What's New for Security Cloud Control

First Published: 2021-04-16

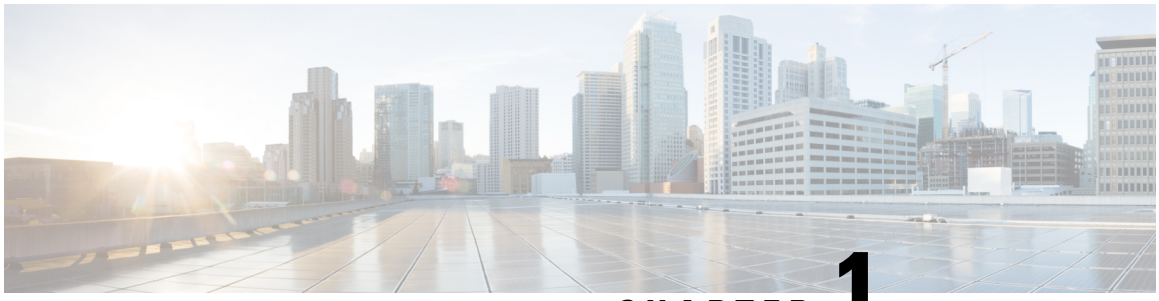
Last Modified: 2024-11-08

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

PART I

New Features in Security Cloud Control



CHAPTER 1

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.

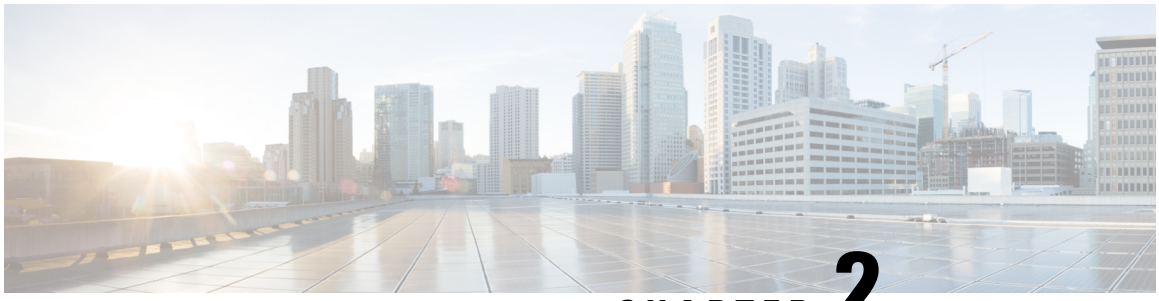
January 2024

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



CHAPTER 2

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-Premises Firewall Management Center Network Objects Using CDO

You can now manage and share network objects from a CDO-managed On-Premises Firewall Management Center to threat defense devices managed by other On-Premises 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-Premises 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.

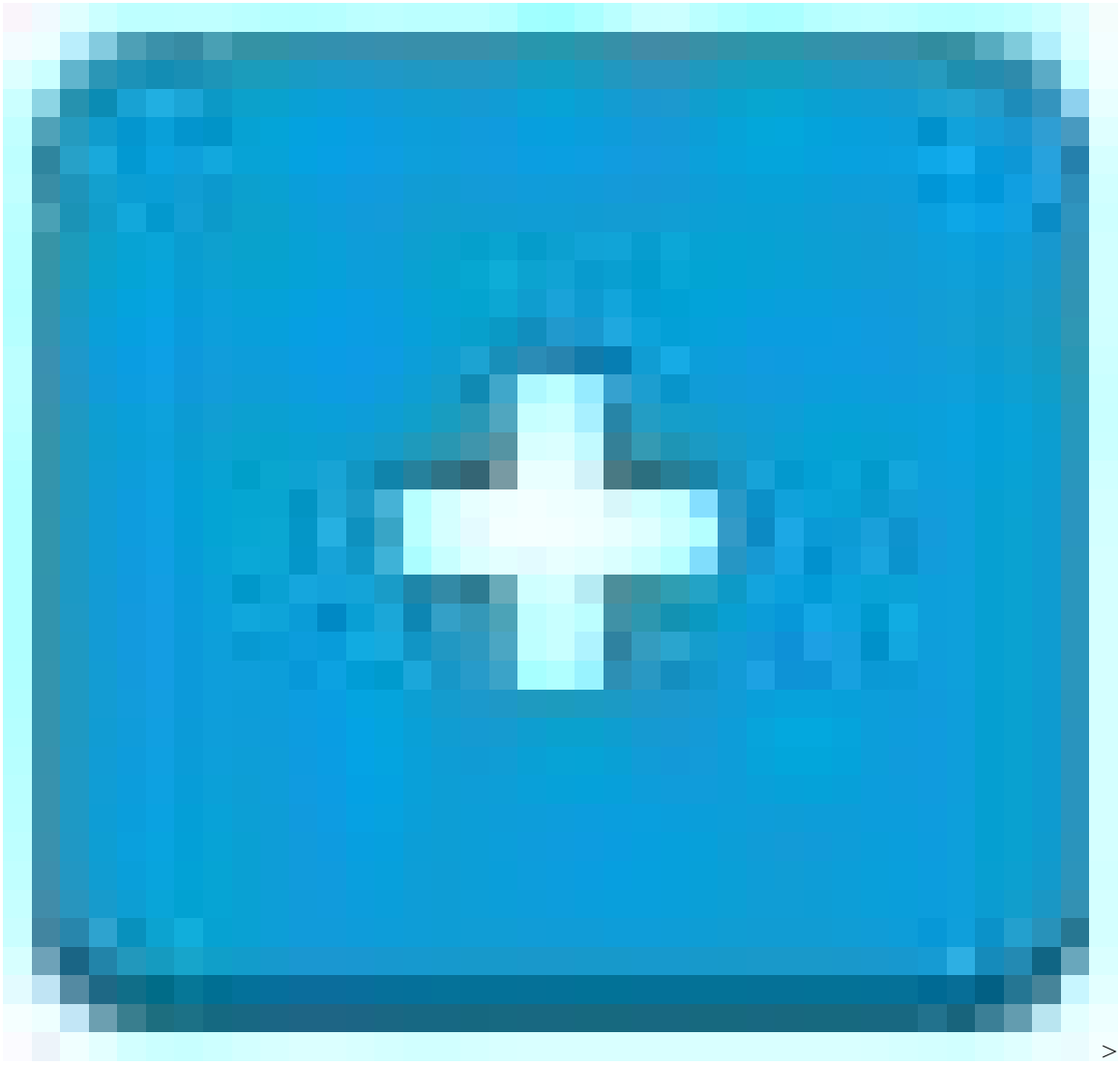
See Schedule Remote Device Backups for more information.

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 Zero-Touch Provisioning

You can now select an On-Premises Firewall Management Center as the managing platform when you onboard a threat defense device with the zero-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 Zero-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.

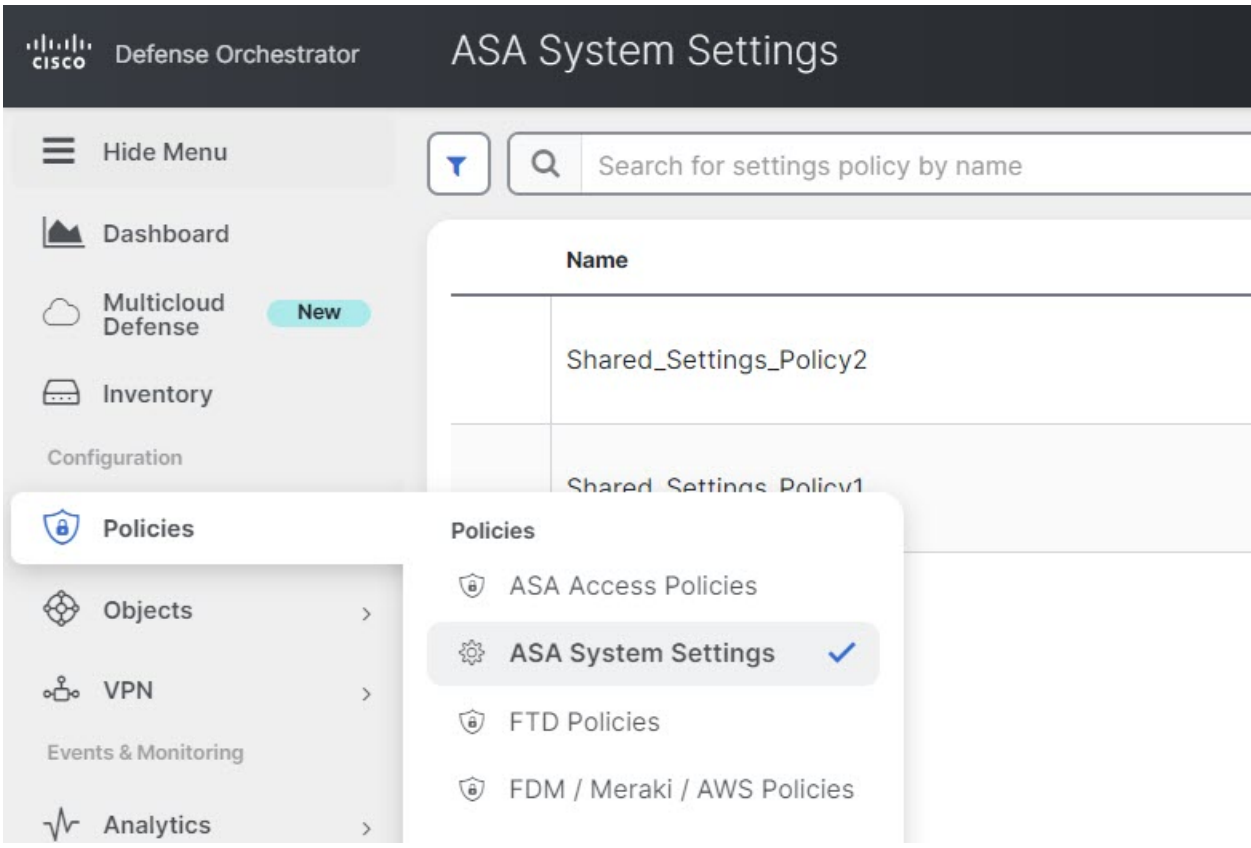
October 12, 2023

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**.



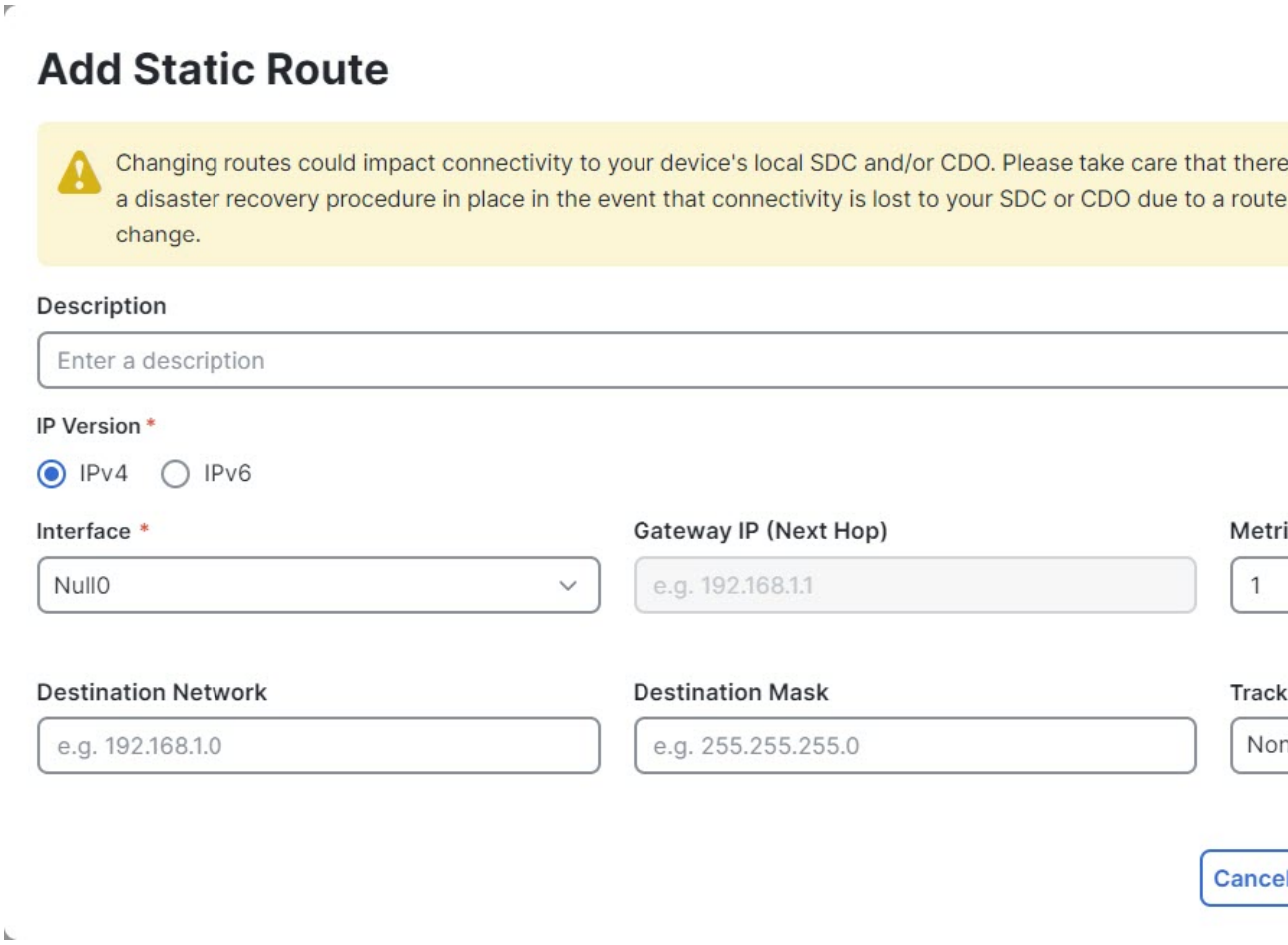
October 05, 2023

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

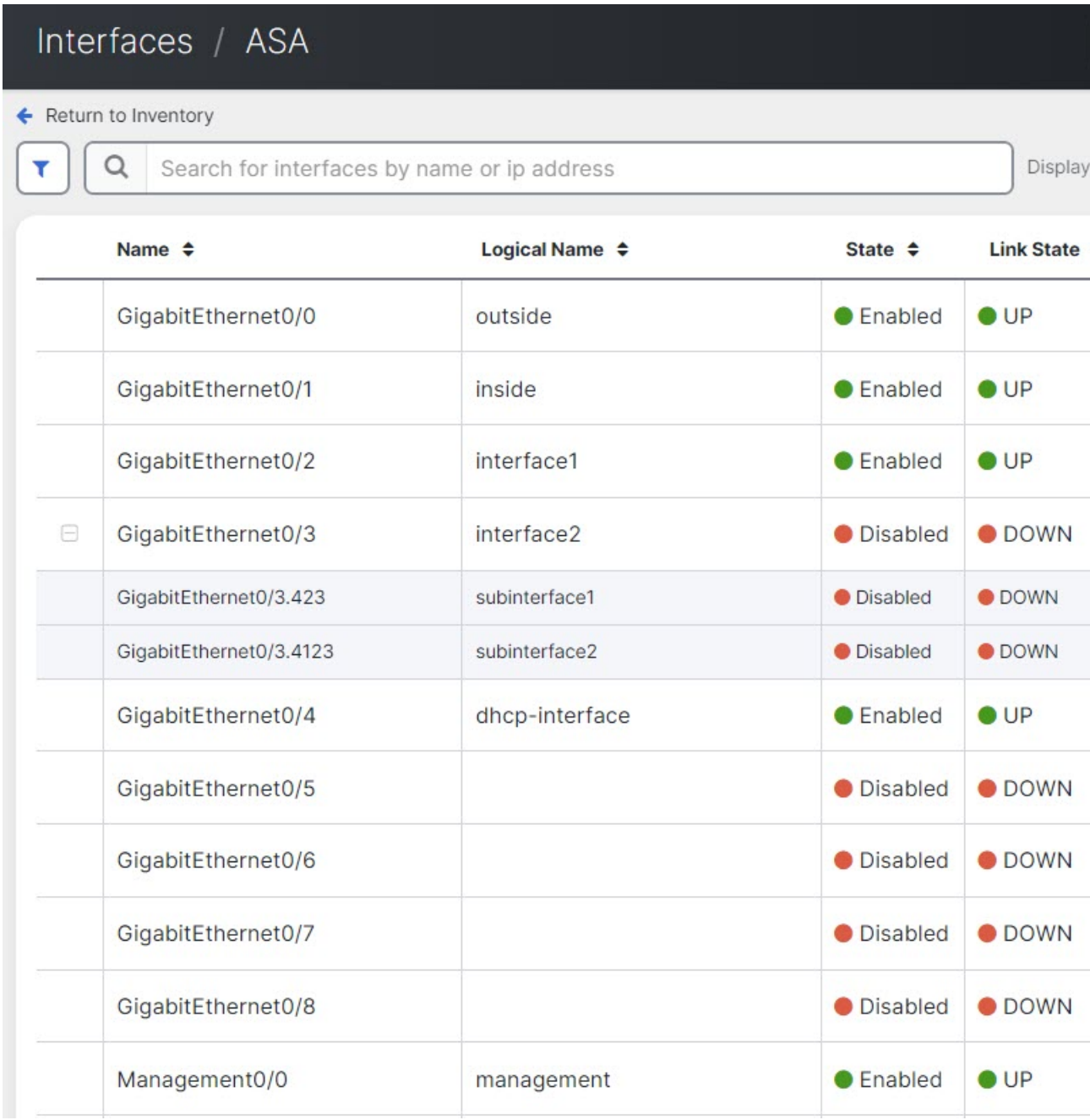
Configure ASA Interfaces using CDO User Interface

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**.

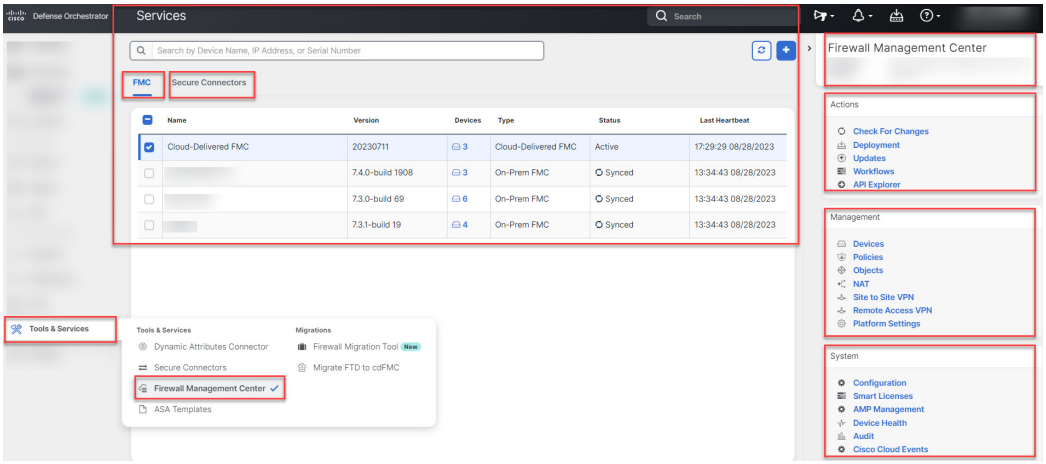

Interfaces / ASA
Return to Inventory
Search for interfaces by name or ip address
Display
Name
Logical Name
State
Link State
GigabitEthernet0/0
outside
Enabled
UP
GigabitEthernet0/1
inside
Enabled
UP
GigabitEthernet0/2
interface1
Enabled
UP
GigabitEthernet0/3
interface2
Disabled
DOWN
GigabitEthernet0/3.423
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

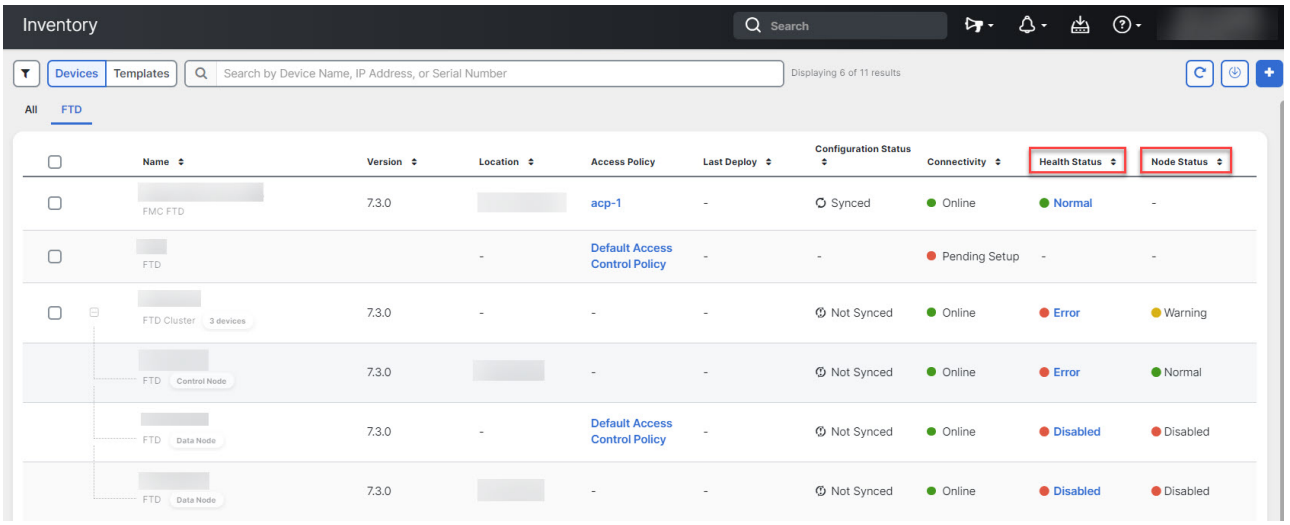
You can now manage your cloud-delivered Firewall Management Center, On-Prem Firewall Management Centers, and secure connectors from the new **Services** page. Choose **Tools & Services** > **Firewall Management Center** or **Secure Connectors**. Refer View Services Page Information to know more.



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-premises 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-premises 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

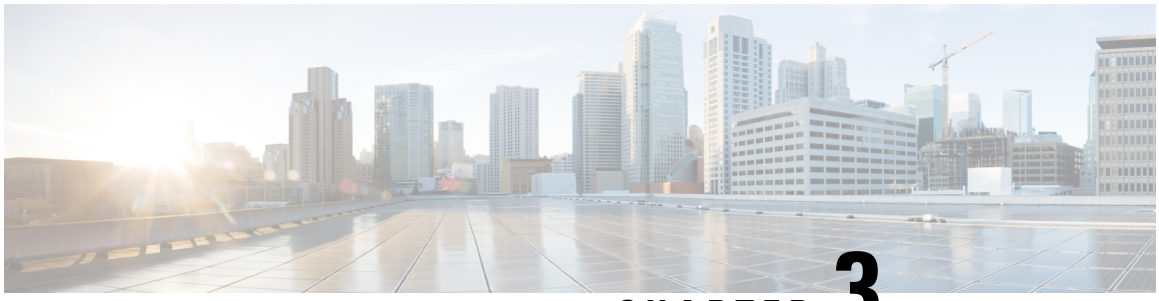
Monitor Remote Access VPN Sessions of FTDs

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.

January 18, 2023



CHAPTER 3

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

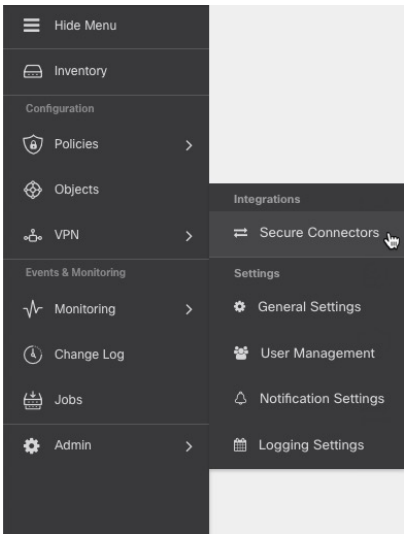
ASA Policy Support for IPv6

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 Zero-Touch Provisioning or by using a registration key or serial number.

February 2022

February 03, 2022

Active Directory (AD) Groups in User Management

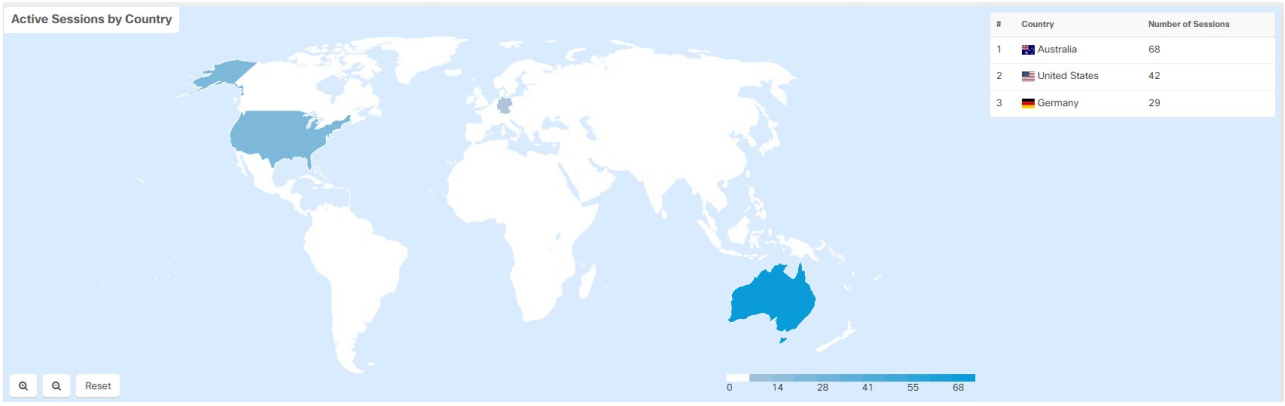
For an easier way to manage users in CDO, you can now map your Active Directory (AD) groups in CDO instead of managing individual users. Any user changes, such as a new user(s) addition, removing existing user(s), or changing roles can now be done in Active Directory without changing anything within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



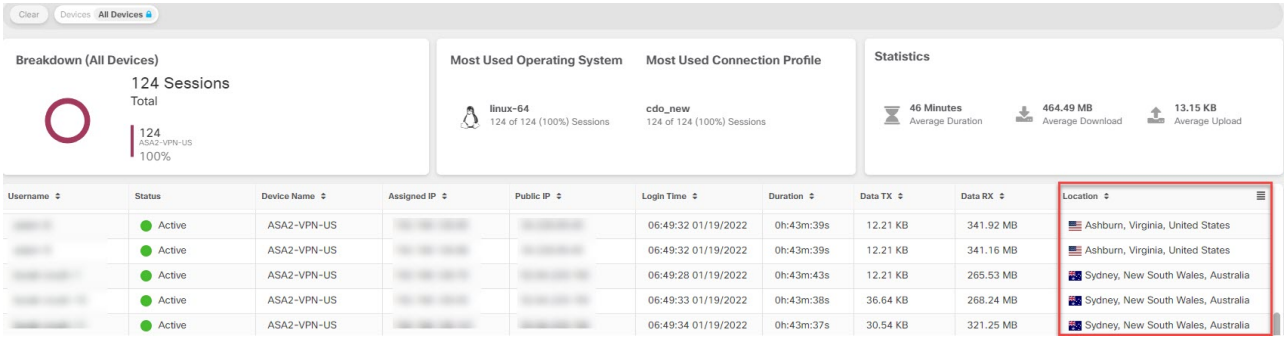
For more information, see "Monitoring Remote Access Virtual Private Network Sessions" in Managing FTD with Cisco Defense Orchestrator or Managing ASA with Cisco Defense Orchestrator depending on your firewall.

January 2022

January 20, 2022

Geolocation Information of Remote Access VPN Users

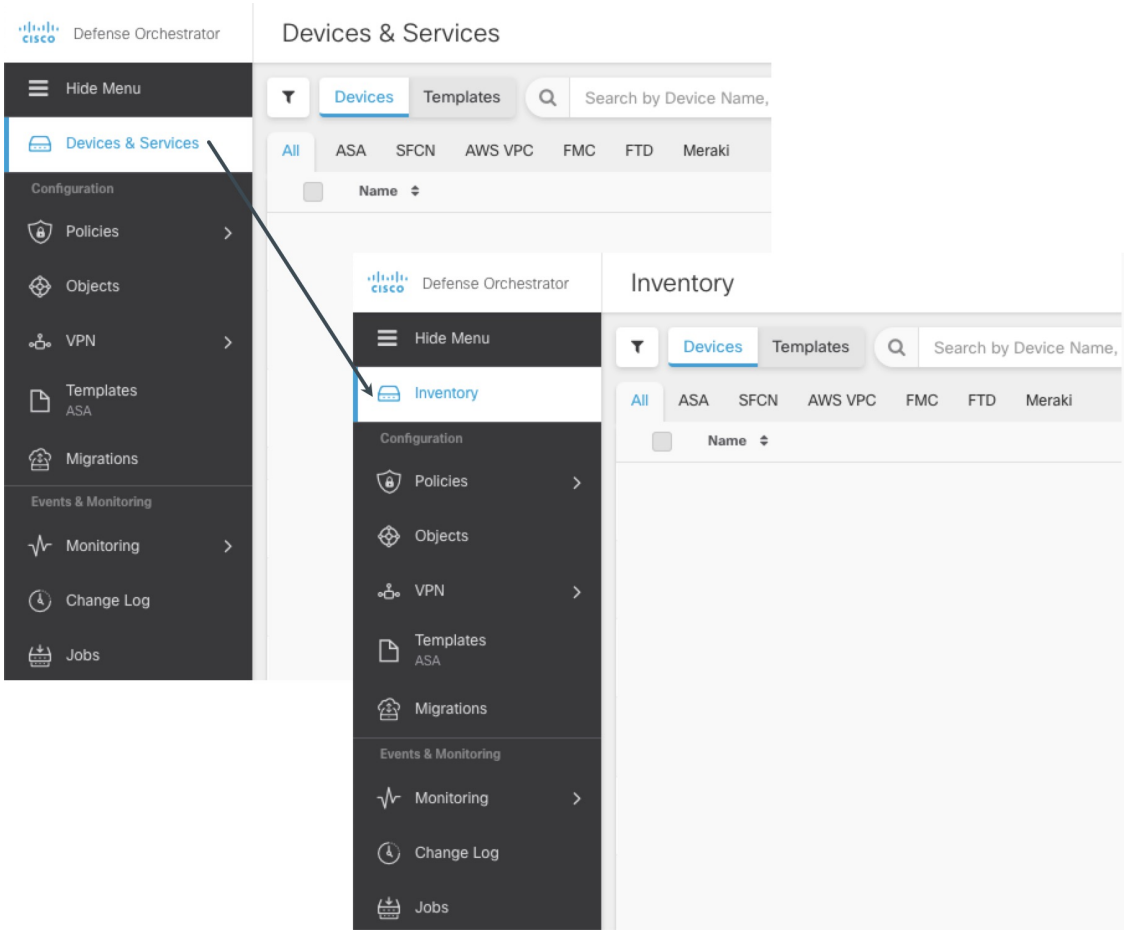
The remote access VPN monitoring page now shows the location of all users who are connected to the VPN headend. CDO obtains this information by geolocating the public IP addresses of the users. This information is available on live and historical views. On clicking the location in the **User Details**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

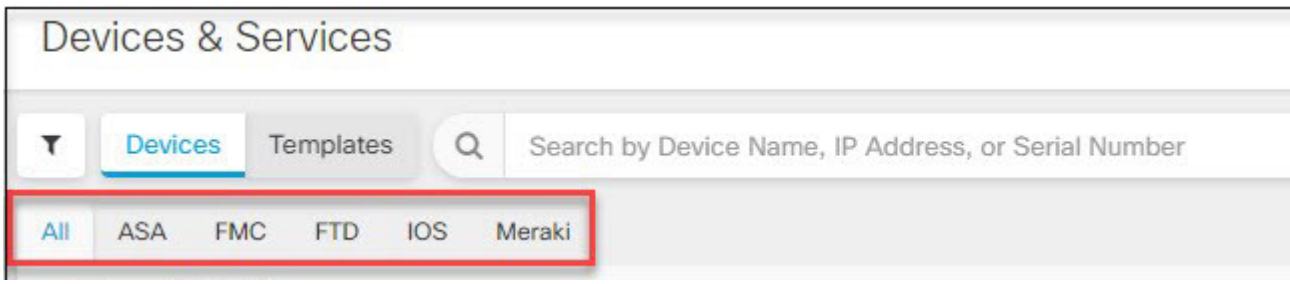
The Devices & Services page has been renamed, "Inventory." The Inventory table lists all the devices and services you manage with CDO. No features were added or removed as a result of the name change.



January 13, 2022

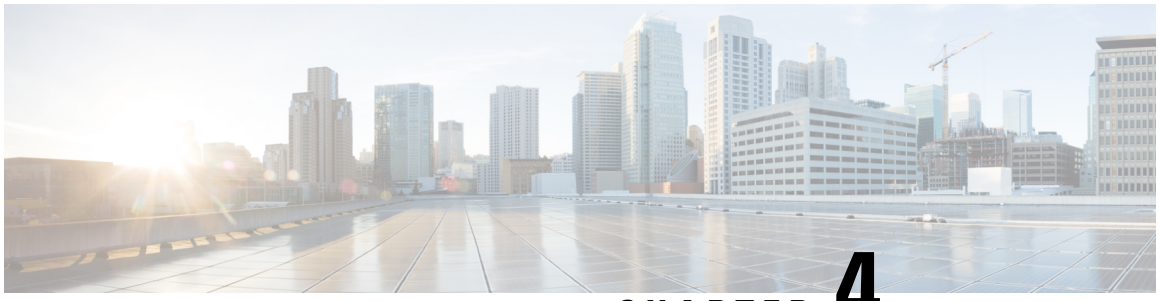
Enhanced Devices & Services Interface

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

PART II

New Features in Cloud-Delivered Firewall Management Center



CHAPTER 4

New Features in Cloud-delivered Firewall Management Center 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 8, 2024

Table 1: Features in Version 20241030

Feature	Minimum Threat Defense	Details
Platform		
Secure Firewall 1200.	7.6.0	We introduced the Secure Firewall 1200, which includes these models: • Secure Firewall 1210CX, with 8x1000BASE-T ports • Secure Firewall 1210CP, with 8x1000BASE-T ports. Ports 1/5-1/8 support power over Ethernet (PoE). • Secure Firewall 1220CX, with 8x1000BASE-T ports and two SFP+ ports. See: Cisco Secure Firewall CSF-1210CE, CSF-1210CP, and CSF-1220CX Hardware Installation Guide
Disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200.	7.6.0	You can now disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200. By default, the port is enabled. New/modified threat defense CLI commands: **system support usb show**, **system support usb port disable**, **system support usb port enable** New/modified FXOS CLI commands for the Secure Firewall 3100 in multi-instance mode: **show usb-port**, **disable USB port**, **enable usb-port** See: Cisco Secure Firewall Threat Defense Command Reference and Cisco Firepower 4100/9300 FXOS Command Reference
Device Management		

Feature	Minimum Threat Defense	Details
Device templates.	7.4.1	Device templates allow you to deploy multiple branch devices with pre-provisioned initial device configurations (zero-touch provisioning). You can also apply configuration changes to multiple devices with different interface configurations, and clone configuration parameters from existing devices. Restrictions: You can use device templates to configure a device as a spoke in a site-to-site VPN topology, but not as a hub. A device can be part of multiple hub-and-spoke site-to-site VPN topologies. New/modified screens: **Devices** > **Template Management** Supported platforms: Firepower 1000/2100, Secure Firewall 1200/3100. Note that Firepower 2100 support is for threat defense 7.4.1–7.4.x only; those devices cannot run Version 7.6.0. Learn more: • See "Device Management Using Device Templates" • See "Onboard Threat Defense Devices using Device Templates to Cloud-delivered Firewall Management Center using Zero-Touch Provisioning.
AAA for user-defined VRF interfaces.	7.6.0	A device's authentication, authorization, and accounting (AAA) is now supported on user-defined Virtual Routing and Forwarding (VRF) interfaces. The default is to use the management interface. In device platform settings, you can now associate a security zone or interface group having the VRF interface, with a configured external authentication server. New/modified screens: **Devices** > **Platform Settings** > **External Authentication** See: Enable Virtual-Router-Aware Interface for External Authentication of Platform
Policy Analyzer & Optimizer cross-launch for access control.	Any	The Policy Analyzer & Optimizer evaluates access control policies for anomalies such as redundant or shadowed rules, and can take action to fix discovered anomalies. You can now launch the Policy Analyzer & Optimizer directly from the access control policy page. Choose **Policies** > **Access Control**, select policies, and click **Analyze Policies**.
High Availability/Scalability		
Multi-instance mode for the Secure Firewall 4200.	7.6.0	Multi-instance mode is now supported on the Secure Firewall 4200. See: Multi-Instance Mode for the Secure Firewall 3100/4200

Feature	Minimum Threat Defense	Details
Multi-instance mode conversion in the management center for the Secure Firewall 3100/4200.	7.6.0	You can now register an application-mode device to the management center and then convert it to multi-instance mode without having to use the CLI. New/modified screens: • **Devices** > **Device Management** > > **Convert to Multi-Instance** • **Devices** > **Device Management** > **Select Bulk Action** > **Convert to Multi-Instance**
16-node clusters for the Secure Firewall 3100/4200.	7.6.0	For the Secure Firewall 3100 and 4200, the maximum nodes were increased from 8 to 16. See: Clustering for the Secure Firewall 3100/4200
Individual interface mode for Secure Firewall 3100/4200 clusters.	7.6.0	Individual interfaces are normal routed interfaces, each with their own local IP address used for routing. The main cluster IP address for each interface is a fixed address that always belongs to the control node. When the control node changes, the main cluster IP address moves to the new control node, so management of the cluster continues seamlessly. Load balancing must be configured separately on the upstream switch. Restrictions: Not supported for container instances. New/modified screens: • **Devices** > **Device Management** > **Add Cluster** • **Devices** > **Device Management** > **Cluster** > **Interfaces / EIGRP / OSPF / OSPFv3 / BGP** • **Objects** > **Object Management** > **Address Pools** > **MAC Address Pool** See: Clustering for the Secure Firewall 3100/4200 and Address Pools
Deploy threat defense virtual clusters across multiple AWS availability zones.	7.6.0	You can now deploy threat defense virtual clusters across multiple availability zones in an AWS region. This enables continuous traffic inspection and dynamic scaling (AWS Auto Scaling) during disaster recovery. See: Deploy a Threat Defense Virtual Cluster on AWS
Deploy threat defense virtual for AWS in two-arm-mode with GWLB.	7.6.0	You can now deploy threat defense virtual for AWS in two-arm-mode with GWLB. This allows you to directly forward internet-bound traffic after traffic inspection, while also performing network address translation (NAT). Two-arm mode is supported in single and multi-VPC environments. Restrictions: Not supported with clustering. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide

Feature	Minimum Threat Defense	Details
Interfaces		
Deploy without the diagnostic interface on threat defense virtual for Azure and GCP.	7.4.1	You can now deploy without the diagnostic interface on threat defense virtual for Azure and GCP. Previously, we required one management, one diagnostic, and at least two data interfaces. New interface requirements are: • Azure: one management, two data (max eight) • GCP: one management, three data (max eight) Restrictions: This feature is supported for new deployments only. It is not supported for upgraded devices. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
SD-WAN		
SD-WAN wizard.	Hub: 7.6.0 Spoke: 7.3.0	A new wizard allows you to easily configure VPN tunnels between your centralized headquarters and remote branch sites. New/modified screens: **Devices** > **VPN** > **Site To Site** > **Add** > **SD-WAN Topology** See: Configure an SD-WAN Topology Using the SD-WAN Wizard
Access Control: Threat Detection and Application Identification		
QUIC decryption.	7.6.0 with Snort 3	You can configure the decryption policy to apply to sessions running on the QUIC protocol. QUIC decryption is disabled by default. You can selectively enable QUIC decryption per decryption policy and write decryption rules to apply to QUIC traffic. By decrypting QUIC connections, the system can then inspect the connections for intrusion, malware, or other issues. You can also apply granular control and filtering of decrypted QUIC connections based on specific criteria in the access control policy. We modified the decryption policy Advanced Settings to include the option to enable QUIC decryption. See: Decryption Policy Advanced Options

Feature	Minimum Threat Defense	Details
Snort ML: neural network-based exploit detector.	7.6.0 with Snort 3	A new Snort 3 inspector, snort_ml, uses neural network-based machine learning (ML) to detect known and 0-day attacks without needing multiple preset rules. The inspector subscribes to HTTP events and looks for the HTTP URI, which in turn is used by a neural network to detect exploits (currently limited to SQL injections). The new inspector is currently disabled in all default policies except maximum detection. A new intrusion rule, GID:411 SID:1, generates an event when the snort_ml detects an attack. This rule is also currently disabled in all default policies except maximum detection. See: Snort 3 Inspector Reference
Allow Cisco Talos to conduct advanced threat hunting and intelligence gathering using your traffic.	7.6.0 with Snort 3	**Upgrade impact. Upgrade enables telemetry.** You can help Talos (Cisco's threat intelligence team) develop a more comprehensive understanding of the threat landscape by enabling threat hunting telemetry. With this feature, events from special intrusion rules are sent to Talos to help with threat analysis, intelligence gathering, and development of better protection strategies. This setting is enabled by default in new and upgraded deployments. New/modified screens: **System** (⚙) > **Configuration** > **Intrusion Policy Preferences** > **Talos Threat Hunting Telemetry** See: Intrusion Policy Preferences
Access Control: Identity		
Passive identity agent for Microsoft AD.	Any	This feature is introduced. The passive identity agent identity source sends session data from Microsoft Active Directory (AD) to the management center. Passive identity agent software is supported on: • Microsoft AD server (Windows Server 2008 or later) • Microsoft AD domain controller (Windows Server 2008 or later) • Any client connected to the domain you want to monitor (Windows 8 or later) See: User Control With the Passive Identity Agent.

Feature	Minimum Threat Defense	Details
pxGrid Cloud Identity Source.		The Cisco Identity Services Engine (Cisco ISE) pxGrid Cloud Identity Source enables you to use subscription and user data from Cisco ISE in cloud-delivered Firewall Management Center access control rules. The pxGrid cloud identity source enables the use of constantly changing dynamic objects from ISE to be used for user control in access control policies in the cloud-delivered Firewall Management Center. New/updated screens: **Integration** > **Other Integrations** > **Identity Sources** > **Identity Services Engine (pxGrid Cloud)** See: User Control with the pxGrid Cloud Identity Source
New connectors for Cisco Secure Dynamic Attributes Connector	Any	Cisco Secure Dynamic Attributes Connector now supports AWS security groups, AWS service tags, and Cisco Cyber Vision. Version restrictions: For on-prem Cisco Secure Dynamic Attributes Connector integrations, requires Version 3.0. See Amazon Web Services Connector—About User Permissions and Imported Data,
Microsoft Azure AD realms for active or passive authentication.	Active: 7.6.0 with Snort 3 Passive: 7.4.1 with Snort 3	You can now use Microsoft Azure Active Directory (AD) realms for active and passive authentication: • Active authentication using Azure AD: Use Azure AD as a captive portal. • Passive authentication using Cisco ISE (introduced in Version 7.4.0): The management center gets groups from Azure AD and logged-in user session data from ISE. We use SAML (Security Assertion Markup Language) to establish a trust relationship between a service provider (the devices that handle authentication requests) and an identity provider (Azure AD). For upgraded management centers, existing Azure AD realms are displayed as SAML - Azure AD realms. **Upgrade impact**. If you had a Microsoft Azure AD realm configured before the upgrade, it is displayed as a SAML - Azure AD realm configured for passive authentication. All previous user session data is preserved. New/modified screens: **Integration** > **Other Integrations** > **Realms** > **Add Realm** > **SAML - Azure AD** New/modified CLI commands: none See: Create a Microsoft Azure AD (SAML) Realm.
Event Logging and Analysis		

Feature	Minimum Threat Defense	Details
MITRE and other enrichment information in connection events.	7.6.0 with Snort 3	MITRE and other enrichment information in connection events makes it easy to access contextual information for detected threats. This includes information from Talos and from the encrypted visibility engine (EVE). For EVE enrichment, you must enable EVE. Connection events have two new fields, available in both the unified and classic event viewers: • **MITRE ATT&CK**: Click the progression graph to see an expanded view of threat details, including tactics and techniques. • **Other Enrichment**: Click to see any other available enrichment information, including from EVE. The new Talos Connectivity Status health module monitors management center connectivity with Talos, which is required for this feature. For the specific internet resources required, see Internet Access Requirements. See Configure EVE.
Administration		
New theme for the management center..	Any	We introduced new left-hand navigation for the cloud-deilvered Firewall Management Center for streamlined usability; and updated the look and feel of the interface.

August 23, 2024

Table 2: Features in Version 20240808

Feature	Minimum Threat Defense	Details
Platform		

Feature	Minimum Threat Defense	Details
Threat defense Version 7.6.0 support.	7.6.0	You can now manage threat defense devices running Version 7.6.0. **Note** The Firepower 2100 is deprecated in Version 7.6.0. Although you can continue managing these devices running Version 7.0.3–7.4.x, you cannot upgrade them further. Because there is a single configuration guide that covers the latest version, for features that are only supported with older devices, refer to the *on-prem* management center guide that matches your threat defense version. **Note** The cloud-delivered Firewall Management Center supports a wider range of managed device versions than on-prem management centers. If you are using an on-prem management center for analytics with Version 7.0.x devices, we recommend you upgrade those devices to at least Version 7.2.x, if possible. This will allow you to get events from those older devices while also adding devices running the latest release. For more information, see End of support: analytics-only capabilities with the full range of threat defense devices.
High Availability/Scalability		

Feature	Minimum Threat Defense	Details
Multi-instance mode for the Secure Firewall 3100.	7.4.1	You can deploy the Secure Firewall 3100 as a single device (*appliance mode*) or as multiple container instances (*multi-instance mode*). In multi-instance mode, you can deploy multiple container instances on a single chassis that act as completely independent devices. Note that in multi-instance mode, you upgrade the operating system and the firmware (*chassis upgrade*) separately from the container instances (*threat defense upgrade*). New/modified screens: • **Inventory** > **FTD Chassis** • **Devices** > **Device Management** > **Device** > **Chassis Manager** • **Devices** > **Platform Settings** > **New Policy** > **Chassis Platform Settings** • **Devices** > **Chassis Upgrade** New/modified threat defense CLI commands: **configure multi-instance network ipv4**, **configure multi-instance network ipv6** New/modified FXOS CLI commands: **create device-manager**, **set deploymode** Platform restrictions: Not supported on the Secure Firewall 3105. See: Use Multi-Instance Mode for the Secure Firewall and Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center
Access Control: Threat Detection and Application Identification		
Easily bypass decryption for sensitive and undecryptable traffic.	Any	It is now easier to bypass decryption for sensitive and undecryptable traffic, which protects users and improves performance. New decryption policies now include predefined rules that, if enabled, can automatically bypass decryption for sensitive URL categories (such as finance or medical), undecryptable distinguished names, and undecryptable applications. Distinguished names and applications are undecryptable typically because they use TLS/SSL certificate pinning, which is itself not decryptable. For outbound decryption, you enable/disable these rules as part of creating the policy. For inbound decryption, the rules are disabled by default. After the policy is created, you can edit, reorder, or delete the rules entirely. New/modified screens: **Policies** > **Access Control** > **Decryption** > **Create Decryption Policy** See: Create a Decryption Policy See: Create a Decryption Policy

Feature	Minimum Threat Defense	Details
Access Control: Identity		
Microsoft Azure AD as a user identity source.	7.4.2	You can use a Microsoft Azure Active Directory (Azure AD) realm with ISE to authenticate users and get user sessions for user control. New/modified screens: • **Integration** > **Other Integrations** > **Realms** > **Add Realm** > **Azure AD** • **Integration** > **Other Integrations** > **Realms** > Actions, such as downloading users, copying, editing, and deleting Supported ISE versions: 3.0 patch 5+, 3.1 (any patch level), 3.2 (any patch level) See: Create a Microsoft Azure Active Directory Realm
Health Monitoring		
Collect health data without alerting.	Any	You can now disable health alerts/health alert sub-types for ASP Drop, CPU, and Memory health modules, while continuing to collect health data. This allows you to minimize health alert noise and focus on the most critical issues. New/modified screens: In any health policy (**System** (⚙) > **Health** > **Policy**), there are now checkboxes that enable and disable ASP Drop (threat defense only), CPU, and Memory health alert sub-types. See: Health Policies
Apply a default health policy upon device registration.	Any	You can now choose a default health policy to apply upon device registration. On the health policy page, the policy name indicates which is the default. If you want to use a different policy for a specific device post-registration, change it there. You cannot delete the default device health policy. New/modified screens: **System** (⚙) > **Health** > **Policy** > **More** (⋮) > **Set as Default** See: Set a Default Health Policy

Feature	Minimum Threat Defense	Details
Chassis-level health alerts for the Firepower 4100/9300.	7.4.1	You can now view chassis-level health alerts for Firepower 4100/9300 by registering the chassis to the management center as a read-only device. You must also enable the Firewall Threat Defense Platform Faults health module and apply the health policy. The alerts appear in the Message Center, the health monitor (in the left pane, under Devices, select the chassis), and in the health events view. You can also add a chassis (and view health alerts for) the Secure Firewall 3100 in multi-instance mode. For those devices, you use the management center to manage the chassis. But for the Firepower 4100/9300 chassis, you still must use the chassis manager or the FXOS CLI. New/modified screens: **Inventory** > **FTD Chassis** See: Onboard a Chassis
Administration		
Threat defense high availability automatically resumes after restoring from backup.	7.6.0	When replacing a failed unit in a high availability pair, you no longer have to manually resume high availability after the restore completes and the device reboots. You should still confirm that high availability has resumed before you deploy. Version restrictions: Not supported with threat defense Version 7.0–7.0.6, 7.1.x, 7.2.0–7.2.9, 7.3.x, or 7.4.0–7.4.2. See: Restore Security Cloud Control-Managed Devices
Change management ticket takeover; more features in the approval workflow.	Any	You can now take over another user's ticket. This is useful if a ticket is blocking other updates to a policy and the user is unavailable. These features are now included in the approval workflow: decryption policies, DNS policies, file and malware policies, network discovery, certificates and certificate groups, cipher suite lists, Distinguished Name objects, Sinkhole objects. See: Change Management
Troubleshooting		

Feature	Minimum Threat Defense	Details
Troubleshoot Snort 3 performance issues with a CPU and rule profiler.	7.6.0 with Snort 3	New CPU and rule profilers help you troubleshoot Snort 3 performance issues. You can now monitor: • CPU time taken by Snort 3 modules/inspectors to process packets. • CPU resources each module is consuming, relative to the total CPU consumed by the Snort 3 process. • Modules with unsatisfactory performance when Snort 3 is consuming high CPU. • Intrusion rules with unsatisfactory performance. New/modified screens: **Devices** > **Troubleshoot** > **Snort 3 Profiling** Platform restrictions: Not supported for container instances. See: Advanced Troubleshooting for the Secure Firewall Threat Defense Device See: Advanced Troubleshooting for the Secure Firewall Threat Defense Device
Deprecated Features		

Feature	Minimum Threat Defense	Details
End of support: analytics-only capabilities with the full range of threat defense devices.	Any	If you are using an on-prem management center for analytics with Version 7.0.x devices, we recommend you upgrade those devices to at least Version 7.2.x, if possible. This will allow you to get events from those older devices while also adding devices running the latest release. The cloud-delivered Firewall Management Center supports a wider range of managed device versions than on-prem management centers. This can cause issues if you use an on-prem management center for analytics because devices can be "too old" or "too new" to co-manage. You can be prevented from: • Registering newer devices to the analytics management center because older devices are blocking the required management center upgrade. • Upgrading co-managed devices to the latest release, because the analytics management center is "stuck" at an older release. • Reverting device upgrade, if revert would take the device out of compatibility with the analytics management center. For example, consider a scenario where you want to add co-managed Version 7.6.0 devices to a deployment that currently includes co-managed Version 7.0.x devices. The cloud-delivered Firewall Management Center can manage this full range of devices, but the on-prem analytics management center cannot. In order of preference, you can: • Upgrade the Version 7.0.x devices to at least Version 7.2.0, upgrade the analytics management center to Version 7.6.0, then add the Version 7.6.0 devices to both management centers. • Remove the Version 7.0.x devices from the analytics management center, upgrade the analytics management center to Version 7.6.0, then add the Version 7.6.0 devices to both management centers. • Leave the analytics management center as it is and do not add your Version 7.6.0 devices. That is, your choices are: • To get events from all devices, upgrade (or replace) the analytics management center and your older devices. • To forgo events from older devices, upgrade (or replace) the analytics management center only. • To forgo events from newer devices, leave the analytics management center at an older release.

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 30, 2024

Table 3: Features in Version 20240514

Feature	Minimum Threat Defense	Details
Platform Migration		

Feature	Minimum Threat Defense	Details
Migrate clustered threat defense devices from an on-prem management center to the cloud-delivered Firewall Management Center.	7.0.6 7.2.1	Clustered Secure Firewall Threat Defense devices are now migrated along with the rest of the configuration when they are migrated from the on-prem 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
Deployment and Policy Management		
Change management.	Any	You can enable change management if your organization needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed. We added the **System** (⚙) > **Configuration** > **Change Management** page to enable the feature. When enabled, there is a **System** (⚙) > **Change Management Workflow** page, and a new **Ticket** (📋) quick access icon in the menu. See: Change Management

April 2, 2024

This release introduces stability, hardening, and performance enhancements.

February 13, 2024

Table 4: Features in Version 20240203

Feature	Minimum Threat Defense	Details
Platform		
Threat defense Version 7.4.1 support.	7.4.1	You can now manage threat defense devices running Version 7.4.1.
Network modules for the Secure Firewall 3130 and 3140.	7.4.1	The Secure Firewall 3130 and 3140 now support these network modules: • 2-port 100G QSFP+ network module (FPR3K-XNM-2X100G) See: Cisco Secure Firewall 3110, 3120, 3130, and 3140 Hardware Installation Guide

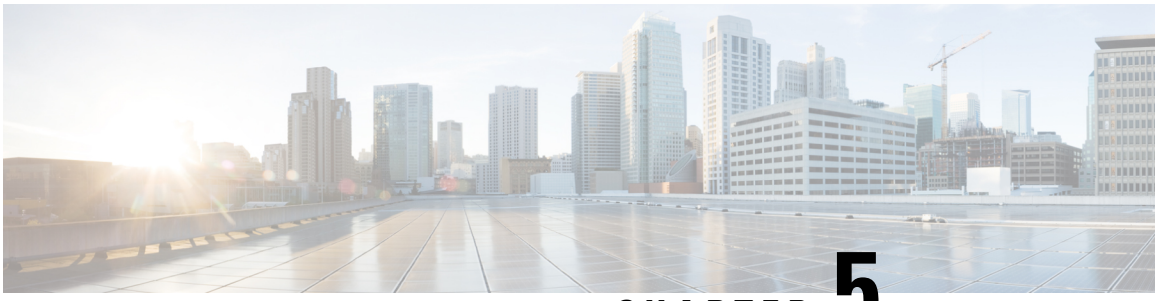
Feature	Minimum Threat Defense	Details
Optical transceivers for Firepower 9300 network modules.	7.4.1	The Firepower 9300 now supports these optical transceivers: • QSFP-40/100-SRBD • QSFP-100G-SR1.2 • QSFP-100G-SM-SR On these network modules: • FPR9K-NM-4X100G • FPR9K-NM-2X100G • FPR9K-DNM-2X100G See: Cisco Firepower 9300 Hardware Installation Guide
Performance profile support for the Secure Firewall 3100.	7.4.1	The performance profile settings available in the platform settings policy now apply to the Secure Firewall 3100. Previously, this feature was supported on the Firepower 4100/9300, the Secure Firewall 4200, and on threat defense virtual. See: Configure the Performance Profile
NAT		
Create network groups while editing NAT rules.	Any	You can now create network groups in addition to network objects while editing a NAT rule. See: Customizing NAT Rules for Multiple Devices
Device Management		
Device management services supported on user-defined VRF interfaces.	Any	Device management services configured in the threat defense platform settings (NetFlow, SSH access, SNMP hosts, syslog servers) are now supported on user-defined Virtual Routing and Forwarding (VRF) interfaces. Platform restrictions: Not supported with container instances or clustered devices. See Platform Settings
SD-WAN		
SD-WAN Summary dashboard	7.4.1	The WAN Summary dashboard provides a snapshot of your WAN devices and their interfaces. It provides insight into your WAN network and information about device health, interface connectivity, application throughput, and VPN connectivity. You can monitor the WAN links and take proactive and prompt recovery measures. In addition, you can also monitor the WAN interface application performance using the **Application Monitoring** tab. New/modified screens: **Analysis** > **SD-WAN Summary** See: SD-WAN Summary Dashboard

Feature	Minimum Threat Defense	Details
Access Control: Identity		
Captive portal support for multiple Active Directory realms (realm sequences).	7.4.1	**Upgrade impact. Update custom authentication forms.** You can configure active authentication for either an LDAP realm; or a Microsoft Active Directory realm or a realm sequence. In addition, you can configure a passive authentication rule to fall back to active authentication using either a realm or a realm sequence. You can optionally share sessions between managed devices that share the same identity policy in access control rules. In addition, you have the option to require users to authenticate again when they access the system using a different managed device than they accessed previously. If you use the HTTP Response Page authentication type, after you upgrade threat defense, you must add **`<select name="realm" id="realm"></select>`** to your custom authentication form. This allows the user to choose between realms. Restrictions: Not supported with Microsoft Azure Active Directory. New/modified screens: • **Policies** > **Identity** > **(edit policy)** > **Active Authentication** > **Share active authentication sessions across firewalls** • **Identity policy** > **(edit)** > **Add Rule** > **Passive Authentication** > **Realms & Settings** > **Use active authentication if passive or VPN identity cannot be established** • **Identity policy** > **(edit)** > **Add Rule** > **Active Authentication** > **Realms & Settings** > **Use active authentication if passive or VPN identity cannot be established** See: How to Configure the Captive Portal for User Control
Share captive portal active authentication sessions across firewalls.	7.4.1	Determines whether or not users are required to authenticate when their authentication session is sent to a different managed device than one they previously connected to. If your organization requires users to authenticate every time they change locations or sites, you should *disable* this option. • (Default.) Enable to allow users to authenticate with any managed device associated with the active authentication identity rule. • Disable to require the user to authenticate with a different managed device, even if they have already authenticated with another managed device to which the active authentication rule is deployed. New/modified screens: **Policies** > **Identity** > **(edit policy)** > **Active Authentication** > **Share active authentication sessions across firewalls** See: How to Configure the Captive Portal for User Control
Deployment and Policy Management		

Feature	Minimum Threat Defense	Details
View and generate reports on configuration changes since your last deployment.	Any	You can generate, view, and download (as a zip file) the following reports on configuration changes since your last deployment: • A policy changes report for each device that previews the additions, changes, or deletions in the policy, or the objects that are to be deployed on the device. • A consolidated report that categorizes each device based on the status of policy changes report generation. This is especially useful after you upgrade threat defense devices, so that you can see the changes made by the upgrade before you deploy. New/modified screens: **Deploy** > **Advanced Deploy**. See: Download Policy Changes Report for Multiple Devices
Suggested release notifications.	Any	The management center now notifies you when a new suggested release is available. If you don't want to upgrade right now, you can have the system remind you later, or defer reminders until the next suggested release. The new upgrade page also indicates suggested releases. See: Cisco Secure Firewall Management Center New Features by Release
Enable revert from the threat defense upgrade wizard.	Any	You can now enable revert from the threat defense upgrade wizard. Other version restrictions: You must be upgrading threat defense to Version 7.2+. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center
View detailed upgrade status from the threat defense upgrade wizard.	Any	The final page of the threat defense upgrade wizard now allows you to monitor upgrade progress. This is in addition to the existing monitoring capability on the Upgrade tab on the Device Management page, and on the Message Center. Note that as long as you have not started a new upgrade flow, **Devices** > **Threat Defense Upgrade** brings you back to this final wizard page, where you can view the detailed status for the current (or most recently complete) device upgrade. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center

Feature	Minimum Threat Defense	Details
Firmware upgrades included in FXOS upgrades.	Any	**Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.** For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1 now include firmware upgrades. Secure Firewall 3100 in multi-instance mode (new in Version 7.4.1) also bundles FXOS and firmware upgrades. If any firmware component on the device is older than the one included in the FXOS bundle, the FXOS upgrade also updates the firmware. If the firmware is upgraded, the device reboots twice—once for FXOS and once for the firmware. Just as with software and operating system upgrades, do not make or deploy configuration changes during firmware upgrade. Even if the system appears inactive, do not manually reboot or shut down during firmware upgrade. See: Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide
Upgrade		
Improved upgrade starting page and package management.	Any	A new upgrade page makes it easier to choose, download, manage, and apply upgrades to your entire deployment. The page lists all upgrade packages that apply to your current deployment, with suggested releases specially marked. You can easily choose and direct-download packages from Cisco, as well as manually upload and delete packages. Patches are not listed unless you have at least one appliance at the appropriate maintenance release (or you manually uploaded the patch). You must manually upload hotfixes. New/modified screens: • **System** (⚙) > **Product Upgrades** is now where you upgrade devices, as well as manage upgrade packages. • **System** (⚙) > **Content Updates** is now where you update intrusion rules, the VDB, and the GeoDB. • **Devices** > **Threat Defense Upgrade** takes you directly to the threat defense upgrade wizard. Deprecated screens/options: • **System** (⚙) > **Updates** is deprecated. All threat defense upgrades now use the wizard. • The **Add Upgrade Package** button on the threat defense upgrade wizard has been replaced by a **Manage Upgrade Packages** link to the new upgrade page. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center
Administration		

Feature	Minimum Threat Defense	Details
Updated internet access requirements for direct-downloading software upgrades.	Any	The management center has changed its direct-download location for software upgrade packages from sourcefire.com to amazonaws.com. See: Internet Access Requirements
Scheduled tasks download patches and VDB updates only.	Any	The **Download Latest Update** scheduled task no longer downloads maintenance releases; now it only downloads the latest applicable patches and VDB updates. To direct-download maintenance (and major) releases to the management center, use **System** (⚙) > **Product Upgrades**. See: Software Update Automation
Smaller VDB for lower memory Snort 2 devices.	Any with Snort 2	For VDB 363+, the system now installs a smaller VDB (also called *VDB lite*) on lower memory devices running Snort 2. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Lower memory devices: ASA-5508-X and ASA 5516-X See: Update the Vulnerability Database
Deprecated Features		
Deprecated: DHCP relay trusted interfaces with FlexConfig.	Any	You can now use the management center web interface to configure interfaces as trusted interfaces to preserve DHCP Option 82. If you do this, these settings override any existing FlexConfigs, although you should remove them. See: Configure the DHCP Relay Agent
Deprecated: Merging downloadable access control list with a Cisco attribute-value pair ACL for RADIUS identity sources with FlexConfig.	Any	This feature is now supported in the management center web interface.
Deprecated: Health alerts for `frequent drain of events`.	7.4.1	The Disk Usage health module no longer alerts with `frequent drain of events`. You may continue to see these alerts until you either deploy health policies to managed devices (stops the display of alerts) or upgrade devices to Version 7.4.1+ (stops the sending of alerts). See: Disk Usage and Drain of Events Health Monitor Alerts



CHAPTER 5

New Features in Cloud-delivered Firewall Management Center 2023

November 30, 2023

Table 5: New Features: Version 20231117

Feature	Min. Threat Defense	Details
Administration		
Schedule a Secure Firewall Threat Defense Device Backup in Cloud-delivered Firewall Management Center	Any	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.

October 19, 2023

Table 6: New Features: Version 20230929

Feature	Min. Threat Defense	Details
Platform		
Threat defense Version 7.4.0 support.	7.4.0	You can now manage threat defense devices running Version 7.4.0. Version 7.4.0 is available *only* on the Secure Firewall 4200. You must use a Secure Firewall 4200 for features that require Version 7.4.0. Support for all other platforms resumes in Version 7.4.1.
Secure Firewall 4200.	7.4.0	You can now manage the Secure Firewall 4215, 4225, and 4245 with cloud-delivered Firewall Management Center. These devices support the following new network modules: • 2-port 100G QSFP+ network module (FPR4K-XNM-2X100G) • 4-port 200G QSFP+ network module (FPR4K-XNM-4X200G) See: Cisco Secure Firewall 4215, 4225, and 4245 Hardware Installation Guide
Performance profile support for the Secure Firewall 4200.	7.4.0	The performance profile settings available in the platform settings policy now apply to the Secure Firewall 4200. Previously, this feature was supported only on the Firepower 4100/9300 and on threat defense virtual. See: Configure the Performance Profile
Numbering convention for cloud-delivered Firewall Management system.	Any	The cloud-delivered Firewall Management system is a feature of CDO. For the purposes of troubleshooting, we identify the version number of the cloud-delivered Firewall Management Center on the FMC Services page. See: View Services Page Information.
Platform Migration		
Migrate from Firepower 1000/2100 to Secure Firewall 3100.	Any	You can now easily migrate configurations from the Firepower 1000/2100 to the Secure Firewall 3100. New/modified screens: **Devices** > **Device Management** > **Migrate** Platform restrictions: Migration not supported from the Firepower 1010 or 1010E. See: Migrate the Configuration to a new Model.

Feature	Min. Threat Defense	Details
Migrate devices from Firepower Management Center 1000/2500/4500 to cloud-delivered Firewall Management Center.	Any	

Feature	Min. Threat Defense	Details
		You can migrate devices from Firepower Management Center 1000/2500/4500 to cloud-delivered Firewall Management Center. To migrate devices, you must *temporarily* upgrade the on-prem management center from Version 7.0.3 (7.0.5 recommended) to Version 7.4.0. This temporary upgrade is required because Version 7.0 management centers do not support device migration to the cloud. Additionally, only standalone and high availability threat defense devices running Version 7.0.3+ (7.0.5 recommended) are eligible for migration. Cluster migration is not supported at this time. **Important** Version 7.4.0 is only supported on the 1000/2500/4500 during the migration process. You should minimize the time between management center upgrade and device migration. To summarize the migration process: **1.** Prepare for upgrade and migration. Read, understand, and meet all the prerequisites outlined in the release notes, upgrade guides, and migration guide. Before you upgrade, it is especially important that the on-prem management center is "ready to go," that is, managing only the devices you want to migrate, configuration impact assessed (such as VPN impact), freshly deployed, fully backed up, all appliances in good health, and so on. You should also provision, license, and prepare the cloud tenant. This must include a strategy for security event logging; you cannot retain the on-prem management center for analytics because it will be running an unsupported version. **2.** Upgrade the on-prem management center and all its managed devices to at least Version 7.0.3 (Version 7.0.5 recommended). If you are already running the minimum version, you can skip this step. **3.** Upgrade the on-prem management center to Version 7.4.0. Unzip (but do not untar) the upgrade package before uploading it to the management center. Download from: Special Release. **4.** Onboard the on-prem management center to CDO. **5.** Migrate all devices from the on-prem management center to the cloud-delivered Firewall Management Center as described in the migration guide. When you select devices to migrate, make sure you choose **Delete FTD from On-Prem FMC**. Note that the device is not fully deleted unless you commit the changes or 14 days pass. **6.** Verify migration success. If the migration does not function to your expectations, you have 14 days to switch back or it is committed automatically. However, note that Version 7.4.0 is unsupported for general operations. To return the on-prem management center to a supported version you must remove the re-migrated devices, re image back to Version 7.0.x, restore from backup, and reregister the devices.

Feature	Min. Threat Defense	Details
		See: • Cisco Secure Firewall Threat Defense Release Notes • Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 • Migrate On-Prem Management Center Managed Secure Firewall Threat Defense to Cloud-delivered Firewall Management Center If you have questions or need assistance at any point in the migration process, contact Cisco TAC.
S2S VPN support in FTD to cloud migration. Migrate threat defense devices with VPN policies from on-prem to cloud-delivered Firewall Management Center.	7.0.3-7.0.x 7.2 or later	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
Interfaces		

Feature	Min. Threat Defense	Details
Merged management and diagnostic interfaces.	7.4.0	**Upgrade impact. Merge interfaces after upgrade.** For new devices using 7.4 and later, you cannot use the legacy diagnostic interface. Only the merged management interface is available. If you upgraded to 7.4 or later and: • You did not have any configuration for the diagnostic interface, then the interfaces will merge automatically. • You have configuration for the diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate diagnostic interface. Note that support for the diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including Management) in the configuration. For platform settings, this means: • You can no longer enable HTTP, ICMP, or SMTP for diagnostic. • For SNMP, you can allow hosts on management instead of diagnostic. • For Syslog servers, you can reach them on management instead of diagnostic. • If Platform Settings for syslog servers or SNMP hosts specify the diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices. • DNS lookups no longer fall back to the management-only routing table if you do not specify interfaces. New/modified screens: **Devices** > **Device Management** > **Interfaces** New/modified commands: **show management-interface convergence** See: Merge the Management and Diagnostic Interfaces
VXLAN VTEP IPv6 support.	7.4.0	You can now specify an IPv6 address for the VXLAN VTEP interface. IPv6 is not supported for the threat defense virtual cluster control link or for Geneve encapsulation. New/modified screens: • **Devices** > **Device Management** > **Edit Device** > **VTEP** > **Add VTEP** • **Devices** > **Device Management** > **Edit Devices** > **Interfaces** > **Add Interfaces** > **VNI Interface** See: Configure Geneve Interfaces

Feature	Min. Threat Defense	Details
Loopback interface support for BGP and management traffic.	7.4.0	You can now use loopback interfaces for AAA, BGP, DNS, HTTP, ICMP, IPsec flow offload, NetFlow, SNMP, SSH, and syslog. New/modified screens: **Devices** > **Device Management** > Edit device > **Interfaces** > **Add Interfaces** > **Loopback Interface** See: Configure Loopback Interfaces
Loopback and management type interface group objects.	7.4.0	You can create interface group objects with only management-only or loopback interfaces. You can use these groups for management features such as DNS servers, HTTP access, or SSH. Loopback groups are available for any feature that can utilize loopback interfaces. However, it's important to note that DNS does not support management interfaces. New/modified screens: **Objects** > **Object Management** > **Interface** > **Add** > **Interface Group** See: Interface
High Availability/Scalability		
Reduced "false failovers" for threat defense high availability.	7.4.0	Other version restrictions: Not supported with threat defense Version 7.3.x. See: Heartbeat Module Redundancy
SD-WAN		
Policy-based routing using HTTP path monitoring.	7.2.0	Policy-based routing (PBR) can now use the performance metrics (RTT, jitter, packet-lost, and MOS) collected by path monitoring through HTTP client on the application domain rather than the metrics on a specific destination IP. HTTP-based application monitoring option is enabled by default for the interface. You can configure a PBR policy with match ACL having the monitored applications and interface ordering for path determination. New/modified screens: **Devices** > **Device Management** > Edit device > Edit interface > **Path Monitoring** > **Enable HTTP based Application Monitoring** check box. Platform restrictions: Not supported for clustered devices. See: Configure Path Monitoring Settings
Policy-based routing with user identity and SGTs.	7.4.0	You can now classify network traffic based on users, user groups, and SGTs in PBR policies. Select the identity and SGT objects while defining the extended ACLs for the PBR policies. New/modified screens: **Objects** > **Object Management** > **Access List** > **Extended** > Add/Edit Extended Access List > Add/Edit Extended Access List Entry > **Users** and **Security Group Tag** See: Configure Extended ACL Objects
VPN		

Feature	Min. Threat Defense	Details
IPsec flow offload on the VTI loopback interface for the Secure Firewall 4200.	7.4.0	On the Secure Firewall 4200, qualifying IPsec connections through the VTI loopback interface are offloaded by default. Previously, this feature was supported for physical interfaces on the Secure Firewall 3100. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command. Other requirements: FPGA firmware 6.2+ See: IPSec Flow Offload
Crypto debugging enhancements for the Secure Firewall 4200.	7.4.0	We made the following enhancements to crypto debugging: • The crypto archive is now available in text and binary formats. • Additional SSL counters are available for debugging. • Remove stuck encrypt rules from the ASP table without rebooting the device. New/modified CLI commands: **show counters** See: Troubleshooting Using Crypto Archives
VPN: Remote Access		
Customize Secure Client messages, icons, images, and connect/disconnect scripts.	7.2.0	You can now customize Secure Client and deploy these customizations to the VPN headend. The following are the supported Secure Client customizations: • GUI text and messages • Icons and images • Scripts • Binaries • Customized Installer Transforms • Localized Installer Transforms Threat defense distributes these customizations to the endpoint when an end user connects from the Secure Client. New/modified screens: • **Objects** > **Object Management** > **VPN** > **Secure Client Customization** • **Devices** > **Remote Access** > Edit VPN policy > **Advanced** > **Secure Client Customization** See: Customize Secure Client
VPN: Site to Site		

Feature	Min. Threat Defense	Details
Easily exempt site-to-site VPN traffic from NAT translation.	Any	We now make it easier to exempt site-to-site VPN traffic from NAT translation. New/modified screens: • Enable NAT exemptions for an endpoint: **Devices** > **VPN** > **Site To Site** > **Add/Edit Site to Site VPN** > **Add/Edit Endpoint** > **Exempt VPN traffic from network address translation** • View NAT exempt rules for devices that do not have a NAT policy: **Devices** > **NAT** > **NAT Exemptions** • View NAT exempt rules for a single device: **Devices** > **NAT** > **Threat Defense NAT Policy** > **NAT Exemptions** See: NAT Exemption
Easily view IKE and IPsec session details for VPN nodes.	Any	You can view the IKE and IPsec session details of VPN nodes in a user-friendly format in the Site-to-Site VPN dashboard. New/modified screens: **Overview** > **Site to Site VPN** > Under the Tunnel Status widget, hover over a topology, click **View**, and then click the **CLI Details** tab. See: Monitoring the Site-to-Site VPNs
Access Control: Threat Detection and Application Identification		
Sensitive data detection and masking.	7.4.0 with Snort 3	**Upgrade impact. New rules in default policies take effect.** Sensitive data such as social security numbers, credit card numbers, emails, and so on may be leaked onto the internet, intentionally or accidentally. Sensitive data detection is used to detect and generate events on possible sensitive data leakage and generates events only if there is a transfer of significant amount of Personally Identifiable Information (PII) data. Sensitive data detection can mask PII in the output of events, using built-in patterns. Disabling data masking is not supported. See: Custom Rules in Snort 3

Feature	Min. Threat Defense	Details
Clientless zero-trust access.	7.4.0 with Snort 3	We introduced Zero Trust Access that allows you to authenticate and authorize access to protected web based resources, applications, or data from inside (on-premises) or outside (remote) the network using an external SAML Identity Provider (IdP) policy. The configuration consists of a Zero Trust Application Policy (ZTAP), Application Group, and Applications. New/modified screens: • **Policies** > **Zero Trust Application** • **Analysis** > **Connections** > **Events** • **Overview** > **Dashboard** > **Zero Trust** New/modified CLI commands: • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics** See: Zero Trust Access.
Routing		
Configure graceful restart for BGP on IPv6 networks.	7.3.0	You can now configure BGP graceful restart for IPv6 networks on managed devices version 7.3 and later. New/modified screens: **Devices** > **Device Management** > Edit device > **Routing** > **BGP** > **IPv6** > **Neighbor** > Add/Edit Neighbor. See: Configure BGP Neighbor Settings
Virtual routing with dynamic VTI.	7.4.0	You can now configure a virtual router with a dynamic VTI for a route-based site-to-site VPN. New/modified screens: **Devices** > **Device Management** > Edit Device > **Routing** > **Virtual Router Properties** > Dynamic VTI interfaces under **Available Interfaces** Platform restrictions: Supported only on native mode standalone or high availability devices. Not supported for container instances or clustered devices. See: About Virtual Routers and Dynamic VTI
Access Control: Threat Detection and Application Identification		

Feature	Min. Threat Defense	Details
Encrypted visibility engine enhancements.	7.4.0 with Snort 3	Encrypted Visibility Engine (EVE) can now: • Block malicious communications in encrypted traffic based on threat score. • Determine client applications based on EVE-detected processes. • Reassemble fragmented Client Hello packets for detection purposes. New/modified screens: Use the access control policy's advanced settings to enable EVE and configure these settings. See: Encrypted Visibility Engine
Exempt specific networks and ports from bypassing or throttling elephant flows.	7.4.0 with Snort 3	You can now exempt specific networks and ports from bypassing or throttling elephant flows. New/modified screens: • When you configure elephant flow detection in the access control policy's advanced settings, if you enable the **Elephant Flow Remediation** option, you can now click **Add Rule** and specify traffic that you want to exempt from bypass or throttling. • When the system detects an elephant flow that is exempted from bypass or throttling, it generates a mid-flow connection event with the reason **Elephant Flow Exempted**. Platform restrictions: Not supported on the Firepower 2100 series. See: Elephant Flow Detection
Improved JavaScript inspection.	7.4.0 with Snort 3	We improved JavaScript inspection, which is done by normalizing the JavaScript and matching rules against the normalized content. See: HTTP Inspect Inspector and Cisco Secure Firewall Management Center Snort 3 Configuration Guide
Access Control: Identity		
Cisco Secure Dynamic Attributes Connector on the management center.	Any	You can now configure the Cisco Secure Dynamic Attributes Connector on the management center. Previously, it was only available as a standalone application. See: Cisco Secure Dynamic Attributes Connector
Event Logging and Analysis		
Configure threat defense devices as NetFlow exporters from the management center web interface.	Any	NetFlow is a Cisco application that provides statistics on packets flows. You can now use the management center web interface to configure threat defense devices as NetFlow exporters. If you have an existing NetFlow FlexConfig and redo your configurations in the web interface, you cannot deploy until you remove the deprecated FlexConfigs. New/modified screens: **Devices** > **Platform Settings** > **Threat Defense Settings Policy** > **NetFlow** See: Configure NetFlow
Health Monitoring		

Feature	Min. Threat Defense	Details
New asp drop metrics.	7.4.0	You can add over 600 new asp (accelerated security path) drop metrics to a new or existing device health dashboard. Make sure you choose the **ASP Drops** metric group. New/modified screens: **System** (⚙) > **Health** > **Monitor** > **Device** See: show asp drop Command Usage
Administration		
Support for IPv6 URLs when checking certificate revocation.	7.4.0	Previously, threat defense supported only IPv4 OCSP URLs. Now, threat defense supports both IPv4 and IPv6 OCSP URLs. See: Certificate Enrollment Object Revocation Options
Store threat defense backup files in a secure remote location.	Any	When you back up a device, the cloud-delivered Firewall Management Center stores the backup files in its secure cloud storage. See: Backup/Restore
Usability, Performance, and Troubleshooting		
Usability enhancements.	Any	You can now: • Manage Smart Licensing for threat defense clusters from **System** (⚙) > **Smart Licenses**. Previously, you had to use the Device Management page. See: Licenses for Clustering • Download a report of Message Center notifications. In the Message Center, click the new **Download Report** icon, next to the **Show Notifications** slider. See: Managing System Messages. • Download a report of all registered devices. On **Devices** > **Device Management**, click the new **Download Device List Report** link, at the top right of the page. See: Download the Managed Device List. • Easily create custom health monitoring dashboards, and easily edit existing dashboards. See: Correlating Device Metrics
Specify the direction of traffic to be captured with packet capture for the Secure Firewall 4200.	7.4.0	On the Secure Firewall 4200, you can use a new **direction** keyword with the **capture** command. New/modified CLI commands: **capture***capture_name***switchinterface***interface_name* [**direction** { **both** | **egress** | **ingress** }] See: Cisco Secure Firewall Threat Defense Command Reference
Management Center REST API		

Feature	Min. Threat Defense	Details
Cloud-delivered Firewall Management Center REST API.	Feature dependent	For information on changes to the management center REST API, see What's New in the API quick start guide.

Table 7: Deprecated Features: Version 20230929

Feature	Deprecated in Threat Defense	Details
Deprecated: NetFlow with FlexConfig.	Any	You can now configure threat defense devices as NetFlow exporters from the management center web interface. If you do this, you cannot deploy until you remove any deprecated FlexConfigs. See: Configure NetFlow
Deprecated: `high unmanaged disk usage` alerts.	7.0.6 7.2.4 7.4.0	The Disk Usage health module no longer alerts with `high unmanaged disk usage`. You may continue to see these alerts until you either deploy health policies to managed devices (stops the display of alerts), or upgrade the devices to Version 7.0.6, 7.2.4, or 7.4 (stops the sending of alerts). For information on the remaining Disk Usage alerts, see Disk Usage and Drain of Events Health Monitor Alerts.

August 3, 2023

Table 8: New Features: August 3, 2023

Feature	Description
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 20, 2023

Table 9: New Features: July 20, 2023

Feature	Description
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. Minimum threat defense: • 7.0.3 and later 7.0.x versions • 7.2 and later versions

June 8, 2023

Table 10: New Features: June 8, 2023

Feature	Description
EasyDeploy for Secure Firewall Threat Defense with AWS or Azure	You can now create and deploy a Secure Firewall Threat Defense device with either an AWS or Azure environment simultaneously. Onboard the device with Security Cloud Control and manage the environment in cloud-delivered Firewall Management Center. See Deploy a Threat Defense Device with AWS and Deploy a Threat Defense Device with an Azure VNet respectively for more information. Minimum threat defense: • 7.0.3 and later 7.0.x versions • 7.2 and later versions

May 25, 2023

Table 11: New Features: May 25, 2023

Feature	Description
Threat defense Version 7.3.1 support.	You can now manage threat defense devices running Version 7.3.1.

Feature	Description
Firepower 1010E.	You can now manage the Firepower 1010E, which does not support power over Ethernet (PoE), with cloud-delivered Firewall Management Center. Minimum threat defense: 7.2.3

March 9, 2023

This release introduces stability, hardening, and performance enhancements.

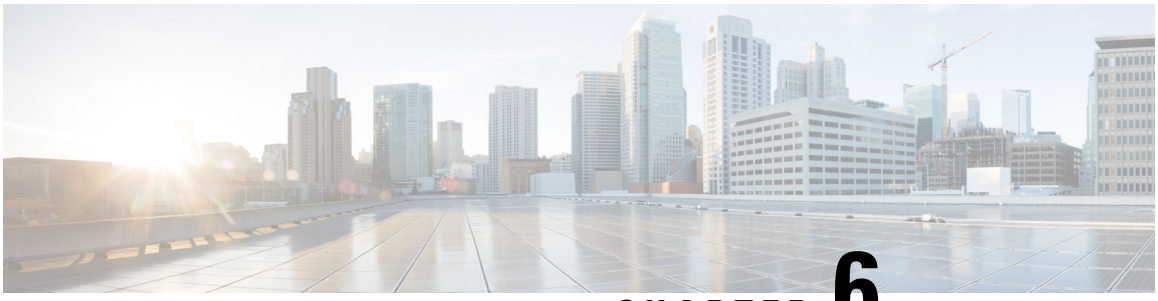
February 16, 2023

This release introduces stability, hardening, and performance enhancements.

January 18, 2023

Table 12: New Features: January 18, 2023

Feature	Description
Remote Access VPN	
Monitor remote access VPN sessions in CDO.	You can now use CDO to monitor RA VPN sessions on threat defense devices managed by the cloud-delivered Firewall Management Center. You can see a a list of active and historical sessions, as well as the details of the device and user associated with each session. Supported threat defense versions: • 7.0.3 and later 7.0.x versions • 7.2 and later versions For more information, see Monitor Remote Access VPN Sessions in the configuration guide.



CHAPTER 6

New Features in Cloud-delivered Firewall Management Center 2022

December 13, 2022

Table 13: New Features: December 13, 2022

Feature	Description
Onboarding to CDO and Threat Defense Upgrades	
Additional Device Support and Onboarding	You can now onboard clustered devices, AWS VPC environments, and Azure VNET environments to cloud-delivered Firewall Management Center. Onboarding these devices currently requires login credentials. Clustered devices must be already formed in their designated managing platform. See the following topics at https://docs.defenseorchestrator.com for more information: • Onboard a Cluster • Onboard a Device Associated with an AWS VPC. • Onboard an Azure VNet Environment

Feature	Description
Unattended Threat Defense Upgrade	The threat defense upgrade wizard now supports unattended upgrades, using a new Unattended Mode menu. You just need to select the target version and the devices you want to upgrade, specify a few upgrade options, and step away. You can even log out or close the browser. With an unattended upgrade, the system automatically copies needed upgrade packages to devices, performs compatibility and readiness checks, and begins the upgrade. Just as happens when you manually step through the wizard, any devices that do not "pass" a stage in the upgrade (for example, failing checks) are not included in the next stage. After the upgrade completes, you pick up with the verification and post-upgrade tasks. You can pause and restart unattended mode during the copy and checks phases. However, pausing unattended mode does not stop tasks in progress. Copies and checks that have started will run to completion. Similarly, you cannot cancel an upgrade in progress by stopping unattended mode; to cancel an upgrade, use the Upgrade Status pop-up, accessible from the Upgrade tab on Device Management page, and from the Message Center. See *Upgrade Threat Defense* in the Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center.
Auto-upgrade to Snort 3	When you upgrade threat defense to Version 7.3+, you can no longer disable the Upgrade Snort 2 to Snort 3 option. After the software upgrade, all eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. Although you can switch individual devices back, Snort 2 will be deprecated in a future release and we strongly recommend you stop using it now. For devices that are ineligible for auto-upgrade because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For migration assistance, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide.
CDO-managed Secure Firewall Threat Defense Devices on Firepower 4100/9300	The Firepower 4100/9300 is a flexible security platform on which you can install one or more logical devices. Before you can add the threat defense to the management center, you must configure chassis interfaces, add a logical device, and assign interfaces to the device on the Firepower 4100/9300 chassis using the Secure Firewall chassis manager or the FXOS CLI. You can now create a CDO-managed, standalone logical threat defense device on the Firepower 4100/9300, by configuring CDO as the manager when creating the device. See *Configure Logical Devices* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator
Interfaces	

Feature	Description
IPv6 DHCP Enhancements	The Dynamic Host Configuration Protocol (DHCP) provides network configuration parameters, such as IP addresses, to DHCP clients. The threat defense device can provide a DHCP server to DHCP clients attached to threat defense device interfaces. The DHCP server provides network configuration parameters directly to DHCP clients. The cloud-delivered Firewall Management Center now supports the following IPv6 addressing features for Secure Firewall Threat Defense devices: • DHCPv6 Address Client: Threat defense obtains an IPv6 global address and optional default route from the DHCPv6 server. • DHCPv6 Prefix Delegation Client: Threat defense obtains delegated prefix(es) from a DHCPv6 server. It can then use these prefixes to configure other threat defense interface addresses so that StateLess Address Auto Configuration (SLAAC) clients can auto-configure IPv6 addresses on the same network. • BGP router advertisement for delegated prefixes. • DHCPv6 Stateless Server: Threat defense provides other information such as the domain name to SLAAC clients when they send Information Request (IR) packets to threat defense. Threat defense only accepts IR packets and does not assign addresses to the clients. See *Configure IPv6 Addressing* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator for more information.
Support for Loopback Interface	A loopback interface is a software interface that emulates a physical interface. It is reachable through multiple physical interfaces with IPv4 and IPv6 addresses. You can configure a loopback interface for the redundancy of static and dynamic VTI VPN tunnels. See *Regular Firewall Interfaces* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.
Paired Proxy VXLAN for the Threat Defense Virtual for the Azure Gateway Load Balancer	You can configure a paired proxy mode VXLAN interface for the threat defense virtual in Azure for use with the Azure Gateway Load Balancer (GWLB). The threat defense virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy. See *Clustering for Threat Defense Virtual in a Public Cloud* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator to learn more.

Feature	Description
Redundant Manager Access Data Interface	You can now configure a secondary data interface to take over the management functions if the primary interface goes down, when using a data interface for manager access. The device uses SLA monitoring to track the viability of the static routes and an equal-cost multi-path (ECMP) zone that contains both interfaces so management traffic can use both interfaces. See *Configure a Redundant Manager Access Data Interface* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator for more information.
Remote Access VPN	
TLS 1.3 in Remote Access VPN	You can now use TLS 1.3 to encrypt remote access VPN connections. Use threat defense platform settings to specify that the device must use TLS 1.3 protocol when acting as a remote access VPN server. See *Platform Settings* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.
Site to Site VPN	
Support for Dynamic Virtual Tunnel Interface	You can create a dynamic VTI and use it to configure a route-based site-to-site VPN in a hub and spoke topology. Previously, you could use only a static VTI to configure a route-based site-to-site VPN in a hub and spoke topology. Dynamic VTI eases the configuration of peers for large enterprise hub and spoke deployments. A single dynamic VTI can replace several static VTI configurations on the hub. You can add new spokes to a hub without changing the hub configuration. See *Site-to-Site VPNs for Secure Firewall Threat Defense* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator
Routing	
Support for Bidirectional Forwarding Detection	Cloud-delivered Firewall Management Center now supports Bidirectional Forwarding Detection (BFD) configuration on Secure Firewall Threat Defense devices. BFD operates in a unicast, point-to-point mode on top of any data protocol being forwarded between two systems. However, in threat defense, BFD is supported on BGP protocols only. BFD configuration on the device includes creating templates and policies and enabling BFD support in the BGP neighbor settings. See *Bidirectional Forwarding Detection Routing* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator for more information.

Feature	Description
EIGRP (IPv4) routing support on Virtual Tunnel Interface	EIGRP (IPv4) routing is now supported on the Virtual Tunnel Interface. You can now use EIGRP (IPv4) protocol to share routing information and to route traffic flow over a VTI-based VPN tunnel between peers. See *Additional Configurations for VTI* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.
Virtual Tunnel Interface (VTI) Support for OSPF	The IPv4 or IPv6 OSPF can be configured on the VTI interface of a threat defense device. You can use OSPF to share routing information and route traffic through a VTI-based VPN tunnel between the devices. See *Site-to-Site VPNs for Secure Firewall Threat Defense* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.
Access Control and Threat Detection	
Decryption Policy	Feature renamed from *SSL policy* to *decryption policy* to better reflect what it does. We now enable you to configure a decryption policy with one or more **Decrypt - Resign** or **Decrypt - Known Key** rules at the same time. Get started by going to **Policies** > **Access Control** > **Decryption**. The Create Decryption Policy dialog box now has two tab pages: **Outbound Connections** and **Inbound Connections**. Use the **Outbound Connections** tab page to configure one or more decryption rules with a **Decrypt - Resign** rule action. (You can either upload or generate certificate authorities at the same time). Each combination of a CA with networks and ports results in one decryption rule. Use the Inbound Connections tab page to configure one or more decryption rules with a Decrypt - Known Key rule action. (You can upload your server's certificate at the same time.) Each combination of a server certificate with networks and ports results in one decryption rule.
Health Monitoring	
Cloud-delivered Firewall Management Center Deployment Notifications on CDO	CDO now notifies you about the status of deployments that are performed on the cloud-delivered Firewall Management Center. The notification messages include information on whether the deployment has succeeded, failed, or is in progress, the time and date of the deployment, and a link to the deployment history page of the cloud-delivered Firewall Management Center. See *Notifications* in Managing FDM Devices with Cisco Defense Orchestrator for more information.

Feature	Description
Cluster Health Monitor Settings	You can now edit cluster health monitor settings in the cloud-delivered Firewall Management Center web interface. If you configure these settings with the FlexConfig in a previous version, the system allows you to deploy, but also warns you to redo the configuration because the FlexConfig settings take precedence. See *Edit Cluster Health Monitor Settings* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator to learn more.
Improved Health Monitoring for Device Clusters	You can now use the health monitor for each cluster to view overall cluster status, load distribution metrics, performance metrics, cluster control link (CCL) and data throughput, and so on. See *Cluster Health Monitor* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator to learn more.
New Health Monitoring Alerts	The cloud-delivered Firewall Management Center now provides new health modules to monitor the temperature and power supply on a Firepower 4100/9300 chassis. Using the new Environment Status and Power Supply health modules, you can create a custom health dashboard and set threshold values for temperature and power supply on your physical appliance. See *Health Monitor Alerts* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator to learn more.
Licensing	
Carrier License	Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. The cloud-delivered Firewall Management Center now supports Carrier license, in addition to the existing smart licenses. The Carrier license allows GTP/GPRS, Diameter, SCTP, and M3UA inspection configurations. See *Licenses* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.
Usability, Performance, and Troubleshooting	

Feature	Description
Core Allocation Performance Profiles	The CPU cores on the Secure Firewall Threat Defense device are assigned to two of the main system processes: Lina and Snort. Lina handles VPN connections, routing, and other basic layer 3/4 processing. Snort provides advanced inspection, including intrusion and malware prevention, URL filtering, application filtering, and other features that require deep packet inspection. You can now adjust the percentage of system cores assigned to the data plane and Snort to adjust system performance, using the performance profiles. Based on your relative use of VPN and intrusion policies, you can choose a desired performance profile. See *Configure the Performance Profile* in Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator for more information.
Identity	
Proxy Sequence	A *proxy sequence* is one or more managed devices that can be used to communicate with an LDAP, Active Directory, or ISE/ISE-PIC server. It is necessary only if Security Cloud Control cannot communicate with your Active Directory or ISE/ISE-PIC server. (For example, Security Cloud Control 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. Create a proxy sequence by going to **Integration** > **Other Integrations** > **Realms** > **Proxy Sequence**.

October 20, 2022

Support for Configuring Next-Hop IP Addresses in a Policy-based Route Map

Policy-Based Routing (PBR) helps route network traffic for specified applications based on your priorities, such as source port, destination address, destination port, protocol, applications, or a combination of these objects, rather than by destination network criteria. For example, you can use PBR to route your high-priority network traffic over a high-bandwidth, expensive link and your lower priority network traffic over a lower bandwidth, lower cost link.

The cloud-delivered Firewall Management Center now supports defining next-hop IP addresses when creating a policy-based route map. See *About Policy Based Routing* and *Configure Policy-Based Routing Policy* in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator for more information.

URL Filtering Enhancements

URL filtering lets you control access to websites that the users on your network can use. You can filter websites based on category and reputation, for which your device needs a URL-filtering license, or manually by specifying URLs. The category and reputation-based filtering—the quicker and smarter way to filter URLs—uses Cisco's up-to-date threat intelligence information and is highly recommended.

The cloud-delivered Firewall Management Center can now query for up-to-date URL category and reputation information directly from the Cisco Talos cloud instead of using the local database information. The local database gets updated every 24 to 48 hours. See *URL Filtering Options* in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator for detailed information.

Umbrella Tunnel Integration with Secure Firewall Threat Defense using Cloud-delivered Firewall Management Center

You can now automatically deploy IPsec IKEv2 tunnels to Umbrella from a threat defense device using cloud-delivered Firewall Management Center. This tunnel forwards all internet-bound traffic to the Umbrella Secure Internet Gateway (SIG) for inspection and filtering. Create a SASE topology, a new type of static VTI-based site-to-site VPN topology, using a simple wizard to configure and deploy the Umbrella tunnels.

See *About Umbrella SASE Topology* in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator for more information.

Support for Remote Access VPN Policy in FTD to Cloud Migration

CDO now imports the remote access VPN policy during the migration of the FTD to cloud.

See *Migrate FTD to Cloud* in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator for more information.

Migrate Flex Configured Routing Policies

Cloud-delivered Firewall Management Center now supports the migration of Flex configured ECMP, VxLAN, and EIGRP policies using the Migration Config option in the user interface.

See *Migrating FlexConfig Policies* in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator for more information.

Smart Licensing Standardization

The license names used by cloud-delivered Firewall Management Center have been changed.

Table 14: Smart License Name Changes

Old Name	is now	New Name
Base	is now	Essentials
Threat	is now	IPS
Malware	is now	Malware Defense
RA VPN/AnyConnect License	is now	Cisco Secure Client
AnyConnect Plus	is now	Secure Client Advantage

Old Name	is now	New Name
AnyConnect Apex	is now	Secure Client Premier
AnyConnect Apex and Plus	is now	Secure Client Premier and Advantage
AnyConnect VPN Only	is now	Secure Client VPN Only

See *License Types and Restrictions* in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator for more information.

June 9, 2022

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