Cisco Secure Firewall Threat Defense Release Notes, Version 7.2.x

First Published: 2022-06-06

Last Modified: 2024-10-22

Cisco Secure Firewall Threat Defense Release Notes

This document contains release information for:

- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center (on-prem)
- Cisco Secure Firewall device manager

For cloud deployments, see the Cisco Cloud-Delivered Firewall Management Center Release Notes or What's New for Cisco Defense Orchestrator.

Release Dates

Table 1: Version 7.2 Dates

Version	Build	Date	Platforms
7.2.9	44	2024-10-22	All
7.2.8.1	17	2024-08-26	All
7.2.8	25	2024-06-24	All
7.2.7	500	2024-04-29	All
7.2.6	168	2024-04-22	No longer available.
	167	2024-03-19	No longer available.
7.2.5.2	4	2024-05-06	All
7.2.5.1	29	2023-11-14	All
7.2.5	208	2023-07-27	All
7.2.4.1	43	2023-07-27	All
7.2.4	169	2023-05-10	Management center
	165	2023-05-03	Devices

Version	Build	Date	Platforms
7.2.3.1	13	2023-04-18	Management center
7.2.3	77	2023-02-27	All
7.2.2	54	2022-11-29	All
7.2.1	40	2022-10-03	All
7.2.0.1	12	2022-08-10	All
7.2.0	82	2022-06-06	All

Compatibility

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

For compatibility information, see:

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

Features

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

Note Patches are largely limited to urgent bug fixes: Bugs, on page 44. If a patch does include a feature or behavior change, it is described in the section for the "parent" 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. Having to enable a new setting or deploy a policy post-upgrade to take advantage of a new feature does not count as upgrade impact.

The feature descriptions below include upgrade impact where appropriate. For a more complete list of features with upgrade impact by version, see Upgrade Impact Features, on page 37.

Snort 3

Snort 3 is the default inspection engine for threat defense.

Snort 3 features for management center deployments also apply to device manager, even if they are not listed as new device manager features. However, keep in mind that the management center may offer more configurable options than device manager.

Important If you are still using the Snort 2 inspection engine, switch to Snort 3 now for improved detection and performance. Snort 2 will be deprecated in a future release and will eventually prevent threat defense upgrade.

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. 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 below include information on deprecated FlexConfigs when appropriate. For a full list of deprecated FlexConfigs, see your configuration guide.

Caution 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.

REST API

For information on what's new in the REST API, see the Secure Firewall Management Center REST API Quick Start Guide or the Cisco Secure Firewall Threat Defense REST API Guide.

Cisco Success Network Telemetry

Cisco Success Network sends usage information and statistics to Cisco, which are essential to provide you with technical support. For information on what's new with telemetry, see Cisco Success Network Telemetry Data Collected from Cisco Secure Firewall Management Center.

Language Preferences

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.

Management Center Features in Version 7.2.9

Table 2: Management Center Features in Version 7.2.9

Feature	Minimum FMC	Minimum FTD	Details
Administration			
Cisco Security Cloud regions: India and Australia.	7.2.9 7.6.0	7.2.9 7.6.0	Cisco Security Cloud integration now supports the India and Australia regional clouds. New/modified screens: • Version 7.6.0+ : **Integration** > **Cisco Security Cloud** > **Current Region** • Version 7.2.9–7.2.x: **Integration** > **SecureX** > **Current Region** Version restrictions: Not supported with Version 7.2.0–7.2.8, 7.3.x, or 7.4.0–7.4.2.

Management Center Features in Version 7.2.8

Table 3: Management Center Features in Version 7.2.8

Feature	Minimum Management Center	Minimum Threat Defense	Details
Platform			
Threat defense virtual for Megaport.	7.2.8	7.2.8	We introduced threat defense virtual for Megaport (Megaport Virtual Edge). High availability is supported; clustering is not. Version restrictions: Initially, you may not be able to freshly deploy Versions 7.3.x or 7.4.x. Instead, deploy Version 7.2.8–7.2.x and upgrade. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide

Management Center Features in Version 7.2.7

This release introduces stability, hardening, and performance enhancements. See Resolved Bugs in Version 7.2.7, on page 60.

Management Center Features in Version 7.2.6

Due to CSCwi63113, Version 7.2.6 was deferred on 2024-04-29 and is no longer available for download. If you downloaded it, do not use it. If you are running this version, upgrade. The features listed here are also available in Version 7.2.7.

Table 4: Management Center Features in Version 7.2.6

Feature	Minimum Management Center	Minimum Threat Defense	Details
Reintroduced Features			
Reintroduced features.	7.2.6	Feature dependent	Version 7.2.6 reintroduces the following features, enhancements, and critical fixes: • Updated web analytics provider. Upgrade impact.
Interfaces			
Configure DHCP relay trusted interfaces from the management center web interface.	7.2.6 7.4.1	Any	**Upgrade impact. Redo any related FlexConfigs after upgrade.** You can now use the management center web interface to configure interfaces as trusted interfaces to preserve DHCP Option 82. If you do this, these settings override any existing FlexConfigs, although you should remove them. DHCP Option 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. Normally, if the threat defense DHCP relay agent receives a DHCP packet with Option 82 already set, but the giaddr field (which specifies the DHCP relay agent address that is set by the relay agent before it forwards the packet to the server) is set to 0, then threat defense will drop that packet by default. You can preserve Option 82 and forward the packet by identifying an interface as a trusted interface. New/modified screens: **Devices** > **Device Management** > **Add/Edit Device** > **DHCP** > **DHCP Relay** Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. If you upgrade to an unsupported version, redo your FlexConfigs. See: Configure the DHCP Relay Agent
NAT			
Create network groups while editing NAT rules.	7.2.6 7.4.1	Any	You can now create network groups in addition to network objects while editing a NAT rule. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Customizing NAT Rules for Multiple Devices
High Availability/Scalability: Threat Defense			
Reduced "false failovers" for threat defense high availability.	7.2.6 7.4.0	7.2.6 7.4.0	Other version restrictions: Not supported with management center or threat defense Version 7.3.x. See: Heartbeat Module Redundancy
High Availability: Management Center			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Single backup file for high availability management centers.	7.2.6 7.4.1	Any	When performing a configuration-only backup of the active management center in a high availability pair, the system now creates a single backup file which you can use to restore either unit. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Unified Backup of Management Centers in High Availability
Event Logging and Analysis			
Open the packet tracer from the unified event viewer.	7.2.6 7.4.1	Any	You can now open the packet tracer from the unified event view (**Analysis** > **Unified Events**). Click the ellipsis icon (**...**) next to the desired event and click **Open in Packet Tracer**. Other version restrictions: In Version 7.2.x, use the Expand icon (>) icon instead of the ellipsis icon. Not supported with management center Version 7.3.x or 7.4.0. See: Working with the Unified Event Viewer
Health Monitoring			
Health alerts for excessive disk space used by deployment history (rollback) files.	7.2.6 7.4.1	Any	The Disk Usage health module now alerts if deployment history (rollback) files are using excessive disk space on theged management center. Deploy the management center health policy after upgrade. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Disk Usage for Device Configuration History Files Health Alert
Health alerts for NTP sync issues.	7.2.6 7.4.1	Any	A new Time Server Status health module reports issues with NTP synchronization. Deploy the management center health policy after upgrade. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Time Synchronization and Health Modules
Deployment and Policy Management			

Feature	Minimum Management Center	Minimum Threat Defense	Details
View and generate reports on configuration changes since your last deployment.	7.2.6 7.4.1	Any	You can generate, view, and download (as a zip file) the following reports on configuration changes since your last deployment: • A policy changes report for each device that previews the additions, changes, or deletions in the policy, or the objects that are to be deployed on the device. • A consolidated report that categorizes each device based on the status of policy changes report generation. This is especially useful after you upgrade either the management center or threat defense devices, so that you can see the changes made by the upgrade before you deploy. New/modified screens: **Deploy** > **Advanced Deploy**. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Download Policy Changes Report for Multiple Devices
Set the number of deployment history files to retain for device rollback.	7.2.6 7.4.1	Any	You can now set the number of deployment history files to retain for device rollback, up to ten (the default). This can help you save disk space on the management center. New/modified screens: **Deploy > Deployment History** ( ) **> Deployment Setting > Configuration Version Setting** Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Set the Number of Configuration Versions
Upgrade			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Improved upgrade starting page and package management.	7.2.6 7.4.1	Any	A new upgrade page makes it easier to choose, download, manage, and apply upgrades to your entire deployment. This includes the management center, threat defense devices, and any older NGIPSv/ASA FirePOWER devices. The page lists all upgrade packages that apply to your current deployment, with suggested releases specially marked. You can easily choose and direct-download packages from Cisco, as well as manually upload and delete packages. Internet access is required to retrieve the list/direct download upgrade packages. Otherwise, you are limited to manual management. Patches are not listed unless you have at least one appliance at the appropriate maintenance release (or you manually uploaded the patch). You must manually upload hotfixes. New/modified screens: • **System** (⚙) > **Product Upgrades** is now where you upgrade the management center and all managed devices, as well as manage upgrade packages. • **System** (⚙) > **Content Updates** is now where you update intrusion rules, the VDB, and the GeoDB. • **Devices** > **Threat Defense Upgrade** takes you directly to the threat defense upgrade wizard. • **System** (⚙) > **Users** > **User Role** > **Create User Role** > **Menu-Based Permissions** allows you to grant access to **Content Updates** (VDB, GeoDB, intrusion rules) without allowing access to **Product Upgrades** (system software). Deprecated screens/options: • **System** (⚙) > **Updates** is deprecated. All threat defense upgrades now use the wizard. • The **Add Upgrade Package** button on the threat defense upgrade wizard has been replaced by a **Manage Upgrade Packages** link to the new upgrade page. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center

Feature	Minimum Management Center	Minimum Threat Defense	Details
Enable revert from the threat defense upgrade wizard.	7.2.6 7.4.1	Any, if upgrading to 7.1+	You can now enable revert from the threat defense upgrade wizard. Other version restrictions: You must be upgrading threat defense to Version 7.1+. Not supported with management center Version 7.3.x or 7.4.0. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
Select devices to upgrade from the threat defense upgrade wizard.	7.2.6	Any	Use the wizard to select devices to upgrade. You can now use the threat defense upgrade wizard to select or refine the devices to upgrade. On the wizard, you can toggle the view between selected devices, remaining upgrade candidates, ineligible devices (with reasons why), devices that need the upgrade package, and so on. Previously, you could only use the Device Management page and the process was much less flexible. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
View detailed upgrade status from the threat defense upgrade wizard.	7.2.6 7.4.1	Any	The final page of the threat defense upgrade wizard now allows you to monitor upgrade progress. This is in addition to the existing monitoring capability on the Upgrade tab on the Device Management page, and on the Message Center. Note that as long as you have not started a new upgrade flow, **Devices** > **Threat Defense Upgrade** brings you back to this final wizard page, where you can view the detailed status for the current (or most recently complete) device upgrade. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
Unattended threat defense upgrades.	7.2.6	Any	The threat defense upgrade wizard now supports unattended upgrades, using a new **Unattended Mode** menu. You just need to select the target version and the devices you want to upgrade, specify a few upgrade options, and step away. You can even log out or close the browser. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
Simultaneous threat defense upgrade workflows by different users.	7.2.6	Any	We now allow simultaneous upgrade workflows by different users, as long as you are upgrading different devices. The system prevents you from upgrading devices already in someone else's workflow. Previously, only one upgrade workflow was allowed at a time across all users. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center

Feature	Minimum Management Center	Minimum Threat Defense	Details
Skip pre-upgrade troubleshoot generation for threat defense devices.	7.2.6	Any	You can now skip the automatic generating of troubleshooting files before major and maintenance upgrades by disabling the new **Generate troubleshooting files before upgrade begins** option. This saves time and disk space. To manually generate troubleshooting files for a threat defense device, choose **System** (⚙) > **Health** > **Monitor**, click the device in the left panel, then **View System & Troubleshoot Details**, then **Generate Troubleshooting Files**. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
Suggested release notifications.	7.2.6 7.4.1	Any	The management center now notifies you when a new suggested release is available. If you don't want to upgrade right now, you can have the system remind you later, or defer reminders until the next suggested release. The new upgrade page also indicates suggested releases. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Cisco Secure Firewall Management Center New Features by Release
New upgrade wizard for the management center.	7.2.6 7.4.1	Any	A new upgrade starting page and wizard make it easier to perform management center upgrades. After you use **System** (⚙) > **Product Upgrades** to get the appropriate upgrade package onto the management center, click **Upgrade** to begin. Other version restrictions: Only supported for management center upgrades from Version 7.2.6+/7.4.1+. Not supported for upgrades from Version 7.3.x or 7.4.0. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
Hotfix high availability management centers without pausing synchronization.	7.2.6 7.4.1	Any	Unless otherwise indicated by the hotfix release notes or Cisco TAC, you do not have to pause synchronization to install a hotfix on high availability management centers. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
Administration			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Updated internet access requirements for direct-downloading software upgrades.	7.2.6 7.4.1	Any	**Upgrade impact. The system connects to new resources.** The management center has changed its direct-download location for software upgrade packages from sourcefire.com to amazonaws.com. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See:Internet Access Requirements
Scheduled tasks download patches and VDB updates only.	7.2.6 7.4.1	Any	**Upgrade impact. Scheduled download tasks stop retrieving maintenance releases.** The **Download Latest Update** scheduled task no longer downloads maintenance releases; now it only downloads the latest applicable patches and VDB updates. To direct-download maintenance (and major) releases to the management center, use **System** (⚙) > **Product Upgrades**. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Software Update Automation
Usability, Performance, and Troubleshooting			
Enable/disable access control object optimization.	7.2.6 7.4.1	Any	You can now enable and disable access control object optimization from the management center web interface. New/modified screens: **System** (⚙) > **Configuration** > **Access Control Preferences** > **Object Optimization** Other version restrictions: Access control object optimization is automatically enabled on all management centers upgraded or reimaged to Versions 7.2.4–7.2.5 and 7.4.0, and automatically disabled on all management centers upgraded or reimaged to Version 7.3.x. It is configurable and enabled by default for management centers reimaged to Version 7.2.6+/7.4.1+, but respects your current setting when you upgrade to those releases. See: Access Control Preferences and.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cluster control link ping tool.	7.2.6 7.4.1	Any	You can check to make sure all the cluster nodes can reach each other over the cluster control link by performing a ping. One major cause for the failure of a node to join the cluster is an incorrect cluster control link configuration; for example, the cluster control link MTU may be set higher than the connecting switch MTUs. New/modified screens: **Devices** > **Device Management** > **More** (⋮) > **Cluster Live Status** Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Perform a Ping on the Cluster Control Link
Snort 3 restarts when it uses too much memory, which can trigger HA failover.	7.2.6 7.4.1	7.2.6 with Snort 3 7.4.1 with Snort 3	To improve continuity of operations, excessive memory use by Snort can now trigger high availability failover. This happens because Snort 3 now restarts if the process uses too much memory. 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 memory threshold. Platform restrictions: Not supported with clustered devices. New/modified CLI commands: **configure snort3 memory-monitor**, **show snort3 memory-monitor-status** Other version restrictions: Not supported with management center or threat defense Version 7.3.x or 7.4.0. See: Cisco Secure Firewall Threat Defense Command Reference
Set the frequency of Snort 3 core dumps.	7.2.6 7.4.1	7.2.6 with Snort 3 7.4.1 with Snort 3	You can now set the frequency of Snort 3 core dumps. Instead of generating a core dump every time Snort crashes, you can generate one the next time Snort crashes only. Or, generate one if a crash has not occurred in the last day, or week. Snort 3 core dumps are disabled by default for standalone devices. For high availability and clustered devices, the default frequency is now once per day instead of every time. New/modified CLI commands: **configure coredump snort3**, **show coredump** Other version restrictions: Not supported with management center or threat defense Version 7.3.x or 7.4.0. See: Cisco Secure Firewall Threat Defense Command Reference

Feature	Minimum Management Center	Minimum Threat Defense	Details
Capture dropped packets with the Secure Firewall 3100/4200.	7.2.6 7.4.1	7.2.6 (no 4200) 7.4.1	Packet losses resulting from MAC address table inconsistencies can impact your debugging capabilities. The Secure Firewall 3100/4200 can now capture these dropped packets. New/modified CLI commands: [**drop** { **disable** | **mac-filter** }] in the **capture** command. Other version restrictions: Not supported with management center or threat defense Version 7.3.x or 7.4.0. See: Cisco Secure Firewall Threat Defense Command Reference
Deprecated Features			
Deprecated: DHCP relay trusted interfaces with FlexConfig.	7.2.6 7.4.1	Any	**Upgrade impact. Redo any related FlexConfigs after upgrade.** You can now use the management center web interface to configure interfaces as trusted interfaces to preserve DHCP Option 82. If you do this, these settings override any existing FlexConfigs, although you should remove them. Other version restrictions: This feature is not supported with management center Version 7.3.x or 7.4.0. If you upgrade to an unsupported version, also redo your FlexConfigs. See: Configure the DHCP Relay Agent

Management Center Features in Version 7.2.5

Table 5: Management Center Features in Version 7.2.5

Feature	Minimum Management Center	Minimum Threat Defense	Details
Interfaces			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Management center detects interface sync errors.	7.2.5 7.4.1	Any	**Upgrade impact. You may need to sync interfaces after upgrade.** In some cases, the management center can be missing a configuration for an interface even though the interface is correctly configured and functioning on the device. If this happens, and your management center is running: • Version 7.2.5: Deploy is blocked until you edit the device and sync from the Interfaces page • Version 7.2.6+/7.4.1+: Deploy is allowed with a warning, but you cannot edit interface settings without syncing first. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. The management center will neither block deploy nor warn you of missing configurations. You can still sync interfaces manually if you think you are having an issue. See: Sync Interface Changes with the Management Center

Management Center Features in Version 7.2.4

Table 6: Management Center Features in Version 7.2.4

Feature	Minimum Management Center	Minimum Threat Defense	Details
Default Forward Error Correction (FEC) on Secure Firewall 3100 fixed ports changed to Clause 108 RS-FEC from Clause 74 FC-FEC for 25 GB+ SR, CSR, and LR transceivers.	7.2.4	Any	When you set the FEC to Auto on the Secure Firewall 3100 fixed ports, the default type is now set to Clause 108 RS-FEC instead of Clause 74 FC-FEC for 25 GB+ SR, CSR, and LR transceivers. See: Interface Overview.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Automatically update CA bundles.	7.0.5 7.1.0.3 7.2.4	7.0.5 7.1.0.3 7.2.4	**Upgrade impact. The system connects to Cisco for something new.** The local CA bundle contains certificates to access several Cisco services. The system now automatically queries Cisco for new CA certificates at a daily system-defined time. Previously, you had to upgrade the software to update CA certificates. You can use the CLI to disable this feature. New/modified CLI commands: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** Version restrictions: This feature is included in Versions 7.0.5+, 7.1.0.3+, and 7.2.4+. It is not supported in earlier 7.0, 7.1, or 7.2 releases. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco. See: Firepower Management Center Command Line Reference and Cisco Secure Firewall Threat Defense Command Reference
Access control performance improvements (object optimization).	7.2.4	Any	**Upgrade impact. First deployment after management center upgrade to 7.2.4–7.2.5 or 7.4.0 can take a long time and increase CPU use on managed devices.** Access control object optimization improves performance and consumes fewer device resources when you have access control rules with overlapping networks. The optimizations occur on the *managed device* on the first deploy after the feature is enabled on the management center (including if it is enabled by an upgrade). If you have a high number of rules, the system can take several minutes to an hour to evaluate your policies and perform object optimization. During this time, you may also see higher CPU use on your devices. A similar thing occurs on the first deploy after the feature is disabled (including if it is disabled by upgrade). After this feature is enabled or disabled, we recommend you deploy when it will have the least impact, such as a maintenance window or a low-traffic time. New/modified screens (requires Version 7.2.6): **System** (⚙) > **Configuration** > **Access Control Preferences** > **Object-group optimization**. Other version restrictions: Not supported with management center Version 7.3.x. See: Access Control Preferences

Feature	Minimum Management Center	Minimum Threat Defense	Details
Smaller VDB for lower memory Snort 2 devices.	6.4.0.17 7.0.6 7.2.4 7.3.1.1 7.4.0	Any with Snort 2	**Upgrade impact. Application identification on lower memory devices is affected.** For VDB 363+, the system now installs a smaller VDB (also called *VDB lite*) on lower memory devices running Snort 2. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Lower memory devices: ASA 5506-X series, ASA-5508-X, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X Version restrictions: The ability to install a smaller VDB depends on the version of the management center, not managed devices. If you upgrade the management center from a supported version to an unsupported version, you cannot install VDB 363+ if your deployment includes even one lower memory device. For a list of affected releases, see CSCwd88641. See: Update the Vulnerability Database

Management Center Features in Version 7.2.3

Table 7: Management Center Features in Version 7.2.3

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firepower 1010E.	7.2.3.1 7.3.1.1	7.2.3	We introduced the Firepower 1010E, which does not support power over Ethernet (PoE). Do not use a Version 7.2.3 or Version 7.3.0 management center to manage the Firepower 1010E. Instead, use a Version 7.2.3.1+ or Version 7.3.1.1+ management center. Version restrictions: These devices do not support Version 7.3.x or 7.4.0. Support returns in Version 7.4.1. See: Regular Firewall Interfaces

Management Center Features in Version 7.2.2

This release introduces stability, hardening, and performance enhancements. See Resolved Bugs in Version 7.2.2, on page 125.

Management Center Features in Version 7.2.1

Table 8: Management Center Features in Version 7.2.1

Feature	Minimum Management Center	Minimum Threat Defense	Details
Hardware bypass ("fail-to-wire") network modules for the Secure Firewall 3100.	7.2.1	7.2.1	We introduced these hardware bypass network modules for the Secure Firewall 3100: • 6-port 1G SFP Hardware Bypass Network Module, SX (multimode) (FPR-X-NM-6X1SX-F) • 6-port 10G SFP Hardware Bypass Network Module, SR (multimode) (FPR-X-NM-6X10SR-F) • 6-port 10G SFP Hardware Bypass Network Module, LR (single mode) (FPR-X-NM-6X10LR-F) • 6-port 25G SFP Hardware Bypass Network Module, SR (multimode) (FPR-X-NM-X25SR-F) • 6-port 25G Hardware Bypass Network Module, LR (single mode) (FPR-X-NM-6X25LR-F) • 8-port 1G Copper Hardware Bypass Network Module, RJ45 (copper) (FPR-X-NM-8X1G-F) New/modified screens: **Devices > Device Management > Interfaces > Edit Physical Interface** For more information, see Inline Sets and Passive Interfaces.
Intel Ethernet Network Adapter E810-CQDA2 driver with threat defense virtual for KVM.	7.2.1	7.2.1	We now support the Intel Ethernet Network Adapter E810-CQDA2 driver with threat defense virtual for KVM. For more information, see Getting Started with Secure Firewall Threat Defense Virtual and KVM.

Management Center Features in Version 7.2.0

Table 9: Management Center Features in Version 7.2.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Platform			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Snapshots allow quick deploy of threat defense virtual for AWS and Azure.	7.2.0	7.2.0	You can now take a snapshot of a threat defense virtual for AWS or Azure instance, then use that snapshot to quickly deploy new instances. This feature also improves the performance of the autoscale solutions for AWS and Azure. For more information, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.
Analytics mode for cloud-managed threat defense devices.	7.2.0	7.0.3 7.2.0	Concurrently with Version 7.2, we introduced the cloud-delivered Firewall Management Center, which uses the Cisco Defense Orchestrator platform and unites management across multiple Cisco security solutions. We take care of feature updates. On-prem hardware and virtual management centers running Version 7.2+ can "co-manage" cloud-managed threat defense devices, but for event logging and analytics purposes only. You cannot deploy policy to these devices from an on-prem management center. New/modified screens: • When you add a cloud-managed device to an on-prem management center, use the new **CDO Managed Device** check box to specify that it is analytics-only. • View which devices are analytics-only on **Devices > Device Management**. New/modified CLI commands: **configure manager add**, **configure manager delete**, **configure manager edit**, **show managers** Version restrictions: Not supported with threat defense Version 7.1. For more information, see Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator.
ISA 3000 support for shutting down.	7.2.0	7.2.0	Support returns for shutting down the ISA 3000. This feature was introduced in Version 7.0.2 but was temporarily deprecated in Version 7.1.
High Availability/Scalability: Threat Defense			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Clustering for threat defense virtual in both public and private clouds.	7.2.0	7.2.0	You can now configure clustering for the following threat defense virtual platforms: • Threat defense virtual for AWS: 16-node clusters • Threat defense virtual for GCP: 16-node clusters • Threat defense virtual for KVM: 4-node clusters • Threat defense virtual for VMware: 4-node clusters New/modified screens: • **Devices > Device Management > Add Cluster** • **Devices > Device Management > More** menu • **Devices > Device Management > Cluster** For more information, see Clustering for Threat Defense Virtual in a Public Cloud (AWS, GCP) or Clustering for Threat Defense Virtual in a Private Cloud (KVM, VMware).
16-node clusters for the Firepower 4100/9300, and for threat defense virtual for AWS and GCP.	7.2.0	7.2.0	You can now configure 16-node clusters for the Firepower 4100/9300, and for threat defense virtual for AWS and GCP. Note that the Secure Firewall 3100 still only supports 8 nodes. For more information, see Clustering for the Firepower 4100/9300 or Clustering for Threat Defense Virtual in a Public Cloud.
Autoscale for threat defense virtual for AWS gateway load balancers.	7.2.0	7.2.0	We now support autoscale for threat defense virtual for AWS gateway load balancers, using a CloudFormation template. For more information, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.
Autoscale for threat defense virtual for GCP.	7.2.0	7.2.0	**Upgrade impact. Threat defense virtual for GCP cannot upgrade across Version 7.2.0.** We now support autoscale for threat defense virtual for GCP, by positioning a threat defense virtual instance group between a GCP internal load balancer (ILB) and a GCP external load balancer (ELB). Version restrictions: Due to interface changes required to support this feature, threat defense virtual for GCP upgrades cannot cross Version 7.2.0. That is, you cannot upgrade to Version 7.2.0+ from Version 7.1.x and earlier. You must deploy a new instance and redo any device-specific configurations. For more information, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.
Interfaces			

Feature	Minimum Management Center	Minimum Threat Defense	Details
LLDP support for the Firepower 2100 and Secure Firewall 3100.	7.2.0	7.2.0	You can now enable Link Layer Discovery Protocol (LLDP) for Firepower 2100 and Secure Firewall 3100 series interfaces. New/modified screens: **Devices** > **Device Management** > **Interfaces** > > **Hardware Configuration** > **LLDP** New/modified commands: **show lldp status**, **show lldp neighbors**, **show lldp statistics** For more information, see Interface Overview.
Pause frames for flow control for the Secure Firewall 3100.	7.2.0	7.2.0	If you have a traffic burst, dropped packets can occur if the burst exceeds the buffering capacity of the FIFO buffer on the NIC and the receive ring buffers. Enabling pause frames for flow control can alleviate this issue. New/modified screens: **Devices > Device Management > Interfaces > Hardware Configuration > Network Connectivity** For more information, see Interface Overview.
Breakout ports for the Secure Firewall 3130 and 3140.	7.2.0	7.2.0	You can now configure four 10 GB breakout ports for each 40 GB interface on the Secure Firewall 3130 and 3140. New/modified screens: **Devices > Device Management > Chassis Operations** For more information, see Interface Overview.
Configure VXLAN from the management center web interface.	7.2.0	Any	**Upgrade impact. Redo FlexConfigs after upgrade.** You can now use the management center web interface to configure VXLAN interfaces. VXLANs act as Layer 2 virtual network over a Layer 3 physical network to stretch the Layer 2 network. If you configured VXLAN interfaces with FlexConfig in a previous version, they continue to work. In fact, FlexConfig takes precedence in this case—if you redo your VXLAN configurations in the web interface, remove the FlexConfig settings. New/modified screens: • Configure the VTEP source interface: **Devices** > **Device Management** > **VTEP** • Configure the VNI interface: **Devices** > **Device Management** > **Interfaces** > **Add VNI Interface** For more information, see Regular Firewall Interfaces.
NAT			
Enable, disable, or delete more than one NAT rule at a time.	7.2.0	Any	You can select multiple NAT rules and enable, disable, or delete them all at the same time. Enable and disable apply to manual NAT rules only, whereas delete applies to any NAT rule. For more information, see Network Address Translation.

Feature	Minimum Management Center	Minimum Threat Defense	Details
VPN			
Certificate and SAML authentication for RA VPN connection profiles.	7.2.0	7.2.0	We now support certificate and SAML authentication for RA VPN connection profiles. You can authenticate a machine certificate or user certificate before a SAML authentication/authorization is initiated. This can be done using DAP certificate attributes along with user specific SAML DAP attributes. New/modified screens: You can now choose **Certificate & SAML** option when choosing the authentication method for the connection profile in an RA VPN policy. For more information, see Remote Access VPN.
Route-based site-to-site VPN with hub and spoke topology.	7.2.0	7.2.0	We added support for route-based site-to-site VPNs in a hub and spoke topology. Previously, that topology only supported policy-based (crypto map) VPNs. New/modified screens: When you add a new VPN topology and choose **Route Based (VTI)**, you can now also choose **Hub and Spoke**. For more information, see Site-to-Site VPNs.
IPsec flow offload for the Secure Firewall 3100.	7.2.0	7.2.0	On the Secure Firewall 3100, IPsec flows are offloaded by default. After the initial setup of an IPsec site-to-site VPN or remote access VPN security association (SA), IPsec connections are offloaded to the field-programmable gate array (FPGA) in the device, which should improve device performance. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command. For more information, see Site-to-Site VPNs.
Routing			
Configure EIGRP from the management center web interface.	7.2.0	Any	**Upgrade impact. Redo FlexConfigs after upgrade.** You can now use the management center web interface to configure EIGRP. Note that you can only enable EIGRP on interfaces belonging to the device's Global virtual router. If you configured EIGRP with FlexConfig in a previous version, the system allows you to deploy post-upgrade, but also warns you to redo your EIGRP configurations in the web interface. When you are satisfied with the new configuration, you can delete the deprecated FlexConfig objects or commands. To help you with this process, we provide a command-line migration tool. New/modified screens: **Devices** > **Device Management** > **Routing** > **EIGRP** For more information, see EIGRP and Migrating FlexConfig Policies.
Virtual router support for the Firepower 1010.	7.2.0	7.2.0	You can now configure up to five virtual routers on the Firepower 1010. For more information, see Virtual Routers.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Support for VTIs in user-defined virtual routers.	7.2.0	7.2.0	You can now assign virtual tunnel interfaces to user-defined virtual routers. Previously, you could only assign VTIs to Global virtual routers. New/modified screens: **Devices** > **Device Management** > **Routing** > **Virtual Router Properties** For more information, see Virtual Routers.
Policy-based routing with path monitoring.	7.2.0	7.2.0	You can now use path monitoring to collect the performance metrics (RTT, jitter, packet-lost, and MOS) of a device's egress interfaces. Then, you can use these metrics to determine the best path for policy based routing. New/modified screens: • Enable path monitoring and choose metrics to collect: **Devices** > **Device Management** > **Interfaces** > **Path Monitoring** • Use the new **Interface Ordering** option when you are adding a policy based route and specifying a forwarding action: **Devices** > **Device Management** > **Routing** > **Policy Based Routing** • Monitor path metrics in each device's health monitoring dashboard: **System** (⚙) > **Health** > **Monitor** > add dashboard > **Interface - Path Metrics**. New/modified CLI commands: **show policy route**, **show path-monitoring**, **clear path-monitoring** For more information, see Policy Based Routing.
Threat Intelligence			
DNS-based threat intelligence from Cisco Umbrella.	7.2.0	Any	We now support DNS-based Security Intelligence using regularly updated information from Cisco Umbrella. You can use both a local DNS policy and an Umbrella DNS policy, for two layers of protection. New/modified screens: • Configure connection to Umbrella: **Integration** > **Other Integrations** > **Cloud Services** > **Cisco Umbrella Connection** • Configure Umbrella DNS policy: **Policies** > **DNS** > **Add DNS Policy** > **Umbrella DNA Policy** • Associate Umbrella DNS policy with access control: **Policies** > **Access Control** > **Edit Policy** > **Security Intelligence** > **Umbrella DNS Policy** For more information, see DNS Policies.

Feature	Minimum Management Center	Minimum Threat Defense	Details
IP-based threat intelligence from Amazon GuardDuty.	7.2.0	Any	You can now handle traffic based on malicious IP addresses detected by Amazon GuardDuty, when integrated with management center virtual for AWS. The system consumes this threat intelligence via a custom Security Intelligence feed, or via a regularly updated network object group, which you can then use in your security policies. For more information, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.
Access Control: Threat Detection and Application Identification			
Dynamic object management with: • Cloud-delivered Cisco Secure Dynamic Attributes Connector • On-prem Cisco Secure Dynamic Attributes Connector 2.0	7.2.0	Any	Concurrently with Version 7.2, we released the following updates to the Cisco Secure Dynamic Attributes Connector: • Cloud-delivered Cisco Secure Dynamic Attributes Connector (CDO-managed service) Supported management centers: Version 7.1+ and the cloud-delivered management center. Supported virtual/cloud workloads: AWS, Azure, Azure service tags, Google Cloud Connector, GitHub, and Office 365. For more information: *Managing the Cisco Secure Dynamic Attributes Connector with Cisco Defense Orchestrator* chapters in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator. • On-prem Cisco Secure Dynamic Attributes Connector 2.0 Supported management centers: Version 7.0+ and the cloud-delivered management center. Supported virtual/cloud workloads: AWS, Azure, Azure service tags, Google Cloud Connector, GitHub, Office 365, and VMware. For more information: Cisco Secure Dynamic Attributes Connector Configuration Guide 2.0.
Bypass inspection or throttle elephant flows on Snort 3 devices.	7.2.0	7.2.0 with Snort 3	You can now detect and optionally bypass inspection or throttle elephant flows. By default, access control policies are set to generate an event when the system sees an unencrypted connection larger than 1 GB/10 sec; the rate limit is configurable. For the Firepower 2100 series, you can detect elephant flows but not bypass inspection or throttle. For devices running Snort 2 and for devices running Version 7.1 and earlier, continue to use Intelligent Application Bypass (IAB). New/modified screens: We added **Elephant Flow Settings** to the access control policy's Advanced tab. For more information, see Elephant Flow Detection.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Encrypted visibility engine enhancements.	7.2.0	7.2.0 with Snort 3	We made the following enhancements to the encrypted visibility engine (EVE): • EVE can detect the operating system used by the host, which is reported in events and the network map. • EVE can detect application traffic by assigning EVE processes that were identified with high confidence to applications, which you can then use in access control rules to control network traffic. (In Version 7.1, you could see EVE processes for connections, but you could not act on that knowledge.) To add additional assignments, create custom applications/custom application detectors. When adding a detection pattern to your custom detector, choose **Encrypted Visibility Engine** as the application. Then, specify the process name and confidence level. • EVE now works with QUIC traffic. The following connection event fields have changed along with these enhancements: TLS Fingerprint Process Name is now Encrypted Visibility Process Name TLS Fingerprint Process Confidence Score is now Encrypted Visibility Process Confidence Score TLS Fingerprint Malware Confidence is now Encrypted Visibility Threat Confidence TLS Fingerprint Malware Confidence Score is now Encrypted Visibility Threat Confidence Score Detection Type: TLS Fingerprint is now Detection Type: Encrypted Visibility This feature now requires a Threat license. For more information, see Access Control Policies and Application Detection.
TLS 1.3 inspection.	7.2.0	7.2.0 with Snort 3	We now support inspection of TLS 1.3 traffic. New/modified screens: We added the **Enable TLS 1.3 Decryption** option to the Advanced Settings tab in SSL policies. Note that this option is disabled by default. For more information, see SSL Policies.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Improved portscan detection.	7.2.0	7.2.0 with Snort 3	With an improved portscan detector, you can easily configure the system to detect or prevent portscans. You can refine the networks you want to protect, set the sensitivity, and so on. For devices running Snort 2 and for devices running Version 7.1 and earlier, continue to use the network analysis policy for portscan detection. New/modified screens: We added **Threat Detection** to the access control policy's Advanced tab. For more information, see Threat Detection.
VBA macro inspection.	7.2.0	7.2.0 with Snort 3	We now support inspection of VBA (Visual Basic for Applications) macros in Microsoft Office documents, which is done by decompressing the macros and matching rules against the decompressed content. By default, VBA macro decompression is disabled in all system-provided network analysis policies. To enable it use the decompress_vba setting in the imap, smtp, http_inspect, and pop Snort 3 inspectors. To configure custom intrusion rules to match against decompressed macros, use the vba_data option. For more information, see the Snort 3 Inspector Reference and the Cisco Secure Firewall Management Center Snort 3 Configuration Guide.
Improved JavaScript inspection.	7.2.0	7.2.0 with Snort 3	We improved JavaScript inspection, which is done by normalizing the JavaScript and matching rules against the normalized content. A new normalizer's enhancements include improved white-space normalization, semicolon insertions, cross-site script handling, identifier normalization and dealiasing, just-in-time (JIT) inspection, and the ability to inspect external scripts. By default, the new normalizer is enabled in all system-provided network analysis policies. To tweak performance or disable the feature in a custom network analysis policy, use the js_norm (improved normalizer) and normalize_javascript (legacy normalizer) settings in the https_inspect Snort 3 inspector. To configure custom intrusion rules to match against normalized JavaScript, use the js_data option, for example: `alert tcp any any -> any any (msg:"Script detected!"; js_data; content:"var var_0000=1;"; sid:1000001;)` For more information, see HTTP Inspect Inspector in the Snort 3 Inspector Reference, as well as the Cisco Secure Firewall Management Center Snort 3 Configuration Guide.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Improved SMB 3 inspection.	7.2.0	7.2.0 with Snort 3	We now support inspection of SMB 3 traffic in the following situations: • During file server node failover for clusters configured for SMB Transparent Failover. • In multiple file server nodes for clusters using SMB Scale-Out. • Through directory information changes due to SMB Directory Leasing. • Spread across multiple connections due to SMB Multichannel. For more information, see the Snort 3 Inspector Reference and the Cisco Secure Firewall Management Center Snort 3 Configuration Guide.
Event Logging and Analysis			
Improved SecureX integration, SecureX orchestration.	7.2.0	Any	We have streamlined the SecureX integration process. Now, as long as you already have a SecureX account, you just choose your cloud region on the new **Integration > SecureX** page, click **Enable SecureX**, and authenticate to SecureX. The option to send events to the cloud, as well as to enable Cisco Success Network and Cisco Support Diagnostics, are also moved to this new page. When you enable SecureX integration on this new page, licensing and management for the system's cloud connection switches from Cisco Smart Licensing to SecureX. If you already enabled SecureX the "old" way, you must disable and re-enable to get the benefits of this cloud connection management. Note that this page also governs the cloud region for and event types sent to the Secure Network Analytics (Stealthwatch) cloud using Security Analytics and Logging (SaaS), even though the web interface does not indicate this. Previously, these options were on **System** (⚙) **> Integration > Cloud Services**. Enabling SecureX does not affect communications with the Secure Network Analytics cloud; you can send events to both. The management center also now supports SecureX orchestration—a powerful drag-and-drop interface you can use to automate workflows across security tools. After you enable SecureX, you can enable orchestration. As part of this feature, you can no longer use the REST API to configure SecureX integration. You must use the FMC web interface. Version restrictions: This feature is included in Versions 7.0.2+ and 7.2+. It is not supported in Version 7.1. If you use the new method to enable SecureX integration in Version 7.0.x, you cannot upgrade to Version 7.1 unless you disable the feature. We recommend you upgrade to Version 7.2+. See: Cisco Secure Firewall Management Center (7.0.2 and 7.2) and SecureX Integration Guide

Feature	Minimum Management Center	Minimum Threat Defense	Details
Log security events to multiple Secure Network Analytics on-prem data stores.	7.2.0	7.0.0	When you configure a Secure Network Analytics Data Store (multi-node) integration, you can now add multiple flow collectors for security events. You assign each flow collector to one or more threat defense devices running Version 7.0+. New/modified screens: • Setup: **Integration** > **Security Analytics & Logging** > **Secure Network Analytics Data Store** • Modify: **Integration** > **Security Analytics & Logging** > **Update Device Assignments** This feature requires Secure Network Analytics Version 7.1.4. For more information, see the Cisco Security Analytics and Logging (On Premises): Firewall Event Integration Guide.
Database access changes.	7.2.0	Any	We added ten new tables, deprecated one table, and prohibited joins in six tables. We also added fields to various tables for Snort 3 support and to provide timestamps and IP addresses in human-readable format. For more information, see the *What's New* topic in the Cisco Secure Firewall Management Center Database Access Guide, Version 7.2.
eStreamer changes.	7.2.0	Any	A new Python-based reference client has been added to the SDK. Also, you can now request fully qualified events. For more information, see the *What's New* topic in the Cisco Secure Firewall Management Center Event Streamer Integration Guide, Version 7.2.
Deployment and Policy Management			
Auto rollback of a deployment that causes a loss of management connectivity.	7.2.0	7.2.0	You can now enable auto rollback of the configuration if a deployment causes the management connection between the management center and threat defense to go down. Previously, you could only manually roll back a configuration using the **configure policy rollback** command. New/modified screens: • **Devices > Device Management > Device > Deployment Settings** • **Deploy > Advanced Deploy > Preview** • **Deploy > Deployment History > Preview** For more information, see Device Management.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Generate and email a report when you deploy configuration changes.	7.2.0	Any	You can now generate a report for any deploy task. The report contains details about the deployed configuration. New/modified pages: **Deploy** > **Deployment History** ( ) **icon** > **More** ( )**Generate Report** For more information, see Configuration Deployment.
Access control policy locking.	7.2.0	Any	You can now lock an access control policy to prevent other administrators from editing it. Locking the policy ensures that your changes will not be invalidated if another administrator edits the policy and saves changes before you save your changes. Any user who has permission to modify the access control policy has permission to lock it. We added an icon to lock or unlock a policy next to the policy name while editing the policy. In addition, there is a new permission to allow users to unlock policies locked by other administrators: Override Access Control Policy Lock. This permission is enabled by default in the Administrator, Access Admin, and Network Admin roles. For more information, see Access Control Policies.
Object group search is enabled by default.	7.2.0	Any	The **Object Group Search** setting is now enabled by default when you add a device to the management center. New/modified screens: **Devices** > **Device Management** > **Device** > **Advanced Settings** For more information, see Device Management.
Access control rule hit counts persist over reboot.	7.2.0	7.2.0	Rebooting a managed device no longer resets access control rule hit counts to zero. Hit counts are reset only if you actively clear the counters. In addition, counts are maintained by each unit in an HA pair or cluster separately. You can use the **show rule hits** command to see cumulative counters across the HA pair or cluster, or see the counts per node. New/modified CLI commands: **show rule hits** For more information, see the Cisco Secure Firewall Threat Defense Command Reference.

Feature	Minimum Management Center	Minimum Threat Defense	Details
New user interface for the access control policy.	7.2.0	Any	There is a new experimental user interface available for the access control policy. You can continue to use the legacy user interface, or you can try out the new user interface. The new interface has both a table and a grid view for the rules list, the ability to show or hide columns, enhanced search, infinite scroll, a clearer view of the packet flow related to policies associated with the access control policy, and a simplified add/edit dialog box for creating rules. You can freely switch back and forth between the legacy and new user interfaces while editing an access control policy. **Note** The new interface does not have all the features available in the legacy interface, and may have performance issues when displaying a large number of rules. If you experience issues with the new UI, switch back to the legacy UI. Additionally, Cisco TAC welcomes your feedback. If your organization allows it, you can help us improve this feature by making sure web analytics is enabled: **System** (⚙) > **Configuration** > **Web Analytics**. For more information, see Access Control Policies.
Upgrade			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Copy upgrade packages ("peer-to-peer sync") from device to device.	7.2.0	7.2.0	Instead of copying upgrade packages to each device from the management center or internal web server, you can use the threat defense CLI to copy upgrade packages between devices ("peer to peer sync"). This secure and reliable resource-sharing goes over the management network but does not rely on the management center. Each device can accommodate 5 package concurrent transfers. This feature is supported for Version 7.2.x–7.4.x standalone devices managed by the same Version 7.2.x–7.4.x standalone management center. It is not supported for: • Container instances. • Device high availability pairs and clusters. These devices get the package from each other as part of their normal sync process. Copying the upgrade package to one group member automatically syncs it to all group members. • Devices managed by high availability management centers. • Devices managed by the cloud-delivered Firewall Management Center, but added to an on-prem management center in analytics mode. • Devices in different domains, or devices separated by a NAT gateway. • Devices upgrading from Version 7.1 or earlier, regardless of management center version. • Devices running Version 7.6+. New/modified CLI commands: **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status**
Auto-upgrade to Snort 3 after successful threat defense upgrade.	7.2.0	7.2.0	When you use a Version 7.2+ management center to upgrade threat defense to Version 7.2+, you can now choose whether to **Upgrade Snort 2 to Snort 3**. After the software upgrade, eligible devices upgrade from Snort 2 to Snort 3 when you deploy configurations. For devices that are ineligible because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For help, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version. Version restrictions: Not supported for threat defense upgrades to Version 7.0.x or 7.1.x.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Upgrade for single-node clusters.	7.2.0	Any	You can now use the device upgrade page (**Devices** > **Device Upgrade**) to upgrade clusters with only one active node. Any deactivated nodes are also upgraded. Previously, this type of upgrade would fail. This feature is not supported from the system updates page (**System** (⚙)**Updates**). Hitless upgrades are also not supported in this case. Interruptions to traffic flow and inspection depend on the interface configurations of the lone active unit, just as with standalone devices. Supported platforms: Firepower 4100/9300, Secure Firewall 3100
Revert threat defense upgrades from the CLI.	7.2.0	7.2.0	You can now revert threat defense upgrades from the device CLI if communications between the management center and device are disrupted. Note that in high availability/scalability deployments, revert is more successful when all units are reverted simultaneously. When reverting with the CLI, open sessions with all units, verify that revert is possible on each, then start the processes at the same time. **Caution** Reverting from the CLI can cause configurations between the device and the management center to go out of sync, depending on what you changed post-upgrade. This can cause further communication and deployment issues. New/modified CLI commands: **upgrade revert**, **show upgrade revert-info**. For more information, see Revert the Upgrade.
Administration			
Back up and restore threat defense virtual for AWS.	7.2.0	Any	You can now use the management center to back up threat defense virtual for AWS, except device clusters. To restore, use the device CLI. For more information, see Backup/Restore.
Multiple DNS server groups for resolving DNS requests.	7.2.0	Any	You can configure multiple DNS groups for the resolution of DNS requests from client systems. You can use these DNS server groups to resolve requests for different DNS domains. For example, you could have a catch-all default group that uses public DNS servers, for use with connections to the Internet. You could then configure a separate group to use internal DNS servers for internal traffic, for example, any connection to a machine in the example.com domain. Thus, connections to an FQDN using your organization's domain name would be resolved using your internal DNS servers, whereas connections to public servers use external DNS servers. New/modified screens: **Platform Settings** > **DNS** For more information, see Platform Settings.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Configure certificate validation with threat defense by usage type.	7.2.0	7.2.0	You can now specify the usage types where validation is allowed with the trustpoint (the threat defense device): IPsec client connections, SSL client connections, and SSL server certificates. New/modified screens: We added a **Validation Usage** option to certificate enrollment objects: **Objects** > **Object Manager** > **PKI** > **Cert Enrollment**. For more information, see Object Management.
French language option for web interface.	7.2.0	Any	You can now switch the management center web interface to French. New/modified screens: **System** (⚙) **> Configuration > Language** For more information, see System Configuration.
Web interface changes: deployment and user activity integrations.	7.2.0	Any	Version 7.2 changes these management center menu options in all cases. **Deploy > Deployment History** is now **Deploy > Deployment History** (🕘) (bottom right corner) **Deploy > Deployment** is now **Deploy > Advanced Deploy** **Analysis > Users > Active Sessions** is now **Integration > Users > Active Sessions** **Analysis > Users > Users** is now **Integration > Users > Users** **Analysis > Users > User Activity** is now **Integration > Users > User Activity**

Feature	Minimum Management Center	Minimum Threat Defense	Details
Web interface changes: SecureX, threat intelligence, and other integrations.	7.2.0	Any	Version 7.2 changes these management center menu options if you are upgrading from Version 7.0.1 or earlier, or from Version 7.1. **Note** If you are upgrading from Version 7.0.2 or any later Version 7.0.x maintenance release, your menu structure already looks like this. **AMP > AMP Management** is now **Integration > AMP > AMP Management** **AMP > Dynamic Analysis Connections** is now **Integration > AMP > Dynamic Analysis Connections** **Intelligence > Sources** is now **Integration > Intelligence > Sources** **Intelligence > Elements** is now **Integration > Intelligence > Elements** **Intelligence > Settings** is now **Integration > Intelligence > Settings** **Intelligence > Incidents** is now **Integration > Intelligence > Incidents** **System (⚙) > Integration** is now **Integration > Other Integrations** **System (⚙) > Logging > Security Analytics & Logging** is now **Integration > Security Analytics & Logging** **System (⚙) > SecureX** is now **Integration > SecureX**
Troubleshooting			
Dropped packet statistics for the Secure Firewall 3100.	7.2.0	7.2.0	The new **show packet-statistics** threat defense CLI command displays comprehensive information about non-policy related packet drops. Previously this information required using several commands. For more information, see the Cisco Secure Firewall Threat Defense Command Reference.
Deprecated Features			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: EIGRP with FlexConfig.	7.2.0	Any	You can now configure EIGRP routing from the management center web interface. You no longer need these FlexConfig objects: Eigrp_Configure, Eigrp_Interface_Configure, Eigrp_Unconfigure, Eigrp_Unconfigure_all. And these associated text objects: eigrpAS, eigrpNetworks, eigrpDisableAutoSummary, eigrpRouterId, eigrpStubReceiveOnly, eigrpStubRedistributed, eigrpStubConnected, eigrpStubStatic, eigrpStubSummary, eigrpIntfList, eigrpAS, eigrpAuthKey, eigrpAuthKeyId, eigrpHelloInterval, eigrpHoldTime, eigrpDisableSplitHorizon. The system does allow you to deploy post-upgrade, but also warns you to redo your EIGRP configurations. To help you with this process, we provide a command-line migration tool. For details, see Migrating FlexConfig Policies .
Deprecated: VXLAN with FlexConfig.	7.2.0	Any	You can now configure VXLAN interfaces from the management center web interface. You no longer need these FlexConfig objects: VxLAN_Clear_Nve, VxLAN_Clear_Nve_Only, VxLAN_Configure_Port_And_Nve, VxLAN_Make_Nve_Only, VxLAN_Make_Vni. And these associated text objects: vxlan_Port_And_Nve, vxlan_Nve_Only, vxlan_Vni. If you configured VXLAN interfaces with FlexConfig in a previous version, they continue to work. In fact, FlexConfig takes precedence in this case—if you redo your VXLAN configurations in the web interface, remove the FlexConfig settings.
Deprecated: Automatic pre-upgrade troubleshooting.	7.2.0	Any	To save time and disk space, the management center upgrade process no longer automatically generates troubleshooting files before the upgrade begins. Note that device upgrades are unaffected and continue to generate troubleshooting files. To manually generate troubleshooting files for the management center, choose **System** (⚙) > **Health** > **Monitor**, click **Firewall Management Center** in the left panel, then **View System & Troubleshoot Details**, then **Generate Troubleshooting Files**.
Deprecated: Geolocation details.	Any	Any	In May 2022 we split the GeoDB into two packages: a country code package mapping IP addresses to countries/continents, and an IP package containing additional contextual data associated with routable IP addresses. In January 2024, we stopped providing the IP package. This saves disk space and does not affect geolocation rules or traffic handling in any way. Any contextual data is now stale, and upgrading to most later versions deletes the IP package. Options to download the IP package or view contextual data have no effect, and are removed in later versions.

Device Manager Features in Version 7.2.x

Table 10: Device Manager Features in Version 7.2.x

Feature	Description
Platform Features	
Firepower 1010E.	We introduced the Firepower 1010E, which does not support power over Ethernet (PoE). Minimum threat defense: 7.2.3 See: Cabling for the Firepower 1010
Threat defense virtual for GCP.	You can now use device manager to configure threat defense virtual for GCP. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
Threat defense virtual for Megaport.	You can now use device manager to configure threat defense virtual for Megaport (Megaport Virtual Edge). High availability is supported. Minimum threat defense: 7.2.8 Other version restrictions: Initially, you may not be able to freshly deploy Versions 7.3.x or 7.4.x. Instead, deploy Version 7.2.8–7.2.x and upgrade. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
Network modules for the Secure Firewall 3100.	We introduced these network modules for the Secure Firewall 3100: • 6-port 1G SFP Network Module, SX (multimode) (FPR-X-NM-6X1SX-F) • 6-port 10G SFP Network Module, SR (multimode) (FPR-X-NM-6X10SR-F) • 6-port 10G SFP Network Module, LR (single mode) (FPR-X-NM-6X10LR-F) • 6-port 25G SFP Network Module, SR (multimode) (FPR-X-NM-X25SR-F) • 6-port 25G Network Module, LR (single mode) (FPR-X-NM-6X25LR-F) • 8-port 1G Copper Network Module, RJ45 (copper) (FPR-X-NM-8X1G-F) Minimum threat defense: 7.2.1
Intel Ethernet Network Adapter E810-CQDA2 driver with threat defense virtual for KVM.	We now support the Intel Ethernet Network Adapter E810-CQDA2 driver with threat defense virtual for KVM. Minimum threat defense: 7.2.1 See: Deploy the Threat Defense Virtual on KVM
ISA 3000 support for shutting down.	Support returns for shutting down the ISA 3000. This feature was introducted in Version 7.0.2 but was temporarily deprecated in Version 7.1.
Firewall and IPS Features	

Feature	Description
Object-group search is enabled by default for access control.	The CLI configuration command **object-group-search access-control** is now enabled by default for new deployments. If you are configuring the command using FlexConfig, you should evaluate whether that is still needed. If you need to disable the feature, use FlexConfig to implement the **no object-group-search access-control** command. See: Cisco Secure Firewall ASA Series Command Reference
Rule hit counts persist over reboot.	Rebooting a device no longer resets access control rule hit counts to zero. Hit counts are reset only if you actively clear the counters. In addition, counts are maintained by each unit in an HA pair or cluster separately. You can use the **show rule hits** command to see cumulative counters across the HA pair or cluster, or see the counts per node. We modified the following threat defense CLI command: **show rule hits**. See: Examining Rule Hit Counts
VPN Features	
IPsec flow offload.	On the Secure Firewall 3100, IPsec flows are offloaded by default. After the initial setup of an IPsec site-to-site VPN or remote access VPN security association (SA), IPsec connections are offloaded to the field-programmable gate array (FPGA) in the device, which should improve device performance. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command. See: IPSec Flow Offload
Interface Features	
Breakout port support for the Secure Firewall 3130 and 3140.	You can now configure four 10GB breakout ports for each 40GB interface on the Secure Firewall 3130 and 3140. New/modified screens: **Devices** > **Interfaces** See: Manage the Network Module for the Secure Firewall 3100
Enabling or disabling Cisco Trustsec on an interface.	You can enable or disable Cisco Trustsec on physical, subinterface, EtherChannel, VLAN, Management, or BVI interfaces, whether named or unnamed. By default, Cisco Trustsec is enabled automatically when you name an interface. We added the **Propagate Security Group Tag** attribute to the interface configuration dialog boxes, and the **ctsEnabled** attribute to the various interface APIs. See: Configure Advanced Options
Licensing Features	
Permanent License Reservation Support for ISA 3000.	ISA 3000 now supports Universal Permanent License Reservation for approved customers. See: Applying Permanent Licenses in Air-Gapped Networks
Administrative and Troubleshooting Features	

Feature	Description
Ability to force full deployment.	When you deploy changes, the system normally deploys just the changes made since the last successful deployment. However, if you are experiencing problems, you can elect to force a full deployment, which completely refreshes the configuration on the device. We added the **Apply Full Deployment** option to the deployment dialog box. See: Deploying Your Changes
Automatically update CA bundles.	**Upgrade impact. The system connects to Cisco for something new.** The local CA bundle contains certificates to access several Cisco services. The system now automatically queries Cisco for new CA certificates at a daily system-defined time. Previously, you had to upgrade the software to update CA certificates. You can use the CLI to disable this feature. New/modified CLI commands: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** Version restrictions: This feature is included in Versions 7.0.5+, 7.1.0.3+, and 7.2.4+. It is not supported in earlier 7.0, 7.1, or 7.2 releases. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco. See: Cisco Secure Firewall Threat Defense Command Reference
Threat defense REST API version 6.3 (v6).	The threat defense REST API for software version 7.2 is version 6.3. You can use v6 in the API URLs, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. Note that the URL version path element for 6.3 is the same as 6.0, 6.1, and 6.2: v6. Please re-evaluate all existing calls, as changes might have been mode to the resource models you are using. To open the API Explorer, where you can view the resources, log into device manager, then click the more options button (⋮) and choose **API Explorer**. See: Cisco Secure Firewall Threat Defense REST API 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. Having to enable a new setting or deploy a policy post-upgrade to take advantage of a new feature does not count as upgrade impact.

Note Deploying can affect traffic flow and inspection; see the appropriate upgrade guide for details: Cisco Secure Firewall Threat Defense: Install and Upgrade Guides.

Tip Features, enhancements, and critical fixes can skip releases; these skipped releases are usually short-term major versions or early maintenance releases for long-term major versions. To minimize upgrade impact, do not upgrade to a release that deprecates features. In most cases, you can upgrade directly to the latest maintenance release for any major version.

Upgrade Impact Features for Management Center

Check all releases between your current and target version.

Table 11: Upgrade Impact Features for Management Center

Target Version	Features with Upgrade Impact
7.2.6–7.2.x	• Configure DHCP relay trusted interfaces from the management center web interface. • Updated internet access requirements for direct-downloading software upgrades. • Scheduled tasks download patches and VDB updates only. • Updated web analytics provider.
7.2.5-7.2.x	• Management center detects interface sync errors.
7.2.4+	• Automatically update CA bundles.
7.2.4–7.2.x	• Smaller VDB for lower memory Snort 2 devices.
7.2.4–7.2.5	• Access control performance improvements (object optimization).
7.2.0+	• Configure VXLAN from the management center web interface. • Configure EIGRP from the management center web interface.
7.1.0+	• Configure Equal-Cost-Multi-Path (ECMP) from the FMC web interface. • Configure policy based routing from the FMC web interface. • Send intrusion events and retrospective malware events to the Secure Network Analytics cloud from the FMC. • Deprecated (temporary): Improved SecureX integration, SecureX orchestration. • Deprecated: Intrusion incidents and the intrusion event clipboard. • Deprecated: Custom tables for intrusion events.
7.0.0+	• End of support: VMware vSphere/VMware ESXi 6.0. • Deprecated: Port 32137 comms with AMP clouds.

Target Version	Features with Upgrade Impact
6.7.0+	• Changes to PAT address allocation in clustering. • pxGrid 2.0 with ISE/ISE-PIC. • Improved preclassification of files for dynamic analysis. • National Vulnerability Database (NVD) replaces Bugtraq. • Pre-upgrade compatibility check. • Upgrades postpone scheduled tasks. • Upgrades remove PCAP files to save disk space. • Deprecated: Cisco Firepower User Agent software and identity source. • Deprecated: Cisco ISE Endpoint Protection Services (EPS) remediation. • Deprecated: Less secure Diffie-Hellman groups, and encryption and hash algorithms. • Deprecated: Appliance Configuration Resource Utilization heath module (temporary).

Upgrade Impact Features for Threat Defense with Management Center

Check all releases between your current and target version.

Table 12: Upgrade Impact Features for Threat Defense with Management Center

Target Version	Features with Upgrade Impact
7.2.4+	• Automatically update CA bundles.
7.2.0+	• Autoscale for threat defense virtual for GCP.
7.1.0+	• Snort 3 support for inspection of DCE/RPC over SMB2. • Snort 3 support for **ssl_version** and **ssl_state** keywords.
7.0.5–7.0.x	• Automatically update CA bundles.
7.0.0+	• End of support: VMware vSphere/VMware ESXi 6.0. • FTDv performance tiered Smart Licensing. • Deprecated: RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm. • Deprecated: MD5 authentication algorithm and DES encryption for SNMPv3 users.

Target Version	Features with Upgrade Impact
6.7.0+	• Firepower 1100/2100 series SFP interfaces now support disabling auto-negotiation. • ClientHello modification for Decrypt - Known Key TLS/SSL rules. • Pre-upgrade compatibility check. • Improved readiness checks. • Improved FTD upgrade status reporting and cancel/retry options. • Upgrades remove PCAP files to save disk space.

Upgrade Impact Features for Threat Defense with Device Manager

Check all releases between your current and target version.

Table 13: Upgrade Impact Features for Threat Defense with Device Manager

Target Version	Features with Upgrade Impact
7.2.4+	• 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.
7.0.0+	• End of support: VMware vSphere/VMware ESXi 6.0. • DHCP relay configuration using the threat defense API.
6.7.0+	• Support removed for less secure Diffie-Hellman groups, and encryption and hash algorithms. • EIGRP support using Smart CLI. • Threat Defense API support for SNMP configuration.

Upgrade Guidelines

The following sections contain release-specific upgrade warnings and guidelines. You should also check for features and bugs with upgrade impact. For general information on time/disk space requirements and on system behavior during upgrade, see the appropriate upgrade guide: For Assistance, on page 140.

Upgrade Guidelines for Management Center

Table 14: Upgrade Guidelines for Management Center

Target Version	Current Version	Guideline	Details
7.2.8.x	7.2.8.0	Patch uninstall not supported: Version 7.2.8.x to Version 7.2.8.0.	Uninstall is not supported for the Version 7.2.8.1 management center patch. Because patches are cumulative, and because uninstalling returns you to the patch level you upgraded from, this means that uninstall is not supported from any Version 7.2.8.x patch back to Version 7.2.8 (the base version).
7.2.6	6.6.0–7.2.5	Upgrade not recommended: Version 7.2.6.	Due to CSCwi63113, Version 7.2.6 was deferred on 2024-04-29 and is no longer available for download. If you downloaded it, do not use it. If you are running this version, upgrade.
7.0.0–7.2.x	6.4.0–6.7.x	Reconnect with Threat Grid for high availability management centers.	Version 7.0.0 fixes an issue with management center high availability and malware detection where, after failover, the system stopped submitting files for dynamic analysis (CSCvu35704). For the fix to take effect, you must reassociate with the Cisco Threat Grid public cloud after upgrading. After you upgrade the high availability pair to Version 7.0.0+, on the primary management center: 1. Choose **AMP** > **Dynamic Analysis Connections**. 2. Click **Associate** in the table row corresponding to the public cloud. A portal window opens. You do not have to sign in. The reassociation happens in the background, within a few minutes.

Upgrade Guidelines for Threat Defense with Management Center

Table 15: Upgrade Guidelines for Threat Defense with Management Center

Target Version	Current Version	Guideline	Details
7.2.6	6.6.0–7.2.5	Upgrade not recommended: Version 7.2.6.	Due to CSCwi63113, Version 7.2.6 was deferred on 2024-04-29 and is no longer available for download. If you downloaded it, do not use it. If you are running this version, upgrade.
7.2.0–7.6.x	6.7.0–7.1.x	Upgrade prohibited: threat defense virtual for GCP from Version 7.1.x and earlier to Version 7.2.0+.	You cannot upgrade threat defense virtual for GCP from Version 7.1.x and earlier to Version 7.2.0+. You must deploy a new instance.

Target Version	Current Version	Guideline	Details
7.2.0–7.2.6	7.1.x 6.6.0–7.0.2	Unregister and reregister devices after reverting threat defense.	If you revert from Version 7.2.0–7.2.6 to Version 6.6.0–7.0.2 or to Version 7.1.x, unregister and reregister devices after the revert completes (CSCwi31680).
6.7.0–7.2.x	6.4.0–6.6.x	Upgrade failure: Firepower 1010 switch ports with invalid VLAN IDs.	For the Firepower 1010, threat defense upgrades to Version 6.7+ will fail if you configured switch ports with a VLAN ID in the 3968–4047 range. These IDs are for internal use only.

Upgrade Guidelines for Threat Defense with Device Manager

Table 16: Upgrade Guidelines for Threat Defense with Device Manager

Target Version	Current Version	Guideline	Details
7.2.6	6.6.0–7.2.5	Upgrade not recommended: Version 7.2.6.	Due to CSCwi63113, Version 7.2.6 was deferred on 2024-04-29 and is no longer available for download. If you downloaded it, do not use it. If you are running this version, upgrade.
6.7.0–7.2.x	6.4.0–6.6.x	Upgrade failure: Firepower 1010 switch ports with invalid VLAN IDs.	For the Firepower 1010, threat defense upgrades to Version 6.7+ will fail if you configured switch ports with a VLAN ID in the 3968–4047 range. These IDs are for internal use only.

Upgrade Guidelines for the Firepower 4100/9300 Chassis

In most cases, we recommend you use the latest FXOS build in each major version. For release-specific FXOS upgrade warnings and guidelines, as well as features and bugs with upgrade impact, see the FXOS release notes. Check all release notes between your current and target version: http://www.cisco.com/go/firepower9300-rns.

For firmware upgrade guidelines (for upgrades to FXOS 2.13 and earlier), see the firmware upgrade guide: Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.

Upgrade Path

Planning your upgrade path is especially important for large deployments, multi-hop upgrades, and situations where you need to coordinate chassis, hosting environment or other upgrades.

Upgrading the Management Center

The management center must run the same or newer version as its devices. Upgrade the management center to your target version first, then upgrade devices. If you begin with devices running a much older version than the management center, further management center upgrades can be blocked. In this case perform a three (or more) step upgrade: devices first, then the management center, then devices again.

Upgrading Threat Defense with Chassis Upgrade

For the Firepower 4100/9300, major versions require a FXOS upgrade. You should also check for firmware upgrades.

Because you upgrade the chassis first, you will briefly run a supported—but not recommended—combination, where the operating system is "ahead" of threat defense. If the chassis is already well ahead of its devices, further chassis upgrades can be blocked. In this case perform a three (or more) step upgrade: devices first, then the chassis, then devices again. Or, perform a full reimage. In high availability or clustered deployments, upgrade one chassis at a time.

Supported Direct Upgrades

This table shows the supported direct upgrades for management center and threat defense software. Note that although you can upgrade directly to major and maintenance releases, patches change the fourth digit only. You cannot upgrade directly to a patch from a previous major or maintenance release.

For the Firepower 4100/9300, the table also lists companion FXOS versions. If a chassis upgrade is required, 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 17: Supported Direct Upgrades for Major and Maintenance Releases

Current Version	Target Software Version										
	7.6	7.4	7.3	7.2	7.1	7.0	6.7	6.6	6.5	6.4	6.3
	Firepower 4100/9300 FXOS Version for Chassis Upgrades										
	2.16	2.14	2.13	2.12	2.11	2.10	2.9	2.8	2.7	2.6	2.4
7.6	YES	—	—	—	—	—	—	—	—	—	—
7.4	YES	YES †	—	—	—	—	—	—	—	—	—
7.3	YES	YES	YES	—	—	—	—	—	—	—	—
7.2	YES	YES	YES	YES	—	—	—	—	—	—	—
7.1	YES	YES	YES	YES	YES	—	—	—	—	—	—
7.0	—	YES	YES	YES	YES	YES	—	—	—	—	—
6.7	—	—	— *	YES	YES	YES	YES	—	—	—	—
6.6	—	—	—	YES	YES	YES	YES	YES	—	—	—
6.5	—	—	—	—	YES	YES	YES	YES	—	—	—
6.4	—	—	—	—	—	YES	YES	YES	YES	—	—
6.3	—	—	—	—	—	—	YES	YES	YES	YES	—
6.2.3	—	—	—	—	—	—	—	YES	YES	YES	YES

* You cannot upgrade from Version 6.7.x to 7.3.x. You can, however, manage Version 6.7.x devices with a Version 7.3.x management center.

† You cannot upgrade threat defense to Version 7.4.0, which is available as a fresh install on the Secure Firewall 4200 only. Instead, upgrade your management center and devices to Version 7.4.1+.

Bugs

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

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

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 7.2.0

Table last updated: 2024-05-02

Table 18: Open Bugs in Version 7.2.0

Bug ID	Headline
CSCwb43433	Jumbo frame performance has degraded up to -45% on Firepower 2100 series
CSCwb78233	7.2.0 1984 Nutanix vFMC not accessible after upgrade from 7.1.0
CSCwb80789	TLS 1.3 connections to sites previously decrypted may fail
CSCwb87724	Evicted units re-joined existing Cluster but not listed on Control and other evicted vFTD Cluster
CSCwb88887	snp_fp_vxlan_encap_and_grp_send_common: failed to find adj. bp->l3_type = 8, inner_sip message
CSCwb89905	vFTD installed with JF but still FMC shows info about JF getting enabled and to reboot vFTD
CSCwb90105	Upgrade to 7.2 on FTDv for Nutanix is stuck after reboot
CSCwb96990	Early data may cause xtls to not wait for probe response
CSCwb97486	FPR3100: 25G optic may show link up on some 1/10G capable only fiber ports
CSCwb99960	onPremFMC with only CDO Managed devices registered, Malware Event pages shows license warning
CSCwd07838	User cannot filter by device in the new AC policy UI
CSCwd16602	Inconsistencies seen after switching from old UI to new UI without saving the policy

Bug ID	Headline
CSCwd47149	New AC Policy UI: ACP rule list takes a long time to load in case of large rule set
CSCwe14714	Search is slow and semantic based searches are not working in new ACP UI
CSCwe96560	Cannot copy rules from one policy to another policy using new AC policy UI
CSCwh15444	Fetching hit counts takes longer in NEW ACP UI when compared to the legacy ACP UI
CSCwi22693	ACP rule is deleted when discarding changes, post rule reposition.

Resolved Bugs in Version 7.2.9

Table last updated: 2024-10-22

Table 19: Resolved Bugs in Version 7.2.9

Bug ID	Headline
CSCvx74133	App-instance showing as Started instead of Online
CSCvy51481	[ENH] FTD should show error/warning when attaching a not valid certificate to the interface for VPN
CSCvz59859	FXOS fault F1758 description should not be specific to subinterfaces
CSCvz70310	ASA may fail to create NAT rule for SNMP with: "error NAT unable to reserve ports."
CSCwa82791	ENH: Support for snapshots of RX queues on InternalData interfaces when "Blocks free curr" goes low
CSCwb02701	FXOS does not retry NTP sync with servers
CSCwb02741	Time sync status and error message do not elaborate NTP server rejection case
CSCwb03293	IKEv2 debugs: Received Policies and Expected Policies are empty
CSCwc01843	For FTD HA or cluster, incorrect device name may be shown in eventing UI and dashboard statistics
CSCwd65732	2X100G netmod card shows 10 Mbps on first member of port channel when second interface added
CSCwd67100	ASA traceback and reload on Datapath process
CSCwe02012	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe18462	ASA/FTD: Improve GTP Inspection Logging
CSCwe18467	ASA/FTD: GTP Inspection engine serviceability
CSCwe21884	Write wrapper around "kill" command to log who is calling it

Bug ID	Headline
CSCwe34826	Intrusion user not able to change intrusion action and File Policy
CSCwe82107	health alert for [FSM:STAGE:FAILED]: external aaa server configuration
CSCwf16001	HashiCorp Vault's implementation of Shamir's secret sharing used precomp
CSCwf27337	KP: Cleanup/Reformat the second (MSP) disk on FTD reinstall
CSCwf39108	Firewall rings may get stuck and cause packet loss when asp load-balance per-packet auto is used
CSCwf64429	Unable to upload FTD version image to FCM
CSCwf69880	Firewall Traceback and reload due to SNMP thread
CSCwf70275	FTD: TLS Server Identity does not work if size of client hello more than TCP MSS bytes
CSCwf75694	ASA - The GTP inspection dropped the message 'Delete PDP Context Response' due to an invalid TEID=0
CSCwf77994	False critical high CPU alerts for FTD device system cores running instantaneous high usage
CSCwf84318	ASA/FTD traceback and reload on thread DATAPATH
CSCwf99434	Failed to transfer new image file to FPR2130 and traceback was observed
CSCwh09968	ASA/FTD: Traceback and reload due to NAT change and DVTI in use
CSCwh10931	ASA/FTD traceback and reload when invoking "show webvpn saml idp" CLI command
CSCwh13040	Incomplete rootwalk. snmpwalk on 816 MIB is getting timeout.
CSCwh14475	FTD events stopped being sent to FMC, EventHandler logs "publishing blocked"
CSCwh19475	Intermittently flow is getting white-listed by the snort for the unknow app-id traffic.
CSCwh19613	ASA crashed with Saml scenarios
CSCwh27886	Chassis Manager shows HTTP 500 Internal Server error in specific cases
CSCwh28218	Syslog not updating when prefilter rule name changes
CSCwh29276	ASA: Traceback and reload when switching from single to multiple mode
CSCwh40294	ASA traceback due to panic event during SNMP configuration
CSCwh43230	Strong Encryption license is not getting applied to ASA firewalls in HA.
CSCwh45450	2100: Interfaces missing from FTD after removing interfaces as members of a port-channel
CSCwh45935	Lina core observed in 6.4.0.17-22 in Kp with scaled traffic

Bug ID	Headline
CSCwh48776	An issue was discovered in Python before 3.8.18, 3.9.x before 3.9.18,
CSCwh51872	Message asa_log_client exited 1 time(s) seen multiple times
CSCwh52710	evaluate open-vm-tools / VMware Tools on FMC for VMware -- CVE-2023-20900 and VMSA-2023-0019
CSCwh57814	The html/template package does not apply the proper rules for handling o
CSCwh60971	NAT pool is not working properly despite is not reaching the 32k object ID limit.
CSCwh62080	additional command outputs needed in FTD troubleshoot for blocks and ssl cache
CSCwh63211	Lina core at snp_nat_xlate_verify_magic.part and soft traces
CSCwh68068	Firepower WCCP router-id changes randomly when VRFs are configured
CSCwh69156	FTD-HA does not fail over sometimes when snort3 crashes
CSCwh69843	WM DT - ASA in transparent mode doesn't send equal IPv6 Router Advertisement packets to all nodes
CSCwh71262	A flaw was found in glibc. In an uncommon situation, the gaih_inet fun
CSCwh72070	Reload takes forever when reload command is issued on the lina prompt when devices are on HA
CSCwh78118	ASA/FTD traceback and reload on process fsm_send_config_info_initiator
CSCwh81366	[Multi-Instance] Second Hard Drive (FPR-MSP-SSD) not in use
CSCwh83517	VTI tunnel goes down due to route change detected in VRF scenario
CSCwh91065	Lina Traceback : Thread Name: DATAPATH during session terminate
CSCwh92345	crypto_archive file generated after the software upgrade.
CSCwh94029	A flaw was found in the Netfilter subsystem in the Linux kernel. The n
CSCwh94116	A flaw was found in the Netfilter subsystem in the Linux kernel. The x
CSCwh94193	urllib3 is a user-friendly HTTP client library for Python. urllib3 doe
CSCwh95025	GTP connections, under certain circumstances do not get cleared on issuing clear conn.
CSCwh95277	FTD traceback due to system memory exhaustion
CSCwh95443	Datapath hogs causing clustering units to get kicked out of the cluster
CSCwh96055	Management DNS Servers may be unreacheable if data interface is used as the gateway
CSCwh99398	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-34-17852'
CSCwi00713	A memory leak flaw was found in Libtiff's tiffcrop utility. This issue

Bug ID	Headline
CSCwi01323	SNMP OID ifOutDiscards on MIO are always zero despite show interface are non-zero
CSCwi02754	FTD 1120 standby sudden reboot
CSCwi03407	Traceback on FP2140 without any trigger point.
CSCwi04351	FTD upgrade failling on script 999_finish/999_zz_install_bundle.sh
CSCwi05240	ASA - Traceback the standby device while HA sync ACL-DAP
CSCwi06797	ASA/FTD traceback and reload on thread DATAPATH
CSCwi20045	ASA/FTD may traceback and reload in Thread Name 'lina' due to a watchdog in 9.16.3.23 code
CSCwi23964	Python 3.x through 3.10 has an open redirection vulnerability in lib/h
CSCwi24007	An issue was discovered in the Linux kernel before 6.3.3. There is an
CSCwi24116	Twisted is an event-based framework for internet applications. Prior t
CSCwi31480	Alert: Decommission failed, reason: Internal error is not cleared from FCM or CLI after acknowledge
CSCwi31558	File-extracts.logs are not recognised by the diskmanager leading to high disk space
CSCwi31966	FTD ADI debugs may show incorrect server_group and/or realm_id for SAML-authenticated sessions
CSCwi36244	In buc Traceroute 2.0.12 through 2.1.2 before 2.1.3, the wrapper scrip
CSCwi36311	use kill tree function in SMA instead of SIGTERM
CSCwi36843	Detailed logging related to reason behind sub-interface admin state change during operations
CSCwi38662	FTD HA should not be created partially on FMC
CSCwi40193	Hairpinning of DCE/RPC traffic during the suboptimal lookup
CSCwi40302	Deployment fails on new AWS FTDv device with "no username admin"
CSCwi43492	ASA traceback and reload on Thread Name: DATAPATH
CSCwi44208	low memory/stress causing traceback in SNMP
CSCwi44912	ISA3000 Traceback and reload boot loop
CSCwi45878	ASA/FTD: DNS Load Balancing with SAML does not work with VPN Load Balancing
CSCwi48699	ASA traceback and reload on Thread Name: pix_flash_config_thread
CSCwi49770	ASA|FTD Traceback & reload in thread name Datapath

Bug ID	Headline
CSCwi49884	TCP MSS is changed back to the default value when a VTI or loopback interface is created
CSCwi52008	Snort3 traceback and restarts with race conditions
CSCwi53949	Snot3 traceback in TcpReassembler::scan_data_post_ack
CSCwi53987	SSL protocol settings does not modify the FDM GUI certificate configuration or disable TLSv1.1
CSCwi55938	The "show asp drop" command usage requires better updates for cluster-related drops
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
CSCwi56743	MSP Quota setting for instances is not correct
CSCwi57670	RAVPN SAML: External browser gives misleading message when FTD/ASA fails to parse assertion
CSCwi59271	Suppress "End of script output before headers" syslog on FXOS
CSCwi60285	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi61135	Debugs failed to be enabled on SSH session
CSCwi62796	ASA/FTD Traceback and reload related to SSL/DTLS traffic processing
CSCwi63743	ASA/FTD may traceback and reload in Thread Name "appAgent_monitor_nd_thread" & Rip: _lina_assert.
CSCwi64829	traceback and reload around function HA
CSCwi65116	DHCPv6:ASA traceback on Thread Name: DHCPv6 CLIENT.
CSCwi66461	WARN msg(speed not compatible, suspended) while creating port-channel on Victoria CE
CSCwi66676	ASA/FTD may traceback and reload in Thread Name 'webvpn_task'
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'
CSCwi70492	Firewall is in App Sync error in pseudo-standby mode and uses IPs from Active unit
CSCwi71998	"Stream: TCP normalization error in NO_TIMESTAMP" is seen when SSL Policy decrypt all is used
CSCwi72294	FTD: Improve or optimize LSP package verification logic to run it faster

Bug ID	Headline
CSCwi74214	ASA/FTD traceback and reload in Thread Name: IKEv2 Daemon when moving from active to standby HA
CSCwi75198	Standby FTD experiencing periodic traceback and reload
CSCwi75967	CCM ID 62 - LTS18
CSCwi76361	Transparent firewall MAC filter does not capture frames with STP-UplinkFast dst MAC consistently
CSCwi78191	An issue was discovered in drivers/input/input.c in the Linux kernel b
CSCwi78193	An issue was discovered in the Linux kernel before 6.6.8. do_vcc_ioctl
CSCwi78200	A vulnerability was found in GnuTLS. The response times to malformed c
CSCwi78206	A vulnerability was found in GnuTLS, where a cockpit (which uses gnuTL
CSCwi78370	41xx/93xx : Update CiscoSSH (Chassis Manager FXOS) to address CVE-2023-48795
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
CSCwi79393	Policy Deployment Fails when removing the Umbrella DNS Policy from Security Intelligence
CSCwi80979	Snort stripping packet information and injects its packet with 0 bytes data
CSCwi81503	HTTP/HTTPS detection for application needs to fail it's detection earlier
CSCwi81771	Unable to send unknown file disposition to ThreatGrid due to mem cache issue
CSCwi83890	Report file generated for AC policy is empty
CSCwi84314	ASA CLI hangs with 'show run' on multiple SSH
CSCwi84615	some stdout logs not rotated by logrotate
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
CSCwi85953	In rds_recv_track_latency in net/rds/af_rds.c in the Linux kernel thro
CSCwi87382	Traceback and reload on Primary unit while running debugs over the SSH session
CSCwi90571	Access to website via Clientless SSL VPN Fails
CSCwi90751	FTD/ASA - SNMP queries using snmpwalk are not displaying all "nameif" interfaces

Bug ID	Headline
CSCwi90998	ASA SNMP Polling Failure for environmental FXOS DME MIB (.1.3.6.1.4.1.9.9.826.2)
CSCwi92875	Check metadata cache size when generating retrospective events
CSCwi92924	A memory leak problem was found in ctnetlink_create_conntrack in net/n
CSCwi92927	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tab
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
CSCwi95228	"crypto ikev2 limit queue sa_init" resets after reboot
CSCwi95796	FTD SNMP OID 1.3.6.1.4.1.9.9.109.1.1.1.1.7 always returns 0% for SysProc Average
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
CSCwi98274	unzip 5.52 is from 2005 is contains multiple vulnerabilities
CSCwi99429	Policy deployment failure rollback didnt reconfigure the FTD devices
CSCwj00956	Snort process spamming syslog-ng messages so our on KP platform syslog-ng is being killed
CSCwj02505	ASA Checkheaps traceback while entering same engineID twice
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
CSCwj05484	ASA upgrade from 9.16 to 9.18 causing change in AAA ldap attribute values by adding extra slash '\'
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
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
CSCwj08066	A denial of service vulnerability due to a deadlock was found in sctp_
CSCwj08083	An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.1
CSCwj08153	An out-of-memory flaw was found in libtiff that could be triggered by

Bug ID	Headline
CSCwj08667	ASA/FTD Traceback and Reload during ssl session establishment
CSCwj09110	Upload files through Clientless portal is not working as expected after the ASA upgrade
CSCwj09999	FP 3100 MTU change on management interface is NOT persistent across reboots (returns to default MTU)
CSCwj10451	The secondary device reloaded while rebooting the primary device.
CSCwj12131	Bailout when lina_io_write fails persistent with EPIPE errno.
CSCwj12173	Policy cache cleanup thread should cleanup any cache that is left open for a logged out session
CSCwj12924	A flaw was found in the Netfilter subsystem in the Linux kernel. The i
CSCwj13910	Crypto IPSEC SA Output Showing NO SA ERROR With IPSEC Offload Enabled
CSCwj14028	CCM ID 67 - LTS18
CSCwj14624	Backup exits with memory allocation error on 4115
CSCwj14832	SAML: Single sign-on AnyConnect token verification failure is seen after successful authentication
CSCwj14927	FTD: Primary takes active role after reloading
CSCwj15125	ASA/FTD may traceback and reload in Thread Name 'lina' related to Netflow timer infra
CSCwj17447	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-6-26174'
CSCwj19653	FTD - Trace back and reload due to NAT involving fqdn objects
CSCwj20067	ASA: Warning messages not displayed when Static interface NAT are configured
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, “Slot 1: ATA Compact Flash memory” shows a ditterent value
CSCwj23192	extra file check is not reporting with pmtool SecureLSP lsp-rel-xxx command
CSCwj24828	Issue when two FQDN objects with same IP are added in source or destination (FTD/ASA)
CSCwj25975	FTD/ASA : CSR generation with comma between “Company Name” attribute does not work expected

Bug ID	Headline
CSCwj28153	Lina contains outdated libexpat source code
CSCwj28437	Snort3: SQL traffic failure after upgrade due to large invalid sequence numbers and invalid ACKs
CSCwj30825	SFDataCorrelator memory leak after unregistering an active device
CSCwj30980	Addition of debugs & a show command to capture the ID usage in the CTS SXP flow.
CSCwj31918	Segmentation fault with "logger_msg_dispatch" while HA sync
CSCwj32035	Clientless VPN users are unable to reach pages with HTTP Basic Authentication
CSCwj33487	ASA/FTD may traceback and reload while handling DTLS traffic
CSCwj33580	IKEv2 tunnels flap due to fragmentation and throttling caused by multiple ciphers/proposal
CSCwj33891	ASA/FTD Cluster memory exhaustion caused by NAT process during release of port blocks allocations
CSCwj34881	Command to show counters for access-policy filtered with a source IP address gives incorrect result
CSCwj34975	Multiple context interfaces fail to pass traffic
CSCwj35701	Dns-guard prematurely closing conn due to timing condition
CSCwj38871	ASA traceback with thread name SSH
CSCwj38928	High latency observed on FPR31xx or FPR42xx
CSCwj39107	SFDataCorrelator memory growth when pruning a huge number of old service identities
CSCwj40597	FTD: Backups fail on Multi-Instance or standalone with error "Backup died unexpectedly"
CSCwj40665	Additional memory tracking in SFDataCorrelator
CSCwj40761	ASA/FTD may traceback in Threadname: **CTM KC FPGA stats handler**
CSCwj43345	SNMP poll for some OIDs may cause CPU hogs and high latency can be observed for ICMP packets
CSCwj43355	A bug in QEMU could cause a guest I/O operation otherwise addressed to
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
CSCwj44398	when set the route-map in route RIP on FTD, routes update is not working after FTD reload

Bug ID	Headline
CSCwj45822	Cisco Secure Client Unable to complete connection. Cisco Secure Desktop not installed on the client.
CSCwj48704	ASA traceback and reload when accessing file system from ASDM
CSCwj48754	SFDataCorrelator high memory usage when restart with large network map hosts
CSCwj49958	Crypto IPSEC Negotiation Failing At "Failed to compute a hash value"
CSCwj50406	All IPV6 BGP routes configured in device flapping
CSCwj53725	Traceback observed while applying 'no failover' and 'failover' in the ASA standby
CSCwj55036	ASA/FTD: A delay in an async crypto command induces a traceback and subsequently a reload.
CSCwj59861	ASA/FTD may traceback and reload in Thread Name 'lina' due to SCP/SSH process
CSCwj60265	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-1-16803'
CSCwj61885	File descriptor leak when validating upgrade images
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
CSCwj68096	Console Access Stuck for ASAv hosted in CSP after Upgrade to 9.18.3.56
CSCwj68385	Snort3 continuous traceback & reload with each deployment
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
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
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
CSCwj74323	ASAv Memory leak involving PKI/Crypto for VPN
CSCwj76503	Syslogs continue to be sent after disabling logging class on ASA
CSCwj81743	FTD - Trace back and reload due to NAT involving fqdn objects

Bug ID	Headline
CSCwj82285	ASA/FTD may traceback and reload in Thread Name 'sdi_work'
CSCwj82736	TLS Handshake Fails if Fragmented Client Hello Packet is Received Out of Order
CSCwj82903	FDM HA deployment fails with 'ApplicationException: Unable to export to database' error
CSCwj83185	FTD/ASA : Standby FTD traceback and reload after enabling memory tracking
CSCwj83634	Seeing message "reg_fover_nlp_sessions: failover ioctl C_FOREG failed"
CSCwj85106	FMC on upgrade results in FTDv losing its performance tier
CSCwj85333	FPR might drop TLS1.3 connections when hybridized kyber cipher is enabled in web browser
CSCwj86527	SNMP v1 and v2c traps from diagnostic and data ints stop working on a KP/vFTD after product upgrade
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
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
CSCwj89264	FTD HA: Traceback and reload in netsnmp_oid_compare_ll
CSCwj89315	HTTP Response splitting in multiple modules in Apache HTTP Server allo
CSCwj89402	In the Linux kernel, the following vulnerability has been resolved: n
CSCwj89404	In the Linux kernel, the following vulnerability has been resolved: b
CSCwj89406	In the Linux kernel, the following vulnerability has been resolved: b
CSCwj89417	In the Linux kernel, the following vulnerability has been resolved: d
CSCwj89425	In the Linux kernel, the following vulnerability has been resolved: B
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
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
CSCwj90826	Snort2 SSL decryption with known key fails on Chrome v124 and above.

Bug ID	Headline
CSCwj93921	ASA after upgrade to 9.18.4.24 not able to save config with error: "Configuration line too long"
CSCwj95322	disable stat check for file
CSCwj95590	Browser redirects to logon page when the user clicks the WebVPN bookmark
CSCwk00604	ASA Fails to initiate AAA Authentication with IKEv2-EAP and Windows Native VPN Client
CSCwk02332	Snort2 - SSL decryption failing and some websites not loading on Chrome v124+
CSCwk02804	WebVPN connections stuck in CLOSEWAIT state
CSCwk02928	ASA/FTD may traceback and reload in Thread Name PTHREAD
CSCwk04290	FPR 21xx - Traceback in Process Name: lina-mps during normal operations
CSCwk04492	ASA CLI hangs with 'show run' with multiple ssh sessions
CSCwk05800	ASA/FTD SNMP polling fails due to overlapping networks in snmp-server host-group
CSCwk05826	nscd: Stack-based buffer overflow in netgroup cache If the Name Servi
CSCwk05828	nscd: netgroup cache may terminate daemon on memory allocation failure
CSCwk05851	"set ip next-hop" line deleted from config at reload if IP address is matched to a NAME
CSCwk06564	Add New Syslog for Routes for NP add/delete
CSCwk06573	Serviceablity : Improve routing infra debugs and add new for error conditions
CSCwk07934	Clock skew between FXOS and Lina causes SAML assertion processing failure
CSCwk08241	FTD is not resolving FQDN for ACLs intermittently
CSCwk08476	FTD/ASA traceback and reload due to 'show bgp summary' memory leak
CSCwk08576	command to print the debug menu setting of service worker
CSCwk10884	Connectivity failure due to mismatch between l2_table and subinterface mac address
CSCwk11983	High LINA CPU observed due to NetFlow due to 'flow-export delay flow-create' configuration
CSCwk12497	Traceback and reload on active unit due to HA break operation.
CSCwk12673	TCP Session Interrupted if Keep-Alive with 1 Byte is Received
CSCwk12698	SNMP polling of admin context mgmt interface fails to show all interfaces across all contexts
CSCwk13631	Traceback and reload during FTD upgrade due to FQDN network object NAT

Bug ID	Headline
CSCwk13812	ASA/FTD incorrectly forwards extended community attribute after upgrade.
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
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.
CSCwk20823	High Snort3 CPU as encrypted traffic isn't allow listed when TSID enabled
CSCwk20882	ESP sequence number of 0 being sent after SA establishment/rekey
CSCwk21561	Add warning message when configuring CCL MTU
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
CSCwk22993	In the Linux kernel, the following vulnerability has been resolved: t
CSCwk24176	FTD/ASA - VPN traffic flowing through the device may trigger tracebacks and reloads.
CSCwk25117	ENH: Add application support for blocking consecutive AAA failures on LINA
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
CSCwk25759	In the Linux kernel, the following vulnerability has been resolved: B
CSCwk25761	In the Linux kernel, the following vulnerability has been resolved: b
CSCwk25762	In the Linux kernel, the following vulnerability has been resolved: i
CSCwk25764	In the Linux kernel, the following vulnerability has been resolved: H
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
CSCwk27830	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwk27965	Safety Net for Infinite Recursion Crashes due to Bad Stream TCP State in Post-ACK mode
CSCwk31371	NAT_HARDEN: CGNAT breaks when mapped ifc is configured as any

Bug ID	Headline
CSCwk32501	256/1550 block depletion process fover_thread
CSCwk35710	FTD/LINA may traceback and reload when "show capture" command is executed in EEM script
CSCwk36312	High cpu on "update block depletion" causing BGP flap terminated on FTD
CSCwk39974	Umbrella registration status is not synced to newly added data nodes
CSCwk40726	FMC REST API calls to get AC policy data times out, AC policy GUI slowness with larger rule query
CSCwk41065	Product Upgrades page showing 'Unknown Family 66' for FMC upgrade packages
CSCwk44245	In the Linux kernel, the following vulnerability has been resolved: i
CSCwk44246	In the Linux kernel, the following vulnerability has been resolved: i
CSCwk45975	TLS1.3 Decryption configuration on SSL policy is affecting DND traffic.
CSCwk48975	Packet-tracer output incorrectly appends 'control-plane' to drops for data-plane access-group
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
CSCwk56388	GRE traffic getting dropped after failover
CSCwk56443	Network address API calls taking long time to complete
CSCwk57933	Vulnerabilities in linux-kernel CVE-2023-52439
CSCwk57949	Vulnerabilities in linux-kernel CVE-2023-52435
CSCwk59458	21xx: debug log process hangs preventing recovery from stuck writing operations
CSCwk61157	FTD LINA Traceback and Reload dhcp_daemon Thread
CSCwk62297	Evaluation of ssp for OpenSSH regreSSHion vulnerability
CSCwk62381	ASA might traceback and reload due to ssh/client hitting a null pointer while using SCP.
CSCwk63733	HA-monitored interfaces are going into "waiting" state and subsequently to "Failed"
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)
CSCwk68759	Split brain issue in HA failover due to which outage happened on customer network

Bug ID	Headline
CSCwk71866	ASA: Site-to-Site VPN between contexts on the same device drops traffic due to 'ipsec-tun-down'
CSCwk71992	BlastRADIUS vulnerability phase-1 fix for pix-asa - Message Authenticator
CSCwk75030	The IPv6 implementation in the Linux kernel before 6.3 has a net/ipv6/
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
CSCwk75956	ASA/FTD may traceback and reload in Thread Name SSH
CSCwk76142	ASA crashing in thread PIX Garbage Collector with inspect-rtsp enabled.
CSCwk77241	Traffic outage due to 9k block depletion (tcpmod proc) observed on FPR 3100 (HA)
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
CSCwk89836	ASA/FTD may traceback and reload in Thread Name 'strlen'
CSCwk90679	Radius Authentication test fails due to missing radclient command
CSCwk94382	FTD: Lina might fail to respond to CONFIG_XML_REQUEST leading to stuck deployments
CSCwk98990	Large number of stats files can cause events to be delayed
CSCwm01544	Lina traceback and reload in data-path thread
CSCwm02801	Unstable HA causing depolyment failure
CSCwm04650	Increase memory usage leading to tracebacks in Lina.
CSCwm05155	Snort AppID incorrectly identifies SSH traffic as Unknown
CSCwm05520	Disable cluster syn cookie decoding when FTD cluster is deployed with inline-set
CSCwm07389	CGroups errors in ASA Syslog during every reboot
CSCwm12434	Readiness check should be in place for larger undo/ibdata log files
CSCwm12751	In the Linux kernel, the following vulnerability has been resolved: a
CSCwm12757	In the Linux kernel, the following vulnerability has been resolved: t
CSCwm12909	An issue was discovered in the C AMQP client library (aka rabbitmq-c)
CSCwm13141	FTD CLISH/CLI gets locked up when trying to run any show command

Bug ID	Headline
CSCwm13199	SIP traffic is affected due to unexpected behavior with NAT untranslations.
CSCwm14509	Wrong drops seen with Invalid length for 23, 24 and 25 IE-Types during GTP inspection
CSCwm14561	ASA/FTD may traceback and reload in Thread Name 'fover_parse'
CSCwm14729	HW: 3110 not rebooting after power outage, requiring manual power cycle
CSCwm29469	FMC GUI has a limitation to display only 50 SSH rules for FTD (Under platform settings >> SSH)
CSCwm31193	Events or stats are missing after EventHandler logs "Error loading input module"
CSCwm36646	After FMC upgrade results in standby FTDv losing its performance tier for FTD HA
CSCwm42745	Dynamic Site-to-Site tunnels stuck in IN-NEG state When IKE_AUTH Is Missed

Resolved Bugs in Version 7.2.8.1

Table last updated: 2024-08-26

Table 20: Resolved Bugs in Version 7.2.8.1

Bug ID	Headline
CSCwk62296	Address SSP OpenSSH regreSSHion vulnerability

Resolved Bugs in Version 7.2.8

Table last updated: 2024-06-24

Table 21: Resolved Bugs in Version 7.2.8

Bug ID	Headline
CSCwh83021	ASA/FTD HA pair EIGRP routes getting flushed after failover
CSCwj86116	High LINA CPU observed due to NetFlow configuration
CSCwj86341	Threat Defense Upgrade wizard is unable to initiate hotfix installation on FTD clusters

Resolved Bugs in Version 7.2.7

Table last updated: 2024-04-29

Table 22: Resolved Bugs in Version 7.2.7

Bug ID	Headline
CSCwi63113	FTD Boot Loop with SNMP Enabled after reload/upgrade

Resolved Bugs in Version 7.2.6

Due to CSCwi63113, Version 7.2.6 was deferred on 2024-04-29 and is no longer available for download. If you downloaded it, do not use it. If you are running this version, upgrade. The bugs listed here are also fixed in Version 7.2.7.

Table last updated: 2024-04-22

Table 23: Additional Resolved Bugs in Version 7.2.6-168 (Management Center Only)

Bug ID	Headline
CSCwj66339	OGO changing the order of custom object group contents causing an outage at static NAT

Table last updated: 2024-07-26

Table 24: Resolved Bugs in Version 7.2.6-167 (All Platforms)

Bug ID	Headline
CSCvg00130	FTD RA VPN: Rename of IP Address Pool and connection Profile name together causes deployment failure
CSCvj09334	ASA syslog 113005 does not show the user's IP address
CSCvo58100	Incorrect validation msg - Invalid value supplied for input parameter : "?"
CSCvo67978	'test aaa authentication' command shows wrong timeout value
CSCvr50778	FDM does not deploy 'crypto ikev1 am-disable' when aggressive mode is to be disabled
CSCvt43334	Cores generated due to expected/graceful shutdown need to be cleaned up
CSCvu95526	Disable "ca-check" option should be available on FDM
CSCvw31514	ASA is unable to establish SSL connectivity to servers using Self-signed certificate
CSCvx09047	Enabling SSO feature with no/wrong configuration restarts auth-daemon process constantly
CSCvx21458	FMC shows error when editing prefix-list attached to active route-map within BGP protocol
CSCvx37329	Remove Syslog Messages 852001 and 852002 in Firewall Threat Defense
CSCvx44261	SNMPv3: Special characters used in FXOS SNMPv3 configuration causes authentication errors
CSCvx52042	Upgrade to 6.6.1 got failed at 800_post/1025_vrf_policy_upgrade.pl
CSCvx52944	ASA show tech should include recent messages from dpdk.log in the flash
CSCvx69675	FXOS Major Faults about adapter host and virtual interface being down
CSCvy11606	Error Loading Data: Couldnt resolve few of the STDACE BBs

Bug ID	Headline
CSCvy79686	FMC does not broadcast administrator user session end for Realms in a non-leaf FMC Domain
CSCvz56980	Getting Unprocessable URL categories objects when using API call
CSCvz71215	FMC is pushing SLA monitor commands in an incorrect order causing deployment failure.
CSCvz92730	Block snmpd process from getting spawned under FTD pmtool
CSCwa22766	FMC4500/4600 shows virtual license
CSCwa36703	Post FMC upgrade, event data migration task never ends, and shows no progress
CSCwa70323	Unable to push extra domains >1024 Character, as part of Custom Attribute under Anyconnect VPN
CSCwa93215	Primary node disconnected from VPN-Cluster when performed HA failover on Primary with DNS lookup
CSCwa95060	"SFDataCorrelator:Parser [ERROR] Syntax error" on FTD device
CSCwb06575	Windows 11 OS is not selectable when creating a DAP record via FMC
CSCwb41189	LINA time-sync correction
CSCwb55243	snort3 crashinfo sometimes fails to collect all frames
CSCwb61402	FMC: LDAP shell login may fail if LDAP server is slow to query the DNS servers for users
CSCwb61408	FMC: Did not remove unneeded shell external auth users from /etc/passwd
CSCwb71519	ENH: F1661 More details on failure reason and log location
CSCwb75691	DBCheck.pl shows warnings for "health_alarm_static.healthmon_module_id"
CSCwb79062	FMC GUI not displaying correct count of unused network objects
CSCwb80789	TLS 1.3 connections to sites previously decrypted may fail
CSCwb85132	The Device Upgrade page might fail to load when device selection has FTD clusters / HA pairs
CSCwb94431	MFIB RPF failed counter instead of Other drops increments when outgoing interface list is Null
CSCwb95850	Snort down due to missing lua files because of disabled application detectors (PM side)
CSCwc13477	FMC | Interface update Failed. Could not find source interface
CSCwc15032	Unable to configure suppression/threshold for an intrusion rule

Bug ID	Headline
CSCwc30573	Deployment/Tasks Button not seen FMC_UI while doing upgrade tests configured in Light theme
CSCwc31953	Prevention of RSA private key leaks regardless of root cause.
CSCwc39525	FMC HA status alert "degraded - maintenance" seen periodically after upgrade
CSCwc41805	Correlation events matching on Intrusion Event Inline Result does not work properly
CSCwc49655	FTPS getting ssl3_get_record:bad record type during connection for KK and DR rules
CSCwc59564	HA Serviceability Enh: Adding HA heartbeat module in data-plane
CSCwc60227	FMC-GUI bypass session timeout while staying in any Event tab if Refresh Interval is enabled
CSCwc74271	Auth-Daemon process is getting restarted continuously when SSO disabled in HA setup
CSCwc78689	Cannot save realm configuration unless AD Join Password is empty
CSCwc78697	Device is not marked as dirty when Store Fewer Events on FMC or data plane logging is enabled in SAL
CSCwc88118	Identity policy took long time to display the available port menu
CSCwc93687	Error message while editing ACP
CSCwc94148	Deploy page fails to load if any FTD cluster or HA device state is not proper in DB
CSCwc98050	ASAv- management interface config from controller Node not replicated to newly joined data Node
CSCwd03246	UI does not respect session timeout when in real time mode
CSCwd04436	User/group download may fail if a different realm is changed and saved
CSCwd07098	25G CU SFPs not working in Brentwood 8x25G netmod
CSCwd10121	Invalid query seen in MonetDB merovingian.log
CSCwd10822	Failover trigger due to Inspection engine in other unit has failed due to disk failure
CSCwd14432	"Inspection Interruption" is seen as YES but snort3 didn't restart
CSCwd24106	ISE Connection Monitor shows inaccurate alert status
CSCwd29891	No events for FPR1010 chassis temperature on health monitor
CSCwd30298	FTD: FTPS Data Channel connection impacted by TLS Server Identity and Discovery Probe sent by FTD
CSCwd31806	ASAv show crashinfo printing in loop continuously

Bug ID	Headline
CSCwd32952	Active and Standby device details not available in FMC logs during FTD HA break
CSCwd34079	FTD: Traceback & reload in process name lina
CSCwd34413	SEC-WEB-CLCKJACK failure on FMC: frame ancestors directive missing
CSCwd39506	SSL Policy DND default Rule fails on error unsupported cipher suite and SKE error.
CSCwd41986	Packet-Tracer interfaces not showing up in UI after updating interface name from lower to upper case
CSCwd42072	SRU installation failure.
CSCwd42347	FMC not showing any alerts/warnings when deploying changes of prefix list with same seq #
CSCwd45451	FMC: Script to change hostname/IP on FTD's when FMC's Ip/hostname is changed
CSCwd46182	Periodic sync failures are not reported to users
CSCwd46780	ASA/FTD: Traceback and reload in Thread Name: appAgent_reply_processor_thread
CSCwd53635	AWS: SSL decryption failing with Geneve tunnel interface
CSCwd55642	Stale CPU core health events seen on FMC UI post upgrade to 7.0.0+.
CSCwd56296	FTD Lina traceback and reload in Thread Name 'IP Init Thread'
CSCwd57927	FMC UI may become unavailable and show "System processes are starting" message after upgrade
CSCwd62729	FDM QW/QP: All URL traffic blocked in BAT/BQT test
CSCwd65598	cdFMC: SFDataCorrelator cores and user to group map not updated on sensor
CSCwd65781	Saving capture with special characters fails to download - Error Timed out
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
CSCwd75782	FMC External Auth test error "Encryption method is configured but you did not upload a certificate."
CSCwd77581	Cisco ASA and FTD ICMPv6 Message Processing Denial of Service Vulnerability
CSCwd78940	Traps are not getting generated in UUT for config change in multicontext
CSCwd80284	Import/export fails with backend error
CSCwd81538	FTD Traffic failure due to 9344 block depletion in peer_proxy_tx_q

Bug ID	Headline
CSCwd83141	CCL/CLU filters are not working correctly
CSCwd83441	FMC should display the status of physical FTD interfaces bundled in port-channel
CSCwd84046	Microsoft SCEP enrollment fails to get ASA identity cert - Unable to verify PKCS7
CSCwd85073	Snort3 stream core found init_tcp_packet_analysis
CSCwd86226	Standby FMC show FMC-HA as healthy when Active unit Sybase is down
CSCwd86783	Disabling NAVL guids from userappid.conf doesn't work
CSCwd87129	seeing error on access policies on FMC - "Error during policy validation"
CSCwd87438	Enhance logging mechanism for syslogs
CSCwd89811	Traffic fails in Azure ASAv Clustering after "timeout conn" seconds
CSCwd91013	FMC | Deployment failure in csm_snapshot_error
CSCwd93316	No Inspect Interruption warning when deploy after FMC upgrade
CSCwd93376	Clientless VPN users are unable to download large files through the WebVPN portal
CSCwd95043	Cisco ASA and FTD VPN Web Client Services Client-Side Request Smuggling Vulnerability
CSCwd97020	ASA/FTD: External IDP SAML authentication fails with Bad Request message
CSCwd99592	Optimization of Side Bar loading for HealthMon page
CSCwe01977	ASA/FTD may traceback and reload after a reload with DHCPv6 configured
CSCwe03631	Need to provide rate-limit on "logging history <mode>"
CSCwe04746	Unexpected "No Traffic" health alert on Standby HA Data Interface where no data flows
CSCwe06826	Email alert incorrectly send for a successful database backup
CSCwe10872	Internal Error while editing PPPoE configurations
CSCwe11754	Nodes randomly fail to join cluster due to internal clustering error
CSCwe12645	Secondary state flips between Ready & Failed when node is rebooted and mgmt interface is shutdown
CSCwe13627	FMC Unable to fetch VPN troubleshooting logs.
CSCwe14062	FTD/Lina or ASA traceback and reload related to thread ctm_qat_engine
CSCwe14590	FMC deployment preview showing full config instead of delta.

Bug ID	Headline
CSCwe16730	Deployment failing - "Error while printing show-xml-response file contents" XML response too big
CSCwe18446	Support cluster pending_rejoin in virtual platform FTDv
CSCwe18472	[FTD Multi-Instance][SNMP] - CPU OIDs return incomplete list of associated CPUs
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 */; *"
CSCwe21037	Snort mem used alert should be consistent with value from top.log
CSCwe21831	add warning to FTD platform settings when VPN Logging Settings logging level is informational
CSCwe22254	After disabling malware analysis, high disk usage on /dev/shm/snort
CSCwe22431	[SXP-UserIP Muted Leader]FMC HA Join flushes FW IP_SGT Mapping and restreams in registered sensors.
CSCwe25154	KP - core.SAMsgThread core created while HA switchover in multicontext
CSCwe25187	FMC External authentication getting "Internal error"
CSCwe26342	ASA Traceback & reload citing thread name: asacli/0
CSCwe26612	FTD taking longer than expected to form OSPF adjacencies after a failover switchover
CSCwe27503	Logging class Support for routing
CSCwe28362	Copy and pasting rules is broken and give blank error message in ID policy
CSCwe28912	FPR 4115- primary unit lost all HA config after ftd HA upgrade
CSCwe29381	Sybase arbiter is not up on FMC HA
CSCwe29498	occasional failure to load light-modal-ac-rule-xx.css with a net::ERR_TOO_MANY_RETRIES error
CSCwe30359	Traffic drops with huge rule evaluation on snort
CSCwe30687	dvti memory leak on mp_counter_alloc
CSCwe33282	FTD: The upgrade was unsuccessful because the httpd process was not running
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]
CSCwe38353	stream_tcp PDUs does not capture vlan ID

Bug ID	Headline
CSCwe39514	Host cache logs flooding the box
CSCwe41766	FTD may not reboot as expect post upgrade if bundled FXOS version is the same on old and new version
CSCwe42582	Error thrown on AC Rule creation/update and save after index creation
CSCwe43965	Remove the limit of 30characters in the rule name which a rule is moved from ACP to Prefilter
CSCwe45211	Need to Warn the users before triggering a full deployment on FTD managed by FDM
CSCwe45879	Frequent errors seen regarding failures to load bulkcsv files that don't exist
CSCwe47485	FTD: CLISH slowness due to command execution locking LINA prompt
CSCwe48997	FDM: Cannot create multiple RA-VPN profiles with different SAML servers that have the same SAML IDP\u2028
CSCwe49185	Generate password does not meet requirements while in CC mode
CSCwe51296	Not able to remove group policy from RAVPN via REST API
CSCwe51489	Unable to process query error on events; FMC UI; monetdb maximum connections reached
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
CSCwe54999	Protocol Down with lower CPU instances on ESXi 8 for ASAv and FTDv
CSCwe55556	logging is getting disabled if ssl rules are reordered
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
CSCwe58323	FMC EIGRP 'For input string: "route-map"' error when configuring EIGRP post 7.2 upgrade
CSCwe58620	FMC Connection Events page "Error: Unable to process this query. Please contact support."
CSCwe58635	Readiness Check Failed [ERROR] Fatal error: Enterprise Object integrity check failed with errors
CSCwe58980	/var/sf/QueryPoolData fills up with warehouse directories
CSCwe59664	DAP policy created in FMC Gui, to detect a Windows OS with a hotfix, will not work as expected

Bug ID	Headline
CSCwe59889	Create Identity Services Engine via API returns 404 Client Error: Not Found
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
CSCwe62951	FSIC db include Python byte-code files and can result in health alert and system integrity failure.
CSCwe63493	Post backup restore multiple processes are not up. No errors are observed during backup or restore.
CSCwe63759	Cluster hardening fixes
CSCwe66137	SSO user gets logged in to FMC UI if a valid local user credentials are pre-populated in the browser
CSCwe66360	Snort3 out of memory and process exit unexpectedly due to memory not released by flows
CSCwe67180	FTD HA app-sync failure, due to corruption in cache files.
CSCwe69388	FMC should push the AnyConnect Custom attribute defer keyword as lowercase instead of capitalized
CSCwe69824	validation check on FMC GUI causing issue and throwing error when adding new NAT objects
CSCwe71084	IN clause does not work for externalization queries after upgrading to 7.0.x
CSCwe71238	Requests from intelligence page fail after RMQ was stopped for some time
CSCwe72330	FTD LINA traceback and reload in Datapath thread after adding Static Routing
CSCwe74899	CD App Sync error is App Config Apply Failed on Secondary/Standby after backup restore on RMA device
CSCwe75055	[FMC model migration] Health monitoring on FMC reporting errors
CSCwe75267	Cannot Force Break FTD HA Pair
CSCwe76036	ndclientd error message 'Local Disk is full' needs to provide mount details which is full
CSCwe78377	Network Discovery: Performance issues caused by the use of \u2018any\u2019 network object in the rules
CSCwe78674	User Group Download fetches less data than available or fails with "Size limit exceeded" error
CSCwe79954	LDAP External auth config fails to deploy to FTD if same LDAP server is added as Primary and backup
CSCwe80273	FMC device search page removes FTD from the groups and put them back to ungrouped

Bug ID	Headline
CSCwe80915	Intrusion Event Information under statistics tab is empty
CSCwe81135	ac-policy rule section showing non-existing index page in old ac-policy UI
CSCwe81449	Moving the app-agent logging to asynchronous logging mechanism(Same as SNMP).
CSCwe81841	FXOS needs to provide a command that will display the total power on hours of chassis/blade
CSCwe82631	FMC isn't allowing to create more than 30 VLAN interfaces
CSCwe82766	[Azure FMCv] Deployment with SSH key option is not adding the keys correctly.
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
CSCwe86029	FMC system restore authentication error during FMC re-image when using FTP/SCP protocol
CSCwe86350	email alert to scheduled activity is not working after upgrading to 7.2
CSCwe86687	Apache Commons FileUpload before 1.5 does not limit the number of reques
CSCwe86690	In Apache MINA, a specifically crafted, malformed HTTP request may cause
CSCwe86693	An issue in protobuf-java allowed the interleaving of com.google.protobu
CSCwe86923	In Apache MINA, a specifically crafted, malformed HTTP request may cause
CSCwe87134	ASA/FTD: Traceback and reload due to high rate of SCTP traffic
CSCwe87789	Script to trigger HA when RSS memory threshold exceeds configurable threshold
CSCwe87831	FMC UI response is very slow: Add health module monitoring FMC ntpd server(s) accessibility
CSCwe88496	"Failed to convert snort 2 custom rules. Refer /var/sf/htdocs/ips/snort.rej for more details."
CSCwe88802	FTD readiness and upgrade passed with exception log as ProgressReport' has no attribute 'KB_UNIT'
CSCwe88808	FMC UI stuck after completing compatibility check
CSCwe89024	FTS under AC Policy Listing page with 'obj' gives Error Moving Data error with CTS DB
CSCwe89305	vFMC300 to FMC2600 migration failure with error "migration from R to N is not allowed"
CSCwe89818	External Auth on FMC may throw err "Can't use string ("") as a HASH ref while "strict refs" in use"

Bug ID	Headline
CSCwe90168	Unable to Access FMC GUI when using Certificate Authentication
CSCwe90195	Local rules are not seen in the UI after converting from Snort2 to Snort3 in 7.2.4-82 FMC
CSCwe90596	Elephant flow detection disabled on FMC, getting enabled on FTD after random deployment
CSCwe91652	Database backup failed on KVM FMC
CSCwe91738	improve serviceability to handle TLS 1.3 only flows when TLS 1.3 decryption is not enabled
CSCwe91958	correlation events based on connection events do not contain Security Intelligence Category content
CSCwe92723	Phase 2 NAP delay seen in 7.0.1 while deploying policy
CSCwe93061	FTD returns no output of "show elephant-flow status" when efd.lua file's content is empty
CSCwe93137	KP - multimode: ASA traceback observed during HA node break and rejoin.
CSCwe93162	FP1140 7.0.4 Deployment keep failing with error "Can\'t use an undefined value as a HASH reference"
CSCwe93489	Threat-detection does not recognize exception objects with a prefix in IPv6
CSCwe93566	need to turn off default TLS 1.1 (deprecated) support for the FDM GUI
CSCwe93736	ASA not updating Timezone despite taking commands
CSCwe94789	Umbrella DNS Negate of Bypass Domain Field is not generated from FMC
CSCwe95729	Cisco ASA & FTD SAML Authentication Bypass Vulnerability
CSCwe95797	SecureX page in FMC GUI blank after FMC upgrade
CSCwe97094	Cross launching packet tracer from Unified Events page
CSCwe97939	ASA/FTD Cluster: Change "cluster replication delay" with max value increase from 15 to 50 sec
CSCwe98319	ASAConfig multiple restarts are leaking 16K memory in every Restart leading to ZMQ Out Of Memory.
CSCwe98430	AC policy deploy failing on 7.2.4 FMC to 6.7 FTD
CSCwe98435	Selective policy deploy with Identity Policy (captive-portal) and SSL Policy (dp-tcp-proxy) CLI
CSCwe99905	Getting an error while saving report template
CSCwf00483	Found Orphaned SFTop10Cacher processes

Bug ID	Headline
CSCwf00514	RRD files cannot be updated if the timestamp is ahead of time as a result of a system clock drift
CSCwf00736	CSM backup failed within FMC backup due to modification of file while tar was reading it
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
CSCwf02005	ActionQueue task sandbox data update throws SQL Error post 7.2.4 upgrade
CSCwf02453	reload-threshold should not be an option under show memory
CSCwf03345	Recovery from RMU failures due to control link going to bad state
CSCwf03912	New CLI for config clu_update/keepalive interval
CSCwf04915	FP1000:Update LINA asa.log files to avoid recursive messages-<date>.1.gz rotated filenames
CSCwf06255	7.2.4-129 - GCP cluster - health check failures
CSCwf06261	Health Monitoring exports negative snort swap memory metric value
CSCwf06318	Readiness check needs to be allowed to run without pausing FMC HA
CSCwf08320	SSE does not update relevant information after first discovery of an asset.
CSCwf08387	LSP version not updated to latest in LINA Prompt in SSP_CLUSTER with 7.2.4 build.
CSCwf08790	FMC Restore of remote backup fails due to no space left on the device
CSCwf09024	Misleading trace log about state transition
CSCwf10295	Snort3 is not closing the pcap file handle and disk is getting full
CSCwf10422	"Security Intelligence feed download failed" displayed even though it succeeded
CSCwf11877	TPK 3110 - Firmware version MISMATCH after upgrade to 7.2.4-144
CSCwf12521	Unable to load intrusion policy page on FMC GUI
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)
CSCwf14257	FTD container restored from backup fails to register to FMC due to Peer send bad hash error
CSCwf15532	HA Sync Failed health alert generated for both FMC units in HA pair - HA subsequently recovered

Bug ID	Headline
CSCwf15863	Very specific "vpn-idle-timeout" values cause continuous SSL session disconnects and reconnects
CSCwf15978	xml2js version 0.4.23 allows an external attacker to edit or add new pro
CSCwf16679	HA Serviceability Enh: Maintain HA NLP client stats and HA CTL NLP counters for current App-sync
CSCwf17389	ASA accepts replayed SAML assertions for RA VPN authentication
CSCwf18144	Firepower hotfixes should not be allowed to install when already installed previously
CSCwf19562	Changes to lamplighter logs written to /var/log/tid_process.log
CSCwf19621	Unable to edit name or inspection mode of intrusion policy
CSCwf19681	Secondary FMC should allow edit of FTD IP/hostname details under device tab
CSCwf20215	admin user should be excluded from CLI shell access filter
CSCwf20958	No logrotate and max size is configured for Health.log file
CSCwf21204	DBCheck shouldn't run against MonetDB if user is collecting config backup alone
CSCwf22241	Security zones are not showing in AC policy UI
CSCwf22568	FTD HA Creation fails resulting in devices showing up in an inconsistent state on the FMC
CSCwf22637	Network Object Group overrides not visible or be edited from FMC GUI
CSCwf22854	Not able to add files with file names which has '\u' to clean list from Malware Summary page
CSCwf23997	Upgrade readiness check shows failed in GUI for all sensors due to sensor display name characters.
CSCwf24818	Unable to change admin user password after FMC migration if it had LOM access
CSCwf25144	FMC backup management page showing "Verifying Backup" for FTD sensors.
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
CSCwf26264	FMC backup restore page takes around 5 mins to load when remote storage is unreachable
CSCwf26350	User is not informed of the dependent IPS when policy import fails.
CSCwf28063	SSE disconnect breaks cloud lookups after restoration.

Bug ID	Headline
CSCwf30542	Snort3 crash found during cleaning up a CHP object
CSCwf30824	Add CIMC reset as auto-recovery for CIMC IPMI hung issues
CSCwf32890	Standby FMC SSH connection getting disconnected frequently.
CSCwf33904	[IMS_7_4_0] - Virtual FDM Upgrade fails: HA configStatus='OUT_OF_SYNC after UpgradeOnStandby
CSCwf34123	Reordering columns in report designer is glitchy when using Atomic
CSCwf34892	Flooding log in trace file , fo_chk_peer_down_ifcs
CSCwf35173	SFTunnel Fails to Properly Establish due to running_config.conf file misconfiguration
CSCwf35223	SGT Troubleshooting the ability to correlate to IP Address
CSCwf35233	Cisco Adaptive Security Appliance Software and Firepower Threat Defense DoS
CSCwf35346	FMC should handle error appropriately when ISE reports error during SXP download
CSCwf35500	FXOS/SSP: System should provide better visibility of DIMM Correctable error events
CSCwf36011	Drop rule is not being removed when snmp unification on blade is removed.
CSCwf36391	Third heartbeat packet is not sent before declaring the application health failure
CSCwf36419	ASA/FTD: Traceback and reload with Thread Name 'PTHREAD'
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
CSCwf40594	Wyoming/SFCN ASA: Wrong values shown DBRG in show crypto ssl objects CLI
CSCwf40674	REST API [PUT]: PC called without h/w config, existing h/w config is set to null in the DB
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
CSCwf42234	S2S dashboard SVTI tunnel details are missing after upgrade
CSCwf43033	diskmanager silo covering /var/sf/htdocs/img/dashboard/no-cache/ needs much lower hwm and lwm

Bug ID	Headline
CSCwf43247	NMAP Remediation scan tasks remain in pending state in action queue table, does not clear out
CSCwf43850	ECMP + NAT for ipsec sessions support request for Firepower.
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
CSCwf45106	securex sse integration needs instructions updated
CSCwf49254	cannot unregister FTD from Cisco Cloud in FDM if already unregistered/unenrolled from cloud side
CSCwf49640	Show dns ip-cache has old bids after switching snort versions, which affects path-monitoring output.
CSCwf52810	ASA SNMP polling not working and showing "Unable to honour this request now" on show commands
CSCwf53210	[Enhancement] No of config archives should be configurable from UI
CSCwf55014	serviceability improvement for CSCwe28912 where HA state in failed state.
CSCwf55236	Unable to delete custom rule group even when excluded from all the ips policies
CSCwf56291	FMC config archives retention reverts to default if ca_purge tool was used prior to 7.2.4 upgrade
CSCwf56404	ca_purge tool needs to restart Tomcat
CSCwf57315	Reconcile FMC state: FMC Upgrade needs to create upgrade status file to support FTD Upgrade guards.
CSCwf57850	TelemetryApp process keeps exiting every minute after upgrading the FMC
CSCwf57856	FXOS Traceback and reload caused by leak on MTS buffer queue
CSCwf59176	FXOS raises a fault for administratively disabled management interface
CSCwf59571	FTD/Lina - ZMQ issue OUT OF MEMORY. due to less Msglyr pool memory on certain platforms
CSCwf59643	FTD: HA App sync failure due to fover interface flap on standby unit
CSCwf62103	FMC needs to properly validate QoS policy rules before allowing deployment to FTD
CSCwf62729	Cisco ASA/FTD Firepower 2100 SSL/TLS Denial of Service Vulnerability
CSCwf63358	FTD Diskmanager.log is corrupt causing hm_du module to alert false high disk usage

Bug ID	Headline
CSCwf63589	FTD snmpd process traceback and restart
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
CSCwf66271	Unable to list down the interface under the device exclude policy
CSCwf66307	The exclude policy to exclude interface status will be removed on FMC after a while
CSCwf66333	Selecting "All interfaces " under FTD exclude policy for interface status module doesn't work
CSCwf66387	[IMS_7_4_0] FTD revert fails "The management state validation cannot be done, Cannot revert"
CSCwf67337	FMC taking long times to save override objects even if not modified
CSCwf68335	vFMC: Scheduled deployment failing
CSCwf69313	Correlation events for Connection Tracker <, <=, = or != rules show data for unrelated connections
CSCwf69475	Transfer Packets option change to NO automatically when change the device name in device management
CSCwf71602	FMC not generating FTD S2S VPN alerts when down or idle
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
CSCwf77995	Azure FTDv, managed locally by FDM, goes in boot cycle/reload loop after the first deployment
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
CSCwf81320	Unable to configure and deploy IPv6 DNS server for RAVPN in FMC 7.2.4
CSCwf82093	When communications are disabled for FTD from FMC UI backend shows connection is staying enabled.
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

Bug ID	Headline
CSCwf82644	SI Feeds get downloaded despite the feed updates being user disabled
CSCwf84588	Disable TLS 1.1 permanently for sftunnel communication
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
CSCwf86860	FMC GUI | ACP page gets blank and hang while doing search in rules and moving to last pages
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
CSCwf88124	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
CSCwf91381	Adi: Log specific host FQDN used for bulk download and websocket connections
CSCwf92047	ENH: FMC, Disable 'create client' under eStremer tab in the GUI when it is running in UCAPL mode
CSCwf92182	Cisco Firepower Management Center Software SQL Injection Vulnerability
CSCwf92439	Deployment blocked due to port object with IP range max limit 131838 in NAT64
CSCwf92661	ASA|FTD: Traceback & reload due to a free buffer corruption
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
CSCwf95288	FPR1k Switchport passing CDP traffic
CSCwf98546	snort minidumps no longer managed by diskmanager after moving to var/common
CSCwf99303	Management UI presents self-signed cert rather than custom CA signed one after upgrade
CSCwh00123	In Multi-manager scenario,cdFMC&Analytics FMC,FTD should only receive identity feeds from Config FMC
CSCwh00692	Traceback @<capture_file_show+605 at ../infrastructure/capture/capture_file_finesse.c:282>
CSCwh02561	Port-channel interface speed changes from 10G to 1G after a policy deployment

Bug ID	Headline
CSCwh04185	Snort crash in active response
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
CSCwh08215	Upgrade from 7.2.x to 7.2.5 may fail if there is null value observed in speed/duplex in interface
CSCwh08388	FMC GUI Not Saving Interface Settings
CSCwh08403	FMC HA - Health Policy - Applied count shows "0" appliance
CSCwh08481	ASA traceback on Lina process with FREEB and VPN functions
CSCwh08683	FTDv/AWS - NTP clock offset between Lina and FTD cluster
CSCwh09113	FPR1010 in HA failed to send or receive to GARP/ARP with error "edsa_rcv: out_drop"
CSCwh10087	core-compressor fails due to core filename with white space
CSCwh12009	EOStore failed error is outputted after deleting shared rule layer.
CSCwh13474	PSEQ (Power-Sequencer) firmware - remove device-id check
CSCwh13551	Encrypted Visibility Engine (EVE) dashboard tab and widgets not added to FMC GUI upon upgrade
CSCwh13625	Encrypted Visibility Engine (EVE) FMC dashboard tab and widgets not renamed after 7.1 > 7.2+ upgrade
CSCwh13821	ASA/FTD may traceback and reload in when changing capture buffer size
CSCwh14352	Lina CiscoSSL upgrade to 1.1.1v and FOM 7.3a
CSCwh14731	External authentication fails if the object name contains space characters
CSCwh14863	FTD 7.0.4 cluster drops Oracle's sqlnet packets due to tcp-not-syn
CSCwh16301	Incorrect Hit count statistics on ASA Cluster only for Cluster-wide output
CSCwh16759	SNMP is not working on the primary active ASA unit in multi-context environment
CSCwh17052	Lack of validation of string length creating object/category names using API
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

Bug ID	Headline
CSCwh19897	ASA/FTD Cluster: Reuse of TCP Randomized Sequence number on two different conns with same 5 tuple
CSCwh21337	FTD - Issue with the LSP package code during deploy rollback.
CSCwh21474	ASA traceback when re-configuring access-list
CSCwh21772	Upgrade FxOS CiscoSSL to version 1.1.1v and FOM 7.3a
CSCwh22317	LILO validation during Readiness Check missing
CSCwh22348	sfdatacorrelator crashing due to table corruption 'rua_event_xxxxx'
CSCwh22783	Stale manager presence on FTD after failed registration to cdFMC, causes new registration to fail.
CSCwh22888	FXOS: Remove enforcement of blades going into degraded state after multiple DIMM correctable errors
CSCwh24321	FXOS: Alperton 100G NetMod not being acknowledged properly
CSCwh24826	FMC upgrade stuck at 1039_fmc_rabbitmq_enable
CSCwh24901	'Frequent drain of events (not unprocessed events) to be removed from FMC
CSCwh25928	FMC userrole missing permissions may cause Tomcat to continuously restart after upgrade to 7.2.4
CSCwh27510	Negotiation to Cold Standby taking 30mins on TPK with 900 sub-interfaces
CSCwh28007	While editing AC-policy rules, the rule order number becomes misaligned.
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
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
CSCwh30346	ASA/FTD: 1 Second failover delay for each NLP NAT rule
CSCwh30676	Ping to the configured systemIP on management interface getting failed in cluster setup.
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
CSCwh35088	Number of files lina-io starts limited to 8 because of which fover log files are missing on HA pair
CSCwh37475	Removal of msie-proxy commands during flexconfig rollback

Bug ID	Headline
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
CSCwh39258	Occasionally External auth may not work after HA failover to Active
CSCwh40106	FTD hosted on KP incorrectly dropping decoded ESP packets if pre-filter action is analyze
CSCwh41305	Snort busy drops for HTTPS traffic through VPN with less traffic - 2K depletion
CSCwh42077	Cisco_Firepower_GEODB_FMC_Update* are not included in diskmanager
CSCwh42233	Some Syslog IDs cannot be configured on Platform Settings.
CSCwh42412	FTD Block 9344 leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwh43945	FTD/ASA traceback and reload may occur when ssl packet debugs are enabled
CSCwh44215	ENH - Exempt TSID probe from going through EVE inspection
CSCwh44479	Configuration archive creation failing and causing deployment preview to throw error
CSCwh47053	ASA/FTD may traceback and reload in Thread Name 'dns_cache_timer'
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
CSCwh49244	"show aaa-server" command always shows the Average round trip time 0ms.
CSCwh50060	Some TLS1.3 probes test site cases fail due to rst+ack not sent out of FTD during timeout
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
CSCwh53745	ASA: unexpected logs for initiating inbound connection for DNS query response
CSCwh54477	The FMC is showing "The password encryption key has not been set" alert for a 11xx/21xx/31xx device
CSCwh55178	FXOS: svc_sam_dcosAG process getting crashed repeatedly on FirePower 4100
CSCwh55543	FMC 4600 v7.2.4 EVE dashboard widget showing corrupt data

Bug ID	Headline
CSCwh56218	ASA: Traceback and reload during 6 nodes cluster synchronization after CCL link failure/recovery
CSCwh57976	Improve CPU utilization in ssl inspection for supported signature algorithm handling
CSCwh58467	ASA does not sent 'warmstart' snmp trap
CSCwh58490	FMC Deployment failed due to internal errors after upgrade
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
CSCwh60504	LINA would randomly generate a traceback and reload on FPR-1K
CSCwh60604	ASA/FTD may traceback and reload in Thread Name 'lina' while processing DAP data
CSCwh60631	Fragmented UDP packet via MPLS tunnel reassemble fail
CSCwh60778	FTD traceback and reload within TLS tracker for TLS 1.3 SSL decryption
CSCwh60783	FTD - Captive portal enabled is still running despite the feature is off
CSCwh62731	FTD Upgrade from 6.6.5 to 7.2.5 removing OGS causing rule expansion on boot
CSCwh63588	FTD SNMPv3 host configuration gets deleted from IPTABLES after adding host-group configuration
CSCwh64704	FDM should provide a way to disable WebVPN portal on FTD
CSCwh65128	LINA show tech-support fails to generate as part of sf_troubleshoot.pl (Troubleshoot file)
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
CSCwh68482	FTD: Traceback and Reload in Process Name: lina
CSCwh68878	Diskmanager process terminated unexpectedly
CSCwh69346	ASA: Traceback and reload when restore configuration using CLI
CSCwh69777	FTD - Incorrect High SNORT memory utilization display with TLS server identity
CSCwh70323	Timestamp entry missing for some syslog messages sent to syslog server
CSCwh70481	Community string sent from router is not matching ASA
CSCwh70905	Secondary lost failover communication on Inside, using IPv6, but next testing of Inside passes

Bug ID	Headline
CSCwh71161	ASA|FTD: Traceback & reload in thread Name: update_mem_reference
CSCwh71589	Coverity 886745: OVERRUN in verify_generic_signature
CSCwh71665	ASA traceback under match_partial_keyword during CPU profiling
CSCwh72522	Error while saving RAVPN withLDAP attribute map containing entry without cisco attr mapping name
CSCwh73727	Snort3 dropping IP protocol 51
CSCwh74219	Upgrade from FMC 7.2.4.1 to 7.2.5 failed at 600_schema/000_install_fmc.sh
CSCwh74586	XTLS: With TSID AC-Policy configured plugin is not disengaging immediately at CH
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
CSCwh79095	Snort generating an excessive number of snort-unified log files with zero bytes
CSCwh80131	S3_Core: crashinfo: increase buffer space to print longer function names
CSCwh83254	ASA/FTD: Traceback and reload on thread name CP Crypto Result Processing
CSCwh84376	In FPR4200/FPR3100-cluster observed core file ?core.lina? observed on device reboot.
CSCwh89289	Snort is getting reloaded during deploy due to diff in timerange and nap conf contents in each run
CSCwh89835	FMC plain-text passwords for radius server and certificate passphrase
CSCwh90018	unused interface object ids may be present in zone configuration after FTD reregistration
CSCwh90693	FTD unregisters the standby FMC immediately after a successful registration
CSCwh90813	FDM Upgrade failure due to expired certificates.
CSCwh91574	FTD: Traceback in threadname cli_xml_request_process
CSCwh93649	File copy via SCP using ciscossh stack fails with error "no such file or directory"
CSCwh93710	Last Rule hit shows a hex value ahead of current time in ASA and ASDM
CSCwh95010	Unexpected traceback on thread name Lina and device experienced reboot
CSCwh95175	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwh99331	syslog not generated "ASA-3-202010: NAT pool exhausted" while passing traffic from iLinux to oLinux

Bug ID	Headline
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
CSCwi02134	FTD sends multiple replicated NetFlow records for the same flow event
CSCwi02919	SNMP Unresponsive when snmp-server host specified
CSCwi03528	Cross ifc access: Revert PING to old non-cross ifc behavior
CSCwi06690	Certificate Encoding Issue when using AnyConnect cert Authentication/Authorisation
CSCwi07068	SFDataCorrelator logs "Killing MySQL connection" every minute, causing performance problems
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
CSCwi12772	ASA cluster traceback Thread Name: DATAPATH-8-17824
CSCwi13134	Hardware bypass not working as expected in FP3140
CSCwi14896	Node kicked out of cluster while enabling or disabling rule profiling
CSCwi15409	ASA/FTD - may traceback and reload in Thread Name 'Unicorn Proxy Thread'
CSCwi15595	ASA traceback and reload during ACL configuration modification
CSCwi16998	CCM Seq 58 - LTS18
CSCwi18581	Firewall traceback and reload due to SSH thread
CSCwi19015	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-13-6022'
CSCwi19145	FTD/ASA may traceback and reload in PKI, syslog, during upgrade
CSCwi19849	VPN load-balancing cluster encryption using Phase 2 deprecated ciphers
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
CSCwi22296	ASA: The logical device may boot into failsafe mode because of an large configuration.
CSCwi24368	Standby manager addition is failed on Primary FMC due to previous entries in table
CSCwi24370	Stale HA transactions need to be moved to failed and subsequent HA transaction needs to be created

Bug ID	Headline
CSCwi24461	Device/port-channel goes down with a core generated for portmanager
CSCwi24880	ASA dropping IPSEC traffic incorrectly when "ip verify reverse-path" is configured
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
CSCwi27402	FTD: Update WM firmware to 1023.0207
CSCwi27459	Snort Crash during selection of signature algorithm ECDSA
CSCwi29934	Cisco FXOS Software Link Layer Discovery Protocol Denial of Service Vulnerability
CSCwi31091	OSPF Redistribution route-map with prefix-list not working after upgrade
CSCwi31766	PSU fan shows critical in show environment output while operating normally
CSCwi32063	ASA/FTD: SSL VPN Second Factor Fields Disappear
CSCwi32759	Username-from-certificate secondary attribute is not extracted if the first attribute is missing
CSCwi34125	ASA: Snmpwalk shows "No Such Instance" for the OID ceSensorExtThresholdValue
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()
CSCwi38061	ASA/FTD traceback and reload due to file descriptor limit being exceeded
CSCwi38957	Policy Apply failed moving from FDM to FMC
CSCwi40487	FTD HA Failure after SNORT crash.
CSCwi40536	ASA/FTD: Traceback and reload when running show tech and under High Memory utilization condition
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
CSCwi43782	GTP inspection dropping packets with IE 152 due to header length being invalid for IE type 152

Bug ID	Headline
CSCwi45630	Snort3 traceback with fqdn traffics
CSCwi46010	ASA/FTD: Cluster incorrectly generating syslog 202010 for invalid packets destined to PAT IP
CSCwi46023	FTD drops double tagged BPDUs.
CSCwi46641	FTDv may traceback and reload in Thread Name 'PTHREAD-3744' when changing interface status
CSCwi50343	Their standalone FTD running 7.2.2 on FPR-4112 experienced a traceback on the SNMP module
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
CSCwi56048	Interface fragment queue may get stuck at 2/3 of fragment database size
CSCwi59525	Multiple lina cores on 7.2.6 KP2110 managed by cdFMC
CSCwi59831	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi62683	The SSH transport protocol with certain OpenSSH extensions, found in ... (CVE-2023-48795)
CSCwi63844	Default Umbrella DNS Policy returns an error after upgrade to FMC 7.2.5.1
CSCwi66103	Lina traceback on RAVPN connection after enabling webvpn debug
CSCwi67629	Devices might change status to "missing the upgrade package" after Readiness Check is initiated
CSCwi68083	Product Upgrades page: Download action creates a lot of "uninitialized value" error messages in log
CSCwi71786	Download failed for Available Upgrade Packages
CSCwi76002	Memory exhaustion due to absence of freeing up mechanism for tmatch
CSCwi76630	FP2100/FP1000: ASA Smart licenses lost after reload
CSCwi79703	Incorrect Timezone Format on FTD When Configured via FXOS
CSCwi80465	CCM ID 63 - LTS18
CSCwi86198	SFData correlator keep terminating on FTDs configured for IDS
CSCwi90040	Cisco ASA and FTD Software Command Injection Vulnerability
CSCwi95708	FTD: Hostname Missing from Syslog Message
CSCwi98284	Cisco ASA and FTD Software Persistent Local Code Execution Vulnerability

Bug ID	Headline
CSCwj02708	Backup generation on FDM fails with the error "Unable to backup Legacy data."
CSCwj10955	Cisco ASA and FTD Software Web Services Denial of Service Vulnerability
CSCwj16633	Issues with FMC Deployment preview (Advanced Preview)
CSCwj23444	Snort 3 Traceback on AppIdSessionApi
CSCwj62530	DOC: Need to show up 10 slots rather than 6 for the HDD for FMC4600/FMC4700
CSCwk02167	DOC: Clarify FTD revert vs uninstall, and provide examples

Resolved Bugs in Version 7.2.5.2

Table last updated: 2024-05-06

Table 25: Resolved Bugs in Version 7.2.5.2

Bug ID	Headline
CSCwe41766	FTD may not reboot as expect post upgrade if bundled FXOS version is the same on old and new version
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

Resolved Bugs in Version 7.2.5.1

Table last updated: 2024-05-22

Table 26: Resolved Bugs in Version 7.2.5.1

Bug ID	Headline
CSCvt25221	FTD traceback in Thread Name cli_xml_server when deploying QoS policy
CSCvx04003	Lack of throttling of ARP miss indications to CP leads to oversubscription
CSCwc51588	Failing to generate FMC Backup/Restore via SMB/SSH
CSCwc62215	FTD unable to sync HA due to snort validation failed
CSCwc78781	ASA/FTD may traceback and reload during ACL changes linked to PBR config
CSCwc82205	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwc99053	FDM: "failover replication http" command may disappear from FTD running config
CSCwd08098	cacert.pem on FMC expired and all the devices showing as disabled.

Bug ID	Headline
CSCwd27186	All traffic blocked due to access-group command missing from FTD config
CSCwd38196	Proxy is engaged even when we have a Definitive DND rule match
CSCwd38583	ASA/FTD: Command "no snmp-server enable oid mempool" enabled by default or enforced during upgrades
CSCwd66820	Cisco Firepower Management Center Object Group Access Control List Bypass Vulnerability
CSCwd86535	ASA/FTD: Traceback and Reload on Netflow timer infra
CSCwd89095	Stratix5950 and ISA3000 LACP channel member SFP port suspended after reload
CSCwe04043	FTD-HA upgrade failed
CSCwe12705	multimode-tmatch_df_hijack_walk traceback observed during shut/unshut on FO connected switch interfa
CSCwe18090	FMC deployment failure:"Validation failed: This is a slav*/ha standby device, rejecting deployment."
CSCwe18216	null connection error seen in logs
CSCwe28407	LINA traceback with icmp_thread
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.
CSCwe39546	FMC: Backup to an unavailable remote host results in the inability to restart the appliance.
CSCwe42061	Deleting a BVI in FTD interfaces is causing packet drops in other BVIs
CSCwe44571	FMC: GEOLOCATION size is causing upgrade failures
CSCwe47671	High memory usage on monetDB, FMC does not show connection events
CSCwe51443	ASA Evaluation of OpenSSL vulnerability CVE-2022-4450
CSCwe55298	Umbrella DNS Policy Doesn't honor Multiple URLs entered into the Bypass Domain Field
CSCwe74089	ASA/FTD may traceback and reload in Thread Name DATAPATH-1-1656
CSCwe79051	Deployment for eigrp / bgp change may cause temporary outage during policy apply
CSCwe82704	PortChannel sub-interfaces configured as data/data-sharing, in multi-instance HA go into "waiting"

Bug ID	Headline
CSCwe83255	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe90720	ASA Traceback and reload in parse thread due ha_msg corruption
CSCwe92905	ngfwManager process continuously restarting leading to ZMQ Out of Memory traceback
CSCwe93176	Snort2 rule assignments missing from ngfw.rules (assignment_data table) after FMC upgrade.
CSCwe99550	Add knob to pause/resume file specific logging in asa log infra.
CSCwf04870	ASA: "Ping <ifc_name> x.x.x.x" is not working as expected starting 9.18.x
CSCwf05295	FTD running on FP1000 series might drop packets on TLS flows after the "Client Hello" message.
CSCwf10910	FTD : Traceback in ZMQ running 7.3.0
CSCwf12005	ASA sends OCSP request without user-agent and host
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'
CSCwf15858	LDAP authentication over SSL not working for users that send large authorisation profiles
CSCwf15902	ASAv in Hyper-V drops packets on management interface
CSCwf16559	getReadinessStatusTaskList pjb request is very frequent when user in Upgrade sensor list page
CSCwf17042	ASDM replaces custom policy-map with default map on class inspect options at backup restore.
CSCwf17406	Failure to remove snort stat files older than 70 days
CSCwf20338	ASA may traceback and reload in Thread Name 'DHCPv6 Relay'
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
CSCwf30716	ASA in multi context shows standby device in failed stated even after MIO HB recovery.
CSCwf31701	ASA traceback and reload with the Thread name: **CP Crypto Result Processing**
CSCwf34152	FMC Fails to deploy or register new FTDs due to SFTunnel Establishment Failure.
CSCwf34500	FTD: GRE traffic is not being load balanced between CPU cores

Bug ID	Headline
CSCwf35207	ASA: Traceback and reload while updating ACLs on ASA
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
CSCwf37160	AnyConnect Ikev2 Login Failed With certificate-group-map Configured
CSCwf42144	ASA/FTD may traceback and reload citing process name "lina"
CSCwf43288	Traceback in Thread Name: ssh/client in a clustered setup
CSCwf43537	Lina crash in thread name: cli_xml_request_process during FTD cluster upgrade
CSCwf44537	99.20.1.16 lina crash on nat_remove_policy_from_np
CSCwf44915	Old LSP packages are not pruned causing high disk utilization
CSCwf47227	Remove Priority-queue command from FTD|| Priority-queue command causes silent egress packet drops
CSCwf48599	VPN load-balancing cluster encryption using deprecated ciphers
CSCwf49486	store_*list_history.pl task is created every 5min without getting closed causing FMC slowness.
CSCwf49573	ASA/FTD: Traceback and reload when issuing 'show memory webvpn all objects'
CSCwf50497	DNS cache entry exhaustion leads to traceback
CSCwf54510	ASA traceback and reload on Thread Name: DHCPRA Monitor
CSCwf56386	vFTD runs out of memory and goes to failed state
CSCwf56811	ASA Traceback & reload on process name lina due to memory header validation
CSCwf58876	KP2140-HA, reloaded primary unit not able to detect the peer unit
CSCwf60311	ASA generating traceback with thread-name: DATAPATH-53-18309 after upgrade to 9.16.4.19
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
CSCwf69901	FTD: Traceback and reload during OSPF redistribution process execution
CSCwf71812	FTD Lina engine may traceback, due to assertion, in datapath

Bug ID	Headline
CSCwf72434	Add meaningful logs when the maximums system limit rules are hit
CSCwf77191	ASA appliance mode - 'connect fxos [admin]' will get ERROR: failed to open connection.
CSCwf78321	ASA: Checkheaps traceback and reload due to Clientless WebVPN
CSCwf81058	FTD: Firepower 3100 Dynamic Flow Offload showing as Enabled
CSCwf82247	Policy deployment fails when a route same prefix/metric is configured in a separate VRF.
CSCwf82742	FTD: SNMP not working on management interface
CSCwf82970	Snort2 engine is crashing after enabling TLS Server Identity Discovery feature
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
CSCwf92646	ECDSA Self-signed certificate using SHA384 for EC521
CSCwf92726	LDAP missing files after upgrade when the Vault token is corrupted
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
CSCwh04231	FMC needs to properly maintain Redis data directory to prevent unbounded disk usage
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
CSCwh11764	ASA/FTD may traceback and reload in Thread Name "RAND_DRBG_bytes" and CTM function on n5 platforms
CSCwh12987	Large SMB servers result in timeouts returning verdicts between FMC and FTD devices
CSCwh14467	File sizes larger than 100MB for AnyConnect/Secure Client images cannot be uploaded on FMC
CSCwh14584	Traceback seen on FTD running on Firepower 2100 series
CSCwh14597	ASA/FTD residual free

Bug ID	Headline
CSCwh15223	Lina crash in snp_fp_tcp_normalizer() when DAQ/Snort sends malformed L3 header
CSCwh21141	The FMC preview deployment shows a wrong information.
CSCwh23100	Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
CSCwh23567	PAC Key file missing on standby on reload
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.
CSCwh28144	Specific OID 1.3.6.1.2.1.25 should not be responding
CSCwh30891	ASA/FTD may traceback and reload in Thread Name 'ssh' when adding SNMPV3 config
CSCwh32118	ASDM management-sessions quota reached due to HTTP sessions stuck in CLOSE_WAIT
CSCwh36005	Policy deployment failed due to "1 errors seen during populateGlobalSnapshot"
CSCwh37733	FTD responding to UDP500 packet with a Mac Address of 0000.000.000
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
CSCwh45108	Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
CSCwh49483	ASA/FTD may traceback and reload while running show inventory
CSCwh52420	AMP Cloud look up timeout frequently.
CSCwh56945	SFDataCorrelator crashing repeatedly in RNA_DB_InsertServiceInfo
CSCwh58999	Devices with classic licenses are failed to register with FMC running version 7.2.X
CSCwh64508	Fixing the regression caused while handling web UI is not getting FTDv Variable
CSCwh69209	Prefilter cannot add Tunnel Endpoints in Tunnel Rule on FMC
CSCwh69815	FTDvs through put got changed to 100Kbps after upgrade

Resolved Bugs in Version 7.2.5

Table last updated: 2024-05-22

Table 27: Resolved Bugs in Version 7.2.5

Bug ID	Headline

Bug ID	Headline
CSCvo60131	Audit log records does not appear in the correct order
CSCwb08189	Microsoft update traffic blocked with Snort version 3 Malware inspection
CSCwb95453	ASA: The timestamp for all logs generated by Admin context are the same
CSCwb95784	cache and dump last 20 rmu request response packets in case failures/delays while reading registers
CSCwd14732	FTD Unable to bind to port 8305 after management IP change
CSCwd16850	More information is required on Syslog 202010 messages for troubleshooting
CSCwd34288	FP1000 - During boot process in LINA mode, broadcasts leaked between interfaces resulting in storm
CSCwd41224	FMC HA webUI is not getting FTDv Variable tier assigned FTDv - Variable
CSCwd67101	FPR1150 : Exec format error seen and the device hung until reload when erase secure all is executed
CSCwd94183	Blade not coming up after FXOS update support on multi-instance due to ssp_ntp.log log rotation prob
CSCwe03529	FTD traceback and reload while deploying PAT POOL
CSCwe06562	FPR1K/FPR2K: Increase in failover time in Transparent Mode with high number of Sub-Interfaces
CSCwe07722	Cluster data unit drops non-VPN traffic with ASP reason "VPN reclassify failure
CSCwe21187	ASA/FTD may drop multicast packets due to no-mcast-intrf ASP drop reason until UDP timeout expires
CSCwe21280	Multicast connection built or teardown syslog messages may not always be generated
CSCwe23801	FPR2100: Mulitple snort3 & snort2 cores got generated and sensor goes down in KP platform
CSCwe29529	FTD MI does not adjust PVID on vlans attached to BVI
CSCwe30867	Workaround to set hwclock from ntp logs on low end platforms
CSCwe44672	Syslog ASA-6-611101 is generated twice for a single ssh connection
CSCwe45569	FTD upgrade from 7.0 to 7.2.x and beyond crashes due to management-access enabled
CSCwe45653	ENH: FXOS need to track Security Module for Disk quota exceeded related issue
CSCwe50993	SNMP on SFR module goes down and won't come back up
CSCwe51286	ASA/FTD may traceback and reload in Thread Name 'lina'

Bug ID	Headline
CSCwe52120	SSL decrypted conns fails when tx chksum-offload is enabled with the egress interface a pppoe.
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'
CSCwe58881	After FMC upgrade, SecureX ribbon redirects to US cloud region regardless of the set cloud region
CSCwe59737	ASA/FTD reboots due to traceback pointing to watchdog timeout on p3_tree_lookup
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
CSCwe62703	New context subcommands are not replicated on HA standby when multiple sessions are opened.
CSCwe63067	ASA/FTD may traceback and reload in Thread Name 'lina' due to due to tcp intercept stat
CSCwe63316	Pri-Active FMC NOT triggering registration TASK for FTD to configure standby manager
CSCwe64043	Cisco ASA and FTD ACLs Not Installed upon Reload
CSCwe65634	ASA - Standby device may traceback and reload during synchronization of ACL DAP
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
CSCwe70202	Multiple times the failover may be disabled by wrongly seeing a different "Mate operational mode".
CSCwe74916	Interface remains DOWN in an Inline-set with propagate link state
CSCwe76722	ASA/FTD: From-the-box ping fails when using a custom VRF
CSCwe78977	ASA/FTD may traceback and reload in Thread Name 'pix_flash_config_thread'
CSCwe79072	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe81684	ASA: Standby failure on parsing of "management-only" not reported to parser/failover subsystem

Bug ID	Headline
CSCwe85432	ASA/FTD traceback and reload on thread DATAPATH-14-11344 when SIP inspection is enabled
CSCwe88772	ASA traceback and reload with process name: cli_xml_request_process
CSCwe90202	ASA: Standby failure on parsing of "management-only" for dynamic configuraiton changes
CSCwe90334	Missing Instance ID in unified_events-2.log
CSCwe93532	ASA/FTD may traceback and reload in Thread Name 'lina'.
CSCwe93537	Threat-detection does not allow to clear individual IPv6 entries
CSCwe94287	FTD DHCP Relay drops NACK if multiple DHCP Servers are configured
CSCwe95729	Cisco ASA & FTD SAML Authentication Bypass Vulnerability
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
CSCwe99040	traceback and reload thread datapath on process tcpmod_proxy_continue_bp
CSCwf00417	FTD: Unable to process a TLS1.2 website with TLS Server Identity with client generating SSL Errors
CSCwf00865	FTD/ASA Hub and spoke (U-turn) VPN fails when one spoke is IPSec flow offloaded and the other isn't
CSCwf01064	TCP ping is completely broken starting in 9.18.2
CSCwf02363	Snort3 Crash in SslServiceDetector after call from nss_passwd_lookup
CSCwf03490	portmanager.sh outputing continuous bash warnings to log files
CSCwf04831	ASA/FTD may traceback and reload in Thread Name 'ci/console'
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"
CSCwf10486	ISE Integration Network filter not accepting multiple comma separated networks
CSCwf12408	ASA: After upgrade to 9.16.4 all type-8 passwords are lost on first reboot
CSCwf14735	traceback and reload in Process Name: lina related to Nat/Pat

Bug ID	Headline
CSCwf14811	TCP normalizer needs stats that show actions like packet drops
CSCwf17814	ASA/FTD may traceback and reload in Thread Name '19', free block checksum failure
CSCwf21106	ASA/FTD: Traceback on thread name: snmp_master_callback_thread during SNMP and interface changes
CSCwf22045	MYSQL, or any TCP high traffic, getting blocked by snort3, with snort-block as Drop-reason
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
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
CSCwf30727	ASA integration with umbrella does not work without validation-usage ssl-server.
CSCwf31820	Firewall may drop packets when routing between global or user VRFs
CSCwf33574	ASA access-list entries have the same hash after upgrade
CSCwf34450	Snort3 crash after the consequent snort restart if duplicate custom apps are present
CSCwf35510	Possible segfault in snort3 when appid tries to delete the app info table
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
CSCwf60584	Health Monitoring to NOT collect route stats for transparent mode FTD
CSCwf62885	FTDv Single-Arm Proxy behind AWS GWLB drops due to geneve-invalid-udp-checksum.
CSCwf71606	Cisco ASA and FTD ACLs Not Installed upon Reload
CSCwf73189	FTD is dropping GRE traffic from WSA due to NAT failure
CSCwf76945	Packet data is still dropped after upgrade
CSCwf85307	[Snort 3] IPS Policy Overrides not working on Chained Intrusion Policies
CSCwf88552	ASA/FTD: Traceback and reload due to NAT L7 inspection rewrite

Bug ID	Headline
CSCwf99173	DOC:When using an SLR, it does not properly documented what happens if one of the licenses expires.
CSCwh01154	FTD: 10Gbps/full interfaces changed to 1Gbps/Auto after upgrade and going to down state

Resolved Bugs in Version 7.2.4.1

Table last updated: 2024-05-22

Table 28: Resolved Bugs in Version 7.2.4.1

Bug ID	Headline
CSCvo60131	Audit log records does not appear in the correct order
CSCwb08189	Microsoft update traffic blocked with Snort version 3 Malware inspection
CSCwb95453	ASA: The timestamp for all logs generated by Admin context are the same
CSCwd14732	FTD Unable to bind to port 8305 after management IP change
CSCwd16850	More information is required on Syslog 202010 messages for troubleshooting
CSCwd34288	FP1000 - During boot process in LINA mode, broadcasts leaked between interfaces resulting in storm
CSCwd41224	FMC HA webUI is not getting FTDv Variable tier assigned FTDv - Variable
CSCwd67101	FPR1150 : Exec format error seen and the device hung until reload when erase secure all is executed
CSCwd94183	Blade not coming up after FXOS update support on multi-instance due to ssp_ntp.log log rotation prob
CSCwe03529	FTD traceback and reload while deploying PAT POOL
CSCwe06562	FPR1K/FPR2K: Increase in failover time in Transparent Mode with high number of Sub-Interfaces
CSCwe07722	Cluster data unit drops non-VPN traffic with ASP reason "VPN reclassify failure
CSCwe21187	ASA/FTD may drop multicast packets due to no-mcast-intrf ASP drop reason until UDP timeout expires
CSCwe21280	Multicast connection built or teardown syslog messages may not always be generated
CSCwe29529	FTD MI does not adjust PVID on vlans attached to BVI
CSCwe30867	Workaround to set hwclock from ntp logs on low end platforms
CSCwe44672	Syslog ASA-6-611101 is generated twice for a single ssh connection

Bug ID	Headline
CSCwe45653	ENH: FXOS need to track Security Module for Disk quota exceeded related issue
CSCwe50993	SNMP on SFR module goes down and won't come back up
CSCwe51286	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe52120	SSL decrypted conns fails when tx chksum-offload is enabled with the egress interface a pppoe.
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'
CSCwe58881	After FMC upgrade, SecureX ribbon redirects to US cloud region regardless of the set cloud region
CSCwe59737	ASA/FTD reboots due to traceback pointing to watchdog timeout on p3_tree_lookup
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
CSCwe62703	New context subcommands are not replicated on HA standby when multiple sessions are opened.
CSCwe63067	ASA/FTD may traceback and reload in Thread Name 'lina' due to due to tcp intercept stat
CSCwe63316	Pri-Active FMC NOT triggering registration TASK for FTD to configure standby manager
CSCwe64043	Cisco ASA and FTD ACLs Not Installed upon Reload
CSCwe65634	ASA - Standby device may traceback and reload during synchronization of ACL DAP
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
CSCwe70202	Multiple times the failover may be disabled by wrongly seeing a different "Mate operational mode".
CSCwe74916	Interface remains DOWN in an Inline-set with propagate link state
CSCwe76722	ASA/FTD: From-the-box ping fails when using a custom VRF
CSCwe78977	ASA/FTD may traceback and reload in Thread Name 'pix_flash_config_thread'

Bug ID	Headline
CSCwe79072	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe81684	ASA: Standby failure on parsing of "management-only" not reported to parser/failover subsystem
CSCwe85432	ASA/FTD traceback and reload on thread DATAPATH-14-11344 when SIP inspection is enabled
CSCwe88772	ASA traceback and reload with process name: cli_xml_request_process
CSCwe90202	ASA: Standby failure on parsing of "management-only" for dynamic configuraiton changes
CSCwe90334	Missing Instance ID in unified_events-2.log
CSCwe93532	ASA/FTD may traceback and reload in Thread Name 'lina'.
CSCwe93537	Threat-detection does not allow to clear individual IPv6 entries
CSCwe94287	FTD DHCP Relay drops NACK if multiple DHCP Servers are configured
CSCwe95729	Cisco ASA & FTD SAML Authentication Bypass Vulnerability
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
CSCwe99040	traceback and reload thread datapath on process tcpmod_proxy_continue_bp
CSCwf00417	Unable to process a TLS1.2 website with TLS Server Identity, it generates ERR_SSL_PROTOCOL_ERROR.
CSCwf00865	FTD/ASA Hub and spoke (U-turn) VPN fails when one spoke is IPSec flow offloaded and the other isn't
CSCwf01064	TCP ping is completely broken starting in 9.18.2
CSCwf02363	Snort3 Crash in SslServiceDetector after call from nss_passwd_lookup
CSCwf03490	portmanager.sh outputing continuous bash warnings to log files
CSCwf04831	ASA/FTD may traceback and reload in Thread Name 'ci/console'
CSCwf06818	Cisco Firepower Threat Defense Software Encrypted Archive File Policy Bypass Vulnerability
CSCwf07791	ASA running out of SNMP PDU and SNMP VAR chunks
CSCwf08043	Lina traceback and reload due to fragmented packets

Bug ID	Headline
CSCwf08515	FPR3100: ASA/FTD High traffic impact on all data interfaces with high counter of "demux drops"
CSCwf10486	ISE Integration Network filter not accepting multiple comma separated networks
CSCwf12408	ASA: After upgrade to 9.16.4 all type-8 passwords are lost on first reboot
CSCwf14735	traceback and reload in Process Name: lina related to Nat/Pat
CSCwf14811	TCP normalizer needs stats that show actions like packet drops
CSCwf17814	ASA/FTD may traceback and reload in Thread Name '19', free block checksum failure
CSCwf21106	ASA/FTD: Traceback on thread name: snmp_master_callback_thread during SNMP and interface changes
CSCwf22045	MYSQL, or any TCP high traffic, getting blocked by snort3, with snort-block as Drop-reason
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
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
CSCwf30727	ASA integration with umbrella does not work without validation-usage ssl-server.
CSCwf31820	Packets are not forwarding between global vrf to user vrf and vice-versa
CSCwf33574	ASA access-list entries have the same hash after upgrade
CSCwf34450	Snort3 crash after the consequent snort restart if duplicate custom apps are present
CSCwf35510	Possible segfault in snort3 when appid tries to delete the app info table
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
CSCwf60584	Health Monitoring to NOT collect route stats for transparent mode FTD
CSCwf62885	FTDv Single-Arm Proxy behind AWS GWLB drops due to geneve-invalid-udp-checksum.
CSCwf71606	Cisco ASA and FTD ACLs Not Installed upon Reload
CSCwf73189	FTD is dropping GRE traffic from WSA due to NAT failure

Bug ID	Headline
CSCwf76945	Packet data is still dropped after upgrade
CSCwf85307	[Snort 3] IPS Policy Overrides not working on Chained Intrusion Policies
CSCwf88552	ASA/FTD: Traceback and reload due to NAT L7 inspection rewrite

Resolved Bugs in Version 7.2.4

Table last updated: 2024-05-22

Table 29: Resolved Bugs in Version 7.2.4

Bug ID	Headline
CSCvo60131	Audit log records does not appear in the correct order
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
CSCvq70838	Traceback in the output of tail-logs command
CSCvs89229	Incorrect rules are highlighted during search in AC rules
CSCvu24703	FTD - Flow-Offload should be able to coexist with Rate-limiting Feature (QoS)
CSCvv18009	Performing packet trace using the sub-interface nameif results in an error
CSCvw90399	FMC HA issues with too many open file descriptors for sfipproxy UDP conn
CSCvx24207	FQDN Object Containing IPv4 and IPv6 Addresses Only Install IPv6 Entries
CSCvx55978	Performance Degradation in GetGroupDependency API
CSCvx65032	FMC ACL Search Move arrows do not work
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
CSCvx86569	Access Control Rule - Comment disappears if clicked to another tab before saving the comment.
CSCvy26676	"Warning:Update failed/in-progress." Cosmetic after successful update
CSCvy38650	Unable to download captured file from FMC Captured files UI

Bug ID	Headline
CSCvy45048	Subsystem query parameter not filtering records for "auditrecords" restapi
CSCvz07004	SNORT2: FTD is performing Full proxy even when SSL rule has DND action.
CSCvz07712	Deployment fails with internal_errors - Cannot get fresh id
CSCvz19364	FXOS does not send any syslog messages when the duplex changes to "Half Duplex"
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
CSCvz40586	Incorrect error when creating two RA-VPN profiles with different SAML servers that have the same IDP
CSCvz41551	FP2100: ASA/FTD with threat-detection statistics may traceback and reload in Thread Name 'lina'
CSCvz42065	IPS policy should be imported when its referred in Access Control policy
CSCvz71596	"Number of interfaces on Active and Standby are not consistent" should trigger warning syslog
CSCvz77213	FTD: show ntp shows managing DC even though NTP sync is done via FXOS
CSCvz94841	Grammatical errors in failover operating mode mismatch error message
CSCwa04262	Cisco ASA Software SSL VPN Client-Side Request Smuggling Vulnerability via "/"URI
CSCwa16626	Syslog over TLS accepting wildcard in middle of FQDN
CSCwa36535	Standby unit failed to join failover due to large config size.
CSCwa59907	LINA observed traceback on thread name "snmp_client_callback_thread"
CSCwa72481	API key corrupted for FMC with multiple interfaces
CSCwa72929	SNMPv3 polling may fail using privacy algorithms AES192/AES256
CSCwa74063	Disable NLP rules installation workaround after mgmt-access into NLP is enabled
CSCwa82850	ASA Failover does not detect context mismatch before declaring joining node as "Standby ready"
CSCwa83133	FMC showing "INVALID ID" under "Traffic by User" Widget but error not seen on Connection Events
CSCwa89116	Clean up session index handling in IKEv2/SNMP/Session-mgr for MIB usage
CSCwa92822	TLS client in the sftunnel TLS tunnel offers curves in CC mode that are not allowed by CC
CSCwa94440	syncd process exits due to invalid GID and database synchronization issue

Bug ID	Headline
CSCwa96920	ASA/FTD may traceback and reload in process Lina
CSCwa97917	ISA3000 in boot loop after powercycle
CSCwb00749	FMC upgrade failure: 114_DB_table_data_integrity_check.pl failed
CSCwb00871	ENH: Reduce latency in log_handler_file to reduce watchdog under scale or stress
CSCwb02955	Modify /800_post/1027_ldap_external_auth_fix.pl to not fail FMC upgrade when objects are corrupt
CSCwb03704	ASA/FTD datapath threads may run into deadlock and generate traceback
CSCwb04000	ASA/FTD: DF bit is being set on packets routed into VTI
CSCwb04975	FTD Snort3 traceback in daq-pdts while handling FQDN based traffic
CSCwb05291	Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability
CSCwb09606	FP2100: ASA/FTD high availability is not resilient to unexpected lacp process termination
CSCwb17362	Losing ssh connection while copying huge file to device though device has enough space.
CSCwb20206	FTD: Logs and Debugs for SSL/TLS traffic drop due to NAP in Detection Mode
CSCwb24306	duplicate log entry for /mnt/disk0/log/asa_snmp.log
CSCwb31551	When inbound packet contains SGT header, FPR2100 cannot distribute properly per 5 tuple
CSCwb32107	FMC shows limited interfaces in policy-based routing config (egress interface selection)
CSCwb38961	Bootstrap After Upgrade failed due to Duplicate Key of Network Object
CSCwb43433	Jumbo frame performance has degraded up to -45% on Firepower 2100 series
CSCwb44048	Event Rate on FMC Health Monitoring Dashboard shows extremely high values
CSCwb44848	ASA/FTD Traceback and reload in Process Name: lina
CSCwb57213	FTD - Unable to resolve DNS when only diagnostic interface is used for DNS lookups
CSCwb57524	FTD upgrade fails - not enough disk space from old FXOS bundles in distributables partition
CSCwb58007	CVE-2022-28199: Evaluation for FTDv and ASAv
CSCwb58554	Resumed SSL sessions with uncached tickets may fail to complete
CSCwb58817	FMC Deploying negative and positive form of BGP password command across deployments

Bug ID	Headline
CSCwb60993	FDM Need to block the deployment when a Security zone object is not associated with an interface
CSCwb66382	ASAv - 9344 Block not created automatically after enabling JumboFrames, breaks OSPF MD5
CSCwb68993	FTD/FDM: SSL connections to sites using RSA certs with 3072 bit keys may fail
CSCwb78323	Update diskmanager to monitor cisco_uridb files in /ngfw/var/sf/cloud_download folder.
CSCwb80108	FP2100/FP1000: Built-in RJ45 ports randomly not coming up after portmanager restart events
CSCwb84901	CIAM: heimdal 1.0.1
CSCwb86171	Breaking FMCv HA in AWS gives VTEP CONFIGURATION IS NOT SUPPORTED FOR CURRENT PERFORMANCE TIER alert
CSCwb88406	FMC-HA upgrade failure due to presence of this file "update.status"
CSCwb88729	FTD - %FTD-3-199015: port-manager: Error: DOM Block Read failure, port X, st = X log false/positive
CSCwb89963	ASA Traceback & reload in thread name: Datapath
CSCwb91598	copying FMC backup to remote storage will fail if FMC has never connected via SSH/SCP to remote host
CSCwb92937	Error 403: Forbidden when expanding in view group objects
CSCwb99375	Config sync fails for command "quit"
CSCwb99960	onPremFMC with only CDO Managed devices registered, Malware Event pages shows license warning
CSCwc00115	FTD registration fails on on-prem FMC
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
CSCwc03332	FTD on FP2100 can take over as HA active unit during reboot process
CSCwc03393	Lina traceback and core file size is beyond 40G and compression fails on FTD
CSCwc03507	No-buffer drops on Internal Data interfaces despite little evidence of CPU hog
CSCwc04959	Disk usage is 100% on secondary FMC .dmp files created utilized all the disk space
CSCwc05375	AnyConnect SAML - Client Certificate Prompt incorrectly appears within External Browser
CSCwc05434	FMC shows 'File Not Stored' after download a file

Bug ID	Headline
CSCwc06833	Deployment failure with ERROR Process Manager failed to verify LSP ICDB
CSCwc07262	Standby ASA goes to booting loop during configuration replication after upgrade to 9.16(3).
CSCwc08374	Azure ASA NIC MAC address for Gigeth 0/1 and 0/2 become out of order when adding interfaces
CSCwc08646	User without password prompted to change password when logged in from SSH Client
CSCwc08683	The interface's LED remains green blinking when the optical fiber is unplugged on FPR1150
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
CSCwc13017	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
CSCwc18285	Conn data-rate command can be enabled or disabled in unprivileged user EXEC mode
CSCwc18524	ASA/FTD Voltage information is missing in the command "show environment"
CSCwc18668	Failed user login on FMC does not record entry in audit log when using external authentication
CSCwc19124	FMC Deployment does not start for cluster devices
CSCwc20153	IPv6 ICMP configuration is added and removed during policy deployment
CSCwc22170	Issue with snort perfstat parsing / Hmdeamon not starting after disk full reported
CSCwc23113	LTP feature not working on KP ASA with 9.18
CSCwc23844	ASAv high CPU and stack memory allocation errors despite over 30% free memory
CSCwc24582	Update diskmanager to monitor deploy directories in /ngfw/var/cisco/deploy/db
CSCwc24906	ASA/FTD traceback and reload on Thread id: 1637
CSCwc25683	JOBS_TABLE not getting purged if deployReports not available
CSCwc26406	FMC: Slowness in Device management page
CSCwc26538	With scaled EFD throttle connections, de-throttle using clear efd-throttle command traceback lina

Bug ID	Headline
CSCwc26648	ASA/FTD Traceback and Reload in Thread name Lina or Datatath
CSCwc27236	FMC Health Monitoring JSON error
CSCwc27424	Unable to removed not used SAL On-Premise FMC configuration
CSCwc27846	Traceback and Reload while HA sync after upgrading and reloading.
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
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
CSCwc28928	ASA: SLA debugs not showing up on VTY sessions
CSCwc31163	FPR1010 upgrade failed - Error running script 200_pre/100_get_snort_from_dc.pl
CSCwc31457	ASA process with cleartext token when not able to encrypt it
CSCwc32245	FMC: Validation check to prevent exponential expansion of NAT rules
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
CSCwc33036	Observed Logs at syslog server side as more than configured message limit per/sec.
CSCwc33076	JOBS_TABLE not getting purged due to foreign Key constraint violation in policy_diff_main
CSCwc33323	FMC 7.0 - Receiving alert "health monitor process: no events received yet" for multiple devices
CSCwc34818	The device is unregistered when Rest API calls script.
CSCwc35181	OSPF template adds "default-information-originate" to area <area-id> nssa statement on hitting OK.
CSCwc35969	cannot add IP from event to global lists (block or do-not-block) if similar IP is already on list
CSCwc36905	ASA traceback and reload due to "Heap memory corrupted at slib_malloc.c
CSCwc37061	SNMP: FMC doesn't reply to OID 1.3.6.1.2.1.25.3.3.1.2
CSCwc37256	SSL AnyConnect access blocked after upgrade
CSCwc37695	In addition to the c_rehash shell command injection identified in CVE-2022-1292
CSCwc38500	FMC: Extended ACL object should support mixed protocols on different entries

Bug ID	Headline
CSCwc38567	ASA/FTD may traceback and reload while executing SCH code
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
CSCwc41180	AWS ASAv Clustering: enable cluster breaking ssh session
CSCwc41592	False positives for Ultrasurf
CSCwc41728	FMC - Cannot Edit Standard ACL with error regarding "Only Host objects allowed"
CSCwc42174	CIAM: mariadb - multiple versions CVE-2022-32081
CSCwc42561	Deploy page listing takes 1.5 to 2 mins with 462 HA device
CSCwc43807	FTD is unusable post reboot if manager is deleted and FIPS is enabled
CSCwc44289	FTD - Traceback and reload when performing IPv4 <> IPv6 NAT translations
CSCwc44608	Selective deployment of IPS may cause outage due to incorrectly written FTD configuration files
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
CSCwc45759	NTP logs will eventually overwrite all useful octeon kernel logs
CSCwc46847	FXOS partition opt_cisco_platform_logs on FP1K/FPR2K may go Full due to ucssh_*.log
CSCwc47586	vFMC upgrade 7.0.4-36 > 7.3.0-1553 failed: Error running script 200_pre/007_check_sru_install.sh
CSCwc48375	Inbound IPSEC SA stuck inactive - many inbound SPIs for one outbound SPI in "show crypto ipsec sa"
CSCwc48853	SFDataCorrelator Discovery Event bottleneck can cause Connection Event delay and backlog
CSCwc49095	ASA/FTD 2100 platform traceback and reload when fragments are coalesced and sent to PDTS
CSCwc49364	mojo_server processes unnecessarily restarting during log rotation
CSCwc49369	When searching IPv6 rule in the access-control policy, no result will show
CSCwc49936	FMC 7.2.0|7.3.0 Integration > Identity Sources page does not load, keeps spinning

Bug ID	Headline
CSCwc49942	Reload mercury when userappid.conf is modified on FMC and deploy is issued
CSCwc49952	Selective deploy enables interaction with SRU interdependent-policies due to FMC API timeout
CSCwc50098	show ssl-policy-config does not show the policy when countries are being used in source/dest network
CSCwc50519	Excessive logging from hm_du.pm may lead to syslog-ng process restarts
CSCwc50846	FTD Upgrade Fail - Readiness Check Successful, but Readiness status never shown
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
CSCwc52357	Estreamer page fails to load in ASDM
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
CSCwc54901	Scheduled tasks may not run on active FMC in HA after switchover or split-brain resolution
CSCwc54984	IKEv2 rekey - Responding Invalid SPI for the new SPI received right after Create_Child_SA response
CSCwc56003	Trigger FTD backup with remote storage option enabled along with retrieval to FMC fails
CSCwc56048	AD username with trailing space causes download of users/groups to fail
CSCwc56952	Able to see the SLA debug logs on both console & VTY sessions even if we enable only on VTY session.
CSCwc57088	Limit the number of deployment jobs in deploy history to 50 as default to avoid slowness
CSCwc57575	FMC: Scheduled backups working fine, but FMC email alerts displaying it failed.
CSCwc60037	ASA fails to rekey with IPSEC ERROR: Failed to allocate an outbound hardware context
CSCwc60907	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 35)

Bug ID	Headline
CSCwc61132	KP-2130 - Observed crash with PPK configured
CSCwc61912	ASA/FTD OSPFv3 does not generate messages Type 8 LSA for IPv6
CSCwc62144	FMC does not use proxy with authentication when accessing AMP cloud services
CSCwc62384	Vulnerabilities on Cisco FTD Captive Portal on TCP port 885
CSCwc63273	SFDataCorrelator host timeout query can block event processing and cause a deadlock restart
CSCwc64333	FMC GUI timeout and issues with loading http page due to exceeded http connections
CSCwc64923	ASA/FTD may traceback and reload in Thread Name 'lina' ip routing ndbshr
CSCwc66671	FMC ACP PDF report generared in blank/0 bytes using UI
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
CSCwc67687	ASA HA failover triggers HTTP server restart failure and ASDM outage
CSCwc67886	ASA/FTD may traceback and reload in Thread Name 'lina_inotify_file_monitor_thread'
CSCwc68543	mismatch in the config pushed from FMC and running config on FTD
CSCwc68656	ASA CLI for TCP Maximum unprocessed segments
CSCwc69583	Portchannel configured from FDM breaks "Use the Data Interfaces as the Gateway" for Mgmt interface
CSCwc69992	Essentials licenses are not assigned to the device and Edit licenses also not working
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
CSCwc74099	FPR2140 ASA Clock Timezone reverts to UTC after appliance restart/reload
CSCwc74103	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-11-32591'
CSCwc74378	FMC UI should disallow simultaneous deactivation of FMC interface management and event channels
CSCwc74841	FMC RSS Feed broken because FeedBurner is no longer active - "Unable to parse feed"

Bug ID	Headline
CSCwc74858	FTD - Traceback in Thread Name: DATAPATH
CSCwc75061	FMC allows shell access for user name with "." but external authentication will fail
CSCwc75082	25G-SR should default to RS-FEC (IEEE CL108) instead of FC-FEC
CSCwc76195	Fail-To-Wire interfaces flaps intermittently due to watchdog timeout in Firepower 2100 platform
CSCwc76913	cdFMC: Policy deployment is failing after upgrade cdFMC
CSCwc77519	FPR1000 ASA/FTD: Primary takes active role after reloading
CSCwc77680	FTD may traceback and reload in Thread Name 'DATAPATH-0-4948'
CSCwc77892	CGroups errors in ASA syslog after startup
CSCwc78296	Database may fail to shut down and/or start up properly during upgrade
CSCwc79366	During the deployment time, device got stuck processing the config request.
CSCwc79682	FMC 7.1+ allows ECMP FlexConfig depoyment
CSCwc80234	"inspect snmp" config difference between active and standby
CSCwc80357	[Deploy Performance] degrade in deployment page on FMC
CSCwc81184	ASA/FTD traceback and reload caused by SNMP process failure
CSCwc81219	Intrusion events intermittently stop appearing in FMC when using snort3
CSCwc81727	Default Domain in VPN group policy objects cannot be deleted
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
CSCwc82124	ASA NAT rules are not working as expected after an upgrade to 9.18.2
CSCwc82188	FTD Traceback and reload when applying long commands from FMC UI or CLISH
CSCwc83037	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 36)
CSCwc83346	ASA/FTD Traceback and reload in Threadname: IKE Daemon
CSCwc86330	Vulnerabilities in spring-framework - multiple versions CVE-2022-22970
CSCwc86391	On slow networks with some packets loss sftunnel may mark connections as STALE
CSCwc87387	Valid DNS requests are being dropped by Lina DNS inspection when Umbrella DNS is configured

Bug ID	Headline
CSCwc87441	for system processes limit the CPUs used to the number of system CPUs
CSCwc87963	ASAv "Unable to retrieve license info. Please try again later"
CSCwc88108	Prefilter policy - Available port menu long response time, Prefilter Network Search takes long time
CSCwc88425	FMC can download only the first 10000 cross-domain user groups
CSCwc88629	Group delete during realm download can cause inconsistent user_to_group map on FTD
CSCwc88897	ASA traceback and reload due to null pointer in Umbrella after modifying DNS inspection policy
CSCwc89661	FTD misses diagnostic data required for investigation of "Communication with NPU lost" error
CSCwc89796	ASA/FTD may traceback and reload in Thread Name 'appagent_async_client_receive_thread' hog detection
CSCwc89924	FXOS ASA/FTD SNMP OID to poll Internal-data 'no buffer' interface counters
CSCwc90091	ASA 9.12(4)47 with user-statistics, will affects the "policy-server xxxx global" visibility.
CSCwc92761	7.3 - Message flood by Use of uninitialized value $unix_time in numeric gt
CSCwc93166	Using write standby in a user context leaves secondary firewall license status in an invalid state
CSCwc93964	ASA using WebVPN tracebacks in Unicorn thread during memory tracking
CSCwc94085	Unable to establish DTLSv1.2 with FIPS enabled after upgrade from 6.6.5.
CSCwc94267	Cluster disabled unit getting registered as standalone in FMC and further deployment failing
CSCwc94466	Cisco ASA/FTD Firepower 2100 SSL/TLS Denial of Service Vulnerability
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
CSCwc96016	Captive portal support in cross domain
CSCwc96136	CCM layer (Seq 38) WR8, LTS18, LTS21
CSCwc96726	R2130 use the Wind River CIS_LTS21_R2130 OS branch for the 7.3.0 Beta2 release.
CSCwc96780	FMC module specific health exclusion disables all health checks

Bug ID	Headline
CSCwc96805	traceback and reload due to tcp intercept stat in thread unicorn
CSCwc97260	Continual ngfwManager process restarts due to incomplete FMC HA device registration
CSCwc98997	FMC - Deployment blocked when ECMP route configured via same interface
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"
CSCwd00583	SNMP 'Confirm Community String' string is not auto-populated after the FMC upgrade
CSCwd00778	ifAdminStatus output is abnormal via snmp polling
CSCwd01032	ASA/FTD may traceback and reload when RAVPN with SAML is configured
CSCwd02864	logging/syslog is impacted by SNMP traps and logging history
CSCwd03104	Cluster status is not updated across 16 node GCP cluster
CSCwd03113	FMC local backup fails cause of "Update Task: Database integrity check failed" - Syslog server issue
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
CSCwd04210	ASA: ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT
CSCwd05443	Config-dispatcher to fail the deployment immediately when download fails, instead of failing later
CSCwd05756	FTD traceback on Lina due to syslog component.
CSCwd05772	Cisco FXOS Software Arbitrary File Write Vulnerability
CSCwd05814	PDTS write from Daq can fail when PDTS buffer is full eventually leads to block depletion
CSCwd06005	ASA/FTD Cluster Traceback and Reload during node leave
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
CSCwd08402	HTTP URI is sometimes missing from intrusion event view
CSCwd08430	Create a resiliency configuration option for SFTunnel to support HA and FTD connectivity

Bug ID	Headline
CSCwd09093	Access rule policy page takes longer time to load
CSCwd09341	Multiple log files have zero bytes due to logrotate failure
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
CSCwd11165	"Move" option is greyed out on Backup-Restore in FMC
CSCwd11303	ASA might generate traceback in ikev2 process and reload
CSCwd11855	ASA/FTD may traceback and reload in Thread Name 'ikev2_fo_event'
CSCwd12334	Deployment fails with Config Error -- proxy paired
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
CSCwd14972	ASA/FTD Traceback and Reload in Thread Name: pix_flash_config_thread
CSCwd16017	Object edit slowness when it is associated with NAT rules
CSCwd16294	GTP inspection drops packets for optional IE Header Length being too short
CSCwd16517	GTP drops not always logged on buffer and syslog
CSCwd16689	ASA/FTD traceback due to block data corruption
CSCwd16712	Device readiness upgrade check failure - sftunnel sync issue due to time change
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
CSCwd17037	SFDataCorrelator RNA-Stop action should not block when database operations are hung
CSCwd17856	ASA goes for traceback/reload with message - snmp_ma_kill_restart: vf is NULL

Bug ID	Headline
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
CSCwd20627	ASA/FTD: NAT configuration deployment failure
CSCwd20900	HTTP Block Response and Interactive Block response pages not being displayed by Snort3
CSCwd22349	ASA: Unable to connect AnyConnect Cert based Auth with "periodic-authentication certificate" enabled
CSCwd22413	EIGRPv6 - Crashed with "mem_lock: Assertion mem_refcount' failed" on LINA.
CSCwd22907	ASA/FTD High CPU in SNMP Notify Thread
CSCwd23188	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwd23913	FTD in HA traceback multiple times after adding a BGP neighbour with prefix list.
CSCwd24072	rsc_5_min.log store location should move to a different partition
CSCwd24289	Cert serial number not displayed properly in PCA debug and syslogs
CSCwd24639	Functional: FMCv patch upgrade is fails
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
CSCwd26466	Incorrect Frequent Drain of Connection Events alert
CSCwd26867	Device should not move to Active state once Reboot is triggered
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
CSCwd30774	FMC HA - files in tmp/Sync are left on secondary when synchronisation task fails
CSCwd30977	FMC deleted some access-rules due to an incorrect delta generated during the policy deployment.
CSCwd31181	Lina traceback and reload - VPN parent channel (SAL) has an invalid underlying channel
CSCwd31960	Management access over VPN not working when custom NAT is configured
CSCwd32892	lost cac.conf after upgrade to 7.2.1 for FMC smart-card auth

Bug ID	Headline
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
CSCwd33721	ADI process may become unstable when downloading a large number of users
CSCwd33811	Cluster registration is failing because DATA_NODE isn't joining the cluster
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
CSCwd37238	TLS connections to Exchange 2007 server may fail
CSCwd37718	Prevent cluster heartbeat probing failure in virtual platform
CSCwd38526	FMC can allow deployment of NAP in test mode with Decrypt policy
CSCwd38774	ASA: Traceback and reload due to clientless webvpn session closure
CSCwd38775	ASA/FTD may traceback and reload in Thread lina
CSCwd38805	Syslog 106016 is not rate-limited by default
CSCwd39039	FMC - Error message "The server response was not understood. Please contact support." on UI
CSCwd39468	ASA/FTD Traceback and reload when configuring ISAKMP captures on device
CSCwd39710	SFDataCorrelator delay in processing events when the intrusion event rate is high
CSCwd40141	Firepower Management Center GUI view for Snort2 Local Intrusion Rules is missing
CSCwd40260	Serviceability Enhancement - Unable to parse payload are silently drop by ASA/FTD
CSCwd40955	Very long validation time during Policy Deployment due to big network object in SSL policy
CSCwd41083	ASA traceback and reload due to DNS inspection
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
CSCwd41553	PIM register packets are not sent to Rendezvous Point (RP) due to PIM tunnel interface down state
CSCwd41806	deployment failed with OOM (out of memory) for policy_apply.pl process

Bug ID	Headline
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
CSCwd44326	Object NAT edit is failing
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
CSCwd47424	Device name always shows as 'firepower' in CDO event view
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
CSCwd52448	Route leaking of local host having /32 mask may lead to crash
CSCwd52995	FMC not opening deployment preview window
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
CSCwd53448	FPR3100: 4x40 network module LEDs do not blink with traffic
CSCwd53635	AWS: SSL decryption failing with Geneve tunnel interface

Bug ID	Headline
CSCwd53863	Data migration from Sybase to MariaDB taking more time due to large data size of POLICY_SNAPSHOT
CSCwd54360	FP2100: FXOS side changes for HA is not resilient to unexpected lacp process termination issue
CSCwd54439	FMC gives an irrelevant error message for Snort2 to Snort3 rules conversion failure
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'
CSCwd56431	Disable asserts in FTD production builds
CSCwd56774	Misleading drop reason in "show asp drop"
CSCwd56834	[IMS_7_3_0/7_2_0] Lina crashed on VMware 2 node cluster during sending GRE traffic
CSCwd56995	Clientless Accessing Web Contents using application/octet-stream vs text/plain
CSCwd57698	Recursive panic under lina_duart_write
CSCwd57784	Config Archive should get created if Rest-GET method failed on device
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
CSCwd58528	Memory depletion while running EMIX traffic profile on QP HA active node
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
CSCwd61410	mdbtrace.log can fill storage on FMC
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

Bug ID	Headline
CSCwd63580	FPR2100: Increase in failover convergence time with ASA in Appliance mode
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
CSCwd65327	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 41)
CSCwd66815	Lina changes to support - Snort3 traceback in daq-pdts while handling FQDN based traffic
CSCwd66822	FDM FPR2k Netmork module interfaces are greyed out post 7.1.0 update
CSCwd68088	ASA|FTD: Implement different TLS diffie-hellman prime based on RFC recommendation
CSCwd68745	QEMU KVM console got stuck in "Booting the kernel" page
CSCwd69139	Snort 3 traceback on stream prune_lru
CSCwd69236	FMC Connection Event stop displaying latest event
CSCwd69454	Port-channel interfaces of secondary unit are in waiting status after reload
CSCwd70490	Port-channel member port status flag and membership status are Down if LACPDUs are not received
CSCwd70716	Clustering is disabled on all data nodes after power off/on
CSCwd71254	ASA/FTD may traceback and reload in idfw fqdn hash lookup
CSCwd72425	internal.cloudapp.net_snort3 core file is generated on DST setup
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

Bug ID	Headline
CSCwd76622	FTD with Snort3 might have memory corruption BT in snort file with same IP traffic scaling
CSCwd76634	FMC import takes too long
CSCwd78123	ASA/FTD traceback and reload when IPSec/Ikev2 vpn session bringup with dh group 31 in fips mode
CSCwd78624	ASA configured with HA may traceback and reload with multiple input/output error messages
CSCwd78940	Traps are not getting generated in UUT for config change in multicontext
CSCwd79388	intrusion events fail to migrate from MariaDB to MonetDB following FMC upgrade from 7.0.3 to 7.1.0
CSCwd80343	MI FTD running 7.0.4 is on High disk utilization
CSCwd80741	Snort drops Bomgar application packets with Early Application Detection enabled
CSCwd81384	FMC upgrade fails: 114_DB_table_data_integrity_check.pl, stating Snort2IPSNAPCleanup.pm not be found
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"
CSCwd83141	CCL/CLU filters are not working correctly
CSCwd83956	snort2 does not match rules based on application SMTP/SMTPS anymore after a while
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.
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

Bug ID	Headline
CSCwd86313	Unable to access Dynamic Access policy
CSCwd86457	Number of objects are not getting updated under policies>>>Security intelligence >>>Block list
CSCwd86929	Cut-Through Proxy does not work with HTTPS traffic
CSCwd87227	High disk usage due to process_stdout.log and process_stderr.log logrotate failure (no rotation)
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
CSCwd89349	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (seq 42)
CSCwd90112	MariaDB crash (segmentation fault) related to netmap query
CSCwd91421	ASA/FTD may traceback and reload in logging_cfg processing
CSCwd92804	FAN LED flashing amber on FPR2100
CSCwd93376	Clientless VPN users are unable to download large files through the WebVPN portal
CSCwd93465	FMCv 7.2.0 - FTD management IP is not correctly updated on the FMC after changing the FTD mngmnt IP
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
CSCwd94840	snort sets tunnel bypass for geneve encoded packets
CSCwd95415	The Standby Device going in failed state due to snort heartbeat failure
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
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

Bug ID	Headline
CSCwd97276	Unified events and connection events pages don't load anymore. DB Cores generated every few minutes
CSCwd98070	Unable to register new devices to buildout FMC 2700 (FMC HA Active)
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.
CSCwe03991	FTD/ASA traceback and reload during to tmatch compilation process
CSCwe04437	collection of top.log.gz in troubleshoot can be corrupt due to race condition
CSCwe05913	FTD traceback/reloads - Icmp error packet processing involves snp_nat_xlate_identity
CSCwe06724	Database table optimization not working for some of the tables
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"
CSCwe07734	ASA goes to failsafe mode after FXOS upgrade
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
CSCwe10548	ASA binding with LDAP as authorization method with missing configuration
CSCwe11119	ASA: Traceback and reload while processing SNMP packets
CSCwe11189	monetdb log use all of disk spaces on /Volume
CSCwe11304	Snort crashing on FTD
CSCwe11727	Purging of Config Archive failed for all the devices if one device has no versions

Bug ID	Headline
CSCwe12407	High Lina memory use due to leaked SSL handles
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
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
CSCwe17858	FMC HA info is not sync'ed reliably to FTD to support CLOUD_SERVICE
CSCwe18859	After device registration or FMC upgrade, devices sometimes don't send events to the FMC
CSCwe18974	ASA/FTD may traceback and reload in Thread Name: CTM Daemon
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
CSCwe21959	Snort3: Process in D state resulting in OOM with jemalloc memory manager
CSCwe22216	Maria DB crashing/holding high CPU and not allowing users to login GUI and CLI
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
CSCwe23139	FTD HA does not break from FMC GUI but HA bootstrap is removed from devices
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/
CSCwe24880	Using proxy authentication in FMC for smart licensing is failing after upgrading to 7.0.5
CSCwe25025	8x10Gb netmod fails to come online
CSCwe25342	ASA/FTD - SNMP related memory leak behavior when snmp-server is not configured

Bug ID	Headline
CSCwe25391	rpc service detector causing snort traceback due to universal address being an empty string
CSCwe26342	ASA Traceback & reload citing thread name: asacli/0
CSCwe28094	ASA/FTD may traceback and reload after executing 'clear counters all' when VPN tunnels are created
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.
CSCwe29583	ASA/FTD may traceback and reload in Thread Name 'None' at lua_getinfo
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
CSCwe30653	FTD upgrade failure at "999_finish/999_zz_install_bundle.sh" due to bad key cert
CSCwe32058	ASA/FTD may traceback and reload in Thread Name 'ci/console' when checking Geneve capture
CSCwe32448	changing time window settings in FMC GUI event viewers may not work with FMC integrated with SecureX
CSCwe36176	ASA/FTD: High failover delay with large number of (sub)interfaces and http server enabled
CSCwe38640	EventHandler warnings if syslog facility is CONSOLE
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
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.
CSCwe42236	FMC: Domain creation fails with error "Index 'netmap_num' for table 'domain_control_info'"

Bug ID	Headline
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
CSCwe44766	IMS: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
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
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
CSCwe49127	log rotation for process_stderr.log and process_stdout.log files may fail due to race condition
CSCwe50946	Management interface link status not getting synced between FXOS and ASA
CSCwe52640	Certain containers have extra gray borders and certain containers are styled incorrectly
CSCwe54567	Manager gets unregistered on its own from the FTD, show manager shows 'No managers configured'
CSCwe58576	FTD:Node not joining cluster with "Health check detected that control left cluster" due to SSL error
CSCwe58700	ASA/FTD: Revision of cluster event message "Health check detected that control left cluster"
CSCwe58881	After FMC upgrade, SecureX ribbon redirects to US cloud region regardless of the set cloud region
CSCwe59380	FTD: "timeout floating-conn" not operating as expected for connections dependent on VRF routing
CSCwe59809	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (seq 45)
CSCwe59919	FTD Traceback and reload on Thread Name "NetSnmp Event mib process"
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
CSCwe63232	ASA/FTD: Ensure flow-offload states within cluster are the same

Bug ID	Headline
CSCwe63316	Pri-Active FMC NOT triggering registration TASK for FTD to configure standby manager
CSCwe64043	Cisco ASA and FTD ACLs Not Installed upon Reload
CSCwe64404	ASA/FTD may traceback and reload
CSCwe64542	TID python processes stuck at 100% CPU
CSCwe64557	ASA: Prevent SFR module configuration on unsuported platforms
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
CSCwe65492	KP Generating invalid core files which cannot be decoded 7.2.4-64
CSCwe66132	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe70558	FTD: unable to run any commands on CLISH prompt
CSCwe70721	Deployment is blocked due to Pre-deploy Validation Error - Invalid endpoint
CSCwe71220	FTD 3100 Crash in Thead Name: CP Processing
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
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
CSCwe74290	SFDataCorrelator spam seen in /var/log/messages
CSCwe74328	AnyConnect - mobile devices are not able to connect when hostscan is enabled
CSCwe75018	Snort2 rule recommendations increases disabled rule count drastically
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
CSCwe81946	vFMC disk space full due to 40GB of /var/lib/mysql/undo* files

Bug ID	Headline
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
CSCwe83812	SFDataCorrelator log spam when network map is full
CSCwe84079	asa_snmp.log is not rotated, resulting in large file size
CSCwe87873	Requirement: Log rotate utility needs to handle the rotating of the asa-appagent.log file
CSCwe89030	Serial number attribute from the subject DN of certificate should be taken as the username
CSCwe89731	Notification Daemon false alarm of Service Down
CSCwe90095	Username-from-certificate feature cannot extract the email attribute
CSCwe90334	Missing Instance ID in unified_events-2.log
CSCwe91674	Mserver restarts frequently
CSCwe91719	Getting "Unknown" for multiple SSL fields when status is Do Not Decrypt (Unsupported Cipher Suite)
CSCwe93202	FXOS REST API: Unable to create a keyring with type "ecdsa"
CSCwe97277	Observed ASA traceback and reload when performing hitless upgrade while VPN traffic running
CSCwe97704	DOC: Add note regarding FTD/Lina syslog message format
CSCwf00417	FTD: Unable to process a TLS1.2 website with TLS Server Identity with client generating SSL Errors
CSCwf01051	standby in disabled state after QP-MI HA 7.0.3 to 7.2.4-126, APPLY_APP_CONFIG_APPLICATION_FAILURE
CSCwf07030	Upgrade Device listing page is taking more than 15 mins to load page fully with 25 FTDs registered
CSCwf10486	ISE Integration Network filter not accepting multiple comma separated networks
CSCwf11004	Can't log with "info" and "debug".
CSCwf19853	FATAL errors in DBCheck due to missing columns in eventdb table
CSCwf24124	SFDataCorrelator process crashing very frequently on the FMC.
CSCwf28592	In some specific scenarios, object optimizer can cause incorrect rules to be deployed to the device

Bug ID	Headline
CSCwf60584	Health Monitoring to NOT collect route stats for transparent mode FTD
CSCwf66773	Comments disappear from access rules when the rule is copied within or out of Access Policy.
CSCwf67791	Images missing on sf.xml file
CSCwf76945	Packet data is still dropped after upgrade
CSCwf85307	[Snort 3] IPS Policy Overrides not working on Chained Intrusion Policies
CSCwf91650	DOC: FMC New Features by Release page outdated suggested release
CSCwh22565	Snort 3 HTTP Intrusion Prevention System Rule Bypass Vulnerability

Resolved Bugs in Version 7.2.3.1

Table last updated: 2023-04-18

Table 30: Resolved Bugs in Version 7.2.3.1

Bug ID	Headline
CSCwe53746	Firepower 1010E speed and duplex are set to "auto" on the FMC, deployment fails

Resolved Bugs in Version 7.2.3

Table last updated: 2023-02-27

Table 31: Resolved Bugs in Version 7.2.3

Bug ID	Headline
CSCwd09341	Multiple log files have zero bytes due to logrotate failure
CSCwd87227	FTD process log files can fill disk and cause system down events and block user login ability
CSCwc37695	In addition to the c_rehash shell command injection identified in CVE-2022-1292

Resolved Bugs in Version 7.2.2

Table last updated: 2020-11-30

Table 32: Resolved Bugs in Version 7.2.2

Bug ID	Headline
CSCwc10241	Temporary HA split-brain following upgrade or device reboot

Resolved Bugs in Version 7.2.1

Table 33: Resolved Bugs in Version 7.2.1

Bug ID	Headline
CSCvo17612	Return error messages when failing to retrieve objects from database
CSCvw82067	ASA/FTD 9344 blocks depleted due to high volume of fragmented traffic
CSCvx24207	FQDN Object Containing IPv4 and IPv6 Addresses Only Install IPv6 Entries
CSCvx68586	Not able to login to UI/SSH on FMC, console login doesn't prompt for password
CSCvy24180	Default variable set missing on FMC
CSCvy50598	BGP table not removing connected route when interface goes down
CSCvy99348	Shutdown command reboots instead of shutting the FP1k device down.
CSCvz36903	ASA traceback and reload while allocating a new block for cluster keepalive packet
CSCvz69729	Unstable client processes may cause LINA zmqio traceback on FTD
CSCwa08640	MonetDB crashing due to file size error
CSCwa59907	LINA observed traceback on thread name "snmp_client_callback_thread"
CSCwa72528	username form cert feature does not work with SER option
CSCwa75966	ASA: Reload and Traceback in Thread Name: Unicorn Proxy Thread with Page fault: Address not mapped
CSCwa85492	URL lookup responding with two categories
CSCwa89347	Cannot add object to network group on FMC
CSCwa97917	ISA3000 in boot loop after powercycle
CSCwa99171	Chassis and application sets the time to Jan 1, 2010 after reboot
CSCwb01633	FXOS misses logs to diagnose root cause of module show-tech file generation failure
CSCwb05291	Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability
CSCwb06847	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-9-11543'
CSCwb08393	SSL policy deploy failing when using special characters on SSL rule names
CSCwb12465	FIPS self-tests must be run when CC mode is enabled - files are missing
CSCwb13294	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 25)
CSCwb17963	Unable to identify dynamic rate liming mechanism & not following msg limit per/sec at syslog server.

Bug ID	Headline
CSCwb19648	SNMP queries for crasLocalAddress are not returning the assigned IPs for SSL/DTLS tunnels.
CSCwb19664	Malware Block false positives triggered after upgrade to version 7.0.1
CSCwb20926	FDM: Policy deployment failure after upgrade due to unused IKEv1 policies
CSCwb38406	GeoDB updates on multi-domain environment requires a manual policy deployment
CSCwb41361	WR8, LTS18 and LTS21 commit id update in CCM layer (seq 26)
CSCwb49416	ASA snmpd Traceback & cores on an active unit
CSCwb51821	Disk usage errors on Firepower Azure device due to large backup unified files under ngfw directory
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
CSCwb54791	ASA DHCP server fails to bind reserved address to Linux devices
CSCwb58007	CVE-2022-28199: Evaluation for FTDv and ASAv
CSCwb59619	PM needs to restart the Disk Manager after creating ramdisk to make DM aware of the ramdisk
CSCwb65447	FTD: AAB cores are not complete and not decoding
CSCwb65718	FMC is stuck on loading SI objects page
CSCwb67040	FP4112|4115 Traceback & reload on Thread Name: netfs_thread_init
CSCwb68642	ASA traceback in Thread Name: SXP CORE
CSCwb69503	ASA unable to configure aes128-gcm@openssh.com when FIPS enabled
CSCwb71460	ASA traceback in Thread Name: fover_parse and triggered by snmp related functions
CSCwb73248	FW traceback in timer infra / netflow timer
CSCwb74357	FXOS is not rotating log files for partition opt_cisco_platform_logs
CSCwb74571	PBR not working on ASA routed mode with zone-members
CSCwb76129	Some SSL patterns not detected after VDB 356 or higher is installed
CSCwb76423	ASA crashes on fp2100 when checking CRL
CSCwb79812	RIP is advertising all connected Anyconnect users and not matching route-map for redistribution
CSCwb80559	FTD offloads SGT tagged packets although it should not

Bug ID	Headline
CSCwb80862	ASA/FTD proxy arps any traffic when using the built-in 'any' object in translated destination
CSCwb82796	ASA/FTD firewall may traceback and reload when tearing down IKE tunnels
CSCwb83388	ASA HA Active/standby tracebacks seen approximately every two months.
CSCwb83691	ASA/FTD traceback and reload due to the initiated capture from FMC
CSCwb84638	Portmanager/LACP improvement to capture logging events on external event restarts
CSCwb85633	Snmpwalk output of memory does not match show memory/show memory detail
CSCwb85822	Deployment failing when collecting policies.
CSCwb86118	TPK ASA: Device might get stuck on ftp copy to disk
CSCwb86339	ACP Network Validation Failure - Unable to parse ip - Can't call method "binip" - Blank Space
CSCwb86565	FMC upgrade fails due Mismatch in number of entries between /etc/passwd and /etc/shadow
CSCwb87498	Lina traceback and reload during EIGRP route update processing.
CSCwb88651	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwb88887	snp_fp_vxlan_encap_and_grp_send_common: failed to find adj. bp->l3_type = 8, inner_sip message
CSCwb89004	FMC DBcheck.pl hungs at "Checking mysql.rna_flow_stats_template against the current schema"
CSCwb89187	Flex Config allow - "timeout icmp-error hh:mm:ss"
CSCwb90074	ASA: Multiple Context Mixed Mode SFR Redirection Validation
CSCwb90105	Upgrade to 7.2 on FTDv for Nutanix is stuck after reboot
CSCwb90532	ASA/FTD traceback and reload on NAT related function nat_policy_find_location
CSCwb91101	SNMP interface threshold doesn't trigger properly when traffic sent to interface ~4gbps
CSCwb92376	FMC syslog-ng daemon fails to start if log facility is set to ALERT
CSCwb92583	upgrade with a large amount of unmonitored disk space used can cause failed upgrade and hung device
CSCwb92709	We can't monitor the interface via "snmpwalk" once interface is removed from context.
CSCwb93932	ASA/FTD traceback and reload with timer services assertion
CSCwb94190	ASA graceful shut down when applying ACL's with forward reference feature and FIPS enabled.

Bug ID	Headline
CSCwb94312	Unable to apply SSH settings to ASA version 9.16 or later
CSCwb95112	Intrusion Policy shows last modified by admin even though changes are made by a different user
CSCwb95787	FPR1010 - No ARP on switchport VLAN interface after portmanager DIED event
CSCwb97251	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCwb97486	FPR3100: 25G optic may show link up on some 1/10G capable only fiber ports
CSCwc01155	New ACP UI does not load if there are manually entered Location IP literal values in that policy
CSCwc02416	Not re-subscribing to ISE topics after certain ISE connectivity issues.
CSCwc02488	ASA/FTD may traceback and reload in Thread Name 'None'
CSCwc02700	Fragmented packets are dropped when unit leaves cluster
CSCwc03069	Interface internal data0/0 is up/up from cli but up/down from SNMP polling
CSCwc03296	Upgrade fails when using DDNS Service with user and password
CSCwc04162	TTL values causing packets to retransmit
CSCwc04187	Watchdog crash on FP1000 during very heavy AnyConnect SSL VPN tunnel establishment
CSCwc05132	Unable to disable "Retrieve to Management Center
CSCwc07015	snort3 crash due to NULL pointer in TLS Client Hello Evaluation
CSCwc08374	Azure ASA NIC MAC address for Gigeth 0/1 and 0/2 become out of order when adding interfaces
CSCwc09414	ASA/FTD may traceback and reload in Thread Name 'ci/console'
CSCwc10483	ASA/FTD - Traceback in Thread Name: appAgent_subscribe_nd_thread
CSCwc10792	ASA/FTD IPSEC debugs missing reason for change of peer address and timer delete
CSCwc10900	URL cloud lookup if enabled on the FMC may not work on newly registered devices.
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
CSCwc12652	Control-Plane ACL Non-Functional After Upgrade to 9.18(1) or 7.2.0-82 Firepower
CSCwc13017	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
CSCwc13382	DCERPC traffic is dropped after upgrade to snort3 due to Parent flow is closed

Bug ID	Headline
CSCwc13994	ASA - Restore not remove the new configuration for an interface setup after backup
CSCwc14885	FMC logs user out when editing any backdraft page
CSCwc15530	Syslog facility "ALERT" should be changed on FDM since is not supported anymore by syslog-ng
CSCwc18218	Database files on disk grow larger than expected for some frequently updated tables
CSCwc18312	"show nat pool cluster" commands run within EEM scripts lead to traceback and reload
CSCwc23075	Upgrade to MariaDB 10.5.16 to get security vulnerability fixes
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
CSCwc25275	AC Policy UI: Cannot search rules while the rules are loading
CSCwc25451	AC Policy New UI: Adding rule inside a category throws index error
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwc28532	9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwc28660	Snort3: NFSv3 mount may fail for traffic through FTD
CSCwc28928	ASA: SLA debugs not showing up on VTY sessions
CSCwc29591	Retrospective file disposition updates fail due to incorrect eventsecond values in fileevent tables
CSCwc30487	High unmanaged disk usage on Firepower 2110 device
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
CSCwc37196	FPR3100: 8x1G copper netmod may incorrectly report obsolete firmware on boot
CSCwc40322	Onboarding on-prem FMC to CDO using SecureX fails due to User Authentication Failed error
CSCwc40850	FMC authentication with SecureX Orchestration fails
CSCwc41590	Upgrade fail & App Instance fail to start with err "CSP_OP_ERROR. CSP signature verification error."
CSCwc41661	FTD Multiple log files with zero byte size.

Bug ID	Headline
CSCwc59953	Snort3 crash with TLS 1.3
CSCwc65907	snort3 hangs in Crash handler which can lead to extended outage time during a snort crash
CSCwc69376	v7.2 post-upgrade performance issues due to excessive intrusionevent partition tables
CSCwc76658	SFDataCorrelator fails to start after <7.1 to >=7.1.0 upgrade due to compliance.rules "session_both"
CSCwc88583	Deployment fails with error Invalid Snort3IntrusionPolicy mode. Supports only inline and inline-test

Resolved Bugs in Version 7.2.0.1

Table 34: Resolved Bugs in Version 7.2.0.1

Bug ID	Headline
CSCwb88651	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwb93932	ASA/FTD traceback and reload with timer services assertion
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability

Resolved Bugs in Version 7.2.0

Table 35: Resolved Bugs in Version 7.2.0

Bug ID	Headline
CSCwa70008	Expired certs cause Security Intelligence updates to fail
CSCvz67001	FMC Event backups to remote SSH storage targets fail
CSCvy46482	Redundant service-object group created while crypto ACL is used in S2S VPN.
CSCwb22359	Portmanager/LACP improvement to avoid false restarts and increase of logging events
CSCwb64551	FMC Backup failure- Monetdb backup failure code 102
CSCwa00038	Disk corruption occurs when /mnt/disk0 partition is full and blade is rebooted
CSCwa40223	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwa45656	SLR license application failes on manged devices
CSCwa34110	FMC should support southern hemisphere DST configurations
CSCwa32956	Connection events are not sent to Firepower Management Center due to deploy race condition

Bug ID	Headline
CSCvz40765	FMC CPU graph displays the wrong number of Snort and System cores
CSCvy19453	SFDataCorrelator performance problems involving redundant new host events with only MAC addresses
CSCwa12688	Radius external authentication object fails to install on FTD due to invalid retries
CSCwb40001	Long delays when executing SNMP commands
CSCwa95694	Snort cores generated intermittently when SSL policy is enabled on the ASA-SFR module
CSCwa08262	AnyConnect users with mapped group-policies take attributes from default GP under the tunnel-group
CSCvz27235	Multiple Cisco Products Snort Modbus Denial of Service Vulnerability
CSCvz14377	Losing admin and other users from Mysql DB and EO
CSCvz80981	SNMPv3 doesn't work for SFR modules running version 7.0
CSCvz68336	SSL decryption not working due to single connection on multiple in-line pairs
CSCvx75683	The 'show cluster info trace' output is overwhelmed by 'tag does not exist' messages
CSCwa79604	Infinitely running jobs in the task list
CSCwa43497	Datapath deadlocks seen on when sending ICMP PMTU for AnyConnect-SSL
CSCvx59252	FXOS is not rotating log files for management interface
CSCwa15093	Access Policy Control Clear Hit Count throwing Error 403: Forbidden
CSCwa06608	WM 1010 HA Failover is not successful when we give failover active in secondary.
CSCvz41761	FMC Does not allow to create an EIGRP authentication secret key using the $ character
CSCwb46481	SNMPv3 not working after upgrade of FMC
CSCvq29993	FPR2100 ONLY - PERMANENT block leak of size 80, 256, and 1550 memory blocks & blackholes traffic
CSCwa70323	Unable to push extra domains >1024 Character, as part of Custom Attribute under Anyconnect VPN
CSCwb46340	Elektra upgrade failed while upgrading
CSCvz77050	Occasionally policy deployment failure are reported as successful
CSCvz61456	Software upgrade on ASA application may failure without obvious reasons
CSCwb16561	FMC GUI does not load Intrusion Policies
CSCwa74984	Cannot open FMC Access Details -> Configuration tab after FMC upgrade

Bug ID	Headline
CSCvy89713	FMC process dbsrv16 has high CPU utilization after the FMC upgrade
CSCvz73583	FTD does not send the authentication information to proxy server when download the VDB and GEODB.
CSCvz02027	Update host from URL if not available in the packet to stop cloud lookup for null host http requests
CSCwa84862	Unable to remove/modify Standard Access List objects in FMC
CSCvz03524	PKI "OCSP revocation check" failing due to sha256 request instead of sha1
CSCwa85340	Unable to generate the PDF with access policy having large nested objects
CSCwa27488	Fail to import with error "is not a table"
CSCwa89689	Server hello done on TLS stripped by FTD after enabling 'early application detection' with snort3
CSCwb50405	ASA/FTD Traceback in crypto hash function
CSCvz08588	User unrecognized alarm for discovered identity realm users
CSCug96057	Devices with same catagory are catagorized with multiple catagory names
CSCwb11939	ASA/FTD MAC modification is seen in handling fragmented packets with INSPECT on
CSCvz09109	Cluster CCL interface capture shows full packets although headers-only is configured
CSCwb20940	FMC: Add validation checks for the combination of SSL/Snort3/NAP in Detection mode
CSCvz90654	FTD Failover unit does not join HA due to "HA state progression failed due to APP SYNC timeout"
CSCwa55868	QP vFTD Policy Deployment with snort2 Failed with Undefined package variable
CSCvz78331	SNMP polling fails after a re-image
CSCwa70482	ASDM on MAC popup remove hostscan/CSD pkg
CSCvz62517	SRU install should validate files upon completion
CSCwa41918	ssl inspection may have unexpected behavior when evicting certificates
CSCvz29656	FMC connection event search causing high memory utilisation for index.cgi
CSCvz78548	Unable to load Devices --> Certificates page
CSCwa79676	FPR1010 in HA Printing Broadcast Storm Alerts for Multiple Interfaces
CSCwa81395	A carefully crafted request body can cause a buffer overflow in the ...

Bug ID	Headline
CSCwa81143	Unable to save the application policy filter. Save tab is stuck and its continuously loading.
CSCvy75131	Occasionally deleted sensor/interfaces are not removed from security zones
CSCvz73957	FTD stops generating Syslog ID 430002 and 430003 with EventHandler cores
CSCvy24921	SNMPv3 - SNMP EngineID changes after every configuration change
CSCvy24435	FMC GUI can be accessed by an expired password when using .cgi with https://FMCIP/login.cgi
CSCwa97423	Deployment rollback causes brief traffic drop due to order of operations
CSCvz89106	Multiple Cisco Products Server Name Identification Data Exfiltration Vulnerability
CSCwa11088	Access rule-ordering gets automatically changed while trying to edit it before page refresh/load
CSCvz62261	Unable to restrict user access when using ASDM
CSCwb19387	ASA SNMP Poll is failing & show display "Unable to honour this request now.Please try again later."
CSCwa98983	7.1.0.1-25 upgrade failed on KP-HA at 800_post/901_reapply_sensor_policy.pl
CSCwa83078	snort3 - resumed sessions not being decrypted can fail
CSCwb42846	Snort instance CPU stuck at 100%
CSCwb59218	Unable to save DAP Endpoint Criteria as "Disabled"
CSCvx90486	In some cases snmpwalk for ifXTable may not return data interfaces
CSCvz76745	SFDataCorrelator memory growth with cloud-based malware events
CSCvz13564	Firepower 2100 FTD: ssh-access-list configuration are lost after upgrading
CSCwa35179	FTD AC VPN certificate is lost across reloads
CSCwb84225	Evaluation OpenJDK CVEs for ASDM & ASA REST API
CSCwa38996	Big number of repetitive messages in snmpd.log leading to huge log size
CSCvy80380	Disk utilization increasing /var/tmp in FPR4150-ASA chassis
CSCwb01126	DNS server configuration is lost if configuring through RA VPN page on FDM 7.1.0
CSCwa68004	FMC 7.0 FlexConfig blocked mac-address-table aging-time for transparent FTD without any alternativ
CSCwb29126	Cannot use underscore (_) in FMC's realm AD Primary Domain configuration
CSCwa99370	ASDM:DAP config missing AAA Attributes type (Radius/LDAP)

Bug ID	Headline
CSCwa89560	NAT rule modification after rule search changes rule order
CSCvy33501	FDM failover pair - new configured sVTI IPSEC SA is not synced to standby. FDM shows HA not in sync
CSCwa75077	Time-range objects incorrectly populated in prefilter rules
CSCwb07319	Entitlement tags contain invalid character.
CSCwa91070	Cgroup triggering oom-k for backup process
CSCwa45369	Execution of commands appears to result in a new zombie process
CSCwb44048	Event Rate on FMC Health Monitoring Dashboard shows extremely high values
CSCvz72467	Cisco FXOS and NX-OS Software Cisco Discovery Protocol Service Denial of Service
CSCwb37999	Customized Variables name cause Snort3 validation failure
CSCvz73315	Connection events are not seen on FMC, SFDataC doesn't process events from to_import dir
CSCwb21704	FDM: Add validation checks for the combination of SSL/Snort3/NAP in Detection mode
CSCwb32841	NAT (any,any) statements in-states the failover interface and resulting on Split Brain events
CSCvz79930	Snort3 .dmp and crashinfo files are not managed by diskmanager
CSCwa51867	FDM IKEv2 S2S PSK Not Deploying Correctly (Changing Asymmetric to Symmetric PSK)
CSCwa39683	log file flooded by ssl_policy log_error messages when ssl debug is enabled
CSCwa25033	Unexpected HTTP/2 data frame causing segfault
CSCwa39680	Snort stops processing packets when SSL decryption debug enabled - Snort2
CSCvz24238	CiscoÂ Firepower Management Center Cross-site Scripting Vulnerability
CSCwa31373	duplicate ACP rules are generated on FMC 6.6.5 after rule copy.
CSCwa43311	Snort blocking and dropping packet, with bigger size(1G) file download
CSCwa32286	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 125, seq 21)
CSCwb24039	ASA traceback and reload on routing
CSCwa46963	Security: CVE-2021-44228 -> Log4j 2 Vulnerability
CSCwb06543	Increase logging level to diagnose LACP process unexpected restart events
CSCwb43018	Implement SNP API to check ifc and ip belongs to HA LU or CMD interface

Bug ID	Headline
CSCvz76652	Proxy URI URL for URL Filtering (beaker service) includes encoded user/password strings
CSCvz51570	FDM: Management interface name mismatch between HA units and FDM UI / CLI
CSCvz66236	Threshold mis-behavior of "-1" after configuring Type:Both for specific rule
CSCwb59488	ASA/FTD Traceback in memory allocation failed
CSCwa42350	ASA installation/upgrade fails due to internal error "Available resources not updated by module"
CSCvz32593	QP4110 and QW4115 in disabled state with CD App Sync error is Rsync is not enabled on active device
CSCwa76621	HM process OOM killed on FTD 1120
CSCvy67765	FTD VTI reports TUNNEL_SRC_IS_UP false despite source interface is up/up and working
CSCvz02076	Snort reload times out causing restart
CSCwa32628	SFDataCorrelator crash at AddFileToPendingHash() due to race condition
CSCwa07390	Config only FMC: SI feed downloaded file does not match expected checksum
CSCwa97910	Connection event report displays the same device twice
CSCwb48686	ASAV will not boot on REDHAT KVM under Dell PowerEdge R650
CSCwa27822	Lina process remains in started status after a major FTD upgrade to 6.7 or 7.0
CSCwb11325	nullPointerException during 100_ftd_onbox_data_import.pl causes upgrade from 7.0.0 to 7.1.0 to fail
CSCwb32721	Syslog IDs 725021 and 725022 are not listed as valid IDs
CSCwa35596	Registered devices may miss on standby FMC due to AnyConnect HostScan class files sync failure
CSCwa26353	snort3 - Policy does not become dirty after updating LSP -when only custom intrusion policies in use
CSCvz70539	Loggerd process is getting killed due to OOM under high logging rate
CSCvr97157	ENH: Enhance the deployment failure behavior on FTD managed by FDM
CSCwb28047	FMC - "Receiving thread exited with an exception: stoi" causing pxGrid to flap
CSCwa21016	Cisco Firepower Threat Defense Software DNS Enforcement Denial of Service Vulnerability
CSCwb16663	Unable to configure NAP under Advanced Tab in AC policy

Bug ID	Headline
CSCvy82655	REST API - Bulk AC rules creation fails with 422 Unprocessable Entity
CSCvt76856	If a connection to Smart Satellite Server is using a certificate, it cannot be reverted
CSCwa77396	Unable to create Monitor Alerts in FMC
CSCvy50797	Policy deployment may fail if platform settings contain DH group1 for SSL
CSCvz91266	FXOS A crafted request uri-path can cause mod_proxy to forward the request to an origin server...
CSCwa86210	When PM disables mysqld, sometimes it is taking longer than expected to fully shutdown.
CSCwa72641	URL incorrectly extracted for TLS v1.2 self signed URLs when "Early application detection" enabled
CSCwa85138	Multiple issues with transactional commit diagnostics
CSCwa48169	ASA/FTD traceback and reload on netsnmp_handler_check_cache function
CSCvx24470	FTD/FDM: RA VPN sessions disconnected after every deployment if custom port for RA VPN is configured
CSCvz96440	FMC should not create archival for NGIPS devices
CSCwa04171	FMC is generating and removing the AAA commands for the realm unnecessarily
CSCwa31488	FDM High Availability cannot be created using Etherchannel as failover interface.
CSCvy65200	Random characters displayed on DNSQuery field for specific queries.
CSCwb31699	Primary takes active role after reload
CSCwb19648	SNMP queries for crasLocalAddress are not returning the assigned IPs for SSL/DTLS tunnels.
CSCvz70688	default-information originate is configured first then Stub command is not allowed for config
CSCwa03732	Deployment gets hung at snapshot generation phase during deploy
CSCvz69699	FMC UI may become inaccessible due to connection leaks in internal database
CSCwa69279	FMC: Unable to configure AnyConnect MTU for group-policy with only IKEv2 protocol enabled
CSCwa62167	CIAM: Apache-http-server CVE-2021-44790 and CVE-2021-44224
CSCwa48849	ssl unexpected behavior with resumed sessions
CSCwa52215	Uploading firmware triggers data port-channel to flap
CSCvy99218	VDB Version shouldn't be update if fails

Bug ID	Headline
CSCwa50145	FPR8000 sensor UI login creates shell user with basic privileges
CSCvz19634	FTD software upgrade may fail at 200_pre/505_revert_prep.sh
CSCwa85220	Authorization Failure in DCCSM bridge during device registration.
CSCwa21061	FTD upgrade fails on 800_post/100_ftd_onbox_data_import.sh
CSCwa98853	Error F0854 FDM Keyring's RSA modulus is invalid
CSCvv59757	FMC event report generation fails if one is already running
CSCvz66506	Continuous ADI traceback and reload on FPR2100 registered to FMC HA
CSCvz85234	Facilities ALERT, AUDIT, CLOCK and KERN do not work in sending Audit Log to syslog from FMC.
CSCvz84733	LACP packets through inline-set are silently dropped
CSCvx89451	ISA3000 shutdown command reboots system and does not shut system down.
CSCvz43325	Active FMC not deregistering sensors after breaking HA
CSCwa55974	FMC should do an abort of any previous configuration sessions before applying new delta
CSCwa77083	Host information is missing when Security Zones are configured in Network Discovery rules
CSCwa42596	ASA with SNMPv3 configuration observes unexpected reloads with snmpd cores
CSCwb84638	Portmanager/LACP improvement to capture logging events on external event restarts
CSCwa31139	FMC does not check for IP overlap with FTD failover interface
CSCwa08084	FMC hardware appliance restore ends with an error "Unknown Failure Condition"
CSCwb08828	FP1010 Switchport access vlan interface in up/up status but not passing traffic
CSCvz53993	Random packet block by Snort in SSL flow
CSCvv82681	RTC unstable clock register read causes "watchdog: BUG: soft lockup - CPU#0 stuck" error on console
CSCwa67145	Realm download fails if one of the groups is deleted on the AD
CSCvu82743	Snort Generator ID 3 rules disabled following Snort reload
CSCwa17918	Unable to uncheck option Always advertise the default route for OSPF
CSCvp15884	FMC SI Health Alerts: SI URL List and Feeds - Failure False Positives
CSCwa55418	multiple db folders current-policy-bundle after deployment with anyconnect package before upgrade

Bug ID	Headline
CSCvz35787	FTD misleading OVER_SUBSCRIBED flow flag for mid-stream flow
CSCwa53088	snort 2 ssl-debug files may not be written
CSCwa29956	"Interface configuration has changed on device" message may be shown after FTD upgrade
CSCwa60574	ASA traceback and reload on snp_ha_trans_alloc_msg_muxbuf_space function
CSCwb38669	LACP policy name set to Null after upgrade to 7.1.0.90 (2.11.1.154) on FPR1150
CSCwb08644	ASA/FTD traceback and reload at IKEv2 from Scaled S2S+AC-DTLS+SNMP long duration test
CSCvz97196	Can't create Flexconfig Object with ldap-naming-attribute pager cause pager is block.
CSCwb09219	ASA/FTD: OCSP may fail to work after upgrade due to "signer certificate not found"
CSCwa85297	Multi-instance internal portchannel VLANs may be misprogrammed causing traffic loss
CSCvz25197	Multiple Cisco Products Snort Modbus Denial of Service Vulnerability
CSCug44895	upload is failed when more number of cursors are returned from PAS
CSCwa67209	FMC may disable autonegotiation for port-channels with 1Gbps SFP fiber members after FTD upgrade
CSCwb24101	Loggerd syslog has stray incorrect timestamps, e.g. well before FirstPacketSecond
CSCwa51862	LSP downloads fail when using proxy
CSCwa78082	FMC intrusion event search produces inconsistent results
CSCwa80040	FMC NFS configuration failling after upgrade from 6.4.0.4 to 7.0.1
CSCvz52430	FDM UI inaccessible 503 Service Unavailable due to five DNS servers configured
CSCwb07981	Traceback: Standby FTD reboots and generates crashinfo and lina core on thread name cli_xml_server
CSCwb02316	"Non stop forwarding not supported on '1'" error while configuring MAC address
CSCwa92883	Deployment Failed at phase-2 with domain snapshot error
CSCvz61463	FP9k SM-44 6.7.0.2 High CPU on radware vdp Cores after upgrade
CSCwa55142	SNORT3 / SSL / Definitive DND verdict when there's an extra DND bottom rule, instead of regular DND
CSCvy88460	Unable to add additional RADIUS authentication objects after upgrade to 6.7.0
CSCvz72771	ASA/FTD may traceback and reload. "c_assert_cond_terminate" in stack trace

Bug ID	Headline
CSCwb07908	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
CSCwa13721	FDM-managed FTD upgrade failure when custom cipher is selected in SSL Settings
CSCvj08826	FMC ibdata1 file might grow large in size
CSCwa14524	Snort cores in pdts_sftls_daq_acquire with SSL activated
CSCwb43629	License and rule counts telemetry data incorrectly generated for HA managed devices
CSCwa31508	Continuous deployment failure on QW-4145 device
CSCwa79905	FMC NAT Policy report generation does not record the rules every 51*x
CSCwa90660	FMC Realm user/group download doesn't spin the task
CSCwb56718	Policy deployment fails with error- Rule update is running but there are no updates in progress.

For Assistance

Upgrade Guides

In management center deployments, the management center must run the same or newer version as its managed devices. Upgrade the management center first, then devices. Note that you always want to use the upgrade guide for the version of management center or device manager that you are *currently* running—not your target version.

Table 36: Upgrade Guides

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

Install Guides

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

Table 37: Install Guides

Platform	Install Guide	Link
Management center hardware	Getting started guide for your management center hardware model.	https://www.cisco.com/go/fmc-install
Management center virtual	Getting started guide for the management center virtual.	https://www.cisco.com/go/fmcv-quick
Threat defense hardware	Getting started or reimage guide for your device model.	https://www.cisco.com/go/ftd-quick
Threat defense virtual	Getting started guide for your threat defense virtual version.	https://www.cisco.com/go/ftdv-quick
FXOS for the Firepower 4100/9300	Configuration guide for your FXOS version, in the *Image Management* chapter.	https://www.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 Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense

More Online Resources

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

- Documentation: http://www.cisco.com/go/threatdefense-72-docs
- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.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