Cisco Secure Firewall Threat Defense Release Notes, Version 7.4.x

First Published: 2023-09-07

Last Modified: 2026-09-16

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 Release Notes for Cloud-Delivered Firewall Management Center or *What's New for Security Cloud Control*.

Release Dates

Table 1: Version 7.4 Dates

Version	Build	Date	Platforms
7.4.8	79	2026-09-15	All
7.4.7	50	2026-04-15	All
7.4.6	7	2026-02-17	Firewall Management Center
7.4.5	2	2026-01-14	Firewall Management Center
7.4.4	462	2026-01-05	All devices
7.4.3	315	2025-10-13	All
7.4.2.4	9	2025-09-25	All
7.4.2.3	4	2025-06-17	All
7.4.2.2	28	2025-03-03	All
7.4.2.1	30	2024-10-09	All
7.4.2	172	2024-07-31	All
7.4.1.1	12	2024-04-15	All

Version	Build	Date	Platforms
7.4.1	172	2023-12-13	All
7.4.0	81	2023-09-07	Firewall Management Center Secure Firewall 4200 series

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, see *Cisco Secure Firewall Threat Defense Compatibility Guide*.

For compatibility, see:

- *Cisco Secure Firewall Management Center Compatibility Guide*
- *Cisco Secure Firewall Threat Defense Compatibility Guide*

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 40.

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 46.

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.

Snort Features

Snort 3 is the default inspection engine for Firewall Threat Defense. Snort 3 features for Firewall Management Center deployments also apply to Firewall Device Manager, even if they are not listed as new Firewall Device Manager features. However, keep in mind that the Firewall Management Center may offer more configurable options than Firewall Device Manager.

Important Snort 2 is deprecated in Version 7.7+, and prevents Firewall Threat Defense upgrade. If you are still using Snort 2 on older devices, switch to Snort 3 for improved detection and performance.

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 7.4.8

There are no new features in this release. See Resolved Bugs in Version 7.4.8, on page 50.

Firewall Management Center Features in Version 7.4.7

Table 2: Firewall Management Center Features in Version 7.4.7

Feature	Minimum Management Center	Minimum Threat Defense	Details
Model Migration			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Migrate Firewall Management Center without upgrading first	7.4.7 (source) 10.0.0 (target)	7.3.0	You can now migrate an older Firewall Management Center to a Version 10.0+ Firewall Management Center without first upgrading the source system to the target version. **Note** Think of this process as a migration plus upgrade. Just as with regular upgrades, minimize impact by going **directly to the latest maintenance release** in your target major version. For release-specific upgrade warnings and guidelines, and for information on features and bugs with upgrade impact, see the Release Notes for Secure Firewall Threat Defense for your target version. Version restrictions: Not supported from a Version 7.6.x or 7.7.x Firewall Management Center. See: *Cisco Secure Firewall Management Center Model Migration Guide*

Firewall Management Center Features in Version 7.4.6

There are no new features in this release. See Resolved Bugs in Version 7.4.6, on page 95.

Firewall Management Center Features in Version 7.4.5

There are no new features in this release. See Resolved Bugs in Version 7.4.5, on page 95.

Firewall Management Center Features in Version 7.4.4

Due to CSCws69719, Version 7.4.4 for the Firewall Management Center was deferred on 202-10-13 and is no longer available for download. If you downloaded it, do not use it. If you are running this version, upgrade.

There are no new features in this release. See Resolved Bugs in Version 7.4.4, on page 96.

Firewall Management Center Features in Version 7.4.3

Table 3: Firewall Management Center Features in Version 7.4.3

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 7.4.3 also has: • New Cisco AMP cloud connection method. Upgrade impact. (7.0.7) • Deprecated Cisco AMP Cloud connection backups. (7.0.7) • Cisco Security Cloud regions: India and Australia. (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) • Firewall Threat Defense and chassis upgrade wizards optimized for lower resolution screens. (7.2.10)
Platform			
DC power supply for the Secure Firewall 4200	7.4.3 7.6.2 7.7.0	7.4.3 7.6.2 7.7.0	The FPR4200-PWR-DC for Secure Firewall 4200 is a 1500 W DC power supply. The dual power supply modules can supply up to 1500 W power across the input voltage range (48 VDC to 60 VDC). The load is shared when both power supply modules are plugged in and running at the same time.
Device Management			
IMDSv2 support for AWS deployments.	7.4.3 7.6.0	7.4.3 7.6.0	Firewall Threat Defense and Firewall Management Center virtual for AWS now support Instance Metadata Service Version 2 (IMDSv2), a security improvement over IMDSv1. When you enable the instance metadata service on AWS, IMDSv2 Optional mode is still the default, but we recommend you choose IMDSv2 Required. We also recommend you switch your upgraded instances. Platform restrictions: Not available for Firewall Management Center Virtual 300 See: Secure Firewall Threat Defense Virtual getting started guides and *Cisco Secure Firewall Management Center Virtual Getting Started Guide*
Health Monitoring			
Independently configure health monitoring for physical and subinterfaces.	7.4.3 7.6.1 7.7.0	Any	You can now disable health monitoring for a physical interface while continuing to monitor and receive health alerts for its subinterfaces. You can disable alerts permanently or temporarily. To do this, configure the device for health monitoring exclusion, edit that configuration to enable module-level exclusion, and finally configure exclusion settings for the Interface Settings health module. New/modified screens: **System** (⚙) > **Health** > **Exclude** See: Health

Feature	Minimum Management Center	Minimum Threat Defense	Details
View health status for devices in leaf domains while logged into the parent domain.	7.4.3 7.6.1 7.7.0	Any	In a multidomain deployment, you can now view health status for devices in leaf domains while logged into the parent domain. See: Health
Performance			
Faster failover for high availability Firewall Threat Defense.	7.4.3 7.6.4 7.7.0	7.4.3 7.6.4 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
Integrations			
Umbrella integration with Firewall Management Center over a proxy.	7.4.3 7.6.1 7.7.10	Any	Umbrella integration with Firewall Management Center now works over a proxy. See: Configuring the Umbrella DNS Connector for Cisco Secure Firewall Management Center

Firewall Management Center Features in Version 7.4.2

Table 4: Firewall Management Center Features in Version 7.4.2

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.4.2 also has: • VMware vSphere/VMware ESXi 8.0 support. (7.2.9) • Asymmetric traffic handling. Upgrade impact. (7.2.9)
Platform			
Firewall Management Center Virtual 300 for Azure.	7.4.2 7.6.0	Any	We introduced the Firewall Management Center Virtual 300 for Azure. It can manage up to 300 devices, and high availability is supported. Migration from the FMCv25 for Azure is also supported. See: *Cisco Secure Firewall Management Center Virtual Getting Started Guide* and *Cisco Secure Firewall Management Center Model Migration Guide*
High Availability: Management Center			

Feature	Minimum Management Center	Minimum Threat Defense	Details
High availability for Firewall Management Center Virtual for Azure.	7.4.2 7.6.0	Any	We now support high availability for Firewall Management Center Virtual for Azure. In a Firewall Threat Defense deployment, you need two identically licensed Firewall Management Centers, as well as one Firewall Threat Defense entitlement for each managed device. For example, to manage 10 devices with an FMCv10 high availability pair, you need two FMCv10 entitlements and 10 Firewall Threat Defense entitlements. If you are managing Version 7.0.x Classic devices only (NGIPSv or ASA FirePOWER), you do not need FMCv entitlements. Platform restrictions: Not supported with FMCv2 See: *Cisco Secure Firewall Management Center Virtual Getting Started Guide* and High Availability

Firewall Management Center Features in Version 7.4.1

Table 5: Firewall Management Center Features in Version 7.4.1

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 7.4.1 also has: • Support for Firewall Threat Defense on all device platforms supported in Version 7.3, and also on the Firepower 1010E (last supported in 7.2). • Updated web analytics provider. Upgrade impact. (7.0.6) • Management center detects interface sync errors. Upgrade impact. (7.2.5) • Configure DHCP relay trusted interfaces from the Firewall Management Center web interface. Upgrade impact. (7.2.6) • Create network groups while editing NAT rules. (7.2.6) • Single backup file for high availability Firewall Management Centers. (7.2.6) • Open the packet tracer from the unified event viewer. (7.2.6) • Health alerts for excessive disk space used by deployment history (rollback) files. (7.2.6) • Health alerts for NTP sync issues. (7.2.6) • View and generate reports on configuration changes since your last deployment. (7.2.6) • Set the number of deployment history files to retain for device rollback. (7.2.6) • Improved upgrade starting page and package management. (7.2.6) • Enable revert from the Firewall Threat Defense upgrade wizard. (7.2.6) • View detailed upgrade status from the Firewall Threat Defense upgrade wizard. (7.2.6) • Suggested release notifications. (7.2.6) • New upgrade wizard for the Firewall Management Center. (7.2.6) • Hotfix high availability Firewall Management Centers without pausing synchronization. (7.2.6) • Updated internet access requirements for direct-downloading software upgrades. Upgrade impact. (7.2.6) • Enable/disable access control object optimization. (7.2.6) • Cluster control link ping tool. (7.2.6) • Set the frequency of Snort 3 core dumps. (7.2.6) • Capture dropped packets with the Secure Firewall 3100/4200. (7.2.6)

Feature	Minimum Management Center	Minimum Threat Defense	Details
Platform			
Network modules for the Secure Firewall 3130 and 3140.	7.4.1	7.4.1	The Secure Firewall 3130 and 3140 now support these network modules: • 2-port 100G QSFP+ network module (FPR3K-XNM-2X100G) See: *Cisco Secure Firewall 3100 Series Hardware Installation Guide*
Optical transceivers for Firepower 9300 network modules.	7.4.1	7.4.1	The Firepower 9300 now supports these optical transceivers: • QSFP-40/100-SRBD • QSFP-100G-SR1.2 • QSFP-100G-SM-SR On these network modules: • FPR9K-NM-4X100G • FPR9K-NM-2X100G • FPR9K-DNM-2X100G See: *Cisco Firepower 9300 Hardware Installation Guide*
Performance profile support for the Secure Firewall 3100.	7.4.1	7.4.1	The performance profile settings available in the platform settings policy now apply to the Secure Firewall 3100. Previously, this feature was supported on the Firepower 4100/9300, the Secure Firewall 4200, and on Firewall Threat Defense Virtual. See: Platform Settings
Interfaces			
Deploy without the diagnostic interface on Firewall Threat Defense Virtual for Azure and GCP.	7.4.1	7.4.1	You can now deploy without the diagnostic interface on Firewall Threat Defense Virtual for Azure and GCP. Previously, we required one management, one diagnostic, and at least two data interfaces. New interface requirements are: • Azure: one management, two data (max eight) • GCP: one management, three data (max eight) Restrictions: This feature is supported for new deployments only. It is not supported for upgraded devices. See: Secure Firewall Threat Defense Virtual getting started guides
Device Management			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Inspect and protect traffic through an Azure Virtual WAN hub.	7.4.1	7.4.1	You can now use Firewall Threat Defense Virtual for Azure to inspect and protect traffic through a Microsoft Azure Virtual WAN hub. This integration allows you to consistently and easily apply security policies and configurations across all spokes in the hub, and to leverage built-in scalability and load balancer capabilities for optimal performance. See: Secure Firewall Threat Defense Virtual getting started guides
Device management services supported on user-defined VRF interfaces.	7.4.1	Any	Device management services configured in the Firewall Threat Defense platform settings (NetFlow, SSH access, SNMP hosts, syslog servers) are now supported on user-defined Virtual Routing and Forwarding (VRF) interfaces. Platform restrictions: Not supported with container instances or clustered devices. See: Platform Settings
High Availability/Scalability: Firewall Threat Defense			
Multi-instance mode for the Secure Firewall 3100.	7.4.1	7.4.1	You can deploy the Secure Firewall 3100 as a single device (*appliance mode*) or as multiple container instances (*multi-instance mode*). In multi-instance mode, you can deploy multiple container instances on a single chassis that act as completely independent devices. Note that in multi-instance mode, you upgrade the operating system and the firmware (*chassis upgrade*) separately from the container instances (*Firewall Threat Defense upgrade*). New/modified screens: • **Devices** > **Device Management** > **Add** > **Chassis** • **Devices** > **Device Management** > **Device** > **Chassis Manager** • **Devices** > **Platform Settings** > **New Policy** > **Chassis Platform Settings** • **Devices** > **Chassis Upgrade** New/modified Firewall Threat Defense CLI commands: **configure multi-instance network ipv4**, **configure multi-instance network ipv6** New/modified FXOS CLI commands: **create device-manager**, **set deploymode** Platform restrictions: Not supported on the Secure Firewall 3105. See: Multi-Instance Mode for the Secure Firewall 3100 and Secure Firewall Threat Defense upgrade guides for Firewall Management Center
16-node clusters for Firewall Threat Defense Virtual for VMware and KVM.	7.4.1	7.4.1	You can now configure 16-node clusters for Firewall Threat Defense Virtual for VMware and Firewall Threat Defense Virtual for KVM. See: Clustering for Firewall Threat Defense Virtual in a Private Cloud

Feature	Minimum Management Center	Minimum Threat Defense	Details
Target failover for clustered Firewall Threat Defense Virtualdevices for AWS.	7.4.1	7.4.1	You can now configure target failover for clustered Firewall Threat Defense Virtual for AWS using the AWS Gateway Load Balancer (GWLB). Platform restrictions: Not available with five and ten-device licenses. See: Clustering for Firewall Threat Defense Virtual in a Public Cloud
Detect configuration mismatches in Firewall Threat Defense high availability pairs.	7.4.1	7.4.1	You can now use the CLI to detect configuration mismatches in Firewall Threat Defense high availability pairs. New/modified CLI commands: **show failover config-sync error**, **show failover config-sync stats** See: High Availability and *Cisco Secure Firewall Threat Defense Command Reference*
High Availability: Management Center			
Firewall Management Center high availability synchronization enhancements.	7.4.1	Any	Firewall Management Center high availability (HA) includes the following synchronization enhancements: • Large configuration history files can cause synchronization to fail in high-latency networks. To prevent this from happening, the device configuration history files are now synchronized in parallel with other configuration data. This enhancement also reduces the synchronization time. • The Firewall Management Center now monitors the configuration history file synchronization process and displays a health alert if the synchronization times out. New/modified screens: You can view these alerts on the following screens: • **Notifications** > **Message Center** > **Health** • **Integration** > **Other Integrations** > **High Availability** > **Status** (under **Summary**) See: High Availability
SD-WAN			
Application monitoring on the SD-WAN Summary dashboard.	7.4.1	7.4.1	You can now monitor WAN interface application performance on the SD-WAN Summary dashboard. New/modified screens: **Overview** > **SD-WAN Summary** > **Application Monitoring** See: VPN Monitoring and Troubleshooting
VPN			

Feature	Minimum Management Center	Minimum Threat Defense	Details
IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100.	7.4.1	7.4.1	**Upgrade impact. Qualifying connections start being offloaded.** On the Secure Firewall 3100, qualifying IPsec connections through the VTI loopback interface are now offloaded by default. Previously, this feature was only supported on physical interfaces. This feature is automatically enabled by the upgrade. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command. See: VPN Overview
Crypto debugging enhancements for the Secure Firewall 3100 and Firepower 4100/9300.	7.4.1	7.4.1	The crypto debugging enhancements introduced in Version 7.4.0 now apply to the Secure Firewall 3100 and the Firepower 4100/9300. Previously, they were only supported on the Secure Firewall 4200. See: Decryption Rules
View details of the VTIs in route-based VPNs.	7.4.1	Any	You can now view the details of route-based VPNs' virtual tunnel interfaces (VTI) on your managed devices. You can also view details of all the dynamically created virtual access interfaces of the dynamic VTIs. New/modified screens: **Device** > **Device Management** > Edit a device > **Interfaces** > **Virtual Tunnels** tab. See: Site-to-Site VPNs
Support for RSA PSS-based certificate	7.4.1	7.4.1	You can now use certificates signed with RSA Probabilistic Signature Scheme (RSA-PSS) method.
Routing			
Configure BFD routing on IS-IS interfaces with FlexConfig.	7.4.1	7.4.1	You can now use FlexConfig to configure Bidirectional Forwarding Detection (BFD) routing on physical, subinterface, and EtherChannel IS-IS interfaces. See: Guidelines for BFD Routing
Access Control: Threat Detection and Application Identification			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Zero trust access enhancements.	7.4.1	7.4.1 with Snort 3	Firewall Management Center now includes the following zero trust access enhancements: • You can configure source NAT for an application. The configured network object or object group translates the incoming request's public network source IP address to a routable IP address inside the application network. • You can troubleshoot the zero trust configuration issues using the diagnostics tool. New/modified screens: **Policies** > **Access Control** > **Zero Trust Application** New/modified CLI commands: **show running-config zero-trust**, **show zero-trust statistics** See: Zero Trust Access, *Cisco Secure Firewall Threat Defense Command Reference*
CIP detection.	7.4.1	7.4.1 with Snort 3	You can now detect and handle Common Industrial Protocol (CIP) by using CIP and Ethernet/IP (ENIP) application conditions in your security policies. See: Access Control Rules
CIP safety detection.	7.4.1	7.4.1 with Snort 3	CIP Safety is a CIP extension that enables the safe operation of industrial automation applications. The CIP inspector can now detect the CIP Safety segments in the CIP traffic. To detect and take action on the CIP Safety segments, enable the CIP inspector in the Firewall Management Center's network Analysis policy and assign it to an access control policy. New/modified screens: **Policies** > **Access Control** > Edit a policy > **Add Rule** > **Applications** tab > Search for CIP Safety in the search box. See: Cisco Secure Firewall Management Center Snort 3 Configuration Guide
Access Control: Identity			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Captive portal support for multiple Active Directory realms (realm sequences).	7.4.1	7.4.1	**Upgrade impact. Update custom authentication forms.** You can configure active authentication for either an LDAP realm; or a Microsoft Active Directory realm or a realm sequence. In addition, you can configure a passive authentication rule to fall back to active authentication using either a realm or a realm sequence. You can optionally share sessions between managed devices that share the same identity policy in access control rules. In addition, you have the option to require users to authenticate again when they access the system using a different managed device than they accessed previously. If you use the HTTP Response Page authentication type, after you upgrade Firewall Threat Defense, you must add **`<select name="realm" id="realm"></select>`** to your custom authentication form. This allows the user to choose between realms. Restrictions: Not supported with Microsoft Azure Active Directory. New/modified screens: • **Policies** > **Identity** > **(edit policy)** > **Active Authentication** > **Share active authentication sessions across firewalls** • **Identity policy** > **(edit)** > **Add Rule** > **Passive Authentication** > **Realms & Settings** > **Use active authentication if passive or VPN identity cannot be established** • **Identity policy** > **(edit)** > **Add Rule** > **Active Authentication** > **Realms & Settings** > **Use active authentication if passive or VPN identity cannot be established** See: User Control with Captive Portal
Share captive portal active authentication sessions across firewalls.	7.4.1	7.4.1	Determines whether or not users are required to authenticate when their authentication session is sent to a different managed device than one they previously connected to. If your organization requires users to authenticate every time they change locations or sites, you should *disable* this option. • (Default.) Enable to allow users to authenticate with any managed device associated with the active authentication identity rule. • Disable to require the user to authenticate with a different managed device, even if they have already authenticated with another managed device to which the active authentication rule is deployed. New/modified screens: **Policies** > **Identity** > **(edit policy)** > **Active Authentication** > **Share active authentication sessions across firewalls** See: User Control with Captive Portal

Feature	Minimum Management Center	Minimum Threat Defense	Details
Merge downloadable access control list with a Cisco attribute-value pair ACL for RADIUS identity sources, using the Firewall Management Center web interface.	7.4.1	Any	**Upgrade impact. Redo any related FlexConfigs after upgrade.** New/modified screens: **Objects** > **Object Management** > **AAA Server** > **RADIUS Server Group** > **Add RADIUS Server Group** > **Merge Downloadable ACL with Cisco AV Pair ACL** New CLI commands: • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl after-avpair** • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl before-avpair** See: Object Management
Health Monitoring			
Chassis-level health alerts for the Firepower 4100/9300.	7.4.1	Any with FXOS 2.14.1	You can now view chassis-level health alerts for Firepower 4100/9300 by registering the chassis to the Firewall Management Center as a read-only device. You must also enable the Firewall Threat Defense Platform Faults health module and apply the health policy. The alerts appear in the Message Center, the health monitor (in the left pane, under Devices, select the chassis), and in the health events view. You can also add a chassis (and view health alerts for) the Secure Firewall 3100 in multi-instance mode. For those devices, you use the Firewall Management Center to manage the chassis. But for the Firepower 4100/9300 chassis, you still must use the chassis manager or the FXOS CLI. New/modified screens: **Devices** > **Device Management** > **Add** > **Chassis** See: Device Management

Feature	Minimum Management Center	Minimum Threat Defense	Details
Improved Firewall Management Center memory usage calculation, alerting, and swap memory monitoring.	7.4.1	Any	**Upgrade impact. Memory usage alert thresholds may be lowered.** We improved the accuracy of Firewall Management Center memory usage and have lowered the default alert thresholds to 88% warning/90% critical. If your thresholds were higher than the new defaults, the upgrade lowers them automatically—you do not have to apply health policies for this change to take place. Note that the Firewall Management Center may now reboot in extremely critical system memory condition if terminating high-memory processes does not work. You can also add new swap memory usage metrics to a new or existing Firewall Management Center health dashboard. Make sure you choose the **Memory** metric group. New/modified screens: • **System** (⚙) > **Health** > **Monitoring** > **Firewall Management Center** > **Add/Edit Dashboard** > **Memory** • **System** (⚙) > **Health** > **Policy** > **Management Center Health Policy** > **Memory** See: Health
Deployment and Policy Management			
Change management.	7.4.1	Any	You can enable change management if your organization needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed. We added the **System**(⚙) > **Configuration** > **Change Management** page to enable the feature. When enabled, there is a **System**(⚙) > **Change Management Workflow** page, and a new **Ticket**(📋) quick access icon in the menu. See: Change Management
Upgrade			
Firmware upgrades included in FXOS upgrades.	7.4.1	Any	**Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.** For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1 now include firmware upgrades. If any firmware component on the device is older than the one included in the FXOS bundle, the FXOS upgrade also updates the firmware. If the firmware is upgraded, the device reboots twice—once for FXOS and once for the firmware. Just as with software and operating system upgrades, do not make or deploy configuration changes during firmware upgrade. Even if the system appears inactive, do not manually reboot or shut down during firmware upgrade. See: *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Automatically generate configuration change reports after Firewall Management Center upgrade.	7.4.1	Any	You can automatically generate reports on configuration changes after major and maintenance Firewall Management Center upgrades. This helps you understand the changes you are about to deploy. After the system generates the reports, you can download them from the Tasks tab in the Message Center. Version restrictions: Only supported for Firewall Management Center upgrades from Version 7.4.1+. Not supported for upgrades to Version 7.4.1 or any earlier version. New/modified screens: **System** > **Configuration** > **Upgrade Configuration** > **Enable Post-Upgrade Report** See: System Configuration
Administration			
Erase the hard drives on a hardware Firewall Management Center.	7.4.1	Any	You can use the Firewall Management Center CLI to reboot and permanently erase its own hard drive data. After the erase is completed, you can install a fresh software image. New/modified CLI commands: **secure erase** See: Secure Firewall Management Center Command Line Reference
Troubleshooting			
Troubleshooting file generation and download available from Device and Cluster pages.	7.4.1	7.4.1	You can generate and download troubleshooting files for each device on the Device page and also for all cluster nodes on the Cluster page. For a cluster, you can download all files as a single compressed file. You can also include cluster logs for the cluster for cluster nodes. You can alternatively trigger file generation from the **Devices** > **Device Management** > **More** > **Troubleshoot Files** menu. New/modified screens: • **Devices** > **Device Management** > **Device** > **General** • **Devices** > **Device Management** > **Cluster** > **General** See: Device Management
Automatic generation of a troubleshooting file on a node when it fails to join the cluster.	7.4.1	7.4.1	If a node fails to join the cluster, a troubleshooting file is automatically generated for the node. You can download the file from **Tasks** or from the **Cluster** page.
View CLI output for a device or device cluster.	7.4.1	Any	You can view a set of pre-defined CLI outputs that can help you troubleshoot the device or cluster. You can also enter any **show** command and see the output. New/modified screens: **Devices** > **Device Management** > **Cluster** > **General** See: Device Management

Feature	Minimum Management Center	Minimum Threat Defense	Details
Quick recovery after data plane failure for the Firepower 1000/2100 and Firepower 4100/9300.	7.4.1	7.4.1	If the data plane process crashes, the system now reloads only the data plane process instead of rebooting the device. Along with the data plane process reload, Snort and a few other processes also get reloaded. However, if the data plane process crashes during bootup, the device follows the normal reload/reboot sequence, which helps avoid a reload process loop from occurring. This feature is enabled by default for both new and upgraded devices. To disable it, use FlexConfig. New/modified CLI commands: **data-plane quick-reload**, **no data-plane quick-reload**, **show data-plane quick-reload status** Supported platforms: Firepower 1000/2100, Firepower 4100/9300 Platform restrictions: Not supported in multi-instance mode. See: *Cisco Secure Firewall Threat Defense Command Reference* and Cisco Secure Firewall ASA Series Command Reference.
Deprecated Features			
Deprecated: Health alerts for `frequent drain of events`.	7.4.1	7.4.1	The Disk Usage health module no longer alerts with `frequent drain of events`. You may continue to see these alerts after Firewall Management Center upgrade until you either deploy health policies to managed devices (stops the display of alerts) or upgrade devices to Version 7.4.1+ (stops the sending of alerts). See: Troubleshooting
Deprecated: VPN Tunnel Status health module.	7.4.1	Any	We deprecated the VPN Tunnel Status health module. Use the VPN dashboards instead. See: VPN Monitoring and Troubleshooting
Deprecated: Merging downloadable access control list with a Cisco attribute-value pair ACL for RADIUS identity sources with FlexConfig.	7.4.1	Any	**Upgrade impact. Redo any related FlexConfigs after upgrade.** This feature is now supported in the Firewall Management Center web interface.

Firewall Management Center Features in Version 7.4.0



Note Version 7.4.0 is available *only* on the Firewall Management Center and the Secure Firewall 4200. A Version 7.4.0 Firewall Management Center can manage older versions of other device models, but you must use a Secure Firewall 4200 for features that require Firewall Threat Defense 7.4.0. Support for all other device platforms resumes in Version 7.4.1.

Table 6: Firewall Management Center Features in Version 7.4.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.4.0 also has: • Smaller VDB for lower memory Snort 2 devices. (7.0.6) • Access control performance improvements (object optimization). Upgrade impact. (7.0.6) • Deprecated: `high unmanaged disk usage` alerts. (7.0.6) • Reduced "false failovers" for Firewall Threat Defense high availability. (7.2.6) • Secure Firewall 3105. (7.3.1)
Platform			
Firewall Management Center 1700, 2700, 4700.	7.4.0	Any	We introduced the Firewall Management Center 1700, 2700, and 4700, which can manage up to 300 devices. Firewall Management Center high availability is supported. See: *Cisco Secure Firewall Management Center 1700, 2700, and 4700 Getting Started Guide*
Firewall Management Center Virtual for Microsoft Hyper-V.	7.4.0	Any	We introduced Firewall Management Center Virtual for Microsoft Hyper-V, which can manage up to 25 devices. Firewall Management Center high availability is supported. See: *Cisco Secure Firewall Management Center Virtual Getting Started Guide*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Secure Firewall 4200.	7.4.0 m	7.4.0	We introduced the Secure Firewall 4215, 4225, and 4245. You must manage these devices with a Firewall Management Center. They do not support device manager. These devices support the following new network modules: • 2-port 100G QSFP+ network module (FPR4K-XNM-2X100G) • 4-port 200G QSFP+ network module (FPR4K-XNM-4X200G) See: *Cisco Secure Firewall 4200 Series Hardware Installation Guide*
Performance profile support for the Secure Firewall 4200.	7.4.0	7.4.0	The performance profile settings available in the platform settings policy now apply to the Secure Firewall 4200. Previously, this feature was supported only on the Firepower 4100/9300 and on Firewall Threat Defense Virtual. See: Platform Settings
Platform Migration			
Migrate Firepower 1000/2100 to Secure Firewall 3100.	7.4.0	Any	You can now easily migrate configurations from the Firepower 1000/2100 to the Secure Firewall 3100. New/modified screens: **Devices** > **Device Management** > **Migrate** Platform restrictions: Migration not supported from the Firepower 1010 or 1010E. See: Device Management
Migrate Firepower Management Center 4600 to Secure Firewall Management Center for AWS.	7.4.0	Any	You can migrate from Firepower Management Center 4600 to Secure Firewall Management Center Virtual for AWS with a 300-device license. See: *Cisco Secure Firewall Management Center Model Migration Guide*
Migrate Firepower Management Center 1600/2600/4600 to Secure Firewall Management Center 1700/2700/4700.	7.4.0	Any	You can migrate from Firepower Management Center 1600/2600/4600 to Secure Firewall Management Center 1700/2700/4700. See: *Cisco Secure Firewall Management Center Model Migration Guide*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Migrate Firepower Management Center 1000/2500/4500 to Secure Firewall Management Center 1700/2700/4700.	7.4.0 only	7.0.0	You can migrate a Firepower Management Center 1000/2500/4500 to a Version 7.4.0 Secure Firewall Management Center 1700/2700/4700. To migrate, you must *temporarily* upgrade the old Firewall Management Center from Version 7.0 to Version 7.4.0. **Important** Migration is supported to/from Version 7.4.0 only, and Version 7.4.0 is only supported on the 1000/2500/4500 during the migration process. Do not upgrade the source or target to later maintenance releases. You should minimize the time between Firewall Management Center upgrade and device migration. To summarize the migration process: **1.** Prepare for upgrade and migration. Read, understand, and meet all the prerequisites outlined in the release notes, upgrade guides, and migration guide. Make sure the old Firewall Management Center is ready to go: freshly deployed, fully backed up, all appliances in good health, etc. You should also set up the new Firewall Management Center. **2.** Upgrade the old Firewall Management Center and all its managed devices to at least Version 7.0.0 (7.0.5 recommended). If you are already running the minimum version, you can skip this step. **3.** Upgrade the old Firewall Management Center to Version 7.4.0. Unzip (but do not untar) the upgrade package before uploading it to the Firewall Management Center. Download from: Special Release. **4.** Migrate the Firewall Management Center as described in the model migration guide. **5.** Verify migration success. If the migration does not function to your expectations and you want to switch back, note that Version 7.4 is unsupported for general operations on the 1000/2500/4500. To return the old Firewall Management Center to a supported version you must reimage back to Version 7.0, restore from backup, and reregister devices. See: • Release Notes for Secure Firewall Threat Defense • Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 • *Cisco Secure Firewall Management Center Model Migration Guide* If you have questions or need assistance at any point in the migration process, contact Cisco TAC.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Migrate devices from Firepower Management Center 1000/2500/4500 to .	7.4.0 only	7.0.3	

Feature	Minimum Management Center	Minimum Threat Defense	Details
			You can migrate devices from Firepower Management Center 1000/2500/4500 to . To migrate devices, you must *temporarily* upgrade the on-prem Firewall Management Center from Version 7.0.3 (7.0.5 recommended) to Version 7.4.0. This temporary upgrade is required because Version 7.0 Firewall Management Centers do not support device migration to the cloud. Additionally, only standalone and high availability Firewall Threat Defense running Version 7.0.3+ (7.0.5 recommended) are eligible for migration. Cluster migration is not supported at this time. **Important** Version 7.4.0 is only supported on the 1000/2500/4500 during the migration process. You should minimize the time between Firewall Management Center upgrade and device migration. To summarize the migration process: **1.** Prepare for upgrade and migration. Read, understand, and meet all the prerequisites outlined in the release notes, upgrade guides, and migration guide. Before you upgrade, it is especially important that the on-prem Firewall Management Center is "ready to go," that is, managing only the devices you want to migrate, configuration impact assessed (such as VPN impact), freshly deployed, fully backed up, all appliances in good health, and so on. You should also provision, license, and prepare the cloud tenant. This must include a strategy for security event logging; you cannot retain the on-prem Firewall Management Center for analytics because it will be running an unsupported version. **2.** Upgrade the on-prem Firewall Management Center and all its managed devices to at least Version 7.0.3 (Version 7.0.5 recommended). If you are already running the minimum version, you can skip this step. **3.** Upgrade the on-prem Firewall Management Center to Version 7.4.0. Unzip (but do not untar) the upgrade package before uploading it to the Firewall Management Center. Download from: Special Release. **4.** Onboard the on-prem Firewall Management Center to CDO. **5.** Migrate all devices from the on-prem Firewall Management Center to the as described in the migration guide. When you select devices to migrate, make sure you choose **Delete FTD from On-Prem FMC**. Note that the device is not fully deleted unless you commit the changes or 14 days pass. **6.** Verify migration success. If the migration does not function to your expectations, you have 14 days

Feature	Minimum Management Center	Minimum Threat Defense	Details
			to switch back or it is committed automatically. However, note that Version 7.4.0 is unsupported for general operations. To return the on-prem Firewall Management Center to a supported version you must remove the re-migrated devices, re image back to Version 7.0.x, restore from backup, and reregister the devices. See: • Release Notes for Secure Firewall Threat Defense • Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 • Migrate On-Premises Management Center Managed Secure Firewall Threat Defense to Cloud-Delivered Firewall Management Center If you have questions or need assistance at any point in the migration process, contact Cisco TAC.
Device Management			
Zero-Touch Provisioning to register the Firepower 1000/2100 and Secure Firewall 3100 to the Firewall Management Center using a serial number.	7.4.0	Mgmt. center *is* publicly reachable: 7.2.0 Mgmt. center *is not* publicly reachable: 7.2.4, 7.4.1	Zero-Touch Provisioning (also called low-touch provisioning) lets you register Firepower 1000/2100 and Secure Firewall 3100 devices to the Firewall Management Center by serial number without having to perform any initial setup on the device. The Firewall Management Center integrates with SecureX and Security Cloud Control for this functionality. New/modified screens: **Devices** > **Device Management** > **Add** > **Device** > **Serial Number** See: Add a Device to the Management Center Using the Serial Number (Low-Touch Provisioning)
Interfaces			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Merged management and diagnostic interfaces.	7.4.0	7.4.0	**Upgrade impact. Merge interfaces after upgrade.** For new devices using 7.4 and later, you cannot use the legacy diagnostic interface. Only the merged management interface is available. If you upgraded to 7.4 or later and: • You did not have any configuration for the diagnostic interface, then the interfaces will merge automatically. • You have configuration for the diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate diagnostic interface. Note that support for the diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including Management) in the configuration. For platform settings, this means: • You can no longer enable HTTP, ICMP, or SMTP for diagnostic. • For SNMP, you can allow hosts on management instead of diagnostic. • For Syslog servers, you can reach them on management instead of diagnostic. • If Platform Settings for syslog servers or SNMP hosts specify the diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices. • DNS lookups no longer fall back to the management-only routing table if you do not specify interfaces. New/modified screens: **Devices** > **Device Management** > **Interfaces** New/modified commands: **show management-interface convergence** See: Interface Overview

Feature	Minimum Management Center	Minimum Threat Defense	Details
VXLAN VTEP IPv6 support.	7.4.0	7.4.0	You can now specify an IPv6 address for the VXLAN VTEP interface. IPv6 is not supported for the Firewall Threat Defense Virtual cluster control link or for Geneve encapsulation. New/modified screens: • **Devices** > **Device Management** > **Edit Device** > **VTEP** > **Add VTEP** • **Devices** > **Device Management** > **Edit Devices** > **Interfaces** > **Add Interfaces** > **VNI Interface** See: Regular Firewall Interfaces
Loopback interface support for BGP and management traffic.	7.4.0	7.4.0	You can now use loopback interfaces for AAA, BGP, DNS, HTTP, ICMP, IPsec flow offload, NetFlow, SNMP, SSH, and syslog. New/modified screens: **Devices** > **Device Management** > Edit device > **Interfaces** > **Add Interfaces** > **Loopback Interface** See: Regular Firewall Interfaces
Loopback and management type interface group objects.	7.4.0	7.4.0	You can create interface group objects with only management-only or loopback interfaces. You can use these groups for management features such as DNS servers, HTTP access, or SSH. Loopback groups are available for any feature that can utilize loopback interfaces. However, it's important to note that DNS does not support management interfaces. New/modified screens: **Objects** > **Object Management** > **Interface** > **Add** > **Interface Group** See: Object Management
High Availability/Scalability: Threat Defense			
Manage Firewall Threat Defense high availability pairs using a data interface.	7.4.0	7.4.0	Firewall Threat Defense high availability now supports using a regular data interface for communication with the Firewall Management Center. Previously, only standalone devices supported this feature. See: Device Management
SD-WAN			
WAN summary dashboard.	7.4.0	7.2.0	The WAN Summary dashboard provides a snapshot of your WAN devices and their interfaces. It provides insight into your WAN network and information about device health, interface connectivity, application throughput, and VPN connectivity. You can monitor the WAN links and take proactive and prompt recovery measures. New/modified screens: **Overview** > **WAN Summary** See: VPN Monitoring and Troubleshooting

Feature	Minimum Management Center	Minimum Threat Defense	Details
Policy-based routing using HTTP path monitoring.	7.4.0	7.2.0	Policy-based routing (PBR) can now use the performance metrics (RTT, jitter, packet-lost, and MOS) collected by path monitoring through HTTP client on the application domain rather than the metrics on a specific destination IP. HTTP-based application monitoring option is enabled by default for the interface. You can configure a PBR policy with match ACL having the monitored applications and interface ordering for path determination. New/modified screens: **Devices** > **Device Management** > Edit device > Edit interface > **Path Monitoring** > **Enable HTTP based Application Monitoring** check box. Platform restrictions: Not supported for clustered devices. See: Policy Based Routing
Policy-based routing with user identity and SGTs.	7.4.0	7.4.0	**Upgrade impact. Check SGT propagation before device upgrade.** You can now classify network traffic based on users, user groups, and SGTs in PBR policies. Select the identity and SGT objects while defining the extended ACLs for the PBR policies. Note that as a result of how this feature was implemented, Firewall Threat Defense can now add egress SGTs to traffic if the egress interface is configured to propagate SGTs. This can happen with ISE integration even if you do not configure policy-based routing. Starting with Version 7.4.0, the **Propagate Security Group Tag** option is disabled by default for new interfaces. But because upgrade respects your current settings, this option may be enabled for existing interfaces. **Important** If you have configured an ISE identity source, before you upgrade, check the **Propagate Security Group Tag** option on your devices' physical, redundant, and subinterfaces and disable it if necessary. If downstream devices are not configured to handle the tags, you could experience traffic loss. New/modified screens: **Objects** > **Object Management** > **Access List** > **Extended** > Add/Edit Extended Access List > Add/Edit Extended Access List Entry > **Users** and **Security Group Tag** See: Object Management
VPN			
IPsec flow offload on the VTI loopback interface for the Secure Firewall 4200.	7.4.0	7.4.0	On the Secure Firewall 4200, qualifying IPsec connections through the VTI loopback interface are offloaded by default. Previously, this feature was supported for physical interfaces on the Secure Firewall 3100. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command. Other requirements: FPGA firmware 6.2+ See: VPN Overview

Feature	Minimum Management Center	Minimum Threat Defense	Details
Crypto debugging enhancements for the Secure Firewall 4200.	7.4.0	7.4.0	We made the following enhancements to crypto debugging: • The crypto archive is now available in text and binary formats. • Additional SSL counters are available for debugging. • Remove stuck encrypt rules from the ASP table without rebooting the device. New/modified CLI commands: **show counters** See: Decryption Rules
VPN: Remote Access			
Customize Secure Client messages, icons, images, and connect/disconnect scripts.	7.4.0	7.1.0	You can now customize Secure Client and deploy these customizations to the VPN headend. The following are the supported Secure Client customizations: • GUI text and messages • Icons and images • Scripts • Binaries • Customized Installer Transforms • Localized Installer Transforms Firewall Threat Defense distributes these customizations to the endpoint when an end user connects from the Secure Client. New/modified screens: • **Objects** > **Object Management** > **VPN** > **Secure Client Customization** • **Devices** > **Remote Access** > Edit VPN policy > **Advanced** > **Secure Client Customization** See: Remote Access VPN
VPN: Site to Site			
Easily view IKE and IPsec session details for VPN nodes.	7.4.0	Any	You can view the IKE and IPsec session details of VPN nodes in a user-friendly format in the Site-to-Site VPN dashboard. New/modified screens: **Overview** > **Site to Site VPN** > Under the Tunnel Status widget, hover over a topology, click **View**, and then click the **CLI Details** tab. See: Site-to-Site VPNs

Feature	Minimum Management Center	Minimum Threat Defense	Details
Site-to-site VPN information in connection events.	7.4.0	7.4.0 with Snort 3	Connection events now contain three new fields: Encrypt Peer, Decrypt Peer, and VPN Action. For policy-based and route-based site-to-site VPN traffic, these fields indicate whether a connection was encrypted or decrypted (or both, for transiting connections), and who by. New/modified screens: **Analysis** > **Connections** > **Events** > **Table View of Events** See: VPN Monitoring and Troubleshooting
Easily exempt site-to-site VPN traffic from NAT translation.	7.4.0	Any	We now make it easier to exempt site-to-site VPN traffic from NAT translation. New/modified screens: • Enable NAT exemptions for an endpoint: **Devices** > **VPN** > **Site To Site** > **Add/Edit Site to Site VPN** > **Add/Edit Endpoint** > **Exempt VPN traffic from network address translation** • View NAT exempt rules for devices that do not have a NAT policy: **Devices** > **NAT** > **NAT Exemptions** • View NAT exempt rules for a single device: **Devices** > **NAT** > **Threat Defense NAT Policy** > **NAT Exemptions** See: Network Address Translation
Routing			
Configure graceful restart for BGP on IPv6 networks.	7.4.0	7.3.0	You can now configure BGP graceful restart for IPv6 networks on managed devices version 7.3 and later. New/modified screens: **Devices** > **Device Management** > Edit device > **Routing** > **BGP** > **IPv6** > **Neighbor** > Add/Edit Neighbor. See: BGP
Virtual routing with dynamic VTI.	7.4.0	7.4.0	You can now configure a virtual router with a dynamic VTI for a route-based site-to-site VPN. New/modified screens: **Devices** > **Device management** > **Edit Device** > **Routing** > **Virtual Router Properties** > **Dynamic VTI interfaces under Available Interfaces** Platform restrictions: Supported only on native mode standalone or high availability devices. Not supported for container instances or clustered devices. See: Virtual Routers
Access Control: Threat Detection and Application Identification			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Clientless zero-trust access.	7.4.0	7.4.0 with Snort 3	Zero Trust Access allows you to authenticate and authorize access to protected web based resources, applications, or data from inside (on-premises) or outside (remote) the network using an external SAML Identity Provider (IdP) policy. The configuration consists of a Zero Trust Application Policy (ZTAP), Application Group, and Applications. New/modified screens: • **Policies** > **Zero Trust Application** • **Analysis** > **Connections** > **Events** • **Overview** > **Dashboard** > **Zero Trust** New/modified CLI commands: • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics** See: Zero Trust Access
Encrypted visibility engine enhancements.	7.4.0	7.4.0 with Snort 3	Encrypted Visibility Engine (EVE) can now: • Block malicious communications in encrypted traffic based on threat score. • Determine client applications based on EVE-detected processes. • Reassemble fragmented Client Hello packets for detection purposes. New/modified screens: Use the access control policy's advanced settings to enable EVE and configure these settings. See: *Custom Snort 3 Intrusion Policies for Access Control*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Exempt specific networks and ports from bypassing or throttling elephant flows.	7.4.0	7.4.0 with Snort 3	You can now exempt specific networks and ports from bypassing or throttling elephant flows. New/modified screens: • When you configure elephant flow detection in the access control policy's advanced settings, if you enable the **Elephant Flow Remediation** option, you can now click **Add Rule** and specify traffic that you want to exempt from bypass or throttling. • When the system detects an elephant flow that is exempted from bypass or throttling, it generates a mid-flow connection event with the reason **Elephant Flow Exempted**. Platform restrictions: Not supported on the Firepower 2100 series. See: *Custom Snort 3 Intrusion Policies for Access Control*
First-packet application identification using custom application detectors.	7.4.0	7.4.0 with Snort 3	A new Lua detector API is now introduced, which maps the IP address, port, and protocol on the very first packet of a TCP session to application protocol (service AppID), client application (client AppID), and web application (payload AppID). This new Lua API *addHostFirstPktApp* is used for performance improvements, reinspection, and early detection of attacks in the traffic. To use this feature, you must upload the Lua detector by specifying the detection criteria in advanced detectors in your custom application detector. See: Application Detection
Sensitive data detection and masking.	7.4.0	7.4.0 with Snort 3	**Upgrade impact. New rules in default policies take effect.** Sensitive data such as social security numbers, credit card numbers, emails, and so on may be leaked onto the internet, intentionally or accidentally. Sensitive data detection is used to detect and generate events on possible sensitive data leakage and generates events only if there is a transfer of significant amount of Personally Identifiable Information (PII) data. Sensitive data detection can mask PII in the output of events, using built-in patterns. Disabling data masking is not supported. See: Custom Rules in Snort 3
Improved JavaScript inspection.	7.4.0	7.4.0 with Snort 3	We improved JavaScript inspection, which is done by normalizing the JavaScript and matching rules against the normalized content. See: HTTP Inspect Inspector and Cisco Secure Firewall Management Center Snort 3 Configuration Guide

Feature	Minimum Management Center	Minimum Threat Defense	Details
MITRE information in file and malware events.	7.4.0	7.4.0	The system now includes MITRE information (from local malware analysis) in file and malware events. Previously, this information was only available for intrusion events. You can view MITRE information in both the classic and unified events views. Note that the MITRE column is hidden by default in both event views. See: Network Malware Protection and File Policies and File/Malware Events and Network File Trajectory
Access Control: Identity			
Cisco Secure Dynamic Attributes Connector on the Firewall Management Center.	7.4.0	Any	You can now configure the Cisco Secure Dynamic Attributes Connector on the Firewall Management Center. Previously, it was only available as a standalone application. See: Cisco Secure Dynamic Attributes Connector
Microsoft Azure AD as a user identity source.	7.4.0	7.4.0	You can use a Microsoft Azure Active Directory (Azure AD) realm with ISE to authenticate users and get user sessions for user control. New/modified screens: • **Integration** > **Other Integrations** > **Realms** > **Add Realm** > **Azure AD** • **Integration** > **Other Integrations** > **Realms** > Actions, such as downloading users, copying, editing, and deleting Supported ISE versions: 3.0 patch 5+, 3.1 (any patch level), 3.2 (any patch level) See: Realms
Event Logging and Analysis			
Configure Firewall Threat Defense devices as NetFlow exporters from the Firewall Management Center web interface.	7.4.0	Any	**Upgrade impact. Redo FlexConfigs after upgrade.** NetFlow is a Cisco application that provides statistics on packets flows. You can now use the Firewall Management Center web interface to configure Firewall Threat Defense devices as NetFlow exporters. If you have an existing NetFlow FlexConfig and redo your configurations in the web interface, you cannot deploy until you remove the deprecated FlexConfigs. New/modified screens: **Devices** > **Platform Settings** > **Threat Defense Settings Policy** > **NetFlow** See: Platform Settings

Feature	Minimum Management Center	Minimum Threat Defense	Details
More information about "unknown" SSL actions in logged encrypted connections.	7.4.0	7.4.0	Serviceability improvements to the event reporting and decryption rule matching. • New **SSL Status** to indicate if the SSL handshake is not complete for an encrypted connection. The **SSL Status** column of the connection event displays “Unknown (Incomplete Handshake)” when the SSL handshake of the logged connection is not complete. • Subject Alternative Names (SANs) for certificates are now used when matching Certificate Authority (CA) names for improved decryption rule matching. New/modified screens: • **Analysis** > **Connections** > **Events** > **SSL Status** • **Analysis** > **Connections** > **Security-Related Events** > **SSL Status** See: Connection and Security-Related Connection Events
Health Monitoring			
Stream telemetry to an external server using OpenConfig.	7.4.0	7.4.0	You can now send metrics and health monitoring information from your Firewall Threat Defense devices to an external server (gNMI collector) using OpenConfig. You can configure either Firewall Threat Defense or the collector to initiate the connection, which is encrypted by TLS. New/modified screens: **System** (⚙) > **Health** > **Policy** > **Firewall Threat Defense Policies** > **Settings** > **OpenConfig Streaming Telemetry** See: Health
New asp drop metrics.	7.4.0	7.4.0	You can add over 600 new asp (accelerated security path) drop metrics to a new or existing device health dashboard. Make sure you choose the **ASP Drops** metric group. New/modified screens: **System** (⚙) > **Health** > **Monitor** > **Device** See: show asp drop Command Usage
Administration			
Send detailed Firewall Management Center audit logs to syslog.	7.4.0	Any	You can stream configuration changes as part of audit log data to syslog by specifying the configuration data format and the hosts. The Firewall Management Center supports backup and restore of the audit configuration log. New/modified screens: **System** (⚙) > **Configuration** > **Audit Log** > **Send Configuration Changes** See: System Configuration

Feature	Minimum Management Center	Minimum Threat Defense	Details
Granular permissions for modifying access control policies and rules.	7.4.0	Any	You can define custom user roles to differentiate between the intrusion configuration in access control policies and rules and the rest of the access control policy and rules. Using these permissions, you can separate the responsibilities of your network administration team and your intrusion administration teams. When defining user roles, you can select the **Policies** > **Access Control** > **Access Control Policy** > **Modify Access Control Policy** > **Modify Threat Configuration** option to allow the selection of intrusion policy, variable set, and file policy in a rule, the configuration of the advanced options for Network Analysis and Intrusion Policies, the configuration of the Security Intelligence policy for the access control policy, and intrusion actions in the policy default action. You can use the **Modify Remaining Access Control Policy Configuration** to control the ability to edit all other aspects of the policy. The existing pre-defined user roles that included the Modify Access Control Policy permission continue to support all sub-permissions; you need to create your own custom roles if you want to apply granular permissions. See: Users
Support for IPv6 URLs when checking certificate revocation.	7.4.0	7.4.0	Previously, Firewall Threat Defense supported only IPv4 OCSP URLs. Now, Firewall Threat Defense supports both IPv4 and IPv6 OCSP URLs. See: System Configuration and Object Management
Default NTP server updated.	7.4.0	Any	The default NTP server for new Firewall Management Center deployments changed from sourcefire.pool.ntp.org to time.cisco.com. We recommend you use the Firewall Management Center to serve time to its own devices. You can update the Firewall Management Center's NTP server on **System** (⚙) > **Configuration** > **Time Synchronization**. See: Security, Internet Access, and Communication Ports
Usability, Performance, and Troubleshooting			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Usability enhancements.	7.4.0	Any	You can now: • Manage Smart Licensing for Firewall Threat Defense clusters from **System** (⚙) > **Smart Licenses**. Previously, you had to use the Device Management page. See: Licensing • Download a report of Message Center notifications. In the Message Center, click the new **Download Report** icon, next to the **Show Notifications** slider. See: Troubleshooting • Download a report of all registered devices. On **Devices** > **Device Management**, click the new **Download Device List Report** link, at the top right of the page. See: Device Management • Clone network and port objects. In the object manager (**Objects** > **Object Management**), click the new **Clone** icon next to a port or network object. You can then change the new object's properties and save it using a new name. See: Object Management • Easily create custom health monitoring dashboards, and easily edit existing dashboards. See: Health
Specify the direction of traffic to be captured with packet capture for the Secure Firewall 4200.	7.4.0	7.4.0	On the Secure Firewall 4200, you can use a new **direction** keyword with the **capture** command. New/modified CLI commands: **capture***capture_name***switchinterface***interface_name* [**direction** { **both** | **egress** | **ingress** }] See: *Cisco Secure Firewall Threat Defense Command Reference*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Snort 3 restarts when it becomes unresponsive, which can trigger HA failover.	7.4.0	7.4.0 with Snort 3	To improve continuity of operations, an unresponsive Snort can now trigger high availability failover. This happens because Snort 3 now restarts if the process becomes unresponsive. Restarting the Snort process briefly interrupts traffic flow and inspection on the device, and in high availability deployments can trigger failover. (In a standalone deployment, interface configurations determine whether traffic drops or passes without inspection during the interruption.) This feature is enabled by default. You can use the CLI to disable it, or configure the time or number of unresponsive threads before Snort restarts. New/modified CLI commands: **configure snort3-watchdog** See: *Cisco Secure Firewall Threat Defense Command Reference*
Deprecated Features			
Deprecated: NetFlow with FlexConfig.	7.4.0	Any	You can now configure Firewall Threat Defense devices as NetFlow exporters from the Firewall Management Center web interface. If you do this, you cannot deploy until you remove any deprecated FlexConfigs. See: Platform Settings

Firewall Device Manager Features in Version 7.4.x

Note Firewall Device Manager support for Version 7.4 features begins with Version 7.4.1. This is because Version 7.4.0 is not available on any platforms that support device manager.

Table 7: Firewall Device Manager Features in Version 7.4.x

Feature	Description
Platform Features	
Network modules for the Secure Firewall 3130 and 3140.	We introduced these network modules for the Secure Firewall 3130 and 3140: • 2-port 100G QSFP+ network module (FPR3K-XNM-2X100G) See: *Cisco Secure Firewall 3100 Series Hardware Installation Guide*
IMDSv2 support for AWS deployments.	Threat defense virtual for AWS now supports Instance Metadata Service Version 2 (IMDSv2), a security improvement over IMDSv1. When you enable the instance metadata service on AWS, IMDSv2 Optional mode is still the default, but we recommend you choose IMDSv2 Required. We also recommend you switch your upgraded instances. See: Secure Firewall Threat Defense Virtual getting started guides
Firewall and IPS Features	

Feature	Description
Sensitive data detection and masking.	**Upgrade impact. New rules in default policies take effect.** Sensitive data such as social security numbers, credit card numbers, emails, and so on may be leaked onto the internet, intentionally or accidentally. Sensitive data detection is used to detect and generate events on possible sensitive data leakage and generates events only if there is a transfer of significant amount of Personally Identifiable Information (PII) data. Sensitive data detection can mask PII in the output of events, using built-in patterns. Disabling data masking is not supported. Requires Snort 3.
VPN Features	
IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100.	**Upgrade impact. Qualifying connections start being offloaded.** On the Secure Firewall 3100, qualifying IPsec connections through the VTI loopback interface are now offloaded by default. Previously, this feature was only supported on physical interfaces. This feature is automatically enabled by the upgrade. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command.
Interface Features	
Merged management and diagnostic interfaces.	**Upgrade impact. Merge interfaces after upgrade.** For new devices using 7.4 and later, you cannot use the legacy diagnostic interface. Only the merged management interface is available. If you upgraded to 7.4 or later, and you did not have any configuration for the diagnostic interface, then the interfaces will merge automatically. If you upgraded to 7.4 or later, and you have configuration for the diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate diagnostic interface. Note that support for the diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including management) in the configuration. New/modified screens: • **Devices** > **Interfaces** > **Management** interface • (Moved to Interfaces) **System Settings** > **Management Interface** • **Devices** > **Interfaces** > **Merge Interface action needed** > **Management Interface Merge** New/modified commands: **show management-interface convergence**

Feature	Description
Deploy without the diagnostic interface on threat defense virtual for Azure and GCP.	You can now deploy without the diagnostic interface on threat defense virtual for Azure and GCP. Azure deployments still require at least two data interfaces, but GCP requires that you replace the diagnostic interface with a data interface, for a new minimum of three. (Previously, threat defense virtual deployments required one management, one diagnostic, and at least two data interfaces.) Restrictions: This feature is supported for new deployments only. It is not supported for upgraded devices. See: Secure Firewall Threat Defense Virtual getting started guides
Inline sets for Firepower 1000 series, Firepower 2100, and Secure Firewall 3100.	You can configure inline sets on Firepower 1000 series, Firepower 2100, and Secure Firewall 3100 devices. We added the inline sets tab to the Interface page.
Licensing Features	
Changes to license names and support for the Carrier license.	Licenses have been renamed: • Threat is now IPS • Malware is now Malware Defense • Base is now Essentials • AnyConnect Apex is now Secure Client Premier • AnyConnect Plus is now Secure Client Advantage • AnyConnect VPN Only is now Secure Client VPN Only In addition, you can now apply the Carrier license, which allows you to configure GTP/GPRS, Diameter, SCTP, and M3UA inspections. Use FlexConfig to configure these features. See: Licensing the System
Administrative and Troubleshooting Features	
Default NTP server updated.	**Upgrade impact. The system connects to new resources.** The default NTP servers have changed from sourcefire.pool.ntp.org to time.cisco.com. To use a different NTP server, select **Device**, then click **Time Services** in the **System Settings** panel.
SAML servers for HTTPS management user access.	You can configure a SAML server to provide external authentication for HTTPS management access. You can configure external users with the following types of authorization access: Administrator, Audit Admin, Cryptographic Admin, Read-Write User, Read-Only User. You can use Common Access Card (CAC) for login when using a SAML server. We updated the SAML identity source object configuration, and the **System Settings** > **Management Access** page to accept them.

Feature	Description
Detect configuration mismatches in threat defense high availability pairs.	You can now use the CLI to detect configuration mismatches in threat defense high availability pairs. New/modified CLI commands: **show failover config-sync error**, **show failover config-sync stats** See: *Cisco Secure Firewall Threat Defense Command Reference*
Capture dropped packets with the Secure Firewall 3100.	Packet losses resulting from MAC address table inconsistencies can impact your debugging capabilities. The Secure Firewall 3100 can now capture these dropped packets. New/modified CLI commands: [**drop** { **disable** | **mac-filter** }] in the **capture** command. See: *Cisco Secure Firewall Threat Defense Command Reference*
Firmware upgrades included in FXOS upgrades.	**Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.** For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1+ now include firmware upgrades. If any firmware component on the device is older than the one included in the FXOS bundle, the FXOS upgrade also updates the firmware. If the firmware is upgraded, the device reboots twice—once for FXOS and once for the firmware. Just as with software and operating system upgrades, do not make or deploy configuration changes during firmware upgrade. Even if the system appears inactive, do not manually reboot or shut down during firmware upgrade. See: *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*
Quick recovery after data plane failure for the Firepower 1000/2100 and Firepower 4100/9300.	When the data plane process on the Firepower 1000/2100 or the Firepower 4100/9300 crashes, the system reloads the process instead of rebooting the device. Reloading the data plane also restarts other processes, including Snort. If the data plane crashes during bootup, the device follows the normal reload/reboot sequence; this avoids a reload loop. This feature is enabled by default for both new and upgraded devices. To disable it, use FlexConfig. New/modified ASA CLI commands: **data-plane quick-reload**, **show data-plane quick-reload status** New/modified threat defense CLI commands: **show data-plane quick-reload status** See: *Cisco Secure Firewall Threat Defense Command Reference* and *Cisco Secure Firewall ASA Series Command Reference*.

Feature	Description
Require the Message-Authenticator attribute in all RADIUS responses.	**Upgrade impact. For the Firepower 4100/9300, check FXOS compatibility before you upgrade Firewall Threat Defense. After Firewall Threat Defense upgrade, enable the option for existing servers.** You can now require the Message-Authenticator attribute in all RADIUS responses, ensuring that the Firewall 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, 7.4.3, 7.6.1, or 7.7+. For the Firepower 4100/9300, may require an FXOS upgrade; for minimum builds, see *Cisco Secure Firewall Threat Defense Compatibility Guide*.

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 46.

Upgrade Impact Features for Firewall Management Center

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

Table 8: Upgrade Impact Features for Firewall Management Center

Current version	Features with upgrade impact
7.4.0–7.4.2 7.2.0–7.2.9 7.1.x 7.0.6 and earlier	• New Cisco AMP cloud connection method. *(*7.7.0)
7.4.0 and earlier	• Improved Firewall Management Center memory usage calculation, alerting, and swap memory monitoring. *(*7.4.1)

Current version	Features with upgrade impact
7.4.0 7.3.x 7.2.5 and earlier	• Configure DHCP relay trusted interfaces from the Firewall Management Center web interface. *(*7.2.6) • Updated internet access requirements for direct-downloading software upgrades. *(*7.2.6)
7.4.0 7.3.x 7.2.0–7.2.5 7.1.x 7.0.5 and earlier	• Updated web analytics provider. *(*7.0.6)
7.3.x and earlier	• Configure Firewall Threat Defense devices as NetFlow exporters from the Firewall Management Center web interface. *(*7.4.0)
7.3.0–7.3.1 7.2.0–7.2.3 7.1.x 7.0.5 and earlier	• Smaller VDB for lower memory Snort 2 devices. *(*7.0.6)
7.3.x 7.2.3 and earlier	• Access control performance improvements (object optimization). *(*7.2.4)
7.3.0 and later	• Deprecated: Scheduled software upgrades. *(*7.3.0)
7.2.x and earlier	• Configure BFD for BGP from the Firewall Management Center web interface. *(*7.3.0)
7.2.0–7.2.9 7.1.x 7.0.7 and earlier	• Updated internet access requirements for Smart Licensing. *(*7.0.8)
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)
7.1.x and earlier	• Configure VXLAN from the Firewall Management Center web interface. *(*7.2.0) • Configure EIGRP from the Firewall Management Center web interface. *(*7.2.0)

Current version	Features with upgrade impact
7.0.x and earlier	• Configure Equal-Cost-Multi-Path (ECMP) from the FMC web interface. (7.1.0) • Configure policy based routing from the FMC web interface. (7.1.0) • Send intrusion events and retrospective malware events to the Secure Network Analytics cloud from the FMC. (7.1.0) • Deprecated: Intrusion incidents and the intrusion event clipboard. (7.1.0) • Deprecated: Custom tables for intrusion events. (7.1.0)

Upgrade Impact Features for Firewall Threat Defense with Firewall Management Center

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

Table 9: Upgrade Impact Features for Firewall Threat Defense with Firewall Management Center

Current version	Features with upgrade impact
7.4.0–7.4.2 7.3.x 7.2.0–7.2.9 7.1.x 7.0.6 and earlier	• Require the Message-Authenticator attribute in all RADIUS responses. (7.0.7)
7.4.0–7.4.1 7.3.x 7.2.9 and earlier	• Asymmetric traffic handling. (7.2.9)
7.4.0 and earlier	• IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100. (7.4.1) • Captive portal support for multiple Active Directory realms (realm sequences). (7.4.1) • Firmware upgrades included in FXOS upgrades. (7.4.1)
7.3.x 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)

Current version	Features with upgrade impact
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)
7.1.x and earlier	• Autoscale for Firewall Threat Defense Virtual for GCP. (7.2.0)
7.0.x and earlier	• Snort 3 support for inspection of DCE/RPC over SMB2. (7.1.0) • Snort 3 support for **ssl_version** and **ssl_state** keywords. (7.1.0)

Upgrade Impact Features for Firewall Threat Defense with Firewall Device Manager

Table 10: Upgrade Impact Features for Firewall Threat Defense with Firewall Device Manager

Target version	Features
7.4.3–7.4.x	• Require the Message-Authenticator attribute in all RADIUS responses.
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.
7.1.0+	• Dynamic Domain Name System (DDNS) support for updating fully-qualified domain name (FQDN) to IP address mappings for system interfaces. • Snort 3 support for inspection of DCE/RPC over SMB2. • Snort 3 support for **ssl_version** and **ssl_state** keywords.

Upgrade Guidelines

These release notes contain upgrade warnings and guidelines that are specific to each release. You should also check for features and bugs with upgrade impact.

See the upgrade guide for general information on time and disk space requirements, and for details on system behavior during upgrade, which can include interruptions to traffic flow and inspection: For Assistance, on page 214.

Upgrade Guidelines for Firewall Management Center

Table 11: Upgrade Guidelines for Firewall Management Center

Current Version	Guideline	Details
7.4.1	Migration failure: do not migrate to Firewall Management Center Version 7.4.1 if you are using Security Intelligence.	Patch the target Firewall Management Center to Version 7.4.1.1 before you begin migration. The source Firewall Management Center can continue to run Version 7.4.1. **Note** Version 7.4.1 is not supported on the Firewall Management Center 1000/2500/4500, even during the migration process. To migrate to Firewall Management Center 1700/2700/4700, we recommend using Version 7.4.2. For more information on model migration, see the *Cisco Secure Firewall Management Center Model Migration Guide*.
7.2.6–7.2.x	Upgrade not recommended: Version 7.2.6–7.2.x to Version 7.3.x–7.4.0.	Upgrading is supported, but will remove critical fixes and enhancements that are included in your current version. Instead, upgrade to Version 7.4.1+.

Upgrade Guidelines for Firewall Threat Defense with Firewall Management Center

Table 12: Upgrade Guidelines for Firewall Threat Defense

Current Version	Guideline	Details
7.0.9 and earlier 7.1.x 7.2.0–7.2.11 7.3.x 7.4.0–7.4.7 7.6.0–7.6.5 7.7.0–7.7.12 10.0.0–10.0.1	Enable IPsec encryption and set an encryption key in remote access VPN (RA VPN) load balancing groups before upgrade.	Certain releases require secure communications among RA VPN load balancing group members. To minimize disruption, follow these guidelines when upgrading *any* group member to one of those releases: • Before upgrade, enable IPsec encryption and set an encryption key in the RA VPN policy advanced settings. Deploy changes. If you do not set an encryption key, incoming connections are denied after the director upgrades. If you do not enable encryption, you will not be able to deploy to upgraded devices. • Upgrade the entire group. Mixed groups are not supported. Even with IPsec encryption and an encryption key, new connections can be load balanced only to devices on the same "side" as the director. That is, if the director is upgraded, connections can be load balanced only to other upgraded devices. If the director is not upgraded, connections can be load balanced only to non-upgraded devices. Plan your upgrade so the side with the director has the capacity to handle incoming connections throughout the upgrade. This requirement applies to: Version 7.0.10, 7.2.12, 7.4.8, 7.6.6, 7.7.13, 10.0.2, 10.1.0.
Any	Use FXOS 2.14.1.163+ to reimage the Firepower 4100/9300 to Version 7.4.2–7.4.x.	Although we document that FXOS 2.14.1.163+ is required for Firewall Threat Defense 7.4.x, this is for reimaging to 7.4.2+. If you are already running an earlier FXOS 2.14.1 build, you can successfully upgrade to 7.4.2+ without upgrading FXOS (CSCwf64429). Note that in most cases, we recommend the latest FXOS build for reimages and upgrades. For more information, see the Firepower 4100/9300 FXOS release notes.
7.1.x 7.0.0–7.0.2	Revert may require unregistering and reregistering.	If you revert from Version 7.4.1 to Version 7.0.0–7.0.2 or to Version 7.1.x, unregister and reregister devices after the revert completes (CSCwi31680).
7.1.x and earlier	Upgrade prohibited: Firewall Threat Defense Virtual for GCP to Version 7.2.0+ from earlier releases.	You cannot upgrade Firewall Threat Defense Virtual for GCP from Version 7.1.x and earlier to Version 7.2.0+. You must deploy a new instance.

Upgrade Guidelines for Firewall Threat Defense with Firewall Device Manager

Table 13: Upgrade Guidelines for Firewall Threat Defense

Current Version	Guideline	Details
7.4.x and earlier	Do not upgrade the Firepower 1010 if a subinterface uses VLAN 1	For models with built-in switches, you cannot create a subinterface using VLAN 1. VLAN 1 is reserved for the logical VLAN interface for switch ports. If you upgrade the Firepower 1010 to Version 7.6+ later, and you have assigned VLAN 1 to a subinterface, you must first change the VLAN ID for your subinterface to a new VLAN. After upgrading, if present, VLAN 1 will be removed from the subinterface.
7.4.1	Use FXOS 2.14.1.163+ to reimage the Firepower 4100/9300 to Version 7.4.2–7.4.x.	Although we document that FXOS 2.14.1.163+ is required for Firewall Threat Defense 7.4.x, this is for reimaging to 7.4.2+. If you are already running an earlier FXOS 2.14.1 build, you can successfully upgrade to 7.4.2+ without upgrading FXOS (CSCwf64429). Note that in most cases, we recommend the latest FXOS build for reimages and upgrades. For more information, see the Firepower 4100/9300 FXOS release notes.

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 214.

Choosing your upgrade target

Go **directly to the latest Version 7.4 release possible** to minimize upgrade and other impact. This is because 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 14: Released before Version 7.4.x, by date

Target version		Current version: confirm yours is listed.				
		from 7.0	from 7.1	from 7.2	from 7.3	from 7.4
to 7.4.8	2026-09-15	7.0.0–7.0.10	7.1.0	7.2.0–7.2.12	7.3.0–7.3.1	7.4.0–7.4.7
to 7.4.7	2026-04-15	7.0.0–7.0.9	7.1.0	7.2.0–7.2.11	7.3.0–7.3.1	7.4.0–7.4.6
to 7.4.6	2026-02-17	7.0.0–7.0.9	7.1.0	7.2.0–7.2.11	7.3.0–7.3.1	7.4.0–7.4.5
to 7.4.5	2026-01-14	7.0.0–7.0.8	7.1.0	7.2.0–7.2.10	7.3.0–7.3.1	7.4.0–7.4.4
to 7.4.4	2026-01-05	7.0.0–7.0.8	7.1.0	7.2.0–7.2.10	7.3.0–7.3.1	7.4.0–7.4.3
to 7.4.3	2025-10-13	7.0.0–7.0.8	7.1.0	7.2.0–7.2.10	7.3.0–7.3.1	7.4.0–7.4.2
to 7.4.2	2024-07-31	7.0.0–7.0.6	7.1.0	7.2.0–7.2.8	7.3.0–7.3.1	7.4.0–7.4.1
to 7.4.1	2023-12-13	7.0.0–7.0.6	7.1.0	7.2.0–7.2.5	7.3.0–7.3.1	7.4.0
to 7.4.0 *	2023-09-07	—	—	—	—	—

* You cannot upgrade managed devices 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.

Upgrading a patched deployment

Critical fixes in patches/vulnerability (fourth-digit) releases can also skip future releases. If you depend on these critical fixes, verify that your target version contains them. For a full list of release dates, see *Cisco Secure Firewall Management Center New Features by Release* 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 46.
- 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 Patches can change the fourth digit only. You cannot upgrade directly to a patch from a previous major or maintenance release. Although a patched device can be managed with an unpatched Firewall Management Center, fully patched deployments undergo enhanced testing.

Table 15: Supported direct upgrades

Current version	Target software version							
	to 10.x	7.7	7.6	7.4	7.3	7.2	7.1	7.0
from 10.x	YES	—	—	—	—	—	—	—
from 7.7	YES	YES	—	—	—	—	—	—
from 7.6	YES	YES	YES	—	—	—	—	—
from 7.4	YES	YES	YES	YES	—	—	—	—
from 7.3	YES	YES	YES	YES	YES	—	—	—
from 7.2	—	YES	YES	YES	YES	YES	—	—
from 7.1	—	—	YES	YES	YES	YES	YES	—
from 7.0	—	—	—	YES	YES	YES	YES	YES
from 6.4	—	—	—	—	—	—	—	YES

Supported FXOS versions for Firepower 4100/9300 upgrades

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

Table 16: Supported FXOS versions for Firepower 4100/9300 upgrades

Target Firewall Threat Defense version	Minimum FXOS version
10.x	2.18.0
7.7	2.17.0
7.6	2.16.0
7.4.1–7.4.x	2.14.1
7.4.0	—
7.3	2.13.0
7.2	2.12.0
7.1	2.11.1
7.0	2.10.1
6.7	2.9.1
6.6	2.8.1

Target Firewall Threat Defense version	Minimum FXOS version
6.4	2.6.1

Supported downgrades

If an upgrade succeeds but the system does not function to your expectations, you may be able to return to a previous version. 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 Release Notes for Cloud-Delivered Firewall Management Center.

Important We do not list open bugs for most 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 7.4.0

Table last updated: 2023-09-11

Table 17: Open Bugs in Version 7.4.0

Bug ID	Headline
CSCwd87510	Deploy failure when flow export destinations are swapped or port value changed
CSCwe36422	IDP SAML missing filter in Zero Trust Policy shows all groups have missing IDP data
CSCwf93776	New User activity page does not display events for Special Identities Realm
CSCwh00002	Azure AD sessions do not get removed after disabling subscription or changing ise configuration
CSCwh04354	Importing a realm with a proxy will fail
CSCwh38213	Editing CSDAC dynamic attribute filter throwing Internal Error
CSCwh41164	OSPFv3 BFD sessions not coming up for more than 7
CSCwh45488	PBR configuration using User Identity is not migrated during FTD migration to cdFMC
CSCwh46657	Save button disabled when updating Zero Trust Policy

Bug ID	Headline
CSCwh49918	New SRU is not immediately installed upon management center upgrade
CSCwh50221	4200 Series: Portchannel in cluster may stay down sometimes when LACP is in active mode
CSCwh50259	EventHandler should not log warning if it fails to open a unified file when the file doesn't exist
CSCws57118	FMC SXP bulk download fails when ISE has SXP disabled

Resolved Bugs in Version 7.4.8

Table last updated: 2026-09-16

Table 18: Resolved Security Bugs in Version 7.4.8

Bug ID	Headline
CSCwc40735	CVE-2019-17567: apache2: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configu
CSCwn63000	CVE-2024-49978: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95189	CVE-2024-53088: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95467	CVE-2024-9681: curl: When curl is asked to use HSTS, the expiry time ...
CSCwo05022	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software EIGRP Denial of Service Vulnerability
CSCwo74389	CVE-2024-26844: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87494	CVE-2023-52939: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87517	CVE-2024-26759: linux-kernel: In the Linux kernel, the following vuln...
CSCwp10206	CVE-2022-49837: linux-kernel: In the Linux kernel, the following vuln...
CSCwp10267	CVE-2022-49901: linux-kernel: In the Linux kernel, the following vuln...
CSCwq60584	CVE-2025-0395: glibc: When the assert() function in the GNU C Library...
CSCwq60626	CVE-2025-0840: binutils: A vulnerability, which was classified as pro...
CSCwq60658	CVE-2025-2784: libsoup: A flaw was found in libsoup. The package is v...
CSCwq60696	CVE-2025-4565: protobuf: Any project that uses Protobuf Pure-Python b...
CSCwq60699	CVE-2025-4802: glibc: Untrusted LD_LIBRARY_PATH environment variable ...
CSCwq66795	CVE-2025-21863: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66797	CVE-2025-21887: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwq66798	CVE-2025-21891: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66808	CVE-2025-22134: vim: When switching to other buffers using the :all c...
CSCwq66815	CVE-2025-24014: vim: Vim is an open source, command line text editor....
CSCwq66818	CVE-2025-24928: libxml2: libxml2 before 2.12.10 and 2.13.x before 2.1...
CSCwq66819	CVE-2025-25724: libarchive: list_item_verbose in tar/util.c in libarc...
CSCwq66820	CVE-2025-26603: vim: Vim is a greatly improved version of the good ol...
CSCwq66821	CVE-2025-27423: vim: Vim is an open source, command line text editor....
CSCwq66825	CVE-2025-29768: vim: Vim, a text editor, is vulnerable to potential d...
CSCwq72910	CVE-2025-5222: icu: A stack buffer overflow was found in Internationl...
CSCwq72966	CVE-2025-49794: libxml2: A use-after-free vulnerability was found in ...
CSCwq72970	CVE-2025-50181: urllib3: urllib3 is a user-friendly HTTP client libra...
CSCwq72974	CVE-2025-53905: vim: Vim is an open source, command line text editor....
CSCwq72975	CVE-2025-53906: vim: Vim is an open source, command line text editor....
CSCwq72980	CVE-2024-0450: python: An issue was found in the CPython `zipfile` mo...
CSCwq72990	CVE-2024-3651: idna: A vulnerability was identified in the kjd/idna l...
CSCwq72992	CVE-2024-4032: python: The “ipaddress” module contained incorrect inf...
CSCwq72999	CVE-2024-5642: python: CPython 3.9 and earlier doesn't disallow confi...
CSCwq73004	CVE-2024-6923: python: There is a MEDIUM severity vulnerability affec...
CSCwq73006	CVE-2024-7264: curl: libcurl's ASN1 parser code has the `GTime2str()`...
CSCwq73012	CVE-2024-10041: pam: A vulnerability was found in PAM. The secret inf...
CSCwr07575	CVE-2025-1215: vim: A vulnerability classified as problematic was fou...
CSCwr07614	CVE-2024-34397: glib: An issue was discovered in GNOME GLib before 2....
CSCwr07615	CVE-2024-34459: libxml2: An issue was discovered in xmllint (from lib...
CSCwr18511	CVE-2024-25176: luajit: LuaJIT through 2.1 and OpenRusty luajit2 befo...
CSCwr18512	CVE-2024-25178: luajit: LuaJIT through 2.1 and OpenRusty luajit2 befo...
CSCwr18529	CVE-2023-52735: linux-kernel: In the Linux kernel, the following vuln...
CSCws34032	ASA/FTD - 'logging tcp-block-reduction' CLI Commands for TCP Syslog Queue Management

Bug ID	Headline
CSCws78984	CVE-2022-2309: libxml2: NULL Pointer Dereference allows attackers to ...
CSCws79422	CVE-2021-47070: linux-kernel: In the Linux kernel, the following vuln...
CSCws79513	CVE-2021-47412: linux-kernel: In the Linux kernel, the following vuln...
CSCws79548	CVE-2021-47498: linux-kernel: In the Linux kernel, the following vuln...
CSCws79622	CVE-2022-3566: linux-kernel: A vulnerability, which was classified as...
CSCws79639	CVE-2022-48624: less: close_altfile in filename.c in less before 606 ...
CSCws79656	CVE-2022-48666: linux-kernel: In the Linux kernel, the following vuln...
CSCws79674	CVE-2022-48744: linux-kernel: In the Linux kernel, the following vuln...
CSCws79980	CVE-2022-49465: linux-kernel: In the Linux kernel, the following vuln...
CSCws80190	CVE-2022-49743: linux-kernel: In the Linux kernel, the following vuln...
CSCws80619	CVE-2023-49582: apr: Lax permissions set by the Apache Portable Runti...
CSCws80668	CVE-2023-52654: linux-kernel: In the Linux kernel, the following vuln...
CSCws80677	CVE-2023-52672: linux-kernel: In the Linux kernel, the following vuln...
CSCws80687	CVE-2023-52683: linux-kernel: In the Linux kernel, the following vuln...
CSCws80715	CVE-2023-52750: linux-kernel: In the Linux kernel, the following vuln...
CSCws80732	CVE-2023-52791: linux-kernel: In the Linux kernel, the following vuln...
CSCws80738	CVE-2023-52803: linux-kernel: In the Linux kernel, the following vuln...
CSCws80747	CVE-2023-52828: linux-kernel: In the Linux kernel, the following vuln...
CSCws80770	CVE-2023-52869: linux-kernel: In the Linux kernel, the following vuln...
CSCws80779	CVE-2023-52881: linux-kernel: In the Linux kernel, the following vuln...
CSCws80826	CVE-2023-53039: linux-kernel: In the Linux kernel, the following vuln...
CSCws80924	CVE-2024-26614: linux-kernel: In the Linux kernel, the following vuln...
CSCws80936	CVE-2024-26880: linux-kernel: In the Linux kernel, the following vuln...
CSCws80940	CVE-2024-26906: linux-kernel: In the Linux kernel, the following vuln...
CSCws80942	CVE-2024-26921: linux-kernel: In the Linux kernel, the following vuln...
CSCws80950	CVE-2024-26935: linux-kernel: In the Linux kernel, the following vuln...
CSCws80969	CVE-2024-26988: linux-kernel: In the Linux kernel, the following vuln...
CSCws81003	CVE-2024-27414: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCws81007	CVE-2024-27417: linux-kernel: In the Linux kernel, the following vuln...
CSCws81012	CVE-2024-27431: linux-kernel: In the Linux kernel, the following vuln...
CSCws81017	CVE-2024-31076: linux-kernel: In the Linux kernel, the following vuln...
CSCws81030	CVE-2024-35805: linux-kernel: In the Linux kernel, the following vuln...
CSCws81054	CVE-2024-35848: linux-kernel: In the Linux kernel, the following vuln...
CSCws81063	CVE-2024-35884: linux-kernel: In the Linux kernel, the following vuln...
CSCws81065	CVE-2024-35886: linux-kernel: In the Linux kernel, the following vuln...
CSCws81072	CVE-2024-35910: linux-kernel: In the Linux kernel, the following vuln...
CSCws81110	CVE-2024-35969: linux-kernel: In the Linux kernel, the following vuln...
CSCws81117	CVE-2024-35976: linux-kernel: In the Linux kernel, the following vuln...
CSCws81126	CVE-2024-36004: linux-kernel: In the Linux kernel, the following vuln...
CSCws81136	CVE-2024-36017: linux-kernel: In the Linux kernel, the following vuln...
CSCws81137	CVE-2024-36020: linux-kernel: In the Linux kernel, the following vuln...
CSCws81180	CVE-2024-36957: linux-kernel: In the Linux kernel, the following vuln...
CSCws81181	CVE-2024-36964: linux-kernel: In the Linux kernel, the following vuln...
CSCws81211	CVE-2024-38596: linux-kernel: In the Linux kernel, the following vuln...
CSCws81213	CVE-2024-38601: linux-kernel: In the Linux kernel, the following vuln...
CSCws81218	CVE-2024-38615: linux-kernel: In the Linux kernel, the following vuln...
CSCws81229	CVE-2024-38659: linux-kernel: In the Linux kernel, the following vuln...
CSCws81265	CVE-2024-40953: linux-kernel: In the Linux kernel, the following vuln...
CSCws81376	CVE-2024-42322: linux-kernel: In the Linux kernel, the following vuln...
CSCws81381	CVE-2024-43374: vim: The UNIX editor Vim prior to version 9.1.0678 ha...
CSCws81404	CVE-2024-45777: grub2: A flaw was found in grub2. The calculation of ...
CSCws81406	CVE-2024-45778: grub2: A stack overflow flaw was found when reading a...
CSCws81407	CVE-2024-45780: grub2: A flaw was found in grub2. When reading tar fi...
CSCws81418	CVE-2024-47081: python-requests: Requests is a HTTP library. Due to a...
CSCws81422	CVE-2024-47619: syslog-ng: syslog-ng is an enhanced log daemo. Prior ...
CSCws81426	CVE-2024-47814: vim: Vim is an open source, command line text editor....

Bug ID	Headline
CSCws81433	CVE-2024-50199: linux-kernel: In the Linux kernel, the following vuln...
CSCws81443	CVE-2024-52332: linux-kernel: In the Linux kernel, the following vuln...
CSCws81446	CVE-2024-53125: linux-kernel: In the Linux kernel, the following vuln...
CSCws81453	CVE-2024-53174: linux-kernel: In the Linux kernel, the following vuln...
CSCws81459	CVE-2024-53194: linux-kernel: In the Linux kernel, the following vuln...
CSCws81463	CVE-2024-53198: linux-kernel: In the Linux kernel, the following vuln...
CSCws81464	CVE-2024-53214: linux-kernel: In the Linux kernel, the following vuln...
CSCws81471	CVE-2024-53241: linux-kernel: In the Linux kernel, the following vuln...
CSCws81472	CVE-2024-53680: linux-kernel: In the Linux kernel, the following vuln...
CSCws81498	CVE-2024-56570: linux-kernel: In the Linux kernel, the following vuln...
CSCws81501	CVE-2024-56584: linux-kernel: In the Linux kernel, the following vuln...
CSCws81762	CVE-2024-57883: linux-kernel: In the Linux kernel, the following vuln...
CSCws81763	CVE-2024-57884: linux-kernel: In the Linux kernel, the following vuln...
CSCws81781	CVE-2024-57929: linux-kernel: In the Linux kernel, the following vuln...
CSCws81792	CVE-2024-57979: linux-kernel: In the Linux kernel, the following vuln...
CSCws81797	CVE-2024-57986: linux-kernel: In the Linux kernel, the following vuln...
CSCws81819	CVE-2024-58083: linux-kernel: In the Linux kernel, the following vuln...
CSCws81825	CVE-2024-58090: linux-kernel: In the Linux kernel, the following vuln...
CSCws81826	CVE-2024-58093: linux-kernel: In the Linux kernel, the following vuln...
CSCws81832	CVE-2024-7254: protobuf: Any project that parses untrusted Protocol B...
CSCws81837	CVE-2025-21648: linux-kernel: In the Linux kernel, the following vuln...
CSCws81839	CVE-2025-21653: linux-kernel: In the Linux kernel, the following vuln...
CSCws81841	CVE-2025-21664: linux-kernel: In the Linux kernel, the following vuln...
CSCws81844	CVE-2025-21702: linux-kernel: In the Linux kernel, the following vuln...
CSCws81849	CVE-2025-21719: linux-kernel: In the Linux kernel, the following vuln...
CSCws81851	CVE-2025-21728: linux-kernel: In the Linux kernel, the following vuln...
CSCws81858	CVE-2025-21765: linux-kernel: In the Linux kernel, the following vuln...
CSCws81860	CVE-2025-21767: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCws81873	CVE-2025-21806: linux-kernel: In the Linux kernel, the following vuln...
CSCws81896	CVE-2025-21926: linux-kernel: In the Linux kernel, the following vuln...
CSCws81907	CVE-2025-21971: linux-kernel: In the Linux kernel, the following vuln...
CSCws81909	CVE-2025-21975: linux-kernel: In the Linux kernel, the following vuln...
CSCws81925	CVE-2025-22045: linux-kernel: In the Linux kernel, the following vuln...
CSCws81928	CVE-2025-22055: linux-kernel: In the Linux kernel, the following vuln...
CSCws81930	CVE-2025-22058: linux-kernel: In the Linux kernel, the following vuln...
CSCws81937	CVE-2025-22075: linux-kernel: In the Linux kernel, the following vuln...
CSCws81942	CVE-2025-22086: linux-kernel: In the Linux kernel, the following vuln...
CSCws81954	CVE-2025-22121: linux-kernel: In the Linux kernel, the following vuln...
CSCws81968	CVE-2025-23143: linux-kernel: In the Linux kernel, the following vuln...
CSCws81977	CVE-2025-23150: linux-kernel: In the Linux kernel, the following vuln...
CSCws81987	CVE-2025-23163: linux-kernel: In the Linux kernel, the following vuln...
CSCws81988	CVE-2025-37738: linux-kernel: In the Linux kernel, the following vuln...
CSCws82696	CVE-2025-37780: linux-kernel: In the Linux kernel, the following vuln...
CSCws82713	CVE-2025-37797: linux-kernel: In the Linux kernel, the following vuln...
CSCws82714	CVE-2025-37798: linux-kernel: In the Linux kernel, the following vuln...
CSCws82717	CVE-2025-37808: linux-kernel: In the Linux kernel, the following vuln...
CSCws82727	CVE-2025-37823: linux-kernel: In the Linux kernel, the following vuln...
CSCws82731	CVE-2025-37830: linux-kernel: In the Linux kernel, the following vuln...
CSCws82735	CVE-2025-37836: linux-kernel: In the Linux kernel, the following vuln...
CSCws82736	CVE-2025-37839: linux-kernel: In the Linux kernel, the following vuln...
CSCws82740	CVE-2025-37844: linux-kernel: In the Linux kernel, the following vuln...
CSCws82809	CVE-2025-37859: linux-kernel: In the Linux kernel, the following vuln...
CSCws82815	CVE-2025-37867: linux-kernel: In the Linux kernel, the following vuln...
CSCws82836	CVE-2025-37885: linux-kernel: In the Linux kernel, the following vuln...
CSCws82838	CVE-2025-37890: linux-kernel: In the Linux kernel, the following vuln...
CSCws82852	CVE-2025-37923: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCws82855	CVE-2025-37927: linux-kernel: In the Linux kernel, the following vuln...
CSCws82861	CVE-2025-37932: linux-kernel: In the Linux kernel, the following vuln...
CSCws82864	CVE-2025-37940: linux-kernel: In the Linux kernel, the following vuln...
CSCwt09824	FTD should not honour a huge time jump from NTP
CSCwt10998	CVE-2026-24061: inetutils: telnetd in GNU Inetutils through 2.7 allow...
CSCwt27261	CVE-2025-14087: glib: A flaw was found in GLib (Gnome Lib). This vuln...
CSCwt27265	CVE-2025-68615: net-snmp: net-snmp is a SNMP application library, too...
CSCwt27267	CVE-2026-0915: glibc: Calling getnetbyaddr or getnetbyaddr_r with a c...
CSCwt27272	CVE-2026-22801: libpng: LIBPNG is a reference library for use in appl...
CSCwt27273	CVE-2026-25646: libpng: LIBPNG is a reference library for use in appl...
CSCwt27275	CVE-2025-5244: binutils: A vulnerability was found in GNU Binutils up...
CSCwt27276	CVE-2025-5245: binutils: A vulnerability classified as critical has b...
CSCwt27282	CVE-2025-13601: glib: A heap-based buffer overflow problem was found ...
CSCwt27284	CVE-2025-15281: glibc: Calling wordexp with WRDE_REUSE in conjunction...
CSCwt27370	Backup-Restore silent failure in Multi-Instance
CSCwt42671	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software IKEv2 Certificate Authentication Denial of Service Vulnerability
CSCwt54632	Snort crashes or a FATAL ERROR occurs after 255 reloads if ngfw.rules includes NCM(Non-contiguous netmask)
CSCwt55803	FPR4225 losing communication with netmod
CSCwt81457	Cisco Secure Firewall Management Center Software Session Fixation Issue
CSCwt85702	Snort3 Watchdog restart caused by a corrupted stream_tcp thread
CSCwt86002	FTD Traffic failure due to 9344 block depletion in peer_proxy_tx_q_lw_rx
CSCwt95974	Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability
CSCwt95997	Cisco Secure Firewall Management Center Software Static Credential Vulnerability
CSCwu02508	Cisco Adaptive Security Appliance and Secure Firewall Threat Defense SSL VPN Denial of Service Vulnerability
CSCwu03757	Cisco Secure Firewall Threat Defense Software Snort 2 SSL/TLS Denial of Service Vulnerability

Bug ID	Headline
CSCwu14285	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software TCP DNS Denial of Service Vulnerability
CSCwu14331	Cisco Secure Firewall Management Center Software sftunnel Root Arbitrary Code Execution Vulnerability
CSCwu16917	Cisco Secure Firewall Management Center and Secure Firewall Threat Defense Software sftunnel Unauthorized Authentication Bypass Vulnerability
CSCwu16938	Cisco Secure Firewall Management Center Software Java Deserialization Remote Code Execution Vulnerability
CSCwu16954	Cisco Secure Firewall Management Center Software sftunnel Deserialization Root Command Execution Vulnerability
CSCwu16965	Cisco Secure Firewall Management Center Software Single Sign-On Token Forgery of Administrator Account Vulnerability
CSCwu24501	Cisco Secure Firewall Management Center Software SQL Injection Vulnerability
CSCwu27275	Cisco Secure Firewall Management Center Software Deserialization Arbitrary Root Command Execution Vulnerability
CSCwu27279	Cisco Secure Firewall Management Center Software Impersonated sftunnel Connection Vulnerability
CSCwu27874	Evaluate Cisco FXOS for CVE-2026-31431 (Copy Fail)
CSCwu32003	ASA: PBR - ISP1 is not taking precedence over ISP2
CSCwu32444	CVE-2026-43284: linux-kernel: In the Linux kernel, the following vul...
CSCwu36643	Cisco Secure Firewall Management Center Software Information Disclosure and Disk Denial of Service Vulnerability
CSCwu42586	Cisco Secure Firewall Management Center Software Low Privileged Arbitrary File Download Vulnerability
CSCwv23051	FMC fails to upload AnyConnect/Secure Client images exceeding 200 MB
CSCwv96220	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability

Table last updated: 2026-09-15

Table 19: Resolved Functional Bugs in Version 7.4.8

Bug ID	Headline
CSCwo13550	Dispatch queue drops have no snapshot or tuple view for dropped flows
CSCws68206	ASA on hyper-v: couldn't configure VLAN after upgrade

Bug ID	Headline
CSCws70200	SMTP fails to get identified with an App Based rule
CSCwt12816	[CTC Tech] IDS Block action appears to block traffic instead of detect-only
CSCwt41591	Traceback and reload in fover or appAgent_reply_processor_thread which may lead to a boot loop
CSCwt58284	System support trace output displaying both udp and icmp traffic even when a strict icmp filter is used.
CSCwt61398	Snort 3 crash in acquire_fqdn with FQDN access rules
CSCwt97728	"Snort3 may crash during flow opaque modification in the DAQ plugin, causing a brief traffic interruption"
CSCwu39000	Snort CPU Usage Shows 0 in FMC Health Monitor
CSCwv49756	The crash is triggered by a specific SNMP host-group configuration.

Resolved Bugs in Version 7.4.7

Table last updated: 2026-04-15

Table 20: Resolved Security Bugs in Version 7.4.7

Bug ID	Headline
CSCwb67583	ASDM Access Issue When SSL VPN And HTTP Server Is Configured On Same Port
CSCwd87510	Deploy failure after interface group or port value change in Netflow collector config or max collector limit of 5 is reached
CSCwf97953	FTD unable to re-join the HA after upgrade from 7.2.0 build 82 to 7.2.5 build 203.
CSCwi76658	NGFWPolicy::Manager::populateGlobalSnapshot() NGFW HA plugin takes longer time to validate
CSCwj34132	unable to register device post restoring the backup
CSCwk22959	Issue summary: Some non-default TLS server configurations can cause un
CSCwm66841	Switch role of FTDHA backup task and backup name have discrepancy in UI SensorList/management page
CSCwm71529	hms process consuming 20GB memory on cdFMC tenant.
CSCwm83089	Cisco FXOS and UCS Manager Software Stored Cross-Site Scripting Vulnerability
CSCwn15505	Observing Lina Core for 2.17 in BS/QP with App Instance Stuck in 'Started' State
CSCwn48245	SEC-PWD-CONTROL - PSB - Proxy password showing in plain text on FMC
CSCwn55253	FMC GUI does not Accept "@" in the username for remote storage used for backups

Bug ID	Headline
CSCwn58273	CVE-2024-47728: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58322	CVE-2024-49888: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58383	CVE-2024-49934: linux-kernel: In the Linux kernel, the following vuln...
CSCwn62998	CVE-2024-49974: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63021	CVE-2024-49996: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63038	CVE-2024-50014: linux-kernel: ext4: fix access to uninitialised lock in fc replay
CSCwn63062	CVE-2024-50055: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63070	CVE-2024-50067: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63112	CVE-2024-50138: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63129	CVE-2024-50154: linux-kernel: In the Linux kernel, the following vuln...
CSCwn69963	Addressing CVEs reported in unicorn zlib library
CSCwn78991	FMC Legacy UI allows you to create time range objects in past time in ACL
CSCwn86187	FTD native: ldap configuration fails to deploy to ftd when using same user as radius
CSCwn91730	FMC API put taking long time to update Extended ACL objects when count is huge like hundreds
CSCwn94711	CVE-2021-47036: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94729	CVE-2021-47199: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94753	CVE-2021-47455: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94754	CVE-2021-47469: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94767	CVE-2021-47552: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94794	CVE-2023-52476: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94839	CVE-2023-52698: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94850	CVE-2023-52757: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94860	CVE-2023-52845: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94897	CVE-2024-26663: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94911	CVE-2024-26739: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94943	CVE-2024-26928: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94947	CVE-2024-27388: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwn94968	CVE-2024-35863: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94969	CVE-2024-35864: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94972	CVE-2024-35867: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94974	CVE-2024-35868: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94977	CVE-2024-35896: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94982	CVE-2024-35925: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94988	CVE-2024-35945: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94989	CVE-2024-35998: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94994	CVE-2024-36286: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95004	CVE-2024-36954: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95005	CVE-2024-36959: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95016	CVE-2024-38662: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95033	CVE-2024-42283: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95040	CVE-2024-43834: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95041	CVE-2024-43835: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95067	CVE-2024-46739: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95084	CVE-2024-46857: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95085	CVE-2024-47678: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95126	CVE-2024-50258: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95137	CVE-2024-50272: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95159	CVE-2024-50301: linux-kernel: security/keys: fix slab-out-of-bounds in key_task_permission
CSCwn95161	CVE-2024-50302: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95163	CVE-2024-50304: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95170	CVE-2024-53052: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95181	CVE-2024-53066: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95213	CVE-2024-53121: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95215	CVE-2024-53124: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwn95222	CVE-2024-53135: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95225	CVE-2024-53138: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95228	CVE-2024-53140: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95233	CVE-2024-53146: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95238	CVE-2024-53157: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95245	CVE-2024-53179: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95259	CVE-2024-55916: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95308	CVE-2024-56647: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95319	CVE-2024-56662: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95320	CVE-2024-56664: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95323	CVE-2024-56672: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95324	CVE-2024-56688: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95339	CVE-2024-56720: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95345	CVE-2024-56728: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95347	CVE-2024-56739: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95354	CVE-2024-56751: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95358	CVE-2024-56756: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95361	CVE-2024-56763: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95365	CVE-2024-56770: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95372	CVE-2024-56779: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95453	CVE-2024-57807: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95456	CVE-2024-57890: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95462	CVE-2024-57938: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95464	CVE-2024-57940: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95466	CVE-2024-8006: libpcap: Remote packet capture support is disabled by ...
CSCwo00332	Firepower wiping SSL trustpoint config after reloading.
CSCwo14426	Unable to save the Ext ACL object - "Only Host and Network in IPv4 and IPv6 format are supported."

Bug ID	Headline
CSCwo35938	IPv6 Management communication is lost due to a missing management-only multicast route.
CSCwo44732	ARP is silently dropping packet for an unreachable next hop
CSCwo51928	Intrusion rules CVE filter does not function for certain input formats
CSCwo55613	CVE-2021-47247: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55647	CVE-2022-23491: python-certifi: Certifi is a curated collection of Ro...
CSCwo55683	CVE-2022-49043: libxml2: xmlXIncludeAddNode in xinclude.c in libxml2 ...
CSCwo55684	CVE-2022-49046: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55707	CVE-2022-49190: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55710	CVE-2022-49215: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55715	CVE-2022-49219: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55868	CVE-2023-52587: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55879	CVE-2023-52612: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55882	CVE-2023-52621: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55883	CVE-2023-52622: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55913	CVE-2023-52879: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55916	CVE-2024-25629: c-ares: c-ares is a C library for asynchronous DNS re...
CSCwo55934	CVE-2024-26659: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55937	CVE-2024-26664: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55940	CVE-2024-26669: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55942	CVE-2024-26671: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55951	CVE-2024-26679: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55956	CVE-2024-26686: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55957	CVE-2024-26687: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55976	CVE-2024-26763: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55977	CVE-2024-26764: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55983	CVE-2024-26773: linux-kernel: In the Linux kernel, the following vuln...
CSCwo55992	CVE-2024-26805: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwo55993	CVE-2024-26809: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56015	CVE-2024-36903: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56019	CVE-2024-36927: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56025	CVE-2024-40945: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56026	CVE-2024-40972: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56029	CVE-2024-40984: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56063	CVE-2024-53217: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56064	CVE-2024-53224: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56068	CVE-2024-56171: libxml2: libxml2 before 2.12.10 and 2.13.x before 2.1...
CSCwo56070	CVE-2024-56568: linux-kernel: In the Linux kernel, the following vuln...
CSCwo56072	CVE-2024-56569: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57045	CVE-2021-47182: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57066	CVE-2024-57874: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57095	CVE-2024-57977: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57100	CVE-2024-57981: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57103	CVE-2024-58005: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57107	CVE-2024-58017: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57116	CVE-2024-9287: python: A vulnerability has been found in the CPython ...
CSCwo57126	CVE-2025-21638: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57128	CVE-2025-21669: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57140	CVE-2025-21690: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57156	CVE-2025-21745: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57161	CVE-2025-21776: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57162	CVE-2025-21779: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57169	CVE-2025-21785: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57171	CVE-2025-21791: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57172	CVE-2025-21814: linux-kernel: In the Linux kernel, the following vuln...
CSCwo57178	CVE-2025-27113: libxml2: libxml2 before 2.12.10 and 2.13.x before 2.1...

Bug ID	Headline
CSCwo73708	The ObjectSerializationDecoder in Apache MINA uses Javaâs native deseria
CSCwo74356	CVE-2021-47212: linux-kernel: In the Linux kernel, the following vuln...
CSCwo74376	CVE-2024-26816: linux-kernel: In the Linux kernel, the following vuln...
CSCwo74380	CVE-2024-26830: linux-kernel: i40e: Do not allow untrusted VF to remove administratively set MAC
CSCwo74394	CVE-2024-26851: linux-kernel: In the Linux kernel, the following vuln...
CSCwo74400	CVE-2024-27437: linux-kernel: In the Linux kernel, the following vuln...
CSCwo74405	CVE-2024-34158: golang: Calling Parse on a "// +build" build tag line...
CSCwo74407	CVE-2024-45336: golang: The HTTP client drops sensitive headers after...
CSCwo74409	CVE-2024-45341: golang: A certificate with a URI which has a IPv6 add...
CSCwo87471	CVE-2022-49546: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87475	CVE-2022-49728: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87490	CVE-2023-52936: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87520	CVE-2025-21640: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87522	CVE-2025-21898: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87535	CVE-2025-21920: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87541	CVE-2025-21928: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87551	CVE-2025-21959: linux-kernel: In the Linux kernel, the following vuln...
CSCwo87578	CVE-2025-32414: libxml2: In libxml2 before 2.13.8 and 2.14.x before 2...
CSCwo91748	Lina: Traceback in thread name ssh on executing show access-list after ACL deletion
CSCwo95633	CVE-2025-21853: linux-kernel: In the Linux kernel, the following vuln...
CSCwo95634	CVE-2025-32415: libxml2: In libxml2 before 2.13.8 and 2.14.x before 2...
CSCwo95774	Vulnerable version of Highcharts used by Context Explorer
CSCwo97439	ACL: ASA may show false "OOB Access-list config change detected" warning after AAA authorization command is applied
CSCwp09920	Policy Deployment: When using MD5 in Site-to-Site VPN, manual deployment fails with validation error, but schedule deployment succeeds.
CSCwp10179	CVE-2021-47265: linux-kernel: In the Linux kernel, the following vuln...
CSCwp10290	CVE-2024-26870: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwp10292	CVE-2024-26891: linux-kernel: In the Linux kernel, the following vuln...
CSCwp10312	CVE-2025-22063: linux-kernel: In the Linux kernel, the following vuln...
CSCwp10317	CVE-2025-37785: linux-kernel: In the Linux kernel, the following vuln...
CSCwp62846	Reverting FTD upgrade silently removes object overrides on the FMC for the reverted FTD
CSCwp98488	PSB: SEC-LOG-NOSENS-FR2 - P12 cert passphrase logged in plaintext in FMC logs
CSCwq18679	ASA from CSM/CLI - no access-list ACL_name line line_nr remark on last ACL line shows message - "Specified remark does not exist"
CSCwq21101	Invalid host header reveals ASA interface IP address
CSCwq39942	CVE-2025-32463: sudo: Sudo before 1.9.17p1 allows local users to obtain
CSCwq39943	CVE-2025-32462: sudo: Before 1.9.17p1, allows users to execute commands on unintended machines.
CSCwq40256	Inbound IPsec packets are dropped by IPsec offload when the crypto map ACL is using specific ports.
CSCwq60624	CVE-2025-0689: grub2: When reading data from disk, the grub's UDF fil...
CSCwq60655	CVE-2025-1125: grub2: When reading data from a hfs filesystem, grub's...
CSCwq60694	CVE-2025-4516: python: There is an issue in CPython when using 'bytes...
CSCwq60714	CVE-2025-6965: sqlite: There exists a vulnerability in SQLite version...
CSCwq60723	CVE-2025-21639: linux-kernel: In the Linux kernel, the following vuln...
CSCwq60729	CVE-2025-21683: linux-kernel: In the Linux kernel, the following vuln...
CSCwq60731	CVE-2025-21700: linux-kernel: In the Linux kernel, the following vuln...
CSCwq64843	Deployment Failure After Removing An Object From ACL Used in DAP
CSCwq66453	CVE-2025-21605: redis: Redis is an open source, in-memory database th...
CSCwq66716	CVE-2025-27363: free-type: An out of bounds write exists in FreeType ...
CSCwq66776	CVE-2025-21760: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66778	CVE-2025-21762: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66779	CVE-2025-21763: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66780	CVE-2025-21764: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66786	CVE-2025-21846: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwq66801	CVE-2025-21999: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66803	CVE-2025-22005: linux-kernel: In the Linux kernel, the following vuln...
CSCwq66826	CVE-2025-32023: redis: Redis is an open source, in-memory database th...
CSCwq66840	CVE-2025-47273: python-setuptools: setuptools is a package that allow...
CSCwq66843	CVE-2025-48367: redis: Redis is an open source, in-memory database th...
CSCwq72989	CVE-2024-3447: qemu: A heap-based buffer overflow was found in the SD...
CSCwq73001	CVE-2024-6345: python-setuptools: A vulnerability in the package_inde...
CSCwq73002	CVE-2024-6505: qemu: A flaw was found in the virtio-net device in QEM...
CSCwq73009	CVE-2024-8088: python: CPython "zipfile" module affecting "zipfile.Path"
CSCwq73011	CVE-2024-8354: qemu: A flaw was found in QEMU. An assertion failure w...
CSCwq73013	CVE-2024-10524: wget: Applications that use Wget to access a remote r...
CSCwq73027	CVE-2024-26627: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73028	CVE-2024-26633: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73029	CVE-2024-26635: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73030	CVE-2024-26641: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73043	CVE-2024-26733: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73044	CVE-2024-26735: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73049	CVE-2024-26747: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73056	CVE-2024-26772: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73059	CVE-2024-26804: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73060	CVE-2024-26808: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73062	CVE-2024-26810: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73063	CVE-2024-26812: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73065	CVE-2024-26843: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73067	CVE-2024-26852: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73073	CVE-2024-26894: linux-kernel: In the Linux kernel, the following vuln...
CSCwq73075	CVE-2024-26924: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwq74738	RAVPN SSL/IKEV2 AUTH FAILURE: AAA PROCESS MISHANDLING BROKEN FIBER CLASS
CSCwq74813	FMC: Copy/Cut/Paste or drag/drop ACE in Extended ACL object, deletes existing Rules
CSCwq82225	Drop counter doesn't increment for embryonic related drops in 'show service policy'
CSCwq85267	Late Release of Memory after Effective Lifetime vulnerability in Apache HTTP Server.
CSCwq85285	HTTP response splitting in the core of Apache HTTP Server allows an attacker who can manipulate the Content-Type response headers
CSCwr07581	CVE-2025-32988: gnutls: A flaw was found in GnuTLS. A double-free vul...
CSCwr07583	CVE-2025-32990: gnutls: A heap-buffer-overflow (off-by-one) flaw was ...
CSCwr07587	CVE-2024-26960: linux-kernel: In the Linux kernel, the following vuln...
CSCwr07589	CVE-2024-26976: linux-kernel: In the Linux kernel, the following vuln...
CSCwr07616	CVE-2024-35823: linux-kernel: In the Linux kernel, the following vuln...
CSCwr07620	CVE-2024-35835: linux-kernel: In the Linux kernel, the following vuln...
CSCwr07633	CVE-2024-35888: linux-kernel: In the Linux kernel, the following vuln...
CSCwr08024	LuaJIT through 2.1 and OpenRusty luajit2 before v2.1-20240314 have an ou
CSCwr08027	LuaJIT through 2.1 and OpenRusty luajit2 before v2.1-20240314 have an un
CSCwr08067	Netty is an asynchronous, event-driven network application framework. Pr
CSCwr08069	Jetty through 9.4.x is prone to a timing channel in util/security/Passwo
CSCwr08070	In Eclipse Jetty HTTP/2 server implementation, when encountering an inva
CSCwr08089	The exception handling code in Eclipse Jetty before 9.2.9.v20150224 allo
CSCwr08161	An integer overflow can be triggered in SQLiteâ€™s 'concat_ws()' function.
CSCwr08162	There exists a vulnerability in SQLite versions before 3.50.2 where the
CSCwr08167	When reading a specially crafted 7Z archive, the construction of the lis
CSCwr08168	When reading a specially crafted 7Z archive, Compress can be made to all
CSCwr18516	CVE-2024-35960: linux-kernel: In the Linux kernel, the following vuln...
CSCwr18518	CVE-2024-38541: linux-kernel: In the Linux kernel, the following vuln...
CSCwr18519	CVE-2024-38612: linux-kernel: In the Linux kernel, the following vuln...
CSCwr18522	CVE-2024-41110: docker: Moby is an open-source project created by Doc...

Bug ID	Headline
CSCwr18525	CVE-2024-58250: ppp: The passprompt plugin in pppd in ppp before 2.5....
CSCwr18527	CVE-2023-24531: golang: Command go env is documented as outputting a ...
CSCwr18660	CVE-2024-46981: redis: Redis is an open source, in-memory database th...
CSCwr18666	CVE-2025-38352: linux-kernel: In the Linux kernel, the following vuln...
CSCwr18667	CVE-2024-35955: linux-kernel: In the Linux kernel, the following vuln...
CSCwr18669	CVE-2024-36623: docker: moby through v25.0.3 has a Race Condition vul...
CSCwr18675	CVE-2024-38473: apache-http-server: Encoding problem in mod_proxy in ...
CSCwr50762	DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTM
CSCwr50784	DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTM
CSCwr50785	DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTM
CSCwr50812	An issue in canvg v.4.0.2 allows an attacker to execute arbitrary code v
CSCwr50813	jsPDF is a library to generate PDFs in JavaScript. Prior to 3.0.2, user
CSCwr50814	jsPDF is a library to generate PDFs in JavaScript. Prior to 3.0.1, user
CSCwr50816	In all versions of the package jspdf, it is possible to use <<script>scr
CSCwr50818	In axios before 1.7.8, lib/helpers/isURLSameOrigin.js does not use a URL
CSCwr50823	axios is a promise based HTTP client for the browser and node.js. The is
CSCwr50830	axios 1.7.2 allows SSRF via unexpected behavior where requests for path
CSCwr50831	Axios is a promise based HTTP client for the browser and Node.js. When A
CSCwr50836	DOMPurify before 3.2.4 has an incorrect template literal regular express
CSCwr58661	Cisco Secure Firewall Adaptive Security Appliance Software TCP Flood Denial of Service Vulnerability
CSCwr80920	SFDataCorrelator backtrace every 1 hour after VDB update on FMC
CSCwr89322	FPR3100 May Not Power On After Upgrade or Reboot
CSCwr99016	FMC should fail the policy deployment in case of any interface/zone installation issues.
CSCws03492	ASP ACL rule (dhcp network scope) fail to be removed during "no nameif" or interface deletion process
CSCws23151	Deployment Failure soon After Removing An Object From ACL Used in DAP even before commit
CSCws35715	ASA/FTD responding without relay_sig parameter in SAML dupicate request

Bug ID	Headline
CSCws50416	Snort 3 Rule update not working if version field not updated
CSCws82462	ASA/FTD traceback and reload after applying capture type isakmp command from LINA CLI

Table last updated: 2026-04-15

Table 21: Resolved Functional Bugs in Version 7.4.7

Bug ID	Headline
CSCvm76755	DP-CP arp-in and adj-absent queues need to be separated
CSCvu71962	User-Role permission for Object-MGMT "Find-Usage"
CSCwb07908	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
CSCwc85758	Last Synchronized date in FMC smart license status is not always accurate
CSCwd55939	scheduled task may not run at all if UTC start times (based on DST) are on different calendar days
CSCwd92327	on 2k platform, external authentication fails for users starting with number
CSCwe13965	Interface statistics and tunnel uptime display support for VTI/DVTI interfaces
CSCwe81291	FTD unit comes up with HA disabled when configuration backup is restored
CSCwe89720	Misleading error message while attemtping to revert upgrade on inelligible device
CSCwe98264	Snort3 cores on Firepower 2100 series FTD in driver code
CSCwf72285	DAP: debug dap trace not fully shown after 3000+ lines
CSCwh05126	FDM HA Switch : Peer fails to get into Active state due to Interface check
CSCwh24932	ASA software on FP3110 showing incorrect serial number in show inventory output
CSCwh51909	Message for upgrade_resume.sh failure failure due to resuming on /new-root should be enhanced
CSCwi03494	S2S tunnels shown inactive on FMC dashboard though tunnels are up on FTD due to out-of-order events
CSCwi31680	Unable to upgrade FTD after revert from a CDFMC-supported version to a non CDFMC-supported version
CSCwi58772	Error 403: Forbidden when tried to access certificate trustpoint enrolment page on FMC Domain user
CSCwi72410	Member interface admin status is not updated on Lina after enabling port-channel interface

Bug ID	Headline
CSCwi80453	Active node reload during peer app sync or config sync causes premature failover, config sync failure, and unexpected reboot
CSCwi81772	Unable to export and import AC-policy in the same FMC version (Snort2 or snort3 IPS corruption related bug, where stale entries are present)
CSCwj21985	Debug: Eth1/1 flapping unexpectedly
CSCwj23860	Counters are not matching between cluster exec and show cluster access-list
CSCwj32736	SNMP walk does not work if IP is configured after SNMP is configured on ngfw management interface.
CSCwj35821	FTD: Invalid counter for TCP_PRX PROBE_TOTAL_ACTIVE_CONN
CSCwj42875	FMC HM showing "normal" eventhough FTD having Comm Failure
CSCwj53663	TPK: FXOS does not cleanup RM queues on MI instance start failure
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
CSCwj61066	Merged PCAP file from 'capture traffic' CLI is smaller than anticipated, or appears to be missing packets
CSCwj61834	IPSecOffload: Traffic gets dropped when esp null encryption is used on the ipsec proposal
CSCwj69780	SNMP host group content change results in SNMP process termination on management interface
CSCwj72560	Error 'Wait for registration to complete' seen in packet tracer page if device template was applied to selected device
CSCwj78144	OSPFv2 connections through inline set in cluster are shown as centralized
CSCwj78450	Removing switch capture configuration from CLI deletes capture PCAP files from disk
CSCwj81031	snmpd core seen in ASA/FTD
CSCwj86320	Standby Unit Interfaces enter "Waiting" Status Post-FTD Upgrade Due to Incorrect "Hello" Message MAC
CSCwj86527	SNMP v1 and v2c traps from diagnostic and data ints stop working on a KP/vFTD after product upgrade
CSCwj87770	FPR2100-ASA Unable to generate CSR without FXOS IP address on SAN field
CSCwj89033	Internal error screen displayed while navigating to next page on syslog ui
CSCwj91494	FXOS LTP: Some platforms return more than one image for analysis

Bug ID	Headline
CSCwj93718	Unable to run "nslookup" command on FXOS
CSCwj98345	Issue with FMC while using RestAPI for creating security zone object
CSCwj98648	Failure to read the signature keys (mult-instance deployment)
CSCwj99362	"show inventory" output shows Name: "power supply 0" on Firepower
CSCwj99620	Post upgrade to 7.4.2-S2S tunnel status is showing empty
CSCwk09488	Incorrect syslog generated on failure to process SGT from ISE during RA authentication
CSCwk10005	Config Sync Optimisation : fover_thread: Hash comparison timeout expired while computing config hash
CSCwk11264	FMC - Timestamps in "Analyze Hit Counts" dialog of AC policy are incorrect
CSCwk14657	Bring back support for portal-access-rule for weblaunch for RAVPN sessions
CSCwk15596	Re-Registering the FMC with on-Prem server is getting failed
CSCwk16332	ASA/FTD traceback and reload with high rate of SIP connections
CSCwk17798	In Multi-Instance FTD mode, the Data-Sharing interface remains in “Waiting” state after unit reboot followed by failover
CSCwk21562	Radius server configuration for FTD external authentication is not deployed to FTD.
CSCwk24684	qemu is being listed in show users cli command
CSCwk32748	FMC UI, when SNMP version is set to disabled, FMC doesn't verify community string
CSCwk32984	FPR3K SFP+(10G) optics:Port Channel mem intf becomes down after reload/flap/reinsertion on peer side
CSCwk33876	Standard Access List Objects can be written with leading whitespace
CSCwk35638	Dangling interfaces exists in SecurityZone/Interface group and interface
CSCwk36512	Add IPv6 to shun CLI
CSCwk38940	Peer sending proposal unacceptable during rekey after switch over for IKEv1 SVTI
CSCwk45257	‘Send Virtual Tunnel Interface IP to the peers’ flag is not properly set for backup VTI in DVTI
CSCwk48026	Increase connection retry count in 200_pre/100_get_snort_from_dc.pl
CSCwk59520	Instrument new logs in the startup process to collect more information
CSCwk62040	Warning should be given when large IP range is used in mapped source along with service keyword

Bug ID	Headline
CSCwk63011	Incorrect network module slot and status information in "show module" command output
CSCwk64643	Failover prompt shows state active while the firewall is in Negotiation
CSCwk70673	Certificate validation fails with trustpool when FIPS is enabled
CSCwk73583	FMC restore should be marked failed when cfgdb dump fails during restore
CSCwk74566	Disable csd/hostscan invokation for clientless/webvpn flow
CSCwk75835	Sftunnel still existing with older IP for standby unit even after changing the ip address from FMC.
CSCwk79288	Partition "/opt/cisco/config" gets full due to btmp file not getting logrotated
CSCwk82462	Cluster disabled while modifying the coredump filesystem
CSCwk83680	Increase sftunnel AUTH_TIMEOUT to 60
CSCwk87599	show conn detail rx-ring 4294967295(max val)filter displaying connection having invalid rx-ring num
CSCwk87700	Multiple core.svc_sam_statsAG on FxOS platforms
CSCwk94449	Include show mgmt-ip-debug in fxos tech support
CSCwk95916	Missing CPU and Memory threshold adjustability under Health Policy
CSCwk97677	TPK-MI FTD instance getting validation error and ftds in splitbrain HA post upgrade 7.6.0-1685
CSCwk99901	Lina crash at compTriggerEventbyName on WM with 100% memory utilization
CSCwm02802	"clear configure interface" causing ACK/FHELLO drops during HA break on standby
CSCwm03198	Migration of TPK native cluster failed because of sftunnel process going down.
CSCwm03287	FP4245 - NPU Accelerator changed speed of 100Gb interface to 10Mb
CSCwm05158	"Failed to upgrade firmware Image" fault should mention the firmware that failed to upgrade
CSCwm07323	Creating cluster bundle tar files for cluster failing with remote storage SSH configured
CSCwm13239	DNS Feed and Network Feed are failed on Standby FMC after upgrade
CSCwm26915	Intermittent ftd_ha_info directory creation failure; WM1120
CSCwm28962	Large number of Error messages in HA fover_trace.log file cause log rotation in small amount of time
CSCwm31501	SFDataCorrelator memory leak for Intrusion event extra data

Bug ID	Headline
CSCwm33529	FXOS MTU Handling for Front Panel and Uplink Ports on Firepower devices require improvement
CSCwm33557	ibdatafix script needs to address cfgdb if the FMC is running version 7.3 or higher.
CSCwm35144	cdFMC: ADI proxy terminated multiple times on TPK MI when used as proxy on REALM
CSCwm38027	one of the instance went to start-failed state on WA4245-760-102
CSCwm40744	Enhance nlp debuggability and provide persistency for the nlp logs
CSCwm48550	Secure Firewall CSF-1200: sma reported fault: Lina has started, but is not yet running
CSCwm49213	Show mod functionality needs to be fixed after change was reverted in CSCwk63011 due to regression
CSCwm56731	ASA 9.16 SSH Client login to User-Context is not working with ecdsa
CSCwm63670	Propogate SGT deployed to FTD if copy deviceconfiguration(SGT configuration UI andLINA doesnt match)
CSCwm69074	ASA PKI - MS cert policy extension not handled properly
CSCwm69085	ASA will crash on certificate display commands
CSCwm70356	Deployment failing with "no nameif" on the failover interface
CSCwm76872	Lina traceback and reload on ztna app disable
CSCwm80210	MI: core.lina.async_thr is generated after reboot
CSCwm82566	FMC displays VPN tunnel status as unknown even when the tunnels are up
CSCwm83033	Invalid Name Warning Missing from FMC after upgrade and Save greyed out (Configure DAP records through Rest API)
CSCwm85795	Access Control Policy export fails due to dangling object on Intrusion Policy Recommendations
CSCwm86414	ASA - Failover config resync failed and unexpected reboot occurred
CSCwm87653	Unused objects deletion taking longer time
CSCwm88812	4200/3100/1200 hardware allow to change AppAgent timer
CSCwm89747	Deployment failed with the reason "Error-no dhcpd enable inside"
CSCwm91406	FTD HA Standby Reloads Repeatedly After Upgrade to 7.4.2.1
CSCwm99199	MariaDB import failure that lead to FMC-HA Synchronization Incomplete
CSCwn04201	SNORT2 High CPU Utilization (100%) during user_enforcement SXP Data Sync

Bug ID	Headline
CSCwn06645	FIPS self-test failure message needed
CSCwn10173	Not able to create ssh session when changing key-lengths
CSCwn14108	Classic license validation on standalone FMC may fail due to lower case letters in license key
CSCwn14458	FMC: Enable validation of "Comment" Field under Automating Policy Deployment Tasks
CSCwn15443	Crash/assertion in snp_vpn_int_api during extended VPN traffic tests
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
CSCwn19159	Few Snort3 IPS rule preset filters are not working correctly
CSCwn22708	FMC does not delete intrusion rules from database when they are removed from LSP
CSCwn23987	Port block distribution issue is seen on 9.18
CSCwn27583	High lina CPU and/or Traceback and reload in spin_lock_get_actual_internal
CSCwn27872	Big chunk of Memory of around 25KB is being allocated on Stack in "eigrp_interface_ioctl" API
CSCwn28902	FMC not using configured proxy for smart licensing
CSCwn30151	ASA crashes on password change attempt
CSCwn31151	Newline character in interface description results in deployment failure
CSCwn32025	FMC Management workflow issue: Cannot remove NetworkObject from group and delete it in same ticket
CSCwn32978	Traceback and reload in Thread Name Datapath
CSCwn35495	Primary FTD instance MAC address is not updated correctly in FXOS during failover
CSCwn36712	NAT divert for 8305 on standby not updating post failover causing the Primary, standby FTD to show offline on FMC
CSCwn37490	ACP copy not possible in Firepower Management Center
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
CSCwn39777	Unreachable Hosts and URLs of syslog configuration Block Device Management Page Loading

Bug ID	Headline
CSCwn39810	FMC to warn users when deploying other configs alongside FlexConfig.
CSCwn40702	ASA traceback and reload in freeb_core_local_internal
CSCwn45194	FMC can generate health alerts when ntp temporary switches to HW local clock from external server
CSCwn46861	Multi-Instance in Secure Firewall not updating sftunnel certificates
CSCwn50760	ASA Traceback after upgrade to 9.20.3.7
CSCwn55195	Deploy Preview comparison PDF report not getting generated
CSCwn55890	SAML DNS LB fails to redirect to local host when local-base-url contains uppercase letters
CSCwn59032	FCM GUI became inaccessible after upgrading to ASA 9.18.4.22 | FPR 2130 Platform Mode
CSCwn59596	“Copy when complete” option not working for SSH Public Shared Key Authentication on FMC
CSCwn60836	FTD: deploy failure when configured L2 access-list. "Cannot mix different types of access lists."
CSCwn61041	Traceback and reload during clear bgp * ipv6 unicast involving watchdog
CSCwn61176	EventHandler not restarted after running system support reset-event-bookmarks on FTD 7.2 and above
CSCwn61232	Memory block corruption: RAVPN SSL/IKEV2 auth failure, AAA SHIM available fibers exhausted
CSCwn64025	ASA: IPv6 EIGRP routes learned from other neighbors are missing in updates after failover
CSCwn64992	FMC1600-K9 PDF download failed in deploy tab
CSCwn65336	FTD is droping TCP syslog messages
CSCwn69340	cdFMC - Unable to save network group object
CSCwn69488	ASA/FTD - Traceback and Reload in Threadname IP RIB Update
CSCwn69653	Ipv6 TCP Syslog are not properly generated on WM-HA Active unit in 7.7.0-1607
CSCwn71426	Clearing all non applicable alerts post license registration success
CSCwn71946	show blocks old core local can lead to unexpected reload.
CSCwn72938	Smart license UI on cdFMC and FMC showing duplicate license count for Malware , IPS , URLFilter and Apex
CSCwn76740	FMC UI login fails with "Unable to authorize access."

Bug ID	Headline
CSCwn78693	FMC: OSPF NSF-awareness (helper mode) cannot be configured on a standalone FTD
CSCwn81118	RTSP packets getting stuck in transmit queue leading to 9k blocks exhaustion.
CSCwn81398	FMC Does not throw error with duplicate entries in input while modifying prefix list through API
CSCwn81833	FMC User permissions allows user to Suspend HA even when "Modify Devices" is not selected
CSCwn84743	User EO revisions accumulate forever, eventually overflowing Pruner's ability to do its job
CSCwn85765	ipv6 ping Vrf name changed after xml processing
CSCwn87164	Validation is missing when PC is used in both DHCP relay agent as well as in server server-side intf
CSCwn90327	FP1150 ASA/FTD - Traceback and reload triggered by watchdog timer
CSCwn91996	WM-DT- FXOS Critical Faults seen due to PortMgr IPC Communication failure.
CSCwn92066	FTD Clish: "more.fxos" process is left running when the ssh terminal session is abruptly terminated
CSCwn92074	FMC managing various lower version vFTDs throws Event Handler errors
CSCwn96963	FTD generates syslog 430002 as VPN Routing without VPN hairpin
CSCwn97341	MonetDB Monitor should detect missing columns in stats partitions
CSCwn97610	Policy Deployment Failure Due to Special Characters in AC Policy Rule Names
CSCwn97630	FTD reboot and traceback in DATAPATH due to IPv6 packet processing
CSCwn97956	Error thrown for individual rule hitcount if rule name contains certain special characters
CSCwn98642	Dynamic Analysis Status Changed time only changes upon submission of a file for dynamic analysis
CSCwn98665	Use of browser Refresh button on the Captured File Summary page may result in an unexpected warning
CSCwn99481	Core file generated completely, but the contents are inconsistent on FPR 2100
CSCwn99640	FTD Upgrade Failure on Script 800_post/020_710_fix_users_and_roles.pl
CSCwn99755	Warning messages from using Analyze button on Captured File Summary page need to be more specific
CSCwo00165	printf: minus sign is not handled properly when width modifier used.
CSCwo01653	Unable to login to FMC GUI due to HTTP 401 UNAUTHORIZED error

Bug ID	Headline
CSCwo03932	Aggressive scale down and scale up of nodes causing the failure
CSCwo05712	Serviceability Enhancement - Make FXOS disk errors more descriptive
CSCwo05899	ZIP files are not being transferred when Archive category is selected from File Policy using snort3
CSCwo06044	Exclude perf monitoring files from device backup
CSCwo06205	Multiple TCP logging host with timestamp option not working with IPv4 & IPv6 host
CSCwo08724	Active HA unit goes into failed state before peer unit gets into a ready state during snort failure
CSCwo09439	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-3-4280'
CSCwo14706	Buffer calculation for new app_bin missing in the upgrade framework
CSCwo14722	Prune the older files in /ngfw/var/cisco/deploy/pkg/var/cisco/packages
CSCwo14737	FTD - LSP Installation/ Deployment Failure
CSCwo14870	FMC upgrade page shows upgrade failed but the device is upgraded
CSCwo15059	Backup may fail with generic "Backup died unexpectedly" error message
CSCwo15715	IKEv2 Rekeys fail due to fragmentation during the IKE Rekey
CSCwo15787	Importing SFO fails with the error "No UUID Provided"
CSCwo18786	Snort3 restart on the first deployment post FMC upgrade.
CSCwo19762	Unable to rejoin data node in cluster after re-enabling mac-address auto in multi-context mode
CSCwo20629	Better handling of invalid/bad data in fleet upgrade workflow.
CSCwo21105	process_stderr.log: Could not open link aggregation log file '/ngfw/var/log/link_aggregation.log'
CSCwo21830	Reduce TS package size
CSCwo22091	FTD sending "0.0.0.0" NAS-IP-Address attribute when authenticating/authorizing using Radius
CSCwo24856	9K block depletion causing slowdown of all traffic through firewall
CSCwo25473	DNS and default gateway are removed on FTD managed through data interface - DNS
CSCwo25624	Deployment failure due to invalid AnyConnect Images and Secure Client Profile references
CSCwo25786	REST Api allows to create a realm without a directory configuration

Bug ID	Headline
CSCwo25834	Enhance Backup Status Notifications for Unified Backup Failures on FMC
CSCwo25854	Upgrade failure after RMA due to Sensor table having incorrect serial number
CSCwo26181	Unexpected SFDataCorrelator exit after deployment to managed devices following VDB install on FMC
CSCwo26725	FMC Site-to-Site Monitoring Dashboard is not working at all
CSCwo27260	Unit taking ~13 secs to become active
CSCwo28967	FMC remote storage test sometimes fails when configured to a server running Solar Winds SCP/SFTP
CSCwo31094	Virtual ASA Traceback and Reload Caused by Disk Access Issues with NFS Enabled
CSCwo33573	FMC Alert: Discover Health Module Compilation Error
CSCwo33733	CIMC Password length restricted to 16 characters with LOM enabled
CSCwo33815	FMC: Deployment takes longer than expected when removing SNMP hosts from Platform Settings
CSCwo34893	Remote storage server password showing in plaintext in httpsd_error_log
CSCwo36485	ASA/FTD traceback and reload in vaccess_nameif_action thread
CSCwo37500	Remote backup generated successfully but configuration database backup is empty
CSCwo38354	Smart license UI showing variable performance tier when stand by FMC is made active
CSCwo41594	SSL Debug Logs Persist After Debug Reset
CSCwo42501	Module show tech generation fails with external authentication
CSCwo45449	Ensure the watchdog triggers even if a single snort3 thread becomes unresponsive.
CSCwo45497	Counter from IKEV2 stats does not match the number of tunnels in VPN-Sessiondb
CSCwo46142	Port-channel member interface flap renders it as an inactive member
CSCwo47498	Disabling OSPFv3 on FMC does not clear passive interface and area config from FTD interfaces
CSCwo47760	FMC IPsec SA remaining key lifetime incorrect conversion of seconds to hh:mm:ss
CSCwo47929	Cluster node got deleted partially and devices have become Standalone on FMC UI
CSCwo48157	syslog-ng may not immediately restart on FTD as expected upon changing FTD host name
CSCwo49229	Fleet copy package fails: Copies completed but failed to be acknowledged by device(s): 1.

Bug ID	Headline
CSCwo49337	FMC - Health Monitor shows 'No Data Available' due to too many open files
CSCwo50417	Warwick Avenue: LLDP neighbours are not discovered if MGMT 1/2 interface is down
CSCwo50551	Decryption policy failed to migrate to cdFMC from on-prem FMC.
CSCwo52139	Error after logging out from FMC UI using SSO with PingId
CSCwo53752	ASA FTD traceback in Checkheaps process after enabling "controller monitor internal-interfaces free-blocks 100" command
CSCwo54265	Upgrading a 7.0.x sensor to 7.0.7 when managed by an FMC via hostname results in errors
CSCwo54996	Traffic failure due to 9344 blocks leak
CSCwo57740	'${dsk_a} missing or inoperable. Rebooting Blade.' error does not specify missing or inoperable disk
CSCwo58033	[Cluster] CPU Utilization of 100% when NAT Pool exhaustion happens in a context.
CSCwo58191	FTD: Large Delay in packets being inspected by snort
CSCwo60436	LINA core observed pointing to "IP RIB Update" thread
CSCwo60579	FTD does not synchronize via NTP from Secondary Management Center in HA when the Primary is down
CSCwo60609	DNS doctoring not working correctly if the doctoring rule is of type dynamic and has any interface
CSCwo61241	Logical App Stuck in 'Start Failed' Due to checkSystemCPUs Failure
CSCwo61788	Failover and state link not accepting valid subnet mask
CSCwo63563	mix of major versions between FMC and FTD causes per-core CPU use health module to not work on FTD
CSCwo65060	FTD HA | Same MAC for port-channels causing network outage.
CSCwo65381	Deployment to FTD Fails at 5% due to corruption with interface object
CSCwo69015	Refresh Icon on Inventory Details Fails to Update Chassis Information for All Models
CSCwo71976	Handle cases where Vault is not running during task execution and add health Alert
CSCwo72352	Memory leak: ASA Fragment size 72 causing memory exhaustion in MEMPOOL_GLOBAL_SHARED POOL
CSCwo73059	Captured file status is not updated if threat score is cached on FTDs
CSCwo73901	Bulk Edit Rules - Security Zone Search does not yield all zones if zone count is more than 1000

Bug ID	Headline
CSCwo74305	Deployment Failure in Hub and Spoke VTI Topology with DHCP Configured VPN Interfaces
CSCwo74496	BFD flap due to ASA not processing incoming BFD packets after unrelated BFD peers go down
CSCwo75024	Columns missing from event partitions
CSCwo75810	SNMP configuration is not applied consistently across same FTDs type and version
CSCwo76165	Deployment failure due to rsync
CSCwo76559	ASA/FTD traceback and reload with SNMP Notify Thread seen on 3110
CSCwo77665	Portscan event in FMC displays incorrect source/destination when set to 'low' setting
CSCwo78969	Traceback in thread name DATAPATH when a unit is re-joining the cluster
CSCwo79004	deployment slowness seen when huge number of policies are present
CSCwo79028	Post-Failover FQDN Resolution Deferred Until Next DNS Poll Interval
CSCwo79080	ENH: UDP traffic flow requires Initiator and Responder fields in the "show conn detail" output.
CSCwo79798	Cryptochecksum changed after reloading.
CSCwo80682	Saving changes under Policy > Alerts > Intrusion Emails in FMC GUI multiple times removes old changes
CSCwo81874	'configure network management-data-interface' allows to configure same IP on data and mgmt interface
CSCwo82639	Local user details not replicated to data nodes in a cluster setup.
CSCwo82658	ASDM: Displays Error of Keypair already exists when adding an identity certificate.
CSCwo84910	Deployment failure not updated on databases of data node
CSCwo85252	FMC page may get stuck in loading state while trying to fetch BGP configuration
CSCwo87219	Boot-Time warning if CPU core count is below minimum requirement
CSCwo87763	ASA/FTD: Primary standby unit becomes Active after reload in HA set up
CSCwo88011	ASA SSH login fails at the first attempt when it is integrated with DUO
CSCwo88204	ASA/FTD traceback and reload triggered by the Smart Call Home process in sch_dispatch_to_url.
CSCwo88518	If command replication fails to any nodes in cluster, send kick the node out from cluster to fmc
CSCwo88745	Policy deploy would not write entries when referenced object is missing

Bug ID	Headline
CSCwo89233	Command replication failure to cluster nodes on command commit noconfirm revert-save after access-list, additional debugs
CSCwo89802	FMC Custom widget to display host count per sensor shows incorrect sensor name
CSCwo90300	"Error during policy validation An internal error is preventing the system... "due to stale sensor ref in security zones
CSCwo91049	Missing RADIUS accounting response messages may result in delays or failures of connectivity from chassis to instances
CSCwo91124	FTD: Excessive logging for UserGroup
CSCwo91436	FPR 4125 Multi instance: High Snort and System Core CPU Usage (100%) Triggering FMC Critical Alerts
CSCwo91631	FMC Unable to Download User Groups from AD Realm via LDAP
CSCwo91965	ASAv restarts unexpectedly
CSCwo92386	cdFMC Not Displaying Interfaces and Security Zones When HA Secondary Device Is Active
CSCwo92447	FMC Displays SSE Enrollment Failure Alarm Despite No Active Integration with SecureX
CSCwo93174	Duplicate VTI cause VPN Flaps
CSCwo93444	FTD Cluster: Incorrect log when snort engine restart times out
CSCwo94483	LINA stays inactive without reloading after traceback on non-CP thread
CSCwo95586	Users with "Modify Threat Configuration" permission are not able to modify Intrusion/File Policies within the Access Control Policy (ACP) rules
CSCwo96377	Secondary Address should only be configurable for FMC-managed FTDs when using data interfaces for management
CSCwo96854	Unable to Edit or Break FTD-HA via FMC GUI because of UI lock issues during create
CSCwo98752	Traceback in threadname DATAPATH while trying to re-join cluster.
CSCwo99544	Excessive number of AD users in FTD External Authentication could lead to deployment failure when disabled.
CSCwp01015	ASA/FTD traceback and reload in function mp_percore
CSCwp01325	Disabled rule parameters incorrectly carried over to new rule in child policy
CSCwp04235	ASA traceback and reload
CSCwp06882	high CPU usage after ASA upgrade from 9.20.3.9 to 9.20.3.16 running on Hyper-V

Bug ID	Headline
CSCwp06995	FMC Restore of remote Unified backup fails due to no space left on the device
CSCwp07108	Lina crash in threat detection due during first deployment after upgrade
CSCwp08772	ASA: tls-proxy maximum-session command error
CSCwp10123	ESP packets encapsulating subsequent fragments are dropped with ASP unexpected-packet drop reason
CSCwp10957	SSL error causing connection to Cisco Smart Software Manager (CSSM) to terminate
CSCwp11382	ASA/FTD: the ssl trust-point command deleted after a reload
CSCwp11503	User Creation Fails with RADIUS Dynamic Provisioning Enabled on Firepower device.
CSCwp11971	FMC GUI Inaccessibility and blank due to 'Malformed JSON String' Exception
CSCwp11985	Deployment is mandatory after FMC upgrade condition should be included in Upgrade code
CSCwp13016	FTD/ASA SSH: Terminal monitor is not showing logs
CSCwp13540	Wrong URL incorrectly displayed for file upload with Japanese text in file path for client-less VPN
CSCwp14919	The Firepower bandwidth_analyzer.pl script does not perform proper input validation for the '--size' option
CSCwp16323	FMC Audit tcp-tls syslog is truncated or incorrectly formatted
CSCwp16529	Negative value displayed for buffer drops when using " show cluster info load-monitor details"
CSCwp16739	ASA crashinfo files not generated on FP4200 devices
CSCwp17700	Syslog format is not properly printed when EMBLEM format is enabled at least in one syslog host
CSCwp18136	ADI cores reading corrupt SXP file
CSCwp22214	Multiple mail drops and enq failures are seen while traffic is going through the box.
CSCwp22237	depoyment failure reason and transcript to be updated on FMC
CSCwp22612	Policy deploy failing on FTD when trying to remove Umbrella DNS Configuration
CSCwp26815	CPU usage by "WebVPN Timer Process" on standby ASA device
CSCwp28801	WA HA: Error while fetching metadata for FTD HA.
CSCwp29273	Case differences in SAML SSO usernames cause login loop
CSCwp29808	FMC reporting IPv6 non overlapped host object-group as fully overlapped object-group

Bug ID	Headline
CSCwp31169	Multiple consumers try to bind to the same ZeroMQ socket
CSCwp32352	Deploy failure when Indexing is not working
CSCwp32949	Deployment failure when selecting ECMP zone member interface in ZTNA policy
CSCwp33077	SAML IdP entityID increase from capped 128 character maximum
CSCwp33410	dmesg and kern.log file flooded with Tx Queue=0 logs
CSCwp37284	"CSRF Token Mismatch" error seen when users click logout from Clientless VPN page
CSCwp38220	Internal error is seen when editing the rule with IPV6 contents
CSCwp38436	The chassis serial number is empty post registration in FMC
CSCwp39266	Traffic drops post deployment when secondary skips app sync and become active immediately after bootstrap config apply
CSCwp39319	ASA Memory leak while processing large CRLs.
CSCwp59765	LDAP users in ACP always show realm out of sync.
CSCwp60896	ASA Clock reverts to UTC after device reload
CSCwp64615	ASA/FTD: ASP drop capture for 'invalid-ip-length' or 'sp-security-failed' does not work with match criteria
CSCwp64709	Table on Syslog Settings tab in FTD platform settings policy may appear with improper dimensions
CSCwp65900	Customer DU CONSULT, NPS 6 - ACP search toggle for exact IP or Port match
CSCwp65952	WA/TPK: EPM FPGA upgrade chooses incorrect bundle
CSCwp66721	Memory leak in SSL crypto causing high Lina memory usage on lower-end devices
CSCwp67341	Opening, imported policy says internal error.
CSCwp67356	HA state should not transition from ColdStandby to Active
CSCwp80058	FMC Auto Deployment Task fails to run repeatedly
CSCwp89969	Prolonged delays in firewall restart/reboot completion
CSCwp90780	Restoring .tgz context file causes allocated interfaces to be removed from 'system' configuration
CSCwp91205	Need to have deploy Warning for IKEv2 Policy with same Priority Conflict in FTD VPN Configurations on FTD
CSCwp92644	FMC Dynamic Objects Limited to 1000

Bug ID	Headline
CSCwp93368	LINA traceback Observed on FTDv Firewalls Deployed in Azure: snp_vxlan_encap_and_send_to_remote_peer
CSCwp95742	FMC Overview Connection Summary Shows No Data by Responder IP
CSCwp97009	Threat/AMP Upgrade tasks are being created soon after HF installation completed
CSCwp97430	Missing Security Zones in zones.conf Affecting ngfw.rules Functionality
CSCwp97862	If failover IPSEC PSK is 78 characters or greater HA breaks with "Could not set failover ipsec pre-shared-key"
CSCwp97933	Inventory details on FMC GUI shows the incorrect compliance mode
CSCwq01683	Stop generating health alerts for transient high CPU utilization
CSCwq07197	Issue with interface status visibility in Firepower Chassis Manager 4225 managed by FMC
CSCwq07441	Memory Leak observed on FP2110 running ASA due to monitoring interface configured in HA
CSCwq07808	FP3105 Traceback and Reload after changing the speed on Ethernet interface
CSCwq13510	FMC generate_certs.pl script fails to regenerate CA Certificate
CSCwq14206	FTD incorrectly transitions TCP state to established when client sends RST after SYN-ACK
CSCwq14900	Audit Logs Display Repeated Session Expiration Entries Even When the System is Idle
CSCwq16926	Traceback and Reload while two processes attempt to free a TD subnet structure
CSCwq17612	Misleading "failover reset" log printed on console when reload triggered by HA.
CSCwq20535	management-data-interface commands fail with "Enable of interface failed" error due to case-sensitive interface name
CSCwq20891	CoA processing stops after DAP
CSCwq23394	FTD may drop traffic in the Azure cloud at mlx5 driver level.
CSCwq26503	Policy Deployment tasks should not be stuck indefinitely
CSCwq26863	FP2110 - ntpd process constantly crashing
CSCwq27217	ASA: Traceback and reload on threat detection, interfaces unstable after that
CSCwq28003	Duplicate messages during deployment to be discarded by CD to avoid further deployment failures
CSCwq29010	Snort3 blocking ESMTP traffic intermittently and trigger IPS signatures: 124:1:2

Bug ID	Headline
CSCwq29375	ASA/FTD - Assert triggered during FP_PUNT replace (aaa account match)
CSCwq29706	Traceback and reload after editing SNMP config, with tmatch
CSCwq30062	Local FTD backups are failing due to a lack of disk space on /tmp.
CSCwq30330	Long running AQ task got killed after timeout on FMC but corresponding backup task on FTD is still running
CSCwq31342	FPR4200 | FPR3100 Multi Instance Chassis Deployment Failed in DNS configuration
CSCwq31988	Errors on all interface of FPR1010 | line protocol is down (not associated with supervisor)
CSCwq36466	expat/xml FW rebooted itself and no crashinfo generated
CSCwq39149	Manually Downloading VDB Update Requires Manually Refreshing the Web Browser to get the VDB Update to be Displayed on the Page
CSCwq43365	Dynamic Attributes Connector Status shows One or more services are unhealthy
CSCwq43711	Idle SSH sessions persist beyond the configured timeout without graceful termination by Fin flag
CSCwq44834	Multicast and broadcast packets do not reach all multi-instance firewalls via shared interface on 3100/4200
CSCwq44862	Intrusion Event Packet Data via syslog/estreamer show no packet data for large packets
CSCwq45017	SmartLicensing should accept certain special characters
CSCwq46058	ASA SNMP Response Issue - Responses Sent Only for Odd OIDs, Not for Even
CSCwq47622	Lina Traceback and Reload after enabling 'TLS Server Identity Discovery'
CSCwq47694	Unable to use the plus sign in the email-id for the identity when configuring an S2S VPN
CSCwq48085	Deployment failure soon after forming FTD HA
CSCwq50189	ASAv deploy failed - console stuck at continuous
CSCwq50190	Multiple System Configurations Missing from FMC GUI Post-Upgrade
CSCwq52188	FTD Traceback while executing 'asp load-balance per-packet'
CSCwq52255	SSH login to FTD management IP address lands in FXOS shell instead of FTD CLISH due to missing /mnt/boot/application/*.def file
CSCwq54109	FTD 3130 HA Lina tracebacks at ikev2_bin2hex_str
CSCwq55841	FMC Upgrade stalls Indefinitely at 999_update_onpremfmc_diskcache.sh

Bug ID	Headline
CSCwq57394	Unable to edit Dynamic Analysis Connection cloud settings when FMC cannot connect to the US cloud
CSCwq59563	FMC uses old DNS server for resolution despite correct configuration
CSCwq60125	FTD is not sending a reset packet when the incoming traffic hits "block with reset" rule
CSCwq60586	FTD upgrade failed due to bundle image existence verification failure
CSCwq61583	FMC API: RAVPN sub-endpoints are unstable (When concurrent GET API calls are made, some might fail returning 404 'Resource not found' error for available UUIDs)
CSCwq61673	FMC does not allow to use IP address with 0 value in last octet as gateway while configuring static route for a device. Error: Enter valid IPv4 host value
CSCwq65499	FTD does not generate any events for the Platform Faults health module if no platform faults are present
CSCwq65955	FPR 4200: HA link arp packets getting dropped, internal uplink linkChange counters incrementing
CSCwq69599	FMC ACP Top User Deleted When Deleting Users With Legacy UI
CSCwq70133	Password Expiry Age does not reset after Password Change
CSCwq70773	show asp rule-engine issues with complete and run time
CSCwq71338	non-SSL traffic wrongly classified as SSLv2 causing drops with TSID enabled
CSCwq72156	SNMP traps are not sent to one of multiple SNMP servers, in certain conditions
CSCwq73733	FMC - Deployment Fails with "Deployment failed due to timeout during configuration generation"
CSCwq73994	ASA : Performance and high CPU usage seen on Hyper-V
CSCwq74204	IKEv1 L2Lvpn fails in phase 2 with "Rejecting IPsec tunnel: no matching crypto map entry" after upgrade
CSCwq74443	HA Primary/Active unit goes to disabled state as "HA state progression failed due to app sync timeout" in build 10.0.0-196
CSCwq74986	FTD: Instance stuck in Boot Loop
CSCwq77481	1140 FTD HA primary failed to reboot after executing the reload command from expert mode
CSCwq77569	SRU Upgrade Fails Due to Leaked Activity IDs from ClusterPostUpgradeHandler
CSCwq78813	Intermittent Blank Screen When Loading Access Control Policy in New UI
CSCwq80142	Possible unregistration when deploying during HA Switchover

Bug ID	Headline
CSCwq83097	FMC modify the BGP password that start with value "0x"
CSCwq83395	Not probing for http Opportunistic TLS
CSCwq85473	FP 4115 ASA Cluster: GTP inspection causing high lina CPU 70% - 90%+ depend on traffic
CSCwq88796	Firepower: SSH access lost after timezone change in platform mode
CSCwq88956	LSP Version not listed in dropdown under Intrusion Policies> Snort3 >Rule Overrides> Advanced Filters
CSCwq89972	FMC UI displays upgrade failure despite successful firewall upgrade
CSCwq90072	ASDM Parsing Failure on Two Contexts
CSCwq91155	Snort perf_monitor_base.csv memory data not getting populated
CSCwq92271	FTD HA devices marked as failed and deployment failure due to exception in CCMtoCDInQHandlerThread
CSCwq92728	ASA client IP missing from TACACS+ authorization request in SSH
CSCwq94584	Http inspector support for OPPORTUNISTIC_TLS
CSCwq95241	Reboots on FP2130 due to missing heimdall PID
CSCwq95649	Unable to upload Secure Firewall Posture image file with a size over 200MB
CSCwq95810	"no http server basic-auth-client ASDM" allows ASDM connections to ASA.
CSCwq96289	MonetDB may fail to start on FMC if maximum parallel/concurrent logins per CLI user is set to 1
CSCwq96870	Interfaces are coming up when the Firepower is shutting down
CSCwq98101	Policy deployment fails when inline-set is configured on FTD HA
CSCwq98155	'Access token invalid' is prompted, if a stress test is made on the ACP
CSCwq98648	Low RAM allocation on ASAv can trigger unexpected behavior in 'asdm image' command
CSCwr00252	Policy Import failure: Object ID Collision Causes ClassCastException
CSCwr00264	Flexconfig policy deletion left the stale references
CSCwr00282	cdFMC: All Device Deploy Validations were failing post deletion of Flexconfig for one device
CSCwr01037	Cleanup of perf_monitor files per instance per day
CSCwr01482	FPR4215 "Not supported" alarm occurred, when insert the SFPs

Bug ID	Headline
CSCwr05406	Traceback in HA stby node while snmpwalk on natAddrMapTable
CSCwr06290	ASA/FTD: Traceback in thread name CP Processing due to DCERPC inspection
CSCwr07401	Disabled manual nat rule is replacing the almost replica manual NAT rule
CSCwr08102	EventHandler wastes CPU re-scanning files that contain no requested events
CSCwr10732	Connection blocking active although "logging permit-hostdown' is set
CSCwr11046	Timeout values not honored after "sftunnel_change_max_conn_check.pl" changes
CSCwr11825	Sftunnel TLS13 connection goes down after upgrade when two interfaces configured with same IP on FMC GUI
CSCwr11851	Standby FMC Fails to Sync ids_event_class_map Table, Resulting in Misclassified Intrusion Events
CSCwr12965	Both the units in HA changed the encryption algorithm simultaneously
CSCwr13617	FMC API is reporting Windows for all AnyConnect images while querying RA VPN policies
CSCwr14186	add context for cmd-invalid-encap asp-drop type in the "show asp drop" command usage
CSCwr15611	ASA/FTD - 1550 Block Depletion Due to Instability of TCP Syslog Channel(s)
CSCwr15697	Block depletion - stuck at ssl_decrypt_cb location
CSCwr19123	FPR HA ESP sequence number discrepancy when standby changes to Active resulting in Anti-replay drops
CSCwr21583	Intermittent deployment stuck "in progress" for few devices
CSCwr21835	Dataplane <> Control Plane may be overwhemed in the event of a massive influx of traffic with no existing ARP Adj present
CSCwr21948	WCCP redirection not working as expected on transparent FTD
CSCwr22508	Device doesn't boot and gets stuck after a successful upgrade
CSCwr24365	SRU-triggered policy deployments occurred following initial/standby FMC during FMC HA & standalone upgrades
CSCwr24726	cloudAgent process error "CloudAgent: [ERROR] Update message is not of type dictionary"
CSCwr24999	FP3140 FTD HA Upgrade Getting Stuck
CSCwr26642	Slow UI and inability to check disk usage on FMC due to NFS configuration
CSCwr26857	File policy stops working due to SMB tcp conn terminated after 1hr for unknown reason despite not idle

Bug ID	Headline
CSCwr27095	Anyconnect users incorrectly get the prompts, based on the previous tunnel-group
CSCwr28908	ASA: Traceback and reload after saving asdm image
CSCwr29547	Empty Dynamic Attribute IP mappings pushed to FTD from FMC Secondary Unit
CSCwr30510	Deleting a domain using domain_manager --deleteDomain <domain_uuid> on FMC CLI brings down the estreamer service
CSCwr31136	SNMP OID Polling for Chassis temperature not giving response
CSCwr31700	RADIUS external auth doing one request per interface when bad username/password attempted
CSCwr31782	Secure Client SAML - External Browser May Prompt for a Certificate when using IKEv2-IPsec and Certificate Mapping
CSCwr32596	Missing Policy Based Routes on FMC PBR Page
CSCwr32852	FTD may generate a large number of "ssl-certs-unified" files.
CSCwr33630	TLS audit syslog configuration and certificates not replicating to secondary FMC in HA deployment
CSCwr35582	Continuous logs_archive.asa-interface-idb.log getting generated on ASA
CSCwr37941	FMC may not complete Cisco Security Cloud integration when using on-prem Smart Software Manager for smart licensing
CSCwr39798	Disable FEC mode when interface speed for 25G interface is reduced to 10G
CSCwr40191	The /api/fmc_netmap/v1/domain/{domainUUID}/hosts API endpoint not showing MAC addresses
CSCwr42577	ASA/FTD may traceback and reload citing Thread Name 'lina' as the faulting thread.
CSCwr42969	Dynamic Offloaded Flows Interrupted midstream
CSCwr43237	FMC is returning status code 400s of GET request for Get Device Data
CSCwr43392	cdFMC 7.7 Fails to Display Health Data for specific FTD's
CSCwr43586	Intermittent drop of self-originated ICMP TTL exceeded messages with reason "Unable to obtain connection lock (connection-lock)"
CSCwr43613	FTD/ASA may traceback and reload
CSCwr43734	FMC/FTD: Policy Deployment failure after disabling NVE Interface config in VTEP Tab of FTD Cluster
CSCwr45484	FTD Policy deployment reported as failed incorrectly on FMC when communications disrupted
CSCwr48605	Lina traceback due to the incorrect option being received in the packet.

Bug ID	Headline
CSCwr49028	Secure client tunnel group authentication is affected when using SDI protocol
CSCwr50466	ASA/FTD: Wrong value shown for X509_STORE_CTX in 'show ssl objects'
CSCwr50630	S2S VPN status for Topology with Extranet shows inconsistence at times. This is because when the tunnel status is received from the device bidirectional update should happen
CSCwr51629	RTSP Flows are dropped with drop reason "First TCP packet not SYN"
CSCwr55089	ASA/FTD - Traceback and Reload in Threadname DATAPATH
CSCwr57566	Unable to create interface object with a "same" name as earlier when we had a network connectivity issue
CSCwr57647	Upgrade failure on FMC on GCP 000_start/112_CF_check.sh
CSCwr58862	ASA/FTD: SCEP enrollment fails with SCEP server reachable over VPN and sourced from inside interface
CSCwr59870	ASAv on Hyper-v encountering boot loop issues when running netvsc driver
CSCwr61303	Lina: Traceback and reload webvpn_session_release
CSCwr61452	ASA traceback and reload due to memory corruption in IPsec SA pointers
CSCwr61629	GeoDB content is not restored when restoring a backup to a freshly deployed FMC
CSCwr62800	High network latency observed on ASAv
CSCwr62993	FTD traceback and reload on DATAPATH
CSCwr63632	Unable to upload VPN client profile package under Objects > Object Management > VPN > Secure client File to FMC while logged in via External User.
CSCwr64866	FTD: SSH/SFTP on port 200 is being misclassified as SRC
CSCwr65540	ASA traceback while disabling GTP inspection
CSCwr66525	WPK node rebooted with lina core while trying to form cluster in snp_nat_allocate_port
CSCwr71075	FP2140 running FTD traceback during deployment
CSCwr72101	Lina: Traceback and reload for watchdog on BGP
CSCwr72407	EIGRP adjacency fails over VTI(IPSEC)
CSCwr72556	Enhance UI error messages to inform users that deployment is not allowed due to version mismatch.
CSCwr72739	FMC scheduled backup task attempts to backup removed managed device resulting in error "Cannot trigger backup since sensor is not reachable"

Bug ID	Headline
CSCwr74420	FTD - FTD RADIUS authentication fails with "bad authenticator" after disabling Management Interface Convergence
CSCwr74751	Device->Certificates page not loading with error "Error in fetching certificate details"
CSCwr74768	Add validation on FMC UI to prevent admin to configure more than allowed IKE policies
CSCwr76081	security intelligence block list event logging can't be disabled
CSCwr78255	Inconsistent Cluster State: All Nodes Acting as Data Nodes with No Control Node
CSCwr79344	ASA/FTD traceback and reload in Lina
CSCwr79875	Warning Users When Creating Rules with Multiple 'Any' Fields in FMC
CSCwr81266	Unable to remove certificate-group-map
CSCwr83390	FPR-4200: Port-channel flaps while generating chassis FPRM
CSCwr83527	FP2110 Critical fault alerts for remote users
CSCwr83703	Deployment failure due to unrecognized command "vpn-simultaneous-logins none"
CSCwr84332	ASA/FTD traceback and reload in L2 vaccess_nameif_action thread
CSCwr85470	FTD silently drops out of order packets
CSCwr87102	Problems may arise when an automated script attempts to deploy to add or delete an SNMP user in a multi-context environment.
CSCwr87450	removing all usages of a DHCP IPv6 pool object from FTD interface config does not delete the object from FTD
CSCwr87762	deployment to FTD from cdFMC after migration from on-prem FMC failed due to handling of DHCP IPv6 pool object
CSCwr87834	Improve logging for correction actions that would lead to mark the network discovery policy dirty
CSCwr88208	ASA/FTD: Fragmentation issue for IKE_Auth packets
CSCwr88733	Collecting "show tech-support fprm" results in corefile in TAR process
CSCwr90859	MariaDB cores due to conflicting queries on VPN_TUNNEL_STATUS
CSCwr94517	ASA traceback and reload while removing capture
CSCwr95502	RADIUS External authentication doesn't work after migration between FMC platforms.
CSCwr96082	ASA: Traceback and reload on ARP code when the pinged device is unreachable

Bug ID	Headline
CSCwr96253	UI does not display dynamic objects when API request does not have ObjectType:IP field
CSCwr98814	'Convert and auto-import' option from the policy sync tab, is currently not correctly copying overridden rule actions to Snort3 rules.
CSCws02848	High cpu on block depletion
CSCws03165	Cannot replace FDM UI certificate due to "SSP Server Unavailable" error
CSCws03807	Memory leak in virtual-access nameif strings
CSCws03882	ASA timestamp getting stuck for syslog messages until the device sync up with NTP
CSCws05886	ASA may traceback during manual failover
CSCws06991	Few FQDNs are not resolving after FTD upgrade
CSCws06997	FTD upgrade failed at 999_z_must_remain_last_finalize_boot.sh
CSCws15230	FMC Audit Logs for configuration change entries show FMC IP instead of FMC Hostname in host field.
CSCws16081	Incorrect Numbering and Missing Policy Rules in ACP Reports on FMC GUI.
CSCws18263	FTD-side fix for Message asa_log_client exited 1 time(s) seen multiple times
CSCws19908	snmpEngineBoots does not increase when ASA reloads
CSCws21377	SFDataCorrelator process on the FMC was stuck during initialization
CSCws22782	FMC's API response contains "-1" for port values
CSCws25638	FPR 3110 MI (shared subinterface) - Traffic outage when disabling multicast routing on one FW instance
CSCws26939	reader command fails to process vpn event unified log files
CSCws27870	LINA May Encounter Traceback and Reload if SSH Session Uses ChaCha20-Poly1305 Cipher
CSCws28726	Platform settings missing in FMC REST API response for Firepower 3100/4200 multi-instance logical devices
CSCws31035	Lina Traceback and reload in Thread: "cli_xml_request_process"
CSCws31878	External auth login for FTD managed by a newer FMC version may fail for new changes done on the server
CSCws33395	FTD Upgrade failure: '999_z_must_remain_last_finalize_boot.sh' Script Fails Due to Missing/Inaccessible 'messages' File in 'var/log'
CSCws33462	Faults generated during first boot on 6.x can't be cleared

Bug ID	Headline
CSCws35109	FTD - AppId fails to extract DNS hostname causing DNS Security Intelligence policy bypass on Snort V3
CSCws35491	The identity cert will miss "ca" if the same cert also installed as device-certificate. Reboot will fail to install identity cert
CSCws36457	While in App-Sync phase, cluster node does not transition to disabled state when CCL interface goes down
CSCws36501	Few Licenses are not being replicated to Standby FMC on FMC HA
CSCws37370	FTD , dcosAG continuously crashing
CSCws39245	Actual username does not appear in SSL policy under child domain only
CSCws39799	Traceback and reload in threadname datapath due to flow-offload.
CSCws43016	Failed to convert snort2 rules to snort 3 in 7.4.3 FMC version
CSCws46901	M6 FMC Direct Install -Kernel crash and device struck during baseline
CSCws49176	Enable out of order packet discovery by default in appid
CSCws50593	Pkt injection failed when using transparent ethernet bridging
CSCws59816	ASA: Traceback with Thread Name DATAPATH-0-13302
CSCws60512	FMC API Explorer Does not log out user sessions
CSCws61024	Appliance enters into fail-safe mode due to warnings thrown by nat config.
CSCws62173	License registration still fails with ssl trustpoint and smart transport mode configured despite fix for CSCwp10957
CSCws64717	Deployment fails when interface has . or _ symbol
CSCws65199	ASA/FTD does not accept "id-kp-ipsecIKE" or "anyExtendedKeyUsage" in EKU for usage type IPSEC VPN Peer
CSCws65834	Lina: asacli Traceback & reload due to SSH/SCP initiated from firewall exec mode
CSCws66111	FMC backup downloads to 0 bytes
CSCws68981	Deployment Failure while removing Passive Interface in OSPF and Interface configuration at the same time
CSCws74680	Unable to delete Dynamic Access Policy
CSCws74734	FTD installing two default routes coming over EIGRP having different metrics
CSCws76541	unresponsive hmdaemon process on the FTD leading to Blank Device metrics on FMC Health Dashboard
CSCws82789	Unable to Edit or Delete Unused Intrusion Policies After Migration

Bug ID	Headline
CSCws82823	CLISH locks up for other commands and deploy is stalled when ping or traceroute is executed in CLISH and cannot be aborted
CSCws84267	Generating Snort3 recommendations fails due to Internal Error
CSCws84421	When the FMC language is set to Japanese, the Device Name changes to an IP address.
CSCws86306	Unable to retrieved SNMP OID crasActGrpName (1.3.6.1.4.1.9.9.392.1.3.22.1.1)
CSCws91179	Warning about the usage of failsafe-exit
CSCws91813	The EoRevisionStore table shows a pattern of size increase early in the week followed by pruning at week's end.
CSCws92318	FMC: Deployments fail when secondary FTD is active in HA due to SF tunnel reconnection race condition
CSCws93424	iOS/Android AnyConnect clients fail AAA/AD authentication with passwordless users
CSCws94641	Unable to make S2S VPN config changes with error "NAT Traversal cannot be disabled on this endpoint"
CSCws94688	DAP Records fetch group policies displayed by their UUID instead of names (policies beyond the first 25 listed alphabetically due to the limit of 25 set when grouppolicies called in DAP)
CSCws94960	FMC DAP policies missing in the UI on the DAP listing page (if there's a DAP policy with an all-numeric record name)
CSCws97908	Trustpoint deletion failure on FMC (if there's a certificate enrolled on the device which has an illegal character (according to JIBX) say 0x02 (^B))
CSCwt01395	Traffic is not hitting the expected rule, instead hitting default deny rule.
CSCwt03935	Allow new Radius user login when Radius user reached maximum limit
CSCwt05296	Unable to use newly created or system defined object IPv4-Private-All-RFC1918 as a filter in events
CSCwt12015	FMC Health Monitoring Generates Excessive Alerts for Undo Log Size Threshold Set Too Low
CSCwt12796	Upgrade of FTD-HA failed on primary FTD
CSCwt13923	sf-backup-inator.pl --> Failed to Call RNA Start For SFDC process
CSCwt14342	In a domain aware FMC environment, pre-deployment validation errors are seen due to sub-domain group policies referencing global Secure Client Profiles, complaining of invalid / non existing file entries
CSCwt18878	FTD sending duplicate syslog messages to the syslog server

Bug ID	Headline
CSCwt24048	FMC-created capture for FTD causes generation of excessive 'capture_*' files to FTD disk
CSCwt24971	FMC: Temporary SSL policy views does not get cleared after session ends
CSCwt25670	Improper URL Alias (group-url) length validation
CSCwt26591	Netflow CLI handling requirement
CSCwt27819	Error/slownesss while saving access control rules in AC policy
CSCwt30840	FTD: Snort3 meta-ack ACTION_BAD_PKT flag contaminates parent packet causing stream holes
CSCwt37654	use-after-free in call_handlers when flow_data list is mutated
CSCwt38633	Adjust timeout during restore command to unlimited for FP2100 platforms
CSCwt39737	PKI in ASA not able to parse "HTTP/1.1 426 Upgrade Required"
CSCwt50719	Clear the IPv4 rp_filter setting to allow FMC with dual management interfaces in same subnet
CSCwt51177	missing column mitigation can cause unintended table drops during upgrade
CSCwt61575	Deployment is failing as same IP config or tunnel is used for multiple spokes

Resolved Bugs in Version 7.4.6

Table last updated: 2026-03-04

Table 22: Resolved Security Bugs in Version 7.4.6

Bug ID	Headline
CSCwr96008	Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability

Resolved Bugs in Version 7.4.5

Table last updated: 2026-01-14

Table 23: Resolved Functional Bugs in Version 7.4.5

Bug ID	Headline
CSCws69719	Dynamic Objects cannot be deleted with FMC 7.4.4

Resolved Bugs in Version 7.4.4

Due to CSCws69719, Version 7.4.4 for the Firewall Management Center was deferred on 202-10-13 and is no longer available for download. If you downloaded it, do not use it. If you are running this version, upgrade. The bugs here are also fixed in Version 7.4.5.

Table last updated: 2026-03-04

Table 24: Resolved Security Bugs in Version 7.4.4

Bug ID	Headline
CSCwp22451	Cisco Secure Firepower Management Center Software SQL Injection Vulnerability
CSCwq01517	Cisco Secure Firepower Management Center Software SQL Injection Vulnerability
CSCwo73885	Cisco Secure Firewall ASA Software and Secure FTD Software Authenticated Command Injection Vulnerability
CSCwq73656	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF Memory Corruption Vulnerability
CSCwn69079	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF Memory Exhaustion Vulnerability
CSCwq56017	Cisco Secure Firewall Management Center and Secure Firewall Threat Defense Software Path Traversal Vulnerability
CSCwr96008	Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability
CSCwq23375	Cisco Secure Firewall Management Center Software Command Injection Vulnerability
CSCwo50716	Cisco Secure Firewall Management Center Software SQL Injection Vulnerability
CSCwq23377	Cisco Secure Firewall Threat Defense Software Snort 3 Visual Basic for Application Denial of Service Vulnerability
CSCwq23369	Cisco Secure Firewall Threat Defense Software Snort 3 Visual Basic for Application Denial of Service Vulnerability
CSCwq23373	Cisco Secure Firewall Threat Defense Software Snort 3 Visual Basic for Application Heap Overflow Denial of Service Vulnerability
CSCwq23372	Cisco Secure Firewall Threat Defense Software Snort 3 Visual Basic for Application Infinite Loop Denial of Service Vulnerability
CSCwq84949	Cisco Secure Firewall Threat Defense Software SSL Decryption Policy Denial of Service Vulnerability
CSCwq01519	Cisco Secure FTD Software Authenticated Command Injection Vulnerability
CSCwq97365	FMC: Realm sync after import, un assigns IPS policies configured in ACEs
CSCwq27947	high cpu and high disk util fault as ucssh process is in never ending loop

Bug ID	Headline
CSCwq86692	Invalid OSPF process popup blocking route-map configuration
CSCwq75339	Multiple Cisco Products Snort 3 DCERPC Vulnerabilities
CSCwq75359	Multiple Cisco Products Snort 3 DCERPC Vulnerabilities
CSCwq01530	Multiple Cisco Products Snort 3 TBD Denial of Service Vulnerability
CSCwq23374	Multiple Cisco Products Snort 3 TBD Denial of Service Vulnerability
CSCwq01529	Multiple Cisco Products Snort 3 TBD Denial of Service Vulnerability

Table last updated: 2026-03-04

Table 25: Resolved Functional Bugs in Version 7.4.4

Bug ID	Headline
CSCwd40371	9300 date setting shows Jan 1 2012 - causing 9300 FTD registration with FMC to fail
CSCwi98704	ActionQueueScra invoked oom-killer
CSCwm67644	FMC find usage feature not showing all associated access control policies for random objects
CSCwm80732	ASA/FTD - Traceback and reload Due to Race Condition in TCP Proxy
CSCwn23175	Configure Multi-Instance in Secure Firewall 3100 Series using patched versions of code
CSCwn57674	fix block loc oper set after free
CSCwn80400	Slow download speeds with AnyConnect over TLS on networks with high latency
CSCwn80643	Snort3 crash with a segmentation fault during end-of-flow processing
CSCwn93411	FXOS reset and reload due to snmpd service failure
CSCwo01616	sfipproxy prometheus configuration is attempted for not supported models and replaces sfipproxy.conf
CSCwo31418	AC policy with Network Group Override object causes deployment failure/rules missing
CSCwo38855	sftunnel and sfipproxy configuration files updates are not atomic
CSCwo46533	sfipproxy may not restart and fail services like User Identities when enable file is not detected
CSCwo56243	Snort3 Traceback due to watchdog during appid NAVL instantiation
CSCwo59534	Memory corruption leading to lina assertion and traceback
CSCwp22743	wpk - 1gsx link remains up on wpk but on switch side it shows as not connected

Bug ID	Headline
CSCwq13032	3100/4200: 1G Management interface flapping after upgrade
CSCwq21442	3RU MI instances offline after baseline/creation
CSCwq48842	FTD: Packets Dropped due to tcp-seq-past-win due to delayed packet through Snort
CSCwq66838	Multiple heartbeat response failures observed from service orchestration
CSCwq79940	tunnel protection ipsec policy feature not working on backup VTI tunnel
CSCwq81480	FTD MI: SNMP polling fails to work after the upgrade
CSCwq85986	FP4225: Interface with SFP - 10/25G_LR_S (or CSR_S) is not coming up after reboot of peer side.
CSCwq86675	Number of sessions in cache for Tomcat are set incorrectly
CSCwq92373	WA MI: Two apps went to Not Responding state with reason: Error in App Instance ftd. sma reported fault: Instance xxx is disabled due to restart loop. Please consider reinstalling this app-instance.
CSCwq96195	DNS-GUARD is not capable to be de-activated on FTD Devices
CSCwr05837	SNMP process continuously restarts
CSCwr06887	Database synchronization should auto-resume post network/checksum issues
CSCwr10747	ASA/FTD may traceback and reload due to memory exhaustion
CSCws03538	Policy Export/Import Issue, Users not getting imported to the access control rule.
CSCws19823	80, 1550 and 9472 block depletion seen on ASA/FTD 2100 when SMB multichannel traffic is sent
CSCws21415	Inotify user watch limits require adjustment for 3100 and 4200 platforms running MI FTDs

Resolved Bugs in Version 7.4.3

Table last updated: 2026-03-04

Table 26: Resolved Security Bugs in Version 7.4.3

Bug ID	Headline
CSCwi65260	Modification of destination entries failed, when Source Object Group and Destination Object Group contain same inner object-group
CSCwi74643	AWS ASAv: Support for IMDSv2
CSCwi81194	An issue was discovered in function _libssh2_packet_add in libssh2 1.10.
CSCwi81197	An exploitable use after free vulnerability exists in the window functio

Bug ID	Headline
CSCwi98274	unzip 5.52 is from 2005 is contains multiple vulnerabilities
CSCwj08021	The DNS message parsing code in 'named' includes a section whose compu
CSCwj08023	Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6
CSCwj08025	The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 whe
CSCwj08035	A flaw in query-handling code can cause 'named' to exit prematurely wi
CSCwj08037	A bad interaction between DNS64 and serve-stale may cause 'named' to c
CSCwj14624	Backup exits with memory allocation error on 4115
CSCwj20804	Cisco ASA and FTD Software VPN Web Server Limited Information Disclosure Vulnerability
CSCwj33129	VPN config isn't getting sync to leaf domain, when FTD moved to leaf domain
CSCwj33187	Internal cached access-group list maintenance issue with unexpected clear configure access-list
CSCwj33734	The Portable Network Graphics library (libpng) 1.0.15 and earlier allows
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
CSCwj68360	Cluster migration - cannot re-register deleted cluster node(AO mode) to on-prem FMC
CSCwj69533	Unable to change authentication methods on default tunnel group when using FDM
CSCwj79229	FMC - plain-text passwords for External Authentication Profile "Radius Server Key"
CSCwk05564	Only US region in FDM Cloud Services.
CSCwk08241	FTD is not resolving FQDN for ACLs intermittently
CSCwk21540	Unable to establish RAVPN session on FTD HA setup
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
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.

Bug ID	Headline
CSCwk71817	FMC: Blast-RADIUS CVE-2024-3596
CSCwk71992	BlastRADIUS vulnerability phase-1 fix for pix-asa - Message Authenticator
CSCwk72477	Custom rule with "metadata:impact_flag red" in Snort3 not detected as Impact Level 1
CSCwk74997	With CVE-ID cannot search the IPS events on the FMC
CSCwk75832	Snort3 reloads when AppID reload and snort restarts are happening simultaneously
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
CSCwm43301	In the Linux kernel fix a possible io_uring deadlock
CSCwm49410	Misconfigured Cross-Origin-Opener-Policy
CSCwm50895	Additional tab/space added in ACL logging messages in EMBLEM format causing ingestion issues
CSCwm77247	FTD Restore Failing because of no space left on the device
CSCwm83088	Cisco FXOS and UCS Manager Software Stored Cross-Site Scripting Vulnerability
CSCwm83089	Cisco FXOS and UCS Manager Software Stored Cross-Site Scripting Vulnerability
CSCwn13597	Customer FQDNs for VPN can be found on the internet unexpectedly
CSCwn49805	Multiple Cisco Products Snort 3 TBD Denial of Service Vulnerability
CSCwn58191	CVE-2024-26595: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58226	CVE-2024-46826: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58244	CVE-2024-47679: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58247	CVE-2024-47684: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58253	CVE-2024-47692: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58254	CVE-2024-47693: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58263	CVE-2024-47705: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58265	CVE-2024-47707: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58281	CVE-2024-47737: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58285	CVE-2024-47745: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58311	CVE-2024-49875: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwn58316	CVE-2024-49881: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58376	CVE-2024-49927: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58404	CVE-2024-49954: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58405	CVE-2024-49955: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58407	CVE-2024-49959: linux-kernel: In the Linux kernel, the following vuln...
CSCwn62947	CVE-2024-26958: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63003	CVE-2024-49983: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63018	CVE-2024-49995: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63027	CVE-2024-50002: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63035	CVE-2024-50010: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63050	CVE-2024-50036: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63051	CVE-2024-50038: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63065	CVE-2024-50058: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63075	CVE-2024-50082: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63076	CVE-2024-50083: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63084	CVE-2024-50095: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63104	CVE-2024-50131: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63114	CVE-2024-50142: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63126	CVE-2024-50151: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63157	CVE-2024-50191: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63162	CVE-2024-50194: linux-kernel: In the Linux kernel, the following vuln...
CSCwn63163	CVE-2024-50195: linux-kernel: In the Linux kernel, the following vuln...
CSCwn69075	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF Heap Corruption Vulnerability
CSCwn69076	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability
CSCwn69078	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability

Bug ID	Headline
CSCwn69081	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability
CSCwn72848	Lina interface fragment db queue size is incorrectly stuck at 4294967295 - ASA/FTD
CSCwn73801	Cisco Secure Firewall Threat Defense Software TLS with Snort 3 Detection Engine Denial of Service Vulnerability
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
CSCwn94836	CVE-2023-52679: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94876	CVE-2024-12084: rsync: A heap-based buffer overflow flaw was found in...
CSCwn94880	CVE-2024-12085: rsync: A flaw was found in rsync which could be trigg...
CSCwn94882	CVE-2024-12086: rsync: A flaw was found in rsync. It could allow a se...
CSCwn94883	CVE-2024-12087: rsync: A path traversal vulnerability exists in rsync...
CSCwn94884	CVE-2024-12088: rsync: A flaw was found in rsync. When using the '--s...
CSCwn94885	CVE-2024-12747: rsync: A flaw was found in rsync. This vulnerability ...
CSCwn94906	CVE-2024-26704: linux-kernel: In the Linux kernel, the following vuln...
CSCwn94998	CVE-2024-36899: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95001	CVE-2024-36940: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95037	CVE-2024-42285: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95045	CVE-2024-44934: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95051	CVE-2024-44987: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95071	CVE-2024-46743: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95083	CVE-2024-46800: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95090	CVE-2024-50047: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95128	CVE-2024-50262: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95173	CVE-2024-53057: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95183	CVE-2024-53068: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95198	CVE-2024-53096: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95200	CVE-2024-53099: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwn95231	CVE-2024-53142: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95244	CVE-2024-53173: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95284	CVE-2024-56601: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95291	CVE-2024-56606: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95294	CVE-2024-56614: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95295	CVE-2024-56615: linux-kernel: In the Linux kernel, the following vuln...
CSCwn95316	CVE-2024-56658: linux-kernel: In the Linux kernel, the following vuln...
CSCwo01785	Memory leak in RAVPN
CSCwo40957	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software IPsec Denial of Service Vulnerability
CSCwo48439	Traceback & Reload in Thread Name Unicorn Admin Handler
CSCwo49925	Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability
CSCwo49926	Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability
CSCwo49932	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Authentication Denial of Service Vulnerability
CSCwo49934	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Memory Exhaustion Denial of Service Vulnerability
CSCwo52298	Duplicate ACLs seen on FMC UI when Access Rules are created through API
CSCwo65318	Cisco Secure Firewall Management Center Software SQL Injection Vulnerabilities
CSCwo70286	Snort2|3 traceback in libdaq initialization phase after deployments
CSCwo71401	Multiple Cisco Products Snort 3 MIME Denial of Service Vulnerabilities
CSCwo71552	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability
CSCwo73886	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Unauthenticated Memory Exhaustion Denial of Service Vulnerability
CSCwo73888	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Lua Code Injection Vulnerability
CSCwo73889	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Lua Interpreter Denial of Service Vulnerability

Bug ID	Headline
CSCwo73891	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Authenticated Memory Exhaustion Denial of Service Vulnerability
CSCwo74009	Cisco FXOS and UCS Manager Software Command Injection Vulnerability
CSCwo74010	Cisco FXOS and UCS Manager Software Command Injection Vulnerability
CSCwo78475	Traffic hits incorrect ACP rules during policy deployment on FTD with dynamic objects
CSCwo88969	Traffic does not match expected ACL when destination contains object-group type network-service
CSCwo91250	Cisco Secure Firewall Management Center Software Radius Remote Code Execution Vulnerability
CSCwo95496	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Lua Code Injection Vulnerability
CSCwp05496	Cleaning of /var/temp backup files post Backup completion not cleaning
CSCwp05866	Cisco Secure Firewall Adaptive Security Appliance Software Multiple Context Mode SCP Unauthorized File Access Vulnerability
CSCwp19051	Updated HTTPD Docker image version
CSCwp29401	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software SAML Reflected Cross-Site Scripting Vulnerability
CSCwp34291	Cisco Secure Firewall Threat Defense Software Snort Deep Inspection Bypass Vulnerability
CSCwp68059	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Services Cross-Site Scripting Vulnerability
CSCwq01516	Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability
CSCwq01526	Cisco Secure FTD Software Authenticated DoS Vulnerability
CSCwq02055	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Services Client-Side Request Smuggling Vulnerability
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
CSCwq15864	Multiple Cisco Products Snort 3 MIME Denial of Service Vulnerabilities
CSCwq24081	Cisco Secure Firewall Adaptive Security Appliance Software SSH Partial Private Key Authentication Bypass Vulnerability

Bug ID	Headline
CSCwq32051	Cisco Adaptive Security Appliance and Firepower Threat Defense Software Command Injection Vulnerability
CSCwq50506	Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability
CSCwq78991	Firewall joins a cluster although gets incomplete ACL policy rules during replication
CSCwq79815	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Unauthorized Access Vulnerability
CSCwq79831	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Remote Code Execution Vulnerability

Table last updated: 2026-04-03

Table 27: Resolved Functional Bugs in Version 7.4.3

Bug ID	Headline
CSCuz96172	ASA PKI - Doesn't recognize the extension 1.3.6.1.4.1.311.21.10 in cert
CSCvi60913	FTD deployment failing due to "address-pool in use"
CSCvp68200	Misleading syslog on ASA regarding tunnel group match using certificate map
CSCvx66624	Write cache is disabled on some FMC M5 appliances
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
CSCwb02741	Time sync status and error message do not elaborate NTP server rejection case
CSCwb31730	syslog %ASA-6-605004 was not seen when Login denied from serial to console
CSCwb77894	Firepower 1000/2100 may boot to ROMMON mode
CSCwc28374	Search Feature of Large Access Control Policy Not Able to Find Searched-For Values
CSCwc57341	Inline pair has incorrect FTW bypass operation mode of 'Phy Bypass'
CSCwd08448	FMC to provide health alert 60 days prior to cacert.pem certificate expiry
CSCwd49767	System popover is empty for Network Admin and Security Approver users
CSCwd54466	New realm user are incorrectly getting mapped to discovered user
CSCwd80348	FMC does not support Umbrella with proxy setting
CSCwd83069	Add capability to disable auto-negotiation for 100G ports
CSCwd86472	Wrong extranet device name and type showing in S2SVPN listing page

Bug ID	Headline
CSCwe28608	Snort returns "Blocked by SSL" with no SSL policy.
CSCwe45584	FP2130 - Incorrect spelling seen in tech_support_brief in FPRM
CSCwe63686	Upgrade readiness failed in WM FDM @009_check_snort_preproc.sh but upgrade to 7.3.1-19 passed
CSCwe88492	Banner login does not display when configured
CSCwe89818	External Auth on FMC may throw err "Can't use string ("") as a HASH ref while "strict refs" in use"
CSCwe92324	FPR31xx - SNMP poll reports incorrect FanTray Status at Down while actually operational
CSCwf04460	The fxos directory disappears after cancelling show tech fprm detail command with Ctr+c is executed.
CSCwf25454	Stale anyconnect entries causing issues with routing
CSCwf61982	Edit search page and unified event viewer very slow to load due to high number of search-related EOs
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
CSCwf78497	EIGRP flexconfig migration 7.2.0, no CLIs should not be migrated if they are not the default config
CSCwh01312	ENH: FMC External Authentication doesn't work for SSH when configured with IPv6.
CSCwh08441	ENH: Add a command or a script to regenerate CA Certificate on FTD
CSCwh11508	FMC should not allow to create faulty snort3 rules with unknown characters
CSCwh17965	[Display]FXOS: PC member interface is shown as down & unassociated/unassigned after reload
CSCwh20736	cdFMC managed FTD show ntp cli output includes an error - uninitialized value
CSCwh21381	Logging improvement for messages exchange between LinaConfigTool and xml server
CSCwh29131	FMC Policy Analysis - Broken Redudancy Logic Check
CSCwh40635	Syslogs over management interface don't go through loggerd after FTD reboot or lina reload
CSCwh44215	ENH - Exempt TSID probe from going through EVE inspection
CSCwh46732	Remote Desktop (RDP) traffic fails with TSID enabled
CSCwh53745	ASA: unexpected logs for initiating inbound connection for DNS query response

Bug ID	Headline
CSCwh56290	After rebooting, the future date set on the FPR2100 platform is not reflected (set clock manually)
CSCwh69156	FTD-HA does not fail over sometimes when snort3 traceback
CSCwh70874	FTD: Policy Deployment failure due to abort as no progress
CSCwh71008	CSF 4200: PSU Fan speed is critical
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
CSCwh73139	Rule with same name exists when trying to edit ACP rules
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
CSCwh91976	WA MI: Traps(linkup/down) from chassis is not seen on NMS even if unification is enabled
CSCwh92156	Firewall shows misleading SCP file copy failure reasons
CSCwh99647	"Proxy thread creation successful" is presented as an Error in syslog messages, during bootup
CSCwi10623	Terminating all or single stale IP address which is in-use even when session is not there
CSCwi11246	Full reassembly fails for post-Snort IPv6 TLS proxy traffic
CSCwi13510	Config-url is accepting directory as the config file
CSCwi15787	Management access over VPN not working when NAT exempt is configured with any->any
CSCwi21894	"zmq_poll return 1" logs on the FTD console
CSCwi21909	FMC: Displaying "missing en-US:BGP" via Deployment Preview when BGP Changes have been Reverted
CSCwi22296	ASA: The logical device may boot into failsafe mode because of an large configuration.
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
CSCwi30683	Excessive new lines in OSPF debugs impairs readability of debugs in syslog messages
CSCwi44148	Incorrect health monitor alerts for ISE-PIC connectivity

Bug ID	Headline
CSCwi44265	low memory/stress causing block double free and reload
CSCwi44488	ASA/FTD: Traceback and reload reload in in process 'lina' due to ikev2_find_child_sa_by_local_spi
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
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
CSCwi52623	Misleading Certificate Attribute Checking Under DAP Endpoint Criteria
CSCwi53949	Snort3 traceback in TcpReassembler::scan_data_post_ack
CSCwi54926	In an FMC HA pair, "Health Monitor" may show incorrect roles when the Secondary unit is Active.
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
CSCwi59453	Bootstrap after upgrade failed - Resume HA with reason deployment already exists
CSCwi61903	Failed reason unknown and unable to proceed with FTD upgrade
CSCwi65870	6x25G netmod ports down with Version 2 QSFPs
CSCwi67998	Policy deployment failures on TPK MI chassis after redeploying same instance
CSCwi68604	Error logs generated for ssh access to ASA when eddsa is used as kex hostkey
CSCwi68970	Creating DAP policy with underscore "_" is not visible as applied to Remote Access VPN policy
CSCwi71076	Device listing taking long due to FTD_HA REST-API delay - Can be seen in loading HealthMon page.
CSCwi72109	aaa port 80 listener configuration not applied during startup in fips mode
CSCwi72158	Devices in HA pair shows as standalone in Threat Defense Upgrade page
CSCwi78064	CloudAgent Smart Agent Exception - The Smart Agent Manager requires NTP to be running on FDM
CSCwi81771	Unable to send unknown file disposition to ThreatGrid due to mem cache issue

Bug ID	Headline
CSCwi83185	FMC deployment failure due to incorrect error message type sent to FMC
CSCwi83821	Reword the CLI message shown after running the 'erase configuration' command
CSCwi83890	Report file generated for AC policy is empty
CSCwi85628	Deployment failure due to Rsync-chunk-checksum slowness
CSCwi89167	Automatic VDB/SRU Download Fails Due to Simultaneous Signature Validation
CSCwi90751	FTD/ASA - SNMP queries using snmpwalk are not displaying all "nameif" interfaces
CSCwi91384	Migration of S2S from ASA to FMC across domains
CSCwi93186	Low touch provisioning fails at initialProvision step
CSCwi94356	Lina traceback and reload in Thread Name: cli_xml_request_process
CSCwi97667	FMC HA sync status shows failed during VDB/SRU installation on Active and standby FMC
CSCwi97948	EIGRP bandwidth is changing after upgrade or after "shutdown"/"no shutdown" commands
CSCwj00027	Backup failure message doesn't help the user
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
CSCwj01418	Patch API response does not include port values when user modifies Source network
CSCwj01785	Network Risk Report on FMC lacks option to select data source, could cause report generation to fail
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
CSCwj07439	comm_alarm raised despite ARP response is successful on LAN and STATE interfaces
CSCwj08980	ICMP replies randomly does not reaching the sender node when initiated from the node.
CSCwj09587	Confusing error message (Timeout) when downloading pcap file when no 'File Download' permission
CSCwj09874	Tomcat and Apache maxHeader size should be increased to avoid 413 errors on some FMC pages

Bug ID	Headline
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
CSCwj12467	"show failover app-sync stats" to be included in "show failover statistics all"
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
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
CSCwj17447	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-6-26174'
CSCwj17969	rna_ip_os_map can grow very large that causes SFDataCorrelator to stop processing events
CSCwj23777	Missing Column(s) in eventdb table
CSCwj25629	Error when running 'show tech-support module detail' on FPR9K
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
CSCwj28445	Allow more than one search strings within applications section in Access control policy
CSCwj28468	Validation required incorrect CLI Access Users in External Auth
CSCwj29113	Instance DNS servers may be silently discarded due to lack of DNS server count validation
CSCwj29599	FDM bootstrap might be interrupted by extra reboot due to firmware upgrade
CSCwj30582	Geolocation updates page should throw an error in case support site in unreachable
CSCwj31382	Wrong IP address on FMC audit logs
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
CSCwj35701	Dns-guard prematurely closing conn due to timing condition

Bug ID	Headline
CSCwj35902	URL Filtering and Cisco-Intelligence-Feed Download Failure
CSCwj39184	FDM /ngfw/var/sf/fwcfg/zones.conf is empty for 7.3.1
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
CSCwj43069	IPv6 rule with manual address entry FMC with ::/0 is not working as expected.
CSCwj43902	FTDv - The interface connected to the AWS GW may have connection issues for DHCP or an idle state.
CSCwj44464	ACP rule may not get applied post-deployment/Deployment failure due to FXOS-FTD timezone mismatch
CSCwj45075	Critical Processes show twice after upgrade to 7.0.6.x
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
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.
CSCwj57435	Cleanup stale logrotate files
CSCwj58442	FTD HA status in ON Prem FMC is corrupted reporting Secondary as Primary
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
CSCwj62959	Deployment failure and rollback when changing parent of subinterface with failover MAC address
CSCwj63048	Internal error during deployment: {0} seen on FDM caused by Lina Timeout
CSCwj63975	Disable health module does not delete UMS messages for that health module.
CSCwj65587	Snmpwalk throws Error messages #"snmp/error: truncating integer value > 32 bits"

Bug ID	Headline
CSCwj65811	FMC gets flooded with"Unable to find SSL rule id for policy" if TLS server identity discovery is on
CSCwj67707	ECDSA certificates are not supported by FMC ISE integration
CSCwj68277	Certificate check in LDAP settings is too restrictive
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
CSCwj69145	FTD: "show asp inspect-dp snort" output shows high CPU
CSCwj69675	Error during policy validation while navigating through AC policy
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
CSCwj72721	Deployment failure and rollback when BGP communities added or removed in route-map match clause
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 > 7.6.0 000_start/000_00_run_cli_kick_start.sh.
CSCwj75123	"show failover config-sync stats" cli output to be included in "show failover statistics all"
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
CSCwj79094	No pxGrid IP-SGT updates on FMC when the pxGrid connection is lost following ISE reboot or restart
CSCwj79895	ENH Logs FP4110 (FXOS 2.10.1.179) Security module stopped responding after device reboot

Bug ID	Headline
CSCwj80384	"App sync TX/RX stats" and "HA NLP client current TX/RX stats" being reset during App Sync
CSCwj80790	cdFMC and onPrem FMC: Device management / listing is showing chassis url for FPR-1K running 7.4.1
CSCwj81115	SFDataCorrelator deadlock on reconfigure after RNAStop and monetdb output queue is full
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
CSCwj83533	FAN is working as expected but FAN LED is in off state.
CSCwj83634	Seeing message "reg_fover_nlp_sessions: failover ioctl C_FOREG failed"
CSCwj84168	SFDataCorrelator log spam, repeatedly purging expired services and client apps
CSCwj85232	FTD failed to join FTD-HA after upgrade revert
CSCwj87501	ASA/FTD may traceback and reload in Thread Name 'fover_FSM_thread'
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
CSCwj91420	Snort3 crashes while collecting flow-ip-profiling
CSCwj93300	FMC: Comments on rule change required not working in Classic Theme Legacy UI
CSCwj93860	CD App Sync error on FDM HA after LINA crash
CSCwj95322	disable stat check for file
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
CSCwj98573	Encountering an unknown error [9999] when attempting to modify the identity policy.
CSCwj98580	Classification mismatch between intrusion and correlation events
CSCwj99941	M6 hardware models are hardly storing only a week old health monitoring data

Bug ID	Headline
CSCwk00401	CdFMC: FTD Migration Failing on Registration Phase
CSCwk00604	ASA Fails to initiate AAA Authentication with IKEv2-EAP and Windows Native VPN Client
CSCwk02804	WebVPN connections stuck in CLOSEWAIT state
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
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.
CSCwk05800	ASA/FTD SNMP polling fails due to overlapping networks in snmp-server host-group
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
CSCwk06564	Add New Syslog for Routes for NP add/delete
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
CSCwk08064	ADI Session Processing Delays return after upgrade to 7.2.x
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
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

Bug ID	Headline
CSCwk12497	Traceback and reload on active unit due to HA break operation.
CSCwk12698	SNMP polling of admin context mgmt interface fails to show all interfaces across all contexts
CSCwk12803	ASA Firepower module option to push software upgrade missing in FMC release
CSCwk13812	ASA/FTD incorrectly forwards extended community attribute after upgrade.
CSCwk14300	TS filename still showing the old IP after FMC management IP is changed
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
CSCwk17536	ASA/FTD: Low Memory Leads to Reload due to process Unified2File_Read
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
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 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.
CSCwk27175	ASA/FTD: Substantial increase in the time taken to load configuration
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'
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
CSCwk33511	low memory/stress causing block double free and reload
CSCwk33516	MonetDB down due to a corrupt table (table missing columns)
CSCwk33577	Devices not listed to add a data node when creating a cluster because of OS version mismatch
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
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)
CSCwk37701	FTD lost connection with cdFMC after FTD backup Restoration
CSCwk37929	Upgrading a standalone 2110 from 6.6.7-223 to 7.2.8-25 causes "Interface Modified" alert on FMC
CSCwk38440	if conn_meta null, dont send packet to snort

Bug ID	Headline
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
CSCwk39974	Umbrella registration status is not synced to newly added data nodes
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)
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
CSCwk42676	Virtual ASA/FTD may traceback and reload in thread PTHREAD
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
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
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
CSCwk55087	ENH: FMC support for DHCP relay on VTI/physical interfaces in ECMP zone
CSCwk56388	GRE traffic getting dropped after failover
CSCwk59009	IPv6 SSL Anyconnect access blocked in HA pair
CSCwk59458	21xx: debug log process hangs preventing recovery from stuck writing operations
CSCwk61157	FTD LINA Traceback and Reload dhcp_daemon Thread

Bug ID	Headline
CSCwk62366	Exception raised while fetching telemetry data from the FMC
CSCwk63586	App instance stuck in STOP_FAILED with error message
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"
CSCwk63993	FMC deployment fails due to S2S VTI VPN does not have any Virtual Tunnel Interface assigned
CSCwk64418	NTP is not synchronising when using SHA-1 authentication
CSCwk70078	Failures and records are not seen in "show failover statistics" after simulating failures
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'
CSCwk73544	Incorrect initialization of the domain_uuid in the sensor table and empeers table in the standby FMC
CSCwk75956	ASA/FTD may traceback and reload in Thread Name SSH
CSCwk76142	ASA crashing in thread PIX Garbage Collector with inspect-rtsp enabled.
CSCwk76362	FTDv traceback in Thread name - PTHREAD
CSCwk76734	Policy deployment fails due to mismatch in 'ip local pool' command between fmc and lina config
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
CSCwk78393	Improve logging for LDAPS SSL errors
CSCwk80292	FMC : DAP configuration "laggy/hangs" when trying to configure via FMC.
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
CSCwk81381	Increase Logging Level for TAm Services
CSCwk82557	FTD upgrade to 7.4.2 via FDM is blocked

Bug ID	Headline
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
CSCwk86404	Login banner not seen at login prompt for a multi-instance FTD on 3100/4200
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	tmp_cisco is consuming high boot volume space and leaking of file descriptors on FMC
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
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'
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
CSCwk97058	FMC - Predeploy validation should error and block deployment if VPN Certificate is in failed state.
CSCwk98920	FMC Health Monitor shows misleading CPU core numbers for Firepower 2100
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/multicast traffic affected on shared interface in multi instance setup

Bug ID	Headline
CSCwm03227	FTD upgrade failure due to multiple DB folders in /ngfw/var/cisco/deploy/tmp_bundle/db/ path
CSCwm03772	CLI "ssl server-max-version" Can't be deployed Via Flex Config
CSCwm03898	Packet captures from FMC GUI doesn't warn the user about an adverse impact on FTD device performance
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.
CSCwm05196	When using time based object in ACP event doesn't show up in FMC
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
CSCwm05960	Generated Crypto checksum changes without configuration change
CSCwm06059	Configure manager command hangs without any output on a TPK in native mode (FTD)
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 impacting external radius authentication
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
CSCwm10676	FMC unable to search Objects when there is a DNS configured
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

Bug ID	Headline
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
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 >> 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
CSCwm31193	Events or stats are missing after EventHandler logs "Error loading input module"
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
CSCwm33552	FMC Does Not Accept Valid IP Range Format in Access List under system configuration settings
CSCwm33613	Default Group Policy is applied when receiving multiple Group Policies in SAML assertion attributes
CSCwm33619	FTD Vault process exits every 1 minute with: Process vaultApp exited normally
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
CSCwm35730	LINA may traceback in Thread Name: Datapath with NAT config
CSCwm36631	FTD Secondary Unit got stuck in Bulk sync state.

Bug ID	Headline
CSCwm37363	Portmanager and lacp sync is not programmatic
CSCwm37455	ASA/FTD will allow local IP pool with invalid netmask
CSCwm37690	NAT Rules Before deleted when policy is saved on FMC
CSCwm38513	Objects get duplicated when policy imported using 'Replace Existing' option
CSCwm38635	TACACS+ traffic is dropped by TLS Server Identity in XTLS module
CSCwm39604	Offbox FMC Application/IPS/URL events validation failed: created network objects not found
CSCwm40278	S2S VPN config removed unexpectedly after deployment
CSCwm41381	File Download fails intermittently with malware & file policy configured
CSCwm41404	FTD wizard on active HA FMC show an error message that refers the other manager as "analytics FMC"
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
CSCwm47235	FTD upgrade may fail in 901_reapply_sensor_policy.pl if policy_deployment.db is corrupt/unavailable
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
CSCwm48621	ENH: Provide option independently enable/disable HM for physical and sub interfaces
CSCwm49458	DNS settings removed in post-upgrade deployment
CSCwm49721	ASA Traceback and Reload due to MEMORY CORRUPTION WAS DETECTED
CSCwm49782	enhance sma 2nd cruz heartbeat logging
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
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"
CSCwm56864	show run access-list command returns warning
CSCwm57511	Issues with extdb Omniquery execution

Bug ID	Headline
CSCwm58260	Snort3 crash on TLS cert have same issuer and common name,but sign algo and public key are different
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.
CSCwm61417	EventHandler can block when multiple SSE consumers are enabled
CSCwm63024	DAP Cert Serial Number check field should be freeform instead of hex format on FMC
CSCwm63648	Set Weight option missing in UI when FTD sensor reverted and re-upgraded
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
CSCwm67414	Unable to edit/delete client module in the RAVPN group policy
CSCwm68003	Re-Enabling multichannel cli post upgrade if disabled prior to upgrade
CSCwm68211	ASA traceback and reload on thread snmp_inspect
CSCwm69907	FMC not sending/synchronizing the RADIUS config file to the FTDs
CSCwm70040	Unable to login to FMC via external LDAP User post FMC Migration.
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

Bug ID	Headline
CSCwm75352	Scheduled tasks do not run when interval is set to 24 hours but do when set to 1 days
CSCwm77046	HTTP Path Data Metrics not Visible in FMC
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
CSCwm79169	ASA/FTD may traceback and reload in DATAPATH-1-20757
CSCwm79807	SFDataCorrelator cores while calling DCEControlMessageReconfigure
CSCwm79920	External auth (Radius) User unable to login to FTD due to mismatched cases during initial login
CSCwm80082	Alert user that FDM is not Supported for FTDv in Openstack if they try to enable it
CSCwm80085	FMC does not clear old Intrusion Policy recommendations when they are regenerated
CSCwm80580	snort "exits normally" in loop every 1 min resulting in complete outage
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 (^)
CSCwm85228	ASA/FTD may traceback and reload in Thread Name "IKEv2 Daemon" while joining failover
CSCwm85497	Secondary FMC indicates the FTD is still upgrading, despite the upgrade being completed.
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
CSCwm87669	Discrepency in the unused object count between the FMC UI and API results
CSCwm89523	'no capture /all' failed to disable capture completely in the backend, causing high datapath CPU
CSCwm90905	GTP inspection drops packet with error ERROR-DROP:MsgType:32
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
CSCwm94610	Enhancement to remove zone check on dhcp relay server facing interfaces .

Bug ID	Headline
CSCwm94752	Identity Mapping Filter shows blank, even though there is a selected network object.
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.
CSCwn00475	Memory Blocks 80 and 9344 leak due to priority-queue
CSCwn01281	GTP inspection not allowing GTP data packets if session create response has cause type 18
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
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
CSCwn09870	FlexConfig objects Policy_Based_Routing and Policy_Based_Routing_Clear cause deployment failure
CSCwn10538	ADI on FTD does not stop after a crash
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
CSCwn13421	Scale cdFMC:Policy deploy fails when Audit log to Syslog is configured with invalid ipv6 syslog host
CSCwn13813	User id mismatch - add extra logs
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'
CSCwn17121	ASA/FTD may traceback and reload in Thread Name 'cli_xml_request_process'.
CSCwn19190	Memory fragmentation resulted in huge pages unavailable for lina

Bug ID	Headline
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'
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
CSCwn22610	fs-daemon hap reset with core generation
CSCwn23362	FTD: Snort AppID Misclassifies NetBIOS-ssn Traffic as Unknown
CSCwn23992	Push messages including UMS are broken when the FMC is reached on port 443
CSCwn24577	ASA booting process may freeze when including 'no pim' or 'no igmp' config
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
CSCwn31166	Snort3 crash in js norm with out-of-range exception during unescaping
CSCwn31653	FTD may traceback and reload in Thread Name "FPRLI_FPR4K-SM-32"
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
CSCwn35470	Serviceability : FQDN Packet based debug and capture trace support

Bug ID	Headline
CSCwn35740	FMC Upgrade slowness is seen at stage 300_os/070_setup_partition.sh while copying cache files
CSCwn36449	Graceful restart flag in FTD OPEN message set to 0 when power is lost
CSCwn36925	LSP deployment fails in MI environments following a patch or hotfix installation failure.
CSCwn37993	Longevity setup:TPK cluster node is displayed as empty cluster in device mgmt page
CSCwn38761	DNS FQDN obj doesn't go unresolved upon FQDN obj deleted on server/intf to reach sever is down in 7.7
CSCwn39081	SNMP walk results in ASCII value for IPSEC Peer instead of an IP address.
CSCwn39159	Undefined value in port object on access policy page with new UI
CSCwn39780	FTD Deployment Resilience: Skip non-critical / non-existing commands to avoid deployment failures.
CSCwn39826	HA should prevent honouring failover requests while copy/config-sync/rollback is in progress
CSCwn39896	SAML SSO Test Configuration and SSO login doesn't work even after a successful configuration
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
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
CSCwn44527	Intrusion policy having same name in different Domains causes IPS policy corruption
CSCwn45049	Coverity System SA warnings 2024-09-09, Coverity Defects 922530 922529 922528 922630 921809 921808
CSCwn45510	S2S VPN tunnel Child SA unsuccessful renegotiation
CSCwn46426	ASA 21xx: 'sh environment temperature' shows incorrect temperature values
CSCwn46685	SFDataCorrelator memory leak on HandleUserLoginInfoMsg
CSCwn46794	FMC UI becomes unresponsive when converting and downloading Snort 2 rules
CSCwn46855	LINA may observe random traceback with Netflow configured

Bug ID	Headline
CSCwn47308	Critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on FPR 1100/2100/3100
CSCwn49391	Frequent traceback after upgrading FTD HA
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
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
CSCwn57940	Deploy preview fails if device is moved from one domain to another domain
CSCwn59632	FTD registration to FMC gets hung when RabbitMQ is down.
CSCwn60726	Traceback and reload with Thread Name: vtemplate process
CSCwn61640	EventHandler cores during startup when sending events to syslog or SNMP for a huge number of rules
CSCwn62960	FMC memory leak after talos_reg.crt becomes active
CSCwn63839	Traceback in thread name Lina on configuring arp permit-nonconnected with BVI
CSCwn64425	Specific IP settings are not kept in FMC GUI for BGP route map object in BGP Clauses after saving.
CSCwn65415	ASA: floating-conn not closing UDP conns if conn was created without ARP entry for next hop
CSCwn70473	SFF_SFP_10G_25G_CSR_S from Finisar ports bouncing when use as HA link
CSCwn71596	Intf Link down (Init, mac-link-down) seen - EtherChannel Membership in Down/Down/Down state after unplug/replug of the cable
CSCwn73318	FMC Health Monitor (HM) graph shows incorrect number of Snort and System CPU cores
CSCwn73351	Asia/Bangkok timezone option not listed in ASA running on firepower1k
CSCwn75667	Banner motd does not display when configured
CSCwn75744	After upgrading FMC, deployment fails because of high SI Objects

Bug ID	Headline
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
CSCwn76546	Update beakerd and libnikita to handle excessive logging issue
CSCwn79553	Unreachable LDAP/AD referrals may cause delays or timeouts in external authentication on FTD
CSCwn80419	Need the SVC Rx/Tx queue as a configurable option
CSCwn80762	FMC does not remove community list override when this is modified.
CSCwn80765	ISA3000 with ASA Refuses SSH Access If CiscoSSH is Enabled
CSCwn81995	Traceback and Reload caused by Memory corruption with SNMP inspection enabled
CSCwn84340	Talos registration cert may fail to generate if smart licensing VA name contains certain characters
CSCwn84557	Lina traceback and reload due to "spin_lock_fair_mode_enqueue"
CSCwn85299	Very High threat confidence is displayed for the threat score 98
CSCwn85913	extdb query error when ordering by count(*)
CSCwn86002	core corruption still seen with switching to quick core feature
CSCwn87249	snort3 : FMC connection event logs do not show URL in DNS query using TCP
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
CSCwn92248	FTD FP2100 port-channel interfaces flap with LACP
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"
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.
CSCwn96928	URL getting allowed even with block rule in place.
CSCwn96929	ASA: Traceback and Reload Under Thread Name SSH

Bug ID	Headline
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
CSCwo00702	Community lists should not throw an error until the last item in the list is being deleted
CSCwo01557	ASA traceback and reload on DATAPATH thread due to memory corruption
CSCwo06959	Malware block not happening due to malware cloud lookup timeout
CSCwo08042	ASAv reloaded unexpectedly with traceback on Unicorn Proxy Thread
CSCwo08306	Command authorization fallback to Local only works for users with privilege 15.
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
CSCwo16016	Users from legacy radius server can login to Standby FMC domain when MA is enabled
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.
CSCwo19986	FTD TS is collecting duplicated data
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
CSCwo26286	Management1 Gateway Configuration Should Be Optional on FPR 4200 Series
CSCwo31467	TLS.- Outlook only supports TLS 1.2 and not 1.3- FMC uses TLS 1.3 by default
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

Bug ID	Headline
CSCwo34580	First cycle of FMC HA periodic sync may fail after resuming sync following FMC software upgrade
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
CSCwo44267	Firepower hits route limit due to ASP table resource exhaustion affecting traffic forwarding
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
CSCwo49425	Logging recipient-address not overriding the logging mail message severity levels
CSCwo49658	After upgrade from newer lower MR to Old Higher MR seeing health module compilation error
CSCwo49744	DNS and default gateway are removed on FTD managed through data interface
CSCwo50885	/mnt/disk0/log folder duplicated on troubleshooting package
CSCwo55662	FMC Rest API returns only the first 1000 network object entries
CSCwo57744	Overrides not working on chained/inherited custom IPS policies
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

Bug ID	Headline
CSCwo62543	Default Pass action for rules in Snort 3 local rule groups may cause blank error in IPS policies
CSCwo64788	FPR9K-SM-56 Cluster - FTD Stuck in an application install loop & error 'pooled address is unknown'
CSCwo65866	Network Outage when Primary FTD Instance is Disabled from FCM
CSCwo65891	Unable to validate change ticket:
CSCwo66872	snmp_logging_thread is utilizing high CPU in control plane
CSCwo67167	FMC health policy and Default Health Policy do not have correct moduleList
CSCwo67540	FPR9K-SM-56 Cluster Node APP_SYNC timeout twice before joining "6" member inter-chassis cluster
CSCwo71052	FPR1010 Ethernet1/1 trunk port is not passing Vlan traffic after a reload
CSCwo71835	The NAS-IP-Address attribute is missing from the Access-Request in FMC
CSCwo73467	Interface mac stuck issue seen with peer switch reloads or after upgrade
CSCwo74265	FTD Upgrade Retry failure (Unable to execute Retry after failure in FTD while upgrading to 7.7.10)
CSCwo75483	SNMP polling to chassis is unsuccessful with FTD Multi-instance in HA used as SNMP agent
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
CSCwo79114	Post reposition or move operation fails then if user saves, it would lead to loss of rules & may cause an outage
CSCwo80223	BFD packets are not dropped for single-hop BFD sessions received via alternate path
CSCwo83389	Difference in RSA key length at multiple spots in FXOS
CSCwo84467	L3 Clustering where BGP immediately comes up while DATA node is still in bulk sync
CSCwo84825	CSF4200 management1/2 interface shows up/up on lina despite physically disconnected
CSCwo86422	Unidirectional communication over ccl leading to split-cluster.
CSCwo86835	SMB remote FMC backups are failing due to relam sync
CSCwo87938	backout change preventing enabling clustering in FIPS mode
CSCwo94274	FP4100/9300 Fatal error: Incomplete chain observed before watchdogs with reset code 0x0040

Bug ID	Headline
CSCwo96941	The total disk keep on increasing on the disk status wizard on the Health Monitor page.
CSCwo98670	FTD MI: SNMP polling fails to work after upgrade
CSCwp00618	Devices show offline due to "Appliance unreachable" due to HMS deadlock inserting to DB
CSCwp03910	Subsequent DNS packets are dropped in a single flow if one domain hits the custom DNS SI block list
CSCwp07785	Error 500: Internal Server Error in FMC when generating report for global domain intrusion policy used in child domain ACP
CSCwp15886	Unable to change few IPS rule actions after upgrading from snort2 to snort3
CSCwp18885	FP9300/4100 may traceback & reload due to a "Kernel Panic"
CSCwp21630	FTD: Traffic Getting Dropped with Reason "Blacklist" following "Pruned memcap flows"
CSCwp24119	FDM stuck deployment task in Queued state
CSCwp25033	An ICMP not reachable storm might cause high CPU on a two units FTD cluster
CSCwp27718	FMC deployment hungs and fail due to "NGFW_UPGRADE is missing in map"
CSCwp28229	File download halts around the 2.1 GB
CSCwp34610	IKEv2-EAP Authentication Fails with Windows and MacOS Native VPN Clients
CSCwp36133	Clarify the working of Fallthrough to Interface PAT (Destination Interface) as it is not working as expected
CSCwp37128	The estreamer debug command is not producing the expected output
CSCwp38565	Clean-up of temporary tar file is not happening when copy to remote storage fails during backup.
CSCwp39148	If a user_ip_map.snapshot exists with an low timestamp value, snapshots are created frequently
CSCwp83345	Cluster: Multi-blade chassis not transmitting broadcast traffic outbound to specific vlan
CSCwp83566	SSL - Issues with DND a particular site after FTD upgrade on Chrome and Edge post upgrade
CSCwp84585	TCP RST Packets Fail to Match Configured Geolocation-Based Rules
CSCwp91460	High disk usage due to snort-unified.log
CSCwp92489	SFDataCorrelator_user_id_mismatch.log overconsumption of disk
CSCwp92495	Adding interface taking more than 30 sec with loading security zones

Bug ID	Headline
CSCwp97402	WA: Traceback and reload due to lock contention on the tmatch table during deployment with large snmp config
CSCwq01305	FMC dashboard dynamic analysis over time is shown as "No Data"
CSCwq09614	Snort may drop SCTP packets and block SCTP connections
CSCwq21442	3RU MI instances offline after baseline/creation
CSCwq21804	FTD: Injected/Trimmed packets dropped by LINA due to invalid-ip-length
CSCwq22206	VPN lost during a rekey with 'IKEv2 negotiation aborted due to ERROR: Platform errors'
CSCwq35960	OSPF: Lina Traceback and Reload on Both Units in High Availability Setup.
CSCwq46783	FMC Authentication Fails with freeradius, "Invalid NAS IP Address" Error Displays Unexpected IP
CSCwq50373	ASA/FTD in HA, snmptranslate process during the boot-up causing High CPU and IPC timeouts, causing split-brain.
CSCwq54643	NAS-IPv6-Address attribute is missing from the Access-Request in FMC
CSCwq64824	UIP control event causes identity to reload potentially blocking packet processing for more than 10 sec
CSCwq70511	Though disabled rules exist , are shown as 0 for Snort3 rule recommendations
CSCwq90162	WM RM 1150: A reboot of an FTD in a HA pair may cause split-brain sometimes, in unknown conditions
CSCwq92436	NAS-Identifier Attribute has always "sshd" value
CSCwr22256	Traceback seen while FQDN list expands more than 200 entries for a resolved ip

Resolved Bugs in Version 7.4.2.4

Table last updated: 2025-09-25

Table 28: Resolved Security Bugs in Version 7.4.2.4

Bug ID	Headline
CSCwq79815	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Unauthorized Access Vulnerability
CSCwq79831	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Remote Code Execution Vulnerability

Resolved Bugs in Version 7.4.2.3

Table last updated: 2025-06-17

Table 29: Resolved Functional Bugs in Version 7.4.2.3

Bug ID	Headline
CSCwn22565	Frequent route updates causes routes to get removed causing outages
CSCwm77673	Policy Deployment Hung at 5% or 8% Deployment - Collecting policies and objects

Resolved Bugs in Version 7.4.2.2

Table last updated: 2025-08-21

Table 30: Resolved Security Bugs in Version 7.4.2.2

Bug ID	Headline
CSCwf89838	OpenPrinting CUPS is a standards-based, open source printing system fo
CSCwh71228	A flaw was found in GLib. GVariant deserialization fails to validate t
CSCwh71231	A flaw was found in GLib. GVariant deserialization is vulnerable to a
CSCwh71232	A flaw was found in glib, where the gvariant deserialization code is v
CSCwh71233	A flaw was found in GLib. The GVariant deserialization code is vulnerable
CSCwh71234	A flaw was found in GLib. GVariant deserialization is vulnerable to an
CSCwh71262	A flaw was found in glibc. In an uncommon situation, the gaih_inet fun
CSCwh71514	Due to a failure in validating the length provided by an attacker-craf
CSCwh71515	An issue in the CPIO command of Busybox v1.33.2 allows attackers to ex
CSCwh71516	Due to failure in validating the length provided by an attacker-crafte
CSCwi00710	urllib3 is a user-friendly HTTP client library for Python. urllib3 pre
CSCwi00713	A memory leak flaw was found in Libtiff's tiffcrop utility. This issue
CSCwi00716	LibTIFF is vulnerable to an integer overflow. This flaw allows remote
CSCwi00717	A vulnerability was found in libtiff due to multiple potential integer
CSCwi05240	ASA - Traceback the standby device while HA sync ACL-DAP
CSCwi24022	An issue was discovered in the Linux kernel through 6.5.9. During a ra
CSCwi24116	Twisted is an event-based framework for internet applications. Prior t
CSCwi49557	cryptography is a package designed to expose cryptographic primitives

Bug ID	Headline
CSCwi57783	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Access Control Rules Bypass Vulnerability
CSCwi60427	This flaw allows a malicious HTTP server to set "super cookies" in cur
CSCwi68163	Postfix through 3.8.4 allows SMTP smuggling unless configured with smt
CSCwi78200	A vulnerability was found in GnuTLS. The response times to malformed c
CSCwi92930	linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a den
CSCwi92932	copy_params in drivers/md/dm-ioctl.c in the Linux kernel through 6.7.1
CSCwj06006	Cisco Secure Firewall Management Center Software XPATH Injection Vulnerability
CSCwj08030	libexpat through 2.5.0 allows a resource consumption denial of service event
CSCwj08031	libexpat through 2.5.0 allows recursive XML Entity Expansion if XML_DT
CSCwj08155	Vim before 9.0.2142 has a stack-based buffer overflow due to a set language map error
CSCwj43353	A DMA reentrancy issue leading to a use-after-free error was found in
CSCwj43355	A bug in QEMU could cause a guest I/O operation otherwise addressed to
CSCwj43376	In the Linux kernel, the following vulnerability has been resolved: b
CSCwj43379	libexpat through 2.6.1 allows an XML Entity Expansion attack when ther
CSCwj43466	A heap-buffer-overflow vulnerability was found in LibTIFF, in extractI
CSCwj89050	Faulty input validation in the core of Apache allows malicious or expl
CSCwj89051	In GNU tar before 1.35, mishandled extension attributes in a PAX archi
CSCwj89054	An attacker may cause an HTTP/2 endpoint to read arbitrary amounts of
CSCwj89218	In the Linux kernel, the following vulnerability has been resolved: b
CSCwj89224	In the Linux kernel, partitioning error existed CVE-2023-52458
CSCwj89315	HTTP Response splitting in multiple modules in Apache HTTP Server allo
CSCwj89324	In the Linux kernel, the following vulnerability has been resolved: i
CSCwj89332	In the Linux kernel, the following vulnerability has been resolved: K
CSCwj89335	In the Linux kernel, the following vulnerability has been resolved: e
CSCwj89337	In the Linux kernel, the following vulnerability has been resolved: s
CSCwj89402	In the Linux kernel, the following vulnerability has been resolved: n
CSCwj89404	In the Linux kernel, the following vulnerability has been resolved: b

Bug ID	Headline
CSCwj89406	In the Linux kernel, the following vulnerability has been resolved: b
CSCwj89411	In the Linux kernel, the following vulnerability has been resolved: a
CSCwj89412	In the Linux kernel, the following vulnerability has been resolved: m
CSCwj89417	In the Linux kernel, the following vulnerability has been resolved: d
CSCwj89429	In the Linux kernel, the following vulnerability has been resolved: R
CSCwj89432	HTTP/2 incoming headers exceeding the limit are temporarily buffered i
CSCwj89434	wall in util-linux through 2.40, often installed with setgid tty permi
CSCwj89435	A flaw was found in GnuTLS. The Minerva attack is a cryptographic vuln
CSCwj89439	A flaw has been discovered in GnuTLS where an application crash can be
CSCwj89445	The iconv() function in the GNU C Library versions 2.39 and older may
CSCwj89447	less through 653 allows OS command execution via a newline character i
CSCwk00129	In the Linux kernel, serial: omap: Don't skip resource freeing if pm_runtime_resume_and_get() failed
CSCwk05826	nscd: Stack-based buffer overflow in netgroup cache If the Name Servi
CSCwk05827	nscd: Null pointer crashes after notfound response If the Name Servic
CSCwk05828	nscd: netgroup cache may terminate daemon on memory allocation failure
CSCwk05830	nscd: netgroup cache assumes NSS callback uses in-buffer strings The
CSCwk22718	In the Linux kernel, the following vulnerability has been resolved: f
CSCwk22987	In the Linux kernel, the following vulnerability has been resolved: U
CSCwk22993	In the Linux kernel, the following vulnerability has been resolved: t
CSCwk25751	In the Linux kernel, the following vulnerability has been resolved: n
CSCwk25755	In the Linux kernel, the following vulnerability has been resolved: n
CSCwk25756	Requests is a HTTP library. Prior to 2.32.0, when making requests thro
CSCwk25762	In the Linux kernel, the following vulnerability has been resolved: i
CSCwk25764	In the Linux kernel, the following vulnerability has been resolved: H
CSCwk25765	In the Linux kernel, the following vulnerability has been resolved: i
CSCwk44165	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability
CSCwk44245	In the Linux kernel, the following vulnerability has been resolved: i

Bug ID	Headline
CSCwk44246	In the Linux kernel, the following vulnerability has been resolved: i
CSCwk44247	In the Linux kernel, the following vulnerability has been resolved: b
CSCwk44248	In the Linux kernel, the following vulnerability has been resolved: n
CSCwk50039	strongSwan versions 5.9.2 through 5.9.5 are affected by authorization
CSCwk50044	The various Is methods (IsPrivate, IsLoopback, etc) did not work as ex
CSCwk50055	url.c in GNU Wget through 1.24.5 mishandles semicolons in the userinfo
CSCwk57933	Vulnerabilities in linux-kernel CVE-2023-52439
CSCwk57949	Vulnerabilities in linux-kernel CVE-2023-52435
CSCwk57953	Vulnerabilities in linux-kernel CVE-2023-52463
CSCwk66255	urllib3 is a user-friendly HTTP client library for Python. When using
CSCwk75030	The IPv6 implementation in the Linux kernel before 6.3 has a net/ipv6/
CSCwk75032	In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can modify the
CSCwk75033	In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can cause inva
CSCwk75035	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vul
CSCwk75036	null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and
CSCwk75037	In the Linux kernel, the following vulnerability has been resolved: x
CSCwk85702	Cisco Secure Firewall Management Center Software HTML Injection Vulnerability
CSCwm03675	In the Linux kernel, the following vulnerability has been resolved: t
CSCwm03678	In the Linux kernel, the following vulnerability has been resolved: b
CSCwm08231	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Network Address Translation DNS Inspection Denial of Service Vulnerability
CSCwm08232	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Network Address Translation DNS Inspection Denial of Service Vulnerability
CSCwm08235	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software DHCP Denial of Service Vulnerability
CSCwm12745	In the Linux kernel, the following vulnerability has been resolved: a
CSCwm12751	In the Linux kernel, for ata: libata-core: Fix null pointer dereference on error
CSCwm12757	In the Linux kernel, for tcp_metrics: validate source addr length
CSCwm12775	In the Linux kernel, the following vulnerability has been resolved: c

Bug ID	Headline
CSCwm12910	Jinja is an extensible templating engine. Special placeholders in the
CSCwm12911	Jinja is an extensible templating engine. The 'xmlattr' filter in affe
CSCwm12913	Vim is an open source command line text editor. Vim < v9.1.0647 has do
CSCwm29875	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm29876	Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.5
CSCwm29880	In the Linux kernel, the following vulnerability has been resolved: i
CSCwm29882	In the Linux kernel, the following vulnerability has been resolved: i
CSCwm29886	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm29889	In the Linux kernel, the following vulnerability has been resolved: b
CSCwm30872	Insufficient Input Validation Vulnerability
CSCwm30886	Insufficient Input Validation Vulnerability
CSCwm41195	Attempting to edit chassis of multinstance FTD gets "Request Timed Out. Retry after sometime."
CSCwm42979	A null pointer dereference flaw was found in the hugetlbfs_fill_super
CSCwm43160	In the Linux kernel, the following vulnerability has been resolved: m
CSCwm43165	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm43183	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm43186	In the Linux kernel, the following vulnerability has been resolved: x
CSCwm43189	In the Linux kernel, the following vulnerability has been resolved: f
CSCwm43193	In the Linux kernel, nvme: avoid double free special payload on discard request retry
CSCwm43304	In the Linux kernel, the following vulnerability has been resolved: p
CSCwm43337	In the Linux kernel, the following vulnerability has been resolved: e
CSCwm43339	In the Linux kernel, the following vulnerability has been resolved: c
CSCwm44719	Cisco Secure Firewall Threat Defense Software Snort 3 Denial of Service Vulnerability
CSCwm57472	In the Linux kernel, for filelock: Remove locks reliably when fcntl/close race is detected
CSCwm57484	In the Linux kernel, within mm: avoid overflows in dirty throttling logic
CSCwm75514	A flaw was found in the python-cryptography package. This issue may al
CSCwm75518	In the Linux kernel, the following vulnerability has been resolved: f

Bug ID	Headline
CSCwm75527	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm75696	In the Linux kernel, for dma: fix call order in dmam_free_coherent dmam_free_coherent()
CSCwm75706	In the Linux kernel, the following vulnerability has been resolved: d
CSCwm75710	Fix a Linux kernel file access permissions access check error
CSCwm75717	In the Linux kernel, the following vulnerability has been resolved: m
CSCwm75719	Fix linux kernel divide by zero error when calling ioctl TIOCSSERIAL with bad baud rate
CSCwm87847	In the Linux kernel, the following vulnerability has been resolved: g
CSCwm87858	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm87876	In the Linux kernel, the following vulnerability has been resolved: s
CSCwm87889	In the Linux kernel, the following vulnerability has been resolved: x
CSCwm87897	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm87928	In the Linux kernel, the following vulnerability has been resolved: v
CSCwm87933	In the Linux kernel, the following vulnerability has been resolved: x
CSCwm87951	In the Linux kernel, the following vulnerability has been resolved: n
CSCwm88098	In the Linux kernel, the following vulnerability has been resolved: m
CSCwm88100	In the Linux kernel, the following vulnerability has been resolved: f
CSCwm88105	An issue was discovered in libexpat before 2.6.3. xmlparse.c does not
CSCwm88115	In the Linux kernel, the following vulnerability has been resolved: e
CSCwm88121	In the Linux kernel, the following vulnerability has been resolved: K
CSCwm88133	In the Linux kernel, the following vulnerability has been resolved: P
CSCwm91176	Cisco ASA/FTD Firepower 3100/4200 Series TLS 1.3 Cipher Denial of Service Vulnerability
CSCwm95070	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwm95187	Redis is an open source, in-memory database that persists on disk. Aut
CSCwm95189	Redis is an open source, in-memory database that persists on disk. An
CSCwm95191	In the Linux kernel, the following vulnerability has been resolved: s
CSCwm95206	In the Linux kernel, the following vulnerability has been resolved: a

Bug ID	Headline
CSCwm95208	In the Linux kernel, the following vulnerability has been resolved: r
CSCwm95213	In the Linux kernel, the following vulnerability has been resolved: e
CSCwm95242	There is a MEDIUM severity vulnerability affecting CPython. Regul
CSCwm95243	There is a LOW severity vulnerability affecting CPython, specifically
CSCwm99884	Cisco Secure Firewall Management Center and Secure Firewall Threat Defense Software Command Injection Vulnerability
CSCwn03652	CVE-2022-48975: linux-kernel: In the Linux kernel, the following vuln...
CSCwn03738	CVE-2024-47659: linux-kernel: In the Linux kernel, the following vuln...
CSCwn03740	CVE-2024-47660: linux-kernel: In the Linux kernel, the following vuln...
CSCwn18575	Cisco Secure Firewall Management Center Software Authorization Bypass Vulnerability
CSCwn18587	Cisco Secure Firewall Management Center Software Authorization Bypass Vulnerability
CSCwn21134	FMC is not pushing no-validation-usage to the trustpoint if user not choosing validation usage type
CSCwn21584	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Web Services Denial of Service Vulnerability
CSCwn31143	CVE-2024-38538: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58152	CVE-2023-52498: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58169	CVE-2023-52572: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58186	CVE-2023-52615: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58215	CVE-2024-46777: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58237	CVE-2024-47668: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58259	CVE-2024-47701: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58284	CVE-2024-47742: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58297	CVE-2024-49858: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58300	CVE-2024-49860: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58314	CVE-2024-49878: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58318	CVE-2024-49882: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58319	CVE-2024-49883: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58320	CVE-2024-49884: linux-kernel: In the Linux kernel, the following vuln...

Bug ID	Headline
CSCwn58323	CVE-2024-49889: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58397	CVE-2024-49948: linux-kernel: In the Linux kernel, the following vuln...
CSCwn58399	CVE-2024-49949: linux-kernel: In the Linux kernel, the following vuln...

Table last updated: 2025-08-21

Table 31: Resolved Functional Bugs in Version 7.4.2.2

Bug ID	Headline
CSCvj85665	ENH: Appliance hostname or ip address should be included in FX-OS syslogs
CSCwb44245	SNORT3: proxy traffic issue on port 80 when tls1.3 inspection enabled
CSCwd87566	ENH: Need the output of "show ssh-client" in FPRM show tech bundle
CSCwf27687	Snort3 TCP flow cache entry growth caused by embryonic connection mismanagement
CSCwh82305	Lina core at swapcontext on FTD during policy deployment
CSCwi56743	MSP Quota setting for instances is not correct
CSCwi84417	Traffic incorrectly matches an ALLOW rule with a time-range object after time has expired
CSCwj34204	Disk quota for the corefile should be revisited based on platform
CSCwj50024	Add support for new Cloud SSX regions for India and Australia
CSCwj56662	FMC HA Wizard shows error "Unable to retrieve high availability status." with other languages
CSCwj63921	Snort3 traceback and reload due to memory corruption in file module
CSCwj77877	Disable/Enable an MI instance results it in "State Failed"
CSCwj81743	FTD - Trace back and reload due to NAT involving fqdn objects
CSCwk27628	CDO: Chassis onboarding to CDO is failing with hostname
CSCwk30049	ASA/FTD May traceback & reload citing Thread Name 'lina' as the faulting thread.
CSCwk36860	IPv6 tunnel packets to DVTI Tunnel source on vrf loopback dropped (acl-drop)
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
CSCwk48628	FTD/FxOS - Upgrade/erase configuration result in App-instance 'Operational State: Starting'

Bug ID	Headline
CSCwk64709	FXOS upgrade failure due to insufficient free space in /mnt/pss (isan.log consumes most of space)
CSCwk75406	FMC in CC-mode audit over syslog not working
CSCwk82337	Policy export fails with error "Unable to process the policy information for Export"
CSCwk88225	Critical fault : [FSM:FAILED]: user configuration(FSM:sam:dme:AaaUserEpUpdateUserEp)
CSCwk97812	RAVPN Certificate Group Map get removed after it is modified on the FMC
CSCwm05520	Disable cluster syn cookie decoding when FTD cluster is deployed with inline-set
CSCwm05949	Continuous loading state and PolicyRPC call remains in pending
CSCwm11515	SNMP trap OID changed after upgrade
CSCwm14729	CSF 3100 series not rebooting after power outage, requiring manual power cycle
CSCwm34786	Platform settings policy hidden on UI
CSCwm35751	FPR3100: Interface may go to half duplex speed is hardcoded to 100mbps
CSCwm40531	FTD/ASA : 1SXF interfaces on FP3100 stay in a link-down state when connected to a Nexus 9K Switch
CSCwm40721	PDTS write from Daq can fail when PDTS buffer is full and it would eventually lead block depletion
CSCwm41847	Serviceability to capture PDTS writing/reading block to help root cause CSCwm36314
CSCwm44412	FTD inline-set ignore reverse flag for inject/rewrite
CSCwm47769	ID attribute of other device during copying config via REST API POST can remove original config
CSCwm49154	FXOS fault F1738 seen in deploymet with Error: CSP_OP_ERROR. CSP signature verification error
CSCwm49940	ha-mode graceful-restart is missing in advanced preview
CSCwm51747	SSH access with public key authentication fails after FXOS upgrade
CSCwm51874	FXOS: messages rotates every 40 minutes due to Notification Daemon messages' being spammed
CSCwm51923	Deployment transcript showing "Enable management access: false"
CSCwm52689	FTDv and FTD on 4100/9300 unlocking based on time is not configurable
CSCwm52973	TPK Low End FPR3100:Changing interface speed from 1g to 100mbps/100mps to 1g bring downs the link

Bug ID	Headline
CSCwm61282	ASA/FTD: RA VPN tunnel causing memory leak leading to traceback & Reload
CSCwm61345	FXOS: Directory /var/tmp Triggering FXOS Fault F0182 due to vdc.log (Excessive Logging,Log Rotation)
CSCwm87409	FMC is sending a wrong value for engineID in SNMPv3 traps
CSCwm95116	ADI crashes on FTD due to both FMC ADIs going unmuted
CSCwn06641	FTD syslog-over-TLS allowing too many curves in CC mode
CSCwn11728	FPR9K-SM-56 module intermittently lock up and cause traffic impact.
CSCwn13672	Bind ESP to VTI Tunnel Source Interface To Avoid Additional Route-Lookup Post Encryption
CSCwn15104	FTD reload with traceback on swapcontext function
CSCwn23031	Can't delete IPS policy when Workflow Mode is enabled
CSCwn29611	Radius user ssh login fails with error: username is not defined with a service type that is valid
CSCwn36449	Graceful restart flag in FTD OPEN message set to 0 when power is lost
CSCwn56950	FMC unnecessary sending "network-service reload" to FTD on every deployment regardless of change
CSCwn57518	FMC : OSPF setting screen cannot be opened in FMC English UI
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
CSCwn78846	Snort3 traceback and reload during user identity reload
CSCwn95451	Last synchronization time in the FMC HA page shows 'Data unavailable' in language other than English
CSCwo07006	Snort3 traceback and reload with stale pointer
CSCwo07139	Stale Snort3 stream inspector flow stash after flow data is cleared
CSCwo07469	External authentication radius SSH login failure with FXOS version 2.14.1.186

Resolved Bugs in Version 7.4.2.1

Table last updated: 2025-03-03

Table 32: Resolved Bugs in Version 7.4.2.1

Bug ID	Headline
CSCwb02741	Time sync status and error message do not elaborate NTP server rejection case
CSCwf34069	Cisco ASA and FTD Remote Access SSL VPN Authentication Targeted Denial of Service Vulnerability
CSCwi85823	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwj08015	FTW no longer working in NM3 on Warwick
CSCwj19125	Cisco ASA and FTD NSG Access Control List Bypass Vulnerability
CSCwj45822	Cisco ASA and FTD Software Remote Access VPN Brute Force Denial of Service Vulnerability
CSCwj49745	Cisco ASA and FTD VPN Web Client Services Cross-Site Scripting Vulnerabilities
CSCwj68540	Cisco Secure Firewall Management Center Software Command Injection Vulnerability
CSCwj77284	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwj82736	TLS Handshake Fails if Fragmented Client Hello Packet is Received Out of Order
CSCwj85106	FMC on upgrade results in FTDv losing its performance tier
CSCwj90826	Snort2 SSL decryption with known key fails on Chrome v124 and above.
CSCwk02332	Snort2 - SSL decryption failing and some websites not loading on Chrome v124+
CSCwk25117	ENH: Add application support for blocking consecutive AAA failures on LINA
CSCwk27628	CDO: Chassis onboarding to CDO is failing with hostname
CSCwk27741	Cisco Firepower Management Center SQL Injection Vulnerability
CSCwk37371	SGT INLINE-TAG added after upgrade to 7.4.x
CSCwk48488	Cisco FTD for Cisco Firepower 2100 Series TCP UDP Snort 2 and Snort 3 DoS Vulnerability
CSCwk53369	Cisco ASA and FTD Software Remote Access VPN Denial of Service Vulnerability
CSCwk62381	ASA might traceback and reload due to ssh/client hitting a null pointer while using SCP.
CSCwk64418	NTP is not synchronising when using SHA-1 authentication
CSCwk64709	FXOS upgrade failure due to insufficient free space in /mnt/pss (isan.log consumes most of space)

Bug ID	Headline
CSCwk67346	DAP policies not working with attribute TRUE/FALSE
CSCwk74813	Cisco Adaptive Security Appliance and Firepower Threat Defense TLS Denial of Service Vulnerability
CSCwk77241	Traffic outage due to 9k block depletion (tcpmod proc) observed on FPR 3100 (HA)
CSCwk82591	Unable to create MI FTD in TPK chassis
CSCwk90663	Configure External Storage fails second time with same backup profile
CSCwk96912	FTD: Username missing in syslog message ID 302013 after upgrade to 7.4.1
CSCwm05155	Snort AppID incorrectly identifies SSH traffic as Unknown
CSCwm14729	CSF 3100 series not rebooting after power outage, requiring manual power cycle
CSCwm34333	FTD - Â Multi-Instance, docker0 interface overlap with private network 172.17.0.0/16
CSCwm35251	FMC4700 displays premature fan speed alerts
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.
CSCwm49153	Cisco Adaptive Security Appliance Software SSH Server Resource DoS Vulnerability

Resolved Bugs in Version 7.4.2

Table last updated: 2024-07-31

Table 33: Resolved Bugs in Version 7.4.2

Bug ID	Headline
CSCvk60075	FMC HA synchronisation task failures should generate alarms
CSCvx37329	Remove Syslog Messages 852001 and 852002 in Firewall Threat Defense
CSCwb02701	FXOS does not retry NTP sync with servers
CSCwb03293	IKEv2 debugs: Received Policies and Expected Policies are empty
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwc31953	Prevention of RSA private key leaks regardless of root cause.
CSCwc33025	mgmt interface taking long time to come up and causing cluster registration issues
CSCwc70142	Deleting a routed mode Etherchannel interface changes member interfaces to switch port mode
CSCwc73773	FMC 7.0.2 Deployment error message is irrelevant | Deployment Failed due to configuration error

Bug ID	Headline
CSCwc76419	Unnecessary FAN error logs needs to be removed from thermal file
CSCwd39442	ssl policy errors: Unable to get server certificate's internal cached status
CSCwd67100	ASA traceback and reload on Datapath process
CSCwd80492	Device Management Applied Policies Widget Defaulting to classic theme when editting
CSCwe02012	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe11124	ENH: Combine firmware bundle packages into FXOS MIO update packages
CSCwe18462	ASA/FTD: Improve GTP Inspection Logging
CSCwe18467	ASA/FTD: GTP Inspection engine serviceability
CSCwe42986	Classic and Unified Events should handle cases when SMC is unreachable
CSCwe47485	FTD: CLISH slowness due to command execution locking LINA prompt
CSCwe79990	Cisco-Intelligence-Feed - Failed to download due to timeout
CSCwe86964	Consul and Consul Enterprise allowed an authenticated user with service:
CSCwe91008	Snort3 is crashing frequently on cd_pdts.so
CSCwe93925	Deployment fails to FTD when reusing/reassigning existing vlan id to diff interface
CSCwe96560	Cannot copy rules from one policy to another policy using the new AC policy UI
CSCwe97939	ASA/FTD Cluster: Change "cluster replication delay" with max value increase from 15 to 50 sec
CSCwf01954	FTD: ADI.conf - send_s2s_vpn_events is set to 0, even after applying s2s vpn health policy
CSCwf16001	HashiCorp Vault's implementation of Shamir's secret sharing used precomp
CSCwf17314	FMC deploy logs rotating faster because of /internal_rest_api/accesscontrol/rapplicationsavailable
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
CSCwf39108	Firewall rings may get stuck and cause packet loss when asp load-balance per-packet auto is used
CSCwf47646	show version system prints errors about PM_Control.sock
CSCwf59529	Identity Policy Active auth snort3 redirect hostname doesn't list all FQDN objects\u0009
CSCwf61280	Failing to dowload FTD image via SAML SSO login

Bug ID	Headline
CSCwf75694	ASA - The GTP inspection dropped the message 'Delete PDP Context Response' due to an invalid TEID=0
CSCwf84318	ASA/FTD traceback and reload on thread DATAPATH
CSCwf99303	Management UI presents self-signed cert rather than custom CA signed one after upgrade
CSCwh12120	Incorrect exit interface choose for VTI traffic next-hop
CSCwh16759	SNMP is not working on the primary active ASA unit in multi-context environment
CSCwh19613	ASA crashed with Saml scenarios
CSCwh22888	FXOS: Remove enforcement of blades going into degraded state after multiple DIMM correctable errors
CSCwh29276	ASA: Traceback and reload when switching from single to multiple mode
CSCwh30257	snort3 crashes observed due to memory corruption in file api
CSCwh30346	ASA/FTD: 1 Second failover delay for each NLP NAT rule
CSCwh34836	Getting an exception on the UI while editing and saving the intrusion policy
CSCwh41606	Extensive logging for a problematic deployment caused logs to rollover important logs
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
CSCwh46657	Save button disabled when updating ZTNA policy
CSCwh47053	ASA/FTD may traceback and reload in Thread Name 'dns_cache_timer'
CSCwh47732	Vulnerabilities in linux-kernel 5.10.79 CVE-2023-3111 and others
CSCwh51872	Message asa_log_client exited 1 time(s) seen multiple times
CSCwh57814	The html/template package does not apply the proper rules for handling o
CSCwh57976	Improve CPU utilization in ssl inspection for supported signature algorithm handling
CSCwh58190	FMC Deployment failure in csm_snapshot_error
CSCwh58467	ASA does not sent 'warmstart' snmp trap
CSCwh58490	FMC Deployment failed due to internal errors after upgrade
CSCwh60504	LINA would randomly generate a traceback and reload on FPR-1K
CSCwh60971	NAT pool is not working properly despite is not reaching the 32k object ID limit.
CSCwh61832	FDM: Allow turn on/off GSP mempool polling via Flexconfig

Bug ID	Headline
CSCwh62731	FTD Upgrade from 6.6.5 to 7.2.5 removing OGS causing rule expansion on boot
CSCwh65128	LINA show tech-support fails to generate as part of sf_troubleshoot.pl (Troubleshoot file)
CSCwh68068	Firepower WCCP router-id changes randomly when VRFs are configured
CSCwh69843	WM DT - ASA in transparent mode doesn't send equal IPv6 Router Advertisement packets to all nodes
CSCwh71235	A flaw was found in QEMU. The async nature of hot-unplug enables a rac
CSCwh71611	ENH: FMC - Ability to Filter Security Zone in Interface Drop Down Selection
CSCwh71665	ASA traceback under match_partial_keyword during CPU profiling
CSCwh72070	Reload takes forever when reload command is issued on the lina prompt when devices are on HA
CSCwh75829	FMC Primary disk degraded error
CSCwh75927	In SQLite 3.31.1, isAuxiliaryVtabOperator allows attackers to trigger a
CSCwh79546	No error message is given when deleting object referred in new object created in another ticket
CSCwh83021	ASA/FTD HA pair EIGRP routes getting flushed after failover
CSCwh83254	ASA/FTD: Traceback and reload on thread name CP Crypto Result Processing
CSCwh83854	Cannot configure Correlation rule because there are no values for GID that exceed 2000
CSCwh84376	In FPR4200/FPR3100-cluster observed core file ?core.lina? observed on device reboot.
CSCwh84610	Disconnecting RA VPN users from the FMC gui fails.
CSCwh84647	Backup restore: silent failure when the device managed locally
CSCwh87058	FTD: Internal certificate generation results to certificate and private key mismatch
CSCwh88150	Need ability to configure SSH public key auth without using root shell
CSCwh89835	FMC plain-text passwords for radius server and certificate passphrase
CSCwh91574	FTD: Traceback in threadname cli_xml_request_process
CSCwh92345	crypto_archive file generated after the software upgrade.
CSCwh92541	Random FTD snort3 traceback
CSCwh93710	Last Rule hit shows a hex value ahead of current time in ASA and ASDM
CSCwh94201	An issue was discovered in drivers/net/ethernet/intel/igb/igb_main.c i

Bug ID	Headline
CSCwh95003	Init process spikes to 100% CPU usage after a failed backup
CSCwh95010	Unexpected traceback on thread name Lina and device experienced reboot
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
CSCwh99331	syslog not generated "ASA-3-202010: NAT pool exhausted" while passing traffic from iLinux to oLinux
CSCwh99398	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-34-17852'
CSCwi01073	Event search with URL object ${example} is displaying no results
CSCwi01085	FTD VMWare tracebacks at PTHREAD-3587
CSCwi01381	ASA/FTD may traceback and reload in Thread Name 'lina'
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
CSCwi02134	FTD sends multiple replicated NetFlow records for the same flow event
CSCwi02599	SSX Eventing continues to go to old tenant upon FTD migration to CDO.
CSCwi02754	FTD 1120 standby sudden reboot
CSCwi02919	SNMP Unresponsive when snmp-server host specified
CSCwi03407	Traceback on FP2140 without any trigger point.
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
CSCwi06690	Certificate Encoding Issue when using AnyConnect cert Authentication/Authorisation
CSCwi06797	ASA/FTD traceback and reload on thread DATAPATH
CSCwi08374	FMC backup fails with "Registration Blocking" failure caused by DCCSM issues
CSCwi11520	FTD OSPFV3 IPV6 Routing: FTD is sending unsupported extended LSA request to neighbor routers
CSCwi12388	HTTP/2 Rapid Reset Attack Affecting Cisco Products: October 2023 - Golang

Bug ID	Headline
CSCwi12772	ASA cluster traceback Thread Name: DATAPATH-8-17824
CSCwi13062	Debug messages seen on console on executing show tech-support fprm detail
CSCwi13134	Hardware bypass not working as expected in FP3140
CSCwi13223	Source of the VTI interface is getting empty
CSCwi15409	ASA/FTD - may traceback and reload in Thread Name 'Unicorn Proxy Thread'
CSCwi15595	ASA traceback and reload during ACL configuration modification
CSCwi16034	FMC does not generate email health notifications for Database Integrity Check failures.
CSCwi17193	CP Session Handling for per site auth is inaccurate for Cluster break and join scenarios
CSCwi17496	Error Text is repeated twice for Interface config if pool range is less than Cluster Nodes plus 1
CSCwi18581	Firewall traceback and reload due to SSH thread
CSCwi18663	FMC-4600: Pre-Filter policy is showing as none
CSCwi19015	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-13-6022'
CSCwi19485	Fail open snort-down is off in inline pairs despite it being enabled and deployed from FMC
CSCwi19849	VPN load-balancing cluster encryption using Phase 2 deprecated ciphers
CSCwi20045	ASA/FTD may traceback and reload in Thread Name 'lina' due to a watchdog in 9.16.3.23 code
CSCwi20848	ASA/FTD high memory usage due to SNMP caused by RAVPN OID polling
CSCwi20955	FTD with may traceback in data-path during deployment when enabling TAP mode
CSCwi21625	FailSafe admin password is not properly sync'd with system context enable pw
CSCwi23545	HA CP clients statistics doesn't show actual Tx/Rx and Reliable Tx/Rx
CSCwi23964	Python 3.x through 3.10 has an open redirection vulnerability in lib/h
CSCwi24004	Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.Th
CSCwi24021	An issue was discovered in the Linux kernel before 6.5.9, exploitable
CSCwi24027	A use-after-free vulnerability was found in drivers/nvme/target/tcp.c`
CSCwi24032	A heap out-of-bounds write vulnerability in the Linux kernel's Linux K
CSCwi24368	Standby manager addition is failed on Primary FMC due to previous entries in table

Bug ID	Headline
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)
CSCwi25842	FMC Analysis Vulnerabilities error "Unable to process this query. Please try the query again."
CSCwi26064	ASA : Modifying a route-map in one context affects other contexts
CSCwi26895	ASA SNMP OID cpmCPUTotalPhysicalIndex returning zero values instead of CPU index values
CSCwi27338	Stale asp entry for TCP 443 remains on standby after changing default port
CSCwi28645	User assigned to a read only custom role is not able to view content of intrusion policy for snort2
CSCwi29538	EIGRP migration failed using 'FlexConfig Policiies' script failed generating database corruption
CSCwi29934	Cisco FXOS Software Link Layer Discovery Protocol Denial of Service Vulnerability
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
CSCwi31563	cdFMC: Table View of Rule Update Import Log UI is throwing error, unable to check SRU update log
CSCwi31766	PSU fan shows critical in show environment output while operating normally
CSCwi31966	FTD ADI debugs may show incorrect server_group and/or realm_id for SAML-authenticated sessions
CSCwi32063	ASA/FTD: SSL VPN Second Factor Fields Disappear
CSCwi32759	Username-from-certificate secondary attribute is not extracted if the first attribute is missing
CSCwi33710	ipv6 table flush exception when cli_firstboot installs bootstrap configuration multi instance

Bug ID	Headline
CSCwi34125	ASA: Snmpwalk shows "No Such Instance" for the OID ceSensorExtThresholdValue
CSCwi34323	After importing AC policy, Realm is not present in UI causing validation error for Azure AD users
CSCwi34719	Unable to SSH into FTD device using External authentication with Radius
CSCwi34730	tls website decryption breaks with ERR_HTTP2_PROTOCOL_ERROR
CSCwi35079	FTD Upgrade logs should contain the certificate name or files
CSCwi35267	TLS1.3: core decode points to tls_trk_try_switch_to_bypass_aux()
CSCwi36311	use kill tree function in SMA instead of SIGTERM
CSCwi36843	Detailed logging related to reason behind sub-interfce 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 traffic during the suboptimal lookup
CSCwi40302	Deployment fails on new AWS FTDv device with "no username admin"
CSCwi40487	FTD HA Failure after SNORT crash.
CSCwi40536	ASA/FTD: Traceback and reload when running show tech and under High Memory utilization condition
CSCwi40674	Umbrella Profile and others cleared incorrectly when editing group policy in the UI
CSCwi41666	MonetDB startup enhancement to clean up large files
CSCwi42295	Radius traffic not passing after ASA upgrade 9.18.2 and above version.
CSCwi42962	installing GeoDB country code package update to FMC does not automatically push updates to FTDs
CSCwi42992	ASA/FTD may traceback and reload in Thread Name IKEv2 Daemon

Bug ID	Headline
CSCwi43240	Deployment fails if Network Discovery policy reference is missing from FMC Database
CSCwi43492	ASA traceback and reload on Thread Name: DATAPATH
CSCwi43782	GTP inspection dropping packets with IE 152 due to header length being invalid for IE type 152
CSCwi44007	FMC Validation failure for large object range and success for object network in NAT64
CSCwi44208	low memory/stress causing traceback in SNMP
CSCwi45408	Monetdb having 14GB of unknown BAT data causing "High unmanaged disk usage on /Volume"
CSCwi45630	Snort3 traceback with fqdn traffics
CSCwi45878	ASA/FTD: DNS Load Balancing with SAML does not work with VPN Load Balancing
CSCwi46010	ASA/FTD: Cluster incorrectly generating syslog 202010 for invalid packets destined to PAT IP
CSCwi46023	FTD drops double tagged BPDUs.
CSCwi46163	Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.
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
CSCwi49076	Sftunnel DEBUG level not logged on FMC/FTD after running DEBUG script
CSCwi49128	Update logs - SSP object serialization during HA
CSCwi49360	A flaw was found in the 9p passthrough filesystem (9pfs) implementatio
CSCwi49506	Before Go 1.20, the RSA based TLS key exchanges used the math/big libr
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
CSCwi50343	Their standalone FTD running 7.2.2 on FPR-4112 experienced a traceback on the SNMP module
CSCwi51793	Error while trying to push SNMP configuration using API

Bug ID	Headline
CSCwi52008	Snort3 crash with race conditions
CSCwi52188	Filtering the Malware Events table by IP address removes events which should remain in the results.
CSCwi53150	Service object-group protocol type mismatch error seen while access-list referencing already
CSCwi53431	Unable to Synch more then 100 environment-data with data unit
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.
CSCwi54995	413 Request Entity Too Large error due to cookies added by FMC/Amplitude
CSCwi55629	ASA/FTD : Port-channels remain down on Firepower 1010 devices after upgrade
CSCwi55842	7.4 - If policy save in progress deploy might indicate failure for only few devices
CSCwi55938	The "show asp drop" command usage requires better updates for cluster-related drops
CSCwi56048	Interface fragment queue may get stuck at 2/3 of fragment database size
CSCwi56441	Readiness check failed on vFTD during upgrade from 741-172 to 760-1270
CSCwi56499	Cut-Through Proxy feature spikes CP CPU with a flood of un-authenticated traffic
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
CSCwi56815	HMS process crash - "interface conversion: interface {} is nil, not map[string]interface {}"
CSCwi58754	Blocking SMB traffic with reason "Blocked by the firewall preprocessor"
CSCwi59271	Suppress "End of script output before headers" syslog on FXOS
CSCwi59525	Multiple lina cores on 7.2.6 KP2110 managed by cdFMC
CSCwi59831	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi59871	High disk usage caused by large write-ahead log in eventdb
CSCwi60151	ZTNA: FMC doesn't accept IdP with local domain
CSCwi60248	A malicious HTTP sender can use chunk extensions to cause a receiver r
CSCwi60256	strongSwan before 5.9.12 has a buffer overflow and possible unauthenti
CSCwi60285	ASA/FTD may traceback and reload in Thread Name 'lina'

Bug ID	Headline
CSCwi60430	CVE-2023-51385 (Medium Sev) In ssh in OpenSSH before 9.6, OS command injection might occur if a us
CSCwi61135	Debugs failed to be enabled on SSH session
CSCwi62683	The SSH transport protocol with certain OpenSSH extensions, found in ... (CVE-2023-48795)
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
CSCwi63113	Null pointer dereference in SNMP that results in traceback and reload
CSCwi63743	ASA/FTD may traceback and reload in Thread Name "appAgent_monitor_nd_thread" & Rip: _lina_assert.
CSCwi64429	MonetDB memory usage grows slowly over time
CSCwi64829	traceback and reload around function HA
CSCwi64993	Correlation policy not work when condition of the rule is "Intrusion Policy" is XXX
CSCwi65116	DHCPv6:ASA traceback on Thread Name: DHCPv6 CLIENT.
CSCwi66103	Lina traceback on RAVPN connection after enabling webvpn debug
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'
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
CSCwi68083	Product Upgrades page: Download action creates a lot of "uninitialized value" error messages in log
CSCwi68132	A heap out-of-bounds write vulnerability in the Linux kernel's Perform
CSCwi68133	A use-after-free vulnerability in the Linux kernel's ipv4: igmp compon
CSCwi68135	A vulnerability was found in SQLite SQLite3 up to 3.43.0 and classifie

Bug ID	Headline
CSCwi68320	During FMC hardware migration failure encountered due to missing prometheus directories
CSCwi68625	Continuous snmpd restarts observed if SNMP host is configured before the IP is configured
CSCwi68833	ASA/FTD: Memory leak caused by Failover not freeing dnscrypt key cache due to unsyned umbrella flow
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
CSCwi70371	Intermittent Packet Losses When VTI Is Sourced From Loopback
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
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
CSCwi72294	FTD: Improve or optimize LSP package verification logic to run it faster
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
CSCwi76630	FP2100/FP1000: ASA Smart licenses lost after reload
CSCwi77415	ASDM connection lost issue is observed in ASAv device due to config issue
CSCwi78189	It was discovered that when exec'ing from a non-leader thread, armed P
CSCwi78206	A vulnerability was found in GnuTLS, where a cockpit (which uses gnuTL
CSCwi78210	An out-of-bounds memory write flaw was found in the Linux kernel\u2019s Tra
CSCwi78370	41xx/93xx : Update CiscoSSH (Chassis Manager FXOS) to address CVE-2023-48795

Bug ID	Headline
CSCwi78626	tds-cloud-events.json getting updated from both cdFMCs (ftd migration from 1 tenant to another)
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
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
CSCwi81193	singlevar in lparser.c in Lua from (including) 5.4.0 up to 5.4.4
CSCwi81195	An issue in the component luaG_runerror of Lua v5.4.4 and below leads to ...
CSCwi81503	HTTP/HTTPS detection for application needs to fail it's detection earlier
CSCwi82189	ACP page goes blank or error thrown if one of the ACP rules has user created app filter
CSCwi82866	MonetDB Monitor triggers for restarting MonetDB based on WAL size are not effective
CSCwi84314	ASA CLI hangs with 'show run' on multiple SSH
CSCwi84809	Incorrect Variable set in derived policy when derived policy is same as default.
CSCwi85277	Upgrade Failed with error "Upgrade failed because of undeployed changes present on the device"
CSCwi85689	TLS Server Identify: 'show asp table socket' output shows multiple TLS_TRK entries
CSCwi85951	A use-after-free flaw was found in the __ext4_remount in fs/ext4/super
CSCwi86036	External Radius authentication fails post upgrade if radius key includes special characters
CSCwi86198	SFData correlator keep terminating on FTDs configured for IDS
CSCwi87382	Traceback and reload on Primary unit while running debugs over the SSH session

Bug ID	Headline
CSCwi89447	Every realm sync indicates an access control policy change
CSCwi90040	Cisco ASA and FTD Software Command Injection Vulnerability
CSCwi90399	FTD/ASA system clock resets to year 2023
CSCwi90571	Access to website via Clientless SSL VPN Fails
CSCwi90998	ASA SNMP Polling Failure for environmental FXOS DME MIB (.1.3.6.1.4.1.9.9.826.2)
CSCwi91588	Heap-use-after-free in Discovery Filter on Snort shutdown
CSCwi91602	7.2 - Deployment doesn't timeout, runs for hours after LSP install
CSCwi92875	Check metadata cache size when generating retrospective events
CSCwi92914	A flaw was found in the networking subsystem of the Linux kernel withi
CSCwi92917	Linux Kernel nftables Use-After-Free Local Privilege Escalation Vulner
CSCwi92927	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tab
CSCwi95228	"crypto ikev2 limit queue sa_init" resets after reboot
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.
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
CSCwi98147	Tomcat restarts in the middle of the LTP flow due to certificate update
CSCwi98284	Cisco ASA and FTD Software Persistent Local Code Execution Vulnerability
CSCwi99429	Policy deployment failure rollback didnt reconfigure the FTD devices
CSCwj00659	FMC: Multiple Email address in Email Alert not working
CSCwj00956	Snort process spamming syslog-ng messages so our on KP platform syslog-ng is being killed
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."

Bug ID	Headline
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
CSCwj03348	vFMC25 OCI to vFMC300 OCI migration failed 'Migration from Y to a is not allowed.'
CSCwj03764	In Spoke dual ISP case if ISP2 is down, VTI tunnels related to ISP1 flapping.
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 '\'
CSCwj06197	"pmtool restartbyid <invalid id>" should give some indication of error
CSCwj07837	Deployment failure due to exceeding logging event list name size
CSCwj08073	libuv is a multi-platform support library with a focus on asynchronous
CSCwj08083	An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.1
CSCwj08203	FMC: fireamp generating too many logs
CSCwj08302	FTD: HostScan scanning results not processed in version 7.4.1
CSCwj08822	cdFMC Multiple health monitor widgets throwing Error while fetching data
CSCwj09110	Upload files through Clientless portal is not working as expected after the ASA upgrade
CSCwj09373	BBManager text based search - lucene
CSCwj09613	User not entitled for packet captures, is still able to open it from the Device Management
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)
CSCwj10009	In Snort 3 policy editor, selecting a Rule Action of \u201cRule Action\u201d causes UI to spin indefinitely
CSCwj10451	The secondary device reloaded while rebooting the primary device.
CSCwj10955	Cisco ASA and FTD Software Web Services Denial of Service Vulnerability
CSCwj12131	Bailout when lina_io_write fails persistent with EPIPE errno.

Bug ID	Headline
CSCwj12168	Never expiring machine user not logged out at various places
CSCwj12173	Policy cache cleanup thread should cleanup any cache that is left open for a logged out session
CSCwj13910	Crypto IPSEC SA Output Showing NO SA ERROR With IPSEC Offload Enabled
CSCwj14492	fpr1k/2k/3k/4200:Need ability to configure SSH public key auth without using root shell
CSCwj14614	FMC: Upgrade fails at "800_post/991_update_scheduled_tasks.pl"
CSCwj14832	SAML: Single sign-on AnyConnect token verification failure is seen after successful authentication
CSCwj15821	Page getting expaned while getting continuous task notifications
CSCwj16119	FP2110: When Leaving On-Box (FDM) Mode Platform API Fails
CSCwj16633	Issues with FMC Deployment preview (Advanced Preview)
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
CSCwj19236	In Object page able to delete and create system provided object
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
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
CSCwj22990	After upgrading the ASA, \u201cSlot 1: ATA Compact Flash memory\u201d shows a ditterent value
CSCwj23192	extra file check is not reporting with pmtool SecureLSP lsp-rel-xxx command
CSCwj24517	LSP Deployment fails in multi instance FP 41xx / 93xx
CSCwj24573	Rabbitmq queues on FMC vHost may not be cleaned up after element removal
CSCwj25066	CCM ID 68 - LTS21 - CISCO_LTS21_R2160 release branch

Bug ID	Headline
CSCwj25975	FTD/ASA : CSR generation with comma between \u201cCompany Name\u201d attribute does not work expected
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.
CSCwj28153	Lina contains outdated libexpat source code
CSCwj28437	Snort3: SQL traffic failure after upgrade due to large invalid sequence numbers and invalid ACKs
CSCwj29351	Health Policy Configuration - Unable to remove device from the policy
CSCwj30825	SFDataCorrelator memory leak after unregistering an active device
CSCwj30962	3140 3 MI instances upgrade failed
CSCwj30980	Addition of debugs & a show command to capture the ID usage in the CTS SXP flow.
CSCwj31816	TLS Secure Client sessions cannot be established on ASA 9.19 and 9.20
CSCwj32035	Clientless VPN users are unable to reach pages with HTTP Basic Authentication
CSCwj33487	ASA/FTD may traceback and reload while handling DTLS traffic
CSCwj33503	Snort3 event PCAPs contain only header data when decrypting HTTP/2
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
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
CSCwj36559	rsync is not happening to standby unit when perform oob changes in active unit.
CSCwj38871	ASA traceback with thread name SSH
CSCwj38928	High latency observed on FPR3120
CSCwj39107	SFDataCorrelator memory growth when pruning a huge number of old service identities
CSCwj39984	Unable to approve ticket due to monitored int in HA and getting Error to contact Cisco Support.

Bug ID	Headline
CSCwj40124	FMC 7.3 Deployment failed due to OOM in PBR Configuration
CSCwj40597	Backups fail on multi-instance 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
CSCwj42025	CCM ID LTS21-100 with RCPL21 update
CSCwj43345	SNMP poll for some OIDs may cause CPU hogs and high latency can be observed for ICMP packets
CSCwj44398	when set the route-map in route RIP on FTD, routes update is not working after FTD reload
CSCwj48308	Stale Health Alerts seen on the UMS after model migration
CSCwj48704	ASA traceback and reload when accessing file system from ASDM
CSCwj48754	SFDataCorrelator high memory usage when restart with large network map hosts
CSCwj48801	4200s have high UDP latency at low packet rates.
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
CSCwj50603	Large write-ahead log may leave monetdb in disabled state
CSCwj51115	FMC backup remote server copy to Solar Winds remote server failing after upgrading to 7.x versions.
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
CSCwj56639	FDM1010E 7.4.1 unable to register to SA, getting "Invalid entitlement tag"
CSCwj56668	False positive ISE bulk download alert error seen on FMC
CSCwj58431	FMC REST API not sending 'deploymentStatus' Attribute

Bug ID	Headline
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'
CSCwj62723	Error message spammed to console on Firepower 2100 devices while enabling SSH config
CSCwj62984	Snort3: MSSQL query traffic corrupted by stream_tcp overlap handling causing SQL HY000
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.
CSCwj66923	cdFMC : Support for new regions in Aus and India
CSCwj67600	Autodeployment failing on cdFMC v20240307 when onboarding a 1010 v7.2.5
CSCwj67787	New User activity page does not load because the VPN bytes in and out are long.
CSCwj68096	Console Access Stuck for ASAv hosted in CSP after Upgrade to 9.18.3.56
CSCwj68783	FTD/ASA-HA configs not in sync as the command sync process is sending configs with special chars
CSCwj69632	Default Hashing Algorithm is SHA1 for Firepower Chassis Manager Certificate on 4110
CSCwj71064	Snort dropping connections with reason blocked or blacklisted by the firewall preprocessor
CSCwj72683	ASA - Bookmarks on the WebVPN portal are unreachable after successful login.
CSCwj73053	ASA may traceback and reload in Thread Name 'DATAPATH-21-16432'
CSCwj73061	SNMP OID for CPUTotal1min omits snort cpu cores entries when polled
CSCwj77700	FTD LINA Traceback and Reload idfw_proc Thread
CSCwj79481	Deployment fails on FTD HA while doing LINA ONLY DEPLOYMENT
CSCwj79736	eStreamer memory leak when the FMC receives events from CDO-managed FTDs
CSCwj80324	Access rule getting pushed with "deny tcp any any" on snort
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'

Bug ID	Headline
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
CSCwj88925	net-snmp provides various tools relating to the Simple Network Managem
CSCwj88928	net-snmp provides various tools relating to the Simple Network Managem
CSCwj88929	net-snmp provides various tools relating to the Simple Network Managem
CSCwj88930	net-snmp provides various tools relating to the Simple Network Managem
CSCwj88931	net-snmp provides various tools relating to the Simple Network Managem
CSCwj88932	net-snmp provides various tools relating to the Simple Network Managem
CSCwj89126	HTTP Response splitting in multiple modules in Apache HTTP Server allows
CSCwj89264	FTD HA: Traceback and reload in netsnmp_oid_compare_ll
CSCwj92784	RAVPN: Failure to create SGT-IP mapping due to ID table exhaustion
CSCwj93921	ASA after upgrade to 9.18.4.24 not able to save config with error: "Configuration line too long"
CSCwj95590	Browser redirects to logon page when the user clicks the WebVPN bookmark
CSCwj98451	FMC got deregistered from Smart License after upgrade
CSCwk00628	Captive portal returns bad request for snort 2 for FMC 7.4.x , FTD version < 7.4
CSCwk02928	ASA/FTD may traceback and reload in Thread Name PTHREAD
CSCwk04492	ASA CLI hangs with 'show run' with multiple ssh sessions
CSCwk05851	"set ip next-hop" line deleted from config at reload if IP address is ma
CSCwk07934	Clock skew between FXOS and Lina causes SAML assertion processing failure
CSCwk08576	command to print the debug menu setting of service worker
CSCwk12065	LSP downloads are not using the Web proxy, when configured.
CSCwk12673	TCP Session Interrupted if Keep-Alive with 1 Byte is Received
CSCwk33634	TLS Client Hello packet is dropped by snort
CSCwk44366	cdFMC Fails to configure-geneve-encapsulation on interface
CSCwk62296	Address SSP OpenSSH regreSSHion vulnerability
CSCwk62297	Evaluation of ssp for OpenSSH regreSSHion vulnerability
CSCwk66252	It was discovered that a nft object or expression could reference a nf

Bug ID	Headline
CSCwk66253	An out-of-bounds access vulnerability involving netfilter was reported

Resolved Bugs in Version 7.4.1.1

Table last updated: 2024-04-24

Table 34: Resolved Bugs in Version 7.4.1.1

Bug ID	Headline
CSCwi23545	HA CP clients statistics doesn't show actual Tx/Rx and Reliable Tx/Rx
CSCwi56441	Readiness check failed on vFTD during upgrade from 741-172 to 760-1270
CSCwi58754	Blocking SMB traffic with reason "Blocked by the firewall preprocessor"
CSCwi70371	Intermittent Packet Losses When VTI Is Sourced From Loopback
CSCwi90040	Cisco ASA and FTD Software Command Injection Vulnerability
CSCwi98284	Cisco ASA and FTD Software Persistent Local Code Execution Vulnerability
CSCwj10955	Cisco ASA and FTD Software Web Services Denial of Service Vulnerability
CSCwj14832	SAML: Single sign-on AnyConnect token verification failure is seen after successful authentication

Resolved Bugs in Version 7.4.1

Table last updated: 2025-02-25

Table 35: Resolved Bugs in Version 7.4.1

Bug ID	Headline
CSCvc06888	FMC should monitor only named interfaces on FTD
CSCvn25053	FMC: critical processes can not boot up including vmsDBEngine
CSCvq48086	ASA concatenates syslog event to other syslog event while sending to the syslog server
CSCvt43334	Cores generated due to expected/graceful shutdown need to be cleaned up
CSCvu22491	FMC fails to connect to SSM with error "Failed to send the message to the server"
CSCvx44261	SNMPv3: Special characters used in FXOS SNMPv3 configuration causes authentication errors
CSCvy31169	deployment failing with - Unable to load container
CSCvy50598	BGP table not removing connected route when interface goes down
CSCvz03407	IPTables.conf file is disappearing resulting in backup and restore failure.

Bug ID	Headline
CSCvz22945	ERROR: Deleted IDB found in in-use queue - message misleading
CSCvz34289	In some cases transition to lightweight proxy doesn't work for Do Not Decrypt flows
CSCvz36903	ASA traceback and reload while allocating a new block for cluster keepalive packet
CSCvz71215	FMC is pushing SLA monitor commands in an incorrect order causing deployment failure.
CSCvz71596	"Number of interfaces on Active and Standby are not consistent" should trigger warning syslog
CSCwa36535	Standby unit failed to join failover due to large config size.
CSCwa53186	FTD with Inline TAP re-writes frame with wrong MAC Address leading to connectivity problems.
CSCwa59907	LINA observed traceback on thread name "snmp_client_callback_thread"
CSCwa70323	Unable to push extra domains >1024 Character, as part of Custom Attribute under Anyconnect VPN
CSCwa72528	user-name from certificate feature does not work with SER option
CSCwa72929	SNMPv3 polling may fail using privacy algorithms AES192/AES256
CSCwa74063	Disable NLP rules installation workaround after mgmt-access into NLP is enabled
CSCwa82791	ENH: Support for snapshots of RX queues on InternalData interfaces when "Blocks free curr" goes low
CSCwa82850	ASA Failover does not detect context mismatch before declaring joining node as "Standby ready"
CSCwa95060	"SFDataCorrelator:Parser [ERROR] Syntax error" on FTD device
CSCwa97917	ISA3000 in boot loop after powercycle
CSCwb00871	ENH: Reduce latency in log_handler_file to reduce watchdog under scale or stress
CSCwb04000	ASA/FTD: DF bit is being set on packets routed into VTI
CSCwb17963	Unable to identify dynamic rate liming mechanism & not following msg limit per/sec at syslog server.
CSCwb31551	When inbound packet contains SGT header, FPR2100 cannot distribute properly per 5 tuple
CSCwb47027	[TPK 3105] Management through data interface not working
CSCwb53172	FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated
CSCwb53328	ASA/FTD Traceback and reload caused by Smart Call Home process sch_dispatch_to_url

Bug ID	Headline
CSCwb55243	snort3 crashinfo sometimes fails to collect all frames
CSCwb66382	ASAv - 9344 Block not created automatically after enabling JumboFrames, breaks OSPF MD5
CSCwb73248	FW traceback in timer infra / netflow timer
CSCwb74571	PBR not working on ASA routed mode with zone-members
CSCwb79062	FMC GUI not displaying correct count of unused network objects
CSCwb79812	RIP is advertising all connected Anyconnect users and not matching route-map for redistribution
CSCwb83691	ASA/FTD traceback and reload due to the initiated capture from FMC
CSCwb87498	Lina traceback and reload during EIGRP route update processing.
CSCwb89963	ASA Traceback & reload in thread name: Datapath
CSCwb90532	ASA/FTD traceback and reload on NAT related function nat_policy_find_location
CSCwb92320	Network Object not visible after Flex migration and unable to save interface change in EIGRP->Setup
CSCwb92709	We can't monitor the interface via "snmpwalk" once interface is removed from context.
CSCwb93932	ASA/FTD failover pair traceback and reload due to connection replication race condition
CSCwb94190	ASA graceful shut down when applying ACL's with forward reference feature and FIPS enabled.
CSCwb94312	Unable to apply SSH settings to ASA version 9.16 or later
CSCwb95784	cache and dump last 20 rmu request response packets in case failures/delays while reading registers
CSCwb95850	Snort down due to missing lua files because of disabled application detectors (PM side)
CSCwb97251	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCwc02488	ASA/FTD may traceback and reload in Thread Name 'None'
CSCwc03069	Interface internal data0/0 is up/up from cli but up/down from SNMP polling
CSCwc03507	No-buffer drops on Internal Data interfaces despite little evidence of CPU hog
CSCwc04187	ASA/FTD on FP1000 may reload during very heavy AnyConnect SSL VPN tunnel establishment
CSCwc05375	AnyConnect SAML - Client Certificate Prompt incorrectly appears within External Browser

Bug ID	Headline
CSCwc07262	Standby ASA goes to booting loop during configuration replication after upgrade to 9.16(3).
CSCwc08646	User without password prompted to change password when logged in from SSH Client
CSCwc09414	ASA/FTD may traceback and reload in Thread Name 'ci/console'
CSCwc10145	FTDv Cluster unit not re-joining cluster with error msg "Failed to open NLP SSL listening socket"
CSCwc10241	Temporary HA split-brain following upgrade or device reboot
CSCwc10483	ASA/FTD - Traceback in Thread Name: appAgent_subscribe_nd_thread
CSCwc11511	FTD: SNMP failures after upgrade to 7.0.2
CSCwc11597	ASA tracebacks after SFR was upgraded to 6.7.0.3
CSCwc11663	ASA traceback and reload when modifying DNS inspection policy via CSM or CLI
CSCwc12322	Digitally signed ASDM image verification error on FPR3100 platforms
CSCwc13017	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
CSCwc13994	ASA - Restore not remove the new configuration for an interface setup after backup
CSCwc17614	FMC M6 4700 10/25G - IP reachability Failed
CSCwc18312	"show nat pool cluster" commands run within EEM scripts lead to traceback and reload
CSCwc18524	ASA/FTD Voltage information is missing in the command "show environment"
CSCwc23356	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-20-7695'
CSCwc23695	ASA/FTD can not parse UPN from SAN field of user's certificate
CSCwc24422	AC SSLVPN with Certificate Authentication and DAP failure if client's machine cert has empty subject
CSCwc24906	ASA/FTD traceback and reload on Thread id: 1637
CSCwc26648	ASA/FTD Traceback and Reload in Thread name Lina or Datatath
CSCwc27846	Traceback and Reload while HA sync after upgrading and reloading.
CSCwc28532	9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwc28684	MI hangs and not repsonding when FTD container instance is reloaded
CSCwc28806	ASA Traceback and Reload on process name Lina
CSCwc28854	Incorrect IF-MIB response when failover is configured on multiple contexts

Bug ID	Headline
CSCwc28928	ASA: SLA debugs not showing up on VTY sessions
CSCwc32246	NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used
CSCwc35583	Snort leaking file descriptors with each u2 file created
CSCwc36905	ASA traceback and reload due to "Heap memory corrupted at slib_malloc.c
CSCwc37256	SSL AnyConnect access blocked after upgrade
CSCwc40352	Lina Netflow sending permited events to Stealthwatch but they are block by snort afterwards
CSCwc40381	ASA : HTTPS traffic authentication issue with Cut-through Proxy enabled
CSCwc44289	FTD - Traceback and reload when performing IPv4 <> IPv6 NAT translations
CSCwc44419	ASA/FTD may traceback and reload in Thread Name: fover_health_monitoring_thread
CSCwc45108	ASA/FTD: GTP inspection causing 9344 sized blocks leak
CSCwc45397	ASA HA - Restore in primary not remove new interface configuration done after backup
CSCwc45575	ASA/FTD traceback and reload when ssh using username with nopassword keyword
CSCwc48375	Inbound IPSEC SA stuck inactive - many inbound SPIs for one outbound SPI in "show crypto ipsec sa"
CSCwc48999	SFDataCorrelator error: Table 'cfgdb.user_ioc_state' doesn't exist
CSCwc49095	ASA/FTD 2100 platform traceback and reload when fragments are coalesced and sent to PDTS
CSCwc50887	FTD - Traceback and reload on NAT IPv4<>IPv6 for UDP flow redirected over CCL link
CSCwc50891	MPLS tagging removed by FTD
CSCwc51326	FXOS-based Firepower platform showing 'no buffer' drops despite high values for RX ring watermarks
CSCwc52351	ASA/FTD Cluster Split Brain due to NAT with "any" and Global IP/range matching broadcast IP
CSCwc53280	ASA parser accepts incomplete network statement under OSPF process and is present in show run
CSCwc54217	syslog related to failover is not outputted in FPR2140
CSCwc54984	IKEv2 rekey - Responding Invalid SPI for the new SPI received right after Create_Child_SA response

Bug ID	Headline
CSCwc60037	ASA fails to rekey with IPSEC ERROR: Failed to allocate an outbound hardware context
CSCwc61912	ASA/FTD OSPFv3 does not generate messages Type 8 LSA for IPv6
CSCwc66757	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwc67031	vti hub with NAT-T enabled pinholes connections are looping and causing snort busy drops
CSCwc67886	ASA/FTD may traceback and reload in Thread Name 'lina_inotify_file_monitor_thread'
CSCwc70962	FTD/ASA "Write Standby" enables ECDSA ciphers causing AC SSLv3 handshake failure
CSCwc72155	ASA/FTD Traceback and reload on function "snp_cluster_trans_allocb"
CSCwc72284	TACACS Accounting includes an incorrect IPv6 address of the client
CSCwc73224	Call home configuration on standby device is lost after reload
CSCwc74103	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-11-32591'
CSCwc74858	FTD - Traceback in Thread Name: DATAPATH
CSCwc77680	FTD may traceback and reload in Thread Name 'DATAPATH-0-4948'
CSCwc77892	CGroups errors in ASA syslog after startup
CSCwc78781	ASA/FTD may traceback and reload during ACL changes linked to PBR config
CSCwc79366	During the deployment time, device got stuck processing the config request.
CSCwc80234	"inspect snmp" config difference between active and standby
CSCwc81184	ASA/FTD traceback and reload caused by SNMP process failure
CSCwc81945	Traffic on data unit gets dropped with "LU allocate xlate failed" on GCP cluster with interface NAT
CSCwc81960	Unable to configure 'match ip address' under route-map when using object-group in access list
CSCwc82188	FTD Traceback and reload when applying long commands from FMC UI or CLISH
CSCwc83346	ASA/FTD Traceback and reload in Threadname: IKE Daemon
CSCwc87387	Valid DNS requests are being dropped by Lina DNS inspection when Umbrella DNS is configured
CSCwc88897	ASA traceback and reload due to null pointer in Umbrella after modifying DNS inspection policy

Bug ID	Headline
CSCwc90091	ASA 9.12(4)47 with user-statistics, will affects the "policy-server xxxx global" visibility.
CSCwc91451	dvti hub core at ctm_sw_ipsec_cleanup_frags+394
CSCwc93166	Using write standby in a user context leaves secondary firewall license status in an invalid state
CSCwc94085	Unable to establish DTLSv1.2 with FIPS enabled after upgrade from 6.6.5.
CSCwc94501	ASA/FTD memory leak and tracebacks due to ctm_n5 resets
CSCwc94547	Lina Traceback and reload when issuing 'debug menu fxos_parser 4'
CSCwc95290	ESP rule missing in vpn-context may cause IPSec traffic drop
CSCwc96805	traceback and reload due to tcp intercept stat in thread unicorn
CSCwc99242	ISA3000 LACP channel member SFP port suspended after reload
CSCwd00386	ASA/FTD may traceback and reload when clearing the configration due to "snp_clear_acl_log_flow_all"
CSCwd00778	ifAdminStatus output is abnormal via snmp polling
CSCwd02864	logging/syslog is impacted by SNMP traps and logging history
CSCwd03793	FTD Traceback and reload
CSCwd03810	ASA Custom login page is not working through webvpn after an upgrade
CSCwd04135	Snort3 unexpectedly dropping packets after 4MB when using file inspection with detection mode NAP
CSCwd04436	User/group download may fail if a different realm is changed and saved
CSCwd04494	Unable to add on-board and netmod interfaces to the same port-channel on Firepower 3110
CSCwd05756	FTD traceback on Lina due to syslog component.
CSCwd06005	ASA/FTD Cluster Traceback and Reload during node leave
CSCwd06592	deployment fails for bad config with error unable load so rules
CSCwd07098	25G CU SFPs not working in Brentwood 8x25G netmod
CSCwd08098	cacert.pem on FMC expired and all the devices showing as disabled.
CSCwd10822	Failover trigger due to Inspection engine in other unit has failed due to disk failure
CSCwd11303	ASA might generate traceback in ikev2 process and reload
CSCwd11855	ASA/FTD may traceback and reload in Thread Name 'ikev2_fo_event'

Bug ID	Headline
CSCwd14972	ASA/FTD Traceback and Reload in Thread Name: pix_flash_config_thread
CSCwd16294	GTP inspection drops packets for optional IE Header Length being too short
CSCwd16689	ASA/FTD traceback due to block data corruption
CSCwd20627	ASA/FTD: NAT configuration deployment failure
CSCwd22349	ASA: Unable to connect AnyConnect Cert based Auth with "periodic-authentication certificate" enabled
CSCwd22907	ASA/FTD High CPU in SNMP Notify Thread
CSCwd23913	FTD in HA traceback multiple times after adding a BGP neighbour with prefix list.
CSCwd24106	ISE Connection Monitor shows inaccurate alert status
CSCwd25201	ASA/FTD SNMP traps enqueued when no SNMP trap server configured
CSCwd25256	ASA/FTD Transactional Commit may result in mismatched rules and traffic loss
CSCwd26867	Device should not move to Active state once Reboot is triggered
CSCwd28037	No nameif during traffic causes the device traceback, lina core is generated.
CSCwd31181	Lina traceback and reload - VPN parent channel (SAL) has an invalid underlying channel
CSCwd31806	ASAv show crashinfo printing in loop continuously
CSCwd31960	Management access over VPN not working when custom NAT is configured
CSCwd33811	Cluster registration is failing because DATA_NODE isn't joining the cluster
CSCwd33962	3130 HA assert: mh->mh_mem_pool > MEMPOOL_UNDEFINED && mh->mh_mem_pool < MEMPOOL_MAX_TYPE
CSCwd34079	FTD: Traceback & reload in process name lina
CSCwd38583	ASA/FTD: Command "no snmp-server enable oid mempool" enabled by default or enforced during upgrades
CSCwd38805	Syslog 106016 is not rate-limited by default
CSCwd40260	Serviceability Enhancement - Unable to parse payload are silently drop by ASA/FTD
CSCwd41083	ASA traceback and reload due to DNS inspection
CSCwd41553	PIM register packets are not sent to Rendezvous Point (RP) due to PIM tunnel interface down state
CSCwd43622	Blade remains online for more than 600 secs after deleting Native logical device on 92.14.0

Bug ID	Headline
CSCwd45451	FMC: Script to change hostname/IP on FTD's when FMC's Ip/hostname is changed
CSCwd47149	New AC Policy UI: ACP rule list takes a long time to load in case of large rule set
CSCwd47278	256 / 1550 Block leak with TLS1.3 session
CSCwd49402	Not able to ping Virtual IP of FTDv cluster
CSCwd54360	FP2100: FXOS side changes for HA is not resilient to unexpected lacp process termination issue
CSCwd60461	Deployment failure while configuring port-channels
CSCwd62666	Multiple messages in a single packet are not handled correctly
CSCwd65239	vFTD Platforms not tracking CPU/Memory metrics for Health Monitoring
CSCwd65781	Saving capture with special characters fails to download - Error Timed out
CSCwd66820	Cisco Firepower Management Center Object Group Access Control List Bypass Vulnerability
CSCwd66822	FDM FPR2k Netmork module interfaces are greyed out post 7.1.0 update
CSCwd68745	QEMU KVM console got stuck in "Booting the kernel" page
CSCwd72425	internal.cloudapp.net_snort3 core file is generated on DST setup
CSCwd73020	Fix Bootup Warning: Counter ID 'TLS13_DOWNSTREAM_CLIENT_CERTIFICATE_VERIFY' is too long
CSCwd79150	Device API healthStatus for cluster devices not aligned with health status on device listing
CSCwd85073	Snort3 stream core found init_tcp_packet_analysis
CSCwd89095	Stratix5950 and ISA3000 LACP channel member SFP port suspended after reload
CSCwd89811	Traffic fails in Azure ASAv Clustering after "timeout conn" seconds
CSCwd90894	ASA: After upgrade cannot connect via ssh to interface
CSCwd98070	Unable to register new devices to buildout FMC 2700 (FMC HA Active)
CSCwe01977	ASA/FTD may traceback and reload after a reload with DHCPv6 configured
CSCwe04043	FTD HA upgrade fails due to one unit starting upgrade before the other rejoins HA pair
CSCwe10670	Identity network filter not removed from FTD
CSCwe10872	Internal Error while editing PPPoE configurations
CSCwe11754	Nodes randomly fail to join cluster due to internal clustering error

Bug ID	Headline
CSCwe11902	FTD: HA crash and interfaces down on FPR4200
CSCwe12645	Secondary state flips between Ready & Failed when node is rebooted and mgmt interface is shutdown
CSCwe12705	multimode-tmatch_df_hijack_walk traceback observed during shut/unshut on FO connected switch interfa
CSCwe13781	IKEv2 Multi-DVTI Hub Support FTD/ASA
CSCwe14714	Search is slow and semantic based searches are not working in new ACP UI
CSCwe15477	Application management interface may be down causing management connectivity failures
CSCwe15924	FMC-HA Sync loss for more then hr due to MariaDB replication is not in good state and recovered
CSCwe19927	Configuring HTTP-proxy on active in a HA setup from UI does not replicate to standby in FDM
CSCwe20646	Defunct mojo process in device listing page
CSCwe21301	Azure FMC not accessible after upgrading from 7.3.0 to 7.4.0
CSCwe21884	Write wrapper around "kill" command to log who is calling it
CSCwe25025	8x10Gb netmod fails to come online
CSCwe25342	ASA/FTD - SNMP related memory leak behavior when snmp-server is not configured
CSCwe25412	Azure D5v2 FTDv unable to send traffic - underruns and deplete DPDK buffers observed
CSCwe28874	FTD registration failure due to empty channelStrings and missing HA_STATE file
CSCwe28912	FPR 4115- primary unit lost all HA config after ftd HA upgrade
CSCwe30359	Traffic drops with huge rule evaluation on snort
CSCwe30687	dvti memory leak on mp_counter_alloc
CSCwe32058	ASA/FTD may traceback and reload in Thread Name 'ci/console' when checking Geneve capture
CSCwe33282	FTD: The upgrade was unsuccessful because the httpd process was not running
CSCwe33819	Snort2 ENH: Use a common pattern matcher list for CN and SNI patterns in apps
CSCwe34269	DBCheck error is unclear when monetdb is in a 'crashed' state
CSCwe34664	The interface is deleted from interface group if the user change the name of it [API]
CSCwe34826	Intrusion user not able to change intrusion action and File Policy

Bug ID	Headline
CSCwe37941	v1_message* and abp* files & sxp bookmark are not cleaned in user_enforcement on device registration
CSCwe38228	Unable to create MI HA after changing resource profile
CSCwe38601	FMC search error: "Error Loading Data Search Service Please Try Again."
CSCwe38640	EventHandler warnings if syslog facility is CONSOLE
CSCwe41766	FTD may not reboot as expect post upgrade if bundled FXOS version is the same on old and new version
CSCwe42061	Deleting a BVI in FTD interfaces is causing packet drops in other BVIs
CSCwe42236	FMC: Domain creation fails with error "Index 'netmap_num' for table 'domain_control_info'"
CSCwe44571	FMC: GEOLOCATION size is causing upgrade failures
CSCwe45569	FTD upgrade from 7.0 to 7.2.x and traceback/reload due to management-access enabled
CSCwe48997	FDM: Cannot create multiple RA-VPN profiles with different SAML servers that have the same SAML IDP\u2028
CSCwe54999	Protocol Down with lower CPU instances on ESXi 8 for ASAv and FTDv
CSCwe55298	Umbrella DNS Policy Doesn't honor Multiple URLs entered into the Bypass Domain Field
CSCwe55308	Memory leak in the MessageService
CSCwe58635	Readiness Check Failed [ERROR] Fatal error: Enterprise Object integrity check failed with errors
CSCwe58700	ASA/FTD: Revision of cluster event message "Health check detected that control left cluster"
CSCwe59889	Create Identity Services Engine via API returns 404 Client Error: Not Found
CSCwe63686	Upgrade readiness failed in WM FDM @009_check_snort_preproc.sh but upgrade to 7.3.1-19 passed
CSCwe63759	Cluster hardening fixes
CSCwe65492	KP Generating invalid core files which cannot be decoded 7.2.4-64
CSCwe65516	show xlate does not display xlate entries for internal interfaces (nlp_int_tap) after enabling ssh.
CSCwe67180	FTD HA app-sync failure, due to corruption in cache files.
CSCwe68840	add syslog ids the range 805003 ? 852002 for rate limit under fmc

Bug ID	Headline
CSCwe69824	validation check on FMC GUI causing issue and throwing error when adding new NAT objects
CSCwe70378	Connections not replicated to Standby FTD
CSCwe71220	FTD Crash in Thead Name: CP Processing
CSCwe73933	SNMPv3 polling may fail using privacy algorithms AES192/AES256
CSCwe75267	Cannot Force Break FTD HA Pair
CSCwe78674	User Group Download fetches less data than available or fails with "Size limit exceeded" error
CSCwe80273	FMC device search page removes FTD from the groups and put them back to ungrouped
CSCwe81274	All the matching network object groups are not listed if the network objects are filtered by name
CSCwe82647	FMCv on KVM does not recognize the platform/model correctly
CSCwe82704	PortChannel sub-interfaces configured as data/data-sharing, in multi-instance HA go into "waiting"
CSCwe83255	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe84079	asa_snmp.log is not rotated, resulting in large file size
CSCwe84695	FMC/FTD Dynamic VPN. Possibility to choose default preshared key from the dropdown list.
CSCwe85156	FTD: 10Gbps/full interfaces changed to 1Gbps/Auto after upgrade and going to down state
CSCwe85439	Change color codes to represent processes in 'Waiting' state
CSCwe87134	ASA/FTD: Traceback and reload due to high rate of SCTP traffic
CSCwe87831	FMC UI response is very slow: Add health module monitoring FMC ntpd server(s) accessibility
CSCwe88802	FTD readiness and upgrade passed with exception log as ProgressReport' has no attribute 'KB_UNIT'
CSCwe90168	Unable to Access FMC GUI when using Certificate Authentication
CSCwe92723	Phase 2 NAP delay seen in 7.0.1 while deploying policy
CSCwe93137	KP - multimode: ASA traceback observed during HA node break and rejoin.
CSCwe93885	FDM Deployment failure after VDB and SRU upgrade
CSCwe95110	Connection events incorrectly show OVERSUBSCRIPTION flow message for passive interface traffic

Bug ID	Headline
CSCwe95462	Health monitoring cores due to health alerts with more than 8 fields
CSCwe95729	Cisco ASA & FTD SAML Authentication Bypass Vulnerability
CSCwe96062	Platform Settings allowed Syslog to add TCP protocol with 514 port
CSCwe97277	Observed ASA traceback and reload when performing hitless upgrade while VPN traffic running
CSCwe98146	Snort3 cores seen in certain conditions with traffic
CSCwe98319	ASAConfig multiple restarts are leaking 16K memory in every Restart leading to ZMQ Out Of Memory.
CSCwe98435	Selective policy deploy with Identity Policy (captive-portal) and SSL Policy (dp-tcp-proxy) CLI
CSCwe98559	snort3 - missing necessary counters for RNA statistics
CSCwf00514	RRD files cannot be updated if the timestamp is ahead of time as a result of a system clock drift
CSCwf00804	EventHandler occasional corrupt bundle record - SFDataCorrelator logs "Error deserializing"
CSCwf01318	sfhassd process is not running after Revert from 7.4.0-1755 to 7.3.0-69
CSCwf03490	portmanager.sh outputing continuous bash warnings to log files
CSCwf04983	3100 unit failed to join the cluster with error "configured object (sys/switch-A/slot-2) not found"
CSCwf05295	FTD running on FP1000 series might drop packets on TLS flows after the "Client Hello" message.
CSCwf06272	Cluster upgrade docs need more info on mixed-version clusters due to upgrade failure/reimage
CSCwf06377	Setting heartbeat timeout to 6sec for Firepower 4100 and 9300
CSCwf06818	Cisco Firepower Threat Defense Software Encrypted Archive File Policy Bypass Vulnerability
CSCwf08790	FMC Restore of remote backup fails due to no space left on the device
CSCwf10494	If the user navigate to Packet Tracer from Device Mgmt page, the selected device is incorrect
CSCwf11877	TPK 3110 - Firmware version MISMATCH after upgrade to 7.2.4-144
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)

Bug ID	Headline
CSCwf14411	getting wrong destination zone on traffic causing traffic to match wrong AC rule
CSCwf15863	Very specific "vpn-idle-timeout" values cause continuous SSL session disconnects and reconnects
CSCwf16559	getReadinessStatusTaskList pjb request is very frequent when user in Upgrade sensor list page
CSCwf16679	HA Serviceability Enh: Maintain HA NLP client stats and HA CTL NLP counters for current App-sync
CSCwf17042	ASDM replaces custom policy-map with default map on class inspect options at backup restore.
CSCwf17858	node is leaving TPK cluster due to interface health check failure
CSCwf18144	Firepower hotfixes should not be allowed to install when already installed previously
CSCwf19621	Unable to edit name or inspection mode of intrusion policy
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
CSCwf22045	MYSQL, or any TCP high traffic, getting blocked by snort3, with snort-block as Drop-reason
CSCwf22637	Network Object Group overrides not visible or be edited from FMC GUI
CSCwf23868	Update Configuration State if sync is skipped
CSCwf24818	Unable to change admin user password after FMC migration if it had LOM access
CSCwf25402	FMC - Import SSL Certificate Pinning from a CSV file may result in a failure to deploy policy on FTD
CSCwf25563	Device list takes longer to load while creating new AC policy
CSCwf25642	High Disk Utilization and Performance issue due to large MariaDB Undo Logs
CSCwf26350	User is not informed of the dependent IPS when policy import fails.
CSCwf27337	KP: Cleanup/Reformat the second (MSP) disk on FTD reinstall
CSCwf30542	Snort3 crash found during cleaning up a CHP object
CSCwf31050	High CPU usage on multiple appliances incorrectly seen on FMC
CSCwf35233	Cisco Adaptive Security Appliance Software and Firepower Threat Defense DoS
CSCwf35573	Traffic may be impacted if TLS Server Identity probe timeout is too long
CSCwf36563	The interface configuration is missing after the FTD upgrade

Bug ID	Headline
CSCwf36621	access-list: Cannot mix different types of access lists.
CSCwf38782	Change in syslog message ASA-3-202010
CSCwf39163	ASAv - High latency is experienced on Azure environment for ICMP ping packets while running snmpwalk
CSCwf39821	FTD: High-Availability unit struck at CD App Sync error due to error ngfwManager restart on peer
CSCwf41187	WINSCP and SFTP detectors do not work as expected
CSCwf41433	ASA/FTD client IP missing from TACACS+ request in SSH authentication
CSCwf42012	Improper load-balancing for traffic on ERSPAN interfaces on FPR 3100/4200
CSCwf42097	PSEQ (Power-Sequencer) firmware may not be upgraded with bundled FXOS upgrade
CSCwf42233	deployment failure with Error-logging FMC MANAGER_VPN_EVENT_LIST
CSCwf42234	S2S dashboard SVTI tunnel details are missing after upgrade
CSCwf43537	Lina crash in thread name: cli_xml_request_process during FTD cluster upgrade
CSCwf43850	ECMP + NAT for ipsec sessions support request for Firepower.
CSCwf44537	99.20.1.16 lina crash on nat_remove_policy_from_np
CSCwf44621	Traceback and reload on Thread DATAPATH-6-21369 and linked to generation of syslog message ID 202010
CSCwf45091	Snort3 matches SMTP_RESPONSE_OVERFLOW (IPS rule 124:3) when SMTPS hosts exchange certificates
CSCwf45094	MariaDB Process in FMC should use jemalloc instead of glibc
CSCwf47227	Remove Priority-queue command from FTD|| Priority-queue command causes silent egress packet drops
CSCwf49486	store_*list_history.pl task is created every 5min without getting closed causing FMC slowness.
CSCwf50497	DNS cache entry exhaustion leads to traceback
CSCwf51512	2100 Reload due to internal links going down and NPU disconnection
CSCwf52810	ASA SNMP polling not working and showing "Unable to honour this request now" on show commands
CSCwf54510	ASA traceback and reload on Thread Name: DHCPRA Monitor
CSCwf55236	Unable to delete custom rule group even when excluded from all the ips policies
CSCwf56386	vFTD runs out of memory and goes to failed state

Bug ID	Headline
CSCwf56811	ASA Traceback & reload on process name lina due to memory header validation
CSCwf59643	FTD: HA App sync failure due to fover interface flap on standby unit
CSCwf60590	"show route all summary" executed on transparent mode FTD is causing CLISH to become Sluggish.
CSCwf62729	7.0.6 - Lina Crash in RAVPN interface with anomaly traffic in both non-FIPS and FIPS mode
CSCwf62820	Failover: standby unit traceback and reload during modifying access-lists
CSCwf63256	Firepower reloads unexpectedly with a traceback
CSCwf63358	FTD Diskmanager.log is corrupt causing hm_du module to alert false high disk usage
CSCwf63872	FTD taking longer than expected to form OSPF adjacencies after a failover switchover
CSCwf64590	Units get kicked out of the cluster randomly due to HB miss | ASA 9.16.3.220
CSCwf66387	[IMS_7_4_0] FTD revert fails "The management state validation cannot be done, Cannot revert"
CSCwf68335	vFMC: Scheduled deployment failing
CSCwf69313	Correlation events for Connection Tracker <, <=, = or != rules show data for unrelated connections
CSCwf69576	Snort Crash with SMB inspection traffic
CSCwf69880	Firewall Traceback and reload due to SNMP thread
CSCwf69901	FTD: Traceback and reload during OSPF redistribution process execution
CSCwf71602	FMC not generating FTD S2S VPN alerts when down or idle
CSCwf72434	Add meaningful logs when the maximums system limit rules are hit
CSCwf73773	Dumping of last 20 rmu request response packets failed
CSCwf74319	Health alert for significant difference of record numbers received with bulk download
CSCwf75214	ASA removes the IKEv2 Remote PSK if the Key String ends with a backslash "\" after reload
CSCwf75695	Duplicate FTD cluster has been created when multiple cluster events comes at same time
CSCwf76945	Packet data is still dropped after upgrade
CSCwf77994	False critical high CPU alerts for FTD device system cores running instantaneous high usage
CSCwf78321	ASA: Checkheaps traceback and reload due to Clientless WebVPN

Bug ID	Headline
CSCwf79279	azure vftd node traceback while loading multiple network-service objects during ns_reload.
CSCwf79372	after HA break, selected list shows both the devices when 1 device selected for upgrade
CSCwf80163	Critical Alert Smart Agent is not registered with Smart Licensing Cloud
CSCwf80183	Snort3 core in navl seen during traffic flow
CSCwf82279	Excessive logging of ssp-multi-instance-mode messages to /opt/cisco/platform/logs/messages
CSCwf82447	Editing identity nat rule disables "perform route lookup" silently
CSCwf82742	FTD: SNMP not working on management interface
CSCwf82970	Snort2 engine is crashing after enabling TLS Server Identity Discovery feature
CSCwf84200	Snort core while running IP Flow Statistics
CSCwf86519	FMC displays VPN status as unknown even if the status is up if one of the peer is extranet
CSCwf86557	Decrypting engine/ssl connections hang with PKI Interface Error seen
CSCwf87070	WM RM - SFP port status of 9 follows port of state of SFP 10|11|12
CSCwf87348	When state-link is flapped HA state changed from Standby-ready to Bulk-sync without failover reason
CSCwf88030	FMC pushes the "shutdown" command on the management interface for the logical device
CSCwf88124	FPR 1010 - Switch ports in trunk mode may not pass vlan traffic after power loss or reboot
CSCwf89959	ASA: ISA3000 does not respond to entPhySensorValue OID SNMP polls
CSCwf91282	import of .SFO to FMC failed due to included local/custom rules having a blank rule message field
CSCwf92135	ASA: Traceback and reload on Tread name "fover_FSM_thread" and ha_ntfy_prog_process_timer
CSCwf92182	Cisco Firepower Management Center Software SQL Injection Vulnerability
CSCwf92371	HA secondary unit disabled after reboot - Process Manager failed to secure LSP
CSCwf92439	Deployment blocked due to port object with IP range max limit 131838 in NAT64
CSCwf92646	ECDSA Self-signed certificate using SHA384 for EC521
CSCwf92661	ASA|FTD: Traceback & reload due to a free buffer corruption

Bug ID	Headline
CSCwf92726	Some Vault secrets including LDAP missing files after upgrade if the Vault token is corrupted
CSCwf94194	FMC: Should not be able to add the same interface to the same ECMP zone
CSCwf94450	FTD Lina traceback Thread Name: DATAPATH due to memory corruption
CSCwf94677	"failover standby config-lock" config is lost after both HA units are reloaded simultaneously
CSCwf95147	OSPFv3 Traffic is Centralized in Transparent Mode
CSCwf96938	FMC: ACP Rule with UDP port 6081 is getting removed after subsequent deployment
CSCwh01673	FTD /ngfw disk space full from Snort3 url db files
CSCwh02457	Radius authentication stopped working after ASAv on AWS upgrade to any higher version than 9.18.2
CSCwh02561	Port-channel interface speed changes from 10G to 1G after a policy deployment
CSCwh04185	Snort crash in active response
CSCwh04365	ASA Traceback & reload on process name lina due to memory header validation - webvpn side fix
CSCwh04395	ASDM application randomly exits/terminates with an alert message on multi-context setup
CSCwh04730	ASA/FTD HA checkheaps crash where memory buffers are corrupted
CSCwh05863	ASA omits port in host field of HTTP header of OCSP request if non-default port begins with 80
CSCwh06452	Interface speed mismatch in SNMP response using OID .1.3.6.1.2.1.2.2
CSCwh08481	ASA traceback on Lina process with FREEB and VPN functions
CSCwh08683	FTDv/AWS - NTP clock offset between Lina and FTD cluster
CSCwh09968	ASA/FTD: Traceback and reload due to NAT change and DVTI in use
CSCwh10087	core-compressor fails due to core filename with white space
CSCwh10931	ASA/FTD traceback and reload when invoking "show webvpn saml idp" CLI command
CSCwh11411	Snort blacklisting traffic during deployment
CSCwh11764	ASA/FTD may traceback and reload in Thread Name "RAND_DRBG_bytes" and CTM function on n5 platforms
CSCwh13625	Encrypted Visibility Engine (EVE) FMC dashboard tab and widgets not renamed after 7.1 > 7.2+ upgrade

Bug ID	Headline
CSCwh13821	ASA/FTD may traceback and reload in when changing capture buffer size
CSCwh14467	File sizes larger than 100MB for AnyConnect/Secure Client images cannot be uploaded on FMC
CSCwh14475	FTD events stopped being sent to FMC, EventHandler logs "publishing blocked"
CSCwh14863	FTD 7.0.4 cluster drops Oracle's sqlnet packets due to tcp-not-syn
CSCwh15109	SRU installation gets stuck at 602_log_package.pl script, causing deployment failure
CSCwh15223	Lina crash in snp_fp_tcp_normalizer() when DAQ/Snort sends malformed L3 header
CSCwh15649	Packet drop due to unexpected-packet drop reason if route to destination is missing in egress VRF
CSCwh16301	Incorrect Hit count statistics on ASA Cluster only for Cluster-wide output
CSCwh17576	Site-to-Site VPN tunnel status on FMC shows down even though it is UP from FTD side
CSCwh18967	Include "show env tech" in FXOS FPRM troubleshoot
CSCwh19897	ASA/FTD Cluster: Reuse of TCP Randomized Sequence number on two different conns with same 5 tuple
CSCwh21141	The FMC preview deployment shows a wrong information.
CSCwh21360	741 - HA & AppAgent - Long term solution for avoiding momentary split-brain situations
CSCwh21420	ASA unexpected HA failover due to MIO blade heartbeat failure
CSCwh21474	ASA traceback when re-configuring access-list
CSCwh22317	LILO validation during Readiness Check missing
CSCwh22348	sfdatacorrelator crashing due to table corruption 'rua_event_xxxxx'
CSCwh22565	Snort 3 HTTP Intrusion Prevention System Rule Bypass Vulnerability
CSCwh23567	PAC Key file missing on standby on reload
CSCwh23863	SYSLOG UDP: One of syslog server is not getting the syslog message with userVRF
CSCwh24826	FMC upgrade stuck at 1039_fmc_rabbitmq_enable
CSCwh24901	'Frequent drain of events (not unprocessed events) to be removed from FMC
CSCwh25351	FTD VMWare: High disk utilization on /dev/sda8 partition caused by file system corruption
CSCwh25928	FMC userrole missing permissions may cause Tomcat to continuously restart after upgrade to 7.2.4

Bug ID	Headline
CSCwh26526	SQL packets involved in large query is drop by SNORT3 with reason snort-block
CSCwh27230	Connections are not cleared after idle timeout when the interfaces are in inline mode.
CSCwh27414	Deploy status is going to deployed right after starting deployment then going to deploying state
CSCwh28007	While editing AC-policy rules, the rule order number becomes misaligned.
CSCwh28144	Specific OID 1.3.6.1.2.1.25 should not be responding
CSCwh28185	dl_task.pl tasks keep getting created every hour when a database query is blocked
CSCwh28206	Firewall Blocking packets after failover due to IP <-> SGT mappings
CSCwh28218	Syslog not updating when prefilter rule name changes
CSCwh29092	FTD (FDM) fails when executing script 800_post/100_ftd_onbox_data_import.sh
CSCwh29167	FMC FlexConfig re-orders objects after a single successful deployment
CSCwh30111	FTD - Upgrade triggers persistent VPN Tunnel health monitor alarm
CSCwh30676	Ping to the configured systemIP on management interface getting failed in cluster setup.
CSCwh30891	ASA/FTD may traceback and reload in Thread Name 'ssh' when adding SNMPV3 config
CSCwh31495	FTD - Traceback and reload due to nat rule removed by CPU core
CSCwh31502	Enhancement for Lina copy operation for startup-config to backup-config.cfg in HA
CSCwh32118	ASDM management-sessions quota reached due to HTTP sessions stuck in CLOSE_WAIT
CSCwh34344	FTD not generating end of connection event after "Deleting Firewall session"
CSCwh36167	DAP: FMC adds characters in a LUA script
CSCwh37475	Removal of msie-proxy commands during flexconfig rollback
CSCwh37655	Snort2:Skip writing malware seed file duing process shutdown
CSCwh37733	FTD responding to UDP500 packet with a Mac Address of 0000.000.000
CSCwh37737	FMC7.2.x EIGRP flexconfig migration fails with internal error due to interface config mismatch
CSCwh38492	FMC Restore is stuck in vault clear stage after mysql restore completed
CSCwh38708	ASA "pager line 25" command doesn't work as expected on few terminal applications

Bug ID	Headline
CSCwh40106	FTD hosted on KP incorrectly dropping decoded ESP packets if pre-filter action is analyze
CSCwh40294	ASA traceback due to panic event during SNMP configuration
CSCwh40968	Large file download failed due to hitting the max segment limit
CSCwh41127	ASA/FTD: NAT64 error "overlaps with inside standby interface address" for Standalone ASA
CSCwh42077	Cisco_Firepower_GEODB_FMC_Update* are not included in diskmanager
CSCwh42412	FTD Block 9344 leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwh44479	Configuration archive creation failing and causing deployment preview to throw error
CSCwh45450	2100: Interfaces missing from FTD after removing interfaces as members of a port-channel
CSCwh47395	Extended Access List Object does not allow IP range configuration
CSCwh47701	ASA allows same BGP Dynamic routing process for Physical Data and management-only interfaces
CSCwh48844	FTD: Failover/High Availability disabled with Mate version 0.0 is not compatible
CSCwh49085	Avoid unnecessary DB operations when processing derived fingerprints
CSCwh49244	"show aaa-server" command always shows the Average round trip time 0ms.
CSCwh49483	ASA/FTD may traceback and reload while running show inventory
CSCwh50221	4200 Series: Portchannel in cluster may stay down sometimes when LACP is in active mode
CSCwh52420	AMP Cloud look up timeout frequently.
CSCwh52526	FMC SSO timesout when user session is active for more than 1 hr (idle timeout)
CSCwh53116	Initiator Country and Continent missing on Custom View on Event viewer
CSCwh53143	ASA:Management access via IPSec tunnel is NOT working
CSCwh53377	FMC does not verify certificate issued to FTD device, when TLS1.3 is used
CSCwh54029	FMC HA : Redundant FTD registration task failing on secondary FMC when FTD is disconnected.
CSCwh54228	FMC: query_engine.log Growing More Quickly Than Expected, Resulting In High Disk Utilization
CSCwh54477	The FMC is showing "The password encryption key has not been set" alert for a 11xx/21xx/31xx device

Bug ID	Headline
CSCwh56945	SFDataCorrelator crashing repeatedly in RNA_DB_InsertServiceInfo
CSCwh58999	Devices with classic licenses are failed to register with FMC running version 7.2.X
CSCwh59199	ASA/FTD traceback and reload with IPSec VPN, possibly involving upgrade
CSCwh59222	SNORT3 - FTD - TSID high cpu, daq polling when ssl enabled is not pulling enough packets
CSCwh59557	Source NAT Rule performing incorrect translation due to interface overload
CSCwh60604	ASA/FTD may traceback and reload in Thread Name 'lina' while processing DAP data
CSCwh60608	VPN Load Balancing Cluster IP address/host name is not on the same subnet as the public interface
CSCwh60631	Fragmented UDP packet via MPLS tunnel reassemble fail
CSCwh61690	Multicast through the box traffic causing high CPU with 1GBps traffic
CSCwh62080	additional command outputs needed in FTD troubleshoot for blocks and ssl cache
CSCwh62473	FMC HA: When logging into the standby FMC stacktraces are always present.
CSCwh63211	Lina core at snp_nat_xlate_verify_magic.part and soft traces
CSCwh63588	FTD SNMPv3 host configuration gets deleted from IPTABLES after adding host-group configuration
CSCwh63663	Cannot use .k12 domain on realm AD Primary Domain configuration
CSCwh64508	Fixing the regression caused while handling web UI is not getting FTDv Variable
CSCwh66359	ASDM can not see log timestamp after enable logging timestamp on cli
CSCwh66636	Configuring and unconfiguring "match ip address test" may lead to traceback
CSCwh66991	sshd restarting during upgrade leading to have /new-root as default root partition
CSCwh68515	Backup fails on migrated FMC
CSCwh68856	Configuration to disable TLS1.3
CSCwh68878	Diskmanager process terminated unexpectedly
CSCwh69209	Prefilter cannot add Tunnel Endpoints in Tunnel Rule on FMC
CSCwh69346	ASA: Traceback and reload when restore configuration using CLI
CSCwh69815	FTDvs through put got changed to 100Kbps after upgrade
CSCwh70323	Timestamp entry missing for some syslog messages sent to syslog server
CSCwh70481	Community string sent from router is not matching ASA

Bug ID	Headline
CSCwh70628	ASA/FTD may traceback and reload due to watchdog time exceeding the default 15 seconds
CSCwh70905	Secondary lost failover communication on Inside, using IPv6, but next testing of Inside passes
CSCwh71050	FXOS : Duplication of NTP entry results in Error message : Unreachable Or Invalid Ntp Server
CSCwh71358	Unable to create VRF via FDM in Firepower 3105 device
CSCwh71589	Coverity 886745: OVERRUN in verify_generic_signature
CSCwh72522	Error while saving RAVPN with LDAP attribute map containing entry without cisco attr mapping name
CSCwh73727	Snort3 dropping IP protocol 51
CSCwh74870	Unexpected high values for DAQ outstanding counter
CSCwh76959	FMC does not save changes made on access list.
CSCwh77348	ASA: Traceback and reload when executing the command "show nat pool detail" on a cluster setup
CSCwh77527	FMC should report user whether it supports or not while configuring remote storage
CSCwh78118	ASA/FTD traceback and reload on process fsm_send_config_info_initiator
CSCwh83328	SNMP fails to poll accurate hostname from FMC
CSCwh83517	VTI tunnel goes down due to route change detected in VRF scenario
CSCwh84833	Every HA sync attempts to disable URL filtering if already disabled.
CSCwh85824	eStreamer JSON parse error and memory leak
CSCwh89289	Snort is getting reloaded during deploy due to diff in timerange and nap conf contents in each run
CSCwh90693	FTD unregisters the standby FMC immediately after a successful registration
CSCwh90813	FDM Upgrade failure due to expired certificates.
CSCwh93649	File copy via SCP using ciscossh stack fails with error "no such file or directory"
CSCwh95175	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwh98563	Import Fails for Policy Description having new line.
CSCwh98733	ASA: Traceback and reload during tests of High number of traffic flows and syslog messages
CSCwh99855	cdFMC : FTD Dashboard does not display any data for last 1 hour or 6 hours.

Bug ID	Headline
CSCwi02599	SSX Eventing continues to go to old tenant upon FTD migration to CDO.
CSCwi03528	Cross ifc access: Revert PING to old non-cross ifc behavior
CSCwi06007	FMC missing validation for syslog port setting
CSCwi07068	SFDataCorrelator logs "Killing MySQL connection" every minute, causing performance problems
CSCwi14132	FMC/cdFMC increase API rate limit
CSCwi14896	Node kicked out of cluster while enabling or disabling rule profiling
CSCwi16571	Capture-traffic Clish command with snort3 not producing a proper resulting capture
CSCwi17713	Cisco ASA and FTD Software Inactive-to-Active ACL Bypass Vulnerability
CSCwi24880	ASA dropping IPSEC traffic incorrectly when "ip verify reverse-path" is configured
CSCwi25340	VPN and certificate configuration is cleared after the deployment - Regression of CSCwh29167
CSCwi27306	LINA would randomly generate a traceback and reload on FPR-1K
CSCwi31091	OSPF Redistribution route-map with prefix-list not working after upgrade
CSCwi82368	Classic licenses needs to be manually added after registering to license during migration/RMA
CSCwi92702	Run All function on FMC Health Monitoring page is greyed out after upgrade
CSCwj02770	FMC Model migration document doesn't have the roll-back steps if they hit failures
CSCwj12773	FMC - Syslog overide in ACP always sent via Management interface
CSCwk14697	Port Configuration Error in M6 FMC Documentation for Eth3 and Eth2 on FMC1700,FMC2700,FMC4700 Models
CSCwk21126	FTD Registration fails if Management interface has the same IP as Data Interface
CSCwk41400	FMC: FTD Subinterface SGT Propagation Default change to disabled
CSCwm05155	Snort AppID incorrectly identifies SSH traffic as Unknown
CSCwm05674	Onboarding on-prem FMC to CDO using SecureX fails due to User Authentication Failed error
CSCwm28201	DOC: Update the Deploy Virtual Auto Scale Solution using GWLB on AWS Guide
CSCwm29768	Connection been logged for rules with no logging enabled
CSCwm58772	snort2 instances restart unexpectedly with OOM during policy deployment

Resolved Bugs in Version 7.4.0

Table last updated: 2025-02-25

Table 36: Resolved Bugs in Version 7.4.0

Bug ID	Headline
CSCvq20057	Improve logging of Secure Firewall (Firepower)backups and retry for gzip when using remote storage
CSCvq25866	Flex config Preview of $SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST throws error
CSCvt25221	FTD traceback in Thread Name cli_xml_server when deploying QoS policy
CSCvu24703	FTD - Flow-Offload should be able to coexist with Rate-limiting Feature (QoS)
CSCvu28887	Filtering Network objects is not working, getting 'Error Loading Data'
CSCvw77924	Radius Key with the ASCII character " configured on FXOS does not work after chassis reload.
CSCvx04003	Lack of throttling of ARP miss indications to CP leads to oversubscription
CSCvx52042	Upgrade to 6.6.1 got failed at 800_post/1025_vrf_policy_upgrade.pl
CSCvx68173	Observed few snort instances stuck at 100%
CSCvx71936	FXOS: Fault "The password encryption key has not been set." displayed on FPR1000 and FPR2100 devices
CSCvx75441	File list preview: Deleting two list having few similar contents throws stacktrace on FMC-UI
CSCvy11606	Error Loading Data: Couldnt resolve few of the STDACE BBs
CSCvy26676	"Warning:Update failed/in-progress." Cosmetic after successful update
CSCvy95809	Crashinfo script is invoked on SFR running snort2 and device fails to upgrade to 7.0
CSCvz07004	SNORT2: FTD is performing Full proxy even when SSL rule has DND action.
CSCvz08312	ENH:FMC Removal and manual reconfiguration of changes for CAC-authenticated users should not happen
CSCvz42065	IPS policy should be imported when its referred in Access Control policy
CSCwa04262	Cisco ASA Software SSL VPN Client-Side Request Smuggling Vulnerability via "/"URI
CSCwa22766	FMC4500/4600 shows virtual license
CSCwa51867	FDM IKEv2 S2S PSK Not Deploying Correctly (Changing Asymmetric to Symmetric PSK)

Bug ID	Headline
CSCwa72481	API key corrupted for FMC with multiple interfaces
CSCwa80040	FMC NFS configuration failling after upgrade from 6.4.0.4 to 7.0.1
CSCwa93215	Primary node disconnected from VPN-Cluster when performed HA failover on Primary with DNS lookup
CSCwb02955	Modify /800_post/1027_ldap_external_auth_fix.pl to not fail FMC upgrade when objects are corrupt
CSCwb08189	Microsoft update traffic blocked with Snort version 3 Malware inspection
CSCwb20926	FDM: Policy deployment failure after upgrade due to unused IKEv1 policies
CSCwb44848	ASA/FTD Traceback and reload in Process Name: lina
CSCwb51821	Disk usage errors on Firepower Azure device due to large backup unified files under ngfw directory
CSCwb67464	FDM bootstrap could be skipped if device rebooted when bootstrap is not completed
CSCwb84677	FMC backup may fail due to monetdb backup failure with return code 102
CSCwb92583	upgrade with a large amount of unmonitored disk space used can cause failed upgrade and hung device
CSCwb94431	MFIB RPF failed counter instead of Other drops increments when outgoing interface list is Null
CSCwb95453	ASA: The timestamp for all logs generated by Admin context are the same
CSCwc03332	FTD on FP2100 can take over as HA active unit during reboot process
CSCwc13477	FMC | Interface update Failed. Could not find source interface
CSCwc23844	ASAv high CPU and stack memory allocation errors despite over 30% free memory
CSCwc28660	Snort3: NFSv3 mount may fail for traffic through FTD
CSCwc30573	Deployment/Tasks Button not seen FMC_UI while doing upgrade tests configured in Light theme
CSCwc32245	FMC: Validation check to prevent exponential expansion of NAT rules
CSCwc44608	Selective deployment of IPS may cause outage due to incorrectly written FTD configuration files
CSCwc45298	Connection Events seen on FMC even though the rule is not configured to send events to FMC
CSCwc49655	FTPS getting ssl3_get_record:bad record type during connection for KK and DR rules
CSCwc49936	FMC 7.2.0|7.3.0 Integration > Identity Sources page does not load, keeps spinning

Bug ID	Headline
CSCwc50519	Excessive logging from hm_du.pm may lead to syslog-ng process restarts
CSCwc51588	Failing to generate FMC Backup/Restore via SMB/SSH
CSCwc52357	Estreamer page fails to load in ASDM
CSCwc59953	Snort3 crash with TLS 1.3
CSCwc61828	Fix multiple crash handler issues
CSCwc62215	FTD unable to sync HA due to snort validation failed
CSCwc64923	ASA/FTD may traceback and reload in Thread Name 'lina' ip routing ndbshr
CSCwc65814	sybase related modules should be removed
CSCwc65907	snort3 hangs in Crash handler which can lead to extended outage time during a snort crash
CSCwc67687	ASA HA failover triggers HTTP server restart failure and ASDM outage
CSCwc74099	FPR2140 ASA Clock Timezone reverts to UTC after appliance restart/reload
CSCwc74271	Auth-Daemon process is getting restarted continuously when SSO disabled
CSCwc74841	FMC RSS Feed broken because FeedBurner is no longer active - "Unable to parse feed"
CSCwc75082	25G-SR should default to RS-FEC (IEEE CL108) instead of FC-FEC
CSCwc76849	link state propagation stops working when performing full chassis reboot
CSCwc77519	FPR1000 ASA/FTD: Primary takes active role after reloading
CSCwc78296	Database may fail to shut down and/or start up properly during upgrade
CSCwc78689	Cannot save realm configuration unless AD Join Password is empty
CSCwc79520	Snort process may trace back in ssl_debug_log_config and generate core file
CSCwc81219	Intrusion events intermittently stop appearing in FMC when using snort3
CSCwc82205	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwc83037	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 36)
CSCwc87963	ASAv "Unable to retrieve license info. Please try again later"
CSCwc89661	FTD misses diagnostic data required for investigation of "Communication with NPU lost" error
CSCwc89924	FXOS ASA/FTD SNMP OID to poll Internal-data 'no buffer' interface counters
CSCwc93964	ASA using WebVPN tracebacks in Unicorn thread during memory tracking

Bug ID	Headline
CSCwc96016	Captive portal support in cross domain
CSCwc96780	FMC module specific health exclusion disables all health checks
CSCwd00583	SNMP 'Confirm Community String' string is not auto-populated after the FMC upgrade
CSCwd04210	ASA: ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT
CSCwd05814	PDTS write from Daq can fail when PDTS buffer is full eventually leads to block depletion
CSCwd07059	multiple snort3 crashes after upgrading FTD from 7.2.0 to 7.2.0.1
CSCwd07278	ASA/FTD tmatch compilation check when unit joins the cluster, when TCM is off
CSCwd09870	AnyConnect SAML using external browser and round robin DNS intermittently fails
CSCwd09967	Deployment Fails with stacktrace: Invalid type (LocalIdentitySource)
CSCwd10497	FTD sensor rules missing from ngfw.rules file after a sensor backup restore execution
CSCwd10880	critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on 2100/3100 devices
CSCwd11005	Missing fqdns_old.conf file causes FTD HA app sync failure
CSCwd13083	FMC - Unable to initiate deployment due to incorrect threat license validation
CSCwd13917	during download from file event on FMC, high CPU use on FMC for 20 minutes before download fails
CSCwd14688	FTD upgrade failure due to Syslog files getting generated/deleted rapidly
CSCwd14732	FTD Unable to bind to port 8305 after management IP change
CSCwd15197	ASA/FTD: Using Round Robin with PAT rules on two or more interfaces breaks IP stickiness
CSCwd16017	Object edit slowness when it is associated with NAT rules
CSCwd16517	GTP drops not always logged on buffer and syslog
CSCwd16902	File events show Action as "Malware Block" for files with correct disposition of unknown
CSCwd16906	ASA/FTD may traceback and reload in Thread Name 'lina' following policy deployment
CSCwd17940	HA did not failover due to misleading status updates from NDClient
CSCwd18744	FPR1K FTD fails to form HA due to reason "Other unit has different set of hwidb index"
CSCwd19053	ASA/FTD may traceback with large number of network objects deployment using distribute-list

Bug ID	Headline
CSCwd20900	HTTP Block Response and Interactive Block response pages not being displayed by Snort3
CSCwd22413	EIGRPv6 - Crashed with "mem_lock: Assertion mem_refcount' failed" on LINA.
CSCwd23188	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwd27186	All traffic blocked due to access-group command missing from FTD config
CSCwd28236	standby unit using both active and standby IPs causing duplicate IP issues due to nat "any"
CSCwd29835	log rotate failing to cycle files, resulting in large file sizes
CSCwd30298	FTD: FTPS Data Channel connection impacted by TLS Server Identity and Discovery Probe sent by FTD
CSCwd30774	FMC HA - files in tmp/Sync are left on secondary when synchronisation task fails
CSCwd32892	lost cac.conf after upgrade to 7.2.1 for FMC smart-card auth
CSCwd33054	DHCP Relay is looping back the DHCP offer packet causing dhcprelay to fail on the FTD/ASA
CSCwd33479	Duplicate SMB session id packets causing snort3 crash
CSCwd34662	LTS18 and LTS21 commit id update in CCM layer (seq 39)
CSCwd35726	Cisco FXOS Software Arbitrary File Write Vulnerability
CSCwd36246	Filtering of jobs in deploy history page is applying the criteria only on Top50 jobs
CSCwd37135	ASA/FTD traceback and reload on thread name fover_fail_check
CSCwd38196	Proxy is engaged even when we have a Definitive DND rule match
CSCwd38526	FMC can allow deployment of NAP in test mode with Decrypt policy
CSCwd39506	SSL Policy DND default Rule fails on error unsupported cipher suite and SKE error.
CSCwd40141	Firepower Management Center GUI view for Snort2 Local Intrusion Rules is missing
CSCwd40955	Very long validation time during Policy Deployment due to big network object in SSL policy
CSCwd41224	FMC HA webUI is not getting FTDv Variable tier assigned FTDv - Variable
CSCwd41466	Re-downloaded users from a forest with trusted domains may become unresolved/un-synchronized
CSCwd41806	deployment failed with OOM (out of memory) for policy_apply.pl process
CSCwd41986	Packet-Tracer interfaces not showing up in UI after updating interface name from lower to upper case

Bug ID	Headline
CSCwd42072	SRU installation failure.
CSCwd42347	FMC not showing any alerts/warnings when deploying changes of prefix list with same seq #
CSCwd42410	Expected snmp output is not found in 'show run | in fxos snmp'
CSCwd42620	Deploying objects with escaped values in the description might cause all future deployments to fail
CSCwd43666	Analyze why there is no logrotate for /opt/cisco/config/var/log/ASAconsole.log
CSCwd43745	FTDv Cluster Health Monitor fails with "Error fetching live status of the cluster"
CSCwd44326	Object NAT edit is failing
CSCwd45048	Pre-login banner on FCM webUI shows extra characters on 92.14.0
CSCwd46061	FPR 2100: 10G interfaces with 1G SFP goes down post reload
CSCwd46182	Periodic sync failures are not reported to users
CSCwd46741	fxos log rotate failing to cycle files, resulting in large file sizes
CSCwd46780	ASA/FTD: Traceback and reload in Thread Name: appAgent_reply_processor_thread
CSCwd47340	FXOS: memory leak in svc_sam_envAG process
CSCwd47442	800_post/1027_ldap_external_auth_fix.pl upgrade error -- reference to missing authentication object
CSCwd47481	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 40)
CSCwd48633	ASA - traceback and reload when Webvpn Portal is used
CSCwd48776	Port-channel interface went down post deployment
CSCwd49636	FMC UI showing disabled/offline for multiple devices as health events are not processed
CSCwd49685	Missing SSL MEMCAP causes deployment failure due timeout waiting for snort detection engines
CSCwd49758	Pre-deployment failure seen in FMC due to huge number policies
CSCwd50131	Upgrades are not cleaning up mysql files leading to alert for 'High unmanaged disk usage on /ngfw'
CSCwd50218	ASA restore is not applying vlan configuration
CSCwd51757	Unable to get polling results using snmp GET for connection rate OID’s
CSCwd51964	Add validation in lua detector api to check for empty patterns for service apps
CSCwd52995	FMC not opening deployment preview window

Bug ID	Headline
CSCwd53135	ASA/FTD: Object Group Search Syslog for flows exceeding threshold
CSCwd53340	FTD PDTS LINA RX queue can become stuck when snort send messages with 4085-4096 bytes size
CSCwd53635	AWS: SSL decryption failing with Geneve tunnel interface
CSCwd53863	Data migration from Sybase to MariaDB taking more time due to large data size of POLICY_SNAPSHOT
CSCwd54439	FMC gives an irrelevant error message for Snort2 to Snort3 rules conversion failure
CSCwd55642	Stale CPU core health events seen on FMC UI post upgrade to 7.0.0+.
CSCwd55673	Need corrections in log_handler_file watchdog crash fix
CSCwd55853	Deployment failure with localpool overlap error after upgrade
CSCwd56254	"show tech-support" generation does not include "show inventory" when run on FTD
CSCwd56296	FTD Lina traceback and reload in Thread Name 'IP Init Thread'
CSCwd56774	Misleading drop reason in "show asp drop"
CSCwd56995	Clientless Accessing Web Contents using application/octet-stream vs text/plain
CSCwd57698	Recursive panic under lina_duart_write
CSCwd57927	FMC UI may become unavailable and show "System processes are starting" message after upgrade
CSCwd58188	Inline-pair's state could not able to auto recover from hardware-bypass to standby mode.
CSCwd58337	allocate more cgroup memory for policy deployment subgroup
CSCwd58417	HA Periodic sync is failing due to cfg files are missing
CSCwd58430	At times AC Policy save takes longer time, may be around 10 or above mins
CSCwd59736	ASA/FTD: Traceback and reload due to SNMP group configuration during upgrade
CSCwd61016	ASA: Standby may get stuck in "Sync Config" status upon reboot when there is EEM is configured
CSCwd61082	FMC UI Showing inaccurate data in S2S VPN Monitoring page
CSCwd62025	FTDv: Policy Deployment failure due to interface setting on failover interface
CSCwd62138	ASA Connections stuck in idle state when DCD is enabled
CSCwd62915	Cross-domain users with non-ASCII characters are not resolved
CSCwd63580	FPR2100: Increase in failover convergence time with ASA in Appliance mode

Bug ID	Headline
CSCwd63722	FTDv Single-Arm Proxy behind AWS GWLB drops due to geneve-invalid-udp-checksum with all 0 checksum
CSCwd63961	AC clients fail to match DAP rules due to attribute value too large
CSCwd64480	Packets through cascading contexts in ASA are dropped in gateway context after software upgrade
CSCwd64919	FXOS is not rotating PoE logs
CSCwd66709	FP4125 2.10.1.166 FTD applications in HA went into not responding state
CSCwd66815	Lina changes to support - Snort3 traceback in daq-pdts while handling FQDN based traffic
CSCwd66820	Cisco Firepower Management Center Object Group Access Control List Bypass Vulnerability
CSCwd68088	ASA|FTD: Implement different TLS diffie-hellman prime based on RFC recommendation
CSCwd69236	FMC Connection Event stop displaying latest event
CSCwd69454	Port-channel interfaces of secondary unit are in waiting status after reload
CSCwd70117	FMC should not accept carriage return in the interface description field of a managed device
CSCwd71254	ASA/FTD may traceback and reload in idfw fqdn hash lookup
CSCwd71274	S2S VPN dashboard shows ipv4 SVTI tunnel down between KP-HA and WA-HA after KP-HA Switch role.
CSCwd72680	FXOS: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
CSCwd72915	FMC 7.1.0.1 Doesn't throw warning that S2S VPN Configs contain deprecated MD5 Hash during deployment
CSCwd73981	FMC: Updates page takes more than 5 minutes to load
CSCwd74116	S2S Tunnels do not come up due to DH computation failure caused by DSID Leak
CSCwd74839	30+ seconds data loss when unit re-join cluster
CSCwd75738	Predefined FlexConfig Text Objects are not exported by Import-Export
CSCwd75782	FMC External Auth test error "Encryption method is configured but you did not upload a certificate."
CSCwd76622	FTD with Snort3 might have memory corruption BT in snort file with same IP traffic scaling
CSCwd76634	FMC import takes too long

Bug ID	Headline
CSCwd76930	FPR3110 Fans' SN in label are different from show inventory cli output
CSCwd77300	Snort crashes while reloading mercury library with any VDB install on 7.3.0 and 7.4.0
CSCwd78624	ASA configured with HA may traceback and reload with multiple input/output error messages
CSCwd79388	intrusion events fail to migrate from MariaDB to MonetDB following FMC upgrade from 7.0.3 to 7.1.0
CSCwd80284	Import/export fails with backend error
CSCwd80343	MI FTD running 7.0.4 is on High disk utilization
CSCwd80741	Snort drops Bomgar application packets with Early Application Detection enabled
CSCwd81538	FTD Traffic failure due to 9344 block depletion in peer_proxy_tx_q
CSCwd81897	Snort3 crash seen sometimes while processing a future flow connection after appid detectors reload
CSCwd82235	LINA Traceback on FPR-1010 under Thread Name: update_cpu_usage
CSCwd82801	Snort outputs massive volume of packet events - IPS event view may show "No Packet Information"
CSCwd83441	FMC should display the status of physical FTD interfaces bundled in port-channel
CSCwd83990	FTD -Snort match incorrect NAP id for traffic
CSCwd84046	Microsoft SCEP enrollment fails to get ASA identity cert - Unable to verify PKCS7
CSCwd84133	ASA/FTD may traceback and reload in Thread Name 'telnet/ci'
CSCwd84153	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwd84868	Observing some devcmd failures and checkheaps traceback when flow offload is not used.
CSCwd84942	Snort mem used alert should read the value from perfstats for snort instance rather than cgroups
CSCwd85178	AWS ASAv PAYG Licensing not working in GovCloud regions.
CSCwd85609	FTDs running 6.6.x show as disconnected on new HM (6.7+) but checks are running and updating
CSCwd85927	Traceback and reload when webvpn users match DAP access-list with 36k elements
CSCwd86313	Unable to access Dynamic Access policy
CSCwd86457	Number of objects are not getting updated under policies>>>Security intelligence >>>Block list

Bug ID	Headline
CSCwd86535	ASA/FTD: Traceback and Reload on Netflow timer infra
CSCwd86783	Disabling NAVL guids from userappid.conf doesn't work
CSCwd86929	Cut-Through Proxy does not work with HTTPS traffic
CSCwd87129	seeing error on access policies on FMC - "Error during policy validation"
CSCwd87438	Enhance logging mechanism for syslogs
CSCwd88585	ASA/FTD NAT Pool Cluster allocation and reservation discrepancy between units
CSCwd88641	Deployment changes to push VDB package based on Device model and snort engine
CSCwd89848	ASA/FTD failure due to heartbeat loss between chassis and blade
CSCwd90112	MariaDB crash (segmentation fault) related to netmap query
CSCwd90846	Software upgrade on FDM fails due to improver next-hop validation
CSCwd91013	FMC | Deployment failure in csm_snapshot_error
CSCwd91421	ASA/FTD may traceback and reload in logging_cfg processing
CSCwd91932	Incorrect Paging and count value for Time Range Object Get API
CSCwd92804	FAN LED flashing amber on FPR2100
CSCwd93316	No Inspect Interruption warning when deploy after FMC upgrade
CSCwd93376	Clientless VPN users are unable to download large files through the WebVPN portal
CSCwd93792	SFDataCorrelator performance degradation involving hosts with many discovered MAC addresses
CSCwd94096	Anyconnect users unable to connect when ASA using different authentication and authorization server
CSCwd94183	Blade not coming up after FXOS update support on multi-instance due to ssp_ntp.log log rotation prob
CSCwd94670	Can't modify RA vpn group policy on FDM 7.3
CSCwd95436	Primary ASA traceback upon rebooting the secondary
CSCwd95908	ASA/FTD traceback and reload, Thread Name: rtcli async executor process
CSCwd96041	FMC SecureX via proxy stops working after upgrade to 7.x
CSCwd96493	Link Up seen for a few seconds on FPR1010 during bootup
CSCwd96500	FTD: Unable to configure WebVPN Keepout or Certificate Map on FPR3100
CSCwd96755	ASA is unexpected reload when doing backup

Bug ID	Headline
CSCwd96766	41xx: Blade does not capture or log a reboot signal
CSCwd96790	High FMC backup file size due to configurations snapshot for all managed devices
CSCwd97020	ASA/FTD: External IDP SAML authentication fails with Bad Request message
CSCwe00757	Summary status dashboard takes more than 3 mins to load upon login
CSCwe00828	Interactive Block action doesn't work when websites are redirected to https
CSCwe00864	License Commands go missing in Cluster data unit if the Cluster join fails.
CSCwe03529	FTD traceback and reload while deploying PAT POOL
CSCwe03631	Need to provide rate-limit on "logging history <mode>"
CSCwe04437	collection of top.log.gz in troubleshoot can be corrupt due to race condition
CSCwe04746	Unexpected "No Traffic" health alert on Standby HA Data Interface where no data flows
CSCwe05913	FTD traceback/reloads - Icmp error packet processing involves snp_nat_xlate_identity
CSCwe06562	FPR1K/FPR2K: Increase in failover time in Transparent Mode with high number of Sub-Interfaces
CSCwe06724	Database table optimization not working for some of the tables
CSCwe06826	Email alert incorrectly send for a successful database backup
CSCwe06828	FMC HA Synchronization can hang forever if no response from SendUserReloadSGTAndEndpointsEvent
CSCwe07103	FMC: Upgrade fails at DB Integrity check due to large number of EO warnings for "rule_comments"
CSCwe07722	Cluster data unit drops non-VPN traffic with ASP reason "VPN reclassify failure
CSCwe07928	On a cloud-delivered FMC there is no way to send events to syslog without sending to SAL/CDO as well
CSCwe08729	FPR1120:connections are getting teardown after switchover in HA
CSCwe08908	Threatgrid integration configuration is not sync'd as part of the FMC HA Synchronisation
CSCwe09074	None option under trustpoint doesn't work when CRL check is failing
CSCwe09121	FTD Deployment failures due to "snort3.validation.lua:5: '=' expected near 'change'"
CSCwe09811	FTD traceback and reload during policy deployment adding/removing/editing of NAT statements.
CSCwe10290	FTD is dropping GRE traffic from WSA

Bug ID	Headline
CSCwe10548	ASA binding with LDAP as authorization method with missing configuration
CSCwe11119	ASA: Traceback and reload while processing SNMP packets
CSCwe11727	Purging of Config Archive failed for all the devices if one device has no versions
CSCwe12407	High Lina memory use due to leaked SSL handles
CSCwe13627	FMC Unable to fetch VPN troubleshooting logs.
CSCwe14174	FTD - 'show memory top-usage' providing improper value for memory allocation
CSCwe14417	FTD: IPSLA Pre-emption not working even when destination becomes reachable
CSCwe14514	ASA/FTD Traceback and reload of Standby Unit while removing capture configurations
CSCwe14590	FMC deployment preview showing full config instead of delta.
CSCwe15111	FMC is not taking BGP default originate configuration via API PUT request.
CSCwe16554	TLS sessions dropped under certain conditions after a fragmented Client Hello
CSCwe16620	FMC Health Monitor does not report alerts for the Interface Status module
CSCwe16730	Deployment failing - "Error while printing show-xml-response file contents" XML response too big
CSCwe17858	FMC HA info is not sync'ed reliably to FTD to support CLOUD_SERVICE
CSCwe18090	FMC deployment failure:"Validation failed: This is a slav*/ha standby device, rejecting deployment."
CSCwe18216	null connection error seen in logs
CSCwe18472	[FTD Multi-Instance][SNMP] - CPU OIDs return incomplete list of associated CPUs
CSCwe18974	ASA/FTD may traceback and reload in Thread Name: CTM Daemon
CSCwe19051	FTD High unmanaged disk usage alert is triggered due to stored files located on /ngfw/Volume/root1/
CSCwe19830	Policy deploy failure "error executing /*!40101 SET character_set_client = @saved_cs_client */; *"
CSCwe20043	256-byte memory block gets depleted on start if jumbo frame is enabled with FTD on ASA5516
CSCwe20714	Traffic drop when primary device is active
CSCwe21037	Snort mem used alert should be consistent with value from top.log
CSCwe21187	ASA/FTD may drop multicast packets due to no-mcast-intrf ASP drop reason until UDP timeout expires

Bug ID	Headline
CSCwe21280	Multicast connection built or teardown syslog messages may not always be generated
CSCwe21831	add warning to FTD platform settings when VPN Logging Settings logging level is informational
CSCwe21959	Snort3: Process in D state resulting in OOM with jemalloc memory manager
CSCwe22254	After disabling malware analysis, high disk usage on /dev/shm/snort
CSCwe22302	Partition "/opt/cisco/config" gets full due to wtmp file not getting logrotated
CSCwe22386	Unexpected firewalls reloads with traceback.
CSCwe22492	Slow UI loading for Table View of Hosts
CSCwe22980	Database integrity check takes several minutes to complete
CSCwe23039	NTP polling frequency changed from 5 minutes to 1 second causes large useless log files
CSCwe23801	FPR2100: Mulitple snort3 & snort2 cores got generated and sensor goes down in KP platform
CSCwe24532	Multiple instances of nvram.out log rotated files under /opt/cisco/platform/logs/
CSCwe25187	FMC External authentication getting "Internal error"
CSCwe25391	rpc service detector causing snort traceback due to universal address being an empty string
CSCwe26342	ASA Traceback & reload citing thread name: asacli/0
CSCwe26612	FTD taking longer than expected to form OSPF adjacencies after a failover switchover
CSCwe28094	ASA/FTD may traceback and reload after executing 'clear counters all' when VPN tunnels are created
CSCwe28362	Copy and pasting rules is broken and give blank error message in ID policy
CSCwe28407	LINA traceback with icmp_thread
CSCwe28726	The command "app-agent heartbeat" is getting removed when deleting any created context
CSCwe29179	CLUSTER: ICMP reply arrives at director earlier than CLU add flow request from flow owner.
CSCwe29498	occasional failure to load light-modal-ac-rule-xx.css with a net::ERR_TOO_MANY_RETRIES error
CSCwe29529	FTD MI does not adjust PVID on vlans attached to BVI
CSCwe29583	ASA/FTD may traceback and reload in Thread Name 'None' at lua_getinfo

Bug ID	Headline
CSCwe29850	ASA/FTD Show chunkstat top command implementation
CSCwe29952	SFDataCorrelator cores due to stuck database query after 1 hour deadlock timeout
CSCwe30228	ASA/FTD might traceback in funtion "snp_fp_l2_capture_internal" due to cf_reinject_hide flag
CSCwe30867	Workaround to set hwclock from ntp logs on low end platforms
CSCwe32448	changing time window settings in FMC GUI event viewers may not work with FMC integrated with SecureX
CSCwe33130	Supervisor does not reboot unresponsive module/blade due to IERR with minor severity sensor ID 79
CSCwe34871	Active authentication sessions are showing in VPN dashboard
CSCwe36176	ASA/FTD: High failover delay with large number of (sub)interfaces and http server enabled
CSCwe37132	TLS Server Identity may cause certain clients to produce mangled Client Hello
CSCwe37453	Gateway is not reachable from standby unit in admin and user context with shared mgmt intf
CSCwe38029	Multiple traceback seen on standby unit.
CSCwe39425	2100: Power switch toggle leads to ungraceful shutdowns and "PowerCycleRequest" reset
CSCwe39431	FMC Upgrade: generation of sftunnel.json file per FTD does not check for duplicate names
CSCwe39546	FMC: Backup to an unavailable remote host results in the inability to restart the appliance.
CSCwe40463	Stale IKEv2 SA formed during simultaneous IKE SA handling when missing delete from the peer
CSCwe41336	FDM WM-HA ssh is not working after upgrading 7.2.3 beta with data interface as management
CSCwe41898	ASA: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
CSCwe43965	Remove the limit of 30characters in the rule name which a rule is moved from ACP to Prefilter
CSCwe44311	FP2100:Update LINA asa.log files to avoid recursive messages-<date>.1.gz rotated filenames
CSCwe44620	Question mark in NAT description causes config mismatch on Data members of an FTD cluster

Bug ID	Headline
CSCwe44672	Syslog ASA-6-611101 is generated twice for a single ssh connection
CSCwe44766	IMS: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
CSCwe45211	Need to Warn the users before triggering a full deployment on FTD managed by FDM
CSCwe45222	Snort3 crashes are seen under Dce2Smb2FileTracker processing of data
CSCwe45779	ASA/FTD drops traffic to BVI if floating conn is not default value due to no valid adjacency
CSCwe45879	Frequent errors seen regarding failures to load bulkcsv files that don't exist
CSCwe48378	Remove FMC drop_cache trigger to prevent Disk I/O increase due to file cache thrashing
CSCwe48432	Unable to save Access Control Policy changes due to Internal error
CSCwe50946	Management interface link status not getting synced between FXOS and ASA
CSCwe50993	SNMP on SFR module goes down and won't come back up
CSCwe51286	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe51296	Not able to remove group policy from RAVPN via REST API
CSCwe51443	ASA Evaluation of OpenSSL vulnerability CVE-2022-4450
CSCwe52120	SSL decrypted conns fails when tx chksum-offload is enabled with the egress interface a pppoe.
CSCwe52499	NGIPSv syslog-tls.conf.tt needs filters removed when in CC mode
CSCwe53089	The user belonging to a subdomain, is unable to collect packet tracer
CSCwe54529	FTD on FPR2140 - Lina traceback and reload by TCP normalization
CSCwe54567	Manager gets unregistered on its own from the FTD, show manager shows 'No managers configured'
CSCwe56452	BGP IPv6 configuration : route-map association with neighbour not getting deployed
CSCwe57218	FMC: Incorrect FTD cluster role status leading to inability to upgrade FTD
CSCwe58207	Memory leak observed on ASA/FTD when logging history is enabled
CSCwe58576	FTD:Node not joining cluster with "Health check detected that control left cluster" due to SSL error
CSCwe58881	After FMC upgrade, SecureX ribbon redirects to US cloud region regardless of the set cloud region
CSCwe58980	/var/sf/QueryPoolData fills up with warehouse directories

Bug ID	Headline
CSCwe59380	FTD: "timeout floating-conn" not operating as expected for connections dependent on VRF routing
CSCwe59664	DAP policy created in FMC Gui, to detect a Windows OS with a hotfix, will not work as expected
CSCwe59737	ASA/FTD reboots due to traceback pointing to watchdog timeout on p3_tree_lookup
CSCwe59919	FTD Traceback and reload on Thread Name "NetSnmp Event mib process"
CSCwe60267	FXOS fault F0853 and F0855 seen despite keyring reporting renewed
CSCwe61599	FTD 2100 -Update daq-ioq mempool to help protect against buffer corruption
CSCwe61703	Unable to delete custom anyconnect attribute --dynamic-split-tunnel from group-policy
CSCwe61928	PIM register packets are not sent to RP after a reload if FTD uses a default gateway to reach the RP
CSCwe61969	ASA Multicontext 'management-only' interface attribute not synced during creation
CSCwe62361	ASA reboots due to heartbeat loss and "Communication with NPU lost"
CSCwe62703	New context subcommands are not replicated on HA standby when multiple sessions are opened.
CSCwe62927	DCCSM session authorization failure cause multiple issues across FMC
CSCwe62971	Policy Deploy Failing when trying to remove Umbrella DNS Connector Configuration
CSCwe62997	ASA/FTD traceback in snp_tracer_format_route
CSCwe63067	ASA/FTD may traceback and reload in Thread Name 'lina' due to due to tcp intercept stat
CSCwe63232	ASA/FTD: Ensure flow-offload states within cluster are the same
CSCwe63266	Need fault/error for invalid firmware MF-111-234949
CSCwe63316	Pri-Active FMC NOT triggering registration TASK for FTD to configure standby manager
CSCwe63493	Post backup restore multiple processes are not up. No errors are observed during backup or restore.
CSCwe64043	Cisco ASA and FTD ACLs Not Installed upon Reload
CSCwe64281	Deployment failed in snapshot generation after upgrading FMC to 7.3
CSCwe64404	ASA/FTD may traceback and reload after changing IP of authentication server
CSCwe64542	TID python processes stuck at 100% CPU
CSCwe64557	ASA: Prevent SFR module configuration on unsuported platforms

Bug ID	Headline
CSCwe64563	The command "neighbor x.x.x.x ha-mode graceful-restart" removed when deleting any created context
CSCwe65245	FP2100 series devices might use excessive memory if there is a very high SNMP polling rate
CSCwe65634	ASA - Standby device may traceback and reload during synchronization of ACL DAP
CSCwe66132	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe67751	Last fragment from SIP IPv6 packets has MF equal to 1, flagging that more packets are expected
CSCwe67816	ASA / FTD Traceback and reload when removing isakmp capture
CSCwe68159	Failover fover_trace.log file is flooding and gets overwritten quickly
CSCwe68917	Snort3 fails to match SMTPS traffic to ACP rules
CSCwe69388	FMC should push the AnyConnect Custom attribute defer keyword as lowercase instead of capitalized
CSCwe70202	Multiple times the failover may be disabled by wrongly seeing a different "Mate operational mode".
CSCwe70558	FTD: unable to run any commands on CLISH prompt
CSCwe70665	Snort high memory alerts still seen despite fix for CSCwd84942
CSCwe70721	Deployment is blocked due to Pre-deploy Validation Error - Invalid endpoint
CSCwe71284	ASA/FTD may traceback and reload in Thread Name DATAPATH-3-21853
CSCwe71672	Selective deployment negating the route configs
CSCwe71673	Selective deployment removing the prefilter-configs
CSCwe71674	Selective deployment removing the Group policy
CSCwe72330	FTD LINA traceback and reload in Datapath thread after adding Static Routing
CSCwe72535	Unable to login to FTD using external authentication
CSCwe73116	Cross-interface-access: ICMP Ping to management access ifc over VPN is broken
CSCwe73240	FMC runs out of space when Snort sends massive numbers of packet logs
CSCwe74059	logrotate is not compressing files on 9.16 ASA or 7.0 FTD
CSCwe74089	ASA/FTD may traceback and reload in Thread Name DATAPATH-1-1656
CSCwe74290	SFDataCorrelator spam seen in /var/log/messages
CSCwe74328	AnyConnect - mobile devices are not able to connect when hostscan is enabled

Bug ID	Headline
CSCwe74899	CD App Sync error is App Config Apply Failed on Secondary/Standby after backup restore on RMA device
CSCwe74916	Interface remains DOWN in an Inline-set with propagate link state
CSCwe75018	Snort2 rule recommendations increases disabled rule count drastically
CSCwe75055	[FMC model migration] Health monitoring on FMC reporting errors
CSCwe75124	Upgraded FMC didn't mark FTD's with Hot Fix as light registered - failed FMC HA sync
CSCwe75207	High rate of network map updates can cause large delays and backlogs in event processing
CSCwe76036	ndclientd error message 'Local Disk is full' needs to provide mount details which is full
CSCwe76722	ASA/FTD: From-the-box ping fails when using a custom VRF
CSCwe77123	ASA/FTD : Degradation for TCP tput on FPR2100 via IPSEC VPN when there is delay between VPN peers
CSCwe77896	Improve Azure AD realm documentation
CSCwe78977	ASA/FTD may traceback and reload in Thread Name 'pix_flash_config_thread'
CSCwe79051	Deployment for eigrp / bgp change may cause temporary outage during policy apply
CSCwe79072	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe79954	LDAP External auth config fails to deploy to FTD if same LDAP server is added as Primary and backup
CSCwe80063	Default DLY value of port-channel sub interface mismatch with parent Portchannel
CSCwe81684	ASA: Standby failure on parsing of "management-only" not reported to parser/failover subsystem
CSCwe82107	health alert for [FSM:STAGE:FAILED]: external aaa server configuration
CSCwe82631	FMC isn't allowing to create more than 30 VLAN interfaces
CSCwe83061	FMC Upgrade from Active-Primary FMC is failed with "Installation failed: Peer Discovery incomplete."
CSCwe83069	Fix Snort3 Memory Utilisation Value
CSCwe83478	Prune target should account for the allocated memory from the thread pruned
CSCwe85432	ASA/FTD traceback and reload on thread DATAPATH-14-11344 when SIP inspection is enabled

Bug ID	Headline
CSCwe86029	FMC system restore authentication error during FMC re-image when using FTP/SCP protocol
CSCwe86225	ASA/FTD traceback and reload due citing thread name: cli_xml_server in tm_job_add
CSCwe86350	email alert to scheduled activity is not working after upgrading to 7.2
CSCwe88496	"Failed to convert snort 2 custom rules. Refer /var/sf/htdocs/ips/snort.rej for more details."
CSCwe88772	ASA traceback and reload with process name: cli_xml_request_process
CSCwe89030	Serial number attribute from the subject DN of certificate should be taken as the username
CSCwe89305	vFMC300 to FMC2600 migration failure with error "migration from R to N is not allowed"
CSCwe89731	Notification Daemon false alarm of Service Down
CSCwe89985	CVIM Console getting stuck in "Booting the kernel" page
CSCwe90095	Username-from-certificate feature cannot extract the email attribute
CSCwe90202	ASA: Standby failure on parsing of "management-only" for dynamic configuraiton changes
CSCwe90334	Missing Instance ID in unified_events-2.log
CSCwe90596	Elephant flow detection disabled on FMC, getting enabled on FTD after random deployment
CSCwe90720	ASA Traceback and reload in parse thread due ha_msg corruption
CSCwe91958	correlation events based on connection events do not contain Security Intelligence Category content
CSCwe92905	ngfwManager process continuously restarting leading to ZMQ Out of Memory traceback
CSCwe93061	FTD returns no output of "show elephant-flow status" when efd.lua file's content is empty
CSCwe93162	FP1140 7.0.4 Deployment keep failing with error "Can\'t use an undefined value as a HASH reference"
CSCwe93176	Snort2 rule assignments missing from ngfw.rules (assignment_data table) after FMC upgrade.
CSCwe93202	FXOS REST API: Unable to create a keyring with type "ecdsa"
CSCwe93489	Threat-detection does not recognize exception objects with a prefix in IPv6
CSCwe93532	ASA/FTD may traceback and reload in Thread Name 'lina'.

Bug ID	Headline
CSCwe93537	Threat-detection does not allow to clear individual IPv6 entries
CSCwe93566	need to turn off default TLS 1.1 (deprecated) support for the FDM GUI
CSCwe93736	ASA not updating Timezone despite taking commands
CSCwe94287	FTD DHCP Relay drops NACK if multiple DHCP Servers are configured
CSCwe94789	Umbrella DNS Negate of Bypass Domain Field is not generated from FMC
CSCwe95757	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe96023	ASa/FTD: SNMP related traceback and reload immediately after upgrade from 6.6.5 to 7.0.1
CSCwe96068	ASA: Configurable CLU for Large amount of under/overruns on CLU RX/TX queues
CSCwe96857	FMC error displaying users page due to wide characters in real name field
CSCwe97325	FDM Cannot create self-signed certificates due to Expiration Date format
CSCwe98430	AC policy deploy failing on 7.2.4 FMC to 6.7 FTD
CSCwe99040	traceback and reload thread datapath on process tcpmod_proxy_continue_bp
CSCwe99550	Add knob to pause/resume file specific logging in asa log infra.
CSCwe99945	DOC: Misleading Documentation of Cisco Firepower 2100 GLC-T and GLC-TE SFP Support
CSCwf00417	FTD: Unable to process a TLS1.2 website with TLS Server Identity with client generating SSL Errors
CSCwf00483	Found Orphaned SFTop10Cacher processes
CSCwf00865	FTD/ASA Hub and spoke (U-turn) VPN fails when one spoke is IPSec flow offloaded and the other isn't
CSCwf01051	standby in disabled state after QP-MI HA 7.0.3 to 7.2.4-126, APPLY_APP_CONFIG_APPLICATION_FAILURE
CSCwf01064	TCP ping is completely broken starting in 9.18.2
CSCwf01954	FTD: ADI.conf - send_s2s_vpn_events is set to 0, even after applying s2s vpn health policy
CSCwf02363	Snort3 Crash in SslServiceDetector after call from nss_passwd_lookup
CSCwf03011	Prune symmetric triggers that existed in sfsnort schema before FMC upgrade to 7.3 version or later
CSCwf04831	ASA/FTD may traceback and reload in Thread Name 'ci/console'
CSCwf04870	ASA: "Ping <ifc_name> x.x.x.x" is not working as expected starting 9.18.x

Bug ID	Headline
CSCwf06318	Readiness check needs to be allowed to run without pausing FMC HA
CSCwf06377	Setting heartbeat timeout to 6sec for BS and QP
CSCwf07030	Upgrade Device listing page is taking more than 15 mins to load page fully with 25 FTDs registered
CSCwf07791	ASA running out of SNMP PDU and SNMP VAR chunks
CSCwf08043	Lina traceback and reload due to fragmented packets
CSCwf08515	FPR3100: ASA/FTD High traffic impact on all data interfaces with high counter of "demux drops"
CSCwf10422	"Security Intelligence feed download failed" displayed even though it succeeded
CSCwf10486	ISE Integration Network filter not accepting multiple comma separated networks
CSCwf10910	FTD : Traceback in ZMQ running 7.3.0
CSCwf12005	ASA sends OCSP request without user-agent and host
CSCwf12408	ASA: After upgrade to 9.16.4 all type-8 passwords are lost on first reboot
CSCwf12521	Unable to load intrusion policy page on FMC GUI
CSCwf12985	FTDv: Traffic failure in VMware Deployments due to dpdk pool exhuastion and rx_buff_alloc_failure
CSCwf14126	ASA Traceback and reload citing process name 'lina'
CSCwf14257	FTD container restored from backup fails to register to FMC due to Peer send bad hash error
CSCwf14735	traceback and reload in Process Name: lina related to Nat/Pat
CSCwf14811	TCP normalizer needs stats that show actions like packet drops
CSCwf15858	LDAP authentication over SSL not working for users that send large authorisation profiles
CSCwf15902	ASAv in Hyper-V drops packets on management interface
CSCwf16108	When enabling backup peer ip on FMC 7.3.1 with a space the VPN IPSec profile would be removed
CSCwf17406	Failure to remove snort stat files older than 70 days
CSCwf17814	ASA/FTD may traceback and reload in Thread Name '19', free block checksum failure
CSCwf19562	Changes to lamplighter logs written to /var/log/tid_process.log
CSCwf19853	FATAL errors in DBCheck due to missing columns in eventdb table

Bug ID	Headline
CSCwf20215	admin user should be excluded from CLI shell access filter
CSCwf20338	ASA may traceback and reload in Thread Name 'DHCPv6 Relay'
CSCwf20958	No logrotate and max size is configured for Health.log file
CSCwf21106	ASA/FTD: Traceback on thread name: snmp_master_callback_thread during SNMP and interface changes
CSCwf22005	ASA Packet-tracer displays the first ACL rule always, though matches the right ACL
CSCwf22568	FTD HA Creation fails resulting in devices showing up in an inconsistent state on the FMC
CSCwf22854	Not able to add files with file names which has '\u' to clean list from Malware Summary page
CSCwf23564	Unable to establish BGP when using MD5 authentication over GRE TUNNEL and FTD as passthrough device
CSCwf24124	SFDataCorrelator process crashing very frequently on the FMC.
CSCwf24773	crashhandler running with test mode snort
CSCwf25144	FMC backup management page showing "Verifying Backup" for FTD sensors.
CSCwf26264	FMC backup restore page takes around 5 mins to load when remote storage is unreachable
CSCwf26407	FP2130- Unable to disassociate member from port channel, deployment fails, member is lost on FTD/FMC
CSCwf26534	ASA/FTD: Connection information in SIP-SDP header remains untranslated with destination static Any
CSCwf26939	FTD may fail to create a NAT rule with error: "IPv4 dst real obj address range is huge"
CSCwf28488	Inconsistent log messages seen when emblem is configured and buffer logging is set to debug
CSCwf28592	In some specific scenarios, object optimizer can cause incorrect rules to be deployed to the device
CSCwf30716	ASA in multi context shows standby device in failed stated even after MIO HB recovery.
CSCwf30727	ASA integration with umbrella does not work without validation-usage ssl-server.
CSCwf31701	ASA traceback and reload with the Thread name: **CP Crypto Result Processing**
CSCwf31820	Firewall may drop packets when routing between global or user VRFs
CSCwf32890	Standby FMC SSH connection getting disconnected frequently.

Bug ID	Headline
CSCwf33574	ASA access-list entries have the same hash after upgrade
CSCwf33904	Virtual FDM Upgrade fails: HA configStatus='OUT_OF_SYNC after UpgradeOnStandby
CSCwf34152	FMC Fails to deploy or register new FTDs due to SFTunnel Establishment Failure.
CSCwf34450	Snort3 crash after the consequent snort restart if duplicate custom apps are present
CSCwf34500	FTD: GRE traffic is load balanced between CPU cores
CSCwf35173	SFTunnel Fails to Properly Establish due to running_config.conf file misconfiguration
CSCwf35207	ASA: Traceback and reload while updating ACLs on ASA
CSCwf35346	FMC should handle error appropriately when ISE reports error during SXP download
CSCwf37160	AnyConnect Ikev2 Login Failed With certificate-group-map Configured
CSCwf39968	FMC UI related issue in Object management page
CSCwf42144	ASA/FTD may traceback and reload citing process name "lina"
CSCwf43247	NMAP Remediation scan tasks remain in pending state in action queue table, does not clear out
CSCwf43288	Traceback in Thread Name: ssh/client in a clustered setup
CSCwf43391	Adding verify check for networks added under network object group in FMC
CSCwf44915	Old LSP packages are not pruned causing high disk utilization
CSCwf47487	CSM backup failed due to modification of CSM audit log file while tar was reading it
CSCwf48599	VPN load-balancing cluster encryption using deprecated ciphers
CSCwf49573	ASA/FTD: Traceback and reload when issuing 'show memory webvpn all objects'
CSCwf51824	FXOS SNMP "property community of sys/svc-ext/snmp-svc is out of range" is unclear to users
CSCwf51933	FTD username with dot fails AAA-RADIUS external authentication login after upgrade
CSCwf54418	Reduce time taken to clear stale IKEv2 SAs formed after Duplicate Detection
CSCwf56291	FMC config archives retention reverts to default if ca_purge tool was used prior to 7.2.4 upgrade
CSCwf57850	TelemetryApp process keeps exiting every minute after upgrading the FMC
CSCwf58876	KP2140-HA, reloaded primary unit not able to detect the peer unit

Bug ID	Headline
CSCwf59571	FTD/Lina - ZMQ issue OUT OF MEMORY. due to less Msglyr pool memory in low end platforms
CSCwf60311	ASA generating traceback with thread-name: DATAPATH-53-18309 after upgrade to 9.16.4.19
CSCwf60584	Health Monitoring to NOT collect route stats for transparent mode FTD
CSCwf62103	FMC needs to properly validate QoS policy rules before allowing deployment to FTD
CSCwf62885	FTDv Single-Arm Proxy behind AWS GWLB drops due to geneve-invalid-udp-checksum.
CSCwf66271	Unable to list down the interface under the device exclude policy
CSCwf71606	Cisco ASA and FTD ACLs Not Installed upon Reload
CSCwf71812	FTD Lina engine may traceback, due to assertion, in datapath
CSCwf72510	Avoid both the devices in HA sends events to FMC
CSCwf73189	FTD is dropping GRE traffic from WSA due to NAT failure
CSCwf76970	Include a warning during break HA when secondary unit is active
CSCwf77191	ASA appliance mode - 'connect fxos [admin]' will get ERROR: failed to open connection.
CSCwf78950	FMC 1600 process ssp_snmp_trap_fwdr high memory utilization
CSCwf81058	FTD: Firepower 3100 Dynamic Flow Offload showing as Enabled
CSCwf81320	Unable to configure and deploy IPv6 DNS server for RAVPN in FMC 7.2.4
CSCwf82247	Policy deployment fails when a route same prefix/metric is configured in a separate VRF.
CSCwf84588	Disable TLS 1.1 permanently for sftunnel communication
CSCwf85307	[Snort 3] IPS Policy Overrides not working on Chained Intrusion Policies
CSCwf86860	FMC GUI | ACP page gets blank and hang while doing search in rules and moving to last pages
CSCwf87761	Copy of Policy causes all devices to be marked as dirty
CSCwf88552	ASA/FTD: Traceback and reload due to NAT L7 inspection rewrite
CSCwf92182	Cisco Firepower Management Center Software SQL Injection Vulnerability
CSCwh12009	EOStore failed error is outputted after deleting shared rule layer.
CSCwh13551	Encrypted Visibility Engine (EVE) dashboard tab and widgets not added to FMC GUI upon upgrade

Bug ID	Headline
CSCwh14731	The authentication object names should not contain white spaces
CSCwh21337	FTD - Issue with the LSP package code during deploy rollback.
CSCwh28779	Unable to save intrusion policy after upgrade to 7.x as the name exceeds 40 characters
CSCwh30276	Rule update filter in Intrusion policy shows inconsistent results

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 37: 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
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 38: 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

Platform	Install Guide	Link
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 1000/2100 and Secure Firewall 3100/4200	Troubleshooting guide, in the *Reimage Procedures* chapter.	*Cisco FXOS Troubleshooting Guide for the Firewall 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-74-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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023–2026 Cisco Systems, Inc. All rights reserved.