Cisco Secure Firewall Threat Defense Release Notes, Version 7.7.x

First Published: 2025-03-05

Last Modified: 2025-08-28

Cisco Secure Firewall Threat Defense Release Notes

This document contains release information for:

- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center (on-prem)
- Cisco Secure Firewall Device Manager

For cloud deployments, see the Cisco Cloud-delivered Firewall Management Center Release Notes or What's New for Security Cloud Control Firewall Management.

Release Dates

Table 1: Version 7.7 Dates

Version	Build	Date	Platforms
7.7.10	3200	2025-08-18	All devices
	3089	2025-08-11	Firewall Management Center
7.7.0	91	2025-03-14	Firewall Management Center
	89	2025-03-05	All devices

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 contact 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

Features

For features in earlier releases, see Cisco Secure Firewall Management Center New Features by Release and Cisco Secure Firewall Device Manager New Features by Release.

Upgrade Impact

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.

The feature descriptions here include upgrade impact where appropriate. For a more complete list of features with upgrade impact by version, see Upgrade Impact Features, on page 18.

Features in Maintenance Releases

Features, enhancements, and critical fixes included in maintenance releases (third-digit) and patches (fourth-digit) can skip future releases, depending on release date, release type (short term vs. long term), and other factors. Minimize upgrade and other impact by going directly to the latest maintenance release in your chosen version. See Choosing your upgrade target, on page 22.

If you are using the web interface in a language other than English, features introduced in maintenance releases and patches may not be translated until the next major release.

Intrusion Rules and Keywords

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. 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

Upgrades can add web interface or Smart CLI support for features that previously required FlexConfig. Although you cannot newly assign or create FlexConfig objects using deprecated commands, in most cases existing FlexConfigs continue to work and you can still deploy. However, sometimes, using deprecated commands can cause deployment issues. The upgrade does not convert FlexConfigs. After upgrade, configure the newly supported features in the web interface or Smart CLI. When you are satisfied with the new configuration, delete the deprecated FlexConfigs.

The feature descriptions here include information on deprecated FlexConfigs when appropriate. For a full list of deprecated FlexConfigs, see your configuration guide.

Integrations and Logging

These integrations and logging facilities may have new features associated with threat defense and management center releases:

- 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 and Cisco Secure Firewall Threat Defense REST API Guide

Firewall Management Center Features in Version 7.7.10

Table 2: Firewall Management Center Features in Version 7.7.10

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.7.10 also has: • Migrate select Firepower 4100/9300 models to Secure Firewall 3100/4200. (7.6.1) • Umbrella integration with Firewall Management Center over a proxy. (7.6.1)
Zero Trust Access			
Universal Zero Trust Network Access (universal ZTNA).	7.7.10	7.7.10	Universal Zero Trust Network Access (universal ZTNA) is a comprehensive solution that provides secure access to internal network resources based on user identity, trust, and posture. It ensures that access to one application does not implicitly grant access to the entire network, as with remote access VPN. New/modified screens: **Policies** > **Zero Trust Application** Requires Cisco Secure Access and Security Cloud Control. Deployment restrictions: Not supported with clustered devices, container instances, or transparent mode. Supported platforms: Secure Firewall 1150, 3100, 4100, 4200, and Firewall Threat Defense Virtual. See: Zero Trust Access

Firewall Management Center Features in Version 7.7.0

Table 3: Firewall Management Center Features in Version 7.7.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.7.0 also has: • New Cisco AMP cloud connection method. Upgrade impact. (7.0.7) • Deprecated Cisco AMP Cloud connection backups. (7.0.7) • Require the Message-Authenticator attribute in all RADIUS responses. Upgrade impact. (7.0.7) • High-bandwidth encrypted application traffic bypasses unnecessary intrusion inspection. (7.2.10) • Independently configure health monitoring for physical and subinterfaces. (7.6.1) • View health status for devices in leaf domains while logged into the parent domain. (7.6.1) • Add device by registration key using basic initial configuration added to the Device (Wizard) (7.6.1) • BGP AS-Override. (7.6.1) • Devices with internet access download upgrade packages from the internet. (7.6.1)
Platform			
Secure Firewall 1230, 1240, and 1250 (rack-mount).	7.7.0	7.7.0	We introduced the Secure Firewall CSF-1230 and CSF-1240: • 8x1Gbps RJ-45 1000BASET/2.5BBASE-T copper • 4x1Gbps SFP+ optical And the Secure Firewall CSF-1250: • 8x2.5Gbps1000BASET/2.5BBASE-T copper • 4x2.5Gbps SFP28 optical See: Cisco Secure Firewall CSF-1230,CSF-1240, and CSF-1250 Hardware Installation Guide
Optical transceivers for the Secure Firewall 4200.	7.7.0	7.7.0	The Secure Firewall 4200 now supports these optical transceivers on the FPR4K-X-NM-2X200/400G network module: QDD-400G-DR4-S, QDD-4x100G-FR-S, QDD-4x100G-LR-S, QDD-400G-SR4.2-BD, QDD-400G-FR4-S, QDD-400G-LR4-S, QDD-400-CUxM, QDD-400-AOCxM, QDD-2X100-LR4-S, QDD-2X100-SR4-S, QDD-4ZQ100-CUxM. See: Cisco Secure Firewall 4215, 4225, and 4245 Hardware Installation Guide

Feature	Minimum Management Center	Minimum Threat Defense	Details
Secure Firewall 1210CP IEEE 802.3bt support (PoE++ and Hi-PoE).	7.7.0	7.7.0	We made the following improvements related to support for IEEE 802.3bt: • PoE++ and Hi-PoE—Up to 90W per port. • Single- and dual-signature powered devices (PDs). • Power budgeting is done on a first-come, first-served basis. • Power budget fields were added to **show power inline**. New/modified screens: **Devices** > **Device Management** > **Interfaces** > **PoE** New/modified commands: **show power inline** See: Regular Firewall Interfaces, Cisco Secure Firewall Threat Defense Command Reference
Instances for AWS, Azure, and GCP.	7.7.0	7.7.0	We added instances for Firewall Management Center Virtual and Firewall Threat Defense Virtual from the following families: • AWS (Amazon Web Services): C6i and C6a • Azure (Microsoft Azure): Dv4 and Dv5 • GCP (Google Cloud Platform): E2, N1, N2D, C2D See: Cisco Secure Firewall Management Center Virtual Getting Started Guide, Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
Unattended provisioning for Firewall Threat Defense Virtual for VMware using ISO-based cloud-init seeding.	7.7.0	7.7.0	You can now quickly deploy Firewall Threat Defense Virtual for VMware using a text file (day0.iso) that contains initial setup details such as hostname, password, management mode, firewall mode, network settings, and deployment type. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
Platform Migration			
Migrate from Firepower Management Center 4600 to Secure Firewall Management Center Virtual 300 for VMware.	7.7.0	Any	You can migrate from Firepower Management Center 4600 to Secure Firewall Management Center Virtual for VMware with a 300-device license. See: Cisco Secure Firewall Management Center Model Migration Guide
Device Management			

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

Feature	Minimum Management Center	Minimum Threat Defense	Details
Management center high availability enhancements.	7.7.0	Any	It is now easier to: • Determine when the peers last synced. • Compare intrusion rule (SRU/LSP) and vulnerability database (VDB) versions on the peers. • Resolve a common device registration issue. When device registration fails on the standby peer when you establish high availability, it is often due to stale manager data on the device. Previously, you used the device CLI to resolve this issue. You can now use the Firewall Management Center web interface—click **Disable Manager**, then **Add Manager**. New/modified screens: **Integrations** > **Other Integrations** > **High Availability** See: High Availability
Threat defense high availability supported with redundant manager access data interfaces.	7.7.0	7.7.0	You can now use redundant manager access data interfaces with Firewall Threat Defense high availability. See: High Availability
Autoscale for Firewall Threat Defense Virtual for Azure clusters.	7.7.0	7.7.0	We now support autoscale for new Firewall Threat Defense Virtual for Azure clusters. You cannot convert upgraded deployments. Platform restrictions: Not supported with FTDv5 or FTDv10. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
VPN: Remote Access			
Geolocation-based RA VPN.	7.7.0	7.7.0	You can now allow or block remote access VPN connections based on country or region. Connections that don't meet your location-based criteria are blocked before authentication and logged for auditing purposes. New/modified screens: **Objects** > **Object Management** > **Access List** > **Service Access** See: Remote Access VPN

Feature	Minimum Management Center	Minimum Threat Defense	Details
Easily configure posture assessment criteria for dynamic access policies.	7.7.0	Any	In dynamic access policies (DAP), you can now easily configure *posture assessment criteria*—that is, file, process, or registry endpoint attributes with unique endpoint IDs that you can then use to configure DAP records. New/modified screens: • **Devices** > **Dynamic Access Policy** > **Add/Edit Policy** > **Posture Assessment Criteria** • **Devices** > **Dynamic Access Policy** > **Add/Edit Policy** > **Add/Edit DAP Record** > **Advanced** > **Endpoint Criteria** See: Dynamic Access Policies
Routing			
Use PBR to handle traffic based on user-defined domains.	7.7.0	7.7.0	You can now use policy based routing to handle traffic based on user-defined domains. Create a basic custom application detector with your domain patterns and the NSG (network service group) tag, then use it in an extended ACL in your PBR policy. See: Policy Based Routing
Access Control: Threat Detection and Application Identification			
Easily block traffic based on TLS version and server certificate status.	7.7.0	7.7.0	New options in the decryption policy wizard make it easier to block traffic based on TLS version and server certificate status. Enabling these options adds predefined rules that do this. After the policy is created, you can edit, reorder, or delete the rules. New/modified screens: **Policies** > **Decryption** > **Create Decryption Policy** > **Blocking** See: Decryption Policies, Decryption Rules
Use EVE to easily bypass decryption for low-risk connections to trusted URLs.	7.7.0	7.7.0	A new Client Threat decryption rule condition and a new option in the decryption policy wizard and make it easier to bypass decryption to trusted URLs for low risk (as identified by EVE) connections. New decryption policies now include predefined rules that do this, using Category (trusted) and Client Threat (low) conditions. The Client Threat condition is new and represents the EVE verdict. For outbound decryption, you enable/disable these rules as part of creating the policy. For inbound decryption, the rules are disabled by default. After the policy is created, you can edit, reorder, or delete the rules. New/modified screens: **Policies** > **Decryption** > **Create Decryption Policy** > **Decryption Exclusions** Version restrictions: You cannot deploy policies with Client Threat rules to older devices. See: Decryption Policies, Decryption Rules

Feature	Minimum Management Center	Minimum Threat Defense	Details
New EVE exceptions.	7.7.0	7.7.0	You can now bypass EVE (encrypted visibility engine) block verdicts based on source network and on destination dynamic attributes. And, when bypassing based on network, you can now use FQDN network objects. Previously, you could only block based on destination network or EVE process name and could not use FQDNs. New/modified screens: • To add an exception from the access control policy, in the advanced settings, edit and enable **Encrypted Visibility Engine**, enable **Block Traffic Based on EVE Score**, and **Add Exception Rule**. • To add an exception from the Unified Events viewer, right-click a connection that was blocked by EVE and select **Add EVE Exception**. See: Cisco Secure Firewall Management Center Snort 3 Configuration Guide
EVE dashboard enhancements.	7.7.0	7.7.0	The Summary dashboard (the default home page for the Firewall Management Center) now includes encrypted visibility engine information in its own tab, including widgets for discovered processes, threat confidence, malicious processes, and connections with detected process names. The widgets for malicious processes and connections with detected process names are new, and show data from Version 7.7+ devices only. The widgets for discovered processes and threat confidence were previously on the Application Statistics dashboard, and show data from all managed devices. Note that you did modify the EVE tab on the Application Statistics dashboard, the upgrade retains your changes but does not add the new widgets. If you did not modify the tab, it is removed. See: Dashboards
Event Logging and Analysis			
SNI information from the ClientHello message in connection events.	7.7.0	7.7.0	Connection events now include the TLS Client SNI field, which shows the SNI (server name indication) information from the ClientHello message. This indicates the hostname a client is trying to connect to. See: Connection and Security-Related Connection Events
‘Pending Rule Match’ reason in connection events.	7.7.0	Any	A new connection event reason, Pending Rule Match, marks a connection that ended before it matched any access control role. See: Connection and Security-Related Connection Events
Health Monitoring			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Get alerts before service authentication certificates expire.	7.7.0	7.7.0	To help prevent unexpected service disruptions, a new Certificate Monitoring health module alerts you before service authentication certificates expire on the Firewall Management Center and managed devices. New/modified screens: **System** (⚙) > **Health** > **Policy** > **Health Modules** > **Certificate Monitoring** See: Health
Monitor the event database.	7.7.0	Any	The Firewall Management Center uses a MonetDB database for firewall events and event-related data like connection summaries. A new MonetDB Statistics health module collects database statistics that you can also see in the health monitor: database size, active connections, memory use, data requests processed, slow-running requests, and so on. This module is enabled for new and upgraded Firewall Management Centers. Troubleshooting best practice is to leave it enabled. New/modified screens: **System** (⚙) > **Health** > **Policy** > **Health Modules** > **MonetDB Statistics** See: Health
Upgrade			
Upgrade Firewall Threat Defense or chassis without a manual readiness check.	7.7.0	7.7.0	You no longer have to run time-consuming pre-upgrade readiness checks for Firewall Threat Defense or chassis upgrades. Instead, these checks are now regularly run by the system and reported in the health monitor. This allows you to preemptively fix any issues that will block upgrade. • The Database module, new for devices, manages monitors database schema and configuration data (*EO*) integrity. • The FXOS Health module, new for devices, monitors the FXOS httpd service on FXOS-based devices. • The Disk Status module is now more robust, alerting on disk health issues reported by daily running of smartctl (a Linux utility for monitoring reliability, predicting failures, and performing other self-tests). Version restrictions: This feature is supported for upgrades *from* Version 7.7+. Devices running earlier versions still require the in-upgrade readiness check. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center

Feature	Minimum Management Center	Minimum Threat Defense	Details
Upgrade Firewall Management Center without a manual readiness check.	7.7.0	Any	You no longer have to run time-consuming pre-upgrade readiness checks for Firewall Management Center upgrades. Instead, these checks are now regularly run by the system and reported in the health monitor. This allows you to preemptively fix any issues that will block upgrade. Version restrictions: This feature is supported for upgrades *from* Version 7.7+. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
Skip post-upgrade deploy for Firewall Management Center.	7.7.0	Any	In many cases, you no longer have to deploy to Snort 3 devices after you upgrade the Firewall Management Center. If deploy is required, affected devices are marked out of date (with a few exceptions). Reasons for needing to manually deploy include: • The upgrade updated the LSP and scheduled LSP updates are off. • The upgrade updated the LSP and scheduled LSP updates are on, but automatic redeploy is off. Devices may not be marked out of date in this case. Note that if automatic redeploy is on, the redeploy will take place on schedule and you do not need to do it manually. • Specific configurations changed by the upgrade require a deploy. • You need to upgrade managed devices immediately. After Firewall Management Center upgrade, you cannot upgrade managed devices until you redeploy, even if they are not marked out of date. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
SRU update moved out of Firewall Management Center upgrade.	7.7.0	Any	**Upgrade impact. After Firewall Management Center upgrades to Version 7.7+, wait for SRU to install.** Instead of upgrading the SRU as part of the upgrade, the system now updates intrusion rules for Snort 2 devices (the *SRU*) after the upgrade completes and the Firewall Management Center reboots. Although this makes the upgrade itself faster, you cannot update intrusion rules, add devices, or deploy configuration changes while the SRU is updating. This occurs regardless of whether you are managing any Snort 2 devices. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
Administration			
Cancel Firewall Threat Defense backups, view detailed backup status.	7.7.0	7.7.0	The Message Center now displays detailed backup status for the Firewall Management Center and its devices. You can also cancel in-progress device backups. See: Backup/Restore

Feature	Minimum Management Center	Minimum Threat Defense	Details
Restrict Firewall Management Center SAML SSO logins to a subdomain.	7.7.0	Any	In a multidomain deployment, you can now restrict Firewall Management Center SAML SSO logins to a subdomain. This can only be configured at the global domain level. See: Users
Clear disk space utility.	7.7.0	7.7.0	A new utility allows you to click to safely remove unneeded files such as old backups, content updates, and troubleshooting files. Low disk space can reduce performance, prevent upgrade, and increase the risk of accidentally deleting important files when trying to recover space. New/modified screens: We added a **Clear disk space** button to the Disk Usage widget on health dashboards: **System** (⚙) > **Health** > **Monitor**. See: Troubleshooting
New dark theme and theme name changes.	7.7.0	Any	There are now three themes available for the Firewall Management Center: • *Light* is a renamed New theme—the left-hand navigation theme introduced recently. • *Dark* is a new left-hand navigation theme that replaces the Dusk theme. If you were using the Dusk theme, you are switched to the Dark theme. • *Legacy* is a renamed Light theme. To change themes, click your username in the top right corner of the Firewall Management Center web interface. See: Users
Performance and Resiliency			
Faster failover for high availability Firewall Threat Defense.	7.7.0	7.7.0	With Firewall Threat Defense high availability failover, the new active device generates multicast packets for each MAC address entry and sends them to all bridge group interfaces, which prompts the upstream switches to update their routing tables. This task now runs asynchronously in the data plane, privileging critical failover tasks in the control plane. This makes failover faster, reducing downtime. See: High Availability
Dynamic flow offload for the Secure Firewall 3100/4200.	7.7.0	7.7.0	Dynamic flow offload is now supported on the Secure Firewall 3100/4200. Previously, it was only supported on the Firepower 4100/9300. This feature is enabled in new and upgraded deployments. Platform restrictions: Not supported with container instances. See: Prefiltering

Feature	Minimum Management Center	Minimum Threat Defense	Details
Use a loopback interface on Firewall Threat Defense Virtual for GCP to receive health probes from the GCP load balancer.	7.7.0	7.7.0	You can now use a dedicated loopback interface on Firewall Threat Defense Virtual for GCP to receive health probes from the GCP load balancer in autoscale deployments. This allows the system to handle health probes more efficiently, improving performance. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
Configure Firewall Threat Defense autorecovery from block depletion using FlexConfig.	7.7.0	7.7.0	To reduce downtime due to service disruption, a new fault manager monitors block depletion and automatically reloads devices when necessary. In high availability deployments, this triggers failover. Fault monitoring is automatically enabled on new and upgraded devices. To disable, use FlexConfig. New/modified FlexConfig commands: • **fault-monitor block-depletion recovery-action** { **none** | **reload** } Specifying **none** turns off automatic reload, but does not turn off fault monitoring. For that, use **no fault-monitoring**. • **fault-monitor block-depletion monitor-interval** *seconds* You can configure how long (in seconds) before the device reloads. New/modified Firewall Threat Defense CLI commands: **show fault-monitor block-depletion** { **status** | **statistics** } Platform restrictions: Not supported for clustered devices. See: Troubleshooting
Troubleshooting			
CPU profiler includes application identification statistics.	7.7.0	7.7.0	The CPU profiler now includes application identification statistics. That is, you can now see the resources used by processing specific application traffic. After you enable CPU profiling, use the CLI to see results. New/modified CLI commands: **system support appid-cpu-profiling status**, **system support appid-cpu-profiling dump** See: Troubleshooting, Cisco Secure Firewall Threat Defense Command Reference
Processing statistics in connection events.	7.7.0	7.7.0	To help with performance troubleshooting, connection events now contain two new fields: Inspection Duration (microseconds) and Inspected Packets. See: Connection and Security-Related Connection Events

Feature	Minimum Management Center	Minimum Threat Defense	Details
New IP flow statistics.	7.7.0	7.7.0	When collecting IP flow statistics from Firewall Threat Defense under the direction of Cisco TAC, a new **all** parameter logs additional statistics to the specified file: port, protocol, application, cumulative latency, and inspection time. New/modified commands: **system support flow-ip-profiling start flow-ip-file** *filename* **all** { **enable** | **disable** } See: Cisco Secure Firewall Threat Defense Command Reference
Cisco RADKit integration.	7.7.0	7.7.0	Cisco RADKit integration allows Cisco TAC engineers to remotely connect with your deployment (including sudo access) for an enhanced troubleshooting experience. You control the appliances and duration of access. This also gives you and Cisco TAC access to diagnostic data and logs. New/modified screens: **Devices** > **Remote Diagnostics** > **Enable the RADKit service** See: Troubleshooting
Security and Hardening			
Limited user privileges for Threat Defense CLI Basic user.	7.7.0	7.7.0	The scope of the Threat Defense CLI Basic user privilege is now limited to the following commands: dig, ping, traceroute. If you have created users with the Basic privilege, evaluate whether you need to change them to the Config privilege. You can change a user's privilege level using the **configure user access** command. See: Cisco Secure Firewall Threat Defense Command Reference
Deprecated Features			
Deprecated: Snort 2.	7.7.0	7.7.0	**Upgrade impact. Cannot upgrade Snort 2 devices.** Snort 2 is deprecated. You cannot upgrade a Snort 2 device to Version 7.7.0+. Although you can use a Version 7.7.0+ Firewall Management Center to manage older Snort 2 devices, you should still switch to Snort 3 for improved detection and performance. Deprecated CLI commands: **show snort counters**, **show snort preprocessor-memory-usage**. See: Cisco Secure Firewall Management Center Snort 3 Configuration Guide
Deprecated: Access control policy legacy interface.	7.7.0	Any	You can no longer use the legacy user interface for access control policies. If you were using it, you switch to the improved user interface introduced in Version 7.2. New/modified screens: **Switch to Legacy UI** toggle is removed

Firewall Device Manager Features in Version 7.7.x

Table 4: Firewall Device Manager Features in Version 7.7.x

Feature	Description
Platform Features	
Secure Firewall 1230, 1240, and 1250 (rack-mount).	We introduced the Secure Firewall CSF-1230 and CSF-1240: • 8x1Gbps RJ-45 1000BASET/2.5BBASE-T copper • 4x1Gbps SFP+ optical And the Secure Firewall CSF-1250: • 8x2.5Gbps1000BASET/2.5BBASE-T copper • 4x2.5Gbps SFP28 optical See: Cisco Secure Firewall CSF-1230,CSF-1240, and CSF-1250 Hardware Installation Guide
Secure Firewall 1210CP IEEE 802.3bt support (PoE++ and Hi-PoE).	We made the following improvements related to support for IEEE 802.3bt: • PoE++ and Hi-PoE—Up to 90W per port. • Single- and dual-signature powered devices (PDs). • Power budgeting is done on a first-come, first-served basis. • Power budget fields were added to **show power inline**. New/modified screens: **Device** > **Interfaces** > **PoE** New/modified commands: **show power inline**
Instances for AWS, Azure, and GCP.	We added instances for threat defense virtual from the following families: • AWS (Amazon Web Services): C6i, C6a • Azure (Microsoft Azure): Dv4, Dv5 • GCP (Google Cloud Platform): E2, N1, N2D, C2D See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
Unattended provisioning for Firewall Threat Defense Virtual for VMware using ISO-based cloud-init seeding.	You can now quickly deploy Firewall Threat Defense Virtual for VMware using a text file (day0.iso) that contains initial setup details such as hostname, password, management mode, firewall mode, network settings, and deployment type. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
Firewall and IPS Features	
Hardware bypass support for inline sets.	If your device model supports hardware bypass, you can now configure it for inline sets containing supported interfaces. We added the **Bypass** option to inline set configuration.

Feature	Description
Deprecated: Snort 2.	**Upgrade impact. Cannot upgrade Snort 2 devices.** Snort 2 is deprecated. You cannot upgrade a Snort 2 device to Version 7.7.0+. We removed the ability to switch to Snort 2, as well as the **show snort counters** and **show snort preprocessor-memory-usage** commands. Before you upgrade, switch to Snort 3. See the *Intrusion Policies* chapter in the guide for your current version: Cisco Secure Firewall Device Manager Configuration Guide.
Administrative Features	
Custom login page.	You can customize the device manager login page, including adding an image and text to the login page. For example, you can include disclaimers and warnings where the user must agree prior to login. The text is also shown for SSH sessions. We added the following page: **System Settings** > **Login Page**.
Custom streaming telemetry using Google Remote Procedure Calls (gRPC).	You can configure the device to send system health and telemetry data to an external telemetry collector that uses Google Remote Procedure Calls (gRPC) to collect data. You can then use your telemetry collector to monitor the device and integrate with your custom telemetry solution. Use the API to configure this feature: /devicesettings/default/telemetrystreamingconfig.
Performance	
Faster failover for high availability Firewall Threat Defense.	With threat defense high availability failover, the new active device generates multicast packets for each MAC address entry and sends them to all bridge group interfaces, which prompts the upstream switches to update their routing tables. This task now runs asynchronously in the data plane, privileging critical failover tasks in the control plane. This makes failover faster, reducing downtime.
High-bandwidth encrypted application traffic bypasses unnecessary intrusion inspection.	Specific high-bandwidth encrypted application traffic now bypasses unncessary intrusion inspection even if the connection matches an Allow rule. Intrusion rule (LSP) and vulnerability database (VDB) updates can change the applications bypassed but right now they are: AnyConnect, IPsec, iCloud Private Relay, QUIC (including HTTP/3), Secure RTCP. Version restrictions: Requires Version 7.2.10+ / 7.6.1+ / 7.7.0+.

Feature	Description
Configure Firewall Threat Defense autorecovery from block depletion using FlexConfig.	To reduce downtime due to service disruption, a new fault manager monitors block depletion and automatically reloads devices when necessary. In high availability deployments, this triggers failover. Fault monitoring is automatically enabled on new and upgraded devices. To disable, use FlexConfig. New/modified FlexConfig commands: - **fault-monitor block-depletion recovery-action** { **none** | **reload** } Specifying **none** turns off automatic reload, but does not turn off fault monitoring. For that, use **no fault-monitoring**. - **fault-monitor block-depletion monitor-interval** *seconds* New/modified threat defense CLI commands: **show fault-monitor block-depletion** { **status** | **statistics** }
Troubleshooting	
CPU profiler includes application identification statistics.	The CPU profiler now includes application identification statistics. After you enable CPU profiling (**cpu profile activate**), you can see the resources used by processing specific application traffic. New/modified CLI commands: **system support appid-cpu-profiling status**, **system support appid-cpu-profiling dump** See: Cisco Secure Firewall Threat Defense Command Reference
New IP flow statistics.	When collecting IP flow statistics from Firewall Threat Defense under the direction of Cisco TAC, a new **all** parameter logs additional statistics to the specified file: port, protocol, application, cumulative latency, and inspection time. New/modified commands: **system support flow-ip-profiling start flow-ip-file** *filename* **all** { **enable** | **disable** } See: Cisco Secure Firewall Threat Defense Command Reference
Security and Hardening	
Limited user privileges for Threat Defense CLI Basic user.	The scope of the Threat Defense CLI Basic user privilege is now limited to the following commands: dig, ping, traceroute. If you have created users with the Basic privilege, evaluate whether you need to change them to the Config privilege. You can change a user’s privilege level using the **configure user access** command. See: Cisco Secure Firewall Threat Defense Command Reference

Feature	Description
Require the Message-Authenticator attribute in all RADIUS responses.	**Upgrade impact. After upgrade, enable for existing servers.** You can now require the Message-Authenticator attribute in all RADIUS responses, ensuring that the threat defense VPN gateway securely verifies every response from the RADIUS server, whether for RA VPN or access to the device itself. The **Require Message-Authenticator for all RADIUS Responses** option is enabled by default for new RADIUS servers. We also recommend you enable it for existing servers. Disabling it may expose firewalls to potential attacks. New CLI commands: **message-authenticator-required** Version restrictions: Requires Version 7.0.7+ / 7.2.10+ / 7.6.1+ / 7.7.0+.

Upgrade Impact Features

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.

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 22.

Upgrade Impact Features for Firewall Management Center

Table 5: Upgrade Impact Features for Firewall Management Center

Target version	Features with upgrade impact
7.7.0+	• SRU update moved out of Firewall Management Center upgrade. • New Cisco AMP cloud connection method.
7.6.0+	• Allow Cisco Talos to conduct advanced threat hunting and intelligence gathering using your traffic. • Cisco Security Cloud replaces SecureX. • Updated internet access requirements for URL filtering. • Updated internet access requirements for intrusion rule updates. • Cisco Success Network and Cisco Support Diagnostics are enabled by default.

Target version	Features with upgrade impact
7.4.1+	• Configure DHCP relay trusted interfaces from the Firewall Management Center web interface. • Updated internet access requirements for direct-downloading software upgrades. • Deprecated: scheduled download of maintenance releases. • Improved Firewall Management Center memory usage calculation, alerting, and swap memory monitoring. • Updated web analytics provider.
7.4.0+	• Configure Firewall Threat Defense devices as NetFlow exporters from the Firewall Management Center web interface. • Access control performance improvements (object optimization). • Smaller VDB for lower memory Snort 2 devices.
7.3.0+	• Configure BFD for BGP from the Firewall Management Center web interface. • Automatically update CA bundles. • Updated internet access requirements for Smart Licensing.

Upgrade Impact Features for Firewall Threat Defense with Firewall Management Center

Table 6: Upgrade Impact Features for Firewall Threat Defense with Firewall Management Center

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

Current version	Features with upgrade impact
7.3.x and earlier	• 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)
7.2.x and earlier	• Auto-upgrade to Snort 3 after successful Firewall Threat Defense upgrade is no longer optional. (7.3.0) • Combined upgrade and install package for Secure Firewall 3100. (7.3.0) • NetFlow support for Snort 3 devices. (7.3.0)
7.2.0–7.2.3 7.1.0–7.1.0.2 7.0.4 and earlier	• Automatically update CA bundles. (7.0.5)

Upgrade Impact Features for Firewall Threat Defense with Firewall Device Manager

Table 7: Upgrade Impact Features for Firewall Threat Defense with Firewall Device Manager

Target version	Features
7.7.0+	• Require the Message-Authenticator attribute in all RADIUS responses. • Deprecated: Snort 2.
7.6.0+	• Updated internet access requirements for URL filtering. • Updated internet access requirements for intrusion rule updates.
7.4.1+	• Merged management and diagnostic interfaces. • IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100. • Sensitive data detection and masking. • Firmware upgrades included in FXOS upgrades. • Default NTP server updated.
7.3.0+	• TLS 1.3 support in SSL decryption policies, and configurable behavior for undecryptable connections. • Combined upgrade and install package for Secure Firewall 3100. • Automatically update CA bundles.

Upgrade Guidelines

The following sections contain release-specific upgrade warnings and guidelines. You should also check for features and bugs with upgrade impact. For general information on time/disk space requirements and on system behavior during upgrade—which can include interruptions to traffic flow and inspection—see the appropriate upgrade guide: For Assistance, on page 81.

Upgrade Guidelines for Firewall Management Center

Table 8: Upgrade Guidelines for Firewall Management Center

Current Version	Guideline	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.

Upgrade Guidelines for Firewall Threat Defense with Firewall Management Center

Table 9: Upgrade Guidelines for Firewall Threat Defense

Current Version	Guideline	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.

Upgrade Guidelines for Firewall Threat Defense with Firewall Device Manager

Table 10: Upgrade Guidelines for Firewall Threat Defense

Current Version	Guideline	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.

Upgrade Guidelines for the Firepower 4100/9300 Chassis

In most cases, we recommend you use the latest build for your FXOS major version.

For release-specific FXOS upgrade warnings and guidelines, as well as features and bugs with upgrade impact, check all release notes between your current and target version: http://www.cisco.com/go/firepower9300-rns.

Upgrade Path

Planning your upgrade path and order is especially important for large deployments, high availability/clustering, multi-hop upgrades, and situations where you need to coordinate chassis, hosting environment, or other upgrades. Those scenarios, as well as information on revert and uninstall, are covered in more detail in the upgrade guide: For Assistance, on page 81.

Choosing your upgrade target

Go **directly to the latest maintenance release** 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 11: Released before Version 7.7.x, by date

Target version		**Current version: confirm yours is listed.**				
		from 7.2	**7.3**	**7.4**	**7.6**	**7.7**
to 7.7.10	2025-08-11	7.2.0–7.2.10	7.3.0–7.3.1	7.4.0–7.4.2	7.6.0–7.6.2	7.7.0
to 7.7.0	2025-03-05	7.2.0–7.2.9	7.3.0–7.3.1	7.4.0–7.4.2	7.6.0	—

Upgrading from a patched deployment

Critical fixes in patches (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 or Cisco Secure Firewall Device Manager 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 22.
- 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.

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.

For the Firepower 4100/9300, the table also 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 12: Supported direct upgrades

Current version	Target software version						
	to 7.7	7.6	7.4 *	7.3	7.2	7.1	7.0
	FXOS version for Firepower 4100/9300 chassis upgrades						
	to 2.17	2.16	2.14	2.13	2.12	2.11	2.10
from 7.7	YES	—	—	—	—	—	—
from 7.6	YES	YES	—	—	—	—	—
from 7.4	YES	YES	YES	—	—	—	—
from 7.3	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.

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.

Bugs

For bugs in earlier releases, see the release notes for those versions. For cloud deployments, see the Cisco Cloud-delivered Firewall Management Center Release Notes.

Important We do not list open bugs for maintenance releases or patches.

Important Bug lists are auto-generated once and may not be subsequently updated. If updated, the 'table last updated' date does not mean that the list was fully accurate on that date—only that some change was made. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes. If you have a support contract, you can obtain up-to-date bug lists with the Cisco Bug Search Tool.

Open Bugs in Version 7.7.0

Table last updated: 2025-03-05

Table 13: Open Bugs in Version 7.7.0

Bug ID	Headline
CSCwn84258	Confusing Verdict for Snort Injects - Change From Block to "Replaced"/"Injected"
CSCwo27175	1240: intermittent exhaustion of asymmetric buffers are observed with teravm tls traffic
CSCwo01338	9.23/SecGW with flow-offload cluster-redirect enabled causes Out of Sequence TCP Packets for TCP 450
CSCwo32191	Deployment Fails due to Config Error response from LINA

Resolved Bugs in Version 7.7.10

Resolved Security Bugs in Version 7.7.10

Table last updated: 2025-08-11

Table 14: Resolved Security Bugs in Version 7.7.10

Bug ID	Headline
CSCwh10931	ASA/FTD traceback and reload when invoking "show webvpn saml idp" CLI command
CSCwn86912	Unable to load Extended ACL objects if the count is more than few hundreds
CSCwn88931	Snort3: Malware Policy not detecting file while performing FTP file transfer via Active FTP
CSCwn91730	FMC API put taking long time to update Extended ACL objects when count is huge like hundreds
CSCwo14426	Unable to save the Ext ACL object - "Only Host and Network in IPv4 and IPv6 format are supported."
CSCwo52298	Duplicate ACLs seen on FMC UI when Access Rules are created through API
CSCwo57216	cdFMC deployment randomly removes ACL/crypto maps when deploying in bulk
CSCwp05496	Cleaning of /var/temp backup files post Backup completion not cleaning
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

Resolved Functional Bugs in Version 7.7.10

Table last updated: 2025-08-11

Table 15: Resolved Functional Bugs in Version 7.7.10

Bug ID	Headline
CSCvx66624	Write cache is disabled on some FMC M5 appliances
CSCwc77650	FMC action_queue.log cosmetic defect "synchronization" misspelled, Expected "Synchronization"
CSCwd80348	FMC does not support Umbrella with proxy setting
CSCwe28608	Snort returns "Blocked by SSL" with no SSL policy.
CSCwe89818	External Auth on FMC may throw err "Can't use string ("") as a HASH ref while "strict refs" in use"
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
CSCwh05126	FDM HA Switch : Peer fails to get into Active state due to Interface check
CSCwh08441	ENH: Add a command or a script to regenerate CA Certificate on FTD
CSCwh53745	ASA: unexpected logs for initiating inbound connection for DNS query response
CSCwk42676	Virtual ASA/FTD may traceback and reload in thread PTHREAD
CSCwm63648	Set Weight option missing in UI when FTD sensor reverted and re-upgraded
CSCwm63890	FMC GUI does not allow saving ECMP configuration when there is a route leak for a VRF
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
CSCwm87669	Discrepency in the unused object count between the FMC UI and API results
CSCwm96652	Cluster assigning wrong nat for unit, traffic not being forwarded properly back to unit
CSCwn00475	Memory Blocks 80 and 9344 leak due to priority-queue
CSCwn06645	FIPS self-test failure message needed

Bug ID	Headline
CSCwn07008	Use of Named interface in SLA Monitor causing cdFMC migration failure
CSCwn13421	Scale cdFMC:Policy deploy fails when Audit log to Syslog is configured with invalid ipv6 syslog host
CSCwn27872	Big chunk of Memory of around 25KB is being allocated on Stack in "eigrp_interface_ioctl" API
CSCwn35495	Primary FTD instance MAC address is not updated correctly in FXOS during failover
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
CSCwn44527	Intrusion policy having same name in different Domains causes IPS policy corruption
CSCwn45510	S2S VPN tunnel Child SA unsuccessful renegotiation
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
CSCwn50961	Send Virtual Tunnel Interface enabled by default on SVTI
CSCwn51136	Mount EFS using NFSv4.1
CSCwn51845	Tracebacks observed in a cluster member running ASA 9.20.3.4
CSCwn60836	FTD: deploy failure when configured L2 access-list. "Cannot mix different types of access lists."
CSCwn63839	Traceback in thread name Lina on configuring arp permit-nonconnected with BVI
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
CSCwn71426	Clearing all non applicable alerts post license registration success
CSCwn71946	show blocks old core local can lead to unexpected reload.
CSCwn73351	Asia/Bangkok timezone option not listed in ASA running on firepower1k

Bug ID	Headline
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."
CSCwn77091	SFDataCorrelator cores after purging orphan hosts
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
CSCwn83268	Realm with greater than 16 directories cannot be deployed in RA-VPN for LDAP
CSCwn84557	Lina traceback and reload due to "spin_lock_fair_mode_enqueue"
CSCwn85765	ipv6 ping Vrf name changed after xml processing
CSCwn87249	snort3 : FMC connection event logs do not show URL in DNS query using TCP
CSCwn89243	Identity NAT should not throw error due to exceeding threshold if destination only objects expand
CSCwn90900	High ASA/FTD memory usage due to polling of RA VPN related SNMP OIDs
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"
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
CSCwn97341	MonetDB Monitor should detect missing columns in stats partitions
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

Bug ID	Headline
CSCwo00702	Community lists should not throw an error until the last item in the list is being deleted
CSCwo01014	Unable to Form HA with Domain Containing "." While Registering FMC
CSCwo01616	sfipproxy prometheus configuration is attempted for not supported models and replaces sfipproxy.conf
CSCwo06044	Exclude perf monitoring files from device backup
CSCwo07498	QUIC: LINA crash in timer with stress test
CSCwo08042	ASAv reloaded unexpectedly with traceback on Unicorn Proxy Thread
CSCwo08306	Command authorization fallback to Local only works for priv 15 users.
CSCwo08449	"Add Device(wizard)" is not working as expected.
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.
CSCwo09618	Enabling debugs with EEM fails
CSCwo12801	Detectors sync issue on FMC upgraded to 7.7
CSCwo13863	Snort3 crashed because don't fragment bit was set and it did not treat ipv4 fragments as fragments
CSCwo14722	Prune the older files in /ngfw/var/cisco/deploy/pkg/var/cisco/packages
CSCwo14737	FTD - LSP Installation/ Deployment Failure
CSCwo15715	IKEv2 Rekeys fail due to fragmentation during the IKE Rekey
CSCwo16016	Users from legacy radius server can login to Standby FMC domain when MA is enabled
CSCwo16049	False alert "Terminating long running backup" on FMC due to UI backup timeout error.
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.
CSCwo21767	Port scan alerts not getting generated for custom configuration
CSCwo21830	Reduce TS package size

Bug ID	Headline
CSCwo24772	debug packet-condition does not work as expected
CSCwo25271	Empty snapshot being sent when when auth-daemon restarts causing user logout
CSCwo25478	auth-daemon process restarts due to race condition
CSCwo25786	REST Api allows to create a realm without a directory configuration
CSCwo26286	Management1 Gateway Configuration Should Be Optional on FPR 4200 Series
CSCwo26725	FMC Site-to-Site Monitoring Dashboard is not working at all
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
CSCwo34220	Random QOS policies are getting negatted and added with subsequent deployment
CSCwo34833	cdFMC: Chassis is always seen as " Not synced" in CDO page even though it is connected and up
CSCwo35585	AMP related health alert during upgrade and typo in the alert message
CSCwo35783	Enhance Debugging for add/update/withdraw of routes with neighbors
CSCwo35788	Serviceability Enhancement - New 'show bgp internal' command for advanced debugging
CSCwo35810	show bgp update-group a.b.c.d displays "no such neighbor" when there is a valid neighbor
CSCwo37055	FMC: Media type displayed on the FMC's FCM is not matching CLI after swapping sfps
CSCwo41250	Traceback & Reload in thread named: DATAPATH-1-23988 during low memory condition
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
CSCwo45848	SecGW: Data node fails to join the cluster with cluster_ccp_make_rpc_call failed to clnt_call error
CSCwo47978	ASA may traceback and reload in Thread Name 'fover_parse'
CSCwo48607	Installation of Hotfix may fail at 800_post/998_expire_ac_policy.pl on the standby FMC

Bug ID	Headline
CSCwo48630	Deployment is failing due to the policy changes report request in progress
CSCwo49425	Logging recipient-address not overriding the logging mail message severity levels
CSCwo49744	DNS and default gateway are removed on FTD managed through data interface
CSCwo50885	/mnt/disk0/log folder duplicated on troubleshooting package
CSCwo53892	FTD health metrics show "No data available" on the FMC
CSCwo55662	FMC Rest API returns only the first 1000 network object entries
CSCwo57744	Overrides not working on chained/inherited custom IPS policies
CSCwo58130	Duplicate entries in EventCatalog can cause incorrect unified2 id to be sent
CSCwo58260	Add "built" and "teardown" messages for the GRE | IPinIP connections to the Lina syslog
CSCwo61240	After renewal FMC CA, the certificate cannot be used for ArcSight integration
CSCwo62543	Default Pass action for rules in Snort 3 local rule groups may cause blank error in IPS policies
CSCwo63951	FMC/FDM Client side certificate used to communicate to Talos did not auto-renew correctly
CSCwo66307	cdFMC: Deployment failed due to the deployment manager is not initialized properly
CSCwo70260	/objects/fqdn filter paramaters not working
CSCwo71835	The NAS-IP-Address attribute is missing from the Access-Request in FMC
CSCwo74265	FTD Upgrade Retry failure (Unable to execute Retry after failure in FTD while upgrading to 7.7.10)
CSCwo74305	Deployment Failure in Hub and Spoke VTI Topology with DHCP Configured VPN Interfaces
CSCwo75810	SNMP configuration is not applied consistently across same FTDs type and version
CSCwo76436	3100 Marvell 4.3.14 CPSS patch for the interface mac stuck issue seen with peer switch reloads
CSCwo76537	UEV breaks with duplicate event indexes
CSCwo76554	TLS handshake fails with reverse SSL flow and TSID (TLS Server Identity) enabled
CSCwo77662	Certain special characters or spaces in RADIUS user passwords cause login failure in FMC
CSCwo77937	minidump core file not generating in MI mode

Bug ID	Headline
CSCwo79114	Post reposition or move operation fails then if user saves, it would to lead loss of rules & may cause an outage
CSCwo83087	Manual router ID does'nt get displayed in UI for BGP general settings
CSCwo85252	FMC page may get stuck in loading state while trying to fetch BGP configuration
CSCwo86835	SMB remote FMC backups are failing due to relam sync
CSCwo91053	fover_trace.log not rotating and growing to a massive size
CSCwo94360	Do not fail parallel write API call from same user session. Retry should be done internally before failing
CSCwo96941	The total disk keep on increasing on the disk status wizard on the Health Monitor page.
CSCwp00618	Devices show offline due to "Appliance unreachable" due to HMS deadlock inserting to DB
CSCwp02255	Snort2 crashes in loop after FMC upgrade
CSCwp03056	Getting VNI int cannot be configured with proxy enabled error during model migration when proxy is disabled on VNI int
CSCwp03910	Subsequent DNS packets are dropped in a single flow if one domain hits the custom DNS SI block list
CSCwp04040	AMP vault credentials are not persisted after cdFMC upgrade
CSCwp08291	cdFMC DR - cdFMC_Snapshot generation failing while trying to copy sftunnel related files.
CSCwp11985	Deployment is mandatory after FMC upgrade condition should be included in Upgrade code
CSCwp15886	Unable to change few IPS rule actions after upgrading from snort2 to snort3
CSCwp15949	The "Module run errors" alert on the FMC GUI should be updated to a more contextually relevant message
CSCwp16546	Tunnel Status shows "No Active Data" when spoke behind NAT on S2S Monitoring UI
CSCwp26878	cdFMC returns 403 forbidden error while configuring webhook alerts
CSCwp32097	Domain filter is non-functional under ACP on cisco-jagan-test
CSCwp83566	SSL - Issues with DND a particular site after FTD upgrade on Chrome and Edge post upgrade
CSCwp92489	SFDataCorrelator_user_id_mismatch.log overconsumption of disk
CSCwp96945	Required Horizontal scroll bar in admin/sensor/remote_backup.cgi

Bug ID	Headline
CSCwp98782	Internal error when saving local rules in Rule Overrides section of IPS policy
CSCwq18259	cdfmc user-preference issue
CSCwq19928	Vault slowness might cause Auth-Daemon deadlock if lease is denied
CSCwq20009	Scrolling in AC Policy UI may result in UI refreshing and displaying blank page if Mandatory Section is empty
CSCwq27820	cdFMC 7.7.10 email notification stopped working
CSCwq30335	Backup Timeout is not sufficient when FTD backups are huge and low bandwidth
CSCwq46783	FMC Authentication Fails with freeradius, "Invalid NAS IP Address" Error Displays Unexpected IP

Resolved Bugs in Version 7.7.0

Resolved Security Bugs in Version 7.7.0

Table last updated: 2025-06-17

Table 16: Resolved Security Bugs in Version 7.7.0

Bug ID	Headline
CSCvk74112	Evaluation of WSA for FreeBSD CVE-2018-6922
CSCvm44463	update RabbitMQ - 3.6.x is EOL
CSCwb38658	SMA: Which appliances are effected Infinite loop in BN_mod_sqrt() (CVE-2022-0778)
CSCwb67583	ASDM Access Issue When SSL VPN And HTTP Server Is Configured On Same Port
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwd50155	Evaluate FMC for CVE-2022-42252
CSCwd65251	WA-B/TPK: "core.sshd" files found on DUT
CSCwe42917	All Cisco EXR products impacted with sudo vulnerability CVE-2023-22809
CSCwe48399	The public API function BIO_new_NDEF is a helper function used for str
CSCwe86964	Consul and Consul Enterprise allowed an authenticated user with service:
CSCwe88928	Health Monitoring shows Unmanaged devices
CSCwf22483	SSH to Chassis allows a 3-way handshake for IPs that are not allowed by the config
CSCwf34069	Cisco ASA and FTD Remote Access SSL VPN Authentication Targeted Denial of Service Vulnerability

Bug ID	Headline
CSCwh10931	ASA/FTD traceback and reload when invoking "show webvpn saml idp" CLI command
CSCwh17395	Evaluation for CVE-2023-38408 on standalone NXOS N9K
CSCwh20307	FMC fails deployment after removing NAT or ACL rule
CSCwh39258	Occasionally External auth may not work after HA failover to Active
CSCwh41094	Cisco FTD TCP/IP Traffic Snort 2/3 Denial of Service Vulnerability
CSCwh52710	evaluate open-vm-tools / VMware Tools on FMC for VMware -- CVE-2023-20900 and VMSA-2023-0019
CSCwh88595	Evaluation of wsa for HTTP/2 Rapid Reset Attack vulnerability
CSCwh94197	MiniZip in zlib through 1.3 has an integer overflow and resultant heap
CSCwi05240	ASA - Traceback the standby device while HA sync ACL-DAP
CSCwi05435	[ENH] FMC to pull FTD device current SRU version rather than device records for SRU deployed.
CSCwi21625	FailSafe admin password is not properly sync'd with system context enable pw
CSCwi29934	Cisco FXOS Software Link Layer Discovery Protocol Denial of Service Vulnerability
CSCwi42291	Cisco Firepower Threat Defense Software TCP Snort 3 Detection Engine Bypass Vulnerability
CSCwi46163	Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.
CSCwi55527	[Snort3] - Ignore malformed packets received from lina with wrong dsize
CSCwi56499	Cut-Through Proxy feature spikes CP CPU with a flood of un-authenticated traffic
CSCwi60430	CVE-2023-51385 (Medium Sev) In ssh in OpenSSH before 9.6, OS command injection might occur if a us
CSCwi61058	Cisco Firepower Management Center Cross Site Scripting Vulnerability
CSCwi62683	The SSH transport protocol with certain OpenSSH extensions, found in ... (CVE-2023-48795)
CSCwi64429	MonetDB memory usage grows slowly over time
CSCwi65260	Modification of destination entries failed, when SOG and DOG contain same inner object-group
CSCwi78063	Cisco FTD Software and FMC Software Code Injection Vulnerability
CSCwi78370	41xx/93xx : Update CiscoSSH (Chassis Manager FXOS) to address CVE-2023-48795
CSCwi78593	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability

Bug ID	Headline
CSCwi78596	Cisco Firepower Management Center SQL Injection Vulnerabilities
CSCwi81503	HTTP/HTTPS detection for application needs to fail it's detection earlier
CSCwi81958	Impact of CVE-2023-48795 On WSA 15.0.0-337
CSCwi90040	Cisco ASA and FTD Software Command Injection Vulnerability
CSCwi96521	Push clear configure access-group to avoid error while applying access group on FTD
CSCwi96562	Cisco ASA and FTD FXOS CLI Root Privilege Escalation Vulnerability
CSCwi98274	unzip 5.52 is from 2005 is contains multiple vulnerabilities
CSCwi98284	Cisco ASA and FTD Software Persistent Local Code Execution Vulnerability
CSCwj03056	FMC username enumeration from API response
CSCwj03348	vFMC25 OCI to vFMC300 OCI migration failed 'Migration from Y to a is not allowed.'
CSCwj06675	Cisco ASA and FTD Software Persistent Local Code Execution Vulnerability
CSCwj08083	An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.1
CSCwj08667	ASA/FTD Traceback and Reload during ssl session establishment
CSCwj09110	Upload files through Clientless portal is not working as expected after the ASA upgrade
CSCwj10955	Cisco ASA and FTD Software Web Services Denial of Service Vulnerability
CSCwj11119	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwj12173	Policy cache cleanup thread should cleanup any cache that is left open for a logged out session
CSCwj14624	Backup exits with memory allocation error on 4115
CSCwj15792	Cisco ASA and FTD Software Dynamic Access Policies Denial of Service Vulnerability
CSCwj19125	Cisco ASA and FTD NSG Access Control List Bypass Vulnerability
CSCwj20804	Cisco ASA and FTD Software VPN Web Server Limited Information Disclosure Vulnerability
CSCwj33187	Internal cached access-group list maintenance issue with unexpected clear configure access-list
CSCwj45632	Deployment failures seen on FDM related to static routes or ACLs
CSCwj45822	Cisco ASA and FTD Software Remote Access VPN Brute Force Denial of Service Vulnerability
CSCwj48754	SFDataCorrelator high memory usage when restart with large network map hosts

Bug ID	Headline
CSCwj49745	Cisco ASA and FTD VPN Web Client Services Cross-Site Scripting Vulnerabilities
CSCwj58955	Can't make any changes on TPK 3110 chassis registered on FMC when chassis under domain
CSCwj59315	Smart license registration failing on FDM post 7.4.1 baseline due to http-proxy
CSCwj63974	Memory manager improvements for webvpn internal lua library
CSCwj68540	Cisco Secure Firewall Management Center Software Command Injection Vulnerability
CSCwj69533	Unable to change authentication methods on default tunnel group when using FDM
CSCwj72683	ASA - Bookmarks on the WebVPN portal are unreachable after successful login.
CSCwj77284	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwj79229	FMC - plain-text passwords for External Authentication Profile "Radius Server Key"
CSCwj91570	Cisco ASA and FTD Software Remote Access VPN Brute Force Denial of Service Vulnerability
CSCwj92223	Cisco Adaptive Security Appliance and Firepower Threat Defense TLS Denial of Service Vulnerability
CSCwj99043	Cisco ASA & FTD Software IKEv2 Denial of Service Vulnerability
CSCwj99068	Cisco ASA and FTD Software IKEv2 VPN Denial of Service Vulnerability
CSCwk05564	Only US region in FDM Cloud Services.
CSCwk07982	Cisco FTD Software for Firepower 1000, 2100, 3100, and 4200 Series Static Credential Vuln
CSCwk08241	FTD is not resolving FQDN for ACLs intermittently
CSCwk12484	Update UI to prevent configuring cipher and/or version filters for Decrypt Resign/Known Key rule
CSCwk12738	Cisco Adaptive Security Virtual Appliance and Secure FTD Virtual SSL VPN DoS Vulnerability
CSCwk21540	Unable to establish RAVPN session on FTD HA setup
CSCwk25117	ENH: Add application support for blocking consecutive AAA failures on LINA
CSCwk37414	Cloud regions dropdown may not show any regions if FMC connectivity is down during upgrade
CSCwk48975	Packet-tracer output incorrectly appends 'control-plane' to drops for data-plane access-group
CSCwk53369	Cisco ASA and FTD Software Remote Access VPN Denial of Service Vulnerability

Bug ID	Headline
CSCwk62296	Address SSP OpenSSH regreSSHion vulnerability
CSCwk62297	Evaluation of ssp for OpenSSH regreSSHion vulnerability
CSCwk67859	FTD and FXOS: RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS): July 2024
CSCwk67902	FTD: RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS): July 2024
CSCwk69454	FDM: Blast-RADIUS CVE-2024-3596
CSCwk69742	FTD: Policy deployment failed due to mismatch of checksum.
CSCwk71817	FMC: Blast-RADIUS CVE-2024-3596
CSCwk71992	BlastRADIUS vulnerability phase-1 fix for pix-asa - Message Authenticator
CSCwk74813	Cisco Adaptive Security Appliance and Firepower Threat Defense TLS Denial of Service Vulnerability
CSCwk74997	With CVE-ID cannot search the IPS events on the FMC
CSCwk75035	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vul
CSCwk75832	Snort3 reloads when AppID reload and snort restarts are happening simultaneously
CSCwk93503	around 400 tasks were created on primary FMC to install VDB updates on standby FMC
CSCwm05570	vFMC upgrade from 7.6.0-68 to 7.7.0-1358 failed @800_post/890_install_version_masked_apps.pl
CSCwm35624	Long boot time seen with one AC rule having object-group and other plain ACL's
CSCwm41195	Attempting to edit chassis of multinstance FTD gets "Request Timed Out. Retry after sometime."
CSCwm44719	FTD Snort3 traceback in daq_pkt_msg
CSCwm48671	Vulnerabilities in freebsd 13.0 CVE-2024-45287 - libnv
CSCwm49153	Cisco Adaptive Security Appliance Software SSH Server Resource DoS Vulnerability
CSCwm49410	Misconfigured Cross-Origin-Opener-Policy
CSCwm77247	FTD Restore Failing because of no space left on the device
CSCwn10158	cdFMC deployment removes ACL/crypto maps when deploying in bulk
CSCwn21134	FMC is not pushing no-validation-usage to the trustpoint if user not choosing validation usage type
CSCwn50488	Vulnerabilities in openssh 9.1p1 CVE-2023-28531

Bug ID	Headline
CSCwn55478	cdFMC Possible NAT negation during deployment if object being reused in NAT Policy on device & ACL
CSCwn69963	Addressing CVEs reported in unicorn zlib library
CSCwo44732	ARP is silently dropping packet for unreachable next-hops
CSCwo57216	cdFMC deployment randomly removes ACL/crypto maps when deploying in bulk

Resolved Functional Bugs in Version 7.7.0

Table last updated: 2025-03-14

Table 17: Additional Resolved Functional Bugs in Version 7.7.0-91 (Management Center Only)

Bug ID	Headline
CSCwo44709	cdFMC multiple protected networks with NAT exempt enabled, NAT exempt CLIs are not getting generated

Table last updated: 2025-08-28

Table 18: Resolved Functional Bugs in Version 7.7.0-89 (All Platforms)

Bug ID	Headline
CSCvi60913	FTD deployment failing due to "address-pool in use"
CSCvj85665	ENH: Appliance hostname or ip address should be included in FX-OS syslogs
CSCvn25053	FMC: critical processes can not boot up including vmsDBEngine
CSCvx44261	SNMPv3: Special characters used in FXOS SNMPv3 configuration causes authentication errors
CSCvx69675	FXOS Major Faults about adapter host and virtual interface being down
CSCvx74133	App-instance showing as Started instead of Online
CSCvz03407	IPTables.conf file is disappearing resulting in backup and restore failure.
CSCvz07712	Deployment fails with internal_errors - Cannot get fresh id
CSCvz59859	FXOS fault F1758 description should not be specific to subinterfaces
CSCvz70310	ASA may fail to create NAT rule for SNMP with: "error NAT unable to reserve ports."
CSCvz85153	show access-control-config doesn't show NAP/IPS policy name
CSCwb44245	SNORT3: proxy traffic issue on port 80 when tls1.3 inspection enabled
CSCwb67073	FMC - Unable to copy/cut/paste NAT rule

Bug ID	Headline
CSCwb77894	Firepower 1000/2100 may boot to ROMMON mode
CSCwb95850	Snort down due to missing lua files because of disabled application detectors (PM side)
CSCwc28374	Search Feature of Large Access Control Policy Not Able to Find Searched-For Values
CSCwc76419	Unnecessary FAN error logs needs to be removed from thermal file
CSCwd08098	cacert.pem on FMC expired and all the devices showing as disabled.
CSCwd08448	FMC to provide health alert 60 days prior to cacert.pem certificate expiry
CSCwd39442	ssl policy errors: Unable to get server certificate's internal cached status
CSCwd55642	Stale CPU core health events seen on FMC UI post upgrade to 7.0.0+.
CSCwd60102	ASA: Delay in new chunk memory allocation when the firewall process a high number of new connections
CSCwd61082	FMC UI Showing inaccurate data in S2S VPN Monitoring page
CSCwd67100	ASA traceback and reload on Datapath process
CSCwd78915	Deployment keep failing due to Config Error -- service-policy policy_map
CSCwd81123	High CPU Utilization on FXOS for processes smConlogger
CSCwd86472	Wrong extranet device name and type showing in S2SVPN listing page
CSCwd99592	Optimization of Side Bar loading for HealthMon page
CSCwe02012	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe13781	IKEv2 Multi-DVTI Hub Support FTD/ASA
CSCwe18462	ASA/FTD: Improve GTP Inspection Logging
CSCwe18467	ASA/FTD: GTP Inspection engine serviceability
CSCwe21884	Write wrapper around "kill" command to log who is calling it
CSCwe22431	[SXP-UserIP Muted Leader]FMC HA Join flushes FW IP_SGT Mapping and restreams in registered sensors.
CSCwe42986	Classic and Unified Events should handle cases when SMC is unreachable
CSCwe63686	Upgrade readiness failed in WM FDM @009_check_snort_preproc.sh but upgrade to 7.3.1-19 passed
CSCwe78474	FPR4100/9300 displays the package-vers as 0.0 after successful firmware upgrade to version 1.0.19

Bug ID	Headline
CSCwe78674	User Group Download fetches less data than available or fails with "Size limit exceeded" error
CSCwe85156	FTD: 10Gbps/full interfaces changed to 1Gbps/Auto after upgrade and going to down state
CSCwe87831	FMC UI response is very slow: Add health module monitoring FMC ntpd server(s) accessibility
CSCwe88492	Banner login does not display when configured
CSCwe89256	Firepower Chassis Manager is not accessible with ECDSA certificates
CSCwe92324	FPR31xx - SNMP poll reports incorrect FanTray Status at Down while actually operational
CSCwe93925	Deployment fails to FTD when reusing/reassigning existing vlan id to diff interface
CSCwe95462	Health monitoring cores due to health alerts with more than 8 fields
CSCwf04460	The fxos directory disappears after cancelling show tech fprm detail command with Ctr+c is executed.
CSCwf06318	Readiness check needs to be allowed to run without pausing FMC HA
CSCwf10494	If the user navigate to Packet Tracer from Device Mgmt page, the selected device is incorrect
CSCwf13674	Deployments can cause certain RAVPN users mapping to get removed.
CSCwf14031	Snort down due to missing lua files because of disabled application detectors (VDB side)
CSCwf14411	getting wrong destination zone on traffic causing traffic to match wrong AC rule
CSCwf17314	FMC deploy logs rotating faster because of /internal_rest_api/accesscontrol/rapplicationsavailable
CSCwf21204	DBCheck shouldn't run against MonetDB if user is collecting config backup alone
CSCwf21640	Correlation rule 'Security Intelligence Category' option is missing DNS and URL values
CSCwf25454	Stale anyconnect entries causing issues with routing
CSCwf26599	Error loading data in NAT page - When unused port object is used
CSCwf27458	AC policy change is not reflected in instance page on edit
CSCwf27687	Snort3 TCP flow cache entry growth caused by embryonic connection mismanagement
CSCwf30824	Add CIMC reset as auto-recovery for CIMC IPMI hung issues
CSCwf31050	High CPU usage on multiple appliances incorrectly seen on FMC

Bug ID	Headline
CSCwf35346	FMC should handle error appropriately when ISE reports error during SXP download
CSCwf35500	FXOS/SSP: System should provide better visibility of DIMM Correctable error events
CSCwf39108	Firewall rings may get stuck and cause packet loss when asp load-balance per-packet auto is used
CSCwf57856	FXOS Traceback and reload caused by leak on MTS buffer queue
CSCwf59529	Identity Policy Active auth snort3 redirect hostname doesn't list all FQDN objects
CSCwf64429	Unable to upload FTD version image to FCM
CSCwf66307	The exclude policy to exclude interface status will be removed on FMC after a while
CSCwf66333	Selecting "All interfaces " under FTD exclude policy for interface status module doesn't work
CSCwf66345	[API] Searching for objects inside groups does not filter in rule editor window
CSCwf66818	FMC VPN Monitoring Dashboard incorrectly shows Standby FTD as VPN Session owner in HA pair
CSCwf70275	FTD: TLS Server Identity does not work if size of client hello more than TCP MSS bytes
CSCwf75694	ASA - The GTP inspection dropped the message 'Delete PDP Context Response' due to an invalid TEID=0
CSCwf77994	False critical high CPU alerts for FTD device system cores running instantaneous high usage
CSCwf78497	EIGRP flexconfig migration 7.2.0, no CLIs should not be migrated if they are not the default config
CSCwf79372	after HA break, selected list shows both the devices when 1 device selected for upgrade
CSCwf82447	Editing identity nat rule disables "perform route lookup" silently
CSCwf84200	Snort core while running IP Flow Statistics
CSCwf84318	ASA/FTD traceback and reload on thread DATAPATH
CSCwf86557	Decrypting engine/ssl connections hang with PKI Interface Error seen
CSCwf92371	HA secondary unit disabled after reboot - Process Manager failed to secure LSP
CSCwf92726	Some Vault secrets including LDAP missing files after upgrade if the Vault token is corrupted
CSCwf99303	Management UI presents self-signed cert rather than custom CA signed one after upgrade
CSCwh03373	Do not enable TLS Server Identity Discovery on FTDv deployed with GWLB

Bug ID	Headline
CSCwh04468	Connection events sent to Syslog Server has "unknown" syslog facility
CSCwh06762	FMC-HA page should show LSP version mismatch details.
CSCwh09113	FPR1010 in HA failed to send or receive to GARP/ARP with error "edsa_rcv: out_drop"
CSCwh11411	Snort blacklisting traffic during deployment
CSCwh11508	FMC should not allow to create faulty snort3 rules with unknown characters
CSCwh12120	Incorrect exit interface choose for VTI traffic next-hop
CSCwh15636	ARP learning issues with Multiple-instance running 100G Netmod
CSCwh17052	Lack of validation of string length creating object/category names using API
CSCwh17965	[Display]FXOS: PC member interface is shown as down & unassociated/unassigned after reload
CSCwh18967	Include "show env tech" in FXOS FPRM troubleshoot
CSCwh19475	Intermittently flow is getting white-listed by the snort for the unknow app-id traffic.
CSCwh22888	FXOS: Remove enforcement of blades going into degraded state after multiple DIMM correctable errors
CSCwh24321	FXOS: Alperton 100G NetMod not being acknowledged properly
CSCwh24932	ASA software on FP3110 showing incorrect serial number in show inventory output
CSCwh25406	Snort3 core while running continuous traffic IMS 7.4.1-73
CSCwh27886	Chassis Manager shows HTTP 500 Internal Server error in specific cases
CSCwh29131	FMC Policy Analysis - Broken Redudancy Logic Check
CSCwh30257	snort3 crashes observed due to memory corruption in file api
CSCwh31502	Enhancement for Lina copy operation for startup-config to backup-config.cfg in HA
CSCwh34344	FTD not generating end of connection event after "Deleting Firewall session"
CSCwh34836	Getting an exception on the UI while editing and saving the intrusion policy
CSCwh36005	Policy deployment failed due to "1 errors seen during populateGlobalSnapshot"
CSCwh37655	Snort2:Skip writing malware seed file duing process shutdown
CSCwh41606	Extensive logging for a problematic deployment caused logs to rollover important logs
CSCwh41925	Lina traceback in ZMQ Proxy caused service loss.
CSCwh42077	Cisco_Firepower_GEODB_FMC_Update* are not included in diskmanager

Bug ID	Headline
CSCwh42142	Policy apply stuck because of NTP time issues (previous deploy done in future timestamp)
CSCwh43230	Strong Encryption license is not getting applied to ASA firewalls in HA.
CSCwh43945	FTD/ASA traceback and reload may occur when ssl packet debugs are enabled
CSCwh46732	Remote Desktop (RDP) traffic fails with TSID enabled
CSCwh50221	4200 Series: Portchannel in cluster may stay down sometimes when LACP is in active mode
CSCwh50291	Checkbox of Enable autogeneration of MAC addresses not working properly
CSCwh51438	Add support for 10G-T-X module
CSCwh51872	Message asa_log_client exited 1 time(s) seen multiple times
CSCwh52526	FMC SSO timesout when user session is active for more than 1 hr (idle timeout)
CSCwh53745	ASA: unexpected logs for initiating inbound connection for DNS query response
CSCwh54029	FMC HA : Redundant FTD registration task failing on secondary FMC when FTD is disconnected.
CSCwh54477	The FMC is showing "The password encryption key has not been set" alert for a 11xx/21xx/31xx device
CSCwh55178	Handle mem leak in callhome test command
CSCwh56183	FTD 4115 in HA crashing due to CLI-XML-SERVER issue
CSCwh57976	Improve CPU utilization in ssl inspection for supported signature algorithm handling
CSCwh58190	FMC Deployment failure in csm_snapshot_error
CSCwh58490	FMC Deployment failed due to internal errors after upgrade
CSCwh59222	SNORT3 - FTD - TSID high cpu, daq polling when ssl enabled is not pulling enough packets
CSCwh60971	NAT pool is not working properly despite is not reaching the 32k object ID limit.
CSCwh68068	Firepower WCCP router-id changes randomly when VRFs are configured
CSCwh68878	Diskmanager process terminated unexpectedly
CSCwh69815	FTDvs through put got changed to 100Kbps after upgrade
CSCwh69843	WM DT - ASA in transparent mode doesn't send equal IPv6 Router Advertisement packets to all nodes
CSCwh71008	CSF 4200: PSU Fan speed is critical

Bug ID	Headline
CSCwh71050	FXOS : Duplication of NTP entry results in Error message : Unreachable Or Invalid Ntp Server
CSCwh71161	ASA|FTD: Traceback & reload in thread Name: update_mem_reference
CSCwh72370	FTD: Mariadb might cause OOM due to not-so-effective memory release algorithm in glibc allocator
CSCwh74219	Upgrade from FMC 7.2.4.1 to 7.2.5 failed at 600_schema/000_install_fmc.sh
CSCwh74870	Unexpected high values for DAQ outstanding counter
CSCwh75829	FMC Primary disk degraded error
CSCwh78064	FTD: The crucial upgrade script should not be bypassed by the Upgrade Retry
CSCwh81366	[Multi-Instance] Second Hard Drive (FPR-MSP-SSD) not in use
CSCwh82305	Lina core at swapcontext on Standby FTD during policy deployment
CSCwh82766	Bulk FTD backups to be generated in batches internally
CSCwh83021	ASA/FTD HA pair EIGRP routes getting flushed after failover
CSCwh83301	High CPU Utilization alerts caused by the process Telegraf
CSCwh83328	SNMP fails to poll accurate hostname from FMC
CSCwh83854	Cannot configure Correlation rule because there are no values for GID that exceed 2000
CSCwh84610	Disconnecting RA VPN users from the FMC gui fails.
CSCwh84647	Backup restore: silent failure when the device managed locally
CSCwh84833	Every HA sync attempts to disable URL filtering if already disabled.
CSCwh85824	eStreamer JSON parse error and memory leak
CSCwh87058	FTD: Internal certificate generation results to certificate and private key mismatch
CSCwh90813	FDM Upgrade failure due to expired certificates.
CSCwh91419	FTD installation fails on FPR-2K "Error in App Instance FTD. Available memory not updated by blade"
CSCwh91976	WA MI: Traps(linkup/down) from chassis is not seen on NMS even if unification is enabled
CSCwh92345	crypto_archive file generated after the software upgrade.
CSCwh92541	Random FTD snort3 traceback
CSCwh95003	Init process spikes to 100% CPU usage after a failed backup

Bug ID	Headline
CSCwh95025	GTP connections, under certain circumstances do not get cleared on issuing clear conn.
CSCwh95443	Datapath hogs causing clustering units to get kicked out of the cluster
CSCwh96055	Management DNS Servers may be unreacheable if data interface is used as the gateway
CSCwh99398	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-34-17852'
CSCwi01323	SNMP OID ifOutDiscards on MIO are always zero despite show interface are non-zero
CSCwi01895	Connection drops during file transfers due to HeartBeat failures
CSCwi01981	Thirty-day automatic upgrade revert-info deletion is not resilient to communication failures
CSCwi02039	FMC clean_revert_backup script fails silently without creating any logs
CSCwi02599	SSX Eventing continues to go to old tenant upon FTD migration to CDO.
CSCwi02754	FTD 1120 Traceback and reload on standby unit with SNMP enabled.
CSCwi03407	Traceback on FP2140 without any trigger point.
CSCwi03494	S2S tunnels shown inactive on FMC dashboard though tunnels are up on FTD due to out-of-order events
CSCwi04021	Daily Change Reconciliation Report Randomly Generating Reports with the same time periods
CSCwi04351	FTD upgrade failling on script 999_finish/999_zz_install_bundle.sh
CSCwi05618	FTD HA sync failure due to "CD App Sync error is Failed to apply SSP config on standby"
CSCwi06797	ASA/FTD traceback and reload on thread DATAPATH
CSCwi07068	SFDataCorrelator logs "Killing MySQL connection" every minute, causing performance problems
CSCwi08374	FMC backup fails with "Registration Blocking" failure caused by DCCSM issues
CSCwi13134	Hardware bypass not working as expected in FP3140
CSCwi13223	Source of the VTI interface is getting empty
CSCwi14132	FMC/cdFMC increase API rate limit
CSCwi14896	Node kicked out of cluster while enabling or disabling rule profiling
CSCwi16034	FMC does not generate email health notifications for Database Integrity Check failures.
CSCwi16571	Capture-traffic Clish command with snort3 not producing a proper resulting capture
CSCwi18663	FMC-4600: Pre-Filter policy is showing as none

Bug ID	Headline
CSCwi19485	Fail open snort-down is off in inline pairs despite it being enabled and deployed from FMC
CSCwi21909	FMC: Displaying "missing en-US:BGP" via Deployment Preview when BGP Changes have been Reverted
CSCwi24368	Standby manager addition is failed on Primary FMC due to previous entries in table
CSCwi24370	Stale HA transactions need to be moved to failed and subsequent HA transaction needs to be created
CSCwi24461	Device/port-channel goes down with a core generated for portmanager
CSCwi24814	In FIPS mode, External auth with TLS config enabled, CLI logins are not working (FMC & FTDs)
CSCwi26712	Deployment failed due to missing AnyConnect Profile File
CSCwi27093	FMC error out Invalid IPv4 Network or Host literal from the group while Adding a network in the ACP
CSCwi27402	FTD: Update WM firmware to 1023.0207
CSCwi28645	User assigned to a read only custom role is not able to view content of intrusion policy for snort2
CSCwi29041	Log spam in /var/log/messages: Out of range value for column 'map_id'
CSCwi29538	EIGRP migration failed using 'FlexConfig Policies' script failed generating database corruption
CSCwi30843	Error Fetching Data in Exclude Policy Page when non permanent exclude periods are selected
CSCwi31008	Deployment stuck on FMC when device goes down during deploy and doesn't boot up
CSCwi31480	Alert: Decommission failed, reason: Internal error is not cleared from FCM or CLI after acknowledge
CSCwi31558	File-extracts.logs are not recognised by the diskmanager leading to high disk space
CSCwi31966	FTD ADI debugs may show incorrect server_group and/or realm_id for SAML-authenticated sessions
CSCwi33956	"boot config" is not working after reload on FPR1140
CSCwi34719	Unable to SSH into FTD device using External authentication with Radius
CSCwi34730	tls website decryption breaks with ERR_HTTP2_PROTOCOL_ERROR
CSCwi36311	use kill tree function in SMA instead of SIGTERM

Bug ID	Headline
CSCwi36843	Detailed logging related to reason behind sub-interface admin state change during operations
CSCwi38061	ASA/FTD traceback and reload due to file descriptor limit being exceeded
CSCwi38425	Health Monitor Alerts set in Global are not sending alert from devices assigned in leaf domain
CSCwi38440	Hostnames are replaced with IP addresses in alert email content
CSCwi38449	Module name displayed in the alert got changed and it is differ from the one set in FMC
CSCwi38662	FTD HA should not be created partially on FMC
CSCwi38708	FDM deployment failure
CSCwi38957	Policy Apply failed moving from FDM to FMC
CSCwi40193	Hairpinning of DCE/RPC/FTP traffic during the suboptimal lookup
CSCwi40302	Deployment fails on new AWS FTDv device with "no username admin"
CSCwi40487	FTD HA Failure after SNORT crash.
CSCwi40674	Umbrella Profile and others cleared incorrectly when editing group policy in the UI
CSCwi41666	MonetDB startup enhancement to clean up large files
CSCwi42962	installing GeoDB country code package update to FMC does not automatically push updates to FTDs
CSCwi43240	Deployment fails if Network Discovery policy reference is missing from FMC Database
CSCwi43492	ASA traceback and reload on Thread Name: DATAPATH
CSCwi44007	FMC Validation failure for large object range and success for object network in NAT64
CSCwi44148	Incorrect health monitor alerts for ISE-PIC connectivity
CSCwi44208	low memory/stress causing traceback in SNMP
CSCwi44912	ISA3000 Traceback and reload boot loop
CSCwi44953	We should be skipping sru_install during for Minor patch upgrades and install only on required basis
CSCwi45054	FMC Deployment preview shows different information before and after FTD deploy
CSCwi45408	Monetdb having 14GB of unknown BAT data causing "High unmanaged disk usage on /Volume"
CSCwi45878	ASA/FTD: DNS Load Balancing with SAML does not work with VPN Load Balancing

Bug ID	Headline
CSCwi46641	FTDv may traceback and reload in Thread Name 'PTHREAD-3744' when changing interface status
CSCwi46676	API:/operational/commands not working as swagger indicate
CSCwi47029	"Update file is corrupted" for "Download Latest Cisco Firepower Geolocation Database Update." in FMC
CSCwi48699	ASA traceback and reload on Thread Name: pix_flash_config_thread
CSCwi49770	ASA|FTD Traceback & reload in thread name Datapath
CSCwi49797	Event Searching with Objects and Networks Leads to only showing events matching Objects
CSCwi49829	Threat Defense Service Policy - Reset Connection Upon Timeout not working
CSCwi49884	TCP MSS is changed back to the default value when a VTI or loopback interface is created
CSCwi51611	FTD 7.4.1 Snort shows 100% utilization even at a low traffic rate
CSCwi51941	Unattended mode FTD upgrade from 741 to 76 fails if upgrade pkg is already copied over to devices
CSCwi52008	Snort3 traceback and restarts with race conditions
CSCwi52623	Misleading Certificate Attribute Checking Under DAP Endpoint Criteria
CSCwi53949	Snort3 traceback in TcpReassembler::scan_data_post_ack
CSCwi53987	SSL protocol settings does not modify the FDM GUI certificate configuration or disable TLSv1.1
CSCwi54171	Decryption policy page is empty if user that modified/created policy was deleted.
CSCwi55009	Error thrown if Security Analytics user tries to access Packet Capture page
CSCwi55842	7.4 - If policy save in progress deploy might indicate failure for only few devices
CSCwi56667	ASA Traceback and reload on Thread Name "fover_parse" on Standby after Failover Group changes
CSCwi56733	Internal error when attempting to configure PBR in FMC
CSCwi57476	interface idb logging log rotation to FXOS logrotate utility
CSCwi57670	RAVPN SAML: External browser gives misleading message when FTD/ASA fails to parse assertion
CSCwi58187	Incorrect NAT warnings threshold limit of 131838 IPs
CSCwi59453	Bootstrap after upgrade failed - Resume HA with reason deployment already exists

Bug ID	Headline
CSCwi59871	High disk usage caused by large write-ahead log in eventdb
CSCwi59969	ZTNA: FMC pushes incorrect sp-acs-url parameter - "?" encoded as 0x3F
CSCwi60151	ZTNA: FMC doesn't accept IdP with local domain
CSCwi60285	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi61135	Debugs failed to be enabled on SSH session
CSCwi62796	ASA/FTD Traceback and reload related to SSL/DTLS traffic processing
CSCwi62985	SFDataCorrelator timeout thread deadlock detection core on busy FMC
CSCwi63057	Threat Defense Upgrade wizard might incorrectly show clusters/HAs as disabled
CSCwi63743	ASA/FTD may traceback and reload in Thread Name "appAgent_monitor_nd_thread" & Rip: _lina_assert.
CSCwi64772	Geodb installation notification is stuck or some tasks wont create a notification in UMS
CSCwi64829	traceback and reload around function HA
CSCwi65116	DHCPv6:ASA traceback on Thread Name: DHCPv6 CLIENT.
CSCwi66461	WARN msg(speed not compatible, suspended) while creating port-channel on Victoria CE
CSCwi66570	The report doesn't include "Default Variables" information after change "Variable Sets" name
CSCwi66676	ASA/FTD may traceback and reload in Thread Name 'webvpn_task'
CSCwi67291	Unable to view any events (Connection/Malware/etc) on the FMC Post FMC Upgrade to 7.6
CSCwi67510	FMC: Packet-tracer showing a "Interface not supported" error for VLAN interfaces
CSCwi67629	Devices might change status to "missing the upgrade package" after Readiness Check is initiated
CSCwi67638	FMC configured DAP rule with Azure IDP SAML attributes does not match
CSCwi67998	Policy deployment failures on TPK MI chassis after redeploying same instance
CSCwi68320	During FMC hardware migration failure encountered due to missing prometheus directories
CSCwi68604	Error logs generated for ssh access to ASA when eddsa is used as kex hostkey
CSCwi68625	Continuous snmpd restarts observed if SNMP host is configured before the IP is configured

Bug ID	Headline
CSCwi68833	ASA/FTD: Memory leak caused by Failover not freeing dnscrypt key cache due to unsyned umbrella flow
CSCwi68970	Creating DAP policy with underscore "_" is not visible as applied to Remote Access VPN policy
CSCwi69091	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi69260	upgrade of FMC to 7.2.x removes FlexConfig-provided EIGRP authentication from interfaces on FTDs
CSCwi70492	Firewall is in App Sync error in pseudo-standby mode and uses IPs from Active unit
CSCwi70940	standard error (stderr) not inserted into restore.log when restoring FMC backups
CSCwi71076	Device listing taking long due to FTD_HA REST-API delay - Can be seen in loading HealthMon page.
CSCwi71786	Download failed for Available Upgrade Packages
CSCwi71998	"Stream: TCP normalization error in NO_TIMESTAMP" is seen when SSL Policy decrypt all is used
CSCwi72054	Unable to delete custom DNS Server Group Object post upgrade 7.2.x
CSCwi72158	Devices in HA pair shows as standalone in Threat Defense Upgrade page
CSCwi72294	FTD: Improve or optimize LSP package verification logic to run it faster
CSCwi72410	Member interface admin status is not updated on Lina after enabling port-channel interface
CSCwi74214	ASA/FTD traceback and reload in Thread Name: IKEv2 Daemon when moving from active to standby HA
CSCwi75111	Configuring MTU value via CLI does not apply
CSCwi75198	Standby FTD experiencing periodic traceback and reload
CSCwi76002	Memory exhaustion due to absence of freeing up mechanism for tmatch
CSCwi76361	Transparent firewall MAC filter does not capture frames with STP-UplinkFast dst MAC consistently
CSCwi76642	FXOS capture in Container mode behaves erratically
CSCwi78064	CloudAgent Smart Agent Exception - The Smart Agent Manager requires NTP to be running on FDM
CSCwi78941	FDM deployment fails with error "Some interfaces have been added to or removed from the device"
CSCwi79037	IKEv2 client services is not getting enabled - XML profile is not downloaded

Bug ID	Headline
CSCwi79042	FTD/Lina traceback and reload of HA pairs, in data path, after adding NAT policy
CSCwi79120	some ssh sessions not timing out, leading to ssh and console unable to connect to the FXOS CLI
CSCwi79289	FMC: Add logging for PM functions
CSCwi79393	Policy Deployment Fails when removing the Umbrella DNS Policy from Security Intelligence
CSCwi79538	FMC API Call for Network Object Overrides Returns Different Results for Active vs Standby FW
CSCwi79703	Incorrect Timezone Format on FTD When Configured via FXOS
CSCwi80979	Snort stripping packet information and injects its packet with 0 bytes data
CSCwi81771	Unable to send unknown file disposition to ThreatGrid due to mem cache issue
CSCwi82866	MonetDB Monitor triggers for restarting MonetDB based on WAL size are not effective
CSCwi83185	FMC deployment failure due to incorrect error message type sent to FMC
CSCwi83890	Report file generated for AC policy is empty
CSCwi84314	ASA CLI hangs with 'show run' on multiple SSH
CSCwi84417	Traffic incorrectly matches an ALLOW rule with a time-range object after time has expired
CSCwi84615	some stdout logs not rotated by logrotate
CSCwi85277	Upgrade Failed with error "Upgrade failed because of undeployed changes present on the device"
CSCwi85628	Deployment failure due to Rsync-chunk-checksum slowness
CSCwi85689	TLS Server Identify: 'show asp table socket' output shows multiple TLS_TRK entries
CSCwi86007	Modify UUID during license communication to avoid disrupting customer's licenses
CSCwi86036	External Radius authentication fails post upgrade if radius key includes special characters
CSCwi86187	VTI tunnel showing incorrect port-channel association info in VPN Monitoring page
CSCwi86198	SFData correlator keep terminating on FTDs configured for IDS
CSCwi87382	Traceback and reload on Primary unit while running debugs over the SSH session
CSCwi89167	Automatic VDB/SRU Download Fails Due to Simultaneous Signature Validation
CSCwi89447	Every realm sync indicates an access control policy change

Bug ID	Headline
CSCwi90371	ASA:request to add "logging list" option to the "logging history" command.
CSCwi90399	FTD/ASA system clock resets to year 2023
CSCwi90571	Access to website via Clientless SSL VPN Fails
CSCwi90607	Unable to login to FDM GUI using external user account via RADIUS
CSCwi90751	FTD/ASA - SNMP queries using snmpwalk are not displaying all "nameif" interfaces
CSCwi90998	ASA SNMP Polling Failure for environmental FXOS DME MIB (.1.3.6.1.4.1.9.9.826.2)
CSCwi91166	Need to add reasons for blocks in stream
CSCwi91384	Migration of S2S from ASA to FMC across domains
CSCwi91588	Heap-use-after-free in Discovery Filter on Snort shutdown
CSCwi91602	Deployment doesn't timeout as notification (but not started), runs for hours after LSP install
CSCwi92702	Run All function on FMC Health Monitoring page is greyed out after upgrade
CSCwi94356	Lina traceback and reload in Thread Name: cli_xml_request_process
CSCwi95228	"crypto ikev2 limit queue sa_init" resets after reboot
CSCwi95639	ASA/FTD Optimise Fail-to-Wire (FTW) modules trigger in Reload/Crash scenarios
CSCwi95690	Fault "Adapter 1/x/y is unreachable" due to connectivity failure between supervisor and VIC adapter
CSCwi95708	FTD: Hostname Missing from Syslog Message
CSCwi95796	FTD SNMP OID 1.3.6.1.4.1.9.9.109.1.1.1.1.7 always returns 0% for SysProc Average
CSCwi95871	SSH/SNMP connections to non-admin contexts fail after software upgrade
CSCwi95994	Chromium-based browsers have SSL connection conflicts when FIPS CC is enabled on the firewall.
CSCwi97667	FMC HA sync status shows failed during VDB/SRU installation on Active and standby FMC
CSCwi97836	ASA traceback and reload after configuring capture on nlp_int_tap and deleting context
CSCwi97839	FTD traceback assert in vni_idb_get_mode and reloaded
CSCwi97948	EIGRP bandwidth is changing after upgrade or after "shutdown"/"no shutdown" commands
CSCwi98147	Tomcat restarts in the middle of the LTP flow due to certificate update
CSCwi98704	ActionQueueScra invoked oom-killer

Bug ID	Headline
CSCwi99429	Policy deployment failure rollback didnt reconfigure the FTD devices
CSCwj00027	Backup failure message doesn't help the user
CSCwj00659	FMC: Multiple Email address in Email Alert not working
CSCwj00956	Snort process spamming syslog-ng messages causing syslog-ng termination
CSCwj01197	VMXNET3 driver is not getting loaded automatically on the bootup for FMCv300
CSCwj01346	logging list MANAGER_VPN_EVENT_LIST getting removed and re-applied for every deployment
CSCwj01569	Policy deployment failure in standalone FDM due to an interface error
CSCwj01785	Network Risk Report on FMC lacks option to select data source, could cause report generation to fail
CSCwj02259	Backup failures needs to be displayed with the correct state on GUI
CSCwj02505	ASA Checkheaps traceback while entering same engineID twice
CSCwj02708	Backup generation on FDM fails with the error "Unable to backup Legacy data."
CSCwj03112	pmtool restart of monetdb fails to bring up monetdb, too many files in monetdb Volume directory
CSCwj03253	SFDataCorrelator creates huge numbers of to_import files when MonetDB table partition creation fails
CSCwj03285	FMC : Health Monitor Alert is not properly issued regarding disk usage
CSCwj03764	In Spoke dual ISP case if ISP2 is down, VTI tunnels related to ISP1 flapping.
CSCwj03876	Deleting Snort 3 IPS Rule doesn't Generate Audit Log
CSCwj03937	ENH: FTD Add debug message to indicate "No CRL found in User identity Certificate"
CSCwj04154	FTD management interface DHCP server may fail to start causing connectivity issues or showing faults
CSCwj05151	ASA/FTD may traceback and reload in Thread Name DATAPATH due to GTP Spin Lock Assertion
CSCwj05464	FMC Server Certificate shows Only First 20 Objects
CSCwj05484	ASA upgrade from 9.16 to 9.18 causing change in AAA ldap attribute values by adding extra slash '\'
CSCwj07837	Deployment failure due to exceeding logging event list name size
CSCwj08015	FTW no longer working in NM3 on Warwick
CSCwj08203	FMC: fireamp generating too many logs

Bug ID	Headline
CSCwj08302	FTD: HostScan scanning results not processed in version 7.4.1
CSCwj08980	ICMP replies randomly does not reaching the sender node when initiated from the node.
CSCwj09874	Tomcat and Apache maxHeader size should be increased to avoid 413 errors on some FMC pages
CSCwj09938	Unable to remove suppression from snort3 rule once added
CSCwj09999	FP 3100 MTU change on management interface is NOT persistent across reboots (returns to default MTU)
CSCwj10451	The secondary device reloaded while rebooting the primary device.
CSCwj10923	FTD - sftunnel unstable connectivity issues when control and event are configured in same subnet
CSCwj11331	Web Contents files appear as text/plain when they should be application/octet-stream
CSCwj12168	Never expiring machine user not logged out at various places
CSCwj13910	Crypto IPSEC SA Output Showing NO SA ERROR With IPSEC Offload Enabled
CSCwj14242	Applications are incorrectly identified as TOR and blocked by Snort3
CSCwj14589	FMC-SSE Cloud Configuration SSE Enrollment Failure alert due to empty connector.toml file on the FTD
CSCwj14798	TSS_Daemon process is exiting every minute
CSCwj14832	SAML: Single sign-on AnyConnect token verification failure is seen after successful authentication
CSCwj14927	FTD: Primary takes active role after reloading
CSCwj15125	ASA/FTD may traceback and reload in Thread Name 'lina' related to Netflow timer infra
CSCwj15382	Deploy doesnt show up on FMC upon merging unmerged diagnostic on FTD-HA
CSCwj16279	username containing '@' character works for asa login but fails for 'connect fxos'
CSCwj16521	Policy stuck in loading state on FMC UI
CSCwj17213	Change in Application Client Type attribute
CSCwj17447	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-6-26174'
CSCwj17677	PM restart needs to be blocked or warned the user that it may go for reboot
CSCwj17852	FMC - Inheritance Settings Select Base Policy Menu disappears while scrolling using Light or Dusk UI

Bug ID	Headline
CSCwj17969	rna_ip_os_map can grow very large that causes SFDataCorrelator to stop processing events
CSCwj19252	Object optimisation gets disabled on FMC if next deployment is after two hours
CSCwj19653	FTD - Trace back and reload due to NAT involving fqdn objects
CSCwj20067	ASA: Warning messages not displayed when Static interface NAT are configured
CSCwj20118	FTDv reloads and generate backtrace after push EIGRP config
CSCwj21880	FTD with Interface object optimization enabled is blocking traffic after renaming of zone names
CSCwj21985	Debug: Eth1/1 flapping unexpectedly
CSCwj22086	Active unit goes to disabled state when there is a mismatch in firewall mode
CSCwj22235	Lina traceback and reload due to mps_hash_memory pointing to null hash table
CSCwj22935	Snort version mismatch between FTD HA peers resulted from a reboot during a snort toggled deployment
CSCwj22990	After upgrading the ASA, “Slot 1: ATA Compact Flash memory” shows a ditterent value
CSCwj24517	LSP Deployment fails in multi instance FP 41xx / 93xx
CSCwj25629	Error when running 'show tech-support module detail' on FPR9K
CSCwj25975	FTD/ASA : CSR generation with comma between “Company Name” attribute does not work expected
CSCwj26204	restored FMC backup devices display as "normal" and "healthy" although without connection with FMC
CSCwj26595	FMC allows loading a binary certificate in the External Authentication Object
CSCwj26627	FMC shows a non-User-Friendly Error during a Policy Deployment failure due to snapshot failure
CSCwj27112	Rest API '/devices/devicerecords' is returning mismatch of values for (RA VPN) policy object id
CSCwj28049	Identity Mapping Filter field gets updated with newly created network objects.
CSCwj28437	Snort3: TCP traffic failure after upgrade due to large invalid sequence numbers and invalid ACKs
CSCwj28468	Validation required incorrect CLI Access Users in External Auth
CSCwj29599	Victoria CP might list all on-board interfaces as L3 mode after base-install
CSCwj30825	SFDataCorrelator memory leak after unregistering an active device

Bug ID	Headline
CSCwj30962	3140 3 MI instances upgrade failed
CSCwj30980	Addition of debugs & a show command to capture the ID usage in the CTS SXP flow.
CSCwj31382	Wrong IP address on FMC audit logs
CSCwj31475	F1758 FXOS Fault Observed in ASA Appliances Following FXOS Upgrade
CSCwj31816	TLS Secure Client sessions cannot be established on FTD Due to RSA-PSS Signing Algorithm
CSCwj31904	After upgrade FDM deployment fails "Timeout waiting for snort detection engines to process traffic"
CSCwj31918	Segmentation fault with "logger_msg_dispatch" while HA sync
CSCwj32035	Clientless VPN users are unable to reach pages with HTTP Basic Authentication
CSCwj32823	"strong-encryption-disable" pushed from FMC without any change after FMC upgrade
CSCwj33129	VPN config isn't getting sync to leaf domain, when FTD moved to leaf domain
CSCwj33487	ASA/FTD may traceback and reload while handling DTLS traffic
CSCwj33580	IKEv2 tunnels flap due to fragmentation and throttling caused by multiple ciphers/proposal
CSCwj33891	ASA/FTD Cluster memory exhaustion caused by NAT process during release of port blocks allocations
CSCwj34204	Disk quota for the corefile should be revisited based on platform
CSCwj34235	Snort3 core in FTD stateful signature evaluation
CSCwj34374	SecureX / Cisco Security Cloud registration fails if FMC is behind a proxy server
CSCwj34881	Command to show counters for access-policy filtered with a source IP address gives incorrect result
CSCwj34975	Multiple context interfaces fail to pass traffic
CSCwj35701	Dns-guard prematurely closing conn due to timing condition
CSCwj35902	URL Filtering and Cisco-Intelligence-Feed Download Failure
CSCwj38871	ASA traceback with thread name SSH
CSCwj38928	High latency observed on FPR31xx
CSCwj39107	SFDataCorrelator memory growth when pruning a huge number of old service identities
CSCwj39184	FDM /ngfw/var/sf/fwcfg/zones.conf is empty for 7.3.1

Bug ID	Headline
CSCwj39212	SFDataCorrelator memory growth when processing a huge number of expired user identities
CSCwj39296	FTD compliance mode not accurately shown on FMC for newly registered FTDs
CSCwj40124	FMC 7.3 Deployment failed due to OOM in PBR Configuration
CSCwj40597	FTD: Backups fail on Multi-Instance or standalone with error "Backup died unexpectedly"
CSCwj40665	Additional memory tracking in SFDataCorrelator
CSCwj40761	ASA/FTD may traceback in Threadname: **CTM KC FPGA stats handler**
CSCwj41427	FTD-HA creation is failing because FMC takes longer time to save overrides.
CSCwj41916	FTD-HA upgrade fails to start - Configuration is out of sync between active and standby
CSCwj42875	FMC HM showing "normal" eventhough FTD having Comm Failure
CSCwj43069	IPv6 rule with manual address entry FMC with ::/0 is not working as expected.
CSCwj43345	SNMP poll for some OIDs may cause CPU hogs and high latency can be observed for ICMP packets
CSCwj43902	FTDv - The interface connected to the AWS GW may have connection issues for DHCP or an idle state.
CSCwj44398	when set the route-map in route RIP on FTD, routes update is not working after FTD reload
CSCwj44464	ACP rule may not get applied post-deployment/Deployment failure due to FXOS-FTD timezone mismatch
CSCwj45351	Unable to add additional LDAP attribue maps on upgraded FMC
CSCwj45439	Internal Certificate Import Error : Failed to validate Cert Based EO: Unsupported Key Type
CSCwj48308	Stale Health Alerts seen on the UMS after model migration
CSCwj48801	High latency observed on FPR42xx
CSCwj49958	Crypto IPSEC Negotiation Failing At "Failed to compute a hash value"
CSCwj50064	SSE connection events, FirewallRuleList field is not sent in proper format
CSCwj50406	All IPV6 BGP routes configured in device flapping
CSCwj50557	Snort creating too many snort-unified log files when frequent policy deploys
CSCwj51115	FMC backup remote server copy to Solar Winds remote server failing after upgrading to 7.x versions.

Bug ID	Headline
CSCwj52326	BGP config related to holdtime not being deployed sucessfully
CSCwj53324	object lookup doesn't show referenced policy automatically under object management
CSCwj53725	Traceback observed while applying 'no failover' and 'failover' in the ASA standby
CSCwj54042	Crypto ikev2 policy sequence order alters on interface/sub-interface config changes
CSCwj54644	FMC unable to upload PKCS12 certificate using Passphrase longer than 48 characters in length.
CSCwj54717	Radius secret key of over 14 characters for external authentication does not get deployed (FPR3100)
CSCwj55036	ASA/FTD: A delay in an async crypto command induces a traceback and subsequently a reload.
CSCwj55081	FPR3K loses connectivity to FMC via mgmt data interface on reboot of FPR3K
CSCwj56099	ASA: Running the failsafe-exit command caused the interface to enter a DISABLED state
CSCwj56595	delay in creating process of Readiness/upgrade post initiating from UI
CSCwj56639	FDM1010E 7.4.1 unable to register to SA, getting "Invalid entitlement tag"
CSCwj56662	FMC HA Wizard shows error "Unable to retrieve high availability status." with other languages
CSCwj56668	False positive ISE bulk download alert error seen on FMC
CSCwj57435	Cleanup stale logrotate files
CSCwj58431	FMC REST API not sending 'deploymentStatus' Attribute
CSCwj58442	FTD HA status in ON Prem FMC is corrupted reporting Secondary as Primary
CSCwj59861	ASA/FTD may traceback and reload in Thread Name 'lina' due to SCP/SSH process
CSCwj59981	FMC only accepts a maximum of 30 characters for shared secret key when connecting to RADIUS server
CSCwj60265	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-1-16803'
CSCwj61086	High CPU usage in svc_sam_dme process during deployment post breaking cluster or deleting inline-set
CSCwj61885	File descriptor leak when validating upgrade images
CSCwj62056	cEdge URLF feature is not blocking urls with categories
CSCwj62723	Error message spammed to console on Firepower 2100 devices while enabling SSH config

Bug ID	Headline
CSCwj62959	Deployment failure and rollback when changing parent of subinterface with failover MAC address
CSCwj62984	Snort3: MSSQL query traffic corrupted by stream_tcp overlap handling causing SQL HY000
CSCwj63921	Snort3 traceback and reload due to memory corruption in file module
CSCwj63975	Disable health module does not delete UMS messages for that health module.
CSCwj65587	Snmpwalk throws Error messages #"snmp/error: truncating integer value &gt; 32 bits"
CSCwj65811	FMC gets flooded with"Unable to find SSL rule id for policy" if TLS server identity discovery is on
CSCwj66339	OGO changing the order of custom object group contents causing an outage at static NAT
CSCwj66537	Snort3 crashes due to processing pdf tokenizer with no limits.
CSCwj67707	ECDSA certificates are not supported by FMC ISE integration
CSCwj67787	New User activity page does not load because the VPN bytes in and out are long.
CSCwj68286	FMC GUI errors out when searching for Topology Name that has a decimal point in the name
CSCwj68604	Tomcat and VmsBackendServer down post upgrade if a userrole description is too long
CSCwj69107	Some cloud features may not work if FMC SSO feature is toggled ON but not configured
CSCwj69632	Default Hashing Algorithm is SHA1 for Firepower Chassis Manager Certificate on 4110
CSCwj69780	SNMP host group content change results in SNMP process termination on management interface
CSCwj71064	Snort dropping connections with reason blocked or blacklisted by the firewall preprocessor
CSCwj71443	"FDM Keyring's certificate is invalid, reason: expired" health alert on FMC
CSCwj72013	PAT communication via using PAT pool fails for about 40 seconds when a device joins a cluster
CSCwj72022	Deployment time increased by 30-45 seconds after the upgrade when applying specific Platform Setting
CSCwj72369	sync call got stuck resulting in boot loop
CSCwj72615	VPN status not getting updated on site-to-site monitoring.

Bug ID	Headline
CSCwj72721	Deployment failure and rollback when BGP communities added or removed in route-map match clause
CSCwj73053	ASA may traceback and reload in Thread Name 'DATAPATH-21-16432'
CSCwj73061	SNMP OID for CPUTotal1min omits snort cpu cores entries when polled
CSCwj73171	Snort3: Smaller size packets exceeding the max segment limit cause Snort-block
CSCwj74323	ASAv Memory leak involving PKI/Crypto for VPN
CSCwj74716	tpk_mi upgrade failed from 7.4.1.1 &gt; 7.6.0 000_start/000_00_run_cli_kick_start.sh.
CSCwj77061	Policy Deployment failure in FTD HA node due to timeout for SHOW_XML_REQUEST
CSCwj77504	User group map miss after Hardware FMC model migration from FMC2600 to FMC4700
CSCwj77700	FTD LINA Traceback and Reload idfw_proc Thread
CSCwj79736	eStreamer memory leak when the FMC receives events from CDO-managed FTDs
CSCwj79895	ENH Logs FP4110 (FXOS 2.10.1.179) Security module stopped responding after device reboot
CSCwj80790	cdFMC and onPrem FMC: Device management / listing is showing chassis url for FPR-1K running 7.4.1
CSCwj81031	snmpd core seen in ASA/FTD
CSCwj81115	SFDataCorrelator deadlock on reconfigure after RNAStop and monetdb output queue is full
CSCwj81743	FTD - Trace back and reload due to NAT involving fqdn objects
CSCwj81886	[WM RM]The member interface of the Port-channel is missing on the ASA(1G & 10G) post SFP JOJI/reboot
CSCwj82127	IP-SGT mappings on Lina-side are not being removed, when FMC pxGrid connection is disabled
CSCwj82285	ASA/FTD may traceback and reload in Thread Name 'sdi_work'
CSCwj82736	TLS Handshake Fails if Fragmented Client Hello Packet is Received Out of Order
CSCwj82903	FDM HA deployment fails with 'ApplicationException: Unable to export to database' error
CSCwj83185	FTD/ASA : Standby FTD traceback and reload after enabling memory tracking
CSCwj83238	Rommon Upgrade failed due to mismatch in descriptor table.
CSCwj83533	FAN is working as expected but FAN LED is in off state.

Bug ID	Headline
CSCwj83634	Seeing message "reg_fover_nlp_sessions: failover ioctl C_FOREG failed"
CSCwj84168	SFDataCorrelator log spam, repeatedly purging expired services and client apps
CSCwj85106	FMC on upgrade results in FTDv losing its performance tier
CSCwj85232	FTD failed to join FTD-HA after upgrade revert
CSCwj85333	FPR might drop TLS1.3 connections when hybridized kyber cipher is enabled in web browser
CSCwj86116	High LINA CPU observed due to NetFlow configuration
CSCwj86320	Standby Unit Interfaces enter "Waiting" Status Post-FTD Upgrade Due to Incorrect "Hello" Message MAC
CSCwj87257	Invalid health alert msg - Classic License Expiration Monitor for "License mismatch on stack" on FTD
CSCwj87373	FMC Rest API Internal Server Error when log Interval attribute is not set
CSCwj87501	ASA/FTD may traceback and reload in Thread Name 'fover_FSM_thread'
CSCwj87770	FPR2100-ASA Unable to generate CSR without FXOS IP address on SAN field
CSCwj88400	FTD may traceback and reload in process name lina while processing appAgent msg reply
CSCwj88562	[7.6.0]Radius auth not working with custom secret key
CSCwj88765	FMC Health Monitoring sends incomplete message when language is changed.
CSCwj88843	Larger entries in EoRevisionStore table causing HA Sync to fail mysqldump process
CSCwj89228	FTD /mnt 100% disk utilization due to snort memory mapped files
CSCwj89264	FTD HA: Traceback and reload in netsnmp_oid_compare_ll
CSCwj90826	Snort2 SSL decryption with known key fails on Chrome v124 and above.
CSCwj91341	Failsafe mode default values are unattainable on some platforms need adjustment per platform/mode
CSCwj91420	Snort3 crashes while collecting flow-ip-profiling
CSCwj92784	RAVPN: Failure to create SGT-IP mapping due to ID table exhaustion
CSCwj92973	CdFMC: Device migration with RAVPN fails during import
CSCwj93300	FMC: Comments on rule change required not working in Classic Theme Legacy UI
CSCwj93718	Unable to run "nslookup" command on FXOS
CSCwj93860	CD App Sync error on FDM HA after LINA crash

Bug ID	Headline
CSCwj95322	disable stat check for file
CSCwj95590	Browser redirects to logon page when the user clicks the WebVPN bookmark
CSCwj97444	cdFMC : AC rule shown as removed in policy preview
CSCwj97492	Access rule name shows "invalid ID" instead of the rule names after patching from 7.2.4 to 7.2.5
CSCwj98451	FMC got deregistered from Smart License after upgrade
CSCwj98573	Encountering an unknown error [9999] when attempting to modify the identity policy.
CSCwj98580	Classification mismatch between intrusion and correlation events
CSCwj98648	Failure to read the signature keys (mult-instance deployment)
CSCwj98673	Fail to start a disabled container on chassis reboot and misses to log the activity to Heimdall
CSCwj99362	"show inventory" output shows Name: "power supply 0" on Firepower
CSCwj99620	Post upgrade to 7.4.2-S2S tunnel status is showing empty
CSCwj99941	M6 hardware models are hardly storing only a week old health monitoring data
CSCwk00401	CdFMC: FTD Migration Failing on Registration Phase
CSCwk00604	ASA Fails to initiate AAA Authentication with IKEv2-EAP and Windows Native VPN Client
CSCwk00628	Captive portal returns bad request for snort 2 for FMC 7.4.x , FTD version &lt; 7.4
CSCwk02332	Snort2 - SSL decryption failing and some websites not loading on Chrome v124+
CSCwk02804	WebVPN connections stuck in CLOSEWAIT state
CSCwk02928	ASA/FTD may traceback and reload in Thread Name PTHREAD
CSCwk04216	Realm download task failing with ADI process is not currently available
CSCwk04246	Unable to download users/groups getting Failed to get response from ADI.
CSCwk04290	FPR 21xx - Traceback in Process Name: lina-mps during normal operations
CSCwk04492	ASA CLI hangs with 'show run' with multiple ssh sessions
CSCwk04754	Filtered ACP rules are not greyed out when disabled using Bulk action
CSCwk04893	FTD does not compact files that are used to communicate updates to the SGT/IP mappings
CSCwk04908	FTD Unable to register to FMC due to empty DNS Server configured.

Bug ID	Headline
CSCwk05800	ASA/FTD SNMP polling fails due to overlapping networks in snmp-server host-group
CSCwk05851	"set ip next-hop" line deleted from config at reload if IP address is matched to a NAME
CSCwk06216	Loss of interface mapping with security zones after deployment
CSCwk06264	FMC REST API || ICMP objects with no code value breaking GET call and JSON parsing
CSCwk06573	Serviceablity : Improve routing infra debugs and add new for error conditions
CSCwk06689	On Slow networks, sftunnel continues to label connections as STALE.
CSCwk07250	Upgrade FMC fails while running script 120_check_legacy_private_cloud_for_ampkit.pl
CSCwk07563	Force deploy not re-generating export-cache in the device
CSCwk07934	Clock skew between FXOS and Lina causes SAML assertion processing failure
CSCwk08064	ADI Session Processing Delays return after upgrade to 7.2.x
CSCwk08476	FTD/ASA traceback and reload due to 'show bgp summary' memory leak
CSCwk08576	command to print the debug menu setting of service worker
CSCwk09559	FMC - Custom User role VPN allows user to make changes to Site to Site VPN when Modify is unchecked.
CSCwk09612	Clock skew: FXOS clock diverges from Lina NTP time ~1-10 secs
CSCwk10884	Connectivity failure due to mismatch between l2_table and subinterface mac address
CSCwk11254	"Rule Unavailable" for some local intrusion rules may be shown in intrusion event packet view
CSCwk11381	Deploying an authorization server with an LDAP attribute map results in deployment failure.
CSCwk11983	High LINA CPU observed due to NetFlow due to 'flow-export delay flow-create' configuration
CSCwk11989	Accepting duplicate object/group-object into object-group from multiple ssh sessions
CSCwk12337	RC4 ciphers cannot be disabled on FMC/FTD for captive portal authentication with Kerberos
CSCwk12470	Fatal error: Error running script 800_post/100_ftd_onbox_data_import.sh
CSCwk12497	Traceback and reload on active unit due to HA break operation.
CSCwk12673	TCP Session Interrupted if Keep-Alive with 1 Byte is Received

Bug ID	Headline
CSCwk12698	SNMP polling of admin context mgmt interface fails to show all interfaces across all contexts
CSCwk13812	ASA/FTD incorrectly forwards extended community attribute after upgrade.
CSCwk14300	TS filename still showing the old IP after FMC management IP is changed
CSCwk14657	Bring back support for portal-access-rule for weblaunch for RAVPN sessions
CSCwk14685	FTD : Management interface showing down despite being up and operational
CSCwk14909	Traffic drop with 'rule-transaction-in-progress' after failover with TCM cfgd in multi-ctx mode
CSCwk15596	Re-Registering the FMC with on-Prem server is getting failed
CSCwk16332	ASA/FTD traceback and reload with high rate of SIP connections
CSCwk17637	State Link Stops Sending Hello Messages Post-Failover Triggered by Snort traceback in FTD HA
CSCwk17854	FTD doesn't send Type A query after receiving a refuse error from one DNS server in AAAA query.
CSCwk20882	ESP sequence number of 0 being sent after SA establishment/rekey
CSCwk21533	FMC Users page in sub domain does not load
CSCwk21561	Add warning message when configuring CCL MTU
CSCwk21562	Radius server configuration for FTD external authentication is not deployed to FTD.
CSCwk21915	Upgrade readiness fails due to snort plugins
CSCwk22034	Snmpwalk displays incorrect interface speeds for values greater or equal than 10G
CSCwk22574	Remove SGT frames/packets to allow VTI decryption
CSCwk22759	Issue with Setting Certain Timezones (e.g. GMT+1) on Cisco ASA Firepower in Appliance Mode
CSCwk22814	FMC - Add warning message when configuring CCL MTU
CSCwk24176	FTD/ASA - VPN traffic flowing through the device may trigger tracebacks and reloads.
CSCwk24380	No devices listed in Packet Tracer "Select Device" dropdown
CSCwk24440	Backups may fail on remote storage when the filebackup.tar contents are so huge
CSCwk24597	EventHandler may not send events to the FMC when Snort wrote many zero-length snort-unified files
CSCwk26266	FTD cannot obtain the VPN route if answer only is configured with reverse route injection enabled

Bug ID	Headline
CSCwk26594	temporary backups files shouldn't be kept on remote storage and do not parse other format files
CSCwk26968	Backup feature does not save/restore DAP configuration in multiple context mode.
CSCwk27628	CDO: Chassis onboarding to CDO is failing with hostname
CSCwk27639	FMC 7.2.5 Showing incorrect data of FTD HA at 6.6.5 under fleet upgrade
CSCwk27830	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwk27965	Safety Net for Infinite Recursion Crashes due to Bad Stream TCP State in (IDS)Post-ACK mode
CSCwk28058	FTD memory depletion resulting in traceback and reload
CSCwk28296	SFDataCorrelator stops receiving events on a device channel when the other channel blocks
CSCwk29771	FTD 7.4.1.x sends NAS-IP-Address:0.0.0.0 in Radius Request packet as network interface
CSCwk30965	AppIdSessionData causes snort3 to crash 7.2.6
CSCwk31371	NAT_HARDEN: CGNAT breaks when mapped ifc is configured as any
CSCwk32340	Enable logs to identify corrupted policy when deployment fails with "SNAPSHOT_PG_TIMESTAMP_ERROR"
CSCwk32501	256/1550 block depletion process fover_thread
CSCwk33070	FMC "java.lang.OutOfMemoryError: Java heap space" errors in feed_data_manager.log
CSCwk33387	SNMP for mgmt0/diagnostic outgoing traffic is missing
CSCwk33577	Devices not listed to add a data node when creating a cluster because of OS version mismatch
CSCwk33634	TLS Client Hello packet is dropped by snort
CSCwk33842	FMC Management workflow issue: Cannot remove NetworkObject from group and delete it in same ticket
CSCwk33876	Standard Access List Objects can be written with leading whitespace
CSCwk34786	victoria-DT CX: support of 10 port-channel intf on 1220 CX model
CSCwk34888	Health Alerts are generating for sub interface even when main interface is excluded.
CSCwk34905	ISE connection status health alerts on FMC with ise services down
CSCwk35638	Dangling interfaces exists in SecurityZone/Interface group and interface

Bug ID	Headline
CSCwk35710	FTD/LINA may traceback and reload when "show capture" command is executed in EEM script
CSCwk36144	Update Fan RPM Thresholds for 42xx platforms
CSCwk36312	High cpu on "update block depletion" with secondary effects (Bgp flaps, traffic drops)
CSCwk37371	SGT INLINE-TAG added after upgrade to 7.4.x
CSCwk37701	FTD lost connection with cdFMC after FTD backup Restoration
CSCwk38440	if conn_meta null, dont send packet to snort
CSCwk38851	FMC should not take a policy backup during patch / Hotfix installations.
CSCwk39514	Endpoint Assessment features are not enabled when HostScan package is modified via FMC
CSCwk40335	Trigger Alert/Warning when the associated FQDN IDs of an IP address surpasses the set limit of 8
CSCwk40403	WebEx traffic not getting bypassed in snort3 (allow rules)
CSCwk40726	FMC REST API calls to get AC policy data times out, AC policy GUI slowness with larger rule query
CSCwk41007	ASA/FTD may traceback and reload
CSCwk41396	ASA to FTD migration via FMT causes improper configuration of interface groups in FMC backend config
CSCwk41806	Need to Protect LINA from getting killed by OOM
CSCwk42112	Changes made on health policy are not being saved
CSCwk42266	Zone Based AC rule has missing interface mapping
CSCwk45975	TLS1.3 Decryption configuration on SSL policy is affecting DND traffic.
CSCwk46737	ASA on HA: alloc_ch() alloc from chunk mem Failed message on one context in Standby device
CSCwk47035	CMI is disabled if pre-CMI nameif on diagnostic interface is MANAGEMENT
CSCwk48628	FTD/FxOS - Upgrade/erase configuration result in App-instance 'Operational State: Starting'
CSCwk50179	Potential upgrade failure in 800_post/890_install_version_masked_apps.pl
CSCwk50986	NAT Exemptions in UI will not load when object group is added as protected network
CSCwk52890	FTD / ASA High Memory Usage Due to HTTP-based Path Monitoring

Bug ID	Headline
CSCwk53048	Standby HA FMC entering standalone mode - /var/tmp/compliance.rules which was created was invalid.
CSCwk53257	API call for ftdallinterfaces returns an inaccurate "self" element.
CSCwk53312	Unable to upgrade cluster with status "cluster/HA pair is not eligible'
CSCwk54033	FMC can not connect to private AMP when proxy is enabled in management interface
CSCwk54077	Empty network objects cause cdFMC migration to fail
CSCwk56388	GRE traffic getting dropped after failover
CSCwk59009	IPv6 SSL Anyconnect access blocked in HA pair
CSCwk59520	Instrument new logs in the startup process to collect more information
CSCwk61157	FTD LINA Traceback and Reload dhcp_daemon Thread
CSCwk62366	Exception raised while fetching telemetry data from the FMC
CSCwk62381	ASA might traceback and reload due to ssh/client hitting a null pointer while using SCP.
CSCwk63011	Incorrect network module slot and status information in "show module" command output
CSCwk63733	HA-monitored interfaces are going into "waiting" state and subsequently to "Failed"
CSCwk63811	Terminating Active sessions from new UI Layout throws error- "Error while terminating session"
CSCwk64418	NTP is not synchronising when using SHA-1 authentication
CSCwk64643	Failover prompt shows state active while the firewall is in Negotiation
CSCwk64709	FXOS upgrade failure due to insufficient free space in /mnt/pss (isan.log consumes most of space)
CSCwk67346	DAP policies not working with attribute TRUE/FALSE
CSCwk70078	Failures and records are not seen in "show failover statistics" after simulating failures
CSCwk70673	Certificate validation fails with trustpool when FIPS is enabled
CSCwk70769	FMC: API interface settings differ from GUI settings for Diagnostic Interface
CSCwk71227	FTD running on FPR 2k with LDAP skips backslash when updating ldap.conf
CSCwk71866	ASA: Site-to-Site VPN between contexts on the same device drops traffic due to 'ipsec-tun-down'
CSCwk74592	vFTD upgraded to 7.7.0: Module Compilation Error Health coming

Bug ID	Headline
CSCwk75406	FMC in CC-mode audit over syslog not working
CSCwk75956	ASA/FTD may traceback and reload in Thread Name SSH
CSCwk76362	FTDv traceback in Thread name - PTHREAD
CSCwk76734	Policy deployment fails due to mismatch in 'ip local pool' command between fmc and lina config
CSCwk77241	Traffic outage due to 9k block depletion (tcpmod proc) observed on FPR 3100 (HA)
CSCwk78030	ASA/FTD: Memory Exhaustion due to Threat-Detection
CSCwk78075	FTD does not mark stuck ongoing deployments as failed leading to subsequent deployment failures
CSCwk78242	Empty user attributes in LDAP causes partial user/group download
CSCwk79222	Health alert seen on FMCs : URL/LSP-via Beaker3
CSCwk79288	Partition "/opt/cisco/config" gets full due to btmp file not getting logrotated
CSCwk80518	snort2 'ids_event_msg_map' clean up is not happening when import sfo fails during cdFMC migration.
CSCwk81274	FMC: Not receiving any Email Alert after upgrade
CSCwk82337	Policy export fails with error "Unable to process the policy information for Export"
CSCwk82557	FTD upgrade to 7.4.2 via FDM is blocked
CSCwk82571	VPN Client Application version and OS is not displayed for the FTD Standby peer under User Activity
CSCwk82591	Unable to create MI FTD in TPK chassis
CSCwk83804	Scheduled backups fail to execute on other cluster nodes when there is a change on the control node
CSCwk85012	CSDAC connectors not coming up after FMC upgrade
CSCwk86563	Source Port and Destination Port are swapped during the evaluation of SID
CSCwk86582	'ENDPOINT_TIME_OUT_OF_SYNC' Error Causing SAML Auth to Not Complete
CSCwk87081	cdFMC: tmp_cisco is consuming high boot volume space for the cdFMC tenants
CSCwk87457	ASA/FTD may traceback and reload in Process Name "lina" after device was reloaded
CSCwk88182	FTDv50 traceback during normal operation at PTHREAD-8141 spin_lock_fair_mode_enqueue
CSCwk88201	S2S VPN with 3rd party broken after upgrading FPR 9.20

Bug ID	Headline
CSCwk88225	Critical fault : [FSM:FAILED]: user configuration(FSM:sam:dme:AaaUserEpUpdateUserEp)
CSCwk88571	Partial configuration gets lost for a HA FTD pair, if FMC connectivity is lost during upgrade
CSCwk88913	Keep a FMC backup locally until we copy the file to remote server successfully
CSCwk89061	Search Index shouldn't be failed if any of the port object value is invalid
CSCwk89127	Backup_info table is not being pruned, causing DB queries to slow down
CSCwk89836	ASA/FTD may traceback and reload in Thread Name 'strlen'
CSCwk90663	Configure External Storage fails second time with same backup profile
CSCwk90679	Radius Authentication test fails due to missing radclient command
CSCwk90796	Update dynamic-config-json and reloadLina on FTD when (de)activating custom detector with NSG tag.
CSCwk93762	Device traceback and reload thrice with Panic at spin_lock_fair_mode_enqueu and nlp_init().
CSCwk94382	FTD: Lina might fail to respond to CONFIG_XML_REQUEST leading to stuck deployments
CSCwk94697	FMC allows uploading a binary certificate in Identity Certificate import
CSCwk96912	FTD: Username missing in syslog message ID 302013 after upgrade to 7.4.1
CSCwk97058	FMC - Predeploy validation should error and block deployment if VPN Certificate is in failed state.
CSCwk97812	RAVPN Certificate Group Map get removed after it is modified on the FMC
CSCwk98990	Large number of stats files can cause events to be delayed
CSCwm00154	FTD: Process sftunnel exited unexpectedly with a core file generated
CSCwm01544	Lina traceback and reload in data-path thread
CSCwm01901	Excessive logging of "vpn:vpn [INFO] device" messages in /var/log/messages file
CSCwm02801	Unstable HA causing depolyment failure
CSCwm03142	IPv6 Neighbor Discovery failure on shared interface in multi instance setup
CSCwm03227	FTD upgrade failure due to multiple DB folders in /ngfw/var/cisco/deploy/tmp_bundle/db/ path
CSCwm03287	FP4245 - NPU Accelerator changed speed of 100Gb interface to 10Mb
CSCwm03772	CLI "ssl server-max-version" Can't be deployed Via Flex Config

Bug ID	Headline
CSCwm04021	ASA|FTD Traceback & reload in process name lina
CSCwm04085	Document NAT warning "The NAT rule exceeds the threshold limit of 131,838 IP addresses.."
CSCwm04650	Increase memory usage leading to tracebacks in Lina.
CSCwm05155	Snort AppID incorrectly identifies SSH traffic as Unknown
CSCwm05221	Snort3 file detection fails with asymmetric traffic in IDS passive mode
CSCwm05226	VPN Topology status shows No Active Data in the S2S VPN Dashboard
CSCwm05520	Disable cluster syn cookie decoding when FTD cluster is deployed with inline-set
CSCwm05949	Continuous loading state and PolicyRPC call remains in pending
CSCwm05960	Generated Crypto checksum changes without configuration change
CSCwm06393	Changes in port-channel membership or member status may cause periodic OSPF/EIGRP adjacency flaps
CSCwm07389	CGroups errors in ASA Syslog during every reboot
CSCwm07419	ldap.conf does not get generated using hostname
CSCwm08889	df commands are getting stuck at times due to mount storage points
CSCwm09571	DVTI: Provide info / warning message about interface shut and no shut upon DVTI config modification
CSCwm09680	Log spam and possible network slowness due to failed dns lookups for syslog server
CSCwm11515	SNMP trap OID changed after upgrade
CSCwm12434	Readiness check should be in place for larger undo/ibdata log files
CSCwm12920	Unsupported characters in Azure Display Name causes errors in Access Control Policy
CSCwm13137	Correlation Fails to Detect Connection Duration
CSCwm13141	FTD CLISH/CLI gets locked up when trying to run any show command
CSCwm13199	SIP traffic is affected due to unexpected behavior with NAT untranslations.
CSCwm14509	Wrong drops seen with Invalid length for 23, 24 and 25 IE-Types during GTP inspection
CSCwm14561	ASA/FTD may traceback and reload in Thread Name 'fover_parse'
CSCwm14729	CSF 3100 series not rebooting after power outage, requiring manual power cycle
CSCwm27588	fix to remove space characters in auth object names during FMC upgrade may cause upgrade failure

Bug ID	Headline
CSCwm27687	"custom workflow" GUI show Error 500, after create an custom workflow with Chineses description
CSCwm28007	Browser redirects to blank page when the user clicks the WebVPN bookmark
CSCwm29469	FMC GUI has a limitation to display only 50 SSH rules for FTD (Under platform settings &gt;&gt; SSH)
CSCwm29768	Connection been logged for rules with no logging enabled
CSCwm29929	QoS policy editor on FMC GUI lacks functional pagination when QoS policy has more than 50 rules
CSCwm29941	Prefilter policy not getting applied to child ACP when inherited from base policy
CSCwm30731	The ASA's OSPF routing table is not properly synchronized with the neighbors
CSCwm30786	Increase timeout for SFTunnel Connection Check requests
CSCwm30825	Add connection status file for marking slow SFTunnel connections
CSCwm31353	FTD logs should contain the certificate name or files which are corrupt
CSCwm31562	FMC Health Plug-in for NTPD status analysis is not using localized data
CSCwm33229	SAML Force re-authentication Is Not Enforcing User To re-enter Credentials Upon Retrying To Connect
CSCwm33529	FXOS MTU Handling for Front Panel and Uplink Ports on Firepower devices require improvement
CSCwm33552	FMC Does Not Accept Valid IP Range Format in Access List under system configuration settings
CSCwm33557	ibdatafix script needs to address cfgdb if the FMC is running version 7.3 or higher.
CSCwm33613	Default Group Policy is applied when receiving multiple Group Policies in SAML assertion attributes
CSCwm33619	FTD Vault process exits every 1 minute: "Process vaultApp (23597) exited normally: 256"
CSCwm34333	FTD - Â Multi-Instance, docker0 interface overlap with private network 172.17.0.0/16
CSCwm34786	Platform settings policy hidden on UI
CSCwm35035	SAML Auth Request by FTD Will Always Be Signed By Sha1 Irrelevant Of the Algorithm Configured
CSCwm35051	hostname/IP Address field does not accept domains ending in a number
CSCwm35251	FMC4700 displays premature fan speed alerts
CSCwm35569	Not able to disable PLR post enabling it without name resolution available

Bug ID	Headline
CSCwm35751	FPR3100: Interface may go to half duplex speed is hardcoded to 100mbps
CSCwm36631	FTD Secondary Unit got stuck in Bulk sync state.
CSCwm36646	After FMC upgrade results in standby FTDv losing its performance tier for FTD HA
CSCwm37043	Crash handler notification for snort3 failure not being sent in MI setup.
CSCwm37455	ASA/FTD will allow local IP pool with invalid netmask
CSCwm37690	NAT Rules Before deleted when policy is saved on FMC
CSCwm38299	REST Calls from CDO to cdFMC are failing randomly with null/empty response
CSCwm38513	Objects get duplicated when policy imported using 'Replace Existing' option
CSCwm38635	TACACS+ traffic is dropped by TLS Server Identity in XTLS module
CSCwm40721	PDTS write from Daq can fail when PDTS buffer is full and it would eventually lead block depletion
CSCwm41381	File Download fails intermittently with malware & file policy configured
CSCwm41847	Serviceability to capture PDTS writing/reading block to help root cause CSCwm36314
CSCwm42000	FTD/ASA may traceback and reload in DATAPATH thread
CSCwm42745	Dynamic Site-to-Site tunnels stuck in IN-NEG state When IKE_AUTH Is Missed
CSCwm44412	FTD inline-set ignore reverse flag for inject/rewrite
CSCwm45164	cdFMC: unable to modify the VTI interfaces due to Tunnel type is missing in DB
CSCwm47235	FTD upgrade may fail in 901_reapply_sensor_policy.pl if policy_deployment.db is corrupt/unavailable
CSCwm47769	ID attribute of other device during copying config via REST API POST can remove original config
CSCwm47775	FMC Deployment Failure When Modifying NAT Policy with Block Allocation and Round-Robin Enabled
CSCwm48218	FMC: Unable to save interface config as save button is greyed out
CSCwm49154	FXOS fault F1738 seen in deploymet with Error: CSP_OP_ERROR. CSP signature verification error
CSCwm49213	Show mod functionality needs to be fixed after change was reverted in CSCwk63011 due to regression
CSCwm49458	DNS settings removed in post-upgrade deployment
CSCwm49721	ASA Traceback and Reload due to MEMORY CORRUPTION WAS DETECTED

Bug ID	Headline
CSCwm49782	enhance sma 2nd cruz heartbeat logging
CSCwm49940	ha-mode graceful-restart is missing in advanced preview
CSCwm50591	ASA/FTD: Inbound IPsec packets are dropped when IPsec offload is enabled with VTI and sub-interface
CSCwm50936	100GB interface flaps with Innolight QSFPs in both ends
CSCwm51923	Deployment transcript showing "Enable management access: false"
CSCwm52264	Not able to remove or clear Fault "The password encryption key has not been set."
CSCwm52430	FMC Upgrade Fails at 39% 600_schema/103_csm_cfgdbmigration.sh
CSCwm52931	ASA/FTD may traceback and reload in Thread Name "fover_parse"
CSCwm52973	TPK Low End FPR3100:Changing interface speed from 1g to 100mbps/100mps to 1g bring downs the link
CSCwm56864	show run access-list command returns warning
CSCwm57511	Issues with extdb Omniquery execution
CSCwm58260	Snort3 crash on TLS cert have same issuer and common name,but sign algo and public key are different
CSCwm58600	FMC: Unable to select Secure Client Images in RAVPN Wizard
CSCwm58772	snort2 instances restart unexpectedly with OOM during policy deployment
CSCwm58948	FMC AzureAD User/Groups Download Failing: too many SQL variable
CSCwm60536	SQLNet traffic getting dropped intermittently in Clustering data unit.
CSCwm61282	ASA/FTD: RA VPN tunnel causing memory leak leading to traceback & Reload
CSCwm63024	DAP Cert Serial Number check field should be freeform instead of hex format on FMC
CSCwm63868	FTD - Missing routes on BGP advertised-routes after FTD HA failover event
CSCwm64553	Incompatible members warning message after Po member interface flaps unable to rejoin Po
CSCwm65693	Snort 3 rules display discrepancy in the GUI of FMC.
CSCwm65773	Refresh of Inventory shows incorrect message "Device is not reachable" with sftuunel is UP
CSCwm66653	FMC DHCP Relay Agents and Servers doesn't show in the UI or allow any changes
CSCwm66731	In RAVPN policy edit action getting stuck, when editing LDAP attribute maps
CSCwm68211	ASA traceback and reload on thread snmp_inspect

Bug ID	Headline
CSCwm69907	FMC not sending/synchronizing the RADIUS config file to the FTDs
CSCwm70356	Deployment failing with "no nameif" on the failover interface
CSCwm70490	VDB upgrade is failing on longevity setup
CSCwm70835	ASA traceback and reload due to stack overflow while using APCF file
CSCwm71265	ASA traceback and reload on thread DATAPATH when processing gtpv1 end marker msg for PDP
CSCwm71730	Global search of the objects not working due to stale domain id reference
CSCwm72176	FTD Lina process is brought down if mysql/mariadb is restarted for any reason post FTD startup
CSCwm72757	Snort3 blocking ESMTP traffic intermittently and trigger IPS signatures 124:3:2 and 124:1:2
CSCwm74289	NAT traps have to be rate-limited
CSCwm74973	Deployment failure is not getting listed on the deployment history
CSCwm76721	Upgrade Resume is failing when user triggered Resume after 7.7.0 Build to Build Upgrade failure
CSCwm77673	Policy Deployment Hung at 5/8% Deployment - Collecting policies and objects
CSCwm78241	On cdFMC FTD-HA pair standby node has stale Interface status health alert
CSCwm78288	License showing diffrent tier in FMC UI
CSCwm78351	Potential High CPU usage in Multi-Context Cluster setup with unconditional execution of capture code
CSCwm79807	SFDataCorrelator cores while calling DCEControlMessageReconfigure
CSCwm79920	External auth (Radius) User unable to login to FTD due to mismatched cases during initial login
CSCwm80085	FMC does not clear old Intrusion Policy recommendations when they are regenerated
CSCwm82683	Registration Cleanup Should NOT Run if the peers Directory Cannot Be Opened
CSCwm83580	FMC Remote Storage Error: Use of uninitialized value $^WARNING_BITS in bitwise xor (^)
CSCwm84062	deregistering FMC from smart licensing may result in double consumption of FTD Base licenses
CSCwm85228	ASA/FTD may traceback and reload in Thread Name "IKEv2 Daemon" while joining failover

Bug ID	Headline
CSCwm85497	Secondary FMC indicates the FTD is still upgrading, despite the upgrade being completed.
CSCwm85795	Access Control Policy export fails due to dangling object on Intrusion Policy Recommendations
CSCwm86416	ENH: FMC API: Threat Defense Upgrade Options skip automatic generating of troubleshooting files
CSCwm87310	PBR with default next-hop not allowed without next hop
CSCwm87409	FMC is sending a wrong value for engineID in SNMPv3 traps
CSCwm88812	4200/3100/1200 hardware allow to change AppAgent timer
CSCwm89523	'no capture /all' failed to disable capture completely in the backend, causing high datapath CPU
CSCwm89747	Deployment failed with the reason "Error-no dhcpd enable inside"
CSCwm90900	GTP inspection drops packet with error Reason:(IE-Type:CAUSE(2) IE is missing)
CSCwm90905	GTP inspection drops packet with error ERROR-DROP:MsgType:32
CSCwm91406	FTD HA Standby Reloads Repeatedly After Upgrade to 7.4.2.1
CSCwm92310	FQDNs are unresolved via DNS on data interface after reboot or traceback
CSCwm92397	LINA core observed pointing to "IP RIB Update" thread
CSCwm93119	FMCv is incompatible with certain KVM hypervisor software versions
CSCwm94752	Identity Mapping Filter shows blank, even though there is a selected network object.
CSCwm94971	Secure Client Connection Profile Address Pool not Shown
CSCwm95116	ADI crashes on FTD due to both FMC ADIs going unmuted
CSCwm95328	Copy/Paste for a rule on any UI page other than page 1 results in policy UI loading back to page 1.
CSCwm96280	FTD device stuck in rommon mode after pressing reset button
CSCwm96652	Cluster assigning wrong nat for unit, traffic not being forwarded properly back to unit
CSCwm97054	ASA/FTD traceback and reload with high rate of SIP connections
CSCwm98278	TCP Conn not being flagged as Half-Closed after receiving the ACK for the FIN.
CSCwm99183	cdFMC,SFOExport files are not cleared in tmp folder leading to high disk utilisation.
CSCwn01281	GTP inspection not allowing GTP data packets if session create response has cause type 18

Bug ID	Headline
CSCwn03446	When capture enabled on cluster interface, it always includes CCL IP along with the configured rule
CSCwn03796	Unity style enrollment after registering to the AMPkit portal
CSCwn03807	ASAv traceback seen when doing testing for Anyconnect
CSCwn03835	ASA/FTD may traceback and reload in Thread Name 'SSH Ctxt Thread'
CSCwn05183	FTD HA active node interfaces went down after failed policy deploy
CSCwn08085	vertical scroll bar missing in Available Rules modal in correlation policy editor in most UI themes
CSCwn08400	cdFMC 7.6 not pruning SRU packages, causing device to reach maximum storage space
CSCwn09870	FlexConfig objects Policy_Based_Routing and Policy_Based_Routing_Clear cause deployment failure
CSCwn10538	ADI on FTD does not stop after a crash
CSCwn10680	FTD deployment fails with error "Snort command failed due to bad config"
CSCwn12333	Unable to Delete Radius Authenticated User from FDM UI
CSCwn13187	ASA upgrade failing from 9.20.2.21 to the target version 9.20.3.4
CSCwn13238	Intrusion rule recommendations fail to apply when "Generate" option is used and then applied later
CSCwn13672	Bind ESP to VTI Tunnel Source Interface To Avoid Additional Route-Lookup Post Encryption
CSCwn14130	FTD cluster to traceback and reload after extended PAT is enabled
CSCwn14355	Validation errors after updating Hub and Spoke topology.
CSCwn14447	ASA/FTD may traceback and reload in Thread Name 'ldap_client_thread'
CSCwn14458	FMC: Enable validation of "Comment" Field under Automating Policy Deployment Tasks
CSCwn15104	FTD reload with traceback on swapcontext function
CSCwn15787	FMC RAVPN Active Session termination throws error- "Error while terminating session"
CSCwn16320	Syslog servers below in FTD logging send hostname info as per emblem config for first syslog server
CSCwn17121	ASA/FTD may traceback and reload in Thread Name 'cli_xml_request_process'.

Bug ID	Headline
CSCwn18734	cdFMC- Post device migration deployment validation indicates security zones are missing interfaces
CSCwn19190	Memory fragmentation resulted in huge pages unavailable for lina
CSCwn19498	Unable to add Data nodes to Existing Cluster setup during cluster app-sync phase
CSCwn19690	Critical health alert, module SMART_LICENSE Smart Licensing Agent is not running
CSCwn19706	Admin users are prompted to change local password when authenticating to external server
CSCwn19739	HA would bring data interfaces up while moving from cold standby to failed state
CSCwn19761	Large number of stale revisions in CloudConfig affects FMC performance.
CSCwn20024	ASA may traceback and reload in Thread Name 'ssh'
CSCwn20642	Discrepancy in VPN bytes with RA VPN user activity report
CSCwn21171	FDM is not pushing the trusted CA certificate to the FTD if validation usage not chosen
CSCwn22036	FTD: Management0/0 status went down, line protocol is up after upgrade
CSCwn22456	GTPv2 IE-type 157 (Signaling Priority Indication) is dropped with reason as unknown IE type
CSCwn22708	FMC does not delete intrusion rules from database when they are removed from LSP
CSCwn23031	Can't delete IPS policy when Workflow Mode is enabled
CSCwn23175	Configure Multi-Instance in Secure Firewall 3100 Series using patched versions of code
CSCwn23362	FTD: Snort AppID Misclassifies NetBIOS-ssn Traffic as Unknown
CSCwn24577	ASA booting process may freeze when including 'no pim' or 'no igmp' config
CSCwn25430	Secure Client External Browser package Image shown 2 same packages
CSCwn26165	FTD/ASA May Traceback and Reload - During Deployment / Radius changes - Due to Radius Packets
CSCwn27819	Jumbo frame packets are being fragmented
CSCwn29465	Generic error thrown when a user tries to access Packet-Capture page
CSCwn29609	Extended PAT configuration can be enabled on clustered devices when FMC UI states it will be ignored
CSCwn29611	Radius user ssh login fails with error: username is not defined with a service type that is valid
CSCwn31151	Newline character in interface description results in deployment failure

Bug ID	Headline
CSCwn31166	Snort3 crash in js norm with out-of-range exception during unescaping
CSCwn31240	Traceback and reload due to webvpn dtls flow offload enabled
CSCwn31588	MI: Instances going in split brain when assigned RP with CPU cores between 14-70 on FPR42xx
CSCwn31653	FTD may traceback and reload in Thread Name "FPRLI_FPR4K-SM-32"
CSCwn32025	FMC Management workflow issue: Cannot remove NetworkObject from group and delete it in same ticket
CSCwn32978	Traceback and reload in Thread Name Datapath
CSCwn33750	correlation rules with access control rule name condition will not properly save on standby FMC
CSCwn34259	Monitored interfaces may go in waiting state after upgrade to 9.20.3.7
CSCwn34659	Firewall not initiating TCP request even after receiving the TC bit set in DNS response
CSCwn34707	Multiple Unicorn Admin Handler processes consume all the control plane CPU.
CSCwn34741	SMB remote backup failure due to realm sync
CSCwn36712	nat divert for 8305 on standby not updating post failover causing the Primary, standby FTD to show offline on FMC
CSCwn36925	LSP deployment fails in MI environments following a patch or hotfix installation failure.
CSCwn38109	Raw coredump file not getting deleted on vFTD even after compressed core generation
CSCwn38431	Intenal error seen when trying to include domains in dynamic split tunneling of custom attribute
CSCwn39081	SNMP walk results in ASCII value for IPSEC Peer instead of an IP address.
CSCwn39780	FTD Deployment Resilience: Skip non-critical / non-existing commands to avoid deployment failures.
CSCwn39810	FMC to warn users when deploying other configs alongside FlexConfig.
CSCwn39826	HA should prevent honouring failover requests while copy/config-sync/rollback is in progress
CSCwn39923	Fatal error while upgrading at 000_start/120_check_legacy_private_cloud_for_ampkit.pl.
CSCwn40485	MI: Traffic fails to reach the Secondary FTD when enabled with data-sharing interface
CSCwn40572	MI: Vlan info is not applied at FXOS level when Virtual MAC is configured

Bug ID	Headline
CSCwn42949	Implementing forwarder flow on non-owner units handling distributed secondary flow connections
CSCwn44326	recurring GeoDB updates may fail to install when scheduled at the same time of day as rule updates
CSCwn44335	FXOS - Download command generates an extra "/" over HTTP and HTTPS GET requests
CSCwn45049	Coverity System SA warnings 2024-09-09, Coverity Defects 922530 922529 922528 922630 921809 921808
CSCwn45194	FMC can generate health alerts when ntp temporary switches to HW local clock from external server
CSCwn45510	S2S VPN tunnel Child SA unsuccessful renegotiation
CSCwn46794	FMC UI becomes unresponsive when converting and downloading Snort 2 rules
CSCwn46855	LINA may observe random traceback with Netflow configured
CSCwn46861	Multi-Instance in Secure Firewall not updating sftunnel certificates
CSCwn47308	Critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on FPR 1100/2100/3100
CSCwn49391	Frequent traceback after upgrading FTD HA
CSCwn51845	Tracebacks observed in a cluster member running ASA 9.20.3.4
CSCwn54186	JBDC client throwing error on certain queries after upgrade
CSCwn54561	Modify memory allocation for policy deployment subgroup
CSCwn54837	Application Name Change in VDB Not Reflected During Event Processing
CSCwn54966	Snort3: TCP Midstream Traffic on ACK Normalized by snort and blocked by the Stream Preprocessor
CSCwn55195	Deploy Preview comparison PDF report not getting generated
CSCwn57518	FMC : OSPF setting screen cannot be opened in FMC English UI
CSCwn57940	Deploy preview fails if device is moved from one domain to another domain
CSCwn58715	Health Monitoring UI high-availability widget shows incorrect device information for primary device
CSCwn59632	FTD registration to FMC gets hung when RabbitMQ is down.
CSCwn61176	EventHandler not restarted after running system support reset-event-bookmarks on FTD 7.2 and above
CSCwn63410	Snort3 traceback and reload due to memory corruption caused by a double free operation

Bug ID	Headline
CSCwn63839	Traceback in thread name Lina on configuring arp permit-nonconnected with BVI
CSCwn65415	ASA: floating-conn not closing UDP conns if conn was created without ARP entry for next hop
CSCwn71946	show blocks old core local can lead to crash.
CSCwn73351	Asia/Bangkok timezone option not listed in ASA running on firepower1k
CSCwn73371	False alerts of FMC HA in degraded sync state
CSCwn75536	FMC backup failed while cfgdb dump after upgrading FMC to 7.4.2.1
CSCwn75667	Banner motd does not display when configured
CSCwn75744	After upgrading FMC, deployment fails because of high SI Objects
CSCwn76079	SSH works in admin context but doesn't work in any user context after changing ssh key-exchange
CSCwn76587	RAVPN Active session UI on Security Cloud control not showing all active sessions.
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
CSCwn80765	ISA3000 with ASA Refuses SSH Access If CiscoSSH is Enabled
CSCwn81833	FMC User permissions allows user to Suspend HA even when "Modify Devices" is not selected
CSCwn81995	Traceback and Reload caused by Memory corruption with SNMP inspection enabled
CSCwn85299	Very High threat confidence is displayed for the threat score 98
CSCwn85913	extdb query error when ordering by count(*)
CSCwn90900	High ASA/FTD memory usage due to polling of RA VPN related SNMP OIDs
CSCwn91169	User gets Global Dashboard with unauthorized error when authorized only for a subdomain
CSCwn92074	FMC managing various lower version vFTDs throws Event Handler errors
CSCwn92894	Occasionally, 'show chunkstat top-usage' output does not show all entries
CSCwn93319	ASA/FTD may traceback and reload in Thread Name "DATAPATH"
CSCwn95939	Generate syslog if received CRL is older than cached CRL
CSCwn95945	Generate syslog if received CRL signature validation fails
CSCwn96064	Unknown disposition files take a long time receive status and threat score.

Bug ID	Headline
CSCwn96929	ASA: Traceback and Reload Under Thread Name SSH
CSCwn97630	FTD data unit in cluster experienced traceback and rebooted
CSCwn98402	Debuggability: FP2100 port-channel interfaces flap after upgrade
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
CSCwo01557	ASA traceback and reload on DATAPATH thread due to memory corruption
CSCwo08042	ASAv reloaded unexpectedly with traceback on Unicorn Proxy Thread
CSCwo08306	Command authorization fallback to Local only works for priv 15 users.
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.
CSCwo09618	Enabling debugs with EEM fails
CSCwo18838	ASA/FTD may traceback and reload in Thread Name 'lina_exec_startup_thread'
CSCwo21767	Port scan alerts not getting generated for custom configuration
CSCwo24772	debug packet-condition does not work as expected
CSCwo26258	Default Route Changes from Management0 to Management1 After Reload or Upgrade on FPR 4200 Series
CSCwo31418	AC policy with Network Group Override object causes deployment failure/rules missing
CSCwo35783	Enhance Debugging for add/update/withdraw of routes with neighbors
CSCwo35788	Serviceability Enhancement - New 'show bgp internal' command for advanced debugging
CSCwo41250	Traceback & Reload in thread named: DATAPATH-1-23988 during low memory condition
CSCwo42230	Memory leak leading to split brain
CSCwo46142	Port-channel member interface flap renders it as an inactive member
CSCwo47978	ASA may traceback and reload in Thread Name 'fover_parse'
CSCwo49425	Logging recipient-address not overriding the logging mail message severity levels
CSCwo49744	DNS and default gateway are removed on FTD managed through data interface

Bug ID	Headline
CSCwo54996	Traffic failure due to 9344 blocks leak
CSCwo58191	FTD: Large Delay in packets being inspected by snort
CSCwo65891	Unable to validate change ticket:
CSCwo66872	snmp_logging_thread is utilizing high CPU in control plane
CSCwo69637	FMC SSL Policy Advanced Settings Changes by 'Admin' Users Not Visible to 'Read-only' Users
CSCwo71052	FPR1010 Ethernet1/1 trunk port is not passing vlan traffic after reload
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
CSCwo76436	TPK: Marvell 4.3.14 CPSS patch for the interface mac stuck issue seen with peer switch reloads
CSCwo77665	Portscan event in FMC displays incorrect source/destination when set to 'low' setting
CSCwo80223	BFD packets are not dropped for single-hop BFD sessions received via alternate path
CSCwo82639	Local user details not replicated to data nodes in a cluster setup.
CSCwo87938	backout change preventing enabling clustering in FIPS mode
CSCwo94483	LINA stays inactive without reloading after traceback if crash occurs on non-CP thread

For Assistance

Upgrade Guides

In Firewall Management Center deployments, the Firewall Management Center must run the same or newer maintenance (third-digit) release as its managed devices. Upgrade the Firewall Management Center first, then devices. Use the upgrade guide for the version you are *currently* running—not your target version.

Table 19: Upgrade Guides

Platform	Upgrade Guide	Link
Firewall Management Center	Firewall Management Center version you are *currently* running.	https://cisco.com/go/fmc-upgrade
Firewall Threat Defense with Firewall Management Center	Firewall Management Center version you are *currently* running.	https://cisco.com/go/ftd-fmc-upgrade
Firewall Threat Defense with device manager	Firewall Threat Defense version you are *currently* running.	https://cisco.com/go/ftd-fdm-upgrade

Platform	Upgrade Guide	Link
Firewall 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 Firewall Threat Defense version on an FXOS device, perform a full reimage—even for devices where the operating system and software are bundled.

Table 20: Install Guides

Platform	Install Guide	Link
Firewall Management Center hardware	Getting started guide for your Firewall Management Center hardware model.	https://cisco.com/go/fmc-install
Firewall Management Center Virtual	Getting started guide for the Firewall Management Center Virtual.	https://cisco.com/go/fmcv-quick
Firewall Threat Defense hardware	Getting started or reimage guide for your device model.	https://cisco.com/go/ftd-quick
Firewall Threat Defense Virtual	Getting started guide for your Firewall 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 Firepower 1000/2100 and Secure Firewall 1200/3100/4200 with Firepower Threat Defense

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-77-docs
- Cisco Support & Download site: https://cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.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

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

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

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

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

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

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

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

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