New Features in 2024

This chapter describes some of the features that were added to Cisco Defense Orchestrator in 2024.

November 2024

Welcome to Security Cloud Control

Cisco Defense Orchestrator is now "Cisco Security Cloud Control."

Security Cloud Control is a new, AI-embedded management solution designed to unify the Cisco Security Cloud, starting with network security. It is a modern micro-app architecture with an updated user interface, common services, and a service-mesh that connects configuration, logs, and alerts across the security cloud.

It manages Secure Firewall Threat Defense and ASA firewalls, Multicloud Defense, and Hypershield with the intent to expand these management capabilities to additional security products. In addition, AI assistants proactively optimize policy and configuration, and find and troubleshoot issues.

Explore these new Security Cloud Control features:

- Centralized management experience of network security solutions
- A guided “Day 0” experience helping you to quickly onboard threat defense devices and discover new features
- Unified dashboard for end-to-end visibility of all of your managed devices
- Upgraded menu navigation and easy network and security application access for streamlined solution usability

- AI Assistant for ease of firewall rule creation and management
- Simplified operations and enhanced security with AIOps insights
- Policy analysis to improve security posture, eliminate misconfiguration, and optimize rules.
- Strengthened protection in hybrid environments with consistent policy enforcement and object sharing
- Improved monitoring of remote access and site-to-site VPN connections
- Increased scalability to support up to 1000 firewalls with a single tenant

For more information, see the Security Cloud Control product page, the Security Cloud Control documentation, and the FAQ.

November 7, 2024

Updates to Firewall Migration Tool

Cisco Security Cloud Control (formerly Cisco Defense Orchestrator) released an updated version of the Firewall Migration Tool. You can now perform bulk update of preshared keys for site-to-site VPN configurations, choose to continue or abort the migration when the configuration being migrated has an error-containing parameter, add your target threat defense device as a spoke to an existing hub and spoke VPN configuration, and do much more. See the Cisco Secure Firewall Migration Tool Release Notes for a list of features included in the release.

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 more.

October 2024

October 17, 2024

Tenant Creation in the Multi-Tenant Portal

You can now create tenants, add users, and enable cloud-delivered Firewall Management Center and Multicloud Defense in the provisioned tenants.

For more information, see Manage Multi-Tenant Portal.

September 2024

September 13, 2024

Analyze and Optimize Security Policies Using Policy Analyzer and Optimizer

You can now use the new Policy Analyzer and Optimizer to analyze your policies, detect anomalies, and receive curated remediation recommendations. Applying these recommendations ensures that your policies are always in an optimal state, which enhances firewall performance. This tool can analyze policies in both cloud-delivered Firewall Management Center and CDO-managed On-Premises Firewall Management Centers, version 7.2 or later. On the left pane, choose **Insights** > **Policy Analyzer and Optimizer**.

See Analyzing, Detecting, and Fixing Policy Anomalies Using Policy Analyzer and Optimizer for more information.

September 5, 2024

Updates to Firewall Migration Tool

You can now configure a threat defense high availability (HA) pair on the migration tool when migrating configurations from a Secure Firewall ASA HA pair to a threat defense device. In addition, you can configure a site-to-site hub and spoke VPN topology when migrating site-to-site VPN configurations from a Secure Firewall ASA.

See Cisco Secure Firewall Migration Tool Release Notes for more information.

Onboard a Secure Firewall Threat Defense 3100, 4100, 4200, or 9300 Chassis Using Cisco Defense Orchestrator

You can now add a Firepower 3100, 4100, 4200, or 9300 chassis to the cloud-delivered Firewall Management Center through Cisco Defense Orchestrator.

The management center and the chassis share a separate management connection using the chassis MGMT interface. The management center offers chassis-level health alerts. For configuring 4100 or 9300, you still need to use the Secure Firewall chassis manager or FXOS CLI. For 3100 or 4200, you can use the chassis management interface within the cloud-delivered Firewall Management Center. See Onboard a Chassis for more information.

August 2024

August 23, 2024

Updates to Cloud-delivered Firewall Management Center

Cisco Defense Orchestrator released an update to the cloud-delivered Firewall Management Center. Here are the highlights of the update! Read the Release Notes for Cloud-delivered Firewall Management Center to learn more.

Platform

- Threat defense Version 7.6.0 support

High Availability/Scalability

- Multi-instance mode for the Secure Firewall 3100

Access Control: Threat Detection and Application Identification

- Bypass decryption for sensitive and undecryptable traffic

Access Control: Identity

- Microsoft Azure AD as a user identity source

Health Monitoring

- Collect health data without alerting
- Chassis-level health alerts for the Firepower 4100/9300

Administration

- Threat defense high availability automatically resumes after restoring from backup.
- Change management ticket takeover; more features in the approval workflow.

Troubleshooting

- Troubleshoot Snort 3 performance issues with a CPU and rule profiler.

Management Center REST API

- Updates to management center REST API.

August 8, 2024

Generic Text Dynamic Attributes Connector Support

A Generic Text Dynamic Attributes Connector, allows you to maintain a list of IP addresses in a text file and then enforce an access control policy using that list. For example, you could use the list of IP addresses in an "allow list" or a "block list" in an access control rule. Periodically, after the text file containing the IP addresses is updated, Cisco Secure Dynamic Attribute Connector updates any access control rules that use that IP address list. You can specify up to 10,000 IP addresses per text file. See "Creating a Generic Text " for more information.

VPN Tunnel Support for Multicloud Defense

You can now create a VPN tunnel in Multicloud Defense with a Multicloud Defense Gateway as one endpoint and a managed device or a cloud service provider such as GCP as the other endpoint. See Multicloud Defense User Guide for more information.

Enhanced Audit Logs in CDO

Audit Logs now display user-related and system-level actions, including User Login, Tenant Association and Disassociation, User Role Change, and Active Directory Group modifications.

For more information, see Audit Logs.

June 2024

June 27, 2024

Upgraded ASA Access Control Policy Interface

CDO now introduces an upgraded ASA access control policy interface featuring enhanced shared access lists, simplified rule management, and enhanced search result navigation.

See Manage ASA Network Security Policy for more information.

June 20, 2024

Added toggle buttons for UTC and local time zones on the CDO **Event Logging** page. With this update, the events generated by your device will now be displayed with timestamps in either the local time zone or UTC, depending on your selection. By default, event timestamps are now displayed in your Local time zone.

For more information, see Change the Time Zone for the Event Timestamps.

June 13, 2024

New Threat Defense Dashboard Widgets for Application Monitoring

CDO now features four new dashboard widgets: **Top Web Applications**, **Top Client Applications**, **Top Blocked Web Applications**, and **Top Users by Blocked Connections**. These new widgets provide you with an at-a-glance view of the most used web and client applications as well as the users with the most blocked connections. Note that the information the threat defense dashboard provides depends on how you license, configure, and deploy the devices in your system. Click **Analytics** > **FTD Dashboard** to view the new dashboard widgets.

See About the FTD Dashboard for more information.

Pause Threat Defense to Cloud-delivered Firewall Management Center Migration to Review Imported Shared Policies

You can now pause the threat defense to the cloud-delivered Firewall Management Center migration process to review the imported shared policy configuration. At this stage, neither the evaluation period is initiated, nor the threat defense's manager is changed, which provides you time to review the configurations. After reviewing the configuration, you can resume the migration process to import the device-specific configuration to the cloud-delivered Firewall Management Center during the scheduled migration period. Click **Tools & Services > Migrate FTD to cdFMC**.

See Threat Defense to Cloud-delivered Firewall Management Center Migration for more information.

June 6, 2024

Firewall Management with Cisco AI Assistant

CDO administrators now have a more efficient way to manage Secure Firewall Threat Defense policies and access documentation with the integration of the Cisco AI Assistant in Cisco Defense Orchestrator (CDO) and cloud-delivered Firewall Management Center. The Cisco AI Assistant has several key features:

- **Pre-Enabled Assistant**: The AI Assistant is enabled by default on every CDO tenant. If needed, you can disable it on the General Settings page of your tenant.
- **Easy Access**: CDO Super Admins and Admin can access the AI Assistant directly from the top menu bar of their tenant's dashboard after logging in.

- **User Orientation**: Upon opening the AI Assistant widget for the first time, users are greeted with a carousel window that introduces the AI Assistant, explains data privacy protections, and provides tips on effective usage.
- **Policy Rule Assistance**: The AI Assistant simplifies the process of creating policy rules on Secure Firewall Threat Defense devices. Administrators can quickly create access control rules using simple prompts.
- **Product Knowledge Resource**: The AI Assistant has ingested CDO's and the cloud-delivered Firewall Management's documentation. If you need help, you can ask it a question.
- **User-Friendly Interface**:
  - **Simple Text Input Box**: Located at the bottom of the window for easy engagement with the Assistant.
  - **Thread History**: The questions, or series of questions, you ask the AI Assistant are called threads. The AI Assistant retains your thread history so you can refer to the questions you've asked.
  - **Feedback**: Provide feedback on the Assistant's responses with thumbs up or thumbs down.

See the Cisco AI Assistant User Guide for more information.

May 2024

May 30, 2024

CDO in India!

CDO is now available in India at https://in.cdo.cisco.com. You can create yourself a tenant in India by going to https://www.getcdo.com.

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.

May 23, 2024

CDO in Australia!

CDO is now available in Australia at https://aus.cdo.cisco.com. You can create yourself a tenant in Australia by going to https://www.getcdo.com.

CDO API

CDO now offers a RESTful API that allows you to programmatically interact with CDO. The API provides access to a wide range of CDO features, including device management and deployment, object management, searches, changelog monitoring, and user management. Learn more by reading the Cisco Defense Orchestrator API Documentation. You can also reach the CDO API documentation by navigating from the user menu located in the top right corner of your CDO tenant.

Note The CDO GraphQL API is no longer supported or available.

Updates to Firewall Migration Tool

CDO now hosts an updated version of the Firewall Migration Tool. You can now optimize network and port objects before migrating them from a Secure Firewall ASA device to a threat defense device. In addition, you can migrate DHCP, DDNS, and SNMPv3 configurations from an FDM-managed device to a threat defense device.

To know more about the other new features, refer to the Cisco Secure Firewall Migration Tool Release Notes.

CDO Tenant Notifications and User Notification Preferences Relocation

The tab for notifications and user preferences have moved. Notifications, now located in the navigation bar located to the left with **Settings** > **Notification Settings**, allow you to manage email subscriptions and third-party service integrations. User Preferences, now located **Username ID** > **Preferences** > **Notification Preferences**, can be configured to trigger whenever a device associated with your tenant experiences a specific action, a device certificate is expiring or has expired, or a background log search starts, finishes or fails. Note that **User Notification Preferences** are unique to each individual user whereas **Tenant Notifications** are applied to every user affiliated with the tenant. See Tenant Management for more information.

Device Certificate Expiry Notification

CDO now monitors the expiration status of the Cisco Secure Client (formerly AnyConnect) certificate, and the management certificate of ASA, FDM-Managed, and FTD devices. It notifies the user when these certificates are nearing their expiration date or have expired.

See Device Certificate Expiry Notification.

May 16, 2024

Cisco Security Cloud Control support for Multicloud Defense

The Cisco Security Cloud Control enterprise now supports adding an existing Multicloud Defense account; you can add a Multicloud Defense tile to your Security Cloud enterprise dashboard to monitor and centralize your management of other Cisco product instances, user identity, and user access management across Cisco Security Cloud portfolio. See Multicloud Defense in Cisco Security Cloud Control in the Multicloud Defense User Guide for more information.

April 2024

April 25, 2024

Dark Theme in CDO

CDO now offers a Dark theme option for a more customizable user interface look. Click the admin drop-down on the top right corner, navigate to **Preferences** > **General Preferences**, and click **Dark** in the **Theme** field. The default theme is the **Light** theme.

See User Settings for more information.

April 18, 2024

Automatically Synchronize Network Objects to On-Prem Secure Firewall Management Centers

You can now automatically and continuously synchronize your network objects in CDO to On-Prem FMCs managed by CDO. Note that this feature is disabled by default. To enable this feature, navigate to **Tools & Services > Firewall Management Center**, select an On-Prem FMC, choose **Settings** in the Actions pane, click **Discover and Manage Network Objects**, and **click Enable automatic sync of network objects**. Ensure you have the Discover and Manage Network Objects toggle enabled.

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

March 2024

March 07, 2024

Improved CDO Tenant Provisioning

You can now create a CDO tenant using an enhanced, faster provisioning process. You can also create new CDO tenants even if you already have tenants. In addition, if you have an On-Premises Firewall Management Center that is not SecureX-enabled, you can now register it to the Cisco Security Cloud through CDO. If you do not have a CDO account, you can create one during the registration process. See Create a CDO Tenant for more information.

Disable Individual Threat Defense Devices From Sending Event Logs to the Cisco Cloud

You can now disable individual cloud-delivered Firewall Management Center-managed threat defense devices (Version 7.4.1 or later) from sending event logs to the Cisco cloud. This device-level control allows you to temporarily stop threat defense devices from sending event logs sent to the cloud, if required. To specify which threat defense devices are to be disabled from sending event logs to the Cisco cloud, click **Inventory**, select the corresponding threat defense devices, and click **Cloud Events** from the **Device Management** pane.

Simplified Secure Device Connector and Secure Event Connector Installation on Ubuntu

You can now easily deploy Secure Device Connector and Secure Event Connector on Ubuntu server using the GitHub project available on the Cisco DevNet site. For more information, refer to this document and watch this video on YouTube.

February 2024

February 13, 2024

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.

January 2024

January 25, 2024

Updates to Firewall Migration Tool

CDO now hosts an updated version of the Firewall Migration Tool. You can now migrate WebVPN configurations from your Secure Firewall ASA devices to Zero Trust Access Policy configurations on threat defense devices managed by the cloud-delivered Firewall Management Center. You can also migrate SNMP, DHCP, DVTI configurations from ASAs to threat defense devices and ECMP routing configurations when migrating from a multi-context ASA device to a single-instance threat defense device. Read the Cisco Secure Firewall Migration Tool Release Notes to know about the other new features included in the release.

January 25, 2024