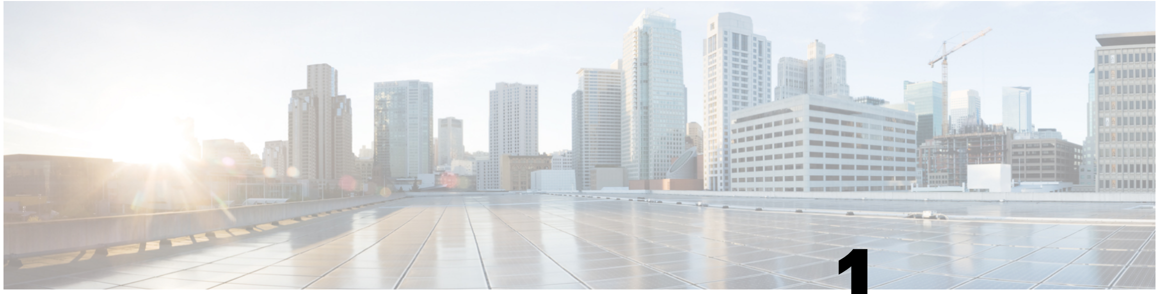
Release Notes for Cloud-Delivered Firewall Management Center

First Published: 2022-11-07

Last Modified: 2025-08-13

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



CHAPTER 1

About Cloud-Delivered Firewall Management Center

Security Cloud Control is 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 REST 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.

The Security Cloud Control operations team is responsible for maintaining the SaaS product. As new features are introduced, the Security Cloud Control operations team updates Security Cloud Control and the Cloud-Delivered Firewall Management Center 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.

Are these release notes for you?

These release notes are for existing Firewall in Security Cloud Control (Security Cloud Control) users who have a Cloud-Delivered Firewall Management Center deployed on their tenant.

Cisco Secure Threat Defense Terminology

Table 1:

Product Name	Description
Cisco Secure Firewall Threat Defense	Cisco's next-generation firewall. The name is often shortened to "Secure Firewall Threat Defense" or "Firewall Threat Defense" in documentation. It can be configured and managed by these device managers: • A Cloud-Delivered Firewall Management Center. • An on-premises Secure Firewall Management Center. • The local device manager included with the threat defense image.
Cloud-Delivered Firewall Management Center	This refers to the version of the Secure Firewall Management Center that is deployed with Security Cloud Control. The Cloud-Delivered Firewall Management Center manages one or more Secure Firewall Threat Defense firewalls. You may see the Cloud-Delivered Firewall Management Center referred to as "management center" in product documentation. **These release notes provide information about this manager.**
On-premises Cisco Secure Firewall Management Center	This manages one or more Cisco Secure Firewall Threat Defense devices. You may see these devices referred to as "Secure Firewall Management Center," or simply "management center" in product documentation. The on-premises Secure Firewall Management Center is managed by the customer. Some images are designed for installation on a physical Firepower appliance, others are virtual images that are installed and managed in the customer's private cloud. The customer performs installation and upgrade tasks.
Cisco Secure Firewall Threat Defense device manager	This manager is delivered with the Secure Threat Defense software image and *only* manages the single Secure Threat Defense device it was delivered with. CDO can manage threat defense devices that are managed by the device manager and are configured for local management. Management tasks for the threat defense device can be performed by CDO or by the device manager and CDO keeps track of which manager performed which task and alerts the CDO user where changes are coming from. Threat defense devices managed by the device manager by CDO cannot be managed by the cloud-delivered Firewall Management Center. In the documentation for Cisco Defense Orchestrator, we refer to a threat defense device managed by the device manager as "an FDM-managed device" or an "FDM."

Important Notice: End-of-Support for Secure Firewall Threat Defense 7.0.*x*

Starting October 22, 2025, Threat Defense 7.0.x is no longer supported with Cloud-Delivered Firewall Management Center. This also ends support for the ASA-5508-X and ASA-5516-X with Cloud-Delivered Firewall Management Center. After support ends, you cannot make or deploy changes to these devices except to upgrade or unregister.

Begin upgrading or replacing affected devices now. Do not add any new Version 7.0.x devices. Before support ends, all devices must be running at least Version 7.2.x. If possible, we recommend the suggested release listed in the Cisco Secure Firewall Threat Defense Compatibility Guide. If you cannot upgrade due to incompatibility, contact your Cisco representative or partner immediately.

See: End-of-Support for Cisco Secure Firewall Threat Defense 7.0.x with Cloud-Delivered Firewall Management Center

CHAPTER 2

New Features in Cloud-Delivered Firewall Management Center 2025

August 14, 2025

Table 2: Features in Version 20250725

Feature	Minimum Threat Defense	Details
Zero Trust Access		
Universal Zero Trust Network Access (universal ZTNA).	7.7.10	Universal Zero Trust Network Access (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. New/modified screens: **Policies** > **Zero Trust Application** Requires Cisco Secure Access and Security Cloud Control. Deployment restrictions: Not supported with clustered devices, container instances, or transparent mode. Supported platforms: Secure Firewall 1150, 3100, 4100, 4200, and Firewall Threat Defense Virtual. See Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control
Administration		

Feature	Minimum Threat Defense	Details
Backup of Threat Defense devices.	Any	The Cloud-Delivered Firewall Management Center now retains only the five most recent Threat Defense device backups. All the older backups are deleted automatically. See About Backup and Restore
Migration		
Multi-instance Threat Defense device migration.	7.6	You can now migrate multi-instance Threat Defense devices that are part of a chassis, such as the Secure Firewall 3100/4200, to the Cloud-Delivered Firewall Management Center using the **Migrate FTD to cdFMC** feature in Security Cloud Control. See Supported Features
Migrate select Firepower 4100/9300 models to Secure Firewall 3100/4200.	• The source devices must be Version 7.2.x and later. • The target devices must be Version 7.4.1 and later.	You can now easily migrate configurations to the Secure Firewall 3100/4200 from these devices: • Firepower 4110, 4120, 4140, 4150 • Firepower 9300: SM-24, SM-36, SM-44 See Threat Defense Model Migration
Multi-instance mode conversion in the Firewall Management Center for the Secure Firewall 3100/4200.	7.6.0	You can now register an application-mode device to the Firewall Management Center and then convert it to multi-instance mode without having to use the CLI. New/modified screens: • **Devices** > **Device Management** > **More** (⋮) > **Convert to Multi-Instance** • **Devices** > **Device Management** > **Select Bulk Action** > **Convert to Multi-Instance** See: Convert a Device to Multi-Instance Mode

July 03, 2025

Table 3: Features in Version 20250604

Feature	Minimum Threat Defense	Details
Troubleshooting		
Cisco RADKit integration.	7.7.0	Cisco RADKit integration allows Cisco TAC engineers to remotely connect with your deployment (including sudo access) for an enhanced troubleshooting experience. You control the appliances and duration of access. This also gives you and Cisco TAC access to diagnostic data and logs. New/modified screens: **Devices** > **Remote Diagnostics** > **Enable the RADKit service** See: Troubleshooting

March 13, 2025

Table 4: Features in Version 20250219

Feature	Minimum Threat Defense	Details
Platform		
Threat defense Version 7.7.0 support.	7.7.0	You can now manage threat defense devices running Version 7.7.0.
Secure Firewall 1230, 1240, and 1250 (rack-mount).	7.7.0	We introduced the Secure Firewall CSF-1230 and CSF-1240: • 8x1Gbps RJ-45 1000BASET/2.5BBASE-T copper • 4x1Gbps SFP+ optical And the Secure Firewall CSF-1250: • 8x2.5Gbps1000BASET/2.5BBASE-T copper • 4x2.5Gbps SFP28 optical See: Cisco Secure Firewall CSF-1230,CSF-1240, and CSF-1250 Hardware Installation Guide

Feature	Minimum Threat Defense	Details
Optical transceivers for the Secure Firewall 4200.	7.7.0	The Secure Firewall 4200 now supports these optical transceivers on the FPR4K-X-NM-2X200/400G network module: QDD-400G-DR4-S, QDD-4x100G-FR-S, QDD-4x100G-LR-S, QDD-400G-SR4.2-BD, QDD-400G-FR4-S, QDD-400G-LR4-S, QDD-400-CUxM, QDD-400-AOCxM, QDD-2X100-LR4-S, QDD-2X100-SR4-S, QDD-4ZQ100-CUxM. See: Cisco Secure Firewall 4215, 4225, and 4245 Hardware Installation Guide
Secure Firewall 1210CP IEEE 802.3bt support (PoE++ and Hi-PoE).	7.7.0	We made the following improvements related to support for IEEE 802.3bt: • PoE++ and Hi-PoE—Up to 90W per port. • Single- and dual-signature powered devices (PDs). • Power budgeting is done on a first-come, first-served basis. • Power budget fields were added to **show power inline**. New/modified screens: **Devices** > **Device Management** > **Interfaces** > **PoE** New/modified commands: **show power inline** See: Regular Firewall Interfaces, Cisco Secure Firewall Threat Defense Command Reference.
Instances for AWS, Azure, and GCP.	7.7.0	We added instances for and Firewall Threat Defense Virtual from the following families: • AWS (Amazon Web Services): C6i and C6a • Azure (Microsoft Azure): Dv4 and Dv5 • GCP (Google Cloud Platform): E2, N1, N2D, C2D See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
Device Management		

Feature	Minimum Threat Defense	Details
Recovery-config mode for emergency on-device configuration and out-of-band configuration detection on the Firewall Management Center.	7.7.0	If you lose the management connection to your device, you can make select configuration changes directly at the device CLI to: • Restore the management connection if you are using a data interface for manager access. • Make select policy changes that can't wait until the connection is restored. After the management connection is restored, the Firewall Management Center will detect the configuration changes on the device. It does not automatically update the device configuration in the Firewall Management Center; you must view the configuration differences, acknowledge that the device configuration is different, and then manually make the same changes in the Firewall Management Center before you deploy. New/modified screens: **Devices** > **Device Management** > **Device** > **Health** > **Out of Band Status** New/modified diagnostic CLI (**system support diagnostic-cli**) command: **configure recovery-config** See Device Settings, Cisco Secure Firewall Threat Defense Command Reference
Interfaces		
Sync Device is now **Sync Interfaces**.	Any	**Sync Device** was changed to **Sync Interfaces** to indicate that this function is only for interface changes. This function no longer detects changes made to the manager access interface; see **Devices** > **Device Management** > **Device** > **Management** > **Manager Access Details: Configuration**. Other out-of-band configuration changes performed at the diagnostic CLI in recovery-config mode need to be discovered at **Devices** > **Device Management** > **Device** > **Health** > **Out of Band Status**. New/modified screens: **Devices** > **Device Management** > **Interfaces** See: Interfaces
High Availability/Scalability		
Threat defense high availability supported with redundant manager access data interfaces.	7.7.0	You can now use redundant manager access data interfaces with Firewall Threat Defense high availability. See: High Availability
Autoscale for Firewall Threat Defense Virtual for Azure clusters.	7.7.0	We now support autoscale for new Firewall Threat Defense Virtual for Azure clusters. You cannot convert upgraded deployments. Platform restrictions: Not supported with FTDv5 or FTDv10. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
VPN: Remote Access		

Feature	Minimum Threat Defense	Details
Geolocation-based RA VPN.	7.7.0	You can now allow or block remote access VPN connections based on country or region. Connections that don't meet your location-based criteria are blocked before authentication and logged for auditing purposes. New/modified screens: **Objects** > **Object Management** > **Access List** > **Service Access** See: Remote Access VPN
Easily configure posture assessment criteria for dynamic access policies.	7.2.0	In dynamic access policies (DAP), you can now easily configure *posture assessment criteria*—that is, file, process, or registry endpoint attributes with unique endpoint IDs that you can then use to configure DAP records. New/modified screens: • **Devices** > **Dynamic Access Policy** > **Add/Edit Policy** > **Posture Assessment Criteria** • **Devices** > **Dynamic Access Policy** > **Add/Edit Policy** > **Add/Edit DAP Record** > **Advanced** > **Endpoint Criteria** See: Dynamic Access Policies
Routing		
BGP AS-Override.	7.7.0	Firewall Threat Defense can now overwrite an ASN received from a peer with its own BGP ASN. This allows other routers peering with Firewall Threat Defense to accept advertised prefixes without detecting a loop based on the contents of the AS_PATH attribute. New/modified screens: **Devices** > **Device Management** > **Add/Edit Device** > **Routing** > **BGP IPv4 or IPv6** > **Add/Edit Neighbor** > **AS Override** See: BGP
Access Control: Threat Detection and Application Identification		
Easily block traffic based on TLS version and server certificate status.	7.7.0	New options in the decryption policy wizard make it easier to block traffic based on TLS version and server certificate status. Enabling these options adds predefined rules that do this. After the policy is created, you can edit, reorder, or delete the rules. New/modified screens: **Policies** > **Decryption** > **Create Decryption Policy** > **Blocking** See: Decryption Policies, Decryption Rules

Feature	Minimum Threat Defense	Details
Use EVE to easily bypass decryption for low-risk connections to trusted URLs.	7.7.0	A new Client Threat decryption rule condition and a new option in the decryption policy wizard and make it easier to bypass decryption to trusted URLs for low risk (as identified by EVE) connections. New decryption policies now include predefined rules that do this, using Category (trusted) and Client Threat (low) conditions. The Client Threat condition is new and represents the EVE verdict. 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. New/modified screens: **Policies** > **Decryption** > **Create Decryption Policy** > **Decryption Exclusions** Version restrictions: You cannot deploy policies with Client Threat rules to older devices. See: Decryption Policies, Decryption Rules
New EVE exceptions.	7.7.0	You can now bypass EVE (encrypted visibility engine) block verdicts based on source network and on destination dynamic attributes. And, when bypassing based on network, you can now use FQDN network objects. Previously, you could only block based on destination network or EVE process name and could not use FQDNs. New/modified screens: • To add an exception from the access control policy, in the advanced settings, edit and enable **Encrypted Visibility Engine**, enable **Block Traffic Based on EVE Score**, and **Add Exception Rule**. • To add an exception from the Unified Events viewer, right-click a connection that was blocked by EVE and select **Add EVE Exception**. See: Cisco Secure Firewall Management Center Snort 3 Configuration Guide
Access Control: Identity		
Multicloud Defense connector for Cisco Secure Dynamic Attributes Connector.	Any	The Multicloud Defense connector sends dynamic application address objects to the configured Cloud-Delivered Firewall Management Center. For more information, see the Address Objects chapter in the *Cisco Multicloud Defense User Guide* and address object API documentation.
Health Monitoring		
Get alerts before service authentication certificates expire.	7.7.0	To help prevent unexpected service disruptions, a new Certificate Monitoring health module alerts you before service authentication certificates expire on managed devices. New/modified screens: **System** (⚙) > **Health** > **Policy** > **Health Modules** > **Certificate Monitoring** See: Health

Feature	Minimum Threat Defense	Details
Independently configure health monitoring for physical and subinterfaces.	Any	You can now disable health monitoring for a physical interface while continuing to monitor and receive health alerts for its subinterfaces. You can disable alerts permanently or temporarily. To do this, configure the device for health monitoring exclusion, edit that configuration to enable module-level exclusion, and finally configure exclusion settings for the Interface Settings health module. New/modified screens: **System** (⚙) > **Health** > **Exclude** See: Health
Upgrade		
Devices with internet access download upgrade packages from the internet.	Any (some restrictions)	You can now begin device and chassis upgrades without the upgrade package. At the appropriate time, devices will get the package directly from the internet. This saves time and Firewall Management Center disk space. Devices without internet access can continue to get the package from the Firewall Management Center or an internal server. Note that devices try the internal server (if configured) before either the internet or the Firewall Management Center. If the internal server download fails, newer devices with internet access try the internet then the Firewall Management Center, while older devices and devices without internet access just try the Firewall Management Center. (In this context, "newer" means Firewall Threat Defense 7.6+ or chassis 7.4.1+.) Restrictions: Firewall Management Center and devices must be able to access the internet. There is no way to force a device with internet access to try the Firewall Management Center before it tries the internet. Not supported for hotfixes. Download location: https://cdo-ftd-images.s3-us-west-2.amazonaws.com/ See: Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center

Feature	Minimum Threat Defense	Details
Upgrade Firewall Threat Defense or chassis without a manual readiness check.	7.7.0	You no longer have to run time-consuming pre-upgrade readiness checks for Firewall Threat Defense or chassis upgrades. Instead, these checks are now regularly run by the system and reported in the health monitor. This allows you to preemptively fix any issues that will block upgrade. • The Database module, new for devices, manages monitors database schema and configuration data (*EO*) integrity. • The FXOS Health module, new for devices, monitors the FXOS httpd service on FXOS-based devices. • The Disk Status module is now more robust, alerting on disk health issues reported by daily running of smartctl (a Linux utility for monitoring reliability, predicting failures, and performing other self-tests). Version restrictions: This feature is supported for upgrades *from* Version 7.7+. Devices running earlier versions still require the in-upgrade readiness check. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center
Administration		
Cancel Firewall Threat Defense backups, view detailed backup status.	7.7.0	The Message Center now displays detailed backup status for the Firewall Management Center and its devices. You can also cancel in-progress device backups. See: Backup/Restore
Clear disk space utility.	7.7.0	A new utility allows you to click to safely remove unneeded files such as old backups, content updates, and troubleshooting files. Low disk space can reduce performance, prevent upgrade, and increase the risk of accidentally deleting important files when trying to recover space. New/modified screens: We added a **Clear disk space** button to the Disk Usage widget on device health dashboards: **System** (⚙) > **Health** > **Monitor**. See: Troubleshooting
Send detailed Firewall Management Center audit logs to syslog.	Any	You can stream configuration changes as part of audit log data to syslog by specifying the configuration data format and the hosts. The Firewall Management Center supports backup and restore of the audit configuration log. New/modified screens: **System** (⚙) > **Configuration** > **Audit Log** > **Send Configuration Changes** See: System Configuration
Performance and Resiliency		

Feature	Minimum Threat Defense	Details
Faster failover for high availability Firewall Threat Defense.	7.7.0	With Firewall Threat Defense high availability failover, the new active device generates multicast packets for each MAC address entry and sends them to all bridge group interfaces, which prompts the upstream switches to update their routing tables. This task now runs asynchronously in the data plane, privileging critical failover tasks in the control plane. This makes failover faster, reducing downtime. See: High Availability
High-bandwidth encrypted application traffic bypasses unnecessary intrusion inspection.	7.7.0	Specific high-bandwidth encrypted application traffic now bypasses unncessary intrusion inspection even if the connection matches an Allow rule. Intrusion rule (LSP) and vulnerability database (VDB) updates can change the applications bypassed but right now they are: AnyConnect, IPsec, iCloud Private Relay, QUIC (including HTTP/3), Webex Media, Secure RTCP.
Configure Firewall Threat Defense autorecovery from block depletion using FlexConfig.	7.7.0	To reduce downtime due to service disruption, a new fault manager monitors block depletion and automatically reloads devices when necessary. In high availability deployments, this triggers failover. Fault monitoring is automatically enabled on new and upgraded devices. To disable, use FlexConfig. New/modified FlexConfig commands: • **fault-monitor block-depletion recovery-action** { **none** | **reload** } Specifying **none** turns off automatic reload, but does not turn off fault monitoring. For that, use **no fault-monitoring**. • **fault-monitor block-depletion monitor-interval** *seconds* You can configure how long (in seconds) before the device reloads. New/modified Firewall Threat Defense CLI commands: **show fault-monitor block-depletion** { **status** | **statistics** } Platform restrictions: Not supported for clustered devices. See: Troubleshooting
Troubleshooting		
CPU profiler includes application identification statistics.	7.7.0	The CPU profiler now includes application identification statistics. That is, you can now see the resources used by processing specific application traffic. After you enable CPU profiling, use the CLI to see results. New/modified CLI commands: **system support appid-cpu-profiling status**, **system support appid-cpu-profiling dump** See: Troubleshooting, Cisco Secure Firewall Threat Defense Command Reference

Feature	Minimum Threat Defense	Details
New IP flow statistics.	7.7.0	When collecting IP flow statistics from Firewall Threat Defense under the direction of Cisco TAC, a new **all** parameter logs additional statistics to the specified file: port, protocol, application, cumulative latency, and inspection time. New/modified commands: **system support flow-ip-profiling start flow-ip-file** *filename* **all** { **enable** | **disable** } See: Cisco Secure Firewall Threat Defense Command Reference
Security and Hardening		
Require the Message-Authenticator attribute in all RADIUS responses.	7.0.7 7.7.0	**Upgrade impact. After threat defense upgrade, enable for existing servers.** You can now require the Message-Authenticator attribute in all RADIUS responses, ensuring that the threat defense VPN gateway securely verifies every response from the RADIUS server, whether for RA VPN or access to the device itself. The **RADIUS Server-Enabled Message Authenticator** option is enabled by default for new RADIUS servers. We also recommend you enable it for existing servers. Disabling it may expose firewalls to potential attacks. New/modified screens: • **Objects** > **AAA Server** > **RADIUS Server Group** > **Add RADIUS Server Group** > **Add RADIUS Server** • **System** (⚙) > **Users** > **External Authentication** > **Add External Authentication Object (RADIUS)** New CLI commands: **message-authenticator-required** Version restrictions: Not supported with Version 7.0–7.0.6, 7.1.x, 7.2.0–7.2.9, 7.3.x, 7.4.0–7.4.2, 7.6.0. Other restrictions: This feature introduced a login bug where the Firewall Management Center treats the RADIUS Class attribute (25) as octets instead of a string, which can break role mapping and cause login failures. For a list of fixed releases, or a workaround if you cannot upgrade, see CSCwq03404. See: Objects Management, Platform Settings
Limited user privileges for Threat Defense CLI Basic user.	7.7.0	The scope of the Threat Defense CLI Basic user privilege is now limited to the following commands: dig, ping, traceroute. If you have created users with the Basic privilege, evaluate whether you need to change them to the Config privilege. You can change a user's privilege level using the **configure user access** command. See: Cisco Secure Firewall Threat Defense Command Reference
Deprecated Features		

Feature	Minimum Threat Defense	Details
Deprecated: Snort 2.	7.7.0	**Upgrade impact. Cannot upgrade Snort 2 devices.** Snort 2 is deprecated. You cannot upgrade a Snort 2 device to Version 7.7.0+. Although you can use a Version 7.7.0+ Firewall Management Center to manage older Snort 2 devices, you should still switch to Snort 3 for improved detection and performance. Deprecated CLI commands: **show snort counters**, **show snort preprocessor-memory-usage**. See: Cisco Secure Firewall Management Center Snort 3 Configuration Guide
Deprecated: Access control policy legacy interface.	Any	You can no longer use the legacy user interface for access control policies. If you were using it, you switch to the improved user interface. New/modified screens: **Switch to Legacy UI** toggle is removed

CHAPTER 3

New Features in Cloud-Delivered Firewall Management Center 2024

Welcome to Security Cloud Control

Cisco Defense Orchestrator is now "Firewall in 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.

December 13, 2024

Table 5: Features in Version 20241127

Feature	Minimum Threat Defense	Details
Licensing		
90-day evaluation license.	7.6.0	The Cloud-Delivered Firewall Management Center now offers a 90-day evaluation license. After this period, you can still onboard threat defense devices, but deployments are blocked until the Cloud-Delivered Firewall Management Center is registered with Cisco Smart Software Manager. You will receive alert notifications on Security Cloud Control when the evaluation period nears expiration. See: Licensing

November 8, 2024

Table 6: 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, where 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

Feature	Minimum Threat Defense	Details
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 Firewall 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		
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 Firewall Threat Defense 7.4.1–7.4.x only; those devices cannot run Version 7.6.0. See: Device Management Using Device Templates and 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

Feature	Minimum Threat Defense	Details
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
Multi-instance mode conversion in the Firewall Management Center for the Secure Firewall 3100/4200.	7.6.0	You can now register an application-mode device to the Firewall Management Center and then convert it to multi-instance mode without having to use the CLI. New/modified screens: • **Devices** > **Device Management** > **More** (⋮) > **Convert to Multi-Instance** • **Devices** > **Device Management** > **Select Bulk Action** > **Convert to Multi-Instance** See: Convert a Device to Multi-Instance Mode
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

Feature	Minimum Threat Defense	Details
Deploy virtual firewall clusters across multiple AWS availability zones.	7.6.0	You can now deploy Firewall 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 Firewall Threat Defense Virtual for AWS in two-arm-mode with GWLB.	7.6.0	You can now deploy Firewall 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
Interfaces		
Deploy without the diagnostic interface on Firewall Threat Defense Virtual for Azure and GCP.	7.4.1	You can now deploy without the diagnostic interface on Firewall 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		

Feature	Minimum Threat Defense	Details
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
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		

Feature	Minimum Threat Defense	Details
Passive identity agent for Microsoft AD.	Any	This feature is introduced. Passive Identity Agent version 1.1 is compatible with 7.6.0 and later and adds the following: • You can use either FQDN, IPv4, or IPv6 to connect from the Passive Identity Agent to the Secure Firewall Management Center or Cisco Security Cloud Control. • Sends both IPv4 and IPv6 user sessions from Microsoft Active Directory (AD) to the Firewall Management Center. • You can zip troubleshooting logs. • When you start the Passive Identity Agent software, a list of prerequisites is displayed. The Passive Identity Agent identity source sends session data from Microsoft Active Directory (AD) to the Firewall 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.
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. Also, the identity source uses constantly changing dynamic objects from Cisco ISE 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

Feature	Minimum Threat Defense	Details
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 Firewall 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 Firewall 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		
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 Firewall Management Center connectivity with Talos, which is required for this feature. See Configure EVE.
Administration		

Feature	Minimum Threat Defense	Details
New theme for the Firewall Management Center.	Any	We updated the look and feel of the Firewall Management Center web interface, including a new left-hand navigation.

August 23, 2024

Table 7: Features in Version 20240808

Feature	Minimum Threat Defense	Details
Platform		
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.
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 (*Firewall 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 Firewall 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 3100/4200 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: Decryption Policies

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: Realms
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 (Firewall Threat Defense only), CPU, and Memory health alert sub-types. See: Health
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: Health

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 Firewall 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 Firewall 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 Secure Firewall Threat Defense to the Cloud-Delivered Firewall Management Center
Administration		
Firewall 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. 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: Troubleshooting
Deprecated Features		
End of support: analytics-only capabilities with the full range of threat defense devices.	Any	You can co-manage a cloud-managed device with a Version 7.2+ on-prem Firewall Management Center for event logging and analytics purposes only. Because the Cloud-Delivered Firewall Management Center supports a wider range of managed device versions than on-prem management centers, you may have issues with devices being "too old" or "too new" to co-manage. See: Cisco Secure Firewall Management Center Compatibility Guide.

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 8: Features in Version 20240514

Feature	Minimum Threat Defense	Details
Platform Migration		
Migrate clustered Firewall Threat Defense devices from an on-prem management center to the Cloud-Delivered Firewall Management Center.	7.0.6 7.2.1	Clustered 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 9: 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
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 Firewall Threat Defense Virtual. See: Platform Settings
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

Feature	Minimum Threat Defense	Details
Device Management		
Device management services supported on user-defined VRF interfaces.	Any	Device management services configured in the Firewall 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
Access Control: Identity		

Feature	Minimum Threat Defense	Details
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 Firewall 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: User Control with Captive Portal
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: User Control with Captive Portal
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 Firewall Threat Defense, 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 Firewall 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 Firewall Threat Defense upgrade wizard.	Any	You can now enable revert from the Firewall Threat Defense upgrade wizard. Version restrictions: You must be upgrading Firewall 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 Firewall Threat Defense upgrade wizard.	Any	The final page of the Firewall 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 Firewall Threat Defense upgrade wizard. Deprecated screens/options: • **System**(⚙) > **Updates** is deprecated. All Firewall Threat Defense upgrades now use the wizard. • The **Add Upgrade Package** button on the Firewall 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 Firewall Management Center has changed its direct-download location for software upgrade packages from sourcefire.com to amazonaws.com.
Deprecated: scheduled download of maintenance releases.	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 Firewall 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
Deprecated Features		
Deprecated: DHCP relay trusted interfaces with FlexConfig.	Any	You can now use the Firewall 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 Firewall 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: Troubleshooting

CHAPTER 4

New Features in Cloud-Delivered Firewall Management Center 2023

November 30, 2023

Table 10: 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 11: 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 Firewall Threat Defense Virtual. See: Platform Settings
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 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: Device Management

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 Firewall 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 Firewall Management Centers do not support device migration to the cloud. Additionally, only standalone and high availability Firewall Threat Defense 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 Firewall 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 Firewall 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 Firewall Management Center for analytics because it will be running an unsupported version. **2.** Upgrade the on-prem Firewall 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 Firewall Management Center to Version 7.4.0. Unzip (but do not untar) the upgrade package before uploading it to the Firewall Management Center. Download from: Special Release. **4.** Onboard the on-prem Firewall Management Center to CDO. **5.** Migrate all devices from the on-prem Firewall 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 Firewall 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-Premises 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: Interface Overview
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 Firewall 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: Regular Firewall 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: Regular Firewall 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: Object Management
High Availability/Scalability		
Reduced "false failovers" for Firewall Threat Defense high availability.	7.4.0 7.2.6	Version restrictions: Not supported with Firewall 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: Policy Based Routing

Feature	Min. Threat Defense	Details
Policy-based routing with user identity and SGTs.	7.4.0	**Upgrade impact. Check SGT propagation before device upgrade.** 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. Note that as a result of how this feature was implemented, Firewall Threat Defense can now add egress SGTs to traffic if the egress interface is configured to propagate SGTs. This can happen with ISE integration even if you do not configure policy-based routing. Starting with Version 7.4.0, the **Propagate Security Group Tag** option is disabled by default for new interfaces. But because upgrade respects your current settings, this option may be enabled for existing interfaces. **Important** If you have configured an ISE identity source, before you upgrade, check the **Propagate Security Group Tag** option on your devices' physical, redundant, and subinterfaces and disable it if necessary. If downstream devices are not configured to handle the tags, you could experience traffic loss. 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: Object Management
VPN		
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: VPN Overview
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**
VPN: Remote Access		

Feature	Min. Threat Defense	Details
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 Firewall 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: Remote Access VPN
VPN: Site to Site		
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: Network Address Translation
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: Site-to-Site VPNs
Access Control: Threat Detection and Application Identification		

Feature	Min. Threat Defense	Details
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
Clientless zero-trust access.	7.4.0 with Snort 3	Zero Trust Access 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** 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: BGP

Feature	Min. Threat Defense	Details
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: Virtual Routers
Access Control: Threat Detection and Application Identification		
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.
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: Cisco Secure Firewall Management Center Snort 3 Configuration Guide
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 Firewall Management Center.	Any	You can now configure the Cisco Secure Dynamic Attributes Connector on the Firewall Management Center. Previously, it was only available as a standalone application. See: Cisco Secure Dynamic Attributes Connector
Event Logging and Analysis		

Feature	Min. Threat Defense	Details
Configure Firewall Threat Defense devices as NetFlow exporters from the Firewall Management Center web interface.	Any	NetFlow is a Cisco application that provides statistics on packets flows. You can now use the Firewall Management Center web interface to configure Firewall 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: Platform Settings
Health Monitoring		
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, Firewall Threat Defense supported only IPv4 OCSP URLs. Now, Firewall Threat Defense supports both IPv4 and IPv6 OCSP URLs. See: Object Management
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 Firewall Threat Defense clusters from **System** (⚙) > **Smart Licenses**. Previously, you had to use the Device Management page. See: Licensing • Download a report of Message Center notifications. In the Message Center, click the new **Download Report** icon, next to the **Show Notifications** slider. See: Troubleshooting • 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: Device Management. • Easily create custom health monitoring dashboards, and easily edit existing dashboards. See: Health

Feature	Min. Threat Defense	Details
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		
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 12: Deprecated Features: Version 20230929

Feature	Deprecated in Threat Defense	Details
Deprecated: NetFlow with FlexConfig.	Any	You can now configure Firewall Threat Defense devices as NetFlow exporters from the Firewall Management Center web interface. If you do this, you cannot deploy until you remove any deprecated FlexConfigs. See: Platform Settings
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, 7.4.x (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 13: 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 14: New Features: July 20, 2023

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

June 8, 2023

Table 15: 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 16: 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.
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 17: 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 5

New Features in Cloud-Delivered Firewall Management Center 2022

December 13, 2022

Table 18: 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 Firewall 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 Firewall 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 Firewall Threat Defense virtual in Azure for use with the Azure Gateway Load Balancer (GWLB). The Firewall 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 heading** > **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 Firewall 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 19: 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.

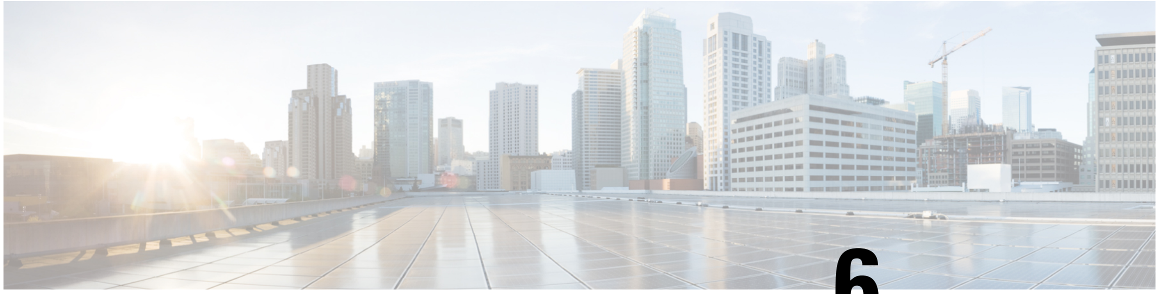
Although you can use one managed device as a proxy sequence, we strongly recommend you set up two or more so that, in the event one managed device cannot communicate with Active Directory or ISE/ISE-PIC, another managed device can take over.

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



CHAPTER 6

Open and Resolved Bugs

This document lists the open and resolved bugs in the cloud-delivered Firewall Management Center as of March 13, 2025.

Note Bug lists are auto-generated once and are not updated between upates of cloud-delivered Firewall Management Center. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes.

Open Bugs

Important Bug lists are auto-generated once and are not subsequently updated. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes. If you have a support contract, you can view the bugs below in the Cisco Bug Search Tool.

Table 20: Open Bugs of Cloud-Delivered Firewall Management Center

Bug ID	Headline
CSCwp32097	Domain filter is non-functional under ACP.
CSCwn34809	CdFMC: AWS FTD device not listed under managed device backup list.
CSCwh24268	CdFMC: Seeing bulk registration issues while migrating Secure Firewall Threat Defense.
CSCwk68830	A ticket is in IN PROGRESS state, unable to create policy - error stating an open ticket is needed.
CSCwm38714	Change management: Error in save of SD-WAN topology if security zone is added inline in the wizard.

Resolved Bugs

Table 21: Resolved Bugs update of Cloud-Delivered Firewall Management Center

Identifier	Headline
CSCwn13421	Scale cloud-delivered Firewall Management Center: Policy deploy fails when Audit log to Syslog is configured with invalid ipv6 syslog host
CSCwj30329	Cloud-Delivered Firewall Management Center: FTD Cluster Registration failing with internal error
CSCwm46752	"Edit configuration" on Secure Firewall 3100 L3 Cluster fails with BGP enabled
CSCwd79150	Device API healthStatus for cluster devices not aligned with health status on device listing
CSCwd88641	Deployment changes to push VDB package based on Device model and snort engine

CHAPTER 7

Documentation and Support Resources

Related Cisco Defense Orchestrator Product Documentation

Here are the locations of other helpful documents:

- Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator
- Links to all other Cisco Defense Orchestrator documentation

Cisco Support Resources

Open a Support Case Within Cloud-Delivered Firewall Management Ceneter

Follow this procedure to open a support case from within the cloud-delivered Firewall Management Center:

1. In the cloud-delivered Firewall Management Center, click the (**Help** (?) icon.
2. Under **Support & Downloads**, click **TAC Support Cases**.

Contact Cisco

These are other methods of contacting the Cisco Technical Assistance Center (TAC):

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts