Features and Issues

August 7, 2026

Resolved issues

Resolved security issues

This table lists the resolved security issues in this specific software release.

Table 1: Resolved security issues in Cloud-Delivered Firewall Management Center Version 20260722

Bug ID	Headline
CSCwt81457	Cisco Secure Firewall Management Center Software Session Fixation Issue
CSCwt95974	Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability
CSCwt95997	Cisco Secure Firewall Management Center Software Static Credential Vulnerability

Resolved functional issues

This table lists the resolved functional issues in this specific software release.

Table 2: Resolved functional issues in Cloud-Delivered Firewall Management Center Version 20260722

Bug ID	Headline
CSCwt27532	Access to UI from specific IP Address getting blocked
CSCwt87846	Deployment Preview, rollback version are missing resulting in preview , rollback functionality not working
CSCwu00518	Allow User Configuration to Restrict Number of Parallel Backups in Configuration File
CSCwu23327	FMC may partially persist configuration when REST API session replacement overlaps activity approval, contributing to integrity and deployment failures with policy/configuration
CSCwu36751	cdFMC getting deployment failure due to the failure in resolving the object
CSCwu54055	FMC UI - VPN configuration save takes very long
CSCwu60911	Device registration or Save operations fails
CSCwu60954	Occasionally cdFMC crossLaunch immediately logs the user out
CSCwv23051	FMC fails to upload AnyConnect/Secure Client images exceeding 200 MB
CSCwv24858	Snort 3 system-defined rule action override fails when the rule belongs to multiple same-named rule groups
CSCwv31630	Block deployment if device is participating in VPN topology where data is corrupted (manifesting in a way that the topology isn't seen on the UI)
CSCwv52841	cdFMC: FTD backups are failing

May 29, 2026

Features

Table 3: Features in Version 20260506

Feature	Supported Threat Defense Version	Details
Administration		

Feature	Supported Threat Defense Version	Details
Device Backup Enhancements: Improved Usability and Scalability	Any	The device backup process has been reengineered with an intuitive user interface, delivering enhanced usability and optimized system performance. Key improvements: • **Advanced Search**: Locate devices efficiently by filtering results based on device type and device groups. • **Unified Backup Notifications**: Monitor backup progress through a consolidated dashboard. View aggregate counts for successful, running, and failed backups, or drill down into individual device tracking for large-scale operations. This update also includes node-level progress monitoring for cluster devices. • **Node-Level Restore**: Download backups for specific nodes within a cluster for restoration, providing greater granularity and control. • **Streamlined Device Actions**: Execute bulk operations efficiently by selecting devices, clusters, or groups through a simplified checkbox interface. • **Downloadable Reports**: Export job-level backup progress reports to facilitate troubleshooting and expedite collaboration with Cisco TAC.
Enhanced Performance	7.4.7 and upcoming releases	Optimizes backup performance to significantly reduce processing time for high-volume devices.
Device Management		
Maximum Firewall Threat Defense Devices Supported	Any	Cloud-Delivered Firewall Management Center supports up to 2,000 Firewall Threat Defense devices per deployment. This total can include a combination of standalone devices, devices in high-availability pairs, and devices that are cluster nodes.
Policy Management		
NAT Templates	Any	NAT templates provide predefined NAT configurations for common use cases, helping administrators quickly create NAT rules with minimal manual input. NAT templates are useful when configuring standard outbound internet access or publishing internal resources to external networks. • The internet access template creates a dynamic Auto NAT rule that translates traffic from internal hosts to the destination interface IP address. • The internal resource access template creates a static Auto NAT rule that maps an internal resource to a translated address so that the resource is reachable from an external network. New/modified pages: **Policies > Network Policies > NAT**

Resolved issues

Resolved security issues

This table lists the resolved security issues in this specific software release.

Table 4: Resolved security issues in Cloud-Delivered Firewall Management Center Version 20260506

Bug ID	Headline
CSCwt25941	Multiple command injections in Remote::SF::Troubleshootingtool (only targets FTD)
CSCwt25947	Command injection in Remote::SF::Troubleshootingtool::deviceDeleteLogFiles (only targets FTD)

Resolved functional issues

This table lists the resolved functional issues in this specific software release.

Table 5: Resolved functional issues in Cloud-Delivered Firewall Management Center Version 20260506

Bug ID	Headline
CSCwo65977	Security Zones show "No Data" when attempting to edit ACP policies rules in FMC GUI post 7.7 upgrade - Indexing issue
CSCws92132	SASE: Restrict the tunnel ID field to 30 characters and custom IKE identity string
CSCws82979	Dynamic object not being updated in FMC when ADI has problems with ADI.conf
CSCws99933	Unable to Access the Access Control Policy.
CSCwt29200	FTD OOM due to hundreds of concurrent SF::DataService::Client::ProcessManifest calls invoking exec_perl.pl processes
CSCwt34022	Scheduled Task (schedule) for device backup has removed the unregistered device from its list for FTD HA device
CSCwt60089	Prometheus snapshot failing on cdFMC due to too many open files.
CSCwb83546	Default External Browser Package needs to be updated
CSCws94688	DAP Records fetch group policies displayed by their UUID instead of names (policies beyond the first 25 listed alphabetically due to the limit of 25 set when grouppolicies called in DAP)
CSCwt34828	The chassis actual status is Offline, but it shown as healthy in the new UI
CSCwt35794	Admin with RO Object Permissions unable to add Static Route for named interfaces

April 24, 2026

Features

Table 6: Features in Version 20260315

Feature	Supported Threat Defense	Details
Model migration		
Migrate Firepower 1100 Series to Secure Firewall 1200 Series	7.3.x and later	Migrate Firepower 1100 Series (1120, 1140, 1150) to: • Secure Firewall 1200 Series (1210CE, 1210CP, 1210CX) (7.6 and later) • Secure Firewall 1200 Series (1230, 1240, 1250) (7.7.x and later) For more information on the migration paths, refer to Supported Devices for Migration.
Migrate Firepower 2100 Series to Secure Firewall 1200 Series	7.4.x and later	Migrate Firepower 2100 Series (2110, 2120, 2130, 2140) to: • Secure Firewall 1200 Series (1210CE, 1210CP, 1210CX) (7.6 and later) • Secure Firewall 1200 Series (1230, 1240, 1250) (7.7.x and later) For more information on the migration paths, refer to Supported Devices for Migration.
Usability		

Feature	Supported Threat Defense	Details
Device Management page enhancements	Any	A redesigned user interface has been launched for the **Device Management** page, offering better usability and enhanced performance. Key improvements include: • **Advanced Search**: Find devices more easily using multiple device-related criteria for more precise results. • **Device Status Banner**: Quickly view the number of devices in **Normal**, **Error**, and **Offline** states, displayed with a color-coded legend for easy identification. • **Performance Enhancements**: Enjoy faster page loading time and pagination that supports up to 1,000 devices per page. • **Streamlined Device Actions**: Perform device actions and bulk operations more efficiently through an intuitive side panel. • **Centralized Troubleshooting**: Access diagnostic tools such as Packet Tracer and Packet Capture from a single, convenient troubleshooting panel. **Note** This enhanced interface is currently in a preliminary phase. You can switch back to the legacy UI to access any features that are not yet available in the new interface. Updated screens: Go to **Devices > Device Management** and enable the **New Device Management UI** toggle button.

Resolved issues

This table lists the resolved issues in this specific software release.

Table 7: Resolved issues in Cloud-Delivered Firewall Management Center Version 20260315

Bug ID	Headline
CSCwo65977	Security Zones show "No Data" when attempting to edit ACP policies rules in FMC GUI post 7.7 upgrade - Indexing issue
CSCws92132	SASE: Restrict the tunnel ID field to 30 characters and custom IKE identity string
CSCws82979	Dynamic object not being updated in FMC when ADI has problems with ADI.conf
CSCws99933	Unable to Access the Access Control Policy.
CSCwt29200	FTD OOM due to hundreds of concurrent SF::DataService::Client::ProcessManifest calls invoking exec_perl.pl processes
CSCwt34022	Scheduled Task (schedule) for device backup has removed the unregistered device from its list for FTD HA device

Bug ID	Headline
CSCwt60089	Prometheus snapshot failing on cdFMC due to too many open files.
CSCwb83546	Default External Browser Package needs to be updated
CSCws94688	DAP Records fetch group policies displayed by their UUID instead of names (policies beyond the first 25 listed alphabetically due to the limit of 25 set when grouppolicies called in DAP)
CSCwt34828	The chassis actual status is Offline, but it shown as healthy in the new UI
CSCwt35794	Admin with RO Object Permissions unable to add Static Route for named interfaces

February 19, 2026

Table 8: Features in Version 20260122

Feature	Minimum Threat Defense	Details
Device Management		
Secure traffic using Cisco Secure Access and Firewall Threat Defense devices	Any	Cisco Secure Access is a cloud-based security service edge (SSE) solution that protects users from internet threats and enables secure access to the internet, SaaS applications, and private resources from any location. Secure Firewall seamlessly integrates with Secure Access for securing your traffic. Cloud-Delivered Firewall Management Center simplifies and automates the IPsec IKEv2 tunnel configuration from Firewall Threat Defense devices to Secure Access using the new SASE wizard. For more information, see Secure traffic using Cisco Secure Access and Firewall Threat Defense devices.

December 15, 2025

Table 9: Features in Version 20251121

Feature	Minimum Threat Defense	Details
Deployment and policy management		
Simultaneous editing of access control policies by multiple users	Any	In previous releases, if two or more users simultaneously edited an access control policy, the first user who saved would retain their changes, and all other users would immediately lose all of their edits. Now, these users have the ability to selectively merge their changes, and changes that do not conflict with the first user's saved changes will automatically be accepted. This improves collaboration between users and reduces the need to lock the policy during edits.

Feature	Minimum Threat Defense	Details
Tenable vulnerability management	10.0.0	Tenable Vulnerability Management is a platform that helps organizations understand, report, and manage known vulnerabilities. When used with the Cloud-Delivered Firewall Management Center, the Tenable connector creates a dynamic object with a list of IP addresses known to have Common Vulnerability Exposures (CVEs) and populates those IP addresses as host entries.
Real-time Policy Analyzer and Optimizer	Any	This feature detects and reports anomalies, such as shadowing or redundancy, in access control rules, when they are being created or edited in the Cloud-Delivered Firewall Management Center in order to streamline policy management. To use this feature, enable AIOps Insights in Security Cloud Control.
Encrypted traffic handling		
New decryption policy user interface, including basic and advanced policy creation	10.0.0	Easily create standard decryption policies using a new interface tailored to the most common and effective scenarios, with single-page certificate management. Or, stick with the legacy wizard and advanced rules-based policy editor. After Cloud-Delivered Firewall Management Center upgrade, existing policies are labeled as legacy policies and continue to work as before. You can switch from a standard policy to legacy, but not from legacy to standard.
Change server certificates without impacting decryption by using an internal certificate to decrypt/reencrypt traffic	10.0.0	You can now use a certificate and key defined in the decryption rule to decrypt traffic. This certificate and key can be the internal server's certificate or it can be a different certificate; in addition, you can change the certificate and key at any time. You can replace the certificate using the API, a system like the Automated Certificate Management Environment (ACME), or using Object Management.
Hardware		
Secure Firewall 200	10.0.0	The Secure Firewall 200 is an affordable security appliance for branch offices and remote locations that balances cost and features. During deployment, the system alerts you to any unsupported configurations. Version restrictions: In Version 10.0.0, the Secure Firewall 220 is the only supported device in the Secure Firewall 200 series.
Secure Firewall 6100	10.0.0	The Secure Firewall 6100 is an ultra-high-end firewall for demanding data center and telecom networks. It has exceptional price-to-performance, modular capability, and high throughput. The Secure Firewall 6100 supports Spanned EtherChannel and Individual interface clustering for up to 4 nodes.

Feature	Minimum Threat Defense	Details
View field-replaceable memory module details for the Secure Firewall 6100	10.0.0	You can view details, including operational status, for the field-replaceable memory module on the Secure Firewall 6100. New/modified screens: Choose **Devices** > **Device Management**, then edit the device and select the **Device** tab. In the **System** section, click **View** next to **Inventory** > **Memory**. New/modified Firewall Threat Defense commands: **show inventory** New/modified FXOS commands: **show dimm detail**
DC power supply for the Secure Firewall 4200	7.4.3, 7.6.2. 7.7.0	The FPR4200-PWR-DC for Secure Firewall 4200 is a 1500 W DC power supply. The dual power supply modules can supply up to 1500 W power across the input voltage range (48 VDC to 60 VDC). The load is shared when both power supply modules are plugged in and running at the same time.
Network module for the Secure Firewall 4200	10.0.0	The FPR4K-XNM-6X1SXF for the Secure Firewall 4200 is a 6-port 1-Gbps SFP hardware bypass network module that operates in SX multimode. This network module has built-in SFP transceivers.
High availability/scalability		
More container instances (21) on the Secure Firewall 4225 in multi-instance mode	10.0.0	The Secure Firewall 4225 in multi-instance mode now supports 21 container instances. The previous limit was 14.
Cluster redirect: flow offload support for the Secure Firewall 4200 asymmetric cluster traffic	10.0.0	For asymmetric flows, cluster redirect lets the forwarding node offload flows to hardware. This feature is enabled by default but can be configured using FlexConfig. When traffic for an existing flow is sent to a different node, then that traffic is redirected to the owner node over the cluster control link. Because asymmetric flows can create a lot of traffic on the cluster control link, letting the forwarder offload these flows can improve performance. Added/modified commands: **flow-offload cluster-redirect** (FlexConfig), **show conn**, **show flow-offload flow**, **show flow-offload info**
IPsec flow offload for traffic on the cluster control link on the Secure Firewall 4200 in distributed site-to-site VPN mode	10.0.0	For asymmetric flows, cluster redirect lets the forwarding node offload flows to hardware. This feature is enabled by default but can be configured using FlexConfig. When traffic for an existing flow is sent to a different node, then that traffic is redirected to the owner node over the cluster control link. Because asymmetric flows can create a lot of traffic on the cluster control link, letting the forwarder offload these flows can improve performance. Added/modified commands: **flow-offload cluster-redirect** (FlexConfig), **show conn**, **show flow-offload flow**, **show flow-offload info**
Identity		

Feature	Minimum Threat Defense	Details
Identity-based dynamic access control	7.3.0 (AD realm) 7.4.0 (Azure AD realm)	Handle traffic based on real-time user posture and risk by correlating identity and device context (from Cisco ISE or pxGrid Cloud) with Cisco Identity Intelligence (from Microsoft Entra ID or Cisco Duo).
pxGrid Cloud identity source	7.3.0 (AD realm) 7.4.0 (Azure AD realm)	The Cisco Identity Services Engine (Cisco ISE) pxGrid Cloud Identity Source enables you to use subscription and user data from a Cisco ISE server or cluster Cisco ISE in access control rules.
Logging and analysis features		
Send security events to Splunk or other SIEM via syslog	10.0.0	A new Splunk integration wizard (**Integrations** > **Splunk**) and updated logging options in access control make it easier to send security events to Splunk (or any other SIEM via syslog)..
Generate and send protocol-aware (enriched) inspector logs via syslog	10.0.0	You can generate protocol-aware (enriched) inspector logs for traffic that you specify. Send these logs via syslog to Splunk or to any syslog server configured as an alert. To use this feature, enable advanced logging in your access control policy's advanced settings. Then, use access control rules to pinpoint the traffic where you want advanced logs. In those rules, enable the protocols you want to inspect. To receive alerts when there are communication issues between devices and the syslog server, enable the Snort 3 Statistics module in the device health policy.
Packet data included with intrusion events sent to Cisco Security Cloud	10.0.0	Packet data is now included with intrusion events sent to Cisco Security Cloud.
Model migration		
Migrate Firepower 4100/9300 to Secure Firewall 3100, 4200, and 6100	Any (source) 7.4.1 (target)	Migrate to the Secure Firewall 3100, 4200, and 6100 from: • Firepower 4112, 4115, 4125, 4145 • Firepower 9300: SM-40, SM-48, SM-56
Migrate Firepower 1010 to Secure Firewall 200 and 1200	Any (source) 7.6.0 (target)	Migrate the Firepower 1010 and 1010E to the Secure Firewall 200 and 1200.
Performance and resiliency		
Block depletion autorecovery for clusters	10.0.0	The firewall block depletion fault manager introduced in Version 7.7.0 now supports clustered devices. Fault monitoring is automatically enabled on new and upgraded devices. To disable, use FlexConfig.

Feature	Minimum Threat Defense	Details
Other performance and resiliency improvements	Feature dependent	We made performance and resiliency improvements to: • Deploying configuration changes • Event logging to external servers such as syslog or Cisco Security Cloud, for the Secure Firewall 4200 and 6100 • Install and upgrade • High availability for Firewall Threat Defense • Snort ML • Zero-touch provisioning
Public and private cloud		
Firewall Threat Defense Virtual for Microsoft Hyper-V	10.0.0	Firewall Threat Defense Virtual now supports Microsoft Hyper-V.
Larger default disk size and the ability to resize the disk post-deployment	10.0.0	Firewall Threat Defense Virtual supports dynamic disk expansion on all virtual platforms. This capability optimizes disk utilization on high-capacity systems (for example, systems with 64 vCPUs and 128 GB RAM), ensuring that large core dump files do not trigger disk-space alerts. The default disk size has also changed.
Unlimited performance tier (FTDvU) for VMware and KVM	10.0.0	Firewall Threat Defense Virtual for VMware and KVM now support an unlimited performance tier (FTDvU). This tier does not rate limit and the RA VPN session limit depends on the allocated resources: • 20,000 sessions with 32 vCPU and 64 GB RAM • 32,000 sessions with 64 vCPU and 128 GB RAM
Azure MANA NIC support	10.0.0	Firewall Threat Defense Virtual for Microsoft Azure now supports MANA NIC hardware, which is optimized for enhanced networking performance. Supported instances: Standard_D8s_v5, Standard_D16s_v5
Nutanix AOS 6.8 support	10.0.0	Firewall Management Center Virtual and Firewall Threat Defense Virtual for Nutanix now support Nutanix AOS 6.8. This includes Virtual Private Cloud (VPC) support, whose flexible and cloud-like network segmentation and isolation allows you to effectively design and scale secure multi-tenant architectures.
OpenStack Caracal support	10.0.0	Firewall Management Center Virtual and Firewall Threat Defense Virtual for OpenStack now support the Caracal release.
OCI Ampere Compute instances	10.0.0	Firewall Threat Defense Virtual for OCI now supports Flex instances powered by an Ampere ARM-based processor. ARM architecture provides high performance with lower power consumption, enabling cost-efficient scaling. Supported instances: VM.Standard.A1.Flex, VM.Standard.A2.Flex

Feature	Minimum Threat Defense	Details
Secure Boot and UEFI firmware support	10.0.0	**Upgrade impact. You cannot revert from Version 10+ to Version 7.7 or earlier.** Firewall Threat Defense Virtual is now compatible with UEFI-based virtual machines. This modern firmware interface replaces legacy BIOS, improves boot performance, and provides enhanced hardware/VM compatibility. Secure Boot ensures that only signed and trusted bootloaders, kernel modules, and drivers are executed when the VM starts. It improves the virtual appliances security. These changes mean that you cannot revert virtual firewalls from Version 10+ to Version 7.7 and earlier. After upgrade, we also recommend you migrate configurations to freshly deployed Version 10+ instances and decommission the old ones.
Routing		
Use PBR to handle traffic based on custom application patterns.	10.0.0	You can now use policy based routing to handle traffic using custom application patterns (basic supported from Version 7.7.0). Create an advanced custom application detector by uploading a Lua file with your detection pattern. Then, use the detector in an extended ACL in your PBR policy. See: Policy Based Routing
IPv6 router advertisements assign RDNSS/DNSSL	10.0.0	You can now configure recursive DNS server (RDNSS) and DNS search list (DNSSL) options to provide DNS servers and domains to SLAAC clients using router advertisements. New/modified screens: **Devices** > **Device Management** > **Interfaces** > **Add/Edit Interfaces** > **IPv6** > **Settings** New/modified commands: **show ipv6 nd detail**, **show ipv6 nd ra dns-search-list**, **show ipv6 nd ra dns server**, **show ipv6 nd summary**
Threat detection and application identification		

Feature	Minimum Threat Defense	Details
EVE improvements	10.0.0 (widgets) Any (all others)	EVE improvements include: • EVE configuration moved from the access control policy advanced settings to thue main access control policy page (in the **More** drop-down list). • New monitor and protect modes. The monitor mode allows you to see EVE verdicts without blocking. • Five-level threat confidence scale now only two levels: high and very high. • EVE is now automatically used for application detection when you enable EVE. • EVE exceptions are now objects, and are automatically shared across all access control policies. • Security-related connection events now include those for connections with malware processes detected by EVE at higher threat confidence levels. • New EVE widgets on the Summary Dashboard provide information on targeted resources, as well as on connections blocked over time. Note that new dashboard widgets only show data for Version 10+ devices.
Default ports in application-based access control rules	Any with Snort 3	For access control rules, a new **Application Default** option on the **Applications** tab lets you limit the rule to the application's default ports. You can also specify that the application be identified on **Any** port, which is the system's previous behavior. Note that any specification on the **Ports** tab overrides these options. You can use the **Ports** tab to limit the rule to one, multiple, or a range of ports.
Dynamic objects and security group tags in DNS rules	10.0.0	You can configure DNS rules in the DNS policy to use dynamic objects or security group tags (SGT). If you are using these types of objects in access control rules already, you can now extend their use to your DNS policy. We added the **Dynamic Attributes** tab to the add/edit DNS rule dialog box.
HTTP command line injection attack detection with Snort ML	10.0.0	Snort ML now detects HTTP command line injection attacks. The snort_ml inspector is currently disabled in all default policies except maximum detection. The intrusion rule that generates an event when the snort_ml detects an attack (GID:411 SID:1) is also currently disabled in all default policies except maximum detection.
Portscan detection for clusters	10.0.0	You can configure threat detection at the cluster level. For nodes in a cluster, detection and prevention happen at the cluster level. Portscans can be detected when they happen across nodes or in an individual node. Shunned hosts are shunned on all devices in the cluster. Shuns are released at the same time on all nodes. Statistics are available at the cluster level.
Troubleshooting and serviceability		

Feature	Minimum Threat Defense	Details
MTU ping test on cluster node join provides more information by trying smaller MTUs	Any	When a node joins the cluster, it checks MTU compatibility by sending a ping to the control node with a packet size matching the cluster control link MTU. If the ping fails, it tries the MTU divided by 2 and keeps dividing by 2 until an MTU ping is successful. A notification is generated so you can fix the MTU to a working value and try again. We recommend increasing the switch MTU size to the recommended value, but if you can't change the switch configuration, a working value for the cluster control link will let you form the cluster. New/modified commands: **show cluster history**
Improved cluster control link health check with high CPU	Any	When a cluster node CPU usage is high, the health check will be suspended, and the node will not be marked as unhealthy. This feature is enabled by default when the CPU usage reaches 90% but can be configured using FlexConfig. New/modified FlexConfig commands: **cpu-healthcheck-threshold**
Ensure temporarily unavailable nodes can rejoin an oversubscribed cluster	10.0.0	Prioritizing critical control traffic increases resiliency in high availability and clustered deployments, especially when forming high availability or rejoining a cluster during times of heavy load. New/modified commands: **show asp priority-polling**, **show cluster info trace**, **show failover trace** Deployment restrictions: Not supported with container instances Platform restrictions: Supported with Secure Firewall 3100, 4200, and 6100 only
Use the packet tracer to modify PCAPs	10.0.0	You can now use the packet tracer to modify the source and destination IP address, source and destination port, and VLAN ID of a PCAP. In transparent mode, you can also modify the destination MAC address. You can then run a trace with the modified PCAP.
Generate a kernel dump on demand, or automatically on crash	10.0.0	You can now use the CLI to configure most hardware devices to generate a Linux kernel dump on crash. After you enable this feature, the device must reboot for it to take effect. Using the **force** keyword reboots the device and generates a kernel dump immediately. Or, manually reboot the device later. The upgrade automatically enables this feature. New CLI command: **system support kernel-crash-dump** Platform restrictions: Supported on all hardware devices except the Secure Firewall 200 and ISA 3000.

Feature	Minimum Threat Defense	Details
Recovery-config mode support for NAT and other interface commands	10.0.0	Recovery-config mode now supports NAT and related object and object-group commands. It also supports the following interface commands: • **duplex** • **fec** • **negotiate-auto** • **speed** These interface commands, in addition to shutdown, are not supported in recovery-config mode on the cluster control link or failover link. New/modified diagnostic CLI (**system support diagnostic-cli**) command: **configure recovery-config** Platform restrictions: Not supported with the Firepower 4100/9300, ISA 3000, or virtual firewall. Not supported for the Secure Firewall 3100/4200 in multi-instance mode.
Minimal system logging	10.0.0	You can now configure minimal (notice and above) system logging. For most devices, the default is full logging. For the new Secure Firewall 220, the default is minimal logging. New/modified CLI commands: **system support logging-show**, **system support logging-full**, **system support logging-minimal**
Upgrade		
New device and chassis upgrade wizard	Any	A new, streamlined upgrade wizard makes it easier to select and prepare devices for upgrade, and to identify issues preventing upgrade. Note that the Firewall Threat Defense wizard takes advantage of a new prepare-only option for unattended mode. This means that while the wizard copies packages and checks readiness, you may see messages about unattended mode running even if you did not explicitly start it.
Prepare-only and skip-checks options for unattended Firewall Threat Defense upgrade	Any	With unattended Firewall Threat Defense upgrades: • Prepare for upgrade only—copy packages and check readiness, but do not perform the actual upgrade. • Skip readiness checks for devices that already passed. These new options are available when you start unattended mode.

Feature	Minimum Threat Defense	Details
New options for downloading upgrade packages	Any	You can now: • Prevent devices from downloading upgrade packages from the internet. That is, you can now require that devices get upgrade packages from the Cloud-Delivered Firewall Management Center or an internal server, even if the devices have internet access. • Specify how long devices retry failed downloads from an internal server or the internet. This setting does not apply to transfers between the Cloud-Delivered Firewall Management Center and device. New/modified screens: **Administration** > **Product Upgrades** > **Global upgrade settings**
Usability		
Redesigned menus for the Cloud-Delivered Firewall Management Center	Any	We redesigned the Cloud-Delivered Firewall Management Center menus to be more intuitive and consistent with the Cisco Security Cloud user interface. A main, single-column menu provides a subset of your most used items, while all items are visible in expanded mode. You can customize which items to include on the main menu to suit your priorities. Preferences are per user. Existing and renamed top-level menus include: • **Overview** is now **Insights & Reports** • **Analysis** is now **Events & Logs** • **Policies**, **Devices**, and **Objects** are the same • **Integration** is now **Integrations** • **System** (⚙) is now **Administration** and appears in the left navigation New top-level menus include: • **Secure Connections** • **Troubleshooting** Some submenus were moved to new main menu locations.

Feature	Minimum Threat Defense	Details
Device Management page enhancements	Any	A redesigned user interface has been launched for the **Device Management** page, offering better usability and enhanced performance. Key improvements include: • **Advanced Search:** Find devices more easily using multiple device-related criteria for more precise results. • **Device Status Banner:** Quickly view the number of devices in **Normal**, **Error**, and **Offline** states, displayed with a color-coded legend for easy identification. • **Performance Enhancements:** Enjoy faster page loading time and pagination that supports up to 1,000 devices per page. • **Streamlined Device Actions:** Perform device actions and bulk operations more efficiently through an intuitive side panel. • **Centralized Troubleshooting:** Access diagnostic tools such as Packet Tracer and Packet Capture from a single, convenient troubleshooting panel. **Note** This enhanced interface is currently in a preliminary phase. You can switch back to the legacy UI to access any features that are not yet available in the new interface. Updated screens: Go to **Devices > Device Management** and enable the **New Device Management UI** toggle button.
VPN		
ACME-based TLS certificate management for remote access VPN	10.0.0	You can now use an ACME certificate to authenticate a managed device as an RA VPN gateway. New/modified screens: **Objects > PKI > Cert Enrollment > Add Cert Enrollment > Enrollment Type > ACME** New/modified commands: **crypto ca trustpoint**
Site-to-site VPN tunnels over IPsec VTIs preserve SGT metadata	10.0.0	Cisco TrustSec uses security group tags (SGTs) to control access and enforce traffic on a network. This option enables SGT propagation over SVTIs and DVTIs of route-based and SD-WAN VPN topologies. To enable SGT propagation on a specific SVTI or DVTI, configure it in individual devices. New/modified screens: • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **SD-WAN Topology** > **Advanced Settings** • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **Route-based VPN** > **Advanced** > **Tunnel**

Feature	Minimum Threat Defense	Details
Site-to-site VPN hub support for ECMP load balancing with dynamic VTIs	10.0.0	You can now enable Equal Cost Multi-Path (ECMP) on the dynamic VTIs of hub devices. All virtual access interfaces on the hub connecting to the same spoke are grouped into an ECMP zone. New/modified screens: • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **SD-WAN Topology** > **Add Hub** • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **Route-based VPN** > **Hub**
Site-to-site VPN support for BFD-based failover	10.0.0	You can now enable the BFD routing protocol on the SVTIs and DVTIs of route-based and SD-WAN VPN topologies. New/modified screens: • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **SD-WAN Topology** > **Advanced Settings** • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **Route-based VPN** > **Advanced** > **Tunnel**
Distributed site-to-site VPN with clustering for the Secure Firewall 4200	10.0.0	A cluster on the Secure Firewall 4200 supports site-to-site VPN in distributed mode. Distributed mode provides the ability to have many site-to-site IPsec IKEv2 VPN connections distributed across members of a cluster, not just on the control node (as in centralized mode). This significantly scales VPN support beyond centralized VPN capabilities and provides high availability. Added/modified commands: **cluster redistribute vpn-sessiondb**, **show cluster vpn-sessiondb**, **cluster vpn-mode**, **show cluster resource usage**, **show vpn-sessiondb**, **show conn detail**, **show crypto ikev2 stats**
Zero trust access		
ACME trustpoint as identity certificate for zero trust access	10.0.0	You can choose an ACME certificate for authenticating a managed device as a SAML SP for a zero-trust application policy. ACME certificates automate the lifecycle management of SSL and TLS certificates, including their auto-renewal. New/modified screens: **Objects** > **PKI** > **Cert Enrollment** > **ACME** New/modified commands: **crypto ca trustpoint**
IPv6 support for zero trust access	10.0.0	Clientless ZTNA now provides secure access to applications connected over IPv6 networks. Limitations: IPv6 source NAT for applications is only for homogeneous scenarios such as NAT66 and NAT44. NAT64 and NAT46 are not supported. New/modified screens: **Policies** > **Zero Trust Application** > **Clientless Policy** > **Add Application** New/modified CLIs: **show running-config zero-trust**

Feature	Minimum Threat Defense	Details
Deprecated features		
End of support: Firewall Threat Defense Version 7.0.x	10.0.0	Cloud-Delivered Firewall Management Center stopped managing Firewall Threat Defense devices, Version 7.0.*x*, as of December 15, 2025. For more information, see frequently asked question.
Deprecated: Enable a DHCP server on the firewall management interface	10.0.0	We deprecated these firewall CLI commands: • **configure network ipv4 dhcp-server-enable** • **configure network ipv4 dhcp-server-disable** • **show network-dhcp-server** See: *Cisco Secure Firewall Threat Defense Command Reference*
Deprecated: Secure Network Analytics manager-only deployments	Any	You can no longer configure a Secure Network Analytics manager-only deployment to store events. Note that manager-only deployments are deprecated in Secure Network Analytics Version 7.5.1. Although existing manager-only integrations continue to work, we recommend you switch to a single-node data store deployment with the latest supported version of Secure Network Analytics. This allows you to take advantage of new features, resolved issues, and performance improvements.
End of support: VMware vSphere/VMware ESXi 6.5, 6.7, and 7.0	Any	**. Upgrade VMware before you upgrade the software.** We discontinued support for virtual deployments on VMware vSphere/VMware ESXi 6.5, 6.7, and 7.0. Upgrade your hosting environment to Version 8.0 before you upgrade any virtual appliance. Version restrictions: Versions 7.3.x and 7.4.0–7.4.1 are not qualified on VMware 8.0. If you run any of these versions, upgrade to VMware 8.0 first. Move to the next step as soon as possible. For best results, perform a multi-step upgrade: first the virtual appliance to 7.4.2–7.7.x, then VMware, then the virtual appliances again.
Deprecated: Monitor device revert in the Message Center	Any	You can no longer monitor device revert from the Message Center. Instead, use the Device Management page (**Devices** > **Device Management**). On the **Upgrade** tab, click **View Details** next to the device you are reverting.
Deprecated: Selected walkthroughs	Any	Some walkthroughs are no longer available. For a list of supported walkthroughs by version, see Walkthroughs in Secure Firewall Management Center.

November 20, 2025

Table 10: Features in Version 20251025

Feature	Minimum Threat Defense	Details
Device Management		
Maximum Firewall Threat Defense Devices Supported.	Any	This release enhances device-management capabilities, supporting up to 1,500 standalone devices, 750 high-availability pairs, or 1,500 cluster nodes. The increased device count improves scalability for complex network environments.

August 14, 2025

Table 11: 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		
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		

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

Open issues

This table lists the currently open issues for Cloud-Delivered Firewall Management Center. As they are resolved, issues move out of this table.

Table 12: Open Issues is Cloud-Delivered Firewall Management Center

Bug ID	Headline
CSCwo13425	Bulk download 400K SXP mappings from ISE takes 80 minutes on FMC4800 with 1500 FTD setup