Feature Highlights of 2023

This chapter describes some of the features that were added to Cisco Defense Orchestrator in 2023.

December 2023

December 14, 2023

Monitor Additional Event Types for Threat Defense Devices

CDO now supports new firewall event types such as AAA, BotNet, Failover, and SSL VPN for threat defense devices.

Navigate **Analytics** > **Event Logging** and filter from the new list of events available under **FTD Events**. See Event Types in CDO for more information.

December 07, 2023

Manage On-Prem Firewall Management Center Network Objects Using CDO

You can now manage and share network objects from a CDO-managed On-Prem Firewall Management Center to threat defense devices managed by other On-Prem Firewall Management Centers, the cloud-delivered Firewall Management Center, and to CDO-managed ASA and threat defense devices. This helps promote consistency in network object definitions across platforms managed by CDO.

After onboarding an On-Prem Firewall Management Center, navigate **Tools & Services** > **Firewall Management Center**, select the device and choose **Settings**, and enable the **Discover & Manage Network Objects** toggle button.

See Discover and Manage On-Prem Firewall Management Center Network Objects for more information.

November 2023

November 30, 2023

Schedule a Secure Firewall Threat Defense Device Backup in Cloud-delivered Firewall Management Center

Use the cloud-delivered Firewall Management Center to perform scheduled backups of the Secure Firewall Threat Defense devices it manages.

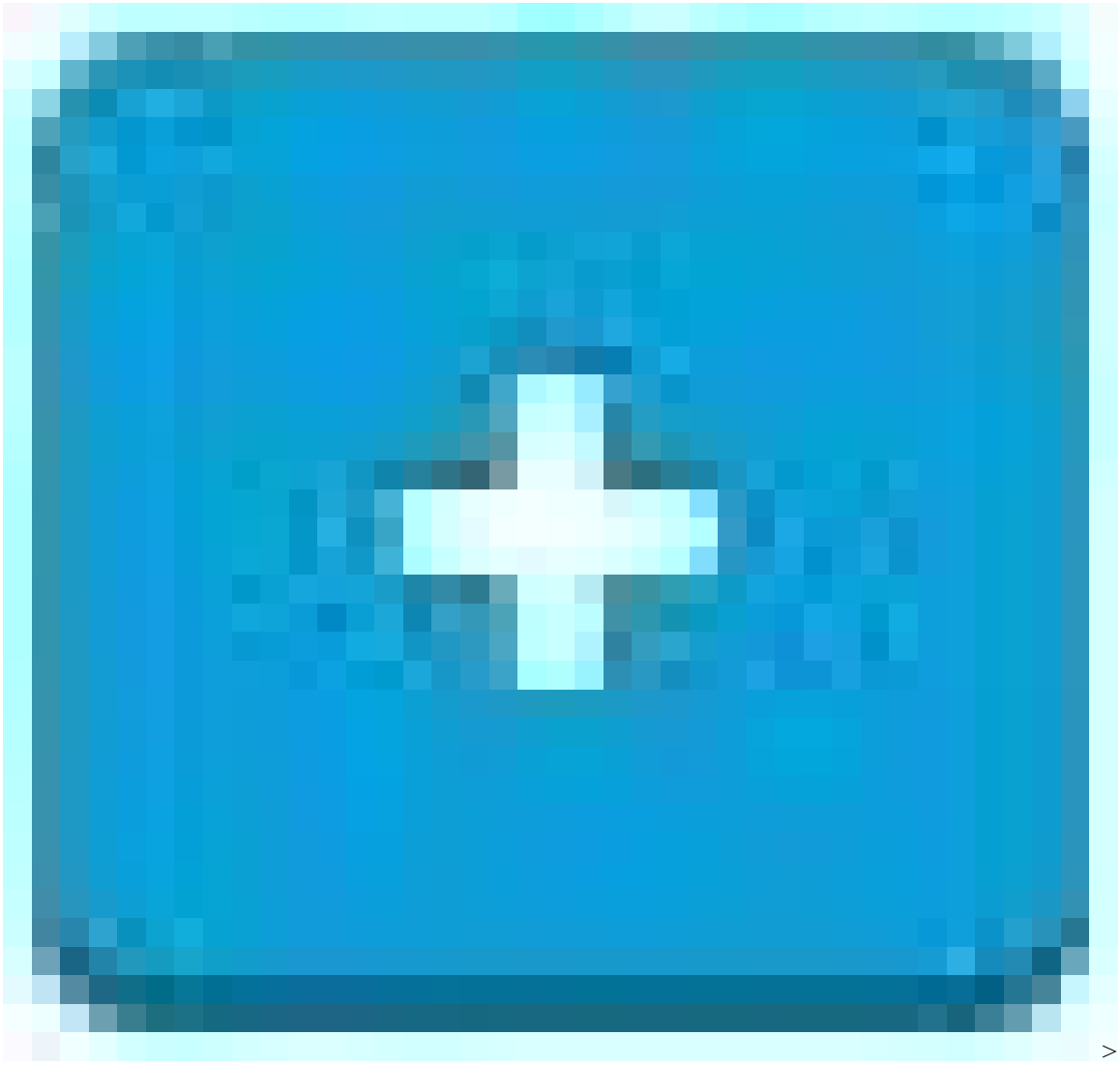
See Schedule Remote Device Backups for more information.

November 14, 2023

Improved Cloud-Delivered Firewall Management Center Provisioning

CDO now provides an enhanced, faster provisioning process for cloud-delivered Firewall Management Center. When you enable the cloud-delivered Firewall Management Center on your tenant, CDO provisions it automatically and notifies you through the CDO notifications center and the applications in which you have

configured incoming webhooks. To enable it, navigate **Tools & Services** > **Firewall Management Center** >



> **FMC** > **Enable Cloud-Delivered FMC**.

See Enable Cloud-delivered Firewall Management Center on Your CDO Tenant and Notification Settings for more information.

November 2, 2023

Onboard a Threat Defense Device to an On-Prem Management Center with Low-Touch Provisioning

You can now select an On-Prem Firewall Management Center as the managing platform when you onboard a threat defense device with the low-touch provisioning method. This supports on-prem management for new devices or devices that have not been previously configured or managed. See Onboard a Secure Firewall Threat Defense Device With Low-Touch Provisioning for more information.

October 2023

October 26, 2023

Updates to Firewall Migration Tool

CDO hosts an updated version of the Firewall Migration Tool. Using this, you can merge multiple transparent firewall-mode contexts that are present in your Secure Firewall ASA devices into a transparent-mode instance and migrate them.

In addition, you can migrate the site-to-site and remote access VPN configurations from your Fortinet and Palo Alto Networks firewalls to the threat defense devices managed by Cisco's cloud-delivered Firewall Management Center. See the Secure Firewall Migration Tool Release Notes for more information.

October 19, 2023

Updates to Cloud-Delivered Firewall Management Center

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 the many new features included in the update. See the Release Notes for Cloud-delivered Firewall Management Center: A Feature of Cisco Defense Orchestratorfor a complete list of the new features.

Migrate Secure Firewall Threat Defense Devices with Site-to-Site VPN Configurations from On-Prem to Cloud-Delivered Firewall Management Center

Site-to-site VPN configurations on Secure Firewall Threat Defense devices are now migrated along with the rest of the configuration when the device is migrated from the on-prem Firewall Management Center to the cloud-delivered Firewall Management Center. See Migrate On-Prem Management Center managed Secure Firewall Threat Defense to Cloud-delivered Firewall Management Center for more information.

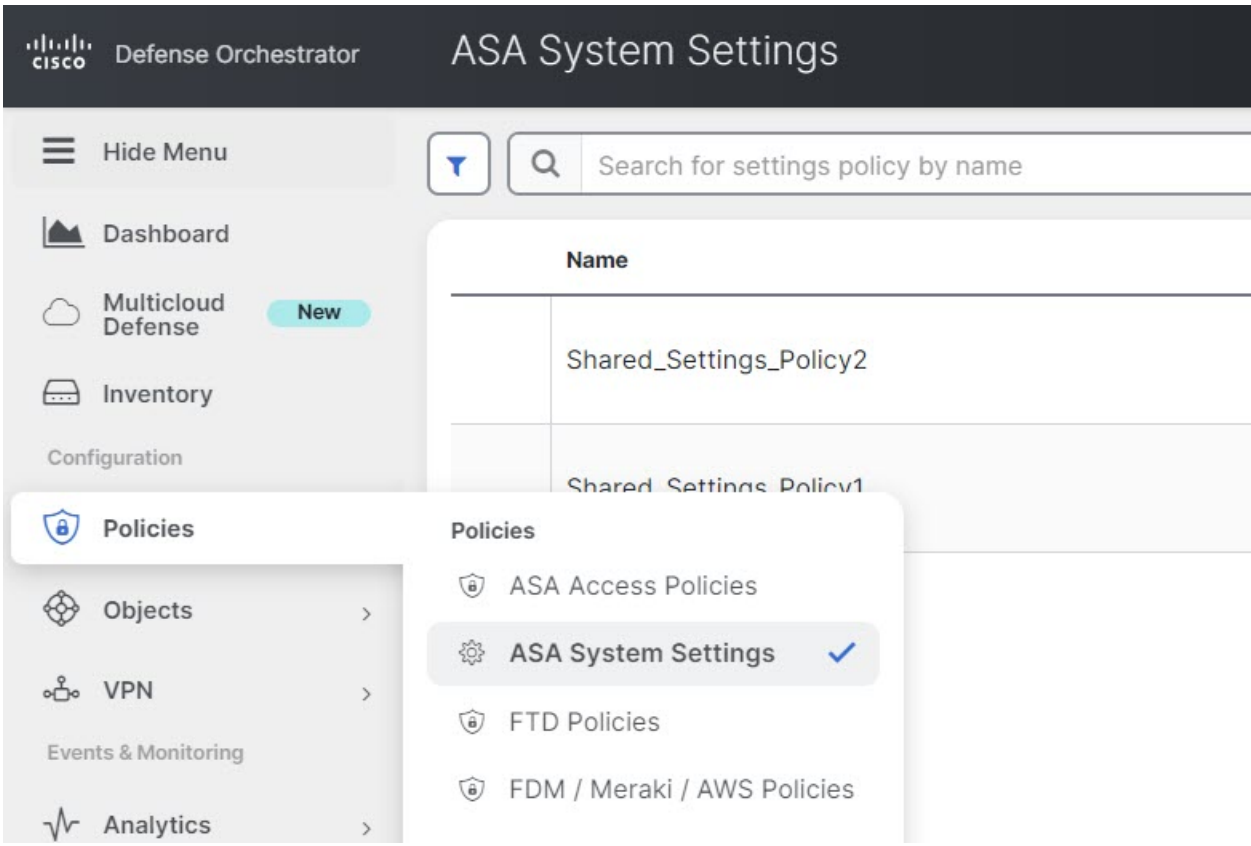
October 12, 2023

ASA System Settings Policy

CDO provides the ability to create a system settings policy to effortlessly manage essential configurations for ASA devices such as domain name services, HTTP, enabling the secure copy server, message logging, and allowing VPN traffic without checking access control lists. You can apply this policy to multiple ASA devices, and any change made to the policy affects all devices using this policy. Additionally, you can individually edit device-specific settings for a single ASA device and override the shared system settings with device-specific values.

See ASA System Settings for more information.

Choose **Policies** > **ASA System Settings**.



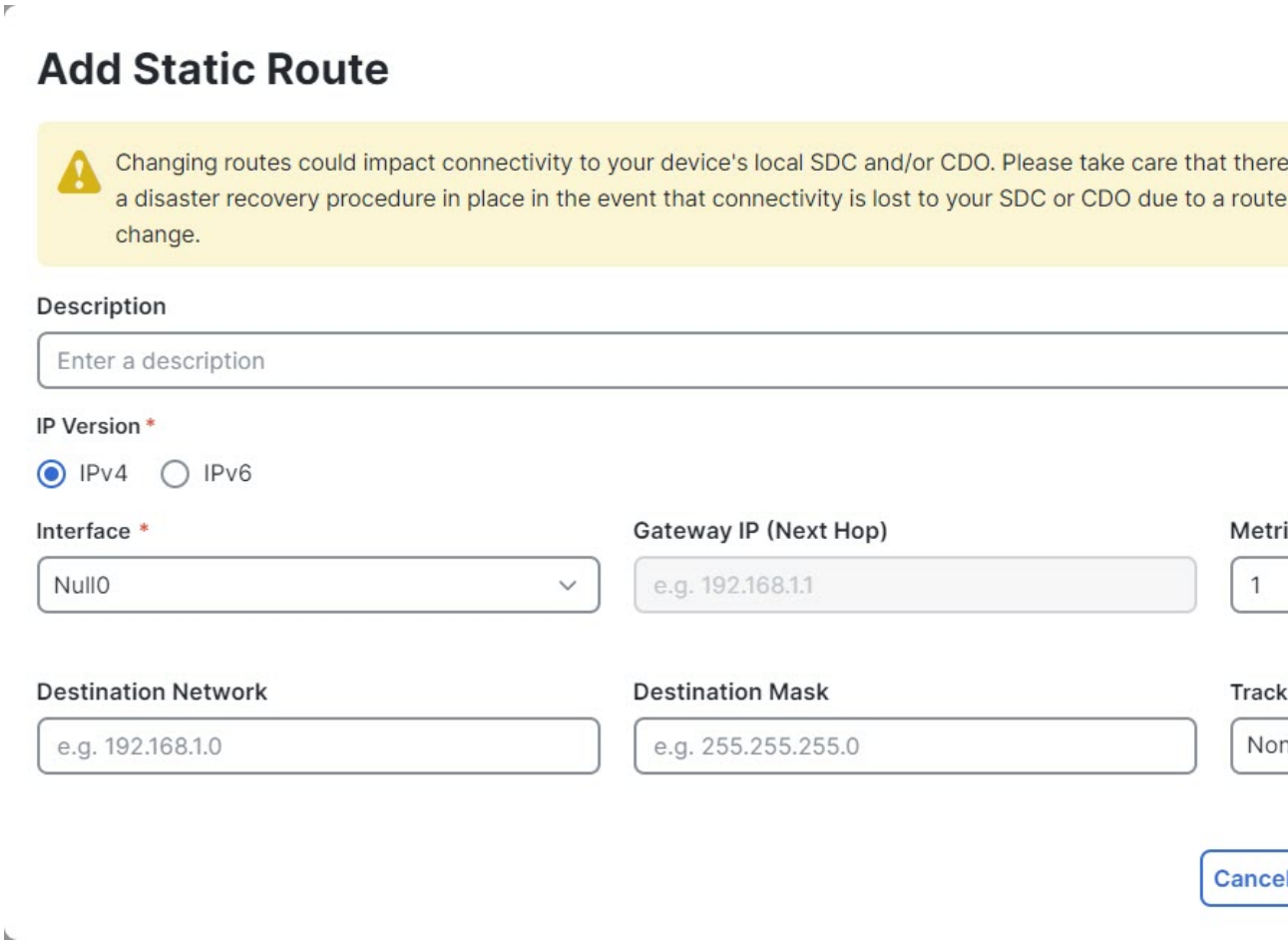
October 05, 2023

CDO Support for ASA Static Routing

You can now use the CDO user interface to configure static routes for the ASA. This feature lets you specify where to send traffic for specific IPv4 or IPv6 destination networks without having to use the CLI.

See ASA Static Routing for more information.

Inventory > **ASA** tab > **Routing**.



Manage CDO Using Terraform

You can now use Terraform to automate the management of your CDO infrastructure using Infrastructure as Code (IaC) principles. CDO now provides a Terraform provider and Terraform modules to quickly deploy secure device connectors and secure event connetors. See Terraform for more information.

September 2023

September 14, 2023

Navigation Change for Secure Event Connectors

You can no longer access the Secure Connectors page by expanding the admin menu in the top right. To manage Secure Connectors, navigate to **Tools & Services** > **Secure Connectors**. See Secure Event Connectors for more information.

September 7, 2023

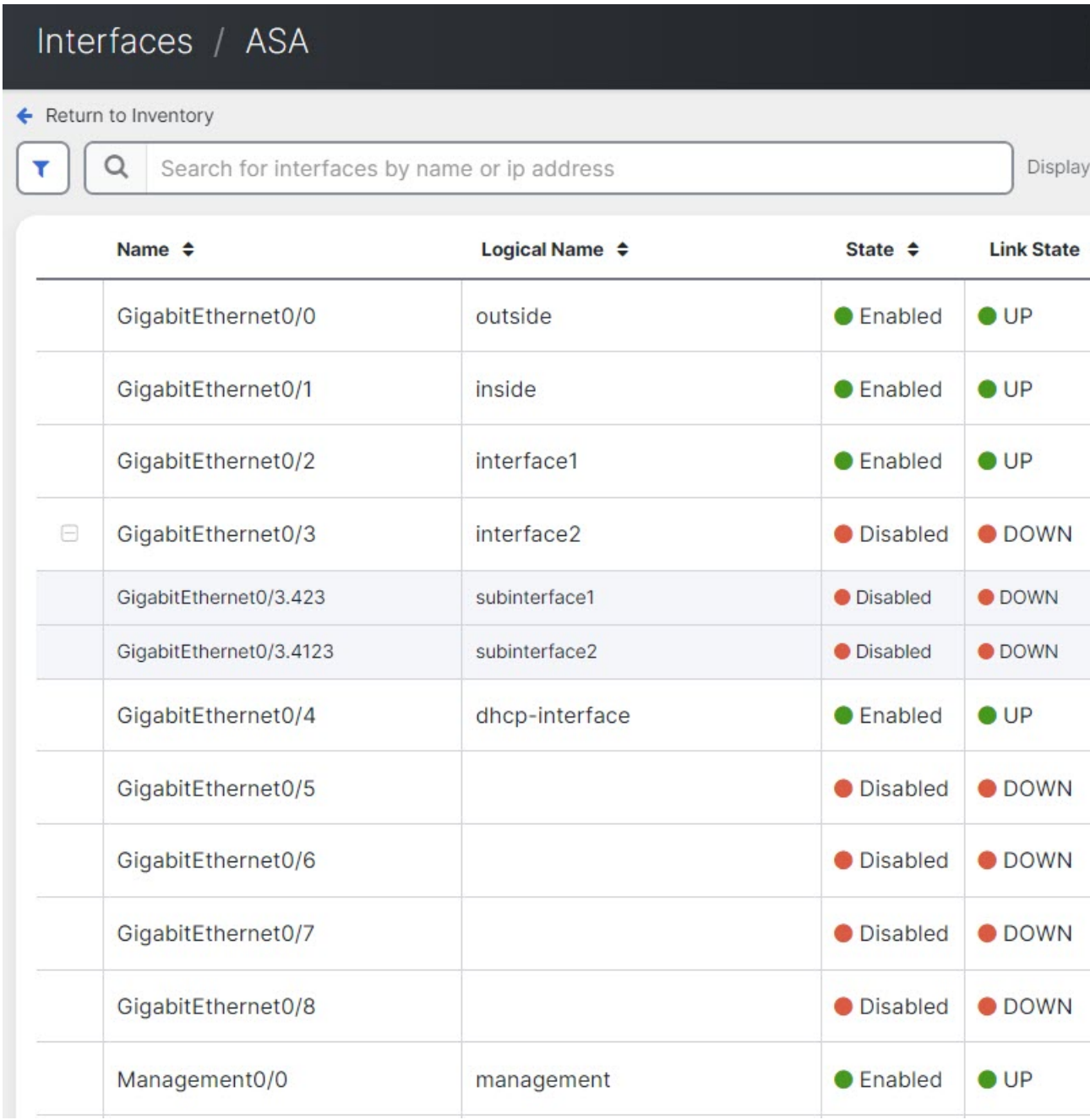
Configure ASA Interfaces using CDO User Interface

You can now configure ASA's physical network interfaces, logical subinterfaces, VLAN, and EtherChannels using a graphical user interface in CDO. You can also view Virtual Tunnel Interfaces that are created during route-based site-to-site VPN.

Note VLAN is only supported for 110 devices.

See Configure ASA Interfaces for more information.

Inventory > **ASA** > **Management** > **Interfaces**.

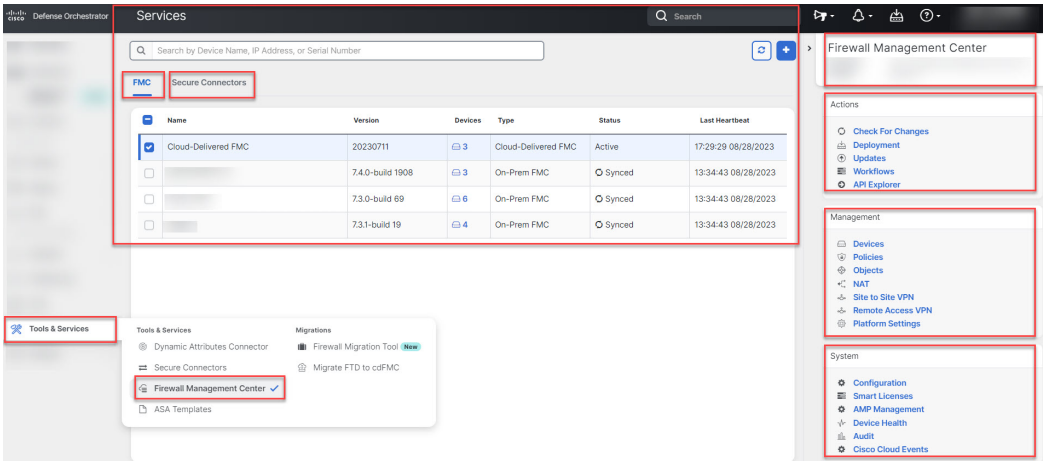

Interfaces / ASA
Return to Inventory
Search for interfaces by name or ip address
Display
Name
Logical Name
State
Link State
GigabitEthernet0/0
outside
Enabled
UP
GigabitEthernet0/1
inside
Enabled
UP
GigabitEthernet0/2
interface1
Enabled
UP
GigabitEthernet0/3
interface2
Disabled
DOWN
GigabitEthernet0/3.423
subinterface1
Disabled
DOWN
GigabitEthernet0/3.4123
subinterface2
Disabled
DOWN
GigabitEthernet0/4
dhcp-interface
Enabled
UP
GigabitEthernet0/5
Disabled
DOWN
GigabitEthernet0/6
Disabled
DOWN
GigabitEthernet0/7
Disabled
DOWN
GigabitEthernet0/8
Disabled
DOWN
Management0/0
management
Enabled
UP

August 2023

August 31, 2023

Manage Your Cloud-Delivered FMC, On-Prem FMCs, and Secure Connectors from the Services Page

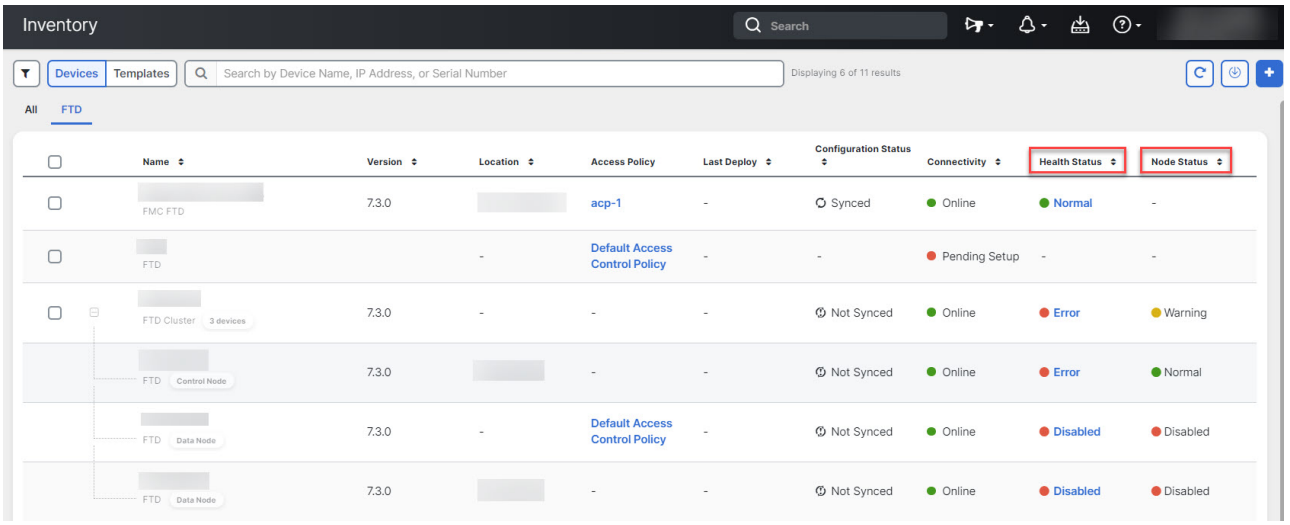
You can now manage your cloud-delivered Firewall Management Center, On-Prem Firewall Management Centers, and secure connectors from the new **Services** page. Choose **Tools & Services** > **Firewall Management Center** or **Secure Connectors**. Refer View Services Page Information to know more.



August 17, 2023

Know the Health Status of Your Threat Defense Devices

CDO now displays the health and node status for threat defense devices on the Inventory page. For more details about the device health, you can click on the health status of a device to navigate to the device's health monitoring page in the cloud-delivered Firewall Management Center or the On-Prem Firewall Management Center user interface. Note that node status is displayed only for threat defense devices managed by cloud-delivered Firewall Management Center.



For more information, see Managing On-Prem FMC with Cisco Defense Orchestrator and Managing Cisco Secure Firewall Threat Defense Devices with Cloud-delivered Firewall Management Center.

August 3, 2023

Updates to Firewall Migration Tool

Cisco Defense Orchestrator now hosts an updated version of the Firewall Migration Tool. You can now merge multiple contexts in your Secure Firewall ASA devices to a routed-mode instance and migrate them to threat defense devices managed by the cloud-delivered Firewall Management Center. In addition, the migration tool now leverages the virtual routing and forwarding (VRF) functionality to replicate the segregated traffic flow observed in a multi-context ASA environment, which will be part of the new merged configuration.

See Migrating Secure Firewall ASA Managed by CDO in *Migrating Firewalls with the Firewall Migration Tool in Cisco Defense Orchestrator* guide for more information.

July 2023

July 20, 2023

EasyDeploy for Virtual Threat Defense Devices Managed by GCP

You can now create a virtual threat defense device and deploy it to a Google Cloud Platform (GCP) project simultaneously. The EasyDeploy method combines the steps required to create a new virtual device and then associating the device with the cloud environment, streamlining the procedure and minimizing the amount of time required for setup.

Note that you **must** have cloud-delivered Firewall Management Center enabled for these onboarding flows. See Deploy a Threat Defense Device to Google Cloud Platform for more information.

July 13, 2023

Open CDO and Cloud-delivered Firewall Management Center Portals on Different Browser Tabs

You can now open CDO and cloud-delivered Firewall Management Center portal pages in different browser tabs and simultaneously work in both CDO and cloud-delivered Firewall Management Center.

See Support to Open CDO and Cloud-delivered Firewall Management Center Applications on Different Tabs for more information.

June 2023

June 29, 2023

Schedule a Background Search in the Event Viewer

You can now run a background search in the Event Viewer on a re-occurring schedule. The schedule supports absolute time (ex May 1 to May 5th) or a sliding window (ex "The last day").

See Schedule a Background Search in the Event Viewer for more information.

Support for New Event Attributes

Now, Security Group, Encrypted Visibility Process Confidence Score, Encrypted Visibility Threat Confidence, Encrypted Visibility Threat Confidence Score, Encrypted Visibility Fingerprint are supported syslog event attributes in CDO's event viewer. When you customize your event logging view you can create a column for any of these newly supported attributes.

June 15, 2023

Migrate Your Firewalls using the Firewall Migration Tool in CDO

You can now migrate configurations from your Secure Firewall ASA devices, FDM-managed threat defense devices, and third-party firewalls such as Check Point, Palo Alto Networks, and Fortinet firewalls to the cloud-delivered Firewall Management Center using the Firewall Migration Tool in Cisco Defense Orchestrator. See Migrating Firewalls with the Firewall Migration Tool in Cisco Defense Orchestrator guide for more information.

June 8, 2023

EasyDeploy for Virtual Threat Defense Devices Managed by AWS and Azure

You can now create a virtual threat defense device and deploy it to an Amazon Web Services (AWS) or Azure environment simultaneously. The easydeploy method combines the steps required to create a new virtual device and then associating the device with the cloud environment, streamlining the procedure and minimizing the amount of time required for setup.

Note that you **must** have cloud-delivered Firewall Management Center enabled for these onboarding flows. See Deploy a Threat Defense Device with AWS and Deploy a Threat Defense Device with an Azure VNet respectively for more information.

June 5, 2023

CDO Introduces the Multicloud Defense Solution

Multicloud Defense Solution specializes in security policy orchestration and protection of cloud network traffic, and cloud applications and workloads. It delivers unified security policies and web protection across multiple cloud types, provides network visibility into your cloud assets, and integrates services like threat intelligence and external logging. It enforces ingress traffic to, and egress traffic from, your cloud account, as well as the "east-west" network traffic within your cloud account.

Multicloud Defense Solution currently supports AWS, Azure, Google Cloud Platform, and Oracle OCI cloud accounts.

See About Multicloud Defense for more information, and Multicloud Defense 90-Day Free Trial to try out the Multicloud Defense Solution.

June 1, 2023

Auto Discovery of On-Prem Secure Firewall Management Centers with SecureXIntegration

CDO now has the ability to onboard all the on-prem management centers associated with the SecureX tenant that is linked to your CDO account. It also onboards the Secure Firewall Threat Defense devices linked to those on-prem management centers. See Auto Onboard an On-Prem Firewall Management Center with SecureX for more information.

April 2023

April 27, 2023

Improved Event Filtering

You can now filter events further with a relative time range. Absolute time range is an explicitly stated time frame. An example of a relative time range is `last 3 days` or `last 3 hours`. This can help target traffic and events that may not necessarily be included in an absolute time range. See Search for Events in the Events Logging Page for more information.

March 2023

March 23, 2023

Background Search for Event Logging

CDO provides you the ability to define a search criteria and search for events in event logs based on any defined search criteria. Using the background search capability, you can perform event log searches in the background, and view the search results once the background search is completed.

Based on the subscription alert and service integrations you have configured, you can be notified once the background search has been completed. Learn more about background searches used with event logging.

January 2023

January 18, 2023

Monitor Remote Access VPN Sessions of FTDs

CDO can now monitor Remote Access VPN sessions of FTDs managed using the cloud-delivered Firewall Management Center in CDO.

The RA VPN monitoring page provides the following information:

- A list of active and historical sessions.
- The details of the device and user associated with each session.