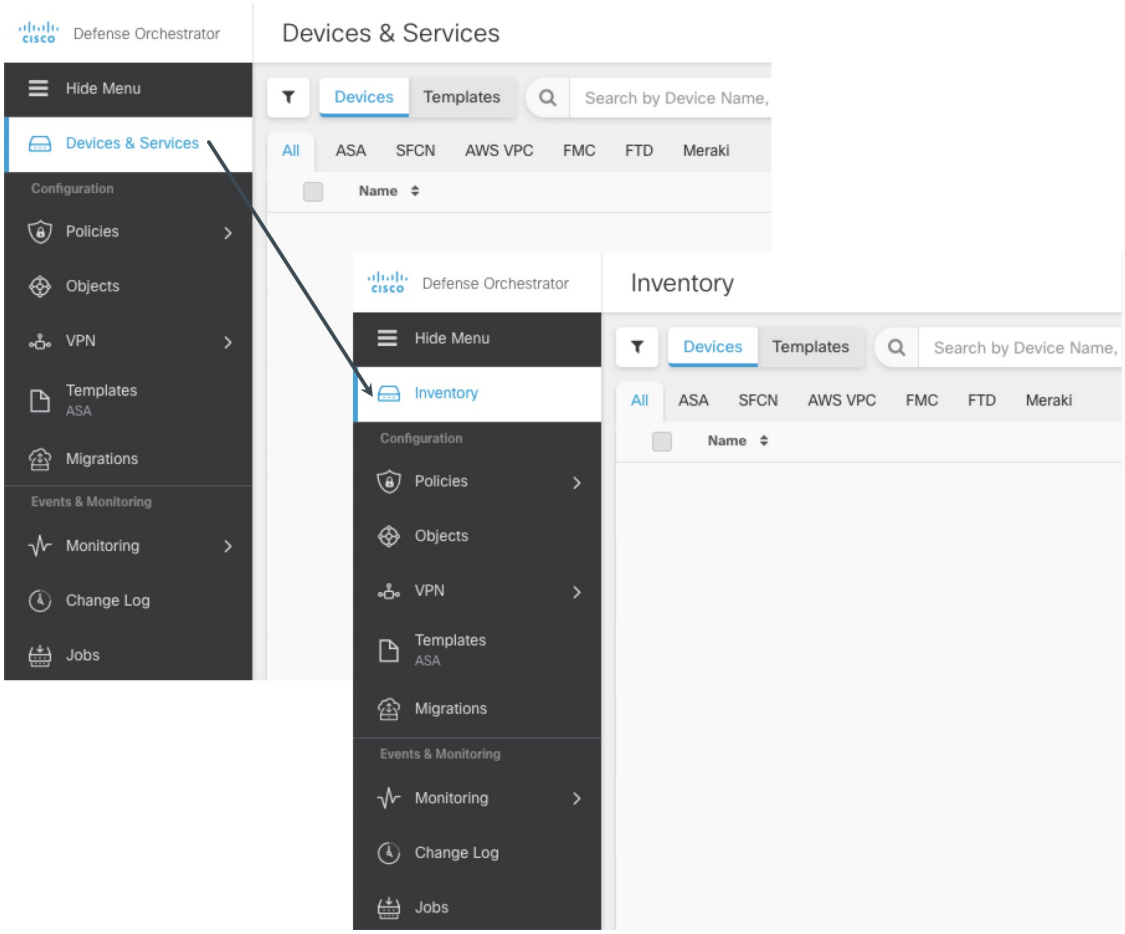
The remote access VPN monitoring page now shows the location of all users who are connected to the VPN headend. CDO obtains this information by geolocating the public IP addresses of the users. This information is available on live and historical views. On clicking the location in the **User Details** area in the left pane, the precise location of the user is shown on a map.



Note This information is available to user sessions that are established after the new CDO deployment and will not be available for existing user sessions.

Devices & Services Page Renamed to Inventory

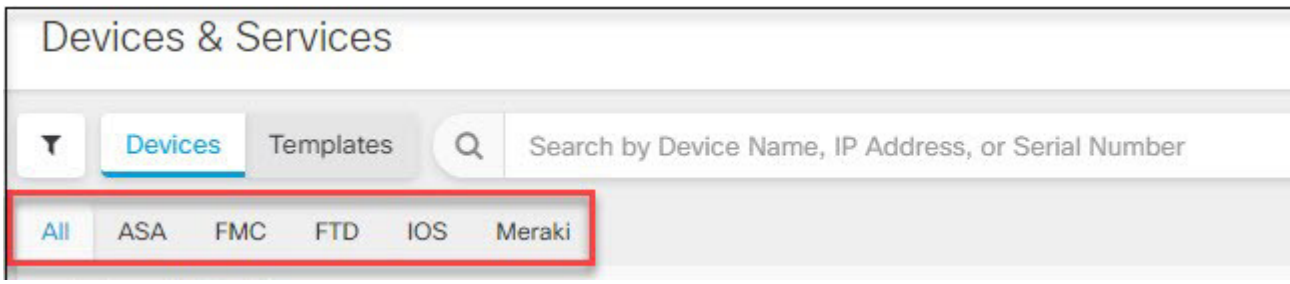
The Devices & Services page has been renamed, "Inventory." The Inventory table lists all the devices and services you manage with CDO. No features were added or removed as a result of the name change.



January 13, 2022

Enhanced Devices & Services Interface

The CDO **Devices & Services** interface now classifies devices and templates based on their type and displays them in the corresponding tabs dedicated to each device type.


Devices & Services
Devices
Templates
Search by Device Name, IP Address, or Serial Number
All
ASA
FMC
FTD
IOS
Meraki