New Features in Cloud-Delivered Firewall Management Center 2025

July 03, 2025

Table 1: 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 2: Features in Version 20250219

Feature	Minimum Threat Defense	Details
Platform		

Feature	Minimum Threat Defense	Details
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
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	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. 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		
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

Feature	Minimum Threat Defense	Details
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