Cisco Secure Firewall Threat Defense Release Notes, Version 7.6.0

First Published: 2024-06-28

Last Modified: 2024-10-04

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 7.6 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
7.6.0	113	2024-09-16	All	All
	41	2024-06-27	—	No longer available.

Compatibility

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

For compatibility information, see:

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

Features

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

Upgrade Impact

A feature has upgrade impact if upgrading and deploying can cause the system *to process traffic or otherwise act differently without any other action on your part*. This is especially common with new threat detection and application identification capabilities. A feature can also have upgrade impact if upgrading requires that you take action before or after upgrade to avoid an undesirable outcome; for example, if you must change a configuration. 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 18.

Snort

Snort 3 is the default inspection engine for threat defense.

Snort 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 7.6.0

Table 2: Management Center Features in Version 7.6.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Platform			
VMware vSphere/VMware ESXi 8.0 support.	7.6.0	7.6.0	You can now deploy management center virtual and threat defense virtual for VMware on VMware vSphere/VMware ESXi 8.0. See: Cisco Secure Firewall Management Center Virtual Getting Started Guide and Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
Disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200.	7.6.0	7.6.0	You can now disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200. By default, the port is enabled. New/modified threat defense CLI commands: **system support usb show**, **system support usb port disable**, **system support usb port enable** New/modified FXOS CLI commands for the Secure Firewall 3100/4200 in multi-instance mode: **show usb-port**, **disable USB port**, **enable usb-port** See: Cisco Secure Firewall Threat Defense Command Reference and Cisco Firepower 4100/9300 FXOS Command Reference
Device Management			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Device templates.	7.6.0	7.4.1	Device templates allow you to deploy multiple branch devices with pre-provisioned initial device configurations (zero-touch provisioning). You can also apply configuration changes to multiple devices with different interface configurations, and clone configuration parameters from existing devices. Restrictions: You can use device templates to configure a device as a spoke in a site-to-site VPN topology, but not as a hub. A device can be part of multiple hub-and-spoke site-to-site VPN topologies. New/modified screens: **Devices** > **Template Management** Supported platforms: Firepower 1000/2100, Secure Firewall 3100. Note that Firepower 2100 support is for threat defense 7.4.1–7.4.x only; those devices cannot run Version 7.6.0. See: Device Management Using Templates
Serial-number registration (zero-touch provisioning) supported from an on-prem management center.	7.6.0	Mgmt. center must be publicly reachable: 7.2.0 Restriction removed: 7.2.4/7.4.0	You can now register a device using its serial number from an on-prem management center. With templates (requires threat defense 7.4.1+ on the device), you can register multiple devices at once. This feature was previously known as low-touch provisioning. Requires Cisco Security Cloud. For upgraded management centers, your existing CDO integration continues to work until you enable Cisco Security Cloud. New/modified screens: **Devices** > **Device Management** > **Add** > **Device (Wizard)** Supported platforms: Firepower 1000/2100, Secure Firewall 3100. Note that Firepower 2100 support is for threat defense 7.4.1–7.4.x only; those devices cannot run Version 7.6.0. See: Add a Device to the Management Center Using the Serial Number (Zero-Touch Provisioning)
IMDSv2 support for AWS deployments.	7.6.0	7.6.0	Threat defense and management center virtual for AWS now support Instance Metadata Service Version 2 (IMDSv2), a security improvement over IMDSv1. When you enable the instance metadata service on AWS, IMDSv2 Optional mode is still the default, but we recommend you choose IMDSv2 Required. We also recommend you switch your upgraded instances. Platform restrictions: Not available for management center virtual 300 See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide and Cisco Secure Firewall Management Center Virtual Getting Started Guide

Feature	Minimum Management Center	Minimum Threat Defense	Details
AAA for user-defined VRF interfaces.	7.6.0	7.6.0	A device's authentication, authorization, and accounting (AAA) is now supported on user-defined Virtual Routing and Forwarding (VRF) interfaces. The default is to use the management interface. In device platform settings, you can now associate a security zone or interface group having the VRF interface, with a configured external authentication server. New/modified screens: **Devices** > **Platform Settings** > **External Authentication** See: Enable Virtual-Router-Aware Interface for External Authentication of Platform
Delete is now **Unregister** on the device management page.	7.6.0	Any	The **Delete** menu choice was renamed to **Unregister** to better indicate that the device, high-availability pair, or cluster is being unregistered from the management center and not deleted from the high availability pair or cluster or having its configuration erased. The device, high-availability pair, or cluster continues to pass traffic until it is re-registered. New/modified screens: **Devices** > **Device Management** > **More** (⋮) See: Unregister a Device from the Management Center
High Availability/Scalability: Threat Defense			
Multi-instance mode for the Secure Firewall 4200.	7.6.0	7.6.0	Multi-instance mode is now supported on the Secure Firewall 4200. See: Multi-Instance Mode for the Secure Firewall 3100/4200
Multi-instance mode conversion in the management center for the Secure Firewall 3100/4200.	7.6.0	7.6.0	You can now register an application-mode device to the management center and then convert it to multi-instance mode without having to use the CLI. New/modified screens: • **Devices** > **Device Management** > > **Convert to Multi-Instance** • **Devices** > **Device Management** > **Select Bulk Action** > **Convert to Multi-Instance** See: Convert a Device to Multi-Instance Mode
16-node clusters for the Secure Firewall 3100/4200.	7.6.0	7.6.0	For the Secure Firewall 3100 and 4200, the maximum nodes were increased from 8 to 16. See: Clustering for the Secure Firewall 3100/4200

Feature	Minimum Management Center	Minimum Threat Defense	Details
Individual interface mode for Secure Firewall 3100/4200 clusters.	7.6.0	7.6.0	Individual interfaces are normal routed interfaces, each with their own local IP address used for routing. The main cluster IP address for each interface is a fixed address that always belongs to the control node. When the control node changes, the main cluster IP address moves to the new control node, so management of the cluster continues seamlessly. Load balancing must be configured separately on the upstream switch. Restrictions: Not supported for container instances. New/modified screens: • **Devices** > **Device Management** > **Add Cluster** • **Devices** > **Device Management** > **Cluster** > **Interfaces / EIGRP / OSPF / OSPFv3 / BGP** • **Objects** > **Object Management** > **Address Pools** > **MAC Address Pool** See: Clustering for the Secure Firewall 3100/4200 and Address Pools
Deploy threat defense virtual clusters across multiple AWS availability zones.	7.6.0	7.6.0	You can now deploy threat defense virtual clusters across multiple availability zones in an AWS region. This enables continuous traffic inspection and dynamic scaling (AWS Auto Scaling) during disaster recovery. See: Deploy a Threat Defense Virtual Cluster on AWS
Deploy threat defense virtual for AWS in two-arm-mode with GWLB.	7.6.0	7.6.0 simplid	You can now deploy threat defense virtual for AWS in two-arm-mode with GWLB. This allows you to directly forward internet-bound traffic after traffic inspection, while also performing network address translation (NAT). Two-arm mode is supported in single and multi-VPC environments. Restrictions: Not supported with clustering. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
SD-WAN			
SD-WAN wizard.	7.6.0	Hub: 7.6.0 Spoke: 7.3.0	A new wizard allows you to easily configure VPN tunnels between your centralized headquarters and remote branch sites. New/modified screens: **Devices** > **VPN** > **Site To Site** > **Add** > **SD-WAN Topology** See: Configure an SD-WAN Topology Using the SD-WAN Wizard
Access Control: Threat Detection and Application Identification			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Snort ML: neural network-based exploit detector.	7.6.0	7.6.0 with Snort 3	A new Snort 3 inspector, snort_ml, uses neural network-based machine learning (ML) to detect known and 0-day attacks without needing multiple preset rules. The inspector subscribes to HTTP events and looks for the HTTP URI, which in turn is used by a neural network to detect exploits (currently limited to SQL injections). The new inspector is currently disabled in all default policies except maximum detection. A new intrusion rule, GID:411 SID:1, generates an event when the snort_ml detects an attack. This rule is also currently disabled in all default policies except maximum detection. See: Snort 3 Inspector Reference
Bypass EVE block verdict for trusted traffic.	7.6.0	Any with Snort 3	You can now bypass EVE (encrypted visibility engine) block verdicts for known trusted traffic, based on destination network or EVE process name. Connections that bypass EVE in this way have the new **EVE Exempted** reason. New/modified screens: • To add an exception from the access control policy, in the advanced settings, edit and enable **Encrypted Visibility Engine**, enable **Block Traffic Based on EVE Score**, and **Add Exception Rule**. • To add an exception from the Unified Events viewer, right-click a connection that was blocked by EVE and select **Add EVE Exception**. See: Encrypted Visibility Engine
Easily bypass decryption for sensitive and undecryptable traffic.	7.6.0	Any	It is now easier to bypass decryption for sensitive and undecryptable traffic, which protects users and improves performance. New decryption policies now include predefined rules that, if enabled, can automatically bypass decryption for sensitive URL categories (such as finance or medical), undecryptable distinguished names, and undecryptable applications. Distinguished names and applications are undecryptable typically because they use TLS/SSL certificate pinning, which is itself not decryptable. For outbound decryption, you enable/disable these rules as part of creating the policy. For inbound decryption, the rules are disabled by default. After the policy is created, you can edit, reorder, or delete the rules entirely. New/modified screens: **Policies** > **Access Control** > **Decryption** > **Create Decryption Policy** See: Create a Decryption Policy

Feature	Minimum Management Center	Minimum Threat Defense	Details
QUIC decryption.	7.6.0	7.6.0 with Snort 3	You can configure the decryption policy to apply to sessions running on the QUIC protocol. QUIC decryption is disabled by default. You can selectively enable QUIC decryption per decryption policy and write decryption rules to apply to QUIC traffic. By decrypting QUIC connections, the system can then inspect the connections for intrusion, malware, or other issues. You can also apply granular control and filtering of decrypted QUIC connections based on specific criteria in the access control policy. We modified the decryption policy Advanced Settings to include the option to enable QUIC decryption. See: Decryption Policy Advanced Options
Allow Cisco Talos to conduct advanced threat hunting and intelligence gathering using your traffic.	7.6.0	7.6.0 with Snort 3	**Upgrade impact. Upgrade enables telemetry.** You can help Talos (Cisco's threat intelligence team) develop a more comprehensive understanding of the threat landscape by enabling threat hunting telemetry. With this feature, events from special intrusion rules are sent to Talos to help with threat analysis, intelligence gathering, and development of better protection strategies. This setting is enabled by default in new and upgraded deployments. New/modified screens: **System** (⚙) > **Configuration** > **Intrusion Policy Preferences** > **Talos Threat Hunting Telemetry** See: Intrusion Policy Preferences
Access Control: Identity			
Passive identity agent for Microsoft AD.	7.6.0	Any	The passive identity agent identity source sends session data from Microsoft Active Directory (AD) to the management center. Passive identity agent software is supported on: • Microsoft AD server (Windows Server 2008 or later) • Microsoft AD domain controller (Windows Server 2008 or later) • Any client connected to the domain you want to monitor (Windows 8 or later) See: User Control With the Passive Identity Agent

Feature	Minimum Management Center	Minimum Threat Defense	Details
Microsoft Azure AD realms for active or passive authentication.	7.6.0	Active: 7.6.0 with Snort 3 Passive: 7.4.1 with Snort 3	You can now use Microsoft Azure Active Directory (AD) realms for active and passive authentication: • Active authentication using Azure AD: Use Azure AD as a captive portal. • Passive authentication using Cisco ISE (introduced in Version 7.4.1): The management center gets groups from Azure AD and logged-in user session data from ISE. We use SAML (Security Assertion Markup Language) to establish a trust relationship between a service provider (the devices that handle authentication requests) and an identity provider (Azure AD). For upgraded management centers, existing Azure AD realms are displayed as SAML - Azure AD realms. See: User Control with Captive Portal
New connectors for Cisco Secure Dynamic Attributes Connector.	7.6.0	Any	Cisco Secure Dynamic Attributes Connector now supports AWS security groups, AWS service tags, and Cisco Cyber Vision. Version restrictions: For on-prem Cisco Secure Dynamic Attributes Connector integrations, requires Version 3.0. See: AWS service groups connector, AWS service tags connector, Cisco Cyber Vision connector
Easily configure an ISE identity source.	7.6.0	7.6.0	The system can use External RESTful Services (ERS) Operator user credentials to log into a Cisco ISE Primary Authentication Node (PAN), download certificates, and configure the identity source. Restrictions: Not supported for ISE-PIC. See: Cisco ISE Quick Configuration
Event Logging and Analysis			

Feature	Minimum Management Center	Minimum Threat Defense	Details
MITRE and other enrichment information in connection events.	7.6.0	7.6.0 with Snort 3	MITRE and other enrichment information in connection events makes it easy to access contextual information for detected threats. This includes information from Talos and from the encrypted visibility engine (EVE). For EVE enrichment, you must enable EVE. Connection events have two new fields, available in both the unified and classic event viewers: • **MITRE ATT&CK**: Click the progression graph to see an expanded view of threat details, including tactics and techniques. • **Other Enrichment**: Click to see any other available enrichment information, including from EVE. The new Talos Connectivity Status health module monitors management center connectivity with Talos, which is required for this feature. For the specific internet resources required, see Internet Access Requirements. See: Connection and Security-Related Connection Event Fields
Easily filter unified events by event type.	7.6.0	Any	The unified events viewer now has buttons under the Search field that allow you to quickly filter by event type. See: Unified Events
Health Monitoring			
Collect health data without alerting.	7.6.0	Any	You can now disable health alerts/health alert sub-types for ASP Drop, CPU, and Memory health modules, while continuing to collect health data. This allows you to minimize health alert noise and focus on the most critical issues. New/modified screens: In any health policy (**System** (⚙) > **Health** > **Policy**), there are now checkboxes that enable and disable ASP Drop (threat defense only), CPU, and Memory health alert sub-types. See: Health
Apply a default health policy upon device registration.	7.6.0	Any	You can now choose a default health policy to apply upon device registration. On the health policy page, the policy name indicates which is the default. If you want to use a different policy for a specific device post-registration, change it there. You cannot delete the default device health policy. New/modified screens: **System** (⚙) > **Health** > **Policy** > **More** (⋮) > **Set as Default** See: Set a Default Health Policy
Deployment and Policy Management			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Policy Analyzer & Optimizer for access control.	From mgmt. center: 7.6.0 From CDO: 7.2.0	Any	The Policy Analyzer & Optimizer evaluates access control policies for anomalies such as redundant or shadowed rules, and can take action to fix discovered anomalies. You can launch the access control Policy Analyzer & Optimizer directly from a Version 7.6+ management center; this requires Cisco Security Cloud. For Versions 7.2–7.4 management centers, use CDO. New/modified screens: • To enable: **Integration** > **Cisco Security Cloud** > **Enable Policy Analyzer & Optimizer** • To analyze policies: **Policies** > **Access Control**, select policies, click **Analyze Policies**. See: Identifying and Fixing Anomalies with Policy Analyzer & Optimizer
Upgrade			
Improved upgrade process for high availability management centers.	7.6.0	Any	Upgrading high availability management centers is now easier: • You no longer have to manually copy the upgrade package to both peers. Depending on your setup, you can have each peer get the package from the support site, or you can copy the package between peers. • You no longer have to manually run the readiness check on both peers. Running it on one runs it on both. • If you do not have enough disk space to run the upgrade, a new **Clean Up Disk Space** option can help. • You no longer have to manually pause synchronization before upgrade, or resolve split brain after the upgrade; the system now does this automatically. Also, your original active/standby roles are preserved. Note that although you can complete most of the upgrade process from one peer (we recommend the standby), you do have to log into the second peer to actually initiate its upgrade. New/modified screens: **System** (⚙) > **Product Upgrades** Version restrictions: This feature applies to upgrades *from* Version 7.6.0 and later, not *to* 7.6.0. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center

Feature	Minimum Management Center	Minimum Threat Defense	Details
Generate and download post-upgrade configuration change reports from the threat defense and chassis upgrade wizards.	7.6.0	Any	You can now generate and download post-upgrade configuration change reports from the threat defense and chassis upgrade wizards, as long as you have not cleared your upgrade workflow. Previously, you used the Advanced Deploy screens to generate the reports and the Message Center to download them. Note that you can still use this method, which is useful if you want to quickly generate change reports for multiple devices, or if you cleared your workflow. New/modified screens: • **Devices** > **Threat Defense Upgrade** > **Configuration Changes** • **Devices** > **Chassis Upgrade** > **Configuration Changes** See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
Threat defense and chassis upgrade wizards optimized for lower resolution screens.	7.6.0	Any	We optimized the threat defense and chassis upgrade wizards for lower resolution screens (and smaller browser windows). Text appears smaller and certain screen elements are hidden. If you change your resolution or window size mid-session, you may need to refresh the page for the web interface to adjust. Note that the minimum screen resolution to use the management center is 1280 x 720. New/modified screens: • **Devices** > **Threat Defense Upgrade** • **Devices** > **Chassis Upgrade**
Administration			
Cisco AI Assistant for Security.	7.6.0	Any	The Cisco AI Assistant for Security can answer questions about your devices and policies and query documentation and reference materials, streamlining your workflow and boosting overall efficiency. Requires Cisco Security Cloud. See: Use Cisco AI Assistant for Security to Manage Your Threat Defense Devices Effectively

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cisco Security Cloud replaces SecureX.	7.6.0	Any	**Upgrade impact. Enable Cisco Security Cloud after upgrade. Remove the SecureX Firefox Extension.** Registering an on-prem management center to the Cisco Security Cloud gives you access to the latest services such as the Cisco AI Assistant for Security, Policy Analyzer & Optimizer, and Cisco XDR Automation (replaces SecureX orchestration). With a Cisco Security Cloud account, you also have a centralized view of your inventory, and can easily perform Zero-Touch Provisioning, establish consistent policies across management centers, send events to the cloud, and enrich your threat hunts and investigations. New/modified screens: **Integration** > **Cisco Security Cloud** Deprecated screens: • **Integration** > **SecureX** • SecureX ribbon. If you are using Mozilla Firefox, remove the Cisco SecureX Ribbon extension. See: Integrate Management Center with the Cisco Security Cloud
Change management ticket takeover; more features in the approval workflow.	7.6.0	Any user	You can now take over another user's ticket. This is useful if a ticket is blocking other updates to a policy and the user is unavailable. These features are now included in the approval workflow: decryption policies, DNS policies, file and malware policies, network discovery, certificates and certificate groups, cipher suite lists, Distinguished Name objects, Sinkhole objects. See: Change Management
Reporting usability improvements.	7.6.0	Any	When including a table in a report, it's now easier to add, delete, sort, and move columns. New/modified screens: • **Overview** > **Reporting** > **Report Templates** > **Create Report Template** > **Add Table View** > **Fields** > **Edit** • To create a report based on your current event view, you now click **Create Report** instead of **Reporting**. See: Modify Fields in the Report Template Table Format Sections
New theme for the management center.	7.6.0	Any	We introduced a new left-hand navigation theme for the management center. To try it, click your user name in the top right corner and select the **New** theme. We also deprecated the Classic theme. If you were using the Classic theme, the upgrade switches you to the Light theme. See: Change the Web Interface Appearance

Feature	Minimum Management Center	Minimum Threat Defense	Details
Subscribe to Cisco newsletters and other product-related communications.	7.6.0	Any	Provide an email address to receive sales and product renewal conversations, new release adoption newsletters, and other product-related communications from Cisco. Each management center internal user has their own email address. New/modified screens: **System** (⚙) > **Users** > **Edit** > **Email Address** See: Add or Edit an Internal User
Updated internet access requirements for URL filtering.	7.6.0	Any	**Upgrade impact. The system connects to new resources.** The system now requires access to *.talos.cisco.com for URL filtering data. It no longer requires access to regsvc.sco.cisco.com or est.sco.cisco.com. For a full list of resources required for this feature, see Internet Access Requirements.
Threat defense high availability automatically resumes after restoring from backup.	Any	7.2.10 7.4.3	When replacing a failed unit in a high availability pair, you no longer have to manually resume high availability after the restore completes and the device reboots. You should still confirm that high availability has resumed before you deploy. Version restrictions: Not supported with threat defense Version 7.0–7.0.6, 7.1.x, 7.2.0–7.2.9, 7.3.x, or 7.4.0–7.4.2. See: Restoring Management Centers and Managed Devices
Performance			
Hardware DTLS 1.2 crypto acceleration for the Secure Firewall 3100/4200.	7.6.0	7.6.0 with Snort 3	The Secure Firewall 3100/4200 now supports DTLS 1.2 cryptographic acceleration and egress optimization, which improves throughput of DTLS-encrypted and decrypted traffic. This is automatically enabled on new and upgraded devices. To disable, use FlexConfig. New/modified FlexConfig commands: **flow-offload-dtls**, **flow-offload-dtls egress-optimization**, **show flow-offload-dtls** See: DTLS Crypto Acceleration
Object group search performance enhancements.	7.6.0	Any	Object group search is now faster and uses fewer CPU resources. New CLI commands: **clear asp table network-object**, **show asp table network-object**, **debug acl ogs** Modified CLI comments (enhanced output): , **packet-tracer**, **show access-list**, **show object-group** See: Configure Object Group Search and Cisco Secure Firewall Threat Defense Command Reference
Troubleshooting			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Troubleshoot Snort 3 performance issues with a CPU and rule profiler.	7.6.0	7.6.0 with Snort 3	New CPU and rule profilers help you troubleshoot Snort 3 performance issues. You can now monitor: • CPU time taken by Snort 3 modules/inspectors to process packets. • CPU resources each module is consuming, relative to the total CPU consumed by the Snort 3 process. • Modules with unsatisfactory performance when Snort 3 is consuming high CPU. • Intrusion rules with unsatisfactory performance. New/modified screens: **Devices** > **Troubleshoot** > **Snort 3 Profiling** Platform restrictions: Not supported for container instances. See: Advanced Troubleshooting for the Secure Firewall Threat Defense Device
Receive additional threat defense troubleshooting syslogs, and view them as unified events. VPN troubleshooting syslogs moved.	7.6.0	Any with Snort 3	You can now configure threat defense devices to send all device troubleshooting syslogs (instead of just VPN troubleshooting syslogs) to the management center. New/modified screens: • To send device troubleshooting syslogs to the management center, use threat defense platform settings: **Devices** > **Platform Settings** > **Syslog** > **Logging to Secure Firewall Management Center** • To view all device troubleshooting syslogs, **Devices** > **Troubleshooting Logs** replaces **Devices** > **VPN** > **Troubleshooting**. • To view device troubleshooting syslogs in context with other events, use **Analysis** > **Unified Events**, where we added a **Troubleshoot Events** type. See: Configure Syslog Logging for Threat Defense Devices and View Troubleshooting Syslogs in the Secure Firewall Management Center
Application detection debug logs in connection-based troubleshooting.	7.6.0	7.6.0 with Snort 3	For connection-based troubleshooting, you can now collect debug logs from application detectors. New/modified CLI commands: **debug packet-module appid** enables and sets the severity level for application detector debug logs. You can choose 3 (error), 4 (warning), or 7 (debug). See: Connection-Based Troubleshooting and Cisco Secure Firewall Threat Defense Command Reference

Feature	Minimum Management Center	Minimum Threat Defense	Details
Packet tracer improvements.	7.6.0	Varies.	Packet tracker improvements allow you to: • Capture and replay identity trace data (requires threat defense 7.6.0 with Snort 3). • Replay packet trace data on NAT-configured devices. • Replay packet trace data that imitates the actual timing of the packets, for a more realistic simulation. • Save packet trace data as PCAP file, which can be viewed using third-party tools like Wireshark. New/modified commands: • To enable the timestamp option, use the **honor-timestamp** keyword in the **packet-tracer** command: **packet-tracer input***ifc_name* **pcap***pcap_filename* [**honor-timestamp**] • To store the device-generated packet trace data as part of the PCAP file, use the **export-pcapng** keyword in the **show packet tracer** command: **show packet-tracer pcap trace** [**export-pcapng**] See: Packet Tracer and Cisco Secure Firewall Threat Defense Command Reference
Cisco Success Network and Cisco Support Diagnostics are enabled by default.	7.6.0	Any	**Upgrade impact. Upgrade opts into Cisco Success Network and Cisco Support Diagnostics.** Cisco Success Network and Cisco Support Diagnostics are now opt-out, instead of opt-in. If you were previously opted out, upgrade changes that. Also, you can no longer opt out when you register the management center to the Cisco Smart Software Manager (CSSM). You can still opt out on **Integration** > **Cisco Security Cloud** > **Cisco Security Cloud Support**. See: Integrate Management Center with the Cisco Security Cloud
Deprecated Features			
End of support: Firepower 2110, 2120, 2130, 2140.	—	7.6.0	You cannot run Version 7.6+ on the Firepower 2110, 2120, 2130, or 2140. Although a newer management center can manage older devices, the Version 7.6 documentation only includes features supported in Version 7.6 threat defense. For features that are only supported with older devices, refer to the management center guide that matches your threat defense version.

Feature	Minimum Management Center	Minimum Threat Defense	Details
End of management support: ASA FirePOWER and NGIPSv.	7.6.0	—	You cannot manage Classic devices (ASA FirePOWER and NGIPSv) with a Version 7.6+ management center. This is because Classic devices cannot be upgraded past Version 7.0, and a Version 7.6 management center can only manage devices as far back as Version 7.1. New/modified screens: For new and upgraded management centers, Classic-specific configurations and screens are removed. This includes platform settings, NAT, syslog logging, licensing, and so on. In some cases, creating threat defense configurations is quicker because you do not have to begin by selecting a device type.
Deprecated: Copy upgrade packages ("peer-to-peer sync") from device to device.	7.6.0	7.6.0	You can no longer use the threat defense CLI to copy upgrade packages between devices over the management network. If you have limited bandwidth between the management center and its devices, configure devices to get upgrade packages directly from an internal web server. Deprecated CLI commands: **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status**
End of support: analytics-only capabilities with the full range of threat defense devices supported with cloud-delivered Firewall Management Center.	Any	7.2.0	If you are co-managing Version 7.0.x devices with cloud-delivered Firewall Management Center and an on-prem analytics-only management center, you cannot upgrade the analytics management center to Version 7.6 (which would allow you to add Version 7.6 devices) until you upgrade the older devices to 7.2+, or replace or remove them. See: Cisco Secure Firewall Management Center Compatibility Guide

Device Manager Features in Version 7.6.0

Table 3: Device Manager Features in Version 7.6.0

Feature	Description
Platform Features	
VMware vSphere/VMware ESXi 8.0 support.	You can now deploy threat defense virtual for VMware on VMware vSphere/VMware ESXi 8.0. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
Disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100.	You can now disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100. By default, the port is enabled. New/modified CLI commands: **system support usb show**, **system support usb port disable**, **system support usb port enable** See: Cisco Secure Firewall Threat Defense Command Reference

Feature	Description
IMDSv2 support for AWS deployments.	Threat defense virtual for AWS now supports Instance Metadata Service Version 2 (IMDSv2), a security improvement over IMDSv1. When you enable the instance metadata service on AWS, IMDSv2 Optional mode is still the default, but we recommend you choose IMDSv2 Required. We also recommend you switch your upgraded instances. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
End of support: Firepower 2110, 2120, 2130, 2140.	You cannot run Version 7.6+ on the Firepower 2110, 2120, 2130, or 2140.
Firewall and IPS Features	
Object group search performance enhancements.	Object group search is now faster and uses fewer resources. New CLI commands: **clear asp table network-object**, **show asp table network-group** Modified CLI comments (enhanced output): **debug acl logs**, **packet-tracer**, **show access-list**, **show object-group** See: Cisco Secure Firewall Threat Defense Command Reference
Administrative and Troubleshooting Features	
Updated internet access requirements for URL filtering.	**Upgrade impact. The system connects to new resources.** The system now requires access to *.talos.cisco.com for URL filtering data. It no longer requires access to regsvc.sco.cisco.com or est.sco.cisco.com.
Canadian French translation for Firewall Device Manager.	Firewall Device Manager includes a Canadian French version in addition to English, Chinese, Japanese, and Korean. You must select Canadian French as the browser language. You cannot see the French version by selecting any other type of French.
Performance Features	
Hardware DTLS 1.2 crypto acceleration for the Secure Firewall 3100.	The Secure Firewall 3100 now supports DTLS 1.2 cryptographic acceleration and egress optimization, which improves throughput of DTLS-encrypted and decrypted traffic. This is automatically enabled on new and upgraded devices. To disable, use FlexConfig. New/modified FlexConfig commands: **flow-offload-dtls**, **flow-offload-dtls egress-optimization**, **show flow-offload-dtls**

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 4: Upgrade Impact Features for Management Center

Target Version	Features with Upgrade Impact
7.6.0+	• Allow Cisco Talos to conduct advanced threat hunting and intelligence gathering using your traffic. • Cisco Security Cloud replaces SecureX. • Updated internet access requirements for URL filtering. • Cisco Success Network and Cisco Support Diagnostics are enabled by default.
7.4.1+	• 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. • Improved management center memory usage calculation, alerting, and swap memory monitoring. • Updated web analytics provider.
7.4.0+	• Configure threat defense devices as NetFlow exporters from the management center web interface. • Access control performance improvements (object optimization). • Smaller VDB for lower memory Snort 2 devices.
7.3.0+	• Configure BFD for BGP from the management center web interface. • Updated internet access requirements for Smart Licensing.
7.2.4+	• Automatically update CA bundles.

Target Version	Features with Upgrade Impact
7.2.0+	• Configure VXLAN from the management center web interface. • Configure EIGRP from the management center web interface.

Upgrade Impact Features for Threat Defense with Management Center

Check all releases between your current and target version.

Table 5: Upgrade Impact Features for Threat Defense with Management Center

Target Version	Features with Upgrade Impact
7.4.1+	• IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100. • Captive portal support for multiple Active Directory realms (realm sequences). • Firmware upgrades included in FXOS upgrades. • Merged management and diagnostic interfaces. • Sensitive data detection and masking.
7.3.0+	• Auto-upgrade to Snort 3 after successful threat defense upgrade is no longer optional. • Combined upgrade and install package for Secure Firewall 3100. • NetFlow support for Snort 3 devices.
7.2.4+	• Automatically update CA bundles.
7.2.0+	• Autoscale for threat defense virtual for GCP.

Upgrade Impact Features for Threat Defense with Device Manager

Check all releases between your current and target version.

Table 6: Upgrade Impact Features for Threat Defense with Device Manager

Target Version	Features with Upgrade Impact
7.6.x	• Updated internet access requirements for URL filtering.
7.4.1+	• Merged management and diagnostic interfaces. • IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100. • Sensitive data detection and masking. • Firmware upgrades included in FXOS upgrades. • Default NTP server updated.

Target Version	Features with Upgrade Impact
7.3.0+	• TLS 1.3 support in SSL decryption policies, and configurable behavior for undecryptable connections. • Combined upgrade and install package for Secure Firewall 3100.
7.2.4+	• Automatically update CA bundles.

Upgrade Guidelines

The following sections contain release-specific upgrade warnings and guidelines. You should also check for features and bugs with upgrade impact. For general information on time/disk space requirements and on system behavior during upgrade, see the appropriate upgrade guide: For Assistance, on page 73.

Upgrade Guidelines for Management Center

Table 7: Upgrade Guidelines for Management Center

Target Version	Current Version	Guideline	Details
7.6.x	7.1.x–7.6.x	There are no upgrade warnings or guidelines for this version right now, but you should still check for features and bugs with upgrade impact.	

Upgrade Guidelines for Threat Defense with Management Center

Table 8: Upgrade Guidelines for Threat Defense with Management Center

Target Version	Current Version	Guideline	Details
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.

Upgrade Guidelines for Threat Defense with Device Manager

Table 9: Upgrade Guidelines for Threat Defense with Device Manager

Target Version	Current Version	Guideline	Details
7.6.x	7.1.x–7.6.x	There are no upgrade warnings or guidelines for this version right now, but you should still check for features and bugs with upgrade impact.	

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.

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

Some devices may require a chassis upgrade (FXOS and firmware) before you upgrade the software:

- Secure Firewall 3100/4200 in multi-instance mode: Any upgrade can require a chassis upgrade. Although you upgrade the chassis and threat defense separately, one package contains the chassis and threat defense upgrades and you perform both from the management center. The compatibility work is done for you. It is possible to have a chassis-only upgrade or a threat defense-only upgrade.
- Firepower 4100/9300: Major versions require a chassis upgrade.

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 10: 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 7.6.0

Table last updated: 2024-09-19

Table 11: Open Bugs in Version 7.6.0

Bug ID	Headline
CSCwj81646	UDP throughput highly variable on snort reload
CSCwk33511	low memory/stress causing block double free and reload
CSCwk36770	FMC - SDWAN - Same IKE identity issues between multiple topologies
CSCwk76563	SDWAN: Same spoke in another topology with different community causes issues in route redistribution
CSCwk90798	FMC HA role switch secondary FMC does not get event configuration and threat hunting is lost on FTD
CSCwk98275	Unable to trigger second immediate backup after first scheduled backup completed
CSCwm34180	Traffic on port-channel/port-channel subinterfaces not working with device template registration
CSCwm38714	Change management: Error in save of SD-WAN topology if security zone is added inline in the wizard
CSCwm40854	Break FTD-HA pair fails on MI app
CSCwm44162	Child domain template adding through Global Device wizard page is not working
CSCwm44656	Erroneous message - Interface 'management0' has no link - during device onboarding
CSCwm46752	Edit configuration on Secure Firewall 3100 L3 Cluster fails with BGP enabled
CSCwm47187	Policy deploy failing constantly after changing interface nameif if interface used in SAML CP rule
CSCwm47308	Policy deployment failing constantly on Secure Firewall cluster data node post cluster break
CSCwm51467	SSL Server check-box is missing only in default new theme for Device- >Certificates- > Add New Cert

Resolved Bugs in Version 7.6.0

Table last updated: 2024-09-16

Table 12: Resolved Bugs in Version 7.6.0

Bug ID	Headline
CSCvn25053	FMC: critical processes can not boot up including vmsDBEngine
CSCvq48086	ASA concatenates syslog event to other syslog event while sending to the syslog server

Bug ID	Headline
CSCvt25221	FTD traceback in Thread Name cli_xml_server when deploying QoS policy
CSCvu24703	FTD - Flow-Offload should be able to coexist with Rate-limiting Feature (QoS)
CSCvx04003	Lack of throttling of ARP miss indications to CP leads to oversubscription
CSCvx37329	Remove Syslog Messages 852001 and 852002 in Firewall Threat Defense
CSCvx44261	SNMPv3: Special characters used in FXOS SNMPv3 configuration causes authentication errors
CSCvx69675	FXOS Major Faults about adapter host and virtual interface being down
CSCvx71936	FXOS: Fault "The password encryption key has not been set." displayed on FPR1000 and FPR2100 devices
CSCvx74133	App-instance showing as Started instead of Online
CSCvz03407	IPTables.conf file is disappearing resulting in backup and restore failure.
CSCvz07712	Deployment fails with internal_errors - Cannot get fresh id
CSCvz22945	ERROR: Deleted IDB found in in-use queue - message misleading
CSCvz56980	Getting Unprocessable URL categories objects when using API call
CSCvz68713	PLR license reservation for ASAv5 is requesting ASAv10
CSCvz70310	ASA may fail to create NAT rule for SNMP with: "error NAT unable to reserve ports."
CSCvz85153	show access-control-config doesn't show NAP/IPS policy name
CSCwa34287	ASA: FPR11xx: Loss of NTP sync following a reload after upgrade
CSCwa35200	Some syslogs for AnyConnect SSL are generated in admin context instead of user context
CSCwa76822	Tune throttling flow control on syslog-ng destinations
CSCwa82791	ENH: Support for snapshots of RX queues on InternalData interfaces when "Blocks free curr" goes low
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
CSCwa99932	ASA/FTD stuck after crash and reboot
CSCwb08189	Microsoft update traffic blocked with Snort version 3 Malware inspection
CSCwb44848	ASA/FTD Traceback and reload in Process Name: lina
CSCwb55243	snort3 crashinfo sometimes fails to collect all frames

Bug ID	Headline
CSCwb94431	MFIB RPF failed counter instead of Other drops increments when outgoing interface list is Null
CSCwb95453	ASA: The timestamp for all logs generated by Admin context are the same
CSCwb95784	cache and dump last 20 rmu request response packets in case failures/delays while reading registers
CSCwb95850	Snort down due to missing lua files because of disabled application detectors (PM side)
CSCwc05375	AnyConnect SAML - Client Certificate Prompt incorrectly appears within External Browser
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwc31953	Prevention of RSA private key leaks regardless of root cause.
CSCwc49655	FTPS getting ssl3_get_record:bad record type during connection for KK and DR rules
CSCwc76419	Unnecessary FAN error logs needs to be removed from thermal file
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'
CSCwc89924	FXOS ASA/FTD SNMP OID to poll Internal-data 'no buffer' interface counters
CSCwd02864	logging/syslog is impacted by SNMP traps and logging history
CSCwd04210	ASA: ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT
CSCwd04436	User/group download may fail if a different realm is changed and saved
CSCwd07098	25G CU SFPs not working in Brentwood 8x25G netmod
CSCwd07278	ASA/FTD tmatch compilation check when unit joins the cluster, when TCM is off
CSCwd08098	cacert.pem on FMC expired and all the devices showing as disabled.
CSCwd09870	AnyConnect SAML using external browser and round robin DNS intermittently fails
CSCwd10822	Failover trigger due to Inspection engine in other unit has failed due to disk failure
CSCwd10880	critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on FPR 1100/2100/3100
CSCwd16906	ASA/FTD may traceback and reload in Thread Name 'lina' following policy deployment
CSCwd22413	ASA/FTD: Traceback and reload in Thread Name: EIGRP-IPv4
CSCwd23188	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwd30856	User with no vpn-filter may get additional access when per-user-override is set

Bug ID	Headline
CSCwd33054	DHCP Relay is looping back the DHCP offer packet causing dhcprelay to fail on the FTD/ASA
CSCwd34079	FTD: Traceback & reload in process name lina
CSCwd37135	ASA/FTD traceback and reload on thread name fover_fail_check
CSCwd38583	ASA/FTD: Command "no snmp-server enable oid mempool" enabled by default or enforced during upgrades
CSCwd39442	ssl policy errors: Unable to get server certificate's internal cached status
CSCwd39506	SSL Policy DND default Rule fails on error unsupported cipher suite and SKE error.
CSCwd43666	Analyze why there is no logrotate for /opt/cisco/config/var/log/ASAconsole.log
CSCwd46061	FPR 2100: 10G interfaces with 1G SFP goes down post reload
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
CSCwd47278	256 / 1550 Block leak with TLS1.3 session
CSCwd50155	Evaluate FMC for CVE-2022-42252
CSCwd50218	ASA restore is not applying vlan configuration
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'
CSCwd56431	Disable asserts in FTD production builds
CSCwd59736	ASA/FTD: Traceback and reload due to SNMP group configuration during upgrade
CSCwd61082	FMC UI Showing inaccurate data in S2S VPN Monitoring page
CSCwd62138	ASA Connections stuck in idle state when DCD is enabled
CSCwd62859	Cisco ASA and FTD AnyConnect SSL/TLS VPN Denial of Service Vulnerability
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

Bug ID	Headline
CSCwd67100	ASA traceback and reload on Datapath process
CSCwd67101	FPR1150 : Exec format error seen and the device hung until reload when erase secure all is executed
CSCwd68088	ASA|FTD: Implement different TLS diffie-hellman prime based on RFC recommendation
CSCwd68745	QEMU KVM console got stuck in "Booting the kernel" page
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
CSCwd71254	ASA/FTD may traceback and reload in idfw fqdn hash lookup
CSCwd72680	FXOS: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
CSCwd74839	30+ seconds data loss when unit re-join cluster
CSCwd76622	FTD with Snort3 might have memory corruption BT in snort file with same IP traffic scaling
CSCwd77581	Cisco ASA and FTD ICMPv6 Message Processing Denial of Service Vulnerability
CSCwd78624	ASA configured with HA may traceback and reload with multiple input/output error messages
CSCwd80343	MI FTD running 7.0.4 is on High disk utilization
CSCwd80741	Snort drops Bomgar application packets with Early Application Detection enabled
CSCwd81123	High CPU Utilization on FXOS for processes smConlogger
CSCwd81538	FTD Traffic failure due to 9344 block depletion in peer_proxy_tx_q
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"
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.
CSCwd85073	Snort3 stream core found init_tcp_packet_analysis

Bug ID	Headline
CSCwd85178	AWS ASAv PAYG Licensing not working in GovCloud regions.
CSCwd85927	Traceback and reload when webvpn users match DAP access-list with 36k elements
CSCwd86535	ASA/FTD: Traceback and Reload on Netflow timer infra
CSCwd86929	Cut-Through Proxy does not work with HTTPS traffic
CSCwd87438	Enhance logging mechanism for syslogs
CSCwd88585	ASA/FTD NAT Pool Cluster allocation and reservation discrepancy between units
CSCwd89095	Stratix5950 and ISA3000 LACP channel member SFP port suspended after reload
CSCwd89811	Traffic fails in Azure ASAv Clustering after "timeout conn" seconds
CSCwd89848	ASA/FTD failure due to heartbeat loss between chassis and blade
CSCwd90894	ASA: After upgrade cannot connect via ssh to interface
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
CSCwd94096	Anyconnect users unable to connect when ASA using different authentication and authorization server
CSCwd94183	Blade not coming up after FXOS update support on multi-instance due to ssp_ntp.log log rotation prob
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
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	FPR41xx/9300: Blade does not capture or log a reboot signal
CSCwd97020	ASA/FTD: External IDP SAML authentication fails with Bad Request message
CSCwd98316	Cisco ASA and FTD Software VPN Packet Validation Vulnerability
CSCwd99592	Optimization of Side Bar loading for HealthMon page
CSCwe00864	License Commands go missing in Cluster data unit if the Cluster join fails.
CSCwe01977	ASA/FTD may traceback and reload after a reload with DHCPv6 configured

Bug ID	Headline
CSCwe02012	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe03529	FTD traceback and reload while deploying PAT POOL
CSCwe03631	Need to provide rate-limit on "logging history <mode>"
CSCwe03991	FTD/ASA traceback and reload during to tmatch compilation process
CSCwe04746	Unexpected "No Traffic" health alert on Standby HA Data Interface where no data flows
CSCwe05913	FTD traceback/reloads - Icmp error packet processing involves snp_nat_xlate_identity
CSCwe06562	FPR1K/FPR2K: Increase in failover time in Transparent Mode with high number of Sub-Interfaces
CSCwe07722	Cluster data unit drops non-VPN traffic with ASP reason "VPN reclassify failure
CSCwe08729	FPR1120:connections are getting teardown after switchover in HA
CSCwe09074	None option under trustpoint doesn't work when CRL check is failing
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
CSCwe10670	Identity network filter not removed from FTD
CSCwe11119	ASA: Traceback and reload while processing SNMP packets
CSCwe11754	Nodes randomly fail to join cluster due to internal clustering error
CSCwe11902	FTD: HA crash and interfaces down on FPR4200
CSCwe12407	High Lina memory use due to leaked SSL handles
CSCwe12645	Secondary state flips between Ready & Failed when node is rebooted and mgmt interface is shutdown
CSCwe12705	multimode-tmatch_df_hijack_walk traceback observed during shut/unshut on FO connected switch interfa
CSCwe13781	IKEv2 Multi-DVTI Hub Support FTD/ASA
CSCwe14174	FTD - 'show memory top-usage' providing improper value for memory allocation
CSCwe14417	FTD: IP SLA Pre-emption not working even when destination becomes reachable
CSCwe14514	ASA/FTD Traceback and reload of Standby Unit while removing capture configurations
CSCwe15280	Multiple Cisco Products Snort 3 Access Control Policy Bypass Vulnerability

Bug ID	Headline
CSCwe16905	cdFMC : User with VPN Sessions Manager Role can't access cdFMC
CSCwe18216	null connection error seen in logs
CSCwe18462	ASA/FTD: Improve GTP Inspection Logging
CSCwe18467	ASA/FTD: GTP Inspection engine serviceability
CSCwe18472	[FTD Multi-Instance][SNMP] - CPU OIDs return incomplete list of associated CPUs
CSCwe18974	ASA/FTD may traceback and reload in Thread Name: CTM Daemon
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
CSCwe20918	Cisco ASA and FTD Software Remote Access SSL VPN Multiple Certificate Auth Bypass
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
CSCwe21884	Write wrapper around "kill" command to log who is calling it
CSCwe21959	Snort3: Process in D state resulting in OOM with jemalloc memory manager
CSCwe22152	SNMPD cores seen in in snmp_sess_close and notifyTable_register_notifications
CSCwe22176	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 43)
CSCwe22302	Partition "/opt/cisco/config" gets full due to wtmp file not getting logrotated
CSCwe22386	Unexpected firewalls reloads with traceback.
CSCwe22431	[SXP-UserIP Muted Leader]FMC HA Join flushes FW IP_SGT Mapping and restreams in registered sensors.
CSCwe23039	NTP polling frequency changed from 5 minutes to 1 second causes large useless log files
CSCwe24532	Multiple instances of nvram.out log rotated files under /opt/cisco/platform/logs/
CSCwe25025	8x10Gb netmod fails to come online
CSCwe25342	ASA/FTD - SNMP related memory leak behavior when snmp-server is not configured
CSCwe25391	rpc service detector causing snort traceback due to universal address being an empty string
CSCwe25412	Azure D5v2 FTDv unable to send traffic - underruns and deplete DPDK buffers observed

Bug ID	Headline
CSCwe26342	ASA Traceback & reload citing thread name: asacli/0
CSCwe26612	FTD taking longer than expected to form OSPF adjacencies after a failover switchover
CSCwe28094	ASA/FTD may traceback and reload after executing 'clear counters all' when VPN tunnels are created
CSCwe28362	Copy and pasting rules is broken and give blank error message in ID policy
CSCwe28407	LINA traceback with icmp_thread
CSCwe28726	The command "app-agent heartbeat" is getting removed when deleting any created context
CSCwe28912	FPR 4115- primary unit lost all HA config after ftd HA upgrade
CSCwe29179	CLUSTER: ICMP reply arrives at director earlier than CLU add flow request from flow owner.
CSCwe29529	FTD MI does not adjust PVID on vlans attached to BVI
CSCwe29583	ASA/FTD may traceback and reload in Thread Name 'None' at lua_getinfo
CSCwe29850	ASA/FTD Show chunkstat top command implementation
CSCwe30228	ASA/FTD might traceback in funtion "snp_fp_l2_capture_internal" due to cf_reinject_hide flag
CSCwe30359	Traffic drops with huge rule evaluation on snort
CSCwe30867	Workaround to set hwclock from ntp logs on low end platforms
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
CSCwe33130	Supervisor does not reboot unresponsive module/blade due to IERR with minor severity sensor ID 79
CSCwe36176	ASA/FTD: High failover delay with large number of (sub)interfaces and http server enabled
CSCwe37132	TLS Server Identity may cause certain clients to produce mangled Client Hello
CSCwe37453	Gateway is not reachable from standby unit in admin and user context with shared mgmt intf
CSCwe38029	Multiple traceback seen on standby unit.
CSCwe39425	2100: Power switch toggle leads to ungraceful shutdowns and "PowerCycleRequest" reset

Bug ID	Headline
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
CSCwe41766	FTD may not reboot as expect post upgrade if bundled FXOS version is the same on old and new version
CSCwe41898	ASA: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
CSCwe42061	Deleting a BVI in FTD interfaces is causing packet drops in other BVIs
CSCwe42986	Classic and Unified Events should handle cases when SMC is unreachable
CSCwe44311	FP2100:Update LINA asa.log files to avoid recursive messages-<date>.1.gz rotated filenames
CSCwe44672	Syslog ASA-6-611101 is generated twice for a single ssh connection
CSCwe45093	User with no vpn-filter may get additional access when per-user-override is set (IKEv2 RAVPN)
CSCwe45569	FTD upgrade from 7.0 to 7.2.x and traceback/reload due to management-access enabled
CSCwe45779	ASA/FTD drops traffic to BVI if floating conn is not default value due to no valid adjacency
CSCwe47485	FTD: CLISH slowness due to command execution locking LINA prompt
CSCwe48399	The public API function BIO_new_NDEF is a helper function used for str
CSCwe50946	Management interface link status not getting synced between FXOS and ASA
CSCwe51286	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe51443	ASA Evaluation of OpenSSL vulnerability CVE-2022-4450
CSCwe52120	SSL decrypted conns fails when tx chksum-offload is enabled with the egress interface a pppoe.
CSCwe54529	FTD on FPR2140 - Lina traceback and reload by TCP normalization
CSCwe54999	Protocol Down with lower CPU instances on ESXi 8 for ASAv and FTDv
CSCwe58207	Memory leak observed on ASA/FTD when logging history is enabled
CSCwe58700	ASA/FTD: Revision of cluster event message "Health check detected that control left cluster"
CSCwe59380	FTD: "timeout floating-conn" not operating as expected for connections dependent on VRF routing

Bug ID	Headline
CSCwe59737	ASA/FTD reboots due to traceback pointing to watchdog timeout on p3_tree_lookup
CSCwe59809	CCM seq 45 - WR6, WR8, LTS18 and LTS21.
CSCwe59919	FTD Traceback and reload on Thread Name "NetSnmp Event mib process"
CSCwe61928	PIM register packets are not sent to RP after a reload if FTD uses a default gateway to reach the RP
CSCwe61969	ASA Multicontext 'management-only' interface attribute not synced during creation
CSCwe62361	ASA reboots due to heartbeat loss and "Communication with NPU lost"
CSCwe62703	New context subcommands are not replicated on HA standby when multiple sessions are opened.
CSCwe62971	Policy Deploy Failing when trying to remove Umbrella DNS Connector Configuration
CSCwe62997	ASA/FTD traceback in snp_tracer_format_route
CSCwe63067	ASA/FTD may traceback and reload in Thread Name 'lina' due to due to tcp intercept stat
CSCwe63232	ASA/FTD: Ensure flow-offload states within cluster are the same
CSCwe63266	Need fault/error for invalid firmware MF-111-234949
CSCwe63493	Post backup restore multiple processes are not up. No errors are observed during backup or restore.
CSCwe63759	Cluster hardening fixes
CSCwe64043	Cisco ASA and FTD ACLs Not Installed upon Reload
CSCwe64404	ASA/FTD may traceback and reload
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
CSCwe65516	show xlate does not display xlate entries for internal interfaces (nlp_int_tap) after enabling ssh.
CSCwe65634	ASA - Standby device may traceback and reload during synchronization of ACL DAP
CSCwe66132	ASA/FTD may traceback and reload in Thread Name 'lina'

Bug ID	Headline
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".
CSCwe70378	Connections not replicated to Standby FTD
CSCwe71220	FTD Crash in Thead Name: CP Processing
CSCwe71284	ASA/FTD may traceback and reload in Thread Name DATAPATH-3-21853
CSCwe72330	FTD LINA traceback and reload in Datapath thread after adding Static Routing
CSCwe72535	Unable to login to FTD using external authentication
CSCwe73116	Cross-interface-access: ICMP Ping to management access ifc over VPN is broken
CSCwe74059	logrotate is not compressing files on 9.16 ASA or 7.0 FTD
CSCwe74089	ASA/FTD may traceback and reload in Thread Name DATAPATH-1-1656
CSCwe74328	AnyConnect - mobile devices are not able to connect when hostscan is enabled
CSCwe74916	Interface remains DOWN in an Inline-set with propagate link state
CSCwe76036	ndclientd error message 'Local Disk is full' needs to provide mount details which is full
CSCwe76722	ASA/FTD: From-the-box ping fails when using a custom VRF
CSCwe77123	ASA/FTD : Degradation for TCP tput on FPR2100 via IPSEC VPN when there is delay between VPN peers
CSCwe78674	User Group Download fetches less data than available or fails with "Size limit exceeded" error
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'
CSCwe80063	Default DLY value of port-channel sub interface mismatch with parent Portchannel
CSCwe81684	ASA: Standby failure on parsing of "management-only" not reported to parser/failover subsystem
CSCwe82107	health alert for [FSM:STAGE:FAILED]: external aaa server configuration

Bug ID	Headline
CSCwe82704	PortChannel sub-interfaces configured as data/data-sharing, in multi-instance HA go into "waiting"
CSCwe83255	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe83478	Prune target should account for the allocated memory from the thread pruned
CSCwe84079	asa_snmp.log is not rotated, resulting in large file size
CSCwe85156	FTD: 10Gbps/full interfaces changed to 1Gbps/Auto after upgrade and going to down state
CSCwe85432	ASA/FTD traceback and reload on thread DATAPATH-14-11344 when SIP inspection is enabled
CSCwe86225	ASA/FTD traceback and reload due citing thread name: cli_xml_server in tm_job_add
CSCwe86964	Consul and Consul Enterprise allowed an authenticated user with service:
CSCwe87134	ASA/FTD: Traceback and reload due to high rate of SCTP traffic
CSCwe87591	Cisco FTD Software SSL/TLS URL Category and Snort 3 Detection Engine Bypass and DOS Vulnerability
CSCwe87831	FMC UI response is very slow: Add health module monitoring FMC ntpd server(s) accessibility
CSCwe88772	ASA traceback and reload with process name: cli_xml_request_process
CSCwe89030	Serial number attribute from the subject DN of certificate should be taken as the username
CSCwe89256	Firepower Chassis Manager is not accessible with ECDSA certificates
CSCwe89731	Notification Daemon false alarm of Service Down
CSCwe89985	CVIM Console getting stuck in "Booting the kernel" page
CSCwe90095	Username-from-certificate feature cannot extract the email attribute
CSCwe90168	Unable to Access FMC GUI when using Certificate Authentication
CSCwe90202	ASA: Standby failure on parsing of "management-only" for dynamic configuraiton changes
CSCwe90596	Elephant flow detection disabled on FMC, getting enabled on FTD after random deployment
CSCwe90720	ASA Traceback and reload in parse thread due ha_msg corruption
CSCwe91008	Snort3 is crashing frequently on cd_pdts.so
CSCwe92324	FPR31xx - SNMP poll reports incorrect FanTray Status at Down while actually operational

Bug ID	Headline
CSCwe92905	ngfwManager process continuously restarting leading to ZMQ Out of Memory traceback
CSCwe93061	FTD returns no output of "show elephant-flow status" when efd.lua file's content is empty
CSCwe93137	KP - multimode: ASA traceback observed during HA node break and rejoin.
CSCwe93202	FXOS REST API: Unable to create a keyring with type "ecdsa"
CSCwe93489	Threat-detection does not recognize exception objects with a prefix in IPv6
CSCwe93532	ASA/FTD may traceback and reload in Thread Name 'lina'.
CSCwe93537	Threat-detection does not allow to clear individual IPv6 entries
CSCwe93561	Cisco ASA and FTD VPN Web Client Services Client-Side Request Smuggling Vulnerability
CSCwe93736	ASA not updating Timezone despite taking commands
CSCwe93925	Deployment fails to FTD when reusing/reassigning existing vlan id to diff interface
CSCwe94287	FTD DHCP Relay drops NACK if multiple DHCP Servers are configured
CSCwe95110	Connection events incorrectly show OVERSUBSCRIPTION flow message for passive interface traffic
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
CSCwe97277	Observed ASA traceback and reload when performing hitless upgrade while VPN traffic running
CSCwe97939	ASA/FTD Cluster: Change "cluster replication delay" with max value increase from 15 to 50 sec
CSCwe98146	Snort3 cores seen in certain conditions with traffic
CSCwe98319	ASAConfig multiple restarts are leaking 16K memory in every Restart leading to ZMQ Out Of Memory.
CSCwe98687	Cisco FTD Software Software for Cisco Firepower 2100 Series Inspection Rules DoS Vulnerability
CSCwe99040	traceback and reload thread datapath on process tcpmod_proxy_continue_bp
CSCwe99550	Add knob to pause/resume file specific logging in asa log infra.

Bug ID	Headline
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'
CSCwf04870	ASA: "Ping <ifc_name> x.x.x.x" is not working as expected starting 9.18.x
CSCwf04983	3100 unit failed to join the cluster with error "configured object (sys/switch-A/slot-2) not found"
CSCwf05295	FTD running on FP1000 series might drop packets on TLS flows after the "Client Hello" message.
CSCwf06318	Readiness check needs to be allowed to run without pausing FMC HA
CSCwf06377	Setting heartbeat timeout to 6sec for Firepower 4100 and 9300
CSCwf07791	ASA running out of SNMP PDU and SNMP VAR chunks
CSCwf08043	Lina traceback and reload due to fragmented packets
CSCwf08387	LSP version not updated to latest in LINA Prompt in SSP_CLUSTER with 7.2.4 build.
CSCwf08515	FPR3100: ASA/FTD High traffic impact on all data interfaces with high counter of "demux drops"
CSCwf10910	FTD : Traceback in ZMQ running 7.3.0
CSCwf11877	TPK 3110 - Firmware version MISMATCH after upgrade to 7.2.4-144
CSCwf12005	ASA sends OCSP request without user-agent and host
CSCwf12408	ASA: After upgrade to 9.16.4 all type-8 passwords are lost on first reboot
CSCwf12985	FTDv: Traffic failure in VMware Deployments due to dpdk pool exhuastion and rx_buff_alloc_failure
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)
CSCwf14126	ASA Traceback and reload citing process name 'lina'
CSCwf14411	getting wrong destination zone on traffic causing traffic to match wrong AC rule

Bug ID	Headline
CSCwf14735	traceback and reload in Process Name: lina related to Nat/Pat
CSCwf14811	TCP normalizer needs stats that show actions like packet drops
CSCwf15858	LDAP authentication over SSL not working for users that send large authorisation profiles
CSCwf15863	Very specific "vpn-idle-timeout" values cause continuous SSL session disconnects and reconnects
CSCwf15902	ASAv in Hyper-V drops packets on management interface
CSCwf16679	HA Serviceability Enh: Maintain HA NLP client stats and HA CTL NLP counters for current App-sync
CSCwf17042	ASDM replaces custom policy-map with default map on class inspect options at backup restore.
CSCwf17314	FMC deploy logs rotating faster because of /internal_rest_api/accesscontrol/rapplicationsavailable
CSCwf17389	ASA accepts replayed SAML assertions for RA VPN authentication
CSCwf17406	Failure to remove snort stat files older than 70 days
CSCwf17814	ASA/FTD may traceback and reload in Thread Name '19', free block checksum failure
CSCwf17858	node is leaving TPK cluster due to interface health check failure
CSCwf20338	ASA may traceback and reload in Thread Name 'DHCPv6 Relay'
CSCwf21106	ASA/FTD: Traceback on thread name: snmp_master_callback_thread during SNMP and interface changes
CSCwf21204	DBCheck shouldn't run against MonetDB if user is collecting config backup alone
CSCwf21640	Correlation rule 'Security Intelligence Category' option is missing DNS and URL values
CSCwf22005	ASA/FTD : Packet-tracer may displays incorrect ACL rule, though produces correct verdict.
CSCwf22045	MYSQL, or any TCP high traffic, getting blocked by snort3, with snort-block as Drop-reason
CSCwf22483	SSH to Chassis allows a 3-way handshake for IPs that are not allowed by the config
CSCwf23564	Unable to establish BGP when using MD5 authentication over GRE TUNNEL and FTD as passthrough device
CSCwf23868	Update Configuration State if sync is skipped
CSCwf24773	crashhandler running with test mode snort

Bug ID	Headline
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
CSCwf26599	Error loading data in NAT page - When unused port object is used
CSCwf26939	FTD may fail to create a NAT rule with error: "IPv4 dst real obj address range is huge"
CSCwf27337	KP: Cleanup/Reformat the second (MSP) disk on FTD reinstall
CSCwf27458	AC policy change is not reflected in instance page on edit
CSCwf28488	Inconsistent log messages seen when emblem is configured and buffer logging is set to debug
CSCwf30542	Snort3 crash found during cleaning up a CHP object
CSCwf30716	ASA in multi context shows standby device in failed stated even after MIO HB recovery.
CSCwf30727	ASA integration with umbrella does not work without validation-usage ssl-server.
CSCwf30824	Add CIMC reset as auto-recovery for CIMC IPMI hung issues
CSCwf31050	[IMS_7_5_MAIN]High CPU usage on multiple appliances
CSCwf31701	ASA traceback and reload with the Thread name: **CP Crypto Result Processing**
CSCwf31820	Firewall may drop packets when routing between global or user VRFs
CSCwf33574	ASA access-list entries have the same hash after upgrade
CSCwf33904	[IMS_7_4_0] - Virtual FDM Upgrade fails: HA configStatus='OUT_OF_SYNC after UpgradeOnStandby
CSCwf34500	FTD: GRE traffic is not being load balanced between CPU cores
CSCwf35207	ASA: Traceback and reload while updating ACLs on ASA
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
CSCwf35573	Traffic may be impacted if TLS Server Identity probe timeout is too long
CSCwf36419	ASA/FTD: Traceback and reload with Thread Name 'PTHREAD'
CSCwf36621	access-list: Cannot mix different types of access lists.
CSCwf37160	AnyConnect Ikev2 Login Failed With certificate-group-map Configured

Bug ID	Headline
CSCwf38782	Change in syslog message ASA-3-202010
CSCwf39108	Firewall rings may get stuck and cause packet loss when asp load-balance per-packet auto is used
CSCwf39163	ASAv - High latency is experienced on Azure environment for ICMP ping packets while running snmpwalk
CSCwf40594	Wyoming/SFCN ASA: Wrong values shown DBRG in show crypto ssl objects CLI
CSCwf41187	WINSCP and SFTP detectors do not work as expected
CSCwf41433	ASA/FTD client IP missing from TACACS+ request in SSH authentication
CSCwf42012	Improper load-balancing for traffic on ERSPAN interfaces on FPR 3100/4200
CSCwf42097	PSEQ (Power-Sequencer) firmware may not be upgraded with bundled FXOS upgrade
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
CSCwf43850	ECMP + NAT for ipsec sessions support request for Firepower.
CSCwf44537	99.20.1.16 lina crash on nat_remove_policy_from_np
CSCwf44621	Traceback and reload on Thread DATAPATH-6-21369 and linked to generation of syslog message ID 202010
CSCwf44915	Old LSP packages are not pruned causing high disk utilization
CSCwf45091	Snort3 matches SMTP_RESPONSE_OVERFLOW (IPS rule 124:3) when SMTPS hosts exchange certificates
CSCwf47227	Remove Priority-queue command from FTD|| Priority-queue command causes silent egress packet drops
CSCwf47924	Cisco ASA and FTD VPN Web Client Services Client-Side Request Smuggling Vulnerability
CSCwf48599	VPN load-balancing cluster encryption using deprecated ciphers
CSCwf49573	ASA/FTD: Traceback and reload when issuing 'show memory webvpn all objects'
CSCwf50497	DNS cache entry exhaustion leads to traceback
CSCwf51512	2100 Reload due to internal links going down and NPU disconnection
CSCwf51824	FXOS SNMP "property community of sys/svc-ext/snmp-svc is out of range" is unclear to users
CSCwf51933	FTD username with dot fails AAA-RADIUS external authentication login after upgrade

Bug ID	Headline
CSCwf52810	ASA SNMP polling not working and showing "Unable to honour this request now" on show commands
CSCwf54418	Reduce time taken to clear stale IKEv2 SAs formed after Duplicate Detection
CSCwf54510	ASA traceback and reload on Thread Name: DHCPRA Monitor
CSCwf56291	FMC config archives retention reverts to default if ca_purge tool was used prior to 7.2.4 upgrade
CSCwf56386	vFTD runs out of memory and goes to failed state
CSCwf56811	ASA Traceback & reload on process name lina due to memory header validation
CSCwf57856	FXOS Traceback and reload caused by leak on MTS buffer queue
CSCwf58876	KP2140-HA, reloaded primary unit not able to detect the peer unit
CSCwf59529	Identity Policy Active auth snort3 redirect hostname doesn't list all FQDN objects\u0009
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
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	Cisco ASA/FTD Firepower 2100 SSL/TLS Denial of Service Vulnerability
CSCwf62820	Failover: standby unit traceback and reload during modifying access-lists
CSCwf62885	FTDv Single-Arm Proxy behind AWS GWLB drops due to geneve-invalid-udp-checksum.
CSCwf63358	FTD Diskmanager.log is corrupt causing hm_du module to alert false high disk usage
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
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
CSCwf69880	Firewall Traceback and reload due to SNMP thread
CSCwf69901	FTD: Traceback and reload during OSPF redistribution process execution

Bug ID	Headline
CSCwf70275	FTD: TLS Server Identity does not work if size of client hello more than TCP MSS bytes
CSCwf71606	Cisco ASA and FTD ACLs Not Installed upon Reload
CSCwf71812	FTD Lina engine may traceback, due to assertion, in datapath
CSCwf72434	Add meaningful logs when the maximums system limit rules are hit
CSCwf72510	Avoid both the devices in HA sends events to FMC
CSCwf73189	FTD is dropping GRE traffic from WSA due to NAT failure
CSCwf73773	Dumping of last 20 rmu request response packets failed
CSCwf75214	ASA removes the IKEv2 Remote PSK if the Key String ends with a backslash "\" after reload
CSCwf75694	ASA - The GTP inspection dropped the message 'Delete PDP Context Response' due to an invalid TEID=0
CSCwf77191	ASA appliance mode - 'connect fxos [admin]' will get ERROR: failed to open connection.
CSCwf77795	FMC QoS dashboard does not show QoS rule matched
CSCwf77994	False critical high CPU alerts for FTD device system cores running instantaneous high usage
CSCwf78321	ASA: Checkheaps traceback and reload due to Clientless WebVPN
CSCwf78950	FMC process ssp_snmp_trap_fwdr high memory utilization
CSCwf79279	azure vftd node traceback while loading multiple network-service objects during ns_reload.
CSCwf79372	after HA break, selected list shows both the devices when 1 device selected for upgrade
CSCwf80183	Snort3 core in navl seen during traffic flow
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.
CSCwf82279	Excessive logging of ssp-multi-instance-mode messages to /opt/cisco/platform/logs/messages
CSCwf82447	Editing identity nat rule disables "perform route lookup" silently
CSCwf82742	FTD: SNMP not working on management interface
CSCwf82970	Snort2 engine is crashing after enabling TLS Server Identity Discovery feature

Bug ID	Headline
CSCwf84200	Snort core while running IP Flow Statistics
CSCwf84318	ASA/FTD traceback and reload on thread DATAPATH
CSCwf85757	Cisco ASA Software and FTD Software SAML Assertion Hijack Vulnerability
CSCwf86557	Decrypting engine/ssl connections hang with PKI Interface Error seen
CSCwf87070	WM RM - SFP port status of 9 follows port of state of SFP 10|11|12
CSCwf87348	When state-link is flapped HA state changed from Standby-ready to Bulk-sync without failover reason
CSCwf88124	Switch ports in trunk mode may not pass vlan traffic after power loss or reboot
CSCwf88552	ASA/FTD: Traceback and reload due to NAT L7 inspection rewrite
CSCwf89265	CDFMC: VDB version rolling back to old version after performing Disaster Recovery
CSCwf89959	ASA: ISA3000 does not respond to entPhySensorValue OID SNMP polls
CSCwf92135	ASA: Traceback and reload on Tread name "fover_FSM_thread" and ha_ntfy_prog_process_timer
CSCwf92308	Traceback: CdFMC - Edit of network object (network/host/range/fqdn) override throws internal error
CSCwf92371	HA secondary unit disabled after reboot - Process Manager failed to secure LSP
CSCwf92646	ECDSA Self-signed certificate using SHA384 for EC521
CSCwf92661	ASA|FTD: Traceback & reload due to a free buffer corruption
CSCwf92726	Some Vault secrets including LDAP missing files after upgrade if the Vault token is corrupted
CSCwf94450	FTD Lina traceback Thread Name: DATAPATH due to memory corruption
CSCwf94677	"failover standby config-lock" config is lost after both HA units are reloaded simultaneously
CSCwf95147	OSPFv3 Traffic is Centralized in Transparent Mode
CSCwf95288	FPR1k Switchport passing CDP traffic
CSCwf96938	FMC: ACP Rule with UDP port 6081 is getting removed after subsequent deployment
CSCwf99303	Management UI presents self-signed cert rather than custom CA signed one after upgrade
CSCwf99434	Failed to transfer new image file to FPR2130 and traceback was observed
CSCwh00692	Traceback @<capture_file_show+605 at ../infrastructure/capture/capture_file_finesse.c:282>

Bug ID	Headline
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
CSCwh03373	Do not enable TLS Server Identity Discovery on FTDv deployed with GWLB
CSCwh04185	Snort crash in active response
CSCwh04365	ASA Traceback & reload on process name lina due to memory header validation - webvpn side fix
CSCwh04395	ASDM application randomly exits/terminates with an alert message on multi-context setup
CSCwh04730	ASA/FTD HA checkheaps crash where memory buffers are corrupted
CSCwh05863	ASA omits port in host field of HTTP header of OCSP request if non-default port begins with 80
CSCwh06452	Interface speed mismatch in SNMP response using OID .1.3.6.1.2.1.2.2
CSCwh08481	ASA traceback on Lina process with FREEB and VPN functions
CSCwh08683	FTDv/AWS - NTP clock offset between Lina and FTD cluster
CSCwh09113	FPR1010 in HA failed to send or receive to GARP/ARP with error "edsa_rcv: out_drop"
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
CSCwh11411	Snort blacklisting traffic during deployment
CSCwh11764	ASA/FTD may traceback and reload in Thread Name "RAND_DRBG_bytes" and CTM function on n5 platforms
CSCwh11960	Max Detect on Detection is blocking some ping traffic
CSCwh12120	Incorrect exit interface choose for VTI traffic next-hop
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
CSCwh14863	FTD 7.0.4 cluster drops Oracle's sqlnet packets due to tcp-not-syn
CSCwh15223	Lina crash in snp_fp_tcp_normalizer() when DAQ/Snort sends malformed L3 header
CSCwh15636	ARP learning issues with Multiple-instance running 100G Netmod
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

Bug ID	Headline
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
CSCwh19475	Intermittently flow is getting white-listed by the snort for the unknow app-id traffic.
CSCwh19897	ASA/FTD Cluster: Reuse of TCP Randomized Sequence number on two different conns with same 5 tuple
CSCwh20307	FMC fails deployment after removing NAT or ACL rule
CSCwh21360	741 - HA & AppAgent - Long term solution for avoiding momentary split-brain situations
CSCwh21381	Logging improvement for messages exchange between LinaConfigTool and xml server
CSCwh21420	ASA unexpected HA failover due to MIO blade heartbeat failure
CSCwh21474	ASA traceback when re-configuring access-list
CSCwh22565	Snort 3 HTTP Intrusion Prevention System Rule Bypass Vulnerability
CSCwh22888	FXOS: Remove enforcement of blades going into degraded state after multiple DIMM correctable errors
CSCwh23100	Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
CSCwh23567	PAC Key file missing on standby on reload
CSCwh24321	FXOS: Alperton 100G NetMod not being acknowledged properly
CSCwh24932	ASA software on FP3110 showing incorrect serial number in show inventory output
CSCwh25351	FTD VMWare: High disk utilization on /dev/sda8 partition caused by file system corruption
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.
CSCwh27886	Chassis Manager shows HTTP 500 Internal Server error in specific cases
CSCwh28144	Specific OID 1.3.6.1.2.1.25 should not be responding
CSCwh28206	Firewall Blocking packets after failover due to IP <-> SGT mappings
CSCwh29276	ASA: Traceback and reload when switching from single to multiple mode
CSCwh30257	snort3 crashes observed due to memory corruption in file api
CSCwh30346	ASA/FTD: 1 Second failover delay for each NLP NAT rule

Bug ID	Headline
CSCwh30676	Ping to the configured systemIP on management interface getting failed in cluster setup.
CSCwh30891	ASA/FTD may traceback and reload in Thread Name 'ssh' when adding SNMPV3 config
CSCwh31495	FTD - Traceback and reload due to nat rule removed by CPU core
CSCwh31502	Enhancement for Lina copy operation for startup-config to backup-config.cfg in HA
CSCwh32118	ASDM management-sessions quota reached due to HTTP sessions stuck in CLOSE_WAIT
CSCwh34344	FTD not generating end of connection event after "Deleting Firewall session"
CSCwh34836	Getting an exception on the UI while editing and saving the intrusion policy
CSCwh36005	Policy deployment failed due to "1 errors seen during populateGlobalSnapshot"
CSCwh37655	Snort2:Skip writing malware seed file duing process shutdown
CSCwh37733	FTD responding to UDP500 packet with a Mac Address of 0000.000.000
CSCwh38708	ASA "pager line 25" command doesn't work as expected on few terminal applications
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
CSCwh40294	ASA traceback due to panic event during SNMP configuration
CSCwh40968	Large file download failed due to hitting the max segment limit
CSCwh41127	ASA/FTD: NAT64 error "overlaps with inside standby interface address" for Standalone ASA
CSCwh41606	Extensive logging for a problematic deployment caused logs to rollover important logs
CSCwh42077	Cisco_Firepower_GEODB_FMC_Update* are not included in diskmanager
CSCwh42412	FTD Block 9344 leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwh43230	Strong Encryption license is not getting applied to ASA firewalls in HA.
CSCwh43945	FTD/ASA traceback and reload may occur when ssl packet debugs are enabled
CSCwh44215	ENH - Exempt TSID probe from going through EVE inspection
CSCwh45108	Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
CSCwh45450	2100: Interfaces missing from FTD after removing interfaces as members of a port-channel

Bug ID	Headline
CSCwh47053	ASA/FTD may traceback and reload in Thread Name 'dns_cache_timer'
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.
CSCwh49483	ASA/FTD may traceback and reload while running show inventory
CSCwh50221	4200 Series: Portchannel in cluster may stay down sometimes when LACP is in active mode
CSCwh51872	Message asa_log_client exited 1 time(s) seen multiple times
CSCwh52526	FMC SSO timesout when user session is active for more than 1 hr (idle timeout)
CSCwh52710	evaluate open-vm-tools / VMware Tools on FMC for VMware -- CVE-2023-20900 and VMSA-2023-0019
CSCwh53143	ASA:Management access via IPSec tunnel is NOT working
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
CSCwh56290	After rebooting, the future date set on the FPR2100 platform is not reflected (set clock manually)
CSCwh57976	Improve CPU utilization in ssl inspection for supported signature algorithm handling
CSCwh58190	FMC Deployment failure in csm_snapshot_error
CSCwh58467	ASA does not sent 'warmstart' snmp trap
CSCwh58490	FMC Deployment failed due to internal errors after upgrade
CSCwh59199	ASA/FTD traceback and reload with IPSec VPN, possibly involving upgrade
CSCwh59222	SNORT3 - FTD - TSID high cpu, daq polling when ssl enabled is not pulling enough packets
CSCwh59557	Source NAT Rule performing incorrect translation due to interface overload
CSCwh60604	ASA/FTD may traceback and reload in Thread Name 'lina' while processing DAP data
CSCwh60631	Fragmented UDP packet via MPLS tunnel reassemble fail
CSCwh60971	NAT pool is not working properly despite is not reaching the 32k object ID limit.

Bug ID	Headline
CSCwh61690	Multicast through the box traffic causing high CPU with 1GBps traffic
CSCwh62731	FTD Upgrade from 6.6.5 to 7.2.5 removing OGS causing rule expansion on boot
CSCwh63211	Lina core at snp_nat_xlate_verify_magic.part and soft traces
CSCwh63588	FTD SNMPv3 host configuration gets deleted from IPTABLES after adding host-group configuration
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
CSCwh68068	Firepower WCCP router-id changes randomly when VRFs are configured
CSCwh68482	FTD: Traceback and Reload in Process Name: lina
CSCwh68856	Configuration to disable TLS1.3
CSCwh68878	Diskmanager process terminated unexpectedly
CSCwh69156	FTD-HA does not fail over sometimes when snort3 crashes
CSCwh69346	ASA: Traceback and reload when restore configuration using CLI
CSCwh69843	WM DT - ASA in transparent mode doesn't send equal IPv6 Router Advertisement packets to all nodes
CSCwh70323	Timestamp entry missing for some syslog messages sent to syslog server
CSCwh70481	Community string sent from router is not matching ASA
CSCwh70628	ASA/FTD may traceback and reload due to watchdog time exceeding the default 15 seconds
CSCwh70905	Secondary lost failover communication on Inside, using IPv6, but next testing of Inside passes
CSCwh71008	CSF 4200: PSU Fan speed is critical
CSCwh71050	FXOS : Duplication of NTP entry results in Error message : Unreachable Or Invalid Ntp Server
CSCwh71358	Unable to create VRF via FDM in Firepower 3105 device
CSCwh71589	Coverity 886745: OVERRUN in verify_generic_signature
CSCwh71665	ASA traceback under match_partial_keyword during CPU profiling
CSCwh72370	FTD: Mariadb might cause OOM due to not-so-effective memory release algorithm in glibc allocator

Bug ID	Headline
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
CSCwh74870	Unexpected high values for DAQ outstanding counter
CSCwh75829	FMC Primary disk degraded error
CSCwh77348	ASA: Traceback and reload when executing the command "show nat pool detail" on a cluster setup
CSCwh78064	FTD: The crucial upgrade script should not be bypassed by the Upgrade Retry
CSCwh78118	ASA/FTD traceback and reload on process fsm_send_config_info_initiator
CSCwh79095	Snort generating an excessive number of snort-unified log files with zero bytes
CSCwh81366	[Multi-Instance] Second Hard Drive (FPR-MSP-SSD) not in use
CSCwh82766	Bulk FTD backups to be generated in batches internally
CSCwh83021	ASA/FTD HA pair EIGRP routes getting flushed after failover
CSCwh83254	ASA/FTD: Traceback and reload on thread name CP Crypto Result Processing
CSCwh83301	High CPU Utilization alerts caused by the process Telegraf
CSCwh83328	SNMP fails to poll accurate hostname from FMC
CSCwh83517	VTI tunnel goes down due to route change detected in VRF scenario
CSCwh83854	Cannot configure Correlation rule because there are no values for GID that exceed 2000
CSCwh84376	In FPR4200/FPR3100-cluster observed core file ?core.lina? observed on device reboot.
CSCwh84610	Disconnecting RA VPN users from the FMC gui fails.
CSCwh84647	Backup restore: silent failure when the device managed locally
CSCwh84833	Every HA sync attempts to disable URL filtering if already disabled.
CSCwh85824	eStreamer JSON parse error and memory leak
CSCwh87058	FTD: Internal certificate generation results to certificate and private key mismatch
CSCwh90693	FTD unregisters the standby FMC immediately after a successful registration
CSCwh91419	FTD installation fails on FPR-2K "Error in App Instance FTD. Available memory not updated by blade"
CSCwh91574	FTD: Traceback in threadname cli_xml_request_process
CSCwh92156	Firewall shows misleading SCP file copy failure reasons

Bug ID	Headline
CSCwh92345	crypto_archive file generated after the software upgrade.
CSCwh92541	Random FTD snort3 traceback
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
CSCwh95003	Init process spikes to 100% CPU usage after a failed backup
CSCwh95010	Unexpected traceback on thread name Lina and device experienced reboot
CSCwh95025	GTP connections, under certain circumstances do not get cleared on issuing clear conn.
CSCwh95175	ASA/FTD may traceback and reload in Thread Name 'lina'
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
CSCwh98733	ASA: Traceback and reload during tests of High number of traffic flows and syslog messages
CSCwh99398	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-34-17852'
CSCwi01085	FTD VMWare tracebacks at PTHREAD-3587
CSCwi01323	SNMP OID ifOutDiscards on MIO are always zero despite show interface are non-zero
CSCwi01381	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi01895	Connection drops during file transfers due to HeartBeat failures
CSCwi01981	Thirty-day automatic upgrade revert-info deletion is not resilient to communication failures
CSCwi02039	FMC clean_revert_backup script fails silently without creating any logs
CSCwi02134	FTD sends multiple replicated NetFlow records for the same flow event
CSCwi02599	SSX Eventing continues to go to old tenant upon FTD migration to CDO.
CSCwi02754	FTD 1120 standby sudden reboot
CSCwi02919	SNMP Unresponsive when snmp-server host specified
CSCwi03407	Traceback on FP2140 without any trigger point.
CSCwi03528	Cross ifc access: Revert PING to old non-cross ifc behavior
CSCwi04021	Daily Change Reconciliation Report Randomly Generating Reports with the same time periods
CSCwi04351	FTD upgrade failling on script 999_finish/999_zz_install_bundle.sh

Bug ID	Headline
CSCwi05240	ASA - Traceback the standby device while HA sync ACL-DAP
CSCwi05435	[ENH] FMC to pull FTD device current SRU version rather than device records for SRU deployed.
CSCwi05618	FTD HA sync failure due to "CD App Sync error is Failed to apply SSP config on standby"
CSCwi06690	Certificate Encoding Issue when using AnyConnect cert Authentication/Authorisation
CSCwi06797	ASA/FTD traceback and reload on thread DATAPATH
CSCwi07068	SFDataCorrelator logs "Killing MySQL connection" every minute, causing performance problems
CSCwi08374	FMC backup fails with "Registration Blocking" failure caused by DCCSM issues
CSCwi11049	Cisco Secure Access: Occasional traffic loss occurring through FWaaS
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
CSCwi13223	Source of the VTI interface is getting empty
CSCwi13510	Config-url is accepting directory as the config file
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
CSCwi16034	FMC does not generate email health notifications for Database Integrity Check failures.
CSCwi16571	Capture-traffic Clish command with snort3 not producing a proper resulting capture
CSCwi18581	Firewall traceback and reload due to SSH thread
CSCwi18663	FMC-4600: Pre-Filter policy is showing as none
CSCwi19015	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-13-6022'
CSCwi19145	FTD/ASA may traceback and reload in PKI, syslog, during upgrade
CSCwi19485	Fail open snort-down is off in inline pairs despite it being enabled and deployed from FMC
CSCwi19849	VPN load-balancing cluster encryption using Phase 2 deprecated ciphers

Bug ID	Headline
CSCwi20045	ASA/FTD may traceback and reload in Thread Name 'lina' due to a watchdog in 9.16.3.23 code
CSCwi20848	ASA/FTD high memory usage due to SNMP caused by RAVPN OID polling
CSCwi20955	FTD with may traceback in data-path during deployment when enabling TAP mode
CSCwi21625	FailSafe admin password is not properly sync'd with system context enable pw
CSCwi22296	ASA: The logical device may boot into failsafe mode because of an large configuration.
CSCwi22693	ACP rule is deleted when discarding changes, post rule reposition.
CSCwi24368	Standby manager addition is failed on Primary FMC due to previous entries in table
CSCwi24370	Stale HA transactions need to be moved to failed and subsequent HA transaction needs to be created
CSCwi24461	Device/port-channel goes down with a core generated for portmanager
CSCwi24814	In FIPS mode, External auth with TLS config enabled, CLI logins are not working (FMC & FTDs)
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
CSCwi28645	User assigned to a read only custom role is not able to view content of intrusion policy for snort2
CSCwi29041	Log spam in /var/log/messages: Out of range value for column 'map_id'
CSCwi29538	EIGRP migration failed using 'FlexConfig Policiies' script failed generating database corruption
CSCwi29934	Cisco FXOS Software Link Layer Discovery Protocol Denial of Service Vulnerability
CSCwi30843	Error Fetching Data in Exclude Policy Page when non permanent exclude periods are selected
CSCwi31008	Deployment stuck on FMC when device goes down during deploy and doesn't boot up
CSCwi31091	OSPF Redistribution route-map with prefix-list not working after upgrade
CSCwi31480	Alert: Decommission failed, reason: Internal error is not cleared from FCM or CLI after acknowledge

Bug ID	Headline
CSCwi31558	File-extracts.logs are not recognised by the diskmanager leading to high disk space
CSCwi31766	PSU fan shows critical in show environment output while operating normally
CSCwi31966	FTD ADI debugs may show incorrect server_group and/or realm_id for SAML-authenticated sessions
CSCwi32063	ASA/FTD: SSL VPN Second Factor Fields Disappear
CSCwi32759	Username-from-certificate secondary attribute is not extracted if the first attribute is missing
CSCwi33710	ipv6 table flush exception when cli_firstboot installs bootstrap configuration multi instance
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
CSCwi35267	TLS1.3: core decode points to tls_trk_try_switch_to_bypass_aux()
CSCwi36311	use kill tree function in SMA instead of SIGTERM
CSCwi36843	Detailed logging related to reason behind sub-interface admin state change during operations
CSCwi38061	ASA/FTD traceback and reload due to file descriptor limit being exceeded
CSCwi38425	Health Monitor Alerts set in Global are not sending alert from devices assigned in leaf domain
CSCwi38440	Hostnames are replaced with IP addresses in alert email content
CSCwi38449	Module name displayed in the alert got changed and it is differ from the one set in FMC
CSCwi38662	FTD HA should not be created partially on FMC
CSCwi38708	FDM deployment failure
CSCwi38957	Policy Apply failed moving from FDM to FMC
CSCwi40193	Hairpinning of DCE/RPC traffic during the suboptimal lookup
CSCwi40302	Deployment fails on new AWS FTDv device with "no username admin"
CSCwi40487	FTD HA Failure after SNORT crash.
CSCwi40536	ASA/FTD: Traceback and reload when running show tech and under High Memory utilization condition
CSCwi40674	Umbrella Profile and others cleared incorrectly when editing group policy in the UI

Bug ID	Headline
CSCwi41666	MonetDB startup enhancement to clean up large files
CSCwi42295	Radius traffic not passing after ASA upgrade 9.18.2 and above version.
CSCwi42962	installing GeoDB country code package update to FMC does not automatically push updates to FTDs
CSCwi42992	ASA/FTD may traceback and reload in Thread Name IKEv2 Daemon
CSCwi43240	Deployment fails if Network Discovery policy reference is missing from FMC Database
CSCwi43492	ASA traceback and reload on Thread Name: DATAPATH
CSCwi43782	GTP inspection dropping packets with IE 152 due to header length being invalid for IE type 152
CSCwi44007	FMC Validation failure for large object range and success for object network in NAT64
CSCwi44148	Incorrect health monitor alerts for ISE-PIC connectivity
CSCwi44208	low memory/stress causing traceback in SNMP
CSCwi44912	ISA3000 Traceback and reload boot loop
CSCwi44953	We should be skipping sru_install during for Minor patch upgrades and install only on required basis
CSCwi45054	FMC Deployment preview shows different information before and after FTD deploy
CSCwi45408	Monetdb having 14GB of unknown BAT data causing "High unmanaged disk usage on /Volume"
CSCwi45630	Snort3 traceback with fqdn traffics
CSCwi45878	ASA/FTD: DNS Load Balancing with SAML does not work with VPN Load Balancing
CSCwi46010	ASA/FTD: Cluster incorrectly generating syslog 202010 for invalid packets destined to PAT IP
CSCwi46023	FTD drops double tagged BPDUs.
CSCwi46163	Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.
CSCwi46641	FTDv may traceback and reload in Thread Name 'PTHREAD-3744' when changing interface status
CSCwi46676	API:/operational/commands not working as swagger indicate
CSCwi47029	"Update file is corrupted" for "Download Latest Cisco Firepower Geolocation Database Update." in FMC
CSCwi48699	ASA traceback and reload on Thread Name: pix_flash_config_thread
CSCwi49770	ASA|FTD Traceback & reload in thread name Datapath

Bug ID	Headline
CSCwi49797	Event Searching with Objects and Networks Leads to only showing events matching Objects
CSCwi49829	Threat Defense Service Policy - Reset Connection Upon Timeout not working
CSCwi50343	Their standalone FTD running 7.2.2 on FPR-4112 experienced a traceback on the SNMP module
CSCwi51611	FTD 7.4.1 Snort shows 100% utilization even at a low traffic rate
CSCwi52008	Snort3 traceback and restarts with race conditions
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
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
CSCwi54171	Decryption policy page is empty if user that modified/created policy was deleted.
CSCwi55009	Error thrown if Security Analytics user tries to access Packet Capture page
CSCwi55629	ASA/FTD : Port-channels remain down on Firepower 1010 devices after upgrade
CSCwi55842	7.4 - If policy save in progress deploy might indicate failure for only few devices
CSCwi56048	Interface fragment queue may get stuck at 2/3 of fragment database size
CSCwi56499	Cut-Through Proxy feature spikes CP CPU with a flood of un-authenticated traffic
CSCwi56667	ASA Traceback and reload on Thread Name "fover_parse" on Standby after Failover Group changes
CSCwi56733	Internal error when attempting to configure PBR in FMC
CSCwi57476	interface idb logging log rotation to FXOS logrotate utility
CSCwi57670	RAVPN SAML: External browser gives misleading message when FTD/ASA fails to parse assertion
CSCwi58754	Blocking SMB traffic with reason "Blocked by the firewall preprocessor"
CSCwi59453	Bootstrap after upgrade failed - Resume HA with reason deployment already exists
CSCwi59525	Multiple lina cores on 7.2.6 KP2110 managed by cdFMC
CSCwi59831	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi59871	High disk usage caused by large write-ahead log in eventdb

Bug ID	Headline
CSCwi59969	ZTNA: FMC pushes incorrect sp-acs-url parameter - "?" encoded as 0x3F
CSCwi60151	ZTNA: FMC doesn't accept IdP with local domain
CSCwi60285	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi60430	CVE-2023-51385 (Medium Sev) In ssh in OpenSSH before 9.6, OS command injection might occur if a us
CSCwi61135	Debugs failed to be enabled on SSH session
CSCwi62683	The SSH transport protocol with certain OpenSSH extensions, found in ... (CVE-2023-48795)
CSCwi62796	ASA/FTD Traceback and reload related to SSL/DTLS traffic processing
CSCwi62985	SFDataCorrelator timeout thread deadlock detection core on busy FMC
CSCwi63057	Threat Defense Upgrade wizard might incorrectly show clusters/HAs as disabled
CSCwi63113	Null pointer dereference in SNMP that results in traceback and reload
CSCwi63743	ASA/FTD may traceback and reload in Thread Name "appAgent_monitor_nd_thread" & Rip: _lina_assert.
CSCwi64429	MonetDB memory usage grows slowly over time
CSCwi64829	traceback and reload around function HA
CSCwi65116	DHCPv6:ASA traceback on Thread Name: DHCPv6 CLIENT.
CSCwi65428	Flow velocity metric in IAB settings is incorrect.
CSCwi66461	WARN msg(speed not compatible, suspended) while creating port-channel on Victoria CE
CSCwi66570	The report doesn't include "Default Variables" information after change "Variable Sets" name
CSCwi66676	ASA/FTD may traceback and reload in Thread Name 'webvpn_task'
CSCwi67510	FMC: Packet-tracer showing a "Interface not supported" error for VLAN interfaces
CSCwi67629	Devices might change status to "missing the upgrade package" after Readiness Check is initiated
CSCwi67638	FMC configured DAP rule with Azure IDP SAML attributes does not match
CSCwi67998	Policy deployment failures on TPK MI chassis after redeploying same instance
CSCwi68320	During FMC hardware migration failure encountered due to missing prometheus directories
CSCwi68604	Error logs generated for ssh access to ASA when eddsa is used as kex hostkey

Bug ID	Headline
CSCwi68625	Continuous snmpd restarts observed if SNMP host is configured before the IP is configured
CSCwi68833	ASA/FTD: Memory leak caused by Failover not freeing dnscrypt key cache due to unsyned umbrella flow
CSCwi68970	Creating DAP policy with underscore "_" is not visible as applied to Remote Access VPN policy
CSCwi69091	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi69260	upgrade of FMC to 7.2.x removes FlexConfig-provided EIGRP authentication from interfaces on FTDs
CSCwi70371	Intermittent Packet Losses When VTI Is Sourced From Loopback
CSCwi70492	Firewall is in App Sync error in pseudo-standby mode and uses IPs from Active unit
CSCwi70940	standard error (stderr) not inserted into restore.log when restoring FMC backups
CSCwi71786	Download failed for Available Upgrade Packages
CSCwi71998	"Stream: TCP normalization error in NO_TIMESTAMP" is seen when SSL Policy decrypt all is used
CSCwi72054	Unable to delete custom DNS Server Group Object post upgrade 7.2.x
CSCwi72158	Devices in HA pair shows as standalone in Threat Defense Upgrade page
CSCwi72294	FTD: Improve or optimize LSP package verification logic to run it faster
CSCwi74214	ASA/FTD traceback and reload in Thread Name: IKEv2 Daemon when moving from active to standby HA
CSCwi75111	Configuring MTU value via CLI does not apply
CSCwi75198	Standby FTD experiencing periodic traceback and reload
CSCwi76002	Memory exhaustion due to absence of freeing up mechanism for tmatch
CSCwi76361	Transparent firewall MAC filter does not capture frames with STP-UplinkFast dst MAC consistently
CSCwi76630	FP2100/FP1000: ASA Smart licenses lost after reload
CSCwi77415	ASDM connection lost issue is observed in ASAv device due to config issue
CSCwi78064	CloudAgent Smart Agent Exception - The Smart Agent Manager requires NTP to be running on FDM
CSCwi78370	41xx/93xx : Update CiscoSSH (Chassis Manager FXOS) to address CVE-2023-48795
CSCwi78941	FDM deployment fails with error "Some interfaces have been added to or removed from the device"

Bug ID	Headline
CSCwi79037	IKEv2 client services is not getting enabled - XML profile is not downloaded
CSCwi79042	FTD/Lina traceback and reload of HA pairs, in data path, after adding NAT policy
CSCwi79120	some ssh sessions not timing out, leading to ssh and console unable to connect to the FXOS CLI
CSCwi79289	FMC: Add logging for PM functions
CSCwi79393	Policy Deployment Fails when removing the Umbrella DNS Policy from Security Intelligence
CSCwi79538	FMC API Call for Network Object Overrides Returns Different Results for Active vs Standby FW
CSCwi79703	Incorrect Timezone Format on FTD When Configured via FXOS
CSCwi80979	Snort stripping packet information and injects its packet with 0 bytes data
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
CSCwi82866	MonetDB Monitor triggers for restarting MonetDB based on WAL size are not effective
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
CSCwi85277	Upgrade Failed with error "Upgrade failed because of undeployed changes present on the device"
CSCwi85689	TLS Server Identify: 'show asp table socket' output shows multiple TLS_TRK entries
CSCwi86007	Modify UUID during license communication to avoid disrupting customer's licenses
CSCwi86036	External Radius authentication fails post upgrade if radius key includes special characters
CSCwi86187	VTI tunnel showing incorrect port-channel association info in VPN Monitoring page
CSCwi86198	SFData correlator keep terminating on FTDs configured for IDS
CSCwi87382	Traceback and reload on Primary unit while running debugs over the SSH session
CSCwi89167	Automatic VDB/SRU Download Fails Due to Simultaneous Signature Validation
CSCwi89447	Every realm sync indicates an access control policy change
CSCwi90040	Cisco ASA and FTD Software Command Injection Vulnerability
CSCwi90371	ASA:request to add "logging list" option to the "logging history" command.

Bug ID	Headline
CSCwi90399	FTD/ASA system clock resets to year 2023
CSCwi90571	Access to website via Clientless SSL VPN Fails
CSCwi90607	Unable to login to FDM GUI using external user account via RADIUS
CSCwi90751	FTD/ASA - SNMP queries using snmpwalk are not displaying all "nameif" interfaces
CSCwi90998	ASA SNMP Polling Failure for environmental FXOS DME MIB (.1.3.6.1.4.1.9.9.826.2)
CSCwi91384	Migration of S2S from ASA to FMC across domains
CSCwi91588	Heap-use-after-free in Discovery Filter on Snort shutdown
CSCwi91602	Deployment doesn't timeout as notification (but not started), runs for hours after LSP install
CSCwi92702	Run All function on FMC Health Monitoring page is greyed out after upgrade
CSCwi95228	"crypto ikev2 limit queue sa_init" resets after reboot
CSCwi95708	FTD: Hostname Missing from Syslog Message
CSCwi95796	FTD SNMP OID 1.3.6.1.4.1.9.9.109.1.1.1.1.7 always returns 0% for SysProc Average
CSCwi95871	SSH/SNMP connections to non-admin contexts fail after software upgrade
CSCwi95994	Chromium-based browsers have SSL connection conflicts when FIPS CC is enabled on the firewall.
CSCwi96521	Push clear configure access-group to avoid error while applying access group on FTD
CSCwi97836	ASA traceback and reload after configuring capture on nlp_int_tap and deleting context
CSCwi97839	FTD traceback assert in vni_idb_get_mode and reloaded
CSCwi97948	EIGRP bandwidth is changing after upgrade or after "shutdown"/"no shutdown" commands
CSCwi98147	Tomcat restarts in the middle of the LTP flow due to certificate update
CSCwi98284	Cisco ASA and FTD Software Persistent Local Code Execution Vulnerability
CSCwi99429	Policy deployment failure rollback didnt reconfigure the FTD devices
CSCwj00659	FMC: Multiple Email address in Email Alert not working
CSCwj00956	Snort process spamming syslog-ng messages so our on KP platform syslog-ng is being killed
CSCwj01197	VMXNET3 driver is not getting loaded automatically on the bootup for FMCv300
CSCwj01346	logging list MANAGER_VPN_EVENT_LIST getting removed and re-applied for every deployment

Bug ID	Headline
CSCwj01569	Policy deployment failure in standalone FDM due to an interface error
CSCwj02259	Backup failures needs to be displayed with the correct state on GUI
CSCwj02505	ASA Checkheaps traceback while entering same engineID twice
CSCwj02708	Backup generation on FDM fails with the error "Unable to backup Legacy data."
CSCwj03112	pmtool restart of monetdb fails to bring up monetdb, too many files in monetdb Volume directory
CSCwj03253	SFDataCorrelator creates huge numbers of to_import files when MonetDB table partition creation fails
CSCwj03285	FMC : Health Monitor Alert is not properly issued regarding disk usage
CSCwj03348	vFMC25 OCI to vFMC300 OCI migration failed 'Migration from Y to a is not allowed.'
CSCwj03764	In Spoke dual ISP case if ISP2 is down, VTI tunnels related to ISP1 flapping.
CSCwj03876	Deleting Snort 3 IPS Rule doesn't Generate Audit Log
CSCwj03937	ENH: FTD Add debug message to indicate "No CRL found in User identity Certificate"
CSCwj04154	Intermittent loss of management traffic due to DHCP service failing to start
CSCwj05151	ASA/FTD may traceback and reload in Thread Name DATAPATH due to GTP Spin Lock Assertion
CSCwj05464	FMC Server Certificate shows Only First 20 Objects
CSCwj05484	ASA upgrade from 9.16 to 9.18 causing change in AAA ldap attribute values by adding extra slash '\'
CSCwj07837	Deployment failure due to exceeding logging event list name size
CSCwj08015	FTW no longer working in NM3 on Warwick
CSCwj08083	An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.1
CSCwj08203	FMC: fireamp generating too many logs
CSCwj08302	FTD: HostScan scanning results not processed in version 7.4.1
CSCwj08980	ICMP replies randomly does not reaching the sender node when initiated from the node.
CSCwj09110	Upload files through Clientless portal is not working as expected after the ASA upgrade
CSCwj09373	BBManager text based search - lucene
CSCwj09938	Unable to remove suppression from snort3 rule once added

Bug ID	Headline
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.
CSCwj10955	Cisco ASA and FTD Software Web Services Denial of Service Vulnerability
CSCwj11331	Web Contents files appear as text/plain when they should be application/octet-stream
CSCwj12168	Never expiring machine user not logged out at various places
CSCwj12173	Policy cache cleanup thread should cleanup any cache that is left open for a logged out session
CSCwj13910	Crypto IPSEC SA Output Showing NO SA ERROR With IPSEC Offload Enabled
CSCwj14589	FMC-SSE Cloud Configuration SSE Enrollment Failure alert due to empty connector.toml file on the FTD
CSCwj14624	Backup exits with memory allocation error on 4115
CSCwj14798	TSS_Daemon process is exiting every minute
CSCwj14832	SAML: Single sign-on AnyConnect token verification failure is seen after successful authentication
CSCwj16279	username containing '@' character works for asa login but fails for 'connect fxos'
CSCwj16521	Policy stuck in loading state on FMC UI
CSCwj17447	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-6-26174'
CSCwj17677	PM restart needs to be blocked or warned the user that it may go for reboot
CSCwj17852	FMC - Inheritance Settings Select Base Policy Menu disappears while scrolling using Light or Dusk UI
CSCwj17969	rna_ip_os_map can grow very large that causes SFDataCorrelator to stop processing events
CSCwj19252	Object optimisation gets disabled on FMC if next deployment is after two hours
CSCwj19653	FTD - Trace back and reload due to NAT involving fqdn objects
CSCwj20067	ASA: Warning messages not displayed when Static interface NAT are configured
CSCwj20118	FTDv reloads and generate backtrace after push EIGRP config
CSCwj21880	FTD with Interface object optimization enabled is blocking traffic after renaming of zone names
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

Bug ID	Headline
CSCwj22990	After upgrading the ASA, \u201cSlot 1: ATA Compact Flash memory\u201d shows a ditterent value
CSCwj24517	LSP Deployment fails in multi instance FP 41xx / 93xx
CSCwj25629	Error when running 'show tech-support module detail' on FPR9K
CSCwj25975	FTD/ASA : CSR generation with comma between \u201cCompany Name\u201d attribute does not work expected
CSCwj26204	restored FMC backup devices display as "normal" and "healthy" although without connection with FMC
CSCwj26595	FMC allows loading a binary certificate in the External Authentication Object
CSCwj26627	FMC shows a non-User-Friendly Error during a Policy Deployment failure due to snapshot failure
CSCwj27112	Rest API '/devices/devicerecords' is returning mismatch of values for (RA VPN) policy object id
CSCwj28049	Identity Mapping Filter field gets updated with newly created network objects.
CSCwj28437	Snort3: 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.
CSCwj31382	Wrong IP address on FMC audit logs
CSCwj31816	TLS Secure Client sessions cannot be established on FTD Due to RSA-PSS Signing Algorithm
CSCwj31904	After upgrade FDM deployment fails "Timeout waiting for snort detection engines to process traffic"
CSCwj31918	Segmentation fault with "logger_msg_dispatch" while HA sync
CSCwj32035	Clientless VPN users are unable to reach pages with HTTP Basic Authentication
CSCwj32823	"strong-encryption-disable" pushed from FMC without any change after FMC upgrade
CSCwj33487	ASA/FTD may traceback and reload while handling DTLS traffic
CSCwj33580	IKEv2 tunnels flap due to fragmentation and throttling caused by multiple ciphers/proposal
CSCwj33891	ASA/FTD Cluster memory exhaustion caused by NAT process during release of port blocks allocations
CSCwj34204	Disk quota for the corefile should be revisited based on platform

Bug ID	Headline
CSCwj34235	Snort3 core in FTD stateful signature evaluation
CSCwj34374	SecureX / Cisco Security Cloud registration fails if FMC is behind a proxy server
CSCwj34881	Command to show counters for access-policy filtered with a source IP address gives incorrect result
CSCwj34975	Multiple context interfaces fail to pass traffic
CSCwj35701	Dns-guard prematurely closing conn due to timing condition
CSCwj35902	URL Filtering and Cisco-Intelligence-Feed Download Failure
CSCwj38871	ASA traceback with thread name SSH
CSCwj38928	High latency observed on FPR3120
CSCwj39107	SFDataCorrelator memory growth when pruning a huge number of old service identities
CSCwj39184	FDM /ngfw/var/sf/fwcfg/zones.conf is empty for 7.3.1
CSCwj39212	SFDataCorrelator memory growth when processing a huge number of expired user identities
CSCwj39296	FTD compliance mode not accurately shown on FMC for newly registered FTDs
CSCwj40124	FMC 7.3 Deployment failed due to OOM in PBR Configuration
CSCwj40597	Backups fail on multi-instance (or standalone) with error "Backup died unexpectedly"
CSCwj40665	Additional memory tracking in SFDataCorrelator
CSCwj40761	ASA/FTD may traceback in Threadname: **CTM KC FPGA stats handler**
CSCwj41427	FTD-HA creation is failing because FMC takes longer time to save overrides.
CSCwj43069	IPv6 rule with manual address entry FMC with ::/0 is not working as expected.
CSCwj43345	SNMP poll for some OIDs may cause CPU hogs and high latency can be observed for ICMP packets
CSCwj44398	when set the route-map in route RIP on FTD, routes update is not working after FTD reload
CSCwj45351	Unable to add additional LDAP attribue maps on FMC 7.2.5
CSCwj45439	Internal Certificate Import Error : Failed to validate Cert Based EO: Unsupported Key Type
CSCwj45822	Cisco Secure Client Unable to complete connection. Cisco Secure Desktop not installed on the client.
CSCwj48308	Stale Health Alerts seen on the UMS after model migration

Bug ID	Headline
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"
CSCwj50064	SSE connection events, FirewallRuleList field is not sent in proper format
CSCwj50406	All IPV6 BGP routes configured in device flapping
CSCwj50557	Snort creating too many snort-unified log files when frequent policy deploys
CSCwj51115	FMC backup remote server copy to Solar Winds remote server failing after upgrading to 7.x versions.
CSCwj52326	BGP config related to holdtime not being deployed sucessfully
CSCwj53324	object lookup doesn't show referenced policy automatically under object management
CSCwj53725	Traceback observed while applying 'no failover' and 'failover' in the ASA standby
CSCwj54042	Crypto ikev2 policy sequence order alters on interface/sub-interface config changes
CSCwj54644	FMC unable to upload PKCS12 certificate using Passphrase longer than 48 characters in length.
CSCwj54717	Radius secret key of over 14 characters for external authentication does not get deployed (FPR3100)
CSCwj55036	ASA/FTD: A delay in an async crypto command induces a traceback and subsequently a reload.
CSCwj55081	FPR3K loses connectivity to FMC via mgmt data interface on reboot of FPR3K
CSCwj56099	ASA: Running the failsafe-exit command caused the interface to enter a DISABLED state
CSCwj56595	delay in creating process of Readiness/upgrade post initiating from UI
CSCwj56639	FDM1010E 7.4.1 unable to register to SA, getting "Invalid entitlement tag"
CSCwj56668	False positive ISE bulk download alert error seen on FMC
CSCwj58431	FMC REST API not sending 'deploymentStatus' Attribute
CSCwj58442	FTD HA status in ON Prem FMC is corrupted reporting Secondary as Primary
CSCwj59315	Smart license registration failing on FDM post 7.4.1 baseline due to http-proxy
CSCwj59861	ASA/FTD may traceback and reload in Thread Name 'lina' due to SCP/SSH process
CSCwj59981	FMC only accepts a maximum of 30 characters for shared secret key when connecting to RADIUS server

Bug ID	Headline
CSCwj60265	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-1-16803'
CSCwj61885	File descriptor leak when validating upgrade images
CSCwj62056	cEdge URLF feature is not blocking urls with categories
CSCwj62723	Error message spammed to console on Firepower 2100 devices while enabling SSH config
CSCwj62959	Deployment failure and rollback when changing parent of subinterface with failover MAC address
CSCwj62984	Snort3: MSSQL query traffic corrupted by stream_tcp overlap handling causing SQL HY000
CSCwj63975	Disable health module does not delete UMS messages for that health module.
CSCwj65587	Snmpwalk throws Error messages #"snmp/error: truncating integer value > 32 bits"
CSCwj65811	FMC gets flooded with"Unable to find SSL rule id for policy" if TLS server identity discovery is on
CSCwj66339	OGO changing the order of custom object group contents causing an outage at static NAT
CSCwj66537	Snort3 crashes due to processing pdf tokenizer with no limits.
CSCwj67600	Autodeployment failing on cdFMC v20240307 when onboarding a 1010 v7.2.5
CSCwj67707	ECDSA certificates are not supported by FMC ISE integration
CSCwj67787	New User activity page does not load because the VPN bytes in and out are long.
CSCwj68096	Console Access Stuck for ASAv hosted in CSP after Upgrade to 9.18.3.56
CSCwj68286	FMC GUI errors out when searching for Topology Name that has a decimal point in the name
CSCwj68604	Tomcat and VmsBackendServer down post upgrade if a userrole description is too long
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
CSCwj69780	SNMP host group content change results in SNMP process termination on management interface
CSCwj71064	Snort dropping connections with reason blocked or blacklisted by the firewall preprocessor
CSCwj71443	"FDM Keyring's certificate is invalid, reason: expired" health alert on FMC

Bug ID	Headline
CSCwj72022	Deployment time increased by 30-45 seconds after the upgrade when applying specific Platform Setting
CSCwj72369	sync call got stuck resulting in boot loop
CSCwj72615	VPN status not getting updated on site-to-site monitoring.
CSCwj72683	ASA - Bookmarks on the WebVPN portal are unreachable after successful login.
CSCwj72721	Deployment failure and rollback when BGP communities added or removed in route-map match clause
CSCwj73053	ASA may traceback and reload in Thread Name 'DATAPATH-21-16432'
CSCwj73061	SNMP OID for CPUTotal1min omits snort cpu cores entries when polled
CSCwj74323	ASAv Memory leak involving PKI/Crypto for VPN
CSCwj74716	tpk_mi upgrade failed from 7.4.1.1 > 7.6.0 000_start/000_00_run_cli_kick_start.sh.
CSCwj77061	Need an configurable parameter to increase the timout for SHOW_XML_REQUEST
CSCwj77504	User group map miss after Hardware FMC model migration from FMC2600 to FMC4700
CSCwj77700	FTD LINA Traceback and Reload idfw_proc Thread
CSCwj79736	eStreamer memory leak when the FMC receives events from CDO-managed FTDs
CSCwj81115	SFDataCorrelator deadlock on reconfigure after RNAStop and monetdb output queue is full
CSCwj81743	FTD - Trace back and reload due to NAT involving fqdn objects
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
CSCwj83533	FAN is working as expected but FAN LED is in off state.
CSCwj83634	Seeing message "reg_fover_nlp_sessions: failover ioctl C_FOREG failed"
CSCwj84168	SFDataCorrelator log spam, repeatedly purging expired services and client apps
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

Bug ID	Headline
CSCwj86116	High LINA CPU observed due to NetFlow configuration
CSCwj86320	Standby Unit Interfaces enter "Waiting" Status Post-FTD Upgrade Due to Incorrect "Hello" Message MAC
CSCwj87257	Invalid health alert msg - Classic License Expiration Monitor for "License mismatch on stack" on FTD
CSCwj87373	FMC Rest API Internal Server Error when log Interval attribute is not set
CSCwj87501	ASA/FTD may traceback and reload in Thread Name 'fover_FSM_thread'
CSCwj87770	FPR2100-ASA Unable to generate CSR without FXOS IP address on SAN field
CSCwj88400	FTD may traceback and reload in process name lina while processing appAgent msg reply
CSCwj88765	FMC Health Monitoring sends incomplete message when language is changed.
CSCwj88843	Larger entries in EoRevisionStore table causing HA Sync to fail mysqldump process
CSCwj89228	FTD /mnt 100% disk utilization due to snort memory mapped files
CSCwj89264	FTD HA: Traceback and reload in netsnmp_oid_compare_ll
CSCwj90826	Snort2 SSL decryption with known key fails on Chrome v124 and above.
CSCwj91341	Failsafe mode default values are unattainable on some platforms need adjustment per platform/mode
CSCwj91420	Snort3 crashes while collecting flow-ip-profiling
CSCwj92784	RAVPN: Failure to create SGT-IP mapping due to ID table exhaustion
CSCwj92973	CdFMC: Device migration with RAVPN fails during import
CSCwj93300	FMC: Comments on rule change required not working in Classic Theme Legacy UI
CSCwj93718	Unable to run "nslookup" command on FXOS
CSCwj95322	disable stat check for file
CSCwj95590	Browser redirects to logon page when the user clicks the WebVPN bookmark
CSCwj97444	cdFMC : AC rule shown as removed in policy preview
CSCwj97492	Access rule name shows "invalid ID" instead of the rule names after patching from 7.2.4 to 7.2.5
CSCwj98451	FMC got deregistered from Smart License after upgrade
CSCwj98573	Encountering an unknown error [9999] when attempting to modify the identity policy.
CSCwj98580	Classification mismatch between intrusion and correlation events

Bug ID	Headline
CSCwj99362	"show inventory" output shows Name: "power supply 0" on Firepower
CSCwj99941	M6 hardware models are hardly storing only a week old health monitoring data
CSCwk00401	CdFMC: FTD Migration Failing on Registration Phase
CSCwk00604	ASA Fails to initiate AAA Authentication with IKEv2-EAP and Windows Native VPN Client
CSCwk00628	Captive portal returns bad request for snort 2 for FMC 7.4.x , FTD version < 7.4
CSCwk02804	WebVPN connections stuck in CLOSEWAIT state
CSCwk02928	ASA/FTD may traceback and reload in Thread Name PTHREAD
CSCwk04216	Realm download task failing with ADI process is not currently available
CSCwk04246	Unable to download users/groups getting Failed to get response from ADI.
CSCwk04290	FPR 21xx - Traceback in Process Name: lina-mps during normal operations
CSCwk04492	ASA CLI hangs with 'show run' with multiple ssh sessions
CSCwk04754	Filtered ACP rules are not greyed out when disabled using Bulk action
CSCwk04893	FTD does not compact files that are used to communicate updates to the SGT/IP mappings
CSCwk04908	FTD Unable to register to FMC due to empty DNS Server configured.
CSCwk05800	ASA/FTD SNMP polling fails due to overlapping networks in snmp-server host-group
CSCwk05851	"set ip next-hop" line deleted from config at reload if IP address is matched to a NAME
CSCwk06216	Loss of interface mapping with security zones after deployment
CSCwk06264	FMC REST API || ICMP objects with no code value breaking GET call and JSON parsing
CSCwk06573	Serviceablity : Improve routing infra debugs and add new for error conditions
CSCwk07563	Force deploy not re-generating export-cache in the device
CSCwk07934	Clock skew between FXOS and Lina causes SAML assertion processing failure
CSCwk08064	ADI Session Processing Delays return after upgrade to 7.2.x
CSCwk08476	FTD/ASA traceback and reload due to 'show bgp summary' memory leak
CSCwk08576	command to print the debug menu setting of service worker
CSCwk09559	FMC - Custom User role VPN allows user to make changes to Site to Site VPN when Modify is unchecked.

Bug ID	Headline
CSCwk09612	Clock skew: FXOS clock diverges from Lina NTP time ~1-10 secs
CSCwk10884	Connectivity failure due to mismatch between l2_table and subinterface mac address
CSCwk11254	"Rule Unavailable" for some local intrusion rules may be shown in intrusion event packet view
CSCwk11381	Deploying an authorization server with an LDAP attribute map results in deployment failure.
CSCwk12337	RC4 ciphers cannot be disabled on FMC/FTD for captive portal authentication with Kerberos
CSCwk12470	Fatal error: Error running script 800_post/100_ftd_onbox_data_import.sh
CSCwk12497	Traceback and reload on active unit due to HA break operation.
CSCwk12673	TCP Session Interrupted if Keep-Alive with 1 Byte is Received
CSCwk12698	SNMP polling of admin context mgmt interface fails to show all interfaces across all contexts
CSCwk13812	ASA/FTD incorrectly forwards extended community attribute after upgrade.
CSCwk14657	Bring back support for portal-access-rule for weblaunch for RAVPN sessions
CSCwk14685	FTD : Management interface showing down despite being up and operational
CSCwk14909	Traffic drop with 'rule-transaction-in-progress' after failover with TCM cfgd in multi-ctx mode
CSCwk17637	State Link Stops Sending Hello Messages Post-Failover Triggered by Snort Crash in FTD HA
CSCwk17854	FTD doesn't send Type A query after receiving a refuse error from one DNS server in AAAA query.
CSCwk20882	ESP sequence number of 0 being sent after SA establishment/rekey
CSCwk21533	FMC Users page in sub domain does not load
CSCwk21561	Add warning message when configuring CCL MTU
CSCwk21562	Radius server configuration for FTD external authentication is not deployed to FTD.
CSCwk22034	Snmpwalk displays incorrect interface speeds for values greater or equal than 10G
CSCwk22814	FMC - Add warning message when configuring CCL MTU
CSCwk24176	FTD/ASA - VPN traffic flowing through the device may trigger tracebacks and reloads.
CSCwk24380	No devices listed in Packet Tracer "Select Device" dropdown
CSCwk24440	Backups may fail on remote storage when the filebackup.tar contents are so huge

Bug ID	Headline
CSCwk24597	EventHandler may not send events to the FMC when Snort wrote many zero-length snort-unified files
CSCwk25117	ENH: Add application support for blocking consecutive AAA failures on LINA
CSCwk26594	temporary backups files shouldn't be kept on remote storage and do not parse other format files
CSCwk26968	Backup feature does not save/restore DAP configuration in multiple context mode.
CSCwk27175	ASA/FTD: Substantial increase in the time taken to load configuration
CSCwk27639	FMC 7.2.5 Showing incorrect data of FTD HA at 6.6.5 under fleet upgrade
CSCwk27830	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwk27965	Safety Net for Infinite Recursion Crashes due to Bad Stream TCP State in Post-ACK mode
CSCwk29771	FTD 7.4.1.x sends NAS-IP-Address:0.0.0.0 in Radius Request packet as network interface
CSCwk31371	NAT_HARDEN: CGNAT breaks when mapped ifc is configured as any
CSCwk32340	Enable logs to identify corrupted policy when deployment fails with "SNAPSHOT_PG_TIMESTAMP_ERROR"
CSCwk32501	256/1550 block depletion process fover_thread
CSCwk33070	FMC "java.lang.OutOfMemoryError: Java heap space" errors in feed_data_manager.log
CSCwk33634	TLS Client Hello packet is dropped by snort
CSCwk33842	FMC Management workflow issue: Cannot remove NetworkObject from group and delete it in same ticket
CSCwk33876	Standard Access List Objects can be written with leading whitespace
CSCwk34888	Health Alerts are generating for sub interface even when main interface is excluded.
CSCwk34905	ISE connection status health alerts on FMC with ise services down
CSCwk36312	High cpu on "update block depletion" causing BGP flap terminated on FTD
CSCwk37371	SGT INLINE-TAG added after upgrade to 7.4.x
CSCwk37701	FTD lost connection with cdFMC after FTD backup Restoration
CSCwk38851	FMC should not take a policy backup during patch / Hotfix installations.
CSCwk39514	Endpoint Assessment features are not enabled when HostScan package is modified via FMC

Bug ID	Headline
CSCwk40726	FMC REST API calls to get AC policy data times out, AC policy GUI slowness with larger rule query
CSCwk41007	ASA/FTD may traceback and reload in Thread Name 'PTHREAD-1756'
CSCwk41806	Need to Protect LINA from getting killed by OOM
CSCwk44366	cdFMC Fails to configure-geneve-encapsulation on interface
CSCwk48975	Packet-tracer output incorrectly appends 'control-plane' to drops for data-plane access-group
CSCwk52448	Unable to deploy changes to migrated 7.0.x version of 21xx 11xx FTD-HA pair to cdFMC from onprem
CSCwk53048	Standby HA FMC entering standalone mode - /var/tmp/compliance.rules which was created was invalid.
CSCwk53257	API call for ftdallinterfaces returns an inaccurate "self" element.
CSCwk53312	Unable to upgrade cluster with status "cluster/HA pair is not eligible'
CSCwk54033	FMC can not connect to private AMP when proxy is enabled in management interface
CSCwk54077	Empty network objects cause cdFMC migration to fail
CSCwk56388	GRE traffic getting dropped after failover
CSCwk59009	IPv6 SSL Anyconnect access blocked in HA pair
CSCwk59520	Instrument new logs in the startup process to collect more information
CSCwk61157	FTD LINA Traceback and Reload dhcp_daemon Thread
CSCwk61479	During migration to cdFMC from onPrem, certain objects are having inconsistency between CSM and EO
CSCwk62296	Address SSP OpenSSH regreSSHion vulnerability
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.
CSCwk64418	NTP is not synchronising when using SHA-1 authentication
CSCwk64643	Failover prompt shows state active while the firewall is in Negotiation
CSCwk64709	FXOS upgrade failure due to insufficient free space in /mnt/pss (isan.log consumes most of space)
CSCwk64759	FMC EIGRP Setup page showing first object duplicated
CSCwk67346	DAP policies not working with attribute TRUE/FALSE

Bug ID	Headline
CSCwk71227	FTD running on FPR 2k with LDAP skips backslash when updating ldap.conf
CSCwk74813	TLS1.3 block allocation causes Hostscan and ASDM communication failures
CSCwk74997	With CVE-ID cannot search the IPS events on the FMC
CSCwk75832	Snort3 crash when AppID reload and snort restarts are happening simultaneously
CSCwk78075	FTD does not mark stuck ongoing deployments as failed leading to subsequent deployment failures
CSCwk78242	Empty user attributes in LDAP causes partial user/group download
CSCwk81274	FMC: Not receiving any Email Alert after upgrade
CSCwk82591	Unable to create MI FTD in TPK chassis
CSCwk86033	Database corruption due to VPN objects post migration to cdFMC
CSCwk87081	cdFMC: tmp_cisco is consuming high boot volume space for the cdFMC tenants
CSCwk88201	S2S VPN with 3rd party broken after upgrading FPR 9.20
CSCwk89127	Backup_info table is not being pruned, causing DB queries to slow down
CSCwk98990	Large number of stats files can cause events to be delayed
CSCwm11515	SNMP trap OID changed after upgrade
CSCwm27588	fix to remove space characters in auth object names during FMC upgrade may cause upgrade failure
CSCwm29768	Connection been logged for rules with no logging enabled
CSCwm45164	cdFMC: unable to modify the VTI interfaces due to Tunnel type is missing in DB

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 13: Upgrade Guides

Platform	Upgrade Guide	Link
Management center	Management center version you are *currently* running.	https://www.cisco.com/go/fmc-upgrade

Platform	Upgrade Guide	Link
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 14: 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 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-76-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