Release Notes for Cisco Secure Firewall Threat Defense with Firewall Management Center, Version 10

First Published: 2025-12-03

Last Modified: 2025-12-03

Cisco Secure Firewall Threat Defense with Firewall Management Center, Version 10

This document contains release information for Cisco Secure Firewall Threat Defense with Secure Firewall Management Center (on-prem).

Note Version 10 begins a new release numbering scheme and cadence. For more information, see the Cisco's Next Generation Firewall Product Line Software Release and Sustaining Bulletin.

Release Dates

Table 1: Version 10 Dates

Version	Build	Date	Platforms
10.0.0	140	2025-12-03	All

Features

Features in Version 10.0.0

This section provides a brief description of the new features introduced in this release.

Highlights

Feature highlights in Version 10.0.0 include:

- Secure Firewall 200
- Secure Firewall 6100
- Redesigned menus for the Firewall Management Center
- New decryption policy user interface, including basic and advanced policy creation

- Identity-based dynamic access control
- Send security events to Splunk or other SIEM via syslog
- EVE improvements

Reintroduced features

These Version 10.0.0 features were actually introduced in earlier releases, but may be new to you depending on your current version:

- Umbrella integration with Firewall Management Center over a proxy. (7.4.3)
- Migrate select Firepower 4100/9300 models to Secure Firewall 3100/4200. (7.6.1)
- Universal Zero Trust Network Access (universal ZTNA) (7.7.10)

Deployment and policy management

Table 2: Deployment and policy management features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Dynamic security policy enforcement with the Cisco ACI Endpoint Update App and Dynamic Attributes Connector	10.0.0	Any	The dynamic attributes connector enables you to send Cisco APIC dynamic endpoint group (EPG) and endpoint security group (ESG) data from Cisco APIC tenants to the Firewall Management Center. Cisco APIC defines endpoint groups (EPGs) and endpoint security groups (ESGs) that have network object groups. Create a connector in the dynamic attributes connector that pulls that data from Cisco APIC tenants to the Firewall Management Center on which you can use those objects in access control rules.
Simultaneous editing of access control policies by multiple users	10.0.0	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.

Encrypted traffic handling

Table 3: Encrypted traffic handling features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
New decryption policy user interface, including basic and advanced policy creation	10.0.0	Any	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 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	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

Table 4: Hardware features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firewall Management Center 1800, 2800, 4800	10.0.0	Any	We introduced the Firewall Management Center 1800, 2800, and 4800, with better performance and more event storage than current models. For these new models, eth0 is the main management port. You can use eth1, eth2, and eth3 as secondary management ports. The SFP ports are eth0 and eth1. This is different from earlier models.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Secure Firewall 200	10.0.0	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. Limitations include: • No clustering or multi-instance mode. • Smaller vulnerability database. • Cloud-based URL filtering and malware analysis only—no local databases or analysis. • Less frequent Security Intelligence updates. • Minimal default system logging; see Minimal system logging. • Limited health alerts. • Identity limits to user IPs, SXP/SGT mappings, endpoint profiles, and dynamic objects. Limits to IP mappings, users, SGTs, endpoint profiles 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	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. You must manage these devices with a Firewall Management Center. They do not support Firewall Device Manager.
View field-replaceable memory module details for the Secure Firewall 6100	10.0.0	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	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	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.

Health monitoring

Table 5: Health monitoring features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Event datastore alerts when connections fail	10.0.0	Any	The MonetDB Statistics health module now alerts when there are no active connections to the event database, which can indicate connection failure.

High availability/scalability

Table 6: High availability/scalability features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
More container instances (21) on the Secure Firewall 4225 in multi-instance mode	10.0.0	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	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	10.0.0	For asymmetric flows in distributed site-to-site VPN mode, IPsec flow offload now lets the flow owner decrypt IPsec traffic in hardware that was forwarded over the cluster control link. This feature is not configurable and is always available with IPsec flow offload. Added/modified commands: **show crypto ipsec sa detail**

Identity

Table 7: Identity features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Identity-based dynamic access control	10.0.0	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	10.0.0	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

Table 8: Logging and analysis features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Send security events to Splunk or other SIEM via syslog	10.0.0	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	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 Security Cloud Control	10.0.0	10.0.0	Packet data is now included with intrusion events sent to Security Cloud Control.

Model migration

Table 9: Firewall Management Center model migration features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firewall Management Center model migration wizard	10.0.0	7.3.0	A new wizard allows you to easily migrate from one Firewall Management Center model to another. See: Cisco Secure Firewall Management Center Model Migration Guide
Migrate Firewall Management Center 1600/2600/4600 to 1800/2800/4800	10.0.0	7.3.0	Migrate from Firepower Management Center 1600/2600/4600 to Firewall Management Center 1800/2800/4800. See: Cisco Secure Firewall Management Center Model Migration Guide
Migrate Firewall Management Center 4600 to Firewall Management Center Virtual 300 for Azure	10.0.0	7.3.0	Migrate from Firepower Management Center 4600 to Secure Firewall Management Center Virtual 300 for Azure. See: Cisco Secure Firewall Management Center Model Migration Guide

Table 10: Firewall Threat Defense model migration features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Migrate Firepower 4100/9300 to Secure Firewall 3100, 4200, and 6100	10.0.0	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	10.0.0	Any (source) 7.6.0 (target)	Migrate the Firepower 1010 and 1010E to the Secure Firewall 200 and 1200.

Performance and resiliency

Table 11: Performance and resiliency features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Block depletion autorecovery for clusters	10.0.0	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 Management Center	Minimum Threat Defense	Details
Other performance and resiliency improvements	Feature dependent	Feature dependent	We made performance and resiliency improvements to: • Deploying configuration changes • Event datastore on the Firewall Management Center • Event logging to external servers such as syslog or Security Cloud Control, 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

Table 12: Public and private cloud features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firewall Threat Defense Virtual for Microsoft Hyper-V	10.0.0	10.0.0	Firewall Threat Defense Virtual now supports Microsoft Hyper-V.
High availability for Firewall Management Center Virtual for OpenStack	10.0.0	Any	Firewall Management Center Virtual for OpenStack now supports high availability. Platform restrictions: Not supported with FMCv2
Larger default disk size and the ability to resize the disk post-deployment	10.0.0	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.
Unlimited performance tier (FTDvU) for VMware and KVM	10.0.0	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

Feature	Minimum Management Center	Minimum Threat Defense	Details
AWS two-arm Multi-AZ cluster support	10.0.0	10.0.0	FTDv for AWS in two-arm-mode now supports Multi-AZ clustering. The GWLB in each AZ (availability zone) steers traffic to local firewalls for inspection and NAT. If one AZ or firewall fails, workloads in other AZs continue with minimal disruption, and you can scale throughput by adding members per AZ. Platform restrictions: Not supported with FTDv5 or FTDv10.
Azure MANA NIC support	10.0.0	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
GCP autoscale with clustered devices	10.0.0	10.0.0	Firewall Threat Defense Virtual now supports GCP autoscale (dynamic scaling) with clustered devices, using a Terraform template.
Nutanix AOS 6.8 support	10.0.0	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	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	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
Secure Boot and UEFI firmware support	10.0.0	10.0.0	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.

Routing

Table 13: Routing features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Use PBR to handle traffic based on custom application patterns.	10.0.0	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	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

Table 14: Threat detection and application identification features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
EVE improvements	10.0.0	10.0.0 (widgets) Any (all others)	**Upgrade impact. Upgrade merges EVE exceptions, changes the EVE blocking level, and begins using EVE for application detection.** EVE improvements include: • EVE configuration moved from the access control policy advanced settings to the 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. Firewall Management Center upgrade changes very low, low, and medium blocking thresholds to high, in policies that block based on EVE threat confidence. • EVE is now automatically used for application detection when you enable EVE. Firewall Management Center upgrade enables EVE-based application detection in access control policies where EVE is enabled. • EVE exceptions are now objects, and are automatically shared across all access control policies. Firewall Management Center upgrade moves existing exceptions to object management. Access control policies that use EVE now use the merged set of exceptions. • 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	10.0.0	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. After Firewall Management Center upgrade, existing application-based rules that do not have manual port conditions are applied to **Any** port. To take advantage of this feature, edit the rules you want to limit.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Dynamic objects and security group tags in DNS rules	10.0.0	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	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 the 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	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.
Unauthorized privacy technology (shadow traffic) detection	10.0.0	10.0.0	A new Shadow Traffic dashboard (**Insights & Reports** > **Dashboard** > **Shadow Traffic**) monitors unauthorized privacy technology such as encrypted DNS, evasive private VPNs, multi-hop proxies, domain fronting, and fake TLS. Also, connection and unified events now have a Shadow Traffic Type field. Shadow traffic monitoring is auto-enabled by the upgrade. To disable it, use the access control policy advanced settings.
Updated internet access requirements for security intelligence feeds	10.0.0	Any	**Upgrade impact. The system connects to new resources.** The system now gets Security Intelligence feeds from: • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com • Security Services Exchange regional cloud If you are using regular Smart Licensing, registering with Smart Software Manager (CSSM) sets up SSE integration. If you are using Specific License Reservation in a non-airgapped deployment, enable Security Cloud Control for access to the Security Services Exchange regional cloud. The system no longer requires access to intelligence.sourcefire.com.

Troubleshooting and serviceability

Table 15: Troubleshooting and serviceability features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
MTU ping test on cluster node join provides more information by trying smaller MTUs	10.0.0	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	10.0.0	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	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	Any	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	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 Management Center	Minimum Threat Defense	Details
Recovery-config mode support for NAT and other interface commands	10.0.0	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	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

Table 16: Upgrade features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
New device and chassis upgrade wizard	10.0.0	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.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Prepare-only and skip-checks options for unattended Firewall Threat Defense upgrade	10.0.0	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.
New options for downloading upgrade packages	10.0.0	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 Firewall Management Center or an internal server, even if the devices have internet access. • Specify how long the system retries failed downloads from an internal server (devices only) or the internet. This setting does not apply to transfers between the Firewall Management Center and device. New/modified screens: **Administration** > **Product Upgrades** > **Global upgrade settings**
Auto-replace outdated Firewall Management Center upgrade scripts	10.0.0	Any	The Firewall Management Center can get new upgrade scripts for itself from the internet, fixing late-breaking upgrade issues without replacing the whole upgrade package. If the Firewall Management Center cannot download new scripts for any reason, the upgrade proceeds as it would have without them. If you encounter issues with Firewall Management Center upgrade, including a failed upgrade or unresponsive system, contact Cisco TAC. Download location: cdo-ftd-images.s3-us-west-2.amazonaws.com

Usability

Table 17: Usability features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Redesigned menus for the Firewall Management Center	10.0.0	Any	We redesigned the Firewall Management Center menus to be more intuitive and consistent with the Security Cloud Control 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.

VPN

Table 18: Remote access VPN features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
ACME-based TLS certificate management for remote access VPN	10.0.0	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**

Table 19: Site-to-site VPN features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Site-to-site VPN tunnels over IPsec VTIs preserve SGT metadata	10.0.0	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**
Site-to-site VPN hub support for ECMP load balancing with dynamic VTIs	10.0.0	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	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	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

Table 20: Zero trust access features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
ACME trustpoint as identity certificate for zero trust access	10.0.0	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	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**

Deprecated features

Table 21: Deprecated features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: Legacy screens used to register a device with a registration key	10.0.0	Any	The legacy screens used to register a device with a registration key are deprecated. On the Device Management page, **Add** > **Device** now launches the wizard and **Add** > **Device (Wizard)** was removed.
Deprecated: Enable a DHCP server on the firewall management interface	10.0.0	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

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: Secure Network Analytics manager-only deployments	10.0.0	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.
Deprecated: database access	10.0.0	Any	External access to the Firewall Management Center database is no longer supported. After upgrade, all integrations stop working. The option to enable database access is removed. The External Database User role and users remain, but cannot be used except to access the online help. We recommend you remove this role from existing users and do not enable it for new users.
End of support: VMware vSphere/VMware ESXi 6.5, 6.7, 7.0, and 7.5	10.0.0	10.0.0	**Upgrade impact. Upgrade VMware before you upgrade the software.** We discontinued support for virtual deployments on VMware vSphere/VMware ESXi 6.5, 6.7, 7.0, and 7.5. 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	10.0.0	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: Legacy theme	10.0.0	Any	We deprecated the Legacy theme. If you were using the Legacy theme, the upgrade switches you to the Light theme.
Deprecated: Selected walkthroughs	10.0.0	Any	Some walkthroughs are no longer available. For a list of supported walkthroughs by version, see Walkthroughs in Secure Firewall Management Center.

Branding

Table 22: Branding in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cisco Security Cloud is now Cisco Security Cloud Control	10.0.0	Any	Cisco Security Cloud is now Cisco Security Cloud Control. Integration allows you to leverage cloud-delivered intelligence, unified visibility, and simplified management.

Related updates and deprecations

Intrusion rules and keywords

Upgrade impact: Upgrades can import and auto-enable new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings.

Details: If a newer intrusion rule uses keywords that are not supported in your current version, that rule is not imported when you update the SRU/LSP. After you upgrade and those keywords become supported, the new intrusion rules are imported and, depending on your IPS configuration, can become auto-enabled and thus start generating events and affecting traffic flow. For details on new keywords, see the Snort release notes: https://www.snort.org/downloads.

FlexConfig

Upgrade impact: Upgrades can add web interface support for features that previously required FlexConfig. Upgrades do not convert FlexConfigs, but can affect your existing FlexConfigs and cause post-upgrade deployment issues.

Details: In most cases, existing FlexConfigs continue to work and you can still deploy. However, you cannot newly assign or create FlexConfig objects using deprecated commands. And sometimes, using deprecated commands can cause deployment issues. After upgrade, configure the newly supported features in the web interface. When you are satisfied with the new configuration, delete the deprecated FlexConfigs. The descriptions here include information on any deprecated FlexConfigs in this major version . For a full list of deprecated FlexConfigs, see your configuration guide.

Integrations and logging

Various integrations and logging facilities (such as the REST API) may have new features associated with firewall releases. See Related resources, on page 57.

Resolved issues

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

Table last updated: 2025-12-03

Table 23: Resolved security issues in Version 10.0.0

ID	Headline
CSCwa38880	Order of access-list/ access-group is different in standby unit. Full sync happens during node-join.
CSCwh10931	ASA/FTD traceback and reload when invoking "show webvpn saml idp" CLI command
CSCwk72477	Custom rule with "metadata:impact_flag red" in Snort3 not detected as Impact Level 1
CSCwm50895	Additional tab/space added in ACL logging messages in EMBLEM format causing ingestion issues
CSCwm82231	Evaluation of multiple Azul Zulu vulnerabilities on openjre ASDM

ID	Headline
CSCwm95074	[FMC HA] Follower accepts data only from 1 leader
CSCwm95189	Redis is an open source, in-memory database that persists on disk. An
CSCwm95191	In the Linux kernel, the following vulnerability has been resolved: s
CSCwn24777	ASA block depletion due to SSL pre auth connections
CSCwn55253	FMC GUI does not Accept "@" in the username for remote storage used for backups
CSCwn73399	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability
CSCwn78991	FMC Legacy UI allows you to create time range objects in past time in ACL
CSCwn86187	FTD native: ldap configuration fails to deploy to ftd when using same user as radius
CSCwn86912	Unable to load Extended ACL objects if the count is more than few hundreds
CSCwn90958	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Authenticated Command Injection Vulnerability
CSCwn91612	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Authenticated Command Injection Vulnerability
CSCwn91730	FMC API put taking long time to update Extended ACL objects when count is huge like hundreds
CSCwo00332	Firepower wiping SSL trustpoint config after reloading.
CSCwo00880	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Server Denial of Service Vulnerability
CSCwo14426	Unable to save the Ext ACL object - "Only Host and Network in IPv4 and IPv6 format are supported."
CSCwo15021	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability
CSCwo15022	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability
CSCwo15023	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability
CSCwo15024	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability
CSCwo15026	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability
CSCwo15027	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability

ID	Headline
CSCwo18850	Cisco Secure Firewall Adaptive Security Appliance, Secure Firewall Threat Defense Software HTTP Server Remote Code Execution Vulnerability
CSCwo20522	Cisco Secure Firewall Management Center Software Command Injection Vulnerability
CSCwo35938	IPv6 Management communication is lost due to a missing management-only multicast route.
CSCwo44732	ARP is silently dropping packet for an unreachable next hop
CSCwo48439	Traceback & Reload in Thread Name Unicorn Admin Handler
CSCwo49928	Cisco Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability
CSCwo52298	Duplicate ACLs seen on FMC UI when Access Rules are created through API
CSCwo56698	Cisco Secure Firewall Threat Defense Software Geolocation Remote Access VPN Bypass Vulnerability
CSCwo71401	Multiple Cisco Products Snort 3 MIME Denial of Service Vulnerabilities
CSCwo78475	Traffic hits incorrect ACP rules during policy deployment on FTD with dynamic objects
CSCwo91250	Cisco Secure Firewall Management Center Software Radius Remote Code Execution Vulnerability
CSCwo91748	Lina: Traceback in thread name ssh on executing show access-list after ACL deletion
CSCwo92790	Route map object ACL match clause overwrited in all route maps objects after saving changes.
CSCwo97439	ACL: ASA may show false "OOB Access-list config change detected" warning after AAA authorization command is applied
CSCwp05496	Cleaning of /var/temp backup files post Backup completion not cleaning
CSCwp09920	Policy Deployment: When using MD5 in Site-to-Site VPN, manual deployment fails with validation error, but schedule deployment succeeds.
CSCwp10889	Packet-tracer displaying incorrect ACL even though traffic action is taken based on the expected ACL.
CSCwp62846	Reverting FTD upgrade silently removes object overrides on the FMC for the reverted FTD
CSCwp66127	PAO logic for access rules POST/PUT api call for spaces in ip addresses in ACL rules
CSCwq03404	External auth login with RADIUS to FMC UI may fail if Class attribute is used
CSCwq10344	FMC RADIUS external authentication access requests missing 6 attributes after FMC upgrade

ID	Headline
CSCwq15864	Multiple Cisco Products Snort 3 MIME Denial of Service Vulnerabilities
CSCwq18679	ASA from CSM/CLI - no access-list ACL_name line line_nr remark on last ACL line shows message - "Specified remark does not exist"
CSCwq21101	Invalid host header reveals ASA interface IP address
CSCwq39943	CVE-2025-32462: sudo: Before 1.9.17p1, allows users to execute commands on unintended machines.
CSCwq40256	Inbound IPsec packets are dropped by IPsec offload when the crypto map ACL is using specific ports.
CSCwq74738	RAVPN SSL/IKEV2 AUTH FAILURE: AAA PROCESS MISHANDLING BROKEN FIBER CLASS
CSCwq74813	FMC: Copy/Cut/Paste or drag/drop ACE in Extended ACL object, deletes existing Rules
CSCwq78991	Firewall joins a cluster although gets incomplete ACL policy rules during replication
CSCwq79815	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Unauthorized Access Vulnerability
CSCwq79831	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Remote Code Execution Vulnerability
CSCwq82095	SAML response rejected with message for certain IDPs
CSCwq82225	Drop counter doesn't increment for embryonic related drops in 'show service policy'
CSCwq86692	Invalid OSPF process popup blocking route-map configuration
CSCwq97365	FMC: Realm sync after import, un assigns IPS policies configured in ACEs
CSCwr04957	Deployment failure or traffic not matching configured rules after renaming several objects
CSCwr60176	uZTNA Private resource not working due to hztna CRT expiration on FTD
CSCwr80920	SFDataCorrelator backtrace every 1 hour after VDB update on FMC
CSCws15464	FMC UI route-map access list stuck

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

Table last updated: 2025-12-03

Table 24: Resolved functional issues in Version 10.0.0

ID	Headline
CSCvh98118	"logging debug-trace persistent" fails for "debug ip ..." related debugs

ID	Headline
CSCvm76755	DP-CP arp-in and adj-absent queues need to be separated
CSCvu71962	User-Role permission for Object-MGMT "Find-Usage"
CSCvx66624	Write cache is disabled on some FMC M5 appliances
CSCwb07908	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
CSCwb34868	Add UI message when user attempts to switch role from standby FMC with pending device registration: Chassis and Device
CSCwc57341	Inline pair has incorrect FTW bypass operation mode of 'Phy Bypass'
CSCwc82675	ASA/FTD : High LINA memory observed after configuring multiple AnyConnect packages
CSCwc85758	Last Synchronized date in FMC smart license status is not always accurate
CSCwd54466	New realm user are incorrectly getting mapped to discovered user
CSCwd55939	scheduled task may not run at all if UTC start times (based on DST) are on different calendar days
CSCwd80348	FMC does not support Umbrella with proxy setting
CSCwd92327	on 2k platform, external authentication fails for users starting with number
CSCwe39331	Snort3 Rule Recommendations - add error message if Network Discovery is not configured
CSCwe89720	Misleading error message while attemtping to revert upgrade on inelligible device
CSCwe89818	External Auth on FMC may throw err "Can't use string ("") as a HASH ref while "strict refs" in use"
CSCwf04460	The fxos directory disappears after cancelling show tech fprm detail command with Ctr+c is executed.
CSCwf25454	Stale anyconnect entries causing issues with routing
CSCwf61982	Edit search page and unified event viewer very slow to load due to high number of search-related EOs
CSCwf72285	DAP: debug dap trace not fully shown after 3000+ lines
CSCwh08441	ENH: Add a command or a script to regenerate CA Certificate on FTD
CSCwh30257	snort3 crashes observed due to memory corruption in file api
CSCwh41925	Lina traceback in ZMQ Proxy caused service loss.
CSCwh53745	ASA: unexpected logs for initiating inbound connection for DNS query response
CSCwi23799	ENH : ASDM does not accept VTI Interface for routes, CLI works

ID	Headline
CSCwi39206	3100/4200: qdma driver watchdog timeout
CSCwi51611	FTD 7.4.1 Snort shows 100% utilization even at a low traffic rate
CSCwi52008	Snort3 traceback and restarts with race conditions
CSCwi95690	Fault "Adapter 1/x/y is unreachable" due to connectivity failure between supervisor and VIC adapter
CSCwj14242	Applications are incorrectly identified as TOR and blocked by Snort3
CSCwj50557	Snort creating too many snort-unified log files when frequent policy deploys
CSCwj63921	Snort3 traceback and reload due to memory corruption in file module
CSCwj66537	Snort3 crashes due to processing pdf tokenizer with no limits.
CSCwj91420	Snort3 crashes while collecting flow-ip-profiling
CSCwk09488	Incorrect syslog generated on failure to process SGT from ISE during RA authentication
CSCwk22814	FMC - Add warning message when configuring CCL MTU
CSCwk33387	SNMP for mgmt0/diagnostic outgoing traffic is missing
CSCwk40403	WebEx traffic not getting bypassed in snort3 (allow rules)
CSCwk42676	Virtual ASA/FTD may traceback and reload in thread PTHREAD
CSCwk64399	ASDM- Unable to edit Secure Client Profile
CSCwk80292	FMC : DAP configuration "laggy/hangs" when trying to configure via FMC.
CSCwk83680	Increase sftunnel AUTH_TIMEOUT to 60
CSCwm04866	debug menu command to prevent 1550 block depletion due to sendinglogs to TCP syslog server
CSCwm05155	Snort AppID incorrectly identifies SSH traffic as Unknown
CSCwm07323	Creating cluster bundle tar files for cluster failing with remote storage SSH configured
CSCwm10676	FMC unable to search Objects when there is a DNS configured
CSCwm27355	Add timestamps into bash_history
CSCwm40278	S2S VPN config removed unexpectedly after deployment
CSCwm41381	File Download fails intermittently with malware & file policy configured
CSCwm51747	SSH access with public key authentication fails after FXOS upgrade
CSCwm61345	FXOS: Directory /var/tmp Triggering FXOS Fault F0182 due to vdc.log (Excessive Logging,Log Rotation)

ID	Headline
CSCwm63648	Set Weight option missing in UI when FTD sensor reverted and re-upgraded
CSCwm63670	Propogate SGT deployed to FTD if copy deviceconfiguration(SGT configuration UI andLINA doesnt match)
CSCwm63890	FMC GUI does not allow saving ECMP configuration when there is a route leak for a VRF
CSCwm67644	FMC find usage feature not showing all associated access control policies for random objects
CSCwm74289	NAT traps have to be rate-limited
CSCwm77055	FMC/FTD: Policy Deployment Fails For Existing FTDv Deployments on Cloud with VNI interfaces
CSCwm80082	Alert user that FDM is not Supported for FTDv in Openstack if they try to enable it
CSCwm80580	snort "exits normally" in loop every 1 min resulting in complete outage
CSCwm82566	FMC displays VPN tunnel status as unknown even when the tunnels are up
CSCwm83033	Invalid Name Warning Missing from FMC after upgrade and Save greyed out (Configure DAP records through Rest API)
CSCwm87653	Unused objects deletion taking longer time
CSCwm87669	Discrepency in the unused object count between the FMC UI and API results
CSCwm94971	Secure Client Connection Profile Address Pool not Shown
CSCwm96652	Cluster assigning wrong nat for unit, traffic not being forwarded properly back to unit
CSCwm99199	MariaDB import failure that lead to FMC-HA Synchronization Incomplete
CSCwn07008	Use of Named interface in SLA Monitor causing cdFMC migration failure
CSCwn07555	Switch FMC-HA fails: MariaDB replication is not in good state - can not sync
CSCwn10661	FTD running on FPR2k devices, using CMI, has no ARP for 203.0.113.129
CSCwn10680	FTD deployment fails with error "Snort command failed due to bad config"
CSCwn19190	Memory fragmentation resulted in huge pages unavailable for lina
CSCwn21227	Snort3 Crashinfo not decoding certain lines with "no unwind info found"
CSCwn21446	FMCv300 not consuming any FMCv300 device license
CSCwn22610	fs-daemon hap reset with core generation
CSCwn25430	Secure Client External Browser package Image shown 2 same packages

ID	Headline
CSCwn26150	policy_deployment.db does not get updated with the correct anyconnect/secure client version
CSCwn27872	Big chunk of Memory of around 25KB is being allocated on Stack in "eigrp_interface_ioctl" API
CSCwn28902	FMC not using configured proxy for smart licensing
CSCwn32978	Traceback and reload in Thread Name Datapath
CSCwn35495	Primary FTD instance MAC address is not updated correctly in FXOS during failover
CSCwn36712	NAT divert for 8305 on standby not updating post failover causing the Primary, standby FTD to show offline on FMC
CSCwn37490	ACP copy not possible in Firepower Management Center
CSCwn37993	Longevity setup:TPK cluster node is displayed as empty cluster in device mgmt page
CSCwn39081	SNMP walk results in ASCII value for IPSEC Peer instead of an IP address.
CSCwn39777	Unreachable Hosts and URLs of syslog configuration Block Device Management Page Loading
CSCwn40572	MI: Vlan info is not applied at FXOS level when Virtual MAC is configured
CSCwn40702	ASA traceback and reload in freeb_core_local_internal
CSCwn42696	FDM Order of reading nested object group indexing is causing deployment failure
CSCwn44527	Intrusion policy having same name in different Domains causes IPS policy corruption
CSCwn45049	Coverity System SA warnings 2024-09-09, Coverity Defects 922530 922529 922528 922630 921809 921808
CSCwn45510	S2S VPN tunnel Child SA unsuccessful renegotiation
CSCwn47308	Critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on FPR 1100/2100/3100
CSCwn49391	Frequent traceback after upgrading FTD HA
CSCwn49611	Remove the File Capture Disk Manager SILO to prevent captured files from overwhelming the Disk Mgr
CSCwn50245	On FMC, Backend server JVM is running out of memory when policies and objects are huge
CSCwn50760	ASA Traceback after upgrade to 9.20.3.7
CSCwn50961	Send Virtual Tunnel Interface enabled by default on SVTI
CSCwn51845	Tracebacks observed in a cluster member running ASA 9.20.3.4

ID	Headline
CSCwn59032	FCM GUI became inaccessible after upgrading to ASA 9.18.4.22 | FPR 2130 Platform Mode
CSCwn59379	Bandwidth information of a port-channel is not getting updated if an interface member goes down.
CSCwn59447	FDM RA VPN SAML UI does not set port in base-url when custom webvpn port is used
CSCwn59596	“Copy when complete” option not working for SSH Public Shared Key Authentication on FMC
CSCwn60726	Traceback and reload with Thread Name: vtemplate process
CSCwn61041	Traceback and reload during clear bgp * ipv6 unicast involving watchdog
CSCwn63839	Traceback in thread name Lina on configuring arp permit-nonconnected with BVI
CSCwn64025	ASA: IPv6 EIGRP routes learned from other neighbors are missing in updates after failover
CSCwn64992	FMC1600-K9 PDF download failed in deploy tab
CSCwn65415	ASA: floating-conn not closing UDP conns if conn was created without ARP entry for next hop
CSCwn69340	cdFMC - Unable to save network group object
CSCwn69488	ASA/FTD - Traceback and Reload in Threadname IP RIB Update
CSCwn71426	Clearing all non applicable alerts post license registration success
CSCwn71596	Intf Link down (Init, mac-link-down) seen - EtherChannel Membership in Down/Down/Down state after unplug/replug of the cable
CSCwn71946	show blocks old core local can lead to unexpected reload.
CSCwn72938	Smart license UI on cdFMC and FMC showing duplicate license count for Malware , IPS , URLFilter and Apex
CSCwn73299	RA VPN Config Error -- Import PKCS12 operation failed - Deployment Failure
CSCwn73351	Asia/Bangkok timezone option not listed in ASA running on firepower1k
CSCwn75667	Banner motd does not display when configured
CSCwn76079	SSH works in admin context but doesn't work in any user context after changing ssh key-exchange
CSCwn76475	Event-list not deployed when using Enable All Syslog Messages
CSCwn76548	Block S2S and remote access configurations for public cloud cluster
CSCwn76740	FMC UI login fails with "Unable to authorize access."

ID	Headline
CSCwn77876	loading an ECDSA certificate into the FMC causes Auth Daemon to crash and reload repeatedly
CSCwn78693	FMC: OSPF NSF-awareness (helper mode) cannot be configured on a standalone FTD
CSCwn79553	Unreachable LDAP/AD referrals may cause delays or timeouts in external authentication on FTD
CSCwn80419	Need the SVC Rx/Tx queue as a configurable option
CSCwn80762	FMC does not remove community list override when this is modified.
CSCwn80765	ISA3000 with ASA Refuses SSH Access If CiscoSSH is Enabled
CSCwn81118	RTSP packets getting stuck in transmit queue leading to 9k blocks exhaustion.
CSCwn81398	FMC Does not throw error with duplicate entries in input while modifying prefix list through API
CSCwn81784	Choosing clause 91 FEC via the FMC sets fec 544 instead of fec 528 on QSFP-100G-CU3M
CSCwn81995	Traceback and Reload caused by Memory corruption with SNMP inspection enabled
CSCwn83268	Realm with greater than 16 directories cannot be deployed in RA-VPN for LDAP
CSCwn84258	Confusing Verdict for Snort Injects - Change From Block to "Replaced"/"Injected"
CSCwn84736	FDM - All IPSec tunnels get reset after changing PFS value for one tunnel
CSCwn84743	User EO revisions accumulate forever, eventually overflowing Pruner's ability to do its job
CSCwn85765	ipv6 ping Vrf name changed after xml processing
CSCwn86002	core corruption still seen with switching to quick core feature
CSCwn87249	snort3 : FMC connection event logs do not show URL in DNS query using TCP
CSCwn87513	ASA clock is out of sync 2 hours when timezone is configured to Europe/Dublin which is GMT.
CSCwn89243	Identity NAT should not throw error due to exceeding threshold if destination only objects expand
CSCwn90327	FP1150 ASA/FTD - Traceback and reload triggered by watchdog timer
CSCwn90798	lucene directory missing from FDM backup
CSCwn90900	High ASA/FTD memory usage due to polling of RA VPN related SNMP OIDs
CSCwn91996	WM-DT-7.7.0-40:: Observed switch config failed and switch Mac error on device console

ID	Headline
CSCwn92066	FTD Clish: "more.fxos" process is left running when the ssh terminal session is abruptly terminated
CSCwn92507	FMC Not listing the any connect images in RAVPN Wizard and FMT tool
CSCwn92894	Occasionally, 'show chunkstat top-usage' output does not show all entries
CSCwn93319	ASA/FTD may traceback and reload in Thread Name "DATAPATH"
CSCwn93411	FXOS reset and reload due to snmpd service failure
CSCwn95719	Create report option should be hidden from Health Events Page on CDFMC
CSCwn95939	Generate syslog if received CRL is older than cached CRL
CSCwn95945	Generate syslog if received CRL signature validation fails
CSCwn96928	URL getting allowed even with block rule in place.
CSCwn96929	ASA: Traceback and Reload Under Thread Name SSH
CSCwn96963	FTD generates syslog 430002 as VPN Routing without VPN hairpin
CSCwn97610	Policy Deployment Failure Due to Special Characters in AC Policy Rule Names
CSCwn97630	FTD reboot and traceback in DATAPATH due to IPv6 packet processing
CSCwn97956	Error thrown for individual rule hitcount if rule name contains certain special characters
CSCwn98402	Debuggability: FP2100 port-channel interfaces flap after upgrade
CSCwn98552	Tunnel Summary and Topology View in S2S monitoring doesn't display the right status.
CSCwn98642	Dynamic Analysis Status Changed time only changes upon submission of a file for dynamic analysis
CSCwn98665	Use of browser Refresh button on the Captured File Summary page may result in an unexpected warning
CSCwn99640	FTD Upgrade Failure on Script 800_post/020_710_fix_users_and_roles.pl
CSCwn99755	Warning messages from using Analyze button on Captured File Summary page need to be more specific
CSCwo00102	Snort3 trimming packets with invalid sequence number due to bad window size information received
CSCwo00225	VNI source MTU is not IPv6 aware after upgrade if configured prior to upgrade
CSCwo00444	Nitrox Engine (Crypto Accelerator) problem affecting crypto hardware offload on FPR3100/4200 platforms
CSCwo00702	Community lists should not throw an error until the last item in the list is being deleted

ID	Headline
CSCwo01616	sfipproxy prometheus configuration is attempted for not supported models and replaces sfipproxy.conf
CSCwo01653	Unable to login to FMC GUI due to HTTP 401 UNAUTHORIZED error
CSCwo03932	Aggressive scale down and scale up of nodes causing the failure
CSCwo05712	Serviceability Enhancement - Make FXOS disk errors more descriptive
CSCwo05801	SNMP walk on FXOS 2.14.1.167 causing warning loop
CSCwo05899	ZIP files are not being transferred when Archive category is selected from File Policy using snort3
CSCwo06044	Exclude perf monitoring files from device backup
CSCwo08042	ASAv reloaded unexpectedly with traceback on Unicorn Proxy Thread
CSCwo08306	Command authorization fallback to Local only works for users with privilege 15.
CSCwo08724	Active HA unit goes into failed state before peer unit gets into a ready state during snort failure
CSCwo09060	SSL trustpoint with 4096 bit RSA keys not allowed by ASA if renewed via CLI
CSCwo09195	Traceback and reload during the deployment after disabling FQDNs.
CSCwo09439	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-3-4280'
CSCwo09618	Enabling debugs with EEM fails
CSCwo09921	The whois lookup command for the FMC GUI does not properly handle errors
CSCwo12801	Detectors sync issue on FMC upgraded to 7.7
CSCwo13550	Dispatch queue drops have no snapshot or tuple view for dropped flows
CSCwo13863	Snort3 crashed because don't fragment bit was set and it did not treat ipv4 fragments as fragments
CSCwo14115	FDM: De Registration stuck with this error: Licensing task is in progress
CSCwo14706	Buffer calculation for new app_bin missing in the upgrade framework
CSCwo14722	Prune the older files in /ngfw/var/cisco/deploy/pkg/var/cisco/packages
CSCwo14737	FTD - LSP Installation/ Deployment Failure
CSCwo14870	FMC upgrade page shows upgrade failed but the device is upgraded
CSCwo15059	Backup may fail with generic "Backup died unexpectedly" error message
CSCwo15715	IKEv2 Rekeys fail due to fragmentation during the IKE Rekey

ID	Headline
CSCwo15787	Importing SFO fails with the error "No UUID Provided"
CSCwo16049	False alert "Terminating long running backup" on FMC due to UI backup timeout error.
CSCwo16488	FXOS allows booting and starting an image installation using a Patch image
CSCwo18786	Snort3 restart on the first deployment post FMC upgrade.
CSCwo18838	ASA/FTD may traceback and reload in Thread Name 'lina_exec_startup_thread'
CSCwo18883	FMC removes prefix-list overides used for BGP and installs defaults values by itself.
CSCwo19762	Unable to rejoin data node in cluster after re-enabling mac-address auto in multi-context mode
CSCwo19986	FTD TS is collecting duplicated data
CSCwo20629	Better handling of invalid/bad data in fleet upgrade workflow.
CSCwo21105	process_stderr.log: Could not open link aggregation log file '/ngfw/var/log/link_aggregation.log'
CSCwo21767	Port scan alerts not getting generated for custom configuration
CSCwo21830	Reduce TS package size
CSCwo22091	FTD sending "0.0.0.0" NAS-IP-Address attribute when authenticating/authorizing using Radius
CSCwo24772	debug packet-condition does not work as expected
CSCwo24856	9K block depletion causing slowdown of all traffic through firewall
CSCwo25236	Suddenly customer lost SSH access to the ASA
CSCwo25271	Empty snapshot being sent when when auth-daemon restarts causing user logout
CSCwo25473	DNS and default gateway are removed on FTD managed through data interface - DNS
CSCwo25478	auth-daemon process restarts due to race condition
CSCwo25624	Deployment failure due to invalid AnyConnect Images and Secure Client Profile references
CSCwo25786	REST Api allows to create a realm without a directory configuration
CSCwo25834	Enhance Backup Status Notifications for Unified Backup Failures on FMC
CSCwo25854	Upgrade failure after RMA due to Sensor table having incorrect serial number
CSCwo26181	Unexpected SFDataCorrelator exit after deployment to managed devices following VDB install on FMC

ID	Headline
CSCwo26258	Default Route Changes from Management0 to Management1 After Reload or Upgrade on FPR 4200 Series
CSCwo26286	Management1 Gateway Configuration Should Be Optional on FPR 4200 Series
CSCwo26725	FMC Site-to-Site Monitoring Dashboard is not working at all
CSCwo27260	Unit taking ~13 secs to become active
CSCwo28967	FMC remote storage test sometimes fails when configured to a server running Solar Winds SCP/SFTP
CSCwo31094	Virtual ASA Traceback and Reload Caused by Disk Access Issues with NFS Enabled
CSCwo31418	AC policy with Network Group Override object causes deployment failure/rules missing
CSCwo31467	TLS.- Outlook only supports TLS 1.2 and not 1.3- FMC uses TLS 1.3 by default
CSCwo32030	LSP upload/download + auto-deploy is failing
CSCwo32845	Disable Reverse Path Filter for Dual Management Interfaces on FPR 4200 Series
CSCwo32943	Active FMC - False alerts of FMC HA in degraded sync state
CSCwo33573	FMC Alert: Discover Health Module Compilation Error
CSCwo33733	CIMC Password length restricted to 16 characters with LOM enabled
CSCwo33815	FMC: Deployment takes longer than expected when removing SNMP hosts from Platform Settings
CSCwo34116	FTD upgrade allowed with dirty policy after FMC upgrade
CSCwo34220	Random QOS policies are getting negatted and added with subsequent deployment
CSCwo34580	First cycle of FMC HA periodic sync may fail after resuming sync following FMC software upgrade
CSCwo34893	Remote storage server password showing in plaintext in httpsd_error_log
CSCwo35585	AMP related health alert during upgrade and typo in the alert message
CSCwo35783	Enhance Debugging for add/update/withdraw of routes with neighbors
CSCwo35784	Deployment due to system upgrade is failing at PREPARE phase in FDM-HA
CSCwo35788	Serviceability Enhancement - New 'show bgp internal' command for advanced debugging
CSCwo36485	ASA/FTD traceback and reload in vaccess_nameif_action thread
CSCwo37055	FMC: Media type displayed on the FMC's FCM is not matching CLI after swapping sfps

ID	Headline
CSCwo37500	Remote backup generated successfully but configuration database backup is empty
CSCwo38354	Smart license UI showing variable performance tier when stand by FMC is made active
CSCwo38829	cdFMC does not show more than 25 realms in the GUI
CSCwo38855	sftunnel and sfipproxy configuration files updates are not atomic
CSCwo39711	Getting " Realm is disabled, enable it on the Realms page " while adding dynamic attributes
CSCwo41250	Traceback & Reload in thread named: DATAPATH-1-23988 during low memory condition
CSCwo41594	SSL Debug Logs Persist After Debug Reset
CSCwo42102	show tech-support fprm detail command is getting stuck for longer duration
CSCwo42139	Snort3 traceback and deployment failure with VDB upgrade
CSCwo42230	Memory leak leading to split brain
CSCwo42326	ENH: Include SystemID in "show system detail" in techsupport file
CSCwo42501	Module show tech generation fails with external authentication
CSCwo45449	Ensure the watchdog triggers even if a single snort3 thread becomes unresponsive.
CSCwo45497	Counter from IKEV2 stats does not match the number of tunnels in VPN-Sessiondb
CSCwo45848	SecGW: Data node fails to join the cluster with cluster_ccp_make_rpc_call failed to clnt_call error
CSCwo46142	Port-channel member interface flap renders it as an inactive member
CSCwo46533	sfipproxy may not restart and fail services like User Identities when enable file is not detected
CSCwo47498	Disabling OSPFv3 on FMC does not clear passive interface and area config from FTD interfaces
CSCwo47760	FMC IPsec SA remaining key lifetime incorrect conversion of seconds to hh:mm:ss
CSCwo47929	Cluster node got deleted partially and devices have become Standalone on FMC UI
CSCwo47978	ASA may traceback and reload in Thread Name 'fover_parse'
CSCwo48157	syslog-ng may not immediately restart on FTD as expected upon changing FTD host name
CSCwo48607	Installation of Hotfix may fail at 800_post/998_expire_ac_policy.pl on the standby FMC
CSCwo48630	Deployment is failing due to the policy changes report request in progress

ID	Headline
CSCwo49337	FMC - Health Monitor shows 'No Data Available' due to too many open files
CSCwo49425	Logging recipient-address not overriding the logging mail message severity levels
CSCwo49658	After upgrade from newer lower MR to Old Higher MR seeing health module compilation error
CSCwo49744	DNS and default gateway are removed on FTD managed through data interface
CSCwo50417	Warwick Avenue: LLDP neighbours are not discovered if MGMT 1/2 interface is down
CSCwo50551	Decryption policy failed to migrate to cdFMC from on-prem FMC.
CSCwo50885	/mnt/disk0/log folder duplicated on troubleshooting package
CSCwo52127	Generic or irrelevant error for remote storage device test/save failures
CSCwo52139	Error after logging out from FMC UI using SSO with PingId
CSCwo53892	FTD health metrics show "No data available" on the FMC
CSCwo54265	Upgrading a 7.0.x sensor to 7.0.7 when managed by an FMC via hostname results in errors
CSCwo54755	Serviceability enhancement for "system support trace" capabilities
CSCwo54996	Traffic failure due to 9344 blocks leak
CSCwo55662	FMC Rest API returns only the first 1000 network object entries
CSCwo56243	Snort3 Traceback due to watchdog during appid NAVL instantiation
CSCwo57740	'${dsk_a} missing or inoperable. Rebooting Blade.' error does not specify missing or inoperable disk
CSCwo57744	Overrides not working on chained/inherited custom IPS policies
CSCwo58033	[Cluster] CPU Utilization of 100% when NAT Pool exhaustion happens in a context.
CSCwo58191	FTD: Large Delay in packets being inspected by snort
CSCwo58260	Add "built" and "teardown" messages for the GRE | IPinIP connections to the Lina syslog
CSCwo60579	FTD does not synchronize via NTP from Secondary Management Center in HA when the Primary is down
CSCwo60609	DNS doctoring not working correctly if the doctoring rule is of type dynamic and has any interface
CSCwo61240	After renewal FMC CA, the certificate cannot be used for ArcSight integration
CSCwo61241	Logical App Stuck in 'Start Failed' Due to checkSystemCPUs Failure

ID	Headline
CSCwo61788	Failover and state link not accepting valid subnet mask
CSCwo62543	Default Pass action for rules in Snort 3 local rule groups may cause blank error in IPS policies
CSCwo63563	mix of major versions between FMC and FTD causes per-core CPU use health module to not work on FTD
CSCwo63951	FMC/FDM Client side certificate used to communicate to Talos did not auto-renew correctly
CSCwo64408	CPU core numbers not specified in results from operational/metrics FMC REST API endpoint
CSCwo64788	FPR9K-SM-56 Cluster - FTD Stuck in an application install loop & error 'pooled address is unknown'
CSCwo65060	FTD HA | Same MAC for port-channels causing network outage.
CSCwo65381	Deployment to FTD Fails at 5% due to corruption with interface object
CSCwo65866	Network Outage when Primary FTD Instance is Disabled from FCM
CSCwo66872	snmp_logging_thread is utilizing high CPU in control plane
CSCwo67167	FMC health policy and Default Health Policy do not have correct moduleList
CSCwo67540	FPR9K-SM-56 Cluster Node APP_SYNC timeout twice before joining "6" member inter-chassis cluster
CSCwo69015	Refresh Icon on Inventory Details Fails to Update Chassis Information for All Models
CSCwo70260	/objects/fqdn filter paramaters not working
CSCwo71052	FPR1010 Ethernet1/1 trunk port is not passing Vlan traffic after a reload
CSCwo71835	The NAS-IP-Address attribute is missing from the Access-Request in FMC
CSCwo73059	Captured file status is not updated if threat score is cached on FTDs
CSCwo73901	Bulk Edit Rules - Security Zone Search does not yield all zones if zone count is more than 1000
CSCwo74305	Deployment Failure in Hub and Spoke VTI Topology with DHCP Configured VPN Interfaces
CSCwo74496	BFD flap due to ASA not processing incoming BFD packets after unrelated BFD peers go down
CSCwo75483	SNMP polling to chassis is unsuccessful with FTD Multi-instance in HA used as SNMP agent
CSCwo75810	SNMP configuration is not applied consistently across same FTDs type and version

ID	Headline
CSCwo76165	Deployment failure due to rsync
CSCwo76436	3100 Marvell 4.3.14 CPSS patch for the interface mac stuck issue seen with peer switch reloads
CSCwo76554	TLS handshake fails with reverse SSL flow and TSID (TLS Server Identity) enabled
CSCwo76559	ASA/FTD traceback and reload with SNMP Notify Thread seen on 3110
CSCwo76644	FMC getting health alert - cgroup_monitor exited 5 time(s)
CSCwo77294	Passive Agent core containers like BEE does not come up beyond 3 crashes.
CSCwo77662	Certain special characters or spaces in RADIUS user passwords cause login failure in FMC
CSCwo77665	Portscan event in FMC displays incorrect source/destination when set to 'low' setting
CSCwo78069	Object search failing due to BB invalid data
CSCwo78775	Deploy failure seen when we use same vlan id in vlan intf and sub intf
CSCwo78969	Traceback in thread name DATAPATH when a unit is re-joining the cluster
CSCwo79004	deployment slowness seen when huge number of policies are present
CSCwo79028	Post-Failover FQDN Resolution Deferred Until Next DNS Poll Interval
CSCwo79114	Post reposition or move operation fails then if user saves, it would lead to loss of rules & may cause an outage
CSCwo79798	Cryptochecksum changed after reloading.
CSCwo80223	BFD packets are not dropped for single-hop BFD sessions received via alternate path
CSCwo80682	Saving changes under Policy > Alerts > Intrusion Emails in FMC GUI multiple times removes old changes
CSCwo82639	Local user details not replicated to data nodes in a cluster setup.
CSCwo82658	ASDM: Displays Error of Keypair already exists when adding an identity certificate.
CSCwo83389	Difference in RSA key length at multiple spots in FXOS
CSCwo84467	L3 Clustering where BGP immediately comes up while DATA node is still in bulk sync
CSCwo84910	Deployment failure not updated on databases of data node
CSCwo85252	FMC page may get stuck in loading state while trying to fetch BGP configuration
CSCwo86422	Unidirectional communication over ccl leading to split-cluster.

ID	Headline
CSCwo86556	FTD Hub-and-Spoke VPN Topology – Backup VTI Fails When DHCP is Used for External IP
CSCwo86835	SMB remote FMC backups are failing due to relam sync
CSCwo87051	FTD Dashboard queries only primary device for FTD HA
CSCwo87219	Boot-Time warning if CPU core count is below minimum requirement
CSCwo87763	ASA/FTD: Primary standby unit becomes Active after reload in HA set up
CSCwo87938	backout change preventing enabling clustering in FIPS mode
CSCwo88204	ASA/FTD traceback and reload triggered by the Smart Call Home process in sch_dispatch_to_url.
CSCwo88518	If command replication fails to any nodes in cluster, send kick the node out from cluster to fmc
CSCwo88745	Policy deploy would not write entries when referenced object is missing
CSCwo89233	Command replication failure to cluster nodes on command commit noconfirm revert-save after access-list, additional debugs
CSCwo89802	FMC Custom widget to display host count per sensor shows incorrect sensor name
CSCwo90300	"Error during policy validation An internal error is preventing the system... "due to stale sensor ref in security zones
CSCwo91049	Missing RADIUS accounting response messages may result in delays or failures of connectivity from chassis to instances
CSCwo91053	fover_trace.log not rotating and growing to a massive size
CSCwo91436	FPR 4125 Multi instance: High Snort and System Core CPU Usage (100%) Triggering FMC Critical Alerts
CSCwo91631	FMC Unable to Download User Groups from AD Realm via LDAP
CSCwo91965	ASAv restarts unexpectedly
CSCwo92226	ASA: asacli Processes Not Terminated When SSH Sessions Are Closed
CSCwo92386	cdFMC Not Displaying Interfaces and Security Zones When HA Secondary Device Is Active
CSCwo92447	FMC Displays SSE Enrollment Failure Alarm Despite No Active Integration with SecureX
CSCwo93174	Duplicate VTI cause VPN Flaps
CSCwo93444	FTD Cluster: Incorrect log when snort engine restart times out
CSCwo94260	FTD: SGT Inline tag stripped from SIP packets

ID	Headline
CSCwo94274	FP4100/9300 Fatal error: Incomplete chain observed before watchdogs with reset code 0x0040
CSCwo94483	LINA stays inactive without reloading after traceback on non-CP thread
CSCwo95586	Users with "Modify Threat Configuration" permission are not able to modify Intrusion/File Policies within the Access Control Policy (ACP) rules
CSCwo95654	Unified Event Viewer does not work with certain filters
CSCwo96377	Secondary Address should only be configurable for FMC-managed FTDs when using data interfaces for management
CSCwo96854	Unable to Edit or Break FTD-HA via FMC GUI because of UI lock issues during create
CSCwo96941	The total disk keep on increasing on the disk status wizard on the Health Monitor page.
CSCwo98670	FTD MI: SNMP polling fails to work after upgrade
CSCwo99544	Excessive number of AD users in FTD External Authentication could lead to deployment failure when disabled.
CSCwo99690	Error Encountered While Disabling the 'Call-Home Reporting Anonymous' Option in Call-Home Configuration
CSCwp00618	Devices show offline due to "Appliance unreachable" due to HMS deadlock inserting to DB
CSCwp00977	FTD Intermittent Syslog Alert: mcelog daemon is not running. Restarting the daemon.
CSCwp01015	ASA/FTD traceback and reload in function mp_percore
CSCwp02224	FPR failover split brain when upgrade primary/standby device's FXOS version
CSCwp02255	Snort2 crashes in loop after FMC upgrade
CSCwp03910	Subsequent DNS packets are dropped in a single flow if one domain hits the custom DNS SI block list
CSCwp04235	ASA traceback and reload
CSCwp06882	high CPU usage after ASA upgrade from 9.20.3.9 to 9.20.3.16 running on Hyper-V
CSCwp06890	SFF_SFP_10G_25G_CSR_S V03 modules from Finisar ports bouncing when connected.
CSCwp06995	FMC Restore of remote Unified backup fails due to no space left on the device
CSCwp07785	Error 500: Internal Server Error in FMC when generating report for global domain intrusion policy used in child domain ACP
CSCwp08772	ASA: tls-proxy maximum-session command error

ID	Headline
CSCwp10957	SSL error causing connection to Cisco Smart Software Manager (CSSM) to terminate
CSCwp11382	ASA/FTD: the ssl trust-point command deleted after a reload
CSCwp11503	User Creation Fails with RADIUS Dynamic Provisioning Enabled on Firepower device.
CSCwp11971	FMC GUI Inaccessibility and blank due to 'Malformed JSON String' Exception
CSCwp11985	Deployment is mandatory after FMC upgrade condition should be included in Upgrade code
CSCwp12712	FMC UI breaks when configuring Client-side interface settings for DHCP Relay
CSCwp13399	Collecting "show tech-support fprm" results into core for tar itself
CSCwp13412	No log file present for troubleshoot generation, if there is any issue with TS generation
CSCwp13540	Wrong URL incorrectly displayed for file upload with Japanese text in file path for client-less VPN
CSCwp14123	Tmatch memory is mostly consumed by ARP-DP.
CSCwp14919	The Firepower bandwidth_analyzer.pl script does not perform proper input validation for the '--size' option
CSCwp15886	Unable to change few IPS rule actions after upgrading from snort2 to snort3
CSCwp16323	FMC Audit tcp-tls syslog is truncated or incorrectly formatted
CSCwp16529	Negative value displayed for buffer drops when using " show cluster info load-monitor details"
CSCwp16546	Tunnel Status shows "No Active Data" when spoke behind NAT on S2S Monitoring UI
CSCwp16739	ASA crashinfo files not generated on FP4200 devices
CSCwp17700	Syslog format is not properly printed when EMBLEM format is enabled at least in one syslog host
CSCwp18136	ADI cores reading corrupt SXP file
CSCwp18885	FP9300/4100 may traceback & reload due to a "Kernel Panic"
CSCwp22214	Multiple mail drops and enq failures are seen while traffic is going through the box.
CSCwp22237	depoyment failure reason and transcript to be updated on FMC
CSCwp22612	Policy deploy failing on FTD when trying to remove Umbrella DNS Configuration
CSCwp22743	wpk - 1gsx link remains up on wpk but on switch side it shows as not connected
CSCwp23893	Error while downloading lsp from support site because VaultApp could not unseal Vault on FMC

ID	Headline
CSCwp24119	FDM stuck deployment task in Queued state
CSCwp25033	An ICMP not reachable storm might cause high CPU on a two units FTD cluster
CSCwp26314	Secure firewall posture image is not available in the ASA device backup when generated from ASDM
CSCwp26815	CPU usage by "WebVPN Timer Process" on standby ASA device
CSCwp26878	cdFMC returns 403 forbidden error while configuring webhook alerts
CSCwp27718	FMC deployment hungs and fail due to "NGFW_UPGRADE is missing in map"
CSCwp29273	Case differences in SAML SSO usernames cause login loop
CSCwp29808	FMC reporting IPv6 non overlapped host object-group as fully overlapped object-group
CSCwp32352	Deploy failure when Indexing is not working
CSCwp32469	Error : Msglyr::ZMQWrapper::registerSender() : Failed to bind ZeroMQ Socket
CSCwp32949	Deployment failure when selecting ECMP zone member interface in ZTNA policy
CSCwp33077	SAML IdP entityID increase from capped 128 character maximum
CSCwp33410	dmesg and kern.log file flooded with Tx Queue=0 logs
CSCwp34610	IKEv2-EAP Authentication Fails with Windows and MacOS Native VPN Clients
CSCwp36133	Clarify the working of Fallthrough to Interface PAT (Destination Interface) as it is not working as expected
CSCwp37128	The estreamer debug command is not producing the expected output
CSCwp37284	"CSRF Token Mismatch" error seen when users click logout from Clientless VPN page
CSCwp38220	Internal error is seen when editing the rule with IPV6 contents
CSCwp38436	The chassis serial number is empty post registration in FMC
CSCwp39148	If a user_ip_map.snapshot exists with an low timestamp value, snapshots are created frequently
CSCwp39266	Traffic drops post deployment when secondary skips app sync and become active immediately after bootstrap config apply
CSCwp39319	ASA Memory leak while processing large CRLs.
CSCwp59765	LDAP users in ACP always show realm out of sync.
CSCwp60027	Capture the reason of reboot in FTD logs

ID	Headline
CSCwp60523	FTD Active Authentication hostname value not included in cp_redirect_params.conf file
CSCwp60849	ASA Core file generated is corrupted
CSCwp60896	ASA Clock reverts to UTC after device reload
CSCwp64615	ASA/FTD: ASP drop capture for 'invalid-ip-length' or 'sp-security-failed' does not work with match criteria
CSCwp65900	Customer DU CONSULT, NPS 6 - ACP search toggle for exact IP or Port match
CSCwp66721	Memory leak in SSL crypto causing high Lina memory usage on lower-end devices running FTD 7.7.0
CSCwp67356	HA state should not transition from ColdStandby to Active
CSCwp80058	FMC Auto Deployment Task fails to run repeatedly
CSCwp80253	URL filtering download failure - talosAgent keeps exiting on FMC
CSCwp83345	Cluster: Multi-blade chassis not transmitting broadcast traffic outbound to specific vlan
CSCwp83566	SSL - Issues with DND a particular site after FTD upgrade on Chrome and Edge post upgrade
CSCwp84585	TCP RST Packets Fail to Match Configured Geolocation-Based Rules
CSCwp84839	Data Node Deregisters from With No Clear Error Message on vFMC in AWS When Deploying Stack Using Private IP's
CSCwp87708	FP1140 Critical FXOS fault alerts (F1000413) after upgrade
CSCwp89969	Prolonged delays in firewall restart/reboot completion
CSCwp90780	Restoring .tgz context file causes allocated interfaces to be removed from 'system' configuration
CSCwp91460	High disk usage due to snort-unified.log
CSCwp92390	FTD - SNMP Walk of FXOS FTD OID Tree Returns Empty or Times Out
CSCwp92489	SFDataCorrelator_user_id_mismatch.log overconsumption of disk
CSCwp92495	Adding interface taking more than 30 sec with loading security zones
CSCwp92644	FMC Dynamic Objects Limited to 1000
CSCwp93368	LINA traceback Observed on FTDv Firewalls Deployed in Azure: snp_vxlan_encap_and_send_to_remote_peer
CSCwp97009	Threat/AMP Upgrade tasks are being created soon after HF installation completed

ID	Headline
CSCwp97402	WA: Traceback and reload due to lock contention on the tmatch table during deployment with large snmp config
CSCwp97430	Missing Security Zones in zones.conf Affecting ngfw.rules Functionality
CSCwp97862	If failover IPSEC PSK is 78 characters or greater HA breaks with "Could not set failover ipsec pre-shared-key"
CSCwp97933	Inventory details on FMC GUI shows the incorrect compliance mode
CSCwp98971	Files missing from FTD troubleshoot file
CSCwp99130	FPR42xx - SNMP poll reports incorrect FanTray Status at Down while actually operational
CSCwq01305	FMC dashboard dynamic analysis over time is shown as "No Data"
CSCwq01683	Stop generating health alerts for transient high CPU utilization
CSCwq07197	Issue with interface status visibility in Firepower Chassis Manager 4225 managed by FMC
CSCwq07441	Memory Leak observed on FP2110 running ASA due to monitoring interface configured in HA
CSCwq07808	FP3105 Traceback and Reload after changing the speed on Ethernet interface
CSCwq09614	Snort may drop SCTP packets and block SCTP connections
CSCwq10546	Schema Validation Error Encountered While Editing AnyConnect/Secure Client Profiles
CSCwq11260	The syslog server called fluentbit can't recognize the fox syslog format and print it
CSCwq13032	3100/4200: 1G Management interface flapping after upgrade
CSCwq13510	CA Certificate Generation Issue Post restoring the Sanitised FMC Backup
CSCwq14900	Audit Logs Display Repeated Session Expiration Entries Even When the System is Idle
CSCwq15499	RAVPN Geolocation: Deployment failing by enabling all or specific countries in service access object
CSCwq16926	Traceback and Reload while two processes attempt to free a TD subnet structure
CSCwq17612	Misleading "failover reset" log printed on console when reload triggered by HA.
CSCwq20535	management-data-interface commands fail with "Enable of interface failed" error due to case-sensitive interface name
CSCwq21442	3RU MI instances offline after baseline/creation
CSCwq21804	FTD: Injected/Trimmed packets dropped by LINA due to invalid-ip-length

ID	Headline
CSCwq22154	FDM Intrusion Events Not Displayed When Browser Language Is Set to Japanese
CSCwq22206	VPN lost during a rekey with 'IKEv2 negotiation aborted due to ERROR: Platform errors'
CSCwq24140	Security module reboot triggered by a CIMC reset.
CSCwq26503	Policy Deployment tasks should not be stuck indefinitely
CSCwq27217	ASA: Traceback and reload on threat detection, interfaces unstable after that
CSCwq27767	Deployment fails deployment with "Deployment failed due to failure in retrieving running configuration information from device."
CSCwq28003	Duplicate messages during deployment to be discarded by CD to avoid further deployment failures
CSCwq28923	Flash Device error: Azure FMC
CSCwq29010	Snort3 blocking ESMTP traffic intermittently and trigger IPS signatures: 124:1:2
CSCwq29375	ASA/FTD - Assert triggered during FP_PUNT replace (aaa account match)
CSCwq29706	Traceback and reload after editing SNMP config, with tmatch
CSCwq30062	Local FTD backups are failing due to a lack of disk space on /tmp.
CSCwq30330	Long running AQ task got killed after timeout on FMC but corresponding backup task on FTD is still running
CSCwq30335	Backup Timeout is not sufficient when FTD backups are huge and low bandwidth
CSCwq30437	FTD backups sizes are huge like close to GB and above
CSCwq31137	Firepower 9300 - DNM-2X100G Interfaces not passing traffic post upgrade to FXOS 2.17.0.518
CSCwq32085	FP3100/4200 rebooting after generating crypto_archive with error on console "KC ILK issue detected"
CSCwq32776	Post FTD HA device deletion, RAVPN VPN references were still present causing deploy failures for existing ones
CSCwq35960	OSPF: Lina Traceback and Reload on Both Units in High Availability Setup.
CSCwq36564	Secondary FMC-HA Peer Exclusion list not taking effect for Network Discovery
CSCwq37434	Rule action 'Disabled' of rule 1:23858 in Secure Firewall Management Center does not align with snort.lua in Firepower
CSCwq40115	Need to remove compatibility popup added by CSCut04399 on ASDM
CSCwq43365	Dynamic Attributes Connector Status shows One or more services are unhealthy

ID	Headline
CSCwq43711	Idle SSH sessions persist beyond the configured timeout without graceful termination by Fin flag
CSCwq44862	Intrusion Event Packet Data via syslog/estreamer show no packet data for large packets
CSCwq45017	update the health alert to specify invalid proxy characters
CSCwq46058	ASA SNMP Response Issue - Responses Sent Only for Odd OIDs, Not for Even
CSCwq46544	debug menu tls-offload option <> to be provided to resolve slow download speed using curl to download large file with SSL Decrypt Resign Policy
CSCwq47622	Lina Traceback and Reload after enabling 'TLS Server Identity Discovery'
CSCwq47694	Unable to use the plus sign in the email-id for the identity when configuring an S2S VPN
CSCwq48085	Deployment failure soon after forming FTD HA
CSCwq48842	FTD: Packets Dropped due to tcp-seq-past-win due to delayed packet through Snort
CSCwq50189	ASAv deploy failed - console stuck at continuous
CSCwq50190	Multiple System Configurations Missing from FMC GUI Post-Upgrade
CSCwq50373	ASA/FTD in HA, snmptranslate process during the boot-up causing High CPU and IPC timeouts, causing split-brain.
CSCwq51981	FTD packer-tracer showing remark rule id in access-list for a rule not getting hit
CSCwq52188	FTD Traceback while executing 'asp load-balance per-packet'
CSCwq52255	SSH login to FTD management IP address lands in FXOS shell instead of FTD CLISH due to missing /mnt/boot/application/*.def file
CSCwq53328	Multicast and unicast packets do not reach the correct instance for random subinterfaces
CSCwq54109	FTD 3130 HA Lina tracebacks at ikev2_bin2hex_str
CSCwq55841	FMC Upgrade stalls Indefinitely at 999_update_onpremfmc_diskcache.sh
CSCwq55887	FMC 7.6 NAT Source and IP Not Populating within Unified Event Viewer
CSCwq56279	7.6 - Firepower 3100 series - Upgrading an HA pair from a version without the fix for CSCwo00444 to 7.6 causes one firewall to go into a traceback/reload loop
CSCwq57394	Unable to edit Dynamic Analysis Connection cloud settings when FMC cannot connect to the US cloud
CSCwq59563	FMC uses old DNS server for resolution despite correct configuration
CSCwq60125	FTD is not sending a reset packet when the incoming traffic hits "block with reset" rule

ID	Headline
CSCwq60586	FTD upgrade failed due to bundle image existence verification failure
CSCwq61673	FMC does not allow to use IP address with 0 value in last octet as gateway while configuring static route for a device. Error: Enter valid IPv4 host value
CSCwq65499	FTD does not generate any events for the Platform Faults health module if no platform faults are present
CSCwq65955	FPR 4200: HA link arp packets getting dropped, internal uplink linkChange counters incrementing
CSCwq69599	FMC ACP Top User Deleted When Deleting Users With Legacy UI
CSCwq70133	Password Expiry Age does not reset after Password Change
CSCwq70362	ASDM: Using the Secure Client VPN Wizard results in an incomplete configuration
CSCwq70773	show asp rule-engine issues with complete and run time
CSCwq71338	non-SSL traffic wrongly classified as SSLv2 causing drops with TSID enabled
CSCwq72156	SNMP traps are not sent to one of multiple SNMP servers, in certain conditions
CSCwq73733	FMC - Deployment Fails with "Deployment failed due to timeout during configuration generation"
CSCwq73994	ASA : Performance and high CPU usage seen on Hyper-V
CSCwq74204	IKEv1 L2Lvpn fails in phase 2 with "Rejecting IPsec tunnel: no matching crypto map entry" after upgrade
CSCwq74936	ASDM fails to connect via ipv6 due to https hostname wrong error
CSCwq74986	FTD: Instance stuck in Boot Loop
CSCwq75116	IPv6 function is stalled, link-local address marked [DUPLICATE] and IPv6 traffic stopped after failover due to split-brain
CSCwq75449	502 Proxy Error when regenerating certificate in ISE Quick Configuration tab
CSCwq76130	Clustering : SNMP traffic drop due to cluster redirect offload
CSCwq77569	SRU Upgrade Fails Due to Leaked Activity IDs from ClusterPostUpgradeHandler
CSCwq77806	Remote Access Monitoring doesn't show client IP correctly.
CSCwq77850	Send Email when complete emails not working with advanced deployment
CSCwq78813	Intermittent Blank Screen When Loading Access Control Policy in New UI
CSCwq79940	tunnel protection ipsec policy feature not working on backup VTI tunnel
CSCwq80142	Possible unregistration when deploying during HA Switchover

ID	Headline
CSCwq81480	FTD MI: SNMP polling fails to work after the upgrade
CSCwq83395	Not probing for http Opportunistic TLS
CSCwq85028	Packet Captures show misleading information when blocked due to TCP server unavailable.
CSCwq85986	FP4225: Interface with SFP - 10/25G_LR_S (or CSR_S) is not coming up after reboot of peer side.
CSCwq86675	Number of sessions in cache for Tomcat are set incorrectly
CSCwq89972	FMC UI displays upgrade failure despite successful firewall upgrade
CSCwq90072	ASDM Parsing Failure on Two Contexts
CSCwq92373	WA MI: Two apps went to Not Responding state with reason: Error in App Instance ftd. sma reported fault: Instance xxx is disabled due to restart loop. Please consider reinstalling this app-instance.
CSCwq92728	ASA client IP missing from TACACS+ authorization request in SSH
CSCwq94584	Http inspector support for OPPORTUNISTIC_TLS
CSCwq95241	Reboots on FP2130 due to missing heimdall PID
CSCwq95649	Unable to upload Secure Firewall Posture image file with a size over 200MB
CSCwq95810	"no http server basic-auth-client ASDM" allows ASDM connections to ASA.
CSCwq95837	Remove Object Overlaps can remove unrelated objects
CSCwq96195	DNS-GUARD is not capable to be de-activated on FTD Devices
CSCwq96289	MonetDB may fail to start on FMC if maximum parallel/concurrent logins per CLI user is set to 1
CSCwq96870	Interfaces are coming up when the Firepower is shutting down
CSCwq97615	FlexConfig migration may cause sudden logout from FMC GUI session
CSCwq98101	Policy deployment fails when inline-set is configured on FTD HA
CSCwq98155	'Access token invalid' is prompted, if a stress test is made on the ACP
CSCwq98648	Low RAM allocation on ASAv can trigger unexpected behavior in 'asdm image' command
CSCwr00264	Flexconfig policy deletion left the stale references
CSCwr00282	cdFMC: All Device Deploy Validations were failing post deletion of Flexconfig for one device
CSCwr00711	Cannot delete interface objects with names over 30 characters.

ID	Headline
CSCwr01482	FPR4215 "Not supported" alarm occurred, when insert the SFPs
CSCwr01763	FDM: UI gets stuck on upgrade progress at 9% when upgrade fails attempting to install an already installed hotfix
CSCwr05406	Traceback in HA stby node while snmpwalk on natAddrMapTable
CSCwr06027	FMC does not accept underscore characters for remote storage hostname settings
CSCwr06290	ASA/FTD: Traceback in thread name CP Processing due to DCERPC inspection
CSCwr06887	Database synchronization should auto-resume post network/checksum issues
CSCwr08102	EventHandler wastes CPU re-scanning files that contain no requested events
CSCwr10732	Connection blocking active although "logging permit-hostdown' is set
CSCwr10756	Summary Dashboard widgets do not wrap or truncate text properly
CSCwr11046	Timeout values not honored after "sftunnel_change_max_conn_check.pl" changes
CSCwr11825	Sftunnel TLS13 connection goes down after upgrade when two interfaces configured with same IP on FMC GUI
CSCwr11851	Standby FMC Fails to Sync ids_event_class_map Table, Resulting in Misclassified Intrusion Events
CSCwr12965	Both the units in HA changed the encryption algorithm simultaneously
CSCwr13617	FMC API is reporting Windows for all AnyConnect images while querying RA VPN policies
CSCwr14186	add context for cmd-invalid-encap asp-drop type in the "show asp drop" command usage
CSCwr15697	Block 80 depletion ssl_decrypt_cb
CSCwr18291	4200 interface image in FMC does not match interface order in device
CSCwr19123	FPR HA ESP sequence number discrepancy when standby changes to Active resulting in Anti-replay drops
CSCwr21323	Use of FMC GUI features via user role escalation may cause user to lose all permissions during GUI session
CSCwr21375	FTD port status not reflecting properly on FMC.
CSCwr21583	Intermittent deployment stuck "in progress" for few devices
CSCwr21683	Deployment changed performance profile, unable to retrieve running configuration
CSCwr22256	Traceback seen while FQDN list expands more than 200 entries for a resolved ip
CSCwr22508	Device doesn't boot and gets stuck after a successful upgrade

ID	Headline
CSCwr24365	SRU-triggered policy deployments occurred following initial/standby FMC during FMC HA & standalone upgrades
CSCwr26642	Slow UI and inability to check disk usage on FMC due to NFS configuration
CSCwr26857	File policy stops working due to SMB tcp conn terminated after 1hr for unknown reason despite not idle
CSCwr27095	Anyconnect users incorrectly get the prompts, based on the previous tunnel-group
CSCwr28908	ASA: Traceback and reload after saving asdm image
CSCwr29314	Show crypto accelerator shows max crypto throughput is 6 Gbps For 3K & 225Mbps for FTDv
CSCwr29547	Empty Dynamic Attribute IP mappings pushed to FTD from FMC Secondary Unit
CSCwr30510	Deleting a domain using domain_manager --deleteDomain <domain_uuid> on FMC CLI brings down the estreamer service
CSCwr31782	Secure Client SAML - External Browser May Prompt for a Certificate when using IKEv2-IPsec and Certificate Mapping
CSCwr32852	FTD may generate a large number of "ssl-certs-unified" files.
CSCwr32923	ndclient stops monitoring snort during deployment causing outage
CSCwr33630	TLS audit syslog configuration and certificates not replicating to secondary FMC in HA deployment
CSCwr35582	Continuous logs_archive.asa-interface-idb.log getting generated on ASA
CSCwr37820	FMC GUI slow time to load web pages post upgrade to 7.6.x
CSCwr37941	FMC may not complete Cisco Security Cloud integration when using on-prem Smart Software Manager for smart licensing
CSCwr42114	FTD HA Upgrade Failed on Secondary Unit Due to HA Being in a Failed State From FMC's Perspective
CSCwr42577	ASA/FTD may traceback and reload citing Thread Name 'lina' as the faulting thread.
CSCwr42969	Dynamic Offloaded Flows Interrupted midstream
CSCwr43237	FMC is returning status code 400s of GET request for Get Device Data
CSCwr43347	Disabled certificate is easily accessible and the sanitisation alone is not fool-proof
CSCwr43392	cdFMC 7.7 Fails to Display Health Data for specific FTD's
CSCwr43586	Intermittent drop of self-originated ICMP TTL exceeded messages with reason "Unable to obtain connection lock (connection-lock)"

ID	Headline
CSCwr43734	FMC/FTD: Policy Deployment failure after disabling NVE Interface config in VTEP Tab of FTD Cluster
CSCwr45484	FTD Policy deployment reported as failed incorrectly on FMC when communications disrupted
CSCwr48605	Lina traceback due to the incorrect option being received in the packet.
CSCwr49028	Secure client tunnel group authentication is affected when using SDI protocol
CSCwr49171	Interlaken (ILK) link between the Nitrox and KC2 failure, causing traffic backpressure / traffic outage
CSCwr50320	Device upgrade using direct downloads from support site doesn't work correctly when FMC is behind a proxy
CSCwr50466	ASA/FTD: Wrong value shown for X509_STORE_CTX in 'show ssl objects'
CSCwr50630	S2S VPN status shows Unknown for Extranet direction while managed direction shows Active (bidirectional tunnel status not synchronized)
CSCwr51629	RTSP Flows are dropped with drop reason "First TCP packet not SYN"
CSCwr54958	GUI: File upload shows generic 'Invalid file size' instead of actionable message with actual and maximum allowed sizes
CSCwr55089	ASA/FTD - Traceback and Reload in Threadname DATAPATH
CSCwr57552	Rate limit conn-limit SNMP traps
CSCwr57647	Upgrade failure on FMC on GCP 000_start/112_CF_check.sh
CSCwr59870	ASAv on Hyper-v encountering boot loop issues when running netvsc driver
CSCwr61224	Detection engine Folder is huge in size for FTD backups
CSCwr61452	ASA traceback and reload due to memory corruption in IPsec SA pointers
CSCwr61629	GeoDB content is not restored when restoring a backup to a freshly deployed FMC
CSCwr62800	High network latency observed on ASAv
CSCwr63632	Unable to upload VPN client profile package under Objects > Object Management > VPN > Secure client File to FMC while logged in via External User.
CSCwr71262	Device goes into bootloop due to missing librte_mbuf.so.22 and librte_ring.so.22
CSCwr72556	Enhance UI error messages to inform users that deployment is not allowed due to version mismatch.
CSCwr74768	Add validation on FMC UI to prevent admin to configure more than allowed IKE policies - Regression CSCwf10137
CSCwr79344	ASA/FTD traceback and reload in Lina

ID	Headline
CSCwr79651	Few Chassis devices are not visible to assign the policies
CSCwr83703	Deployment failure due to unrecognized command "vpn-simultaneous-logins none"
CSCwr84343	ASA/FTD Traceback and reload in L2 table creation failure
CSCwr85470	FTD silently drops out of order packets
CSCwr87450	removing all usages of a DHCP IPv6 pool object from FTD interface config does not delete the object from FTD
CSCws05886	ASA may traceback during manual failover

Open issues

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

Table last updated: 2025-12-03

Table 25: Open issues in Version 10.0.0

ID	Headline
CSCwq55647	10.0: 1240/1250 VPN IKEv2 TCP 450B w/ AVC degraded ~4-5%
CSCwr48919	FTD Performance down -8% on 1200 (Snort side) and 1010/ISA3k
CSCwr95556	Move SQLite databases under /var/sf/sqlite folder to the high endurance partition of FTDs
CSCws01449	FMC UI not accessible for few min due to MySQLUtil [ERROR] UpdateTable: MySQL error 2002
CSCws11646	Secure Firewall 200 not available after backup/restore when using an access control rule with URL categories
CSCws21023	Policy not marked out of date after a vdb upgrade as part of FMC upgrade

Compatibility

Before you upgrade or reimage, make sure the target version is compatible with your deployment. If you cannot upgrade or reimage due to incompatibility, contact your Cisco representative or partner for refresh information.

For compatibility information, see:

- Cisco Secure Firewall Management Center Compatibility Guide
- Cisco Secure Firewall Threat Defense Compatibility Guide
- Cisco Firepower 4100/9300 FXOS Compatibility

Upgrade and downgrade

Choosing your upgrade target

Go **directly to the latest Version 10 release possible** to minimize upgrade and other impact.

Features, enhancements, and critical fixes can skip "future" releases that are ahead by version, but not by release date. For example, if you are up-to-date within major Version A, upgrading to dot-zero Version B can deprecate features and fixes.

If you cannot go to the latest release, at least make sure your current version was released on a date before your target version. In the following table, confirm your current version is listed next to your target version. If it is not, choose a later target.

Table 26: Released before Version 10.x, by date

Target version		Current version: confirm yours is listed.				
		from 7.3	from 7.4	from 7.6	from 7.7	from 10.0
to 10.0.0	2025-12-03	7.3.0–7.3.1	7.4.0–7.4.3	7.6.0–7.6.3	7.7.11	—

Upgrading from a patched deployment

Critical fixes in patches/vulnerability (fourth-digit) releases can also skip future releases. If you depend on these critical fixes, verify that your target version contains them. For a full list of release dates, see Cisco Secure Firewall Management Center New Features by Release.

Supported upgrades and downgrades

This section summarizes upgrade and downgrade capability. For help with:

- Choosing an upgrade target, see Choosing your upgrade target, on page 52.
- Upgrade and downgrade procedures, including general guidelines, best practices, and troubleshooting, see the upgrade guide for the version you are currently running: https://www.cisco.com/go/ftd-upgrade.
- Any upgrade or downgrade issues for this specific release, see Open issues, on page 51, Known issues with Firewall Management Center upgrade, on page 54, and Known issues with Firewall Threat Defense upgrade, on page 56.

Supported upgrades

This table shows the supported direct upgrades for Firewall Management Center and Firewall Threat Defense software.

Note You can upgrade directly to any major (first and second-digit) or maintenance (third digit) release. Patches change the fourth digit only. You cannot upgrade directly to a patch from a previous major or maintenance release. Although a patched device (fourth-digit) can be managed with an unpatched Firewall Management Center, fully patched deployments undergo enhanced testing.

Table 27: Supported direct upgrades

Current version	Target software version							
	to 10.0	7.7	7.6	7.4 *	7.3	7.2	7.1	7.0
from 10.0	YES	—	—	—	—	—	—	—
from 7.7	YES	YES	—	—	—	—	—	—
from 7.6	YES	YES	YES	—	—	—	—	—
from 7.4	YES	YES	YES	YES	—	—	—	—
from 7.3	YES	YES	YES	YES	YES	—	—	—
from 7.2	—	YES	YES	YES	YES	YES	—	—
from 7.1	—	—	YES	YES	YES	YES	YES	—
from 7.0	—	—	—	YES	YES	YES	YES	YES
from 6.4	—	—	—	—	—	—	—	YES

* You cannot upgrade Firewall Threat Defense to Version 7.4.0, which is available as a fresh install on the Secure Firewall 4200 only, and is not supported with Firewall Device Manager. It removes significant features, enhancements, and critical fixes included in earlier versions. Upgrade to a later release.

For the Firepower 4100/9300, this table lists companion FXOS versions. If a chassis upgrade is required, Firewall Threat Defense upgrade is blocked. In most cases we recommend the latest build in each version; for minimum builds see the Cisco Secure Firewall Threat Defense Compatibility Guide.

Table 28: Supported FXOS versions for Firepower 4100/9300 upgrades

Target Firewall Threat Defense version	Minimum FXOS version
10.x	2.18.0
7.7	2.17.0
7.6	2.16.0
7.4.1–7.4.x	2.14.1
7.4.0	—
7.3	2.13.0
7.2	2.12.0
7.1	2.11.1
7.0	2.10.1
6.7	2.9.1

Target Firewall Threat Defense version	Minimum FXOS version
6.6	2.8.1
6.4	2.6.1

Supported downgrades

If an upgrade or patch succeeds but the system does not function to your expectations, you may be able to revert (Firewall Threat Defense upgrades) or uninstall (Firewall Threat Defense and Firewall Management Center patches). For general information, particularly on common scenarios where returning to a previous version is not supported or recommended, see the upgrade guide: https://cisco.com/go/ftd-upgrade.

Known issues with Firewall Management Center upgrade

This section lists upgrade limitations and feature impact for this release. For general guidelines and best practices, see the Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center.

Known issues with Firewall Management Center upgrade

This table lists upgrade limitations for this release.

Table 29: Known issues with Firewall Management Center Version 10 upgrade

Current version	Issue	Details
Any	—	There are no known issues for this version right now, but you should still check for open issues and features with upgrade impact.

Features with upgrade impact for Firewall Management Center

A feature has upgrade impact if upgrading and deploying can cause the system to process traffic or otherwise act differently without any other action on your part. This is especially common with new threat detection and application identification capabilities. A feature can also have upgrade impact if upgrading requires that you take action before or after upgrade to avoid an undesirable outcome; for example, if you must change a configuration.

This table lists and links to descriptions of features that may have upgrade impact. The first column is for your current version and the link indicates when the feature was originally introduced.

Important Minimize upgrade and other impact by going directly to the latest maintenance release in your chosen version. See Choosing your upgrade target, on page 52.

Table 30: Features with upgrade impact for Firewall Management Center Version 10

Current version	Features with upgrade impact
7.7.x and earlier	• EVE improvements *(*10.0.0) • Updated internet access requirements for security intelligence feeds *(*10.0.0) • End of support: VMware vSphere/VMware ESXi 6.5, 6.7, 7.0, and 7.5 *(*10.0.0)
7.6.x and earlier	• SRU update moved out of Firewall Management Center upgrade. *(*7.7.0)
7.6.0 7.4.0–7.4.2 7.2.9 and earlier	• New Cisco AMP cloud connection method. *(*7.7.0)
7.4.x and earlier	• Allow Cisco Talos to conduct advanced threat hunting and intelligence gathering using your traffic. *(*7.6.0) • Security Cloud Control replaces SecureX. *(*7.6.0) • Updated internet access requirements for URL filtering. *(*7.6.0) • Updated internet access requirements for intrusion rule updates. *(*7.6.0) • Security Services Exchange (SSE) integration required for some threat intelligence downloads. *(*7.6.0) • Cisco Success Network and Cisco Support Diagnostics are enabled by default. *(*7.6.0)
7.4.0 and earlier	• Improved Firewall Management Center memory usage calculation, alerting, and swap memory monitoring. *(*7.4.1)
7.4.0 7.3.x 7.2.5 and earlier	• Configure DHCP relay trusted interfaces from the Firewall Management Center web interface. *(*7.2.6) • Updated internet access requirements for direct-downloading software upgrades. *(*7.2.6) • Deprecated: scheduled download of maintenance releases. *(*7.2.6)
7.4.0 7.3.x 7.2.0–7.2.5 7.1.x 7.0.5 and earlier	• Updated web analytics provider. *(*7.0.6)
7.3.x and earlier	• Configure Firewall Threat Defense devices as NetFlow exporters from the Firewall Management Center web interface. *(*7.4.0)

Current version	Features with upgrade impact
7.3.0–7.3.1 7.2.0–7.2.3 7.1.x 7.0.5 and earlier	• Smaller VDB for lower memory Snort 2 devices. (7.0.6)

Known issues with Firewall Threat Defense upgrade

This section lists upgrade limitations and feature impact for this release. For general guidelines and best practices, see the Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center.

Known issues with Firewall Threat Defense upgrade

This table lists upgrade limitations for this release.

Table 31: Known issues with Firewall Threat Defense Version 10 upgrade

Current version	Issue	Details
7.7 or earlier	Revert prohibited: Firewall Threat Defense Virtual Version 10+ to earlier versions.	Security enhancements to the startup framework (bootloader firmware) mean that you cannot revert virtual firewalls from Version 10+ to earlier versions. After upgrade, we also recommend you migrate configurations to freshly deployed Version 10+ instances and decommission the old ones.

Features with upgrade impact for Firewall Threat Defense

A feature has upgrade impact if upgrading and deploying can cause the system to process traffic or otherwise act differently without any other action on your part. This is especially common with new threat detection and application identification capabilities. A feature can also have upgrade impact if upgrading requires that you take action before or after upgrade to avoid an undesirable outcome; for example, if you must change a configuration.

This table lists and links to descriptions of features that may have upgrade impact. The first column is for your current version and the link indicates when the feature was originally introduced.

Important Minimize upgrade and other impact by going directly to the latest maintenance release in your chosen version. See Choosing your upgrade target, on page 52.

Table 32: Features with upgrade impact for Firewall Threat Defense Version 10

Current version	Features with upgrade impact
7.6.0 and earlier	• Deprecated: Snort 2. (7.7.0)

Current version	Features with upgrade impact
7.6.0 7.4.0–7.4.2 7.3.x 7.2.9 and earlier	• Require the Message-Authenticator attribute in all RADIUS responses. (7.0.7)
7.4.0–7.4.1 7.3.x 7.2.9 and earlier	• Asymmetric traffic handling. (7.2.9)
7.4.0 and earlier	• IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100. (7.4.1) • Captive portal support for multiple Active Directory realms (realm sequences). (7.4.1) • Firmware upgrades included in FXOS upgrades. (7.4.1)
7.3.x	• Merged management and diagnostic interfaces. (7.4.0) • Sensitive data detection and masking. (7.4.0) • Policy-based routing with user identity and SGTs. (7.4.0)

Related resources

Which issues are listed?

These release notes list issues for this specific software release. If the lists are not as you expected, try one of the following solutions.

Table 33: Common problems with issue lists

Problem	Solution
There are no open issues listed for a release.	We do not list open issues for maintenance or vulnerability releases.
I can't find the issue I'm looking for.	These release notes lists issues for this specific software release. This software release may contain fixes first introduced and open bugs first identified in other releases. Also, lists are auto-generated. Depending on how and when an issue was categorized or updated in our system, it may not appear in the release notes. If you have a support contract, you can obtain up-to-date lists with the Cisco Bug Search Tool.
There are issues that don't apply to me.	Due to how they are categorized in our system, you may see some issues for Firewall Device Manager deployments. You can safely ignore them.

Upgrade guides

Upgrade the management center first, then devices. Use the upgrade guide for the version you are *currently* running—not your target version.

Table 34: Upgrade Guides

Platform	Upgrade Guide	Link
Management center	Management center version you are *currently* running.	https://cisco.com/go/fmc-upgrade
Threat defense with management center	Management center version you are *currently* running.	https://cisco.com/go/ftd-fmc-upgrade
Threat defense with Cloud-Delivered Firewall Management Center	Cloud-Delivered Firewall Management Center.	https://cisco.com/go/ftd-cdfmc-upgrade

Install guides

If you cannot or do not want to upgrade, you can freshly install major and maintenance releases. This is also called *reimaging*. You cannot reimage to a patch. Install the appropriate major or maintenance release, then apply the patch. If you are reimaging to an earlier threat defense version on an FXOS device, perform a full reimage—even for devices where the operating system and software are bundled.

Table 35: Install Guides

Platform	Install Guide	Link
Management center hardware	Getting started guide for your management center hardware model.	https://cisco.com/go/fmc-install
Management center virtual	Getting started guide for the management center virtual.	https://cisco.com/go/fmcv-quick
Threat defense hardware	Getting started or reimage guide for your device model.	https://cisco.com/go/ftd-quick
Threat defense virtual	Getting started guide for your threat defense virtual version.	https://cisco.com/go/ftdv-quick
FXOS for the Firepower 4100/9300	Configuration guide for your FXOS version, in the *Image Management* chapter.	https://cisco.com/go/firepower9300-config
FXOS for the Firepower 1000 and Secure Firewall 3100/4200	Troubleshooting guide, in the *Reimage Procedures* chapter.	Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense

Integration and logging guides

Various integrations and logging facilities may have new features associated with firewall releases. For details, see the following guides.

Table 36: Related integrations and logging

Feature	Guide
Syslog	Cisco Secure Firewall Threat Defense Syslog Messages
Cisco Success Network	Cisco Success Network Telemetry Data Collected from Cisco Secure Firewall Management Center
REST API	Secure Firewall Management Center REST API Quick Start Guide

FXOS release notes

The Firepower 4100/9300 may require a chassis upgrade before you upgrade threat defense. For information on the companion FXOS release, see the Cisco Firepower 4100/9300 FXOS Release Notes.

More Online Resources

Cisco provides the following online resources to download documentation, software, and tools; to query bugs; and to open service requests. Use these resources to install and configure Cisco software and to troubleshoot and resolve technical issues.

- Documentation: https://cisco.com/go/threatdefense-10-0-docs
- Cisco Support & Download site: https://cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://bst.cloudapps.cisco.com/bugsearch
- Cisco Notification Service: https://cisco.com/cisco/support/notifications.html

Access to most tools on the Cisco Support & Download site requires a Cisco.com user ID and password.

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco 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