

What's New for Security Cloud Control

First Published: 2021-04-16

Last Modified: 2026-10-20

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 –2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

PART I **Security Cloud Control - New Features** 7

CHAPTER 1 **New Features in 2026** 1

- September 2026 1
  - September 17, 2026 1
  - September 10, 2026 2
  - September 3, 2026 2
- August 2026 2
  - August 6, 2026 2
- July 2026 3
  - July 31, 2026 3
  - July 23, 2026 3
  - July 16, 2026 4
- June 2026 4
  - June 04, 2026 4
- May 2026 4
  - May 07, 2026 4
- April 2026 4
  - April 23, 2026 4
- March 2026 5
  - March 26, 2026 5
  - March 19, 2026 5
  - March 12, 2026 6
- February 2026 6
  - February 19, 2026 6
  - February 05, 2026 6

January 2026 7
January 29, 2026 7

CHAPTER 2 New Features in 2025 9
December 2025 9
December 12, 2025 9
December 04, 2025 9
November 2025 10
November 20, 2025 10
November 13, 2025 10
November 06, 2025 10
October 2025 11
October 23, 2025 11
September 2025 11
September 18, 2025 11
August 2025 12
August 28, 2025 12
August 21, 2025 12
August 14, 2025 12
July 2025 13
July 24, 2025 13
July 3, 2025 13
June 2025 14
June 12, 2025 14
April 2025 15
April 23, 2025 15
April 10, 2025 15
March 2025 15
March 13, 2025 15
March 6, 2025 15

CHAPTER 3 New Features in 2024 17
December 2024 17
December 12, 2024 17

December 5, 2024 18
November 2024 18
Welcome to Security Cloud Control 18
November 21, 2024 19
November 7, 2024 19
October 2024 19
October 17, 2024 19
September 2024 19
September 13, 2024 19
September 5, 2024 20
August 2024 20
August 23, 2024 20
August 8, 2024 21
June 2024 22
June 27, 2024 22
June 20, 2024 22
June 13, 2024 22
June 6, 2024 23
May 2024 23
May 30, 2024 23
May 23, 2024 24
May 16, 2024 25
April 2024 25
April 25, 2024 25
April 18, 2024 25
March 2024 25
March 07, 2024 25
February 2024 26
February 13, 2024 26
January 2024 26
January 25, 2024 26

CHAPTER 4 **Feature Highlights of 2023** 27
December 2023 27

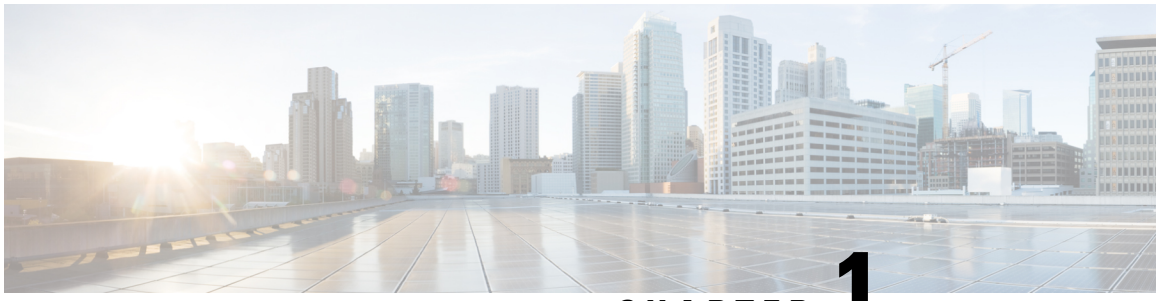
December 14, 2023 27
December 07, 2023 27
November 2023 28
November 30, 2023 28
November 14, 2023 28
November 2, 2023 29
October 2023 30
October 26, 2023 30
October 19, 2023 30
October 12, 2023 30
October 05, 2023 31
September 2023 32
September 14, 2023 32
September 7, 2023 32
August 2023 34
August 31, 2023 34
August 17, 2023 34
August 3, 2023 35
July 2023 35
July 20, 2023 35
July 13, 2023 36
June 2023 36
June 29, 2023 36
June 15, 2023 36
June 8, 2023 36
June 5, 2023 37
June 1, 2023 37
April 2023 37
April 27, 2023 37
March 2023 38
March 23, 2023 38
January 2023 38
January 18, 2023 38



PART I

Security Cloud Control - New Features

- New Features in 2026, on page 1
- New Features in 2025, on page 9
- New Features in 2024, on page 17
- Feature Highlights of 2023, on page 27



CHAPTER 1

New Features in 2026

These are the new Firewall features deployed in Security Cloud Control in 2026.

- September 2026, on page 1
- August 2026, on page 2
- July 2026, on page 3
- June 2026, on page 4
- May 2026, on page 4
- April 2026, on page 4
- March 2026, on page 5
- February 2026, on page 6
- January 2026, on page 7

September 2026

September 17, 2026

Introducing Policy Change Impact Analyzer in AgenticOps

AgenticOps now includes Policy Change Impact Analyzer, helping you assess the potential impact of pending access-control policy changes before deployment. Analyze affected devices, rules, traffic segments, historical connection activity, and inferred impacts to identify possible threat exposure, service disruption, access expansion, or improved security posture.

Policy Change Impact Analyzer is available for deployments in the US, EU, and AUS regions. For more information, see About policy change impact insights.

Introducing Compliance Posture in AgenticOps

AgenticOps now includes Compliance Posture, a capability that evaluates firewall configurations against PCI DSS 4.0.1 requirements. Identify configuration gaps and potential policy issues, generate detailed compliance reports for your devices, and review findings and remediation recommendations to prioritize corrective actions.

Compliance Posture is available for deployments in the US, EU, and AUS regions. For more information, see About compliance insights.

Introducing Agent Workforce

Agent Workforce is now available in Security Cloud Control. It provides specialized agents that help you analyze firewall data, troubleshoot site-to-site VPN connectivity, and remediate high-bandwidth traffic affecting firewall performance and stability.

- **Firewall insight agent**: Analyzes firewall inventory, configurations, policies, routing, and device status.
- **VPN agent**: Troubleshoots site-to-site VPN connectivity, routing, and traffic-flow issues.
- **Elephant flow agent**: Remediates high-bandwidth traffic flows affecting firewall performance and stability.

Agent Workforce capabilities are available for deployments in the US, EU, and AUS regions. For more information, see Agent Workforce.

September 10, 2026

Secure Client upgrades for ASA Remote Access VPN

Security Cloud Control now supports Cisco Secure Client package upgrades for ASA Remote Access VPN headends. This support extends centralized upgrade capabilities to ASA RA VPN deployments, including guided upgrade workflows, multi-device package deployment, visibility into currently installed Secure Client packages, compatibility-based version selection, platform-specific package targeting for Windows, macOS, and Linux, and real-time upgrade status monitoring from the Upgrades page.

For more information, see Upgrade ASA Secure Client packages.

September 3, 2026

Security Cloud Control Firewall Management automation tools and AI skills

Manage and automate Security Cloud Control Firewall Management using a simple CLI and Cisco Ansible collection. Built in AI skills help coding agents find the right commands and modules, validate inputs, handle authentication safely, and verify results. This makes Firewall Management workflows faster, safer, and easier to automate.

For more information, see Automation tools and AI agents.

August 2026

August 6, 2026

Software Upgrade Planner now highlights bugs impacting your device

Software Upgrade Planner now separates bugs into **Impacting bugs** and **Other bugs** on the device details page. Impacting bugs are identified as affecting the selected device and its environment. This helps you focus on the bugs most relevant to the device when reviewing software upgrade options.

For more information, see Manage software upgrades.

Updates to Cloud-Delivered Firewall Management Center

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Read the Release Notes for Cloud-Delivered Firewall Management Center for more information.

July 2026

July 31, 2026

NAT policy anomaly analysis for Firewall Threat Defense devices

Policy Analyzer and Optimizer now provides visibility into Network Address Translation (NAT) policy anomalies for Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center or On-Premises Firewall Management Center. This feature enables users to identify shadowed and redundant NAT rules, analyze anomaly details, and generate comprehensive PDF reports for audit and compliance.

For more information, see Network Address Translation policy analysis.

July 23, 2026

Introducing Capacity and Trend Analyzer

Capacity and Trend Analyzerhelps you proactively monitor infrastructure health by analyzing CPU, memory, throughput, and connection trends. Use anomaly detection and predictive forecasting to identify potential capacity risks, receive alerts for threshold breaches, and plan for future resource demands.

For more information, see Capacity and Trend Analyzer.

AgenticOps support for On-Premises Firewall Management Center

AgenticOps now supports Firewall Threat Defense devices managed by an On-Premises Firewall Management Center integrated with Cisco Security Cloud. This support extends AgenticOps features, including Capacity and Trend Analyzer, Software Upgrade Planner, Best Practices and Recommendations, and Feature Adoption, to your on-prem managed devices.

For information about supported versions of the On-Premises Firewall Management Center, see AgenticOps Support for On-Prem Firewall Management Center

Enhanced Software Upgrade Planner with remediation guidance and threat campaign insights

Software Upgrade Planner now provides remediation guidance with AI-generated summaries for security vulnerabilities and bugs, helping you understand root causes, available workarounds, and remediation guidance. It also highlights active threat campaigns affecting your devices and links to Cisco Talos Intelligence resources for additional context, enabling you to make more informed upgrade decisions.

For more information, see About software upgrade insights.

July 16, 2026

Monitor Security Analytics and Logging (SaaS) service status from Security Cloud Control

The Security Analytics and Logging (SaaS) service status monitoring option in the **Event Logging** page provides you with direct visibility into Security Analytics and Logging (SaaS) service availability from Security Cloud Control. You can monitor service availability, verify whether managed Firewall Threat Defense devices are sending events, and check the last received event details to identify possible ingestion delays or disruptions faster.

For more information, refer to Monitor Security Analytics and Logging (SaaS) service availability.

June 2026

June 04, 2026

Updates to Cloud-Delivered Firewall Management Center

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Refer to the Release Notes for Cloud-Delivered Firewall Management Center for more information.

May 2026

May 07, 2026

Multitenant Device Upgrades Now Available for ASAs

You can now bulk upgrade ASAs across multiple tenants in addition to performing bulk upgrades for Cloud-Delivered Firewall Management Center-managed Secure Firewall Threat Defense devices.

For more information, see About Multitenant Device Upgrades in MSSP Portal.

April 2026

April 23, 2026

Simplify Your Multicloud Security Setup with Cloud Deployment

The new Cloud Deployment feature streamlines the configuration of Firewall Threat Defense Virtual (FTDv) and Multicloud Defense across Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP). Additionally, Oracle Cloud Infrastructure (OCI) is supported in this release by Multicloud Defense gateway only. This guided configuration tool helps you select and launch the optimal enforcement point for your specific use case, ensuring high performance and scalable network security in complex multicloud environments.

With its simplified, step-by-step setup, Cloud Deployment lets you define account settings, traffic flows, and architectural requirements with ease.

For more information, see Cloud Deployment.

Updates to Cloud-Delivered Firewall Management Center

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Refer to the Release Notes for Cloud-Delivered Firewall Management Center for more information.

March 2026

March 26, 2026

Firewall MSP Portal Now Integrated into Security Cloud Control

The Managed Service Provider (MSP) portal is now fully integrated into Security Cloud Control's Multi-Org experience. This unified platform empowers managed service providers to efficiently manage multiple customer organizations from a single, centralized interface.

Key capabilities include:

- Centralized management: Seamlessly manage multiple customer organizations within one portal.
- Comprehensive monitoring: Monitor device health, configurations, and connectivity status across all managed environments.
- Bulk upgrades: Perform upgrades on Secure Firewall Threat Defense devices managed by the Cloud-delivered Firewall Management Center (cdFMC) across all tenants.
- Enhanced visibility: Access detailed, consolidated information for all managed firewall organizations.

What this means for you:

- Access: Use the new portal directly from security.cisco.com.
- Legacy Portal Retirement: The previous MSP portal will be retired soon.
- Support: Going forward, support will be provided exclusively for the integrated Security Cloud Control platform.

For more information, see Overview of Security Cloud Control Firewall Management for Managed Service Providers.

March 19, 2026

Updates to Cloud-Delivered Firewall Management Center

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Refer to the Release Notes for Cloud-Delivered Firewall Management Center for more information.

March 12, 2026

New Smart Licensing Dashboard

Smart Licensing Dashboard has been introduced in Cisco Secure Firewall. This dashboard offers a unified view of license usage, license types, and compliance status, helping you ensure that your devices are licensed and remain compliant. This feature is currently available in limited release. To request access to this limited release feature, please contact your account team or Cisco representative.

For more information, see Overview of Smart Licensing Dashboard.

New Smart Licensing Dashboard for MSSP Portal

Smart Licensing Dashboard has been introduced in the MSSP Portal for Cisco Secure Firewall. This dashboard offers a unified view of license usage, license types, and compliance status, helping you ensure that your devices are licensed and remain compliant. This feature is currently available in limited release. To request access to this limited release feature, please contact your account team or Cisco representative.

For more information, see Overview of Smart Licensing Dashboard.

February 2026

February 19, 2026

New Smart Licensing Dashboard

Smart Licensing Dashboard has been introduced in Cisco Secure Firewall. This dashboard offers a unified view of license usage, license types, and compliance status, helping you ensure that your devices are licensed and remain compliant. This feature is currently available in limited release. To request access to this limited release feature, please contact your account team or Cisco representative.

For more information, see Overview of Smart Licensing Dashboard.

February 05, 2026

Introducing Application Insights

AIOps now features **Application Insights**, which uses ThousandEyes Internet Insights to proactively detect cloud application outages. It shows affected applications, impacted domains, outage duration, and affected regions for the monitored applications.

For more information, see Detect Application Outages.

January 2026

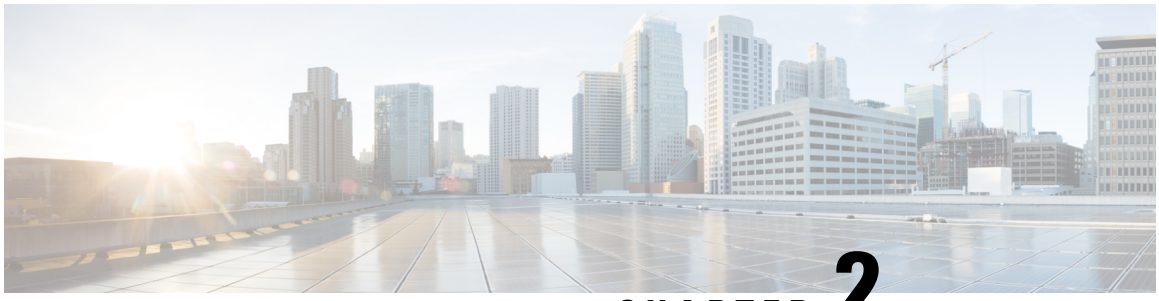
January 29, 2026

Multitenant Device Upgrades in MSSP Portal

With the new upgrades view in the MSSP portal, you can now bulk upgrade Secure Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center (cdFMC) across multiple tenants.

For more information, see About Multitenant Device Upgrades in MSSP Portal.

January 29, 2026



CHAPTER 2

New Features in 2025

These are the new Firewall features deployed in Security Cloud Control in 2025.

- December 2025, on page 9
- November 2025, on page 10
- October 2025, on page 11
- September 2025, on page 11
- August 2025, on page 12
- July 2025, on page 13
- June 2025, on page 14
- April 2025, on page 15
- March 2025, on page 15

December 2025

December 12, 2025

Updates to Cloud-Delivered Firewall Management Center

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Refer to the Release Notes for Cloud-Delivered Firewall Management Center for more information.

Introducing Security Insights in AIOps

In this release, we have introduced **Security** insights to provide visibility into suspicious activities across your organization. You can now identify and respond to evolving security risks, such as **User Risk Spike**, which indicates escalating trust levels and other suspicious user behavior.

See Security Insights.

December 04, 2025

New Health Dashboard for MSSP Portal

In this release, a Health dashboard is introduced for Secure Firewall ASA devices.

This dashboard displays critical performance indicators such as CPU, memory, disk usage, and interface statistics. You can now detect performance bottlenecks early and take proactive actions to maintain optimal operations.

For more information, see About Health Dashboard in the MSSP Portal.

November 2025

November 20, 2025

Updates to Cloud-Delivered Firewall Management Center

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Refer to the Release Notes for Cloud-Delivered Firewall Management Center for more information.

November 13, 2025

MSSP Device Upgrades Using Public APIs

Security Cloud Control Firewall Management now provides new API endpoints for MSSPs to upgrade Cisco Secure Firewall Threat Defense devices across their tenants. An MSSP portal is required for this.

For more information, see Security Cloud Control Firewall Management API Documentation.

November 06, 2025

Security Cloud Control Now Manages Catalyst SD-WAN NGFW features

Security Cloud Control now integrates with Catalyst SD-WAN Manager, enabling you to centrally manage next-generation firewall (NGFW) features, including security policies and objects managed by Catalyst SD-WAN Manager.

With Security Analytics and Logging, you gain visibility into network activity, making it easy to monitor, analyze, and respond to security events. You can also view allowed and blocked intrusion and malware events detected in your network.

For more information, see Managing Cisco Catalyst SD-WAN Firewall Capabilities with Security Cloud Control.

Introducing Tiered Subscription Model for Cisco Security Analytics and Logging

In this release, we have updated Cisco Security Analytics and Logging licensing to offer a new tiered subscription model. This new structure provides a longer default retention period, starting at 1 year, and increased storage options up to 10 TB. You can choose from Essentials, Advantage, or Premier tiers to match your specific needs. This update simplifies pricing and provides you with greater flexibility and value in managing your firewall logs.

For more information, see Cisco Security Analytics and Logging Licenses.

October 2025

October 23, 2025

CLI Support for Firewall Threat Defense Devices Managed by Cloud-delivered Firewall Management Center

You can now access the CLI of Firewall Threat Defense devices managed by Cloud-delivered Firewall Management Center, through the Security Cloud Control interface. Navigate to **Security Devices** > **FTD**, select the FTD, and choose **Command Line Interface** on the right pane.

See Use the Security Cloud Control Command Line Interface Tool for more information.

September 2025

September 18, 2025

Introducing New AIOps Capabilities

AIOps brings AI-driven intelligence to firewall management, delivering proactive insights and actionable guidance to simplify operations and strengthen security.

New capabilities include:

- AIOps Summary Dashboard: A unified view that consolidates insights, giving you a clear snapshot of your device's performance.
- Best Practices and Recommendations: Detailed assessments that highlight deviations from best practices and provide remediation guidance.
- Feature Adoption: Visibility into actively used features categorized by licenses, adoption rates across the tenant, and guidance to improve utilization.
- Software Upgrade Planner: Suggestions on the most suitable upgrade versions for Secure Firewall Threat Defense devices, including visibility into resolved bugs and security vulnerabilities, to streamline upgrade decisions.

These enhancements add to the existing capabilities such as the Policy Analyzer and Optimizer, positioning AIOps as the central hub for proactive and efficient firewall management.

Introducing Device Health Metrics for Secure Firewall ASA Devices

In this release, we have introduced the Device Health Metrics for Secure Firewall ASAdevices. The dashboard displays critical performance indicators such as CPU, memory, disk usage, fan status, and interface statistics. With this visibility, you can detect performance bottlenecks and take proactive action to maintain optimal operations.

For more information, refer to Device Health Metrics.

August 2025

August 28, 2025

CLI Templates now available in Security Cloud Control

You can now manage and export CLI templates as .txt files for configuring new devices. To access CLI templates, click **Administration** in the left pane and choose **Integrations** > **CLI Templates**.

For more information, refer to Manage CLI Templates.

Hardware End-of-Life Filter

You can now filter devices on the **Security Devices** page to identify hardware that is nearing or has passed its last date of support. The detailed view also provides recommended replacement devices to assist with lifecycle planning.

For more information, refer to Security Devices.

August 21, 2025

Security Cloud Control notifications in Microsoft Teams

To get Security Cloud Control notifications in Microsoft Teams, generate an incoming webhook in Teams and enter the webhook URL in Security Cloud Control (**Administration** > **Notification Settings**).

For more information, refer to Incoming Webhooks for Microsoft Teams.

August 14, 2025

Updates to Cloud-Delivered Firewall Management Center

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Refer to the Release Notes for Cloud-Delivered Firewall Management Center for more information.

Universal Zero Trust Network Access (universal ZTNA)

Security Cloud Control released the Universal Zero Trust Network Access (universal ZTNA) feature. Universal ZTNA is a comprehensive solution that provides secure access to internal network resources based on user identity, trust, and posture. It ensures that access to one application does not implicitly grant access to the entire network, as with remote access VPN. Enable universal ZTNA using **Policies** > **Zero Trust Application**. For more information, refer to Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control.

July 2025

July 24, 2025

MSSP Portal: Enhanced Pagination and Sorting of Security Devices

The **Security Devices** page in the MSSP portal now includes dedicated tabs for **Devices**, **Cloud Services**, **Templates**, and **Firewall Managers**. This enhancement improves page performance and streamlines pagination and filtering, enabling a more efficient management of your security assets.

For more information, refer to Security Devices Details.

Updates to Security Cloud Control Firewall Manager APIs

The Security Cloud Control Firewall Manager APIs have been updated to add multiple new API endpoints to collect and view health metrics for ASA devices and view MSSP portal inventory.

Updates to the Event Log Search Feature

The **Background Search** button in the **Event Logging** page has been renamed to **Reports**. The button's functionality remains the same, allowing you to perform event log searches in the background and manage generated reports.

For more information, refer to Search Historical Events in the Background.

Updates to the Cloud-Delivered Firewall Management Center Device Backups

From the next upgrade of Cloud-Delivered Firewall Management Center, only the five most recent Firewall Threat Defense backups will be retained; all older backups will be automatically deleted.

In the event that you have not downloaded the required backups to your private environment following our announcement on May 1, 2025, download the necessary backups before July 31, 2025, to ensure continuous access to your data.

See Restore a Firewall Firewall Threat Defense device for information on how to download device backups.

July 3, 2025

Updates to Cloud-Delivered Firewall Management Center

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Refer to the Release Notes for Cloud-Delivered Firewall Management Center for more information.

Enhanced Event Searching with Sample Filters

In this release, we've introduced sample filters in the Event Logging page to enhance your search experience. These filters instantly populate the search bar with common search queries. This reduces the need to manually type search queries. Simply select a sample filter and edit the search parameters to suit your specific needs.

For more information, refer to Use Sample Filters to Search Events.

Updates to Firewall Migration Tool

Security Cloud Control released an updated version of the Secure Firewall Migration Tool. The key updates include Azure firewall migration to Firewall Threat Defense, Checkpoint and Fortinet firewall migrations to Multicloud Defense, simplified policy management, and more. Refer to Cisco Secure Firewall Migration Tool Release Notes for more information.

June 2025

June 12, 2025

Cisco Security Cloud Control Integrated Platform is Now Available

We are excited to announce the migration of Cisco Security Cloud Control tenants from APJ, AUS, the EU, India, and the U.S. to the Cisco Security Cloud Control integrated platform.

To access the Security Cloud Control integrated platform, go to https://security.cisco.com/ and navigate to **Products > Firewall** from the homepage.

Note that you can continue to access all your current firewall settings and configurations from the **Firewall** dashboard in the Security Cloud Control integrated platform.

Simplified Site-to-Site VPN Wizard

The Security Cloud Control now features an enhanced, consolidated wizard designed to simplify and accelerate the creation of site-to-site VPN tunnels. With this intuitive, step-by-step guided wizard, you can seamlessly configure and manage multiple VPN connections in just a few clicks. The VPN tunnel creation is supported for Secure Firewall ASA, Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense, Multicloud Defense, and extranet devices, providing a centralized and streamlined approach to VPN management.

For more information, see Introduction to Site-to-Site Virtual Private Network.

New Widgets in Storage Utilization Dashboard

We've introduced new widgets to help you identify logging trends and manage storage effectively. Note that these widgets are available only if you are using the optimized version of SAL event logging.

- EPS Trends for tracking event ingest rates.
- Utilization by Event Type and Device Type Trends for monitoring storage usage patterns.
- Utilization by Device Trends, which highlights storage usage of the top devices.

For more information, see View Security Analytics and Logging Storage Usage and Event Ingest Rate.

April 2025

April 23, 2025

End-of-Support announcement for Secure Firewall Threat Defense Version 7.0.*x* devices managed by Cloud-Delivered Firewall Management Center

Starting October 22, 2025, Cloud-Delivered Firewall Management Center will no longer support the management of Secure Firewall Threat Defense devices running Version 7.0.*x*. You are required to upgrade to at least Version 7.2.*x* (Cisco-suggested version is 7.4.2) before October 22, 2025, to ensure continued protection and access to the latest features.

From October 22, 2025, you will not be able to make or deploy changes to Secure Firewall Threat Defense devices running Version 7.0.*x*, except to upgrade or unregister.

For more information, see Frequently Asked Questions.

April 10, 2025

Best Practices and Recommendations in AIOps

The **Best Practices and Recommendations** feature runs assessments on your devices, highlights failed checks, and generates detailed reports. It recommends corrective actions to help you align with Cisco Secure Firewall best practices and enhance overall performance.

For more information, see Implement Best Practices and Recommendations.

March 2025

March 13, 2025

Updates to Cloud-Delivered Firewall Management Center

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Refer to the Release Notes for Cloud-Delivered Firewall Management Center for more information.

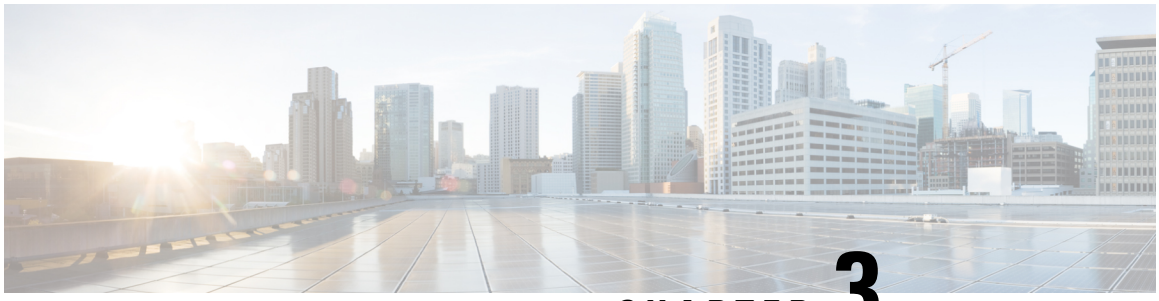
March 6, 2025

Updates to Firewall Migration Tool

Security Cloud Control released an updated version of the Firewall Migration Tool. The new features include migrating configurations from Secure Firewall ASA and Palo Alto Networks firewall to Multicloud Defense.

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

March 6, 2025



CHAPTER 3

New Features in 2024

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

- December 2024, on page 17
- November 2024, on page 18
- October 2024, on page 19
- September 2024, on page 19
- August 2024, on page 20
- June 2024, on page 22
- May 2024, on page 23
- April 2024, on page 25
- March 2024, on page 25
- February 2024, on page 26
- January 2024, on page 26

December 2024

December 12, 2024

Updates to Cloud-Delivered Firewall Management Center

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Refer to the Release Notes for Cloud-Delivered Firewall Management Center for more information.

Cloud-Delivered Firewall Management Center Evaluation License Updates

The Cloud-Delivered Firewall Management Center now offers a 90-day evaluation license. After this period, you can still onboard Firewall Threat Defense devices, but deployments are blocked until the Cloud-Delivered Firewall Management Center is registered with Cisco Smart Software Manager. You'll receive alert notifications on Security Cloud Control when the evaluation period nears expiration.

See Cloud-Delivered Firewall Management Center Licenses for more information.

December 5, 2024

Secure Device Connector and Secure Event Connector Now Maintained on Ubuntu VM

Security Cloud Control has deprecated the use of CentOS 7 for the on-premises Secure Device Connector (SDC) and Secure Event Connector (SEC) because CentOS 7 has reached its end-of-life status. The SDC and SEC are now installed and maintained on an Ubuntu VM. Migrating your SDC and SEC to Ubuntu ensures that you receive updates to those applications.

For more information about the migration process, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

November 2024

Welcome to Security Cloud Control

Cisco Defense Orchestrator is now "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 Firewall 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 21, 2024

Share Event Data With Cisco Talos

You can now enable or disable the sharing of event data with Cisco's threat intelligence group, Talos. Sharing event data helps Talos improve its threat detection and response capabilities, allowing it to provide more targeted security insights for your network. This feature is enabled by default. Click **Administration** > **General Settings** to change this setting.

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

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Refer to the Release Notes for Cloud-Delivered Firewall Management Center for more information.

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

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Refer to the Release Notes for Cloud-Delivered Firewall Management Center for more information.

Highlights include:

Platform

- Firewall 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

- Firewall 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.

Firewall Management Center REST API

- Updates to Firewall 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 Firewall 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 Firewall 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 Firewall Threat Defense to Cloud-Delivered Firewall Management Center Migration to Review Imported Shared Policies

You can now pause the Firewall 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 Firewall 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 Firewall 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

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Refer to the Release Notes for Cloud-Delivered Firewall Management Center for more information.

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 Firewall Threat Defense device. In addition, you can migrate DHCP, DDNS, and SNMPv3 configurations from an FDM-managed device to a Firewall 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 Firewall Threat Defense Devices From Sending Event Logs to the Cisco Cloud

You can now disable individual Cloud-Delivered Firewall Management Center-managed Firewall 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 Firewall Threat Defense devices from sending event logs sent to the cloud, if required. To specify which Firewall Threat Defense devices are to be disabled from sending event logs to the Cisco cloud, click **Inventory**, select the corresponding Firewall 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

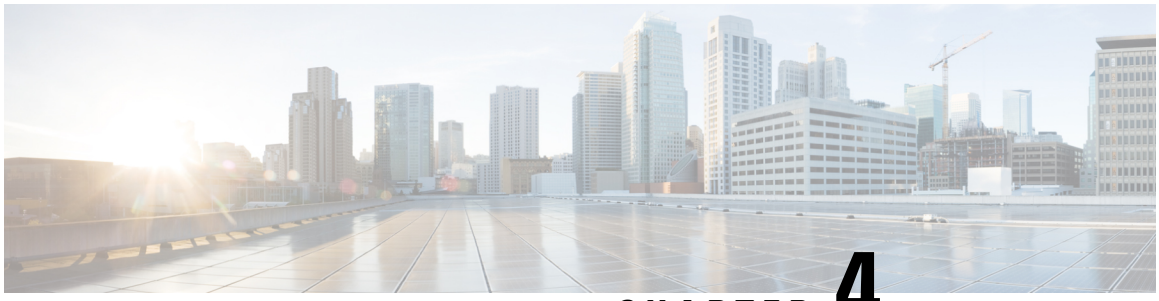
Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Refer to the Release Notes for Cloud-Delivered Firewall Management Center for more information.

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.



CHAPTER 4

Feature Highlights of 2023

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

- December 2023, on page 27
- November 2023, on page 28
- October 2023, on page 30
- September 2023, on page 32
- August 2023, on page 34
- July 2023, on page 35
- June 2023, on page 36
- April 2023, on page 37
- March 2023, on page 38
- January 2023, on page 38

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 Firewall 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.

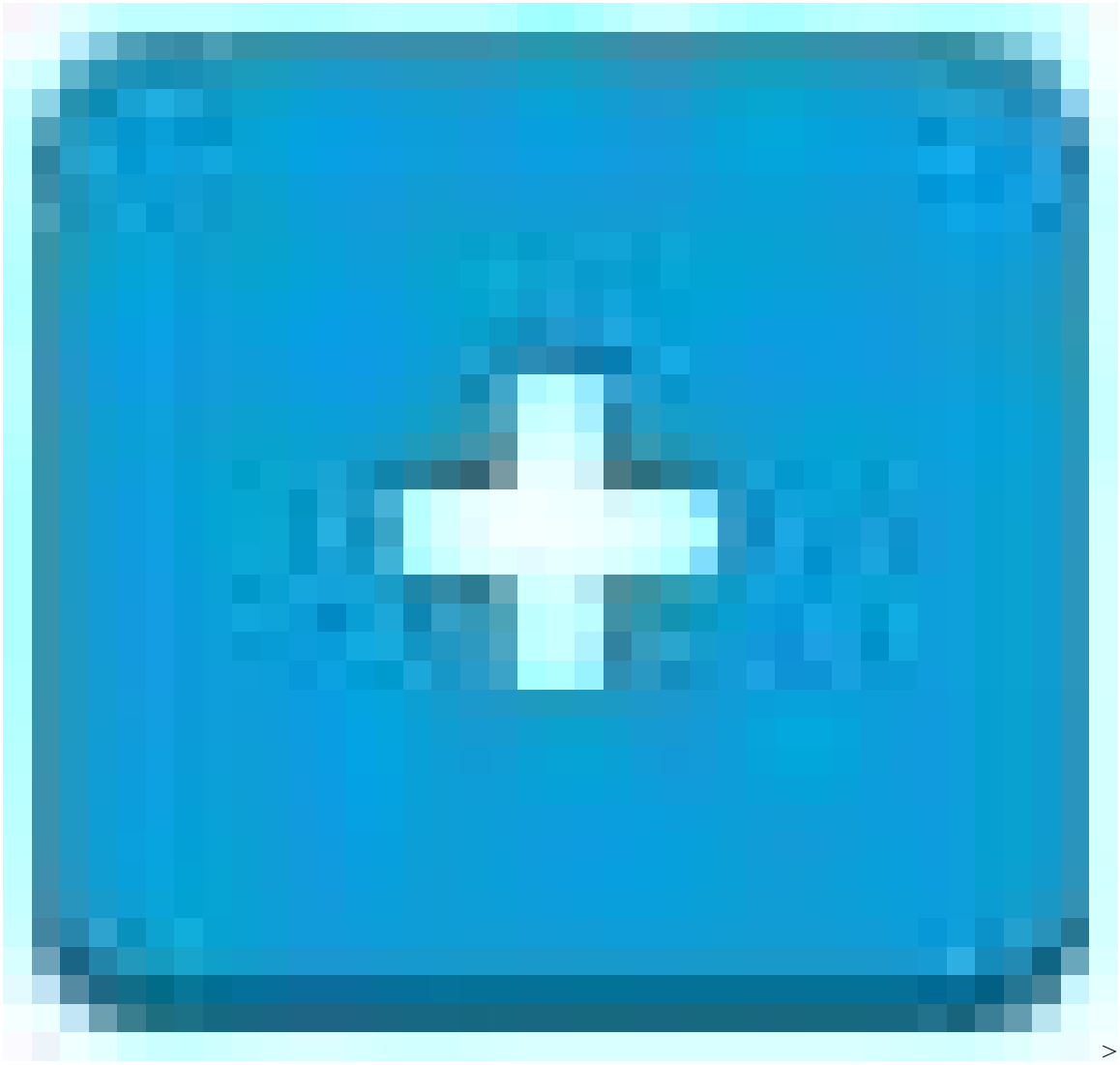
See Schedule Remote Device Backups for more information.

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 Firewall 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

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Refer to the Release Notes for Cloud-Delivered Firewall Management Center for more information.

Migrate 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 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.

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**.

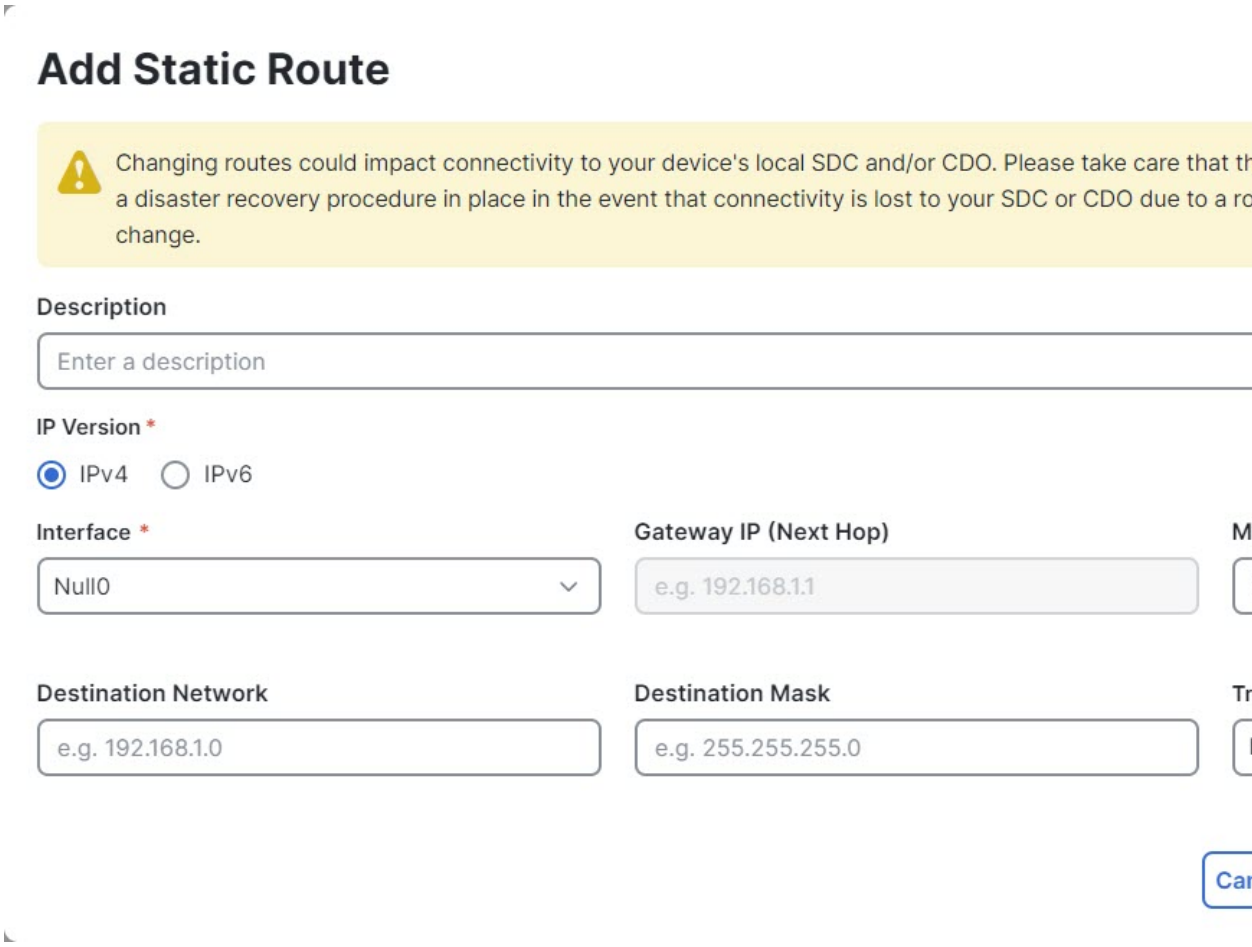
October 05, 2023

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

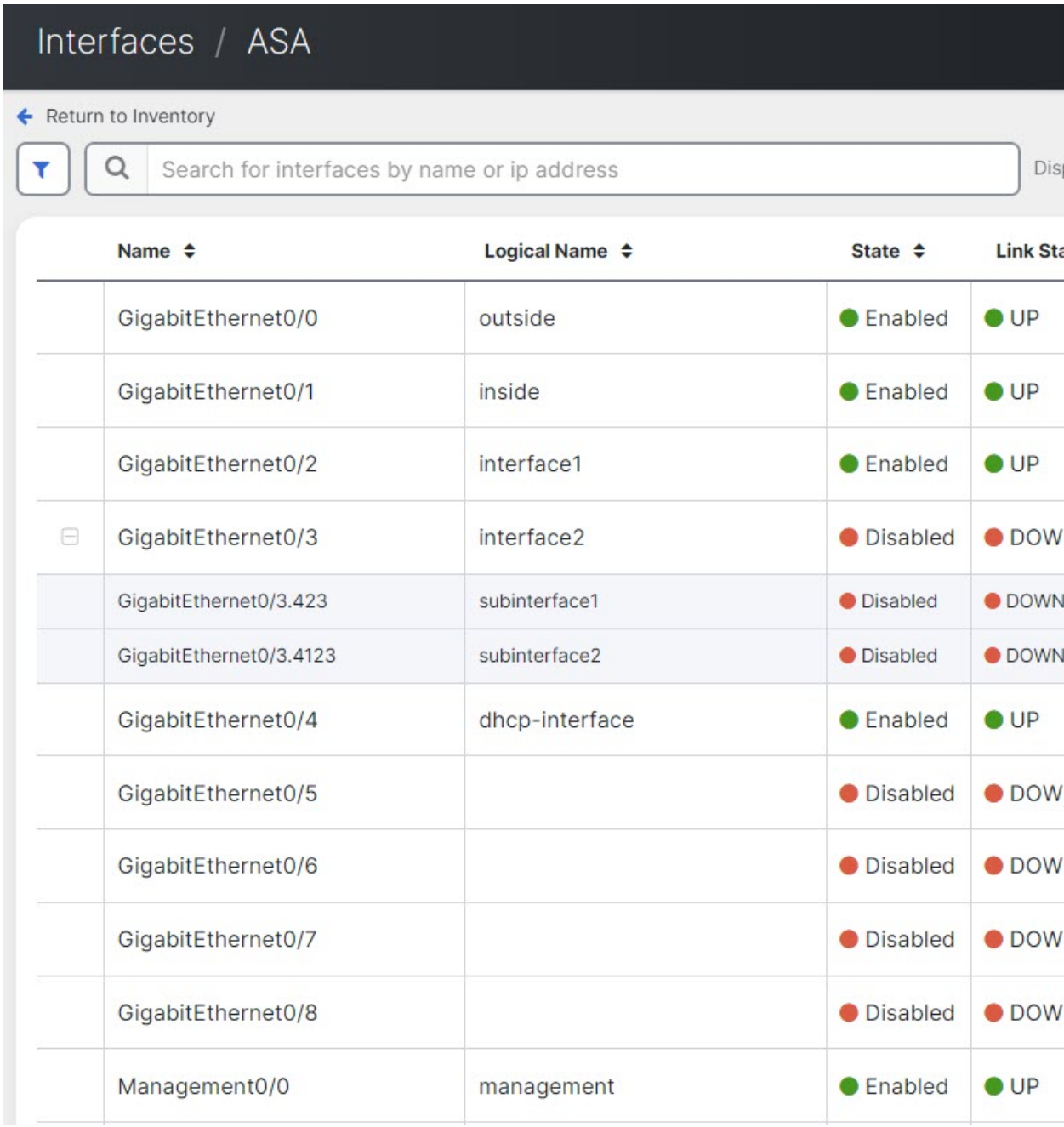
Configure ASA Interfaces using CDO User Interface

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**.

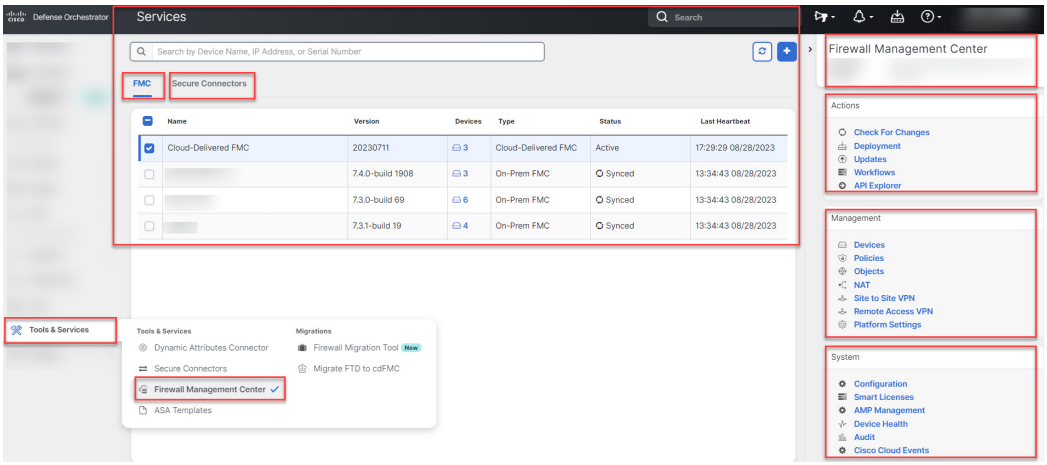

Interfaces / ASA
Return to Inventory
Search for interfaces by name or ip address
Name
Logical Name
State
Link Sta
GigabitEthernet0/0
outside
Enabled
UP
GigabitEthernet0/1
inside
Enabled
UP
GigabitEthernet0/2
interface1
Enabled
UP
GigabitEthernet0/3
interface2
Disabled
DOW
GigabitEthernet0/3.423
subinterface1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

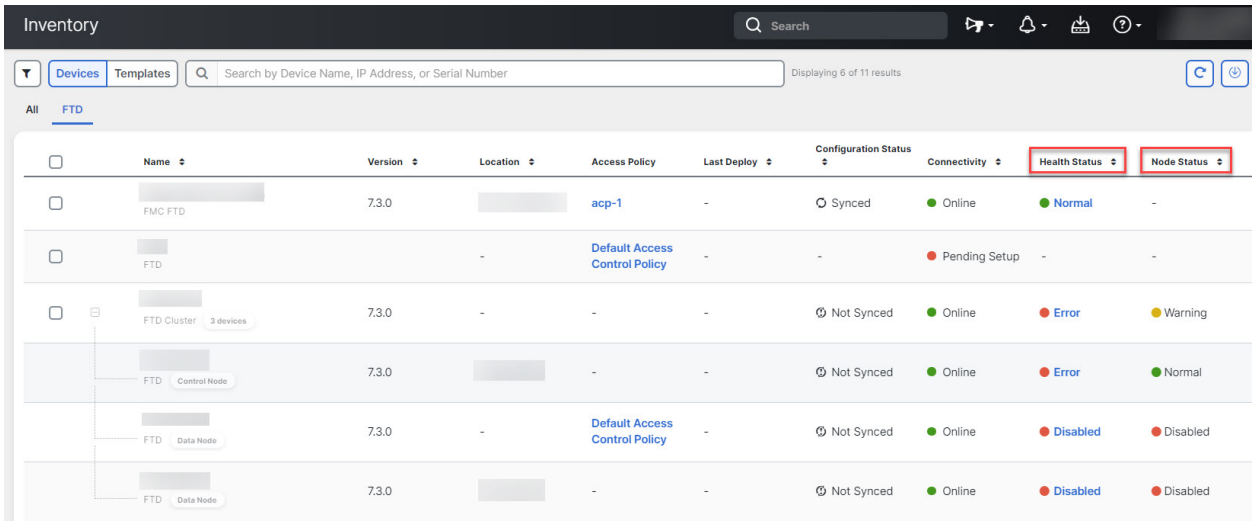
You can now manage your cloud-delivered Firewall Management Center, On-Prem Firewall Management Centers, and secure connectors from the new **Services** page. Choose **Tools & Services** > **Firewall Management Center** or **Secure Connectors**. Refer View Services Page Information to know more.



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 Firewall Threat Defense Devices Managed by GCP

You can now create a virtual Firewall 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 Firewall Threat Defense Devices Managed by AWS and Azure

You can now create a virtual Firewall 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 Firewall 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 Firewall 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.