



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

First Published: 2023-09-07

Last Modified: 2024-05-03

Cisco Secure Firewall Threat Defense Release Notes

This document contains release information for **Version 7.4** of:

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

For Cisco Defense Orchestrator (CDO) deployments, see the [Cisco Cloud-Delivered Firewall Management Center Release Notes](#) or [What's New for Cisco Defense Orchestrator](#).

Release Dates

Table 1: Version 7.4 Dates

Version	Build	Date	Platforms
7.4.1.1	12	2024-04-15	All
7.4.1	172	2023-12-13	All
7.4.0	81	2023-09-07	Management center Secure Firewall 4200 series

Compatibility

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

For compatibility information, see:

- [Cisco Secure Firewall Management Center Compatibility Guide](#)
- [Cisco Secure Firewall Threat Defense Compatibility Guide](#)
- [Cisco Firepower 4100/9300 FXOS Compatibility](#)

Features

This document describes the new and deprecated features for Version 7.4.

For 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; for example, if you must change a configuration.

Snort

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



Important

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

Intrusion Rules and Keywords

Upgrades can import and auto-enable new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. If a newer intrusion rule uses keywords that are not supported in your current version, that rule is not imported when you update the SRU/LSP. After you upgrade and those keywords become supported, the new intrusion rules are imported and, depending on your IPS configuration, can become auto-enabled and thus start generating events and affecting traffic flow.

For details on new keywords, see the Snort release notes: <https://www.snort.org/downloads>.

FlexConfig

Upgrades can add web interface or Smart CLI support for features that previously required FlexConfig. The upgrade does not convert FlexConfigs. After upgrade, configure the newly supported features in the web interface or Smart CLI. When you are satisfied with the new configuration, delete the deprecated FlexConfigs.

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



Caution

Although you cannot newly assign or create FlexConfig objects using deprecated commands, in most cases existing FlexConfigs continue to work and you can still deploy. However, sometimes, using deprecated commands can cause deployment issues.

Management Center Features in Version 7.4.1

Table 2: Management Center Features in Version 7.4.1

Feature	Minimum Management Center	Minimum Threat Defense	Details
Reintroduced Features			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Reintroduced features.	Feature dependent	Feature dependent	

Feature	Minimum Management Center	Minimum Threat Defense	Details
			<p>Version 7.4.1 reintroduces features, enhancements, and critical fixes that were included in maintenance releases to even-numbered versions (7.0.x, 7.2.x), but that were not included in odd-numbered versions (7.1.x, 7.3.x) or in Version 7.4.0.</p> <p>Reintroduced features include:</p> <ul style="list-style-type: none"> • Support for threat defense on all device platforms supported in Version 7.3, and also on the Firepower 1010E (last supported in 7.2). • Management center detects interface sync errors. Upgrade impact. • Updated web analytics provider. Upgrade impact. • Configure DHCP relay trusted interfaces from the management center web interface. Upgrade impact. • Create network groups while editing NAT rules. • Single backup file for high availability management centers. • Open the packet tracer from the unified event viewer. • Health alerts for excessive disk space used by deployment history (rollback) files. Upgrade impact. • Health alerts for NTP sync issues. Upgrade impact. • View and generate reports on configuration changes since your last deployment. • Set the number of deployment history files to retain for device rollback. • Improved upgrade starting page and package management. • Enable revert from the threat defense upgrade wizard. • View detailed upgrade status from the threat defense upgrade wizard. • Suggested release notifications. • New upgrade wizard for the management center. • Hotfix high availability management centers without pausing synchronization. • Updated internet access requirements for direct-downloading software upgrades. Upgrade impact. • Scheduled tasks download patches and VDB updates only. Upgrade impact. • Enable/disable access control object optimization. • Cluster control link ping tool. • Set the frequency of Snort 3 core dumps.

Feature	Minimum Management Center	Minimum Threat Defense	Details
			<ul style="list-style-type: none"> • Capture dropped packets with the Secure Firewall 3100/4200.
Platform			
Network modules for the Secure Firewall 3130 and 3140.	7.4.1	7.4.1	<p>The Secure Firewall 3130 and 3140 now support these network modules:</p> <ul style="list-style-type: none"> • 2-port 100G QSFP+ network module (FPR3K-XNM-2X100G) <p>See: Cisco Secure Firewall 3110, 3120, 3130, and 3140 Hardware Installation Guide</p>
Optical transceivers for Firepower 9300 network modules.	7.4.1	7.4.1	<p>The Firepower 9300 now supports these optical transceivers:</p> <ul style="list-style-type: none"> • QSFP-40/100-SRBD • QSFP-100G-SR1.2 • QSFP-100G-SM-SR <p>On these network modules:</p> <ul style="list-style-type: none"> • FPR9K-NM-4X100G • FPR9K-NM-2X100G • FPR9K-DNM-2X100G <p>See: Cisco Firepower 9300 Hardware Installation Guide</p>
Performance profile support for the Secure Firewall 3100.	7.4.1	7.4.1	<p>The performance profile settings available in the platform settings policy now apply to the Secure Firewall 3100. Previously, this feature was supported on the Firepower 4100/9300, the Secure Firewall 4200, and on threat defense virtual.</p> <p>See: Configure the Performance Profile</p>
Interfaces			
Deploy without the diagnostic interface on threat defense virtual for Azure and GCP.	7.4.1	7.4.1	<p>You can now deploy without the diagnostic interface on threat defense virtual for Azure and GCP. Previously, we required one management, one diagnostic, and at least two data interfaces. New interface requirements are:</p> <ul style="list-style-type: none"> • Azure: one management, two data (max eight) • GCP: one management, three data (max eight) <p>Restrictions: This feature is supported for new deployments only. It is not supported for upgraded devices.</p> <p>See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide</p>
Device Management			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Device management services supported on user-defined VRF interfaces.	7.4.1	Any	<p>Device management services configured in the threat defense platform settings (NetFlow, SSH access, SNMP hosts, syslog servers) are now supported on user-defined Virtual Routing and Forwarding (VRF) interfaces.</p> <p>Platform restrictions: Not supported with container instances or clustered devices.</p> <p>See: Platform Settings</p>
High Availability/Scalability: Threat Defense			
Multi-instance mode for the Secure Firewall 3100.	7.4.1	7.4.1	<p>You can deploy the Secure Firewall 3100 as a single device (<i>appliance mode</i>) or as multiple container instances (<i>multi-instance mode</i>). In multi-instance mode, you can deploy multiple container instances on a single chassis that act as completely independent devices. Note that in multi-instance mode, you upgrade the operating system and the firmware (<i>chassis upgrade</i>) separately from the container instances (<i>threat defense upgrade</i>).</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Devices > Device Management > Add > Chassis • Devices > Device Management > Device > Chassis Manager • Devices > Platform Settings > New Policy > Chassis Platform Settings • Devices > Chassis Upgrade <p>New/modified threat defense CLI commands: configure multi-instance network ipv4, configure multi-instance network ipv6</p> <p>New/modified FXOS CLI commands: create device-manager, set deploymode</p> <p>Platform restrictions: Not supported on the Secure Firewall 3105.</p> <p>See: Multi-Instance Mode for the Secure Firewall 3100 and Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</p>
16-node clusters for threat defense virtual for VMware and KVM.	7.4.1	7.4.1	<p>You can now configure 16-node clusters for threat defense virtual for VMware and threat defense virtual for KVM.</p> <p>See: Clustering for Threat Defense Virtual in a Private Cloud</p>
Target failover for clustered threat defense virtual devices for AWS.	7.4.1	7.4.1	<p>You can now configure target failover for clustered threat defense virtual devices for AWS using the AWS Gateway Load Balancer (GWLB).</p> <p>Platform restrictions: Not available with five and ten-device licenses.</p> <p>See: Configure Target Failover for Threat Defense Clustering with GWLB in AWS</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
Detect configuration mismatches in threat defense high availability pairs.	7.4.1	7.4.1	You can now use the CLI to detect configuration mismatches in threat defense high availability pairs. New/modified CLI commands: show failover config-sync error , show failover config-sync stats See: Troubleshoot Configuration Sync Failure and Cisco Secure Firewall Threat Defense Command Reference

High Availability: Management Center

Management center high availability synchronization enhancements.	7.4.1	Any	Management center high availability (HA) includes the following synchronization enhancements: <ul style="list-style-type: none"> • Large configuration history files can cause synchronization to fail in high-latency networks. To prevent this from happening, the device configuration history files are now synchronized in parallel with other configuration data. This enhancement also reduces the synchronization time. • The management center now monitors the configuration history file synchronization process and displays a health alert if the synchronization times out. New/modified screens: You can view these alerts on the following screens: <ul style="list-style-type: none"> • Notifications > Message Center > Health • Integration > Other Integrations > High Availability > Status (under Summary) See: Viewing Management Center High Availability Status
---	-------	-----	--

SD-WAN

Application monitoring on the SD-WAN Summary dashboard.	7.4.1	7.4.1	You can now monitor WAN interface application performance on the SD-WAN Summary dashboard. New/modified screens: Overview > SD-WAN Summary > Application Monitoring See: WAN Summary Dashboard
---	-------	-------	---

VPN

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

Feature	Minimum Management Center	Minimum Threat Defense	Details
Zero trust access enhancements.	7.4.1	7.4.1 with Snort 3	<p>Management center now includes the following zero trust access enhancements:</p> <ul style="list-style-type: none"> You can configure source NAT for an application. The configured network object or object group translates the incoming request's public network source IP address to a routable IP address inside the application network. You can troubleshoot the zero trust configuration issues using the diagnostics tool. To enhance your experience, we now collect zero trust application policy telemetry data. <p>New/modified screens: Policies > Access Control > Zero Trust Application</p> <p>New/modified CLI commands: show running-config zero-trust, show zero-trust statistics</p> <p>See:</p> <ul style="list-style-type: none"> Create an Application Monitor Zero Trust Sessions Cisco Secure Firewall Threat Defense Command Reference Cisco Success Network Telemetry Data Collected from Cisco Secure Firewall Management Center
CIP detection.	7.4.1	7.4.1 with Snort 3	<p>You can now detect and handle Common Industrial Protocol (CIP) by using CIP and Ethernet/IP (ENIP) application conditions in your security policies.</p> <p>See: Application Rule Conditions</p>
CIP safety detection.	7.4.1	7.4.1 with Snort 3	<p>CIP Safety is a CIP extension that enables the safe operation of industrial automation applications. The CIP inspector can now detect the CIP Safety segments in the CIP traffic. To detect and take action on the CIP Safety segments, enable the CIP inspector in the management center's network Analysis policy and assign it to an access control policy.</p> <p>New/modified screens: Policies > Access Control > Edit a policy > Add Rule > Applications tab > Search for CIP Safety in the search box.</p> <p>See: Cisco Secure Firewall Management Center Snort 3 Configuration Guide</p>

Access Control: Identity

Feature	Minimum Management Center	Minimum Threat Defense	Details
Captive portal support for multiple Active Directory realms (realm sequences).	7.4.1	7.4.1	<p>Upgrade impact. Update custom authentication forms.</p> <p>You can configure active authentication for either an LDAP realm; or a Microsoft Active Directory realm or a realm sequence. In addition, you can configure a passive authentication rule to fall back to active authentication using either a realm or a realm sequence. You can optionally share sessions between managed devices that share the same identity policy in access control rules.</p> <p>In addition, you have the option to require users to authenticate again when they access the system using a different managed device than they accessed previously.</p> <p>If you use the HTTP Response Page authentication type, after you upgrade threat defense, you must add <code><select name="realm" id="realm"></select></code> to your custom authentication form. This allows the user to choose between realms.</p> <p>Restrictions: Not supported with Microsoft Azure Active Directory.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Policies > Identity > (edit policy) > Active Authentication > Share active authentication sessions across firewalls • Identity policy > (edit) > Add Rule > Passive Authentication > Realms & Settings > Use active authentication if passive or VPN identity cannot be established • Identity policy > (edit) > Add Rule > Active Authentication > Realms & Settings > Use active authentication if passive or VPN identity cannot be established <p>See: How to Configure the Captive Portal for User Control</p>
Share captive portal active authentication sessions across firewalls.	7.4.1	7.4.1	<p>Determines whether or not users are required to authenticate when their authentication session is sent to a different managed device than one they previously connected to. If your organization requires users to authenticate every time they change locations or sites, you should <i>disable</i> this option.</p> <ul style="list-style-type: none"> • (Default.) Enable to allow users to authenticate with any managed device associated with the active authentication identity rule. • Disable to require the user to authenticate with a different managed device, even if they have already authenticated with another managed device to which the active authentication rule is deployed. <p>New/modified screens: Policies > Identity > (edit policy) > Active Authentication > Share active authentication sessions across firewalls</p> <p>See: How to Configure the Captive Portal for User Control</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
Merge downloadable access control list with a Cisco attribute-value pair ACL for RADIUS identity sources, using the management center web interface.	7.4.1	Any	<p>Upgrade impact. Redo any related FlexConfigs after upgrade.</p> <p>New/modified screens: Objects > Object Management > AAA Server > RADIUS Server Group > Add RADIUS Server Group > Merge Downloadable ACL with Cisco AV Pair ACL</p> <p>New CLI commands:</p> <ul style="list-style-type: none"> • sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl after-avpair • sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl before-avpair <p>See: RADIUS Server Group Options</p>
Health Monitoring			
Chassis-level health alerts for the Firepower 4100/9300.	7.4.1	Any with FXOS 2.14.1	<p>Upgrade impact. Enable the new health module and apply device health policy after upgrade.</p> <p>You can now view chassis-level health alerts for Firepower 4100/9300 by registering the chassis to the management center as a read-only device. You must also enable the Firewall Threat Defense Platform Faults health module and apply the health policy. The alerts appear in the Message Center, the health monitor (in the left pane, under Devices, select the chassis), and in the health events view.</p> <p>You can also add a chassis (and view health alerts for) the Secure Firewall 3100 in multi-instance mode. For those devices, you use the management center to manage the chassis. But for the Firepower 4100/9300 chassis, you still must use the chassis manager or the FXOS CLI.</p> <p>New/modified screens: Devices > Device Management > Add > Chassis</p> <p>See: Add a Chassis to the Management Center</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
Improved management center memory usage calculation, alerting, and swap memory monitoring.	7.4.1	Any	<p>Upgrade impact. Memory usage alert thresholds may be lowered.</p> <p>We improved the accuracy of management center memory usage and have lowered the default alert thresholds to 88% warning/90% critical. If your thresholds were higher than the new defaults, the upgrade lowers them automatically—you do not have to apply health policies for this change to take place. Note that the management center may now reboot in extremely critical system memory condition if terminating high-memory processes does not work.</p> <p>You can also add new swap memory usage metrics to a new or existing management center health dashboard. Make sure you choose the Memory metric group.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • System (⚙️) > Health > Monitoring > Firewall Management CenterAdd/Edit DashboardMemory • System (⚙️) > Health > Policy > Management Center Health Policy > Memory <p>See: Using Management Center Health Monitor</p>
Deployment and Policy Management			
Change management.	7.4.1	Any	<p>You can enable change management if your organization needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed.</p> <p>We added the System (⚙️) > Configuration > Change Management page to enable the feature. When enabled, there is a System (⚙️) > Change Management Workflow page, and a new Ticket (📄) quick access icon in the menu.</p> <p>See: Change Management</p>
Upgrade			
Firmware upgrades included in FXOS upgrades.	7.4.1	Any	<p>Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.</p> <p>For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1 now include firmware upgrades. If any firmware component on the device is older than the one included in the FXOS bundle, the FXOS upgrade also updates the firmware. If the firmware is upgraded, the device reboots twice—once for FXOS and once for the firmware.</p> <p>Just as with software and operating system upgrades, do not make or deploy configuration changes during firmware upgrade. Even if the system appears inactive, do not manually reboot or shut down during firmware upgrade.</p> <p>See: Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
Automatically generate configuration change reports after management center upgrade.	7.4.1	Any	<p>You can automatically generate reports on configuration changes after major and maintenance management center upgrades. This helps you understand the changes you are about to deploy. After the system generates the reports, you can download them from the Tasks tab in the Message Center.</p> <p>Other version restrictions: Only supported for management center upgrades from Version 7.4.1+. Not supported for upgrades to Version 7.4.1 or any earlier version.</p> <p>New/modified screens: System (⚙️) > Configuration > Upgrade Configuration > Enable Post-Upgrade Report</p> <p>See: Upgrade Configuration</p>
Administration			
Erase the hard drives on a hardware management center.	7.4.1	Any	<p>You can use the management center CLI to reboot and permanently erase its own hard drive data. After the erase is completed, you can install a fresh software image.</p> <p>New/modified CLI commands: secure erase</p> <p>See: Secure Firewall Management Center Command Line Reference</p>
Usability, Performance, and Troubleshooting			
Troubleshooting file generation and download available from Device and Cluster pages.	7.4.1	7.4.1	<p>You can generate and download troubleshooting files for each device on the Device page and also for all cluster nodes on the Cluster page. For a cluster, you can download all files as a single compressed file. You can also include cluster logs for the cluster for cluster nodes. You can alternatively trigger file generation from the Devices > Device Management > More (⚙️) > Troubleshoot Files menu.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Devices > Device Management > Device > General • Devices > Device Management > Cluster > General <p>See: Generate Troubleshooting Files</p>
Automatic generation of a troubleshooting file on a node when it fails to join the cluster.	7.4.1	7.4.1	<p>If a node fails to join the cluster, a troubleshooting file is automatically generated for the node. You can download the file from Tasks or from the Cluster page.</p> <p>See: Troubleshooting the Cluster</p>
View CLI output for a device or device cluster.	7.4.1	Any	<p>You can view a set of pre-defined CLI outputs that can help you troubleshoot the device or cluster. You can also enter any show command and see the output.</p> <p>New/modified screens: Devices > Device Management > Cluster > General</p> <p>See: View CLI Output</p>

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

Management Center Features in Version 7.4.0



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

Table 3: Management Center Features in Version 7.4.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Reintroduced Features			
Reintroduced features.	7.4.0	Feature dependent	<p>Version 7.4.0 reintroduces features, enhancements, and critical fixes that were included in maintenance releases to even-numbered versions (7.0.x, 7.2.x), but that were not included in odd-numbered versions (7.1.x, 7.3.x).</p> <p>Reintroduced features include:</p> <ul style="list-style-type: none"> • Access control performance improvements (object optimization). Upgrade impact. • Reduced "false failovers" for threat defense high availability. • Download only the country code geolocation package. Upgrade impact.
Platform			
Management center 1700, 2700, 4700.	7.4.0	Any	<p>We introduced the Secure Firewall Management Center 1700, 2700, and 4700, which can manage up to 300 devices. Management center high availability is supported.</p> <p>See: Cisco Secure Firewall Management Center 1700, 2700, and 4700 Getting Started Guide</p>
Management center virtual for Microsoft Hyper-V.	7.4.0	Any	<p>We introduced Secure Firewall Management Center Virtual for Microsoft Hyper-V, which can manage up to 25 devices. Management center high availability is supported.</p> <p>See: Cisco Secure Firewall Management Center Virtual Getting Started Guide</p>
Secure Firewall 4200.	7.4.0	7.4.0	<p>We introduced the Secure Firewall 4215, 4225, and 4245. You must manage these devices with a management center. They do not support device manager.</p> <p>These devices support the following new network modules:</p> <ul style="list-style-type: none"> • 2-port 100G QSFP+ network module (FPR4K-XNM-2X100G) • 4-port 200G QSFP+ network module (FPR4K-XNM-4X200G) <p>See: Cisco Secure Firewall 4215, 4225, and 4245 Hardware Installation Guide</p>
Performance profile support for the Secure Firewall 4200.	7.4.0	7.4.0	<p>The performance profile settings available in the platform settings policy now apply to the Secure Firewall 4200. Previously, this feature was supported only on the Firepower 4100/9300 and on threat defense virtual.</p> <p>See: Configure the Performance Profile</p>
Platform Migration			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Migrate from Firepower 1000/2100 to Secure Firewall 3100.	7.4.0	Any	<p>You can now easily migrate configurations from the Firepower 1000/2100 to the Secure Firewall 3100.</p> <p>New/modified screens: Devices > Device Management > Migrate</p> <p>Platform restrictions: Migration not supported from the Firepower 1010 or 1010E.</p> <p>See: About Secure Firewall Threat Defense Model Migration</p>
Migrate from Firepower Management Center 4600 to Secure Firewall Management Center for AWS.	7.4.0	Any	<p>You can migrate from Firepower Management Center 4600 to Secure Firewall Management Center Virtual for AWS with a 300-device license.</p> <p>See: Cisco Secure Firewall Management Center Model Migration Guide</p>
Migrate from Firepower Management Center 1600/2600/4600 to Secure Firewall Management Center 1700/2700/4700.	7.4.0	Any	<p>You can migrate from Firepower Management Center 1600/2600/4600 to Secure Firewall Management Center 1700/2700/4700.</p> <p>See: Cisco Secure Firewall Management Center Model Migration Guide</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
Migrate from Firepower Management Center 1000/2500/4500 to Secure Firewall Management Center 1700/2700/4700.	7.4.0 only	7.0.0	<p>You can migrate Firepower Management Center 1000/2500/4500 to Secure Firewall Management Center 1700/2700/4700. To migrate, you must <i>temporarily</i> upgrade the old management center from Version 7.0 to Version 7.4.0.</p> <p>Important Version 7.4 is only supported on the 1000/2500/4500 during the migration process. You should minimize the time between management center upgrade and device migration.</p> <p>To summarize the migration process:</p> <ol style="list-style-type: none"> 1. Prepare for upgrade and migration. Read, understand, and meet all the prerequisites outlined in the release notes, upgrade guides, and migration guide. Make sure the old management center is ready to go: freshly deployed, fully backed up, all appliances in good health, etc. You should also set up the new management center. 2. Upgrade the old management center and all its managed devices to at least Version 7.0.0 (7.0.5 recommended). If you are already running the minimum version, you can skip this step. 3. Upgrade the old management center to Version 7.4.0. Unzip (but do not untar) the upgrade package before uploading it to the management center. Download from: Special Release. 4. Migrate the management center as described in the model migration guide. 5. Verify migration success. If the migration does not function to your expectations and you want to switch back, note that Version 7.4 is unsupported for general operations on the 1000/2500/4500. To return the old management center to a supported version you must reimage back to Version 7.0, restore from backup, and reregister devices. <p>See:</p> <ul style="list-style-type: none"> • Cisco Secure Firewall Threat Defense Release Notes • Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 • Cisco Secure Firewall Management Center Model Migration Guide <p>If you have questions or need assistance at any point in the migration process, contact Cisco TAC.</p>

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

Feature	Minimum Management Center	Minimum Threat Defense	Details
			<p>You can migrate devices from Firepower Management Center 1000/2500/4500 to cloud-delivered Firewall Management Center.</p> <p>To migrate devices, you must <i>temporarily</i> upgrade the on-prem management center from Version 7.0.3 (7.0.5 recommended) to Version 7.4.0. This temporary upgrade is required because Version 7.0 management centers do not support device migration to the cloud. Additionally, only standalone and high availability threat defense devices running Version 7.0.3+ (7.0.5 recommended) are eligible for migration. Cluster migration is not supported at this time.</p> <p>Important Version 7.4.0 is only supported on the 1000/2500/4500 during the migration process. You should minimize the time between management center upgrade and device migration.</p> <p>To summarize the migration process:</p> <ol style="list-style-type: none"> 1. Prepare for upgrade and migration. Read, understand, and meet all the prerequisites outlined in the release notes, upgrade guides, and migration guide. <p>Before you upgrade, it is especially important that the on-prem management center is "ready to go," that is, managing only the devices you want to migrate, configuration impact assessed (such as VPN impact), freshly deployed, fully backed up, all appliances in good health, and so on.</p> <p>You should also provision, license, and prepare the cloud tenant. This must include a strategy for security event logging; you cannot retain the on-prem management center for analytics because it will be running an unsupported version.</p> 2. Upgrade the on-prem management center and all its managed devices to at least Version 7.0.3 (Version 7.0.5 recommended). <p>If you are already running the minimum version, you can skip this step.</p> 3. Upgrade the on-prem management center to Version 7.4.0. <p>Unzip (but do not untar) the upgrade package before uploading it to the management center. Download from: Special Release.</p> 4. Onboard the on-prem management center to CDO. 5. Migrate all devices from the on-prem management center to the cloud-delivered Firewall Management Center as described in the migration guide. <p>When you select devices to migrate, make sure you choose Delete FTD from On-Prem FMC. Note that the device is not fully deleted unless you commit the changes or 14 days pass.</p> 6. Verify migration success. <p>If the migration does not function to your expectations, you have 14 days to switch back or it is committed automatically. However, note that Version</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
			<p>7.4.0 is unsupported for general operations. To return the on-prem management center to a supported version you must remove the re-migrated devices, re image back to Version 7.0.x, restore from backup, and reregister the devices.</p> <p>See:</p> <ul style="list-style-type: none"> • Cisco Secure Firewall Threat Defense Release Notes • Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 • Migrate On-Prem Management Center Managed Secure Firewall Threat Defense to Cloud-delivered Firewall Management Center <p>If you have questions or need assistance at any point in the migration process, contact Cisco TAC.</p>

Device Management

Low-touch provisioning to register the Firepower 1000/2100 and Secure Firewall 3100 to the management center using a serial number.	7.4.0	<p>Mgmt. center <i>is</i> publicly reachable: 7.2.0</p> <p>Mgmt. center <i>is not</i> publicly reachable: 7.2.4</p>	<p>Low-touch provisioning lets you register Firepower 1000/2100 and Secure Firewall 3100 devices to the management center by serial number without having to perform any initial setup on the device. The management center integrates with SecureX and Cisco Defense Orchestrator for this functionality.</p> <p>New/modified screens: Devices > Device Management > Add > Device > Serial Number</p> <p>Other version restrictions: This feature is not supported on Version 7.3.x or 7.4.0 threat defense devices when the management center is not publicly reachable. Support returns in Version 7.4.1.</p> <p>See: Add a Device to the Management Center Using the Serial Number (Low-Touch Provisioning)</p>
---	-------	---	--

Interfaces

Feature	Minimum Management Center	Minimum Threat Defense	Details
Merged management and diagnostic interfaces.	7.4.0	7.4.0	<p>Upgrade impact. Merge interfaces after upgrade.</p> <p>For new devices using 7.4 and later, you cannot use the legacy diagnostic interface. Only the merged management interface is available.</p> <p>If you upgraded to 7.4 or later and:</p> <ul style="list-style-type: none"> • You did not have any configuration for the diagnostic interface, then the interfaces will merge automatically. • You have configuration for the diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate diagnostic interface. Note that support for the diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. <p>Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including Management) in the configuration.</p> <p>For platform settings, this means:</p> <ul style="list-style-type: none"> • You can no longer enable HTTP, ICMP, or SMTP for diagnostic. • For SNMP, you can allow hosts on management instead of diagnostic. • For Syslog servers, you can reach them on management instead of diagnostic. • If Platform Settings for syslog servers or SNMP hosts specify the diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices. • DNS lookups no longer fall back to the management-only routing table if you do not specify interfaces. <p>New/modified screens: Devices > Device Management > Interfaces</p> <p>New/modified commands: show management-interface convergence</p> <p>See: Merge the Management and Diagnostic Interfaces</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
VXLAN VTEP IPv6 support.	7.4.0	7.4.0	<p>You can now specify an IPv6 address for the VXLAN VTEP interface. IPv6 is not supported for the threat defense virtual cluster control link or for Geneve encapsulation.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Devices > Device Management > Edit Device > VTEP > Add VTEP • Devices > Device Management > Edit Devices > Interfaces > Add Interfaces > VNI Interface <p>See: Configure Geneve Interfaces</p>
Loopback interface support for BGP and management traffic.	7.4.0	7.4.0	<p>You can now use loopback interfaces for AAA, BGP, DNS, HTTP, ICMP, IPsec flow offload, NetFlow, SNMP, SSH, and syslog.</p> <p>New/modified screens: Devices > Device Management > Edit device > Interfaces > Add Interfaces > Loopback Interface</p> <p>See: Configure Loopback Interfaces</p>
Loopback and management type interface group objects.	7.4.0	7.4.0	<p>You can create interface group objects with only management-only or loopback interfaces. You can use these groups for management features such as DNS servers, HTTP access, or SSH. Loopback groups are available for any feature that can utilize loopback interfaces. However, it's important to note that DNS does not support management interfaces.</p> <p>New/modified screens: Objects > Object Management > Interface > Add > Interface Group</p> <p>See: Interface</p>
High Availability/Scalability			
Manage threat defense high availability pairs using a data interface.	7.4.0	7.4.0	<p>Threat defense high availability now supports using a regular data interface for communication with the management center. Previously, only standalone devices supported this feature.</p> <p>See: Using the Threat Defense Data Interface for Management</p>
SD-WAN			
WAN summary dashboard.	7.4.0	7.2.0	<p>The WAN Summary dashboard provides a snapshot of your WAN devices and their interfaces. It provides insight into your WAN network and information about device health, interface connectivity, application throughput, and VPN connectivity. You can monitor the WAN links and take proactive and prompt recovery measures.</p> <p>New/modified screens: Overview > WAN Summary</p> <p>See: WAN Summary Dashboard</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
Policy-based routing using HTTP path monitoring.	7.4.0	7.2.0	<p>Policy-based routing (PBR) can now use the performance metrics (RTT, jitter, packet-lost, and MOS) collected by path monitoring through HTTP client on the application domain rather than the metrics on a specific destination IP. HTTP-based application monitoring option is enabled by default for the interface. You can configure a PBR policy with match ACL having the monitored applications and interface ordering for path determination.</p> <p>New/modified screens: Devices > Device Management > Edit device > Edit interface > Path Monitoring > Enable HTTP based Application Monitoring check box.</p> <p>Platform restrictions: Not supported for clustered devices.</p> <p>See: Configure Path Monitoring Settings</p>
Policy-based routing with user identity and SGTs.	7.4.0	7.4.0	<p>You can now classify the network traffic based on users and user groups, and SGTs in PBR policies. You can select the identity and SGT objects while defining the extended ACLs for the PBR policies.</p> <p>New/modified screens: Objects > Object Management > Access List > Extended > Add/Edit Extended Access List > Add/Edit Extended Access List Entry > Users and Security Group Tag</p> <p>See: Configure Extended ACL Objects</p>
VPN			
IPsec flow offload on the VTI loopback interface for the Secure Firewall 4200.	7.4.0	7.4.0	<p>On the Secure Firewall 4200, qualifying IPsec connections through the VTI loopback interface are offloaded by default. Previously, this feature was supported for physical interfaces on the Secure Firewall 3100.</p> <p>You can change the configuration using FlexConfig and the flow-offload-ipsec command.</p> <p>Other requirements: FPGA firmware 6.2+</p> <p>See: IPsec Flow Offload</p>
Crypto debugging enhancements for the Secure Firewall 4200.	7.4.0	7.4.0	<p>We made the following enhancements to crypto debugging:</p> <ul style="list-style-type: none"> • The crypto archive is now available in text and binary formats. • Additional SSL counters are available for debugging. • Remove stuck encrypt rules from the ASP table without rebooting the device. <p>New/modified CLI commands: show counters</p> <p>See: Troubleshooting Using Crypto Archives</p>

VPN: Remote Access

Feature	Minimum Management Center	Minimum Threat Defense	Details
Customize Secure Client messages, icons, images, and connect/disconnect scripts.	7.4.0	7.1.0	<p>You can now customize Secure Client and deploy these customizations to the VPN headend. The following are the supported Secure Client customizations:</p> <ul style="list-style-type: none"> • GUI text and messages • Icons and images • Scripts • Binaries • Customized Installer Transforms • Localized Installer Transforms <p>Threat defense distributes these customizations to the endpoint when an end user connects from the Secure Client.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Objects > Object Management > VPN > Secure Client Customization • Devices > Remote Access > Edit VPN policy > Advanced > Secure Client Customization <p>See: Customize Cisco Secure Client</p>
VPN: Site to Site			
Easily view IKE and IPsec session details for VPN nodes.	7.4.0	Any	<p>You can view the IKE and IPsec session details of VPN nodes in a user-friendly format in the Site-to-Site VPN dashboard.</p> <p>New/modified screens: Overview > Site to Site VPN > Under the Tunnel Status widget, hover over a topology, click View, and then click the CLI Details tab.</p> <p>See: Monitoring the Site-to-Site VPNs</p>
Site-to-site VPN information in connection events.	7.4.0	7.4.0 with Snort 3	<p>Connection events now contain three new fields: Encrypt Peer, Decrypt Peer, and VPN Action. For policy-based and route-based site-to-site VPN traffic, these fields indicate whether a connection was encrypted or decrypted (or both, for transiting connections), and who by.</p> <p>New/modified screens: Analysis > Connections > Events > Table View of Events</p> <p>See: Site to Site VPN Connection Event Monitoring</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
Easily exempt site-to-site VPN traffic from NAT translation.	7.4.0	Any	<p>We now make it easier to exempt site-to-site VPN traffic from NAT translation.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Enable NAT exemptions for an endpoint: Devices > VPN > Site To Site > Add/Edit Site to Site VPN > Add/Edit Endpoint > Exempt VPN traffic from network address translation • View NAT exempt rules for devices that do not have a NAT policy: Devices > NAT > NAT Exemptions • View NAT exempt rules for a single device: Devices > NAT > Threat Defense NAT Policy > NAT Exemptions <p>See: NAT Exemption</p>

Routing

Configure graceful restart for BGP on IPv6 networks.	7.4.0	7.3.0	<p>You can now configure BGP graceful restart for IPv6 networks on managed devices version 7.3 and later.</p> <p>New/modified screens: Devices > Device Management > Edit device > Routing > BGP > IPv6 > Neighbor > Add/Edit Neighbor.</p> <p>See: Configure BGP Neighbor Settings</p>
Virtual routing with dynamic VTI.	7.4.0	7.4.0	<p>You can now configure a virtual router with a dynamic VTI for a route-based site-to-site VPN.</p> <p>New/modified screens: Devices > Device Management > Edit Device > Routing > Virtual Router Properties > Dynamic VTI interfaces under Available Interfaces</p> <p>Platform restrictions: Supported only on native mode standalone or high availability devices. Not supported for container instances or clustered devices.</p> <p>See: About Virtual Routers and Dynamic VTI</p>

Access Control: Threat Detection and Application Identification

Feature	Minimum Management Center	Minimum Threat Defense	Details
Clientless zero-trust access.	7.4.0	7.4.0 with Snort 3	<p>We introduced Zero Trust Access that allows you to authenticate and authorize access to protected web based resources, applications, or data from inside (on-premises) or outside (remote) the network using an external SAML Identity Provider (IdP) policy.</p> <p>The configuration consists of a Zero Trust Application Policy (ZTAP), Application Group, and Applications.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Policies > Zero Trust Application • Analysis > Connections > Events • Overview > Dashboard > Zero Trust <p>New/modified CLI commands:</p> <ul style="list-style-type: none"> • show running-config zero-trust application • show running-config zero-trust application-group • show zero-trust sessions • show zero-trust statistics • show cluster zero-trust statistics • clear zero-trust sessions application • clear zero-trust sessions user • clear zero-trust statistics <p>See: Zero Trust Access</p>
Encrypted visibility engine enhancements.	7.4.0	7.4.0 with Snort 3	<p>Encrypted Visibility Engine (EVE) can now:</p> <ul style="list-style-type: none"> • Block malicious communications in encrypted traffic based on threat score. • Determine client applications based on EVE-detected processes. • Reassemble fragmented Client Hello packets for detection purposes. <p>New/modified screens: Use the access control policy's advanced settings to enable EVE and configure these settings.</p> <p>See: Encrypted Visibility Engine</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
Exempt specific networks and ports from bypassing or throttling elephant flows.	7.4.0	7.4.0 with Snort 3	<p>You can now exempt specific networks and ports from bypassing or throttling elephant flows.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • When you configure elephant flow detection in the access control policy's advanced settings, if you enable the Elephant Flow Remediation option, you can now click Add Rule and specify traffic that you want to exempt from bypass or throttling. • When the system detects an elephant flow that is exempted from bypass or throttling, it generates a mid-flow connection event with the reason Elephant Flow Exempted. <p>Platform restrictions: Not supported on the Firepower 2100 series.</p> <p>See: Elephant Flow Detection</p>
First-packet application identification using custom application detectors.	7.4.0	7.4.0 with Snort 3	<p>A new Lua detector API is now introduced, which maps the IP address, port, and protocol on the very first packet of a TCP session to application protocol (service AppID), client application (client AppID), and web application (payload AppID). This new Lua API <i>addHostFirstPktApp</i> is used for performance improvements, reinspection, and early detection of attacks in the traffic. To use this feature, you must upload the Lua detector by specifying the detection criteria in advanced detectors in your custom application detector.</p> <p>See: Custom Application Detectors</p>
Sensitive data detection and masking.	7.4.0	7.4.0 with Snort 3	<p>Upgrade impact. New rules in default policies take effect.</p> <p>Sensitive data such as social security numbers, credit card numbers, emails, and so on may be leaked onto the internet, intentionally or accidentally. Sensitive data detection is used to detect and generate events on possible sensitive data leakage and generates events only if there is a transfer of significant amount of Personally Identifiable Information (PII) data. Sensitive data detection can mask PII in the output of events, using built-in patterns.</p> <p>Disabling data masking is not supported.</p> <p>See: Custom Rules in Snort 3</p>
Improved JavaScript inspection.	7.4.0	7.4.0 with Snort 3	<p>We improved JavaScript inspection, which is done by normalizing the JavaScript and matching rules against the normalized content.</p> <p>See: HTTP Inspect Inspector and Cisco Secure Firewall Management Center Snort 3 Configuration Guide</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
MITRE information in file and malware events.	7.4.0	7.4.0	The system now includes MITRE information (from local malware analysis) in file and malware events. Previously, this information was only available for intrusion events. You can view MITRE information in both the classic and unified events views. Note that the MITRE column is hidden by default in both event views. See: Local Malware Analysis and File and Malware Event Fields
Smaller VDB for lower memory Snort 2 devices.	6.4.0.17 7.0.6 7.2.4 7.3.1.1 7.4.0	Any with Snort 2	Upgrade impact. Application identification on lower memory devices is affected. For VDB 363+, the system now installs a smaller VDB (also called <i>VDB lite</i>) on lower memory devices running Snort 2. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Lower memory devices: ASA 5506-X series, ASA-5508-X, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X Version restrictions: The ability to install a smaller VDB depends on the version of the management center, not managed devices. If you upgrade the management center from a supported version to an unsupported version, you cannot install VDB 363+ if your deployment includes even one lower memory device. For a list of affected releases, see CSCwd88641 . See: Update the Vulnerability Database
Access Control: Identity			
Cisco Secure Dynamic Attributes Connector on the management center.	7.4.0	Any	You can now configure the Cisco Secure Dynamic Attributes Connector on the management center. Previously, it was only available as a standalone application. See: Cisco Secure Dynamic Attributes Connector
Microsoft Azure AD as a user identity source.	7.4.0	7.4.0	You can use a Microsoft Azure Active Directory (Azure AD) realm with ISE to authenticate users and get user sessions for user control. New/modified screens: <ul style="list-style-type: none"> • Integration > Other Integrations > Realms > Add Realm > Azure AD • Integration > Other Integrations > Realms > Actions, such as downloading users, copying, editing, and deleting Supported ISE versions: 3.0 patch 5+, 3.1 (any patch level), 3.2 (any patch level) See: Create a Microsoft Azure Active Directory Realm
Event Logging and Analysis			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Configure threat defense devices as NetFlow exporters from the management center web interface.	7.4.0	Any	<p>Upgrade impact. Redo FlexConfigs after upgrade.</p> <p>NetFlow is a Cisco application that provides statistics on packets flows. You can now use the management center web interface to configure threat defense devices as NetFlow exporters. If you have an existing NetFlow FlexConfig and redo your configurations in the web interface, you cannot deploy until you remove the deprecated FlexConfigs.</p> <p>New/modified screens: Devices > Platform Settings > Threat Defense Settings Policy > NetFlow</p> <p>See: Configure NetFlow</p>
More information about "unknown" SSL actions in logged encrypted connections.	7.4.0	7.4.0	<p>Serviceability improvements to the event reporting and decryption rule matching.</p> <ul style="list-style-type: none"> • New SSL Status to indicate if the SSL handshake is not complete for an encrypted connection. The SSL Status column of the connection event displays “Unknown (Incomplete Handshake)” when the SSL handshake of the logged connection is not complete. • Subject Alternative Names (SANs) for certificates are now used when matching Certificate Authority (CA) names for improved decryption rule matching. <p>New/modified screens:</p> <ul style="list-style-type: none"> • Analysis > Connections > Events > SSL Status • Analysis > Connections > Security-Related Events > SSL Status <p>See: Connection and Security-Related Connection Event Fields.</p>
Health Monitoring			
Stream telemetry to an external server using OpenConfig.	7.4.0	7.4.0	<p>You can now send metrics and health monitoring information from your threat defense devices to an external server (gNMI collector) using OpenConfig. You can configure either threat defense or the collector to initiate the connection, which is encrypted by TLS.</p> <p>New/modified screens: System (⚙️) > Health > Policy > Firewall Threat Defense Policies > Settings > OpenConfig Streaming Telemetry</p> <p>See: Send Vendor-Neutral Telemetry Streams Using OpenConfig</p>
New asp drop metrics.	7.4.0	7.4.0	<p>You can add over 600 new asp (accelerated security path) drop metrics to a new or existing device health dashboard. Make sure you choose the ASP Drops metric group.</p> <p>New/modified screens: System (⚙️) > Health > Monitor > Device</p> <p>See: show asp drop Command Usage</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
Administration			
Send detailed management center audit logs to syslog.	7.4.0	Any	<p>You can stream configuration changes as part of audit log data to syslog by specifying the configuration data format and the hosts. The management center supports backup and restore of the audit configuration log.</p> <p>New/modified screens: System (⚙️) > Configuration > Audit Log > Send Configuration Changes</p> <p>See: Stream Audit Logs to Syslog</p>
Granular permissions for modifying access control policies and rules.	7.4.0	Any	<p>You can define custom user roles to differentiate between the intrusion configuration in access control policies and rules and the rest of the access control policy and rules. Using these permissions, you can separate the responsibilities of your network administration team and your intrusion administration teams.</p> <p>When defining user roles, you can select the Policies > Access Control > Access Control Policy > Modify Access Control Policy > Modify Threat Configuration option to allow the selection of intrusion policy, variable set, and file policy in a rule, the configuration of the advanced options for Network Analysis and Intrusion Policies, the configuration of the Security Intelligence policy for the access control policy, and intrusion actions in the policy default action. You can use the Modify Remaining Access Control Policy Configuration to control the ability to edit all other aspects of the policy. The existing pre-defined user roles that included the Modify Access Control Policy permission continue to support all sub-permissions; you need to create your own custom roles if you want to apply granular permissions.</p> <p>See: Create Custom User Roles</p>
Support for IPv6 URLs when checking certificate revocation.	7.4.0	7.4.0	<p>Previously, threat defense supported only IPv4 OCSP URLs. Now, threat defense supports both IPv4 and IPv6 OCSP URLs.</p> <p>See: Requiring Valid HTTPS Client Certificates and Certificate Enrollment Object Revocation Options</p>
Default NTP server updated.	7.4.0	Any	<p>The default NTP server for new management center deployments changed from sourcefire.pool.ntp.org to time.cisco.com. We recommend you use the management center to serve time to its own devices. You can update the management center's NTP server on System (⚙️) > Configuration > Time Synchronization.</p> <p>See: Internet Access Requirements</p>
Usability, Performance, and Troubleshooting			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Usability enhancements.	7.4.0	Any	<p>You can now:</p> <ul style="list-style-type: none"> • Manage Smart Licensing for threat defense clusters from System (⚙️) > Smart Licenses. Previously, you had to use the Device Management page. See: Licensing for Device Clusters • Download a report of Message Center notifications. In the Message Center, click the new Download Report icon, next to the Show Notifications slider. See: Managing System Messages • Download a report of all registered devices. On Devices > Device Management, click the new Download Device List Report link, at the top right of the page. See: Download the Managed Device List • Clone network and port objects. In the object manager (Objects > Object Management), click the new Clone icon next to a port or network object. You can then change the new object's properties and save it using a new name. See: Creating Network Objects and Creating Port Objects • Easily create custom health monitoring dashboards, and easily edit existing dashboards. See: Correlating Device Metrics
Specify the direction of traffic to be captured with packet capture for the Secure Firewall 4200.	7.4.0	7.4.0	<p>On the Secure Firewall 4200, you can use a new direction keyword with the capture command.</p> <p>New/modified CLI commands:</p> <pre>capture capture_nameswitchinterface interface_name [direction { both egress ingress }]</pre> <p>See: Cisco Secure Firewall Threat Defense Command Reference</p>
Snort 3 restarts when it becomes unresponsive, which can trigger HA failover.	7.4.0	7.4.0 with Snort 3	<p>To improve continuity of operations, an unresponsive Snort can now trigger high availability failover. This happens because Snort 3 now restarts if the process becomes unresponsive. Restarting the Snort process briefly interrupts traffic flow and inspection on the device, and in high availability deployments can trigger failover. (In a standalone deployment, interface configurations determine whether traffic drops or passes without inspection during the interruption.)</p> <p>This feature is enabled by default. You can use the CLI to disable it, or configure the time or number of unresponsive threads before Snort restarts.</p> <p>New/modified CLI commands: configure snort3-watchdog</p> <p>See: Cisco Secure Firewall Threat Defense Command Reference</p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cisco Success Network telemetry.	7.4.0	Any	For telemetry changes, see Cisco Success Network Telemetry Data Collected from Cisco Secure Firewall Management Center, Version 7.4.x .
Management Center REST API			
Management center REST API.	7.4.0	Any	For information on changes to the management center REST API, see What's New in Version 7.4 in the API quick start guide.
Deprecated Features			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Temporarily deprecated features.	7.4.0	Any	<p>Although upgrading to Version 7.4.0 is supported, the upgrade will remove critical features, fixes, and enhancements that may be included in your current version. Instead, upgrade to Version 7.4.1+.</p> <p>From Version 7.2.5–7.2.x, upgrading removes:</p> <ul style="list-style-type: none"> • Management center detects interface sync errors. Upgrade impact. <p>From Version 7.2.6–7.2.x, upgrading removes:</p> <ul style="list-style-type: none"> • Updated web analytics provider. Upgrade impact. • Configure DHCP relay trusted interfaces from the management center web interface. Upgrade impact. • Create network groups while editing NAT rules. • Single backup file for high availability management centers. • Open the packet tracer from the unified event viewer. • Health alerts for excessive disk space used by deployment history (rollback) files. Upgrade impact. • Health alerts for NTP sync issues. Upgrade impact. • View and generate reports on configuration changes since your last deployment. • Set the number of deployment history files to retain for device rollback. • Improved upgrade starting page and package management. • Enable revert from the threat defense upgrade wizard. • View detailed upgrade status from the threat defense upgrade wizard. • Suggested release notifications. • New upgrade wizard for the management center. • Hotfix high availability management centers without pausing synchronization. • Updated internet access requirements for direct-downloading software upgrades. Upgrade impact. • Scheduled tasks download patches and VDB updates only. Upgrade impact. • Enable/disable access control object optimization. • Cluster control link ping tool. • Set the frequency of Snort 3 core dumps. • Capture dropped packets with the Secure Firewall 3100/4200.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: NetFlow with FlexConfig.	7.4.0	Any	You can now configure threat defense devices as NetFlow exporters from the management center web interface. If you do this, you cannot deploy until you remove any deprecated FlexConfigs. See: Configure NetFlow

Device Manager Features in Version 7.4.x



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

Table 4: Device Manager Features in Version 7.4.x

Feature	Description
Platform Features	
Firepower 1010E support returns..	Support returns for the Firepower 1010E, which was introduced in Version 7.2.3 and temporarily deprecated in Version 7.3. See: Cabling for the Firepower 1010
Network modules for the Secure Firewall 3130 and 3140.	We introduced these network modules for the Secure Firewall 3130 and 3140: <ul style="list-style-type: none"> • 2-port 100G QSFP+ network module (FPR3K-XNM-2X100G) See: Cisco Secure Firewall 3110, 3120, 3130, and 3140 Hardware Installation Guide
VPN Features	
IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100.	Upgrade impact. Qualifying connections start being offloaded. On the Secure Firewall 3100, qualifying IPsec connections through the VTI loopback interface are now offloaded by default. Previously, this feature was only supported on physical interfaces. This feature is automatically enabled by the upgrade. You can change the configuration using FlexConfig and the flow-offload-ipsec command.
Interface Features	

Feature	Description
<p>Merged management and diagnostic interfaces.</p>	<p>Upgrade impact. Merge interfaces after upgrade.</p> <p>For new devices using 7.4 and later, you cannot use the legacy diagnostic interface. Only the merged management interface is available. If you upgraded to 7.4 or later, and you did not have any configuration for the diagnostic interface, then the interfaces will merge automatically.</p> <p>If you upgraded to 7.4 or later, and you have configuration for the diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate diagnostic interface. Note that support for the diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible.</p> <p>Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including management) in the configuration.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Devices > Interfaces > Management interface • (Moved to Interfaces) System Settings > Management Interface • Devices > Interfaces > Merge Interface action needed > Management Interface Merge <p>New/modified commands: show management-interface convergence</p>
<p>Deploy without the diagnostic interface on threat defense virtual for Azure and GCP.</p>	<p>You can now deploy without the diagnostic interface on threat defense virtual for Azure and GCP. Azure deployments still require at least two data interfaces, but GCP requires that you replace the diagnostic interface with a data interface, for a new minimum of three. (Previously, threat defense virtual deployments required one management, one diagnostic, and at least two data interfaces.)</p> <p>Restrictions: This feature is supported for new deployments only. It is not supported for upgraded devices.</p> <p>See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide</p>
<p>Inline sets for Firepower 1000 series, Firepower 2100, and Secure Firewall 3100.</p>	<p>You can configure inline sets on Firepower 1000 series, Firepower 2100, and Secure Firewall 3100 devices. We added the inline sets tab to the Interface page.</p>

Licensing Features

Feature	Description
Changes to license names and support for the Carrier license.	<p>Licenses have been renamed:</p> <ul style="list-style-type: none"> • Threat is now IPS • Malware is now Malware Defense • Base is now Essentials • AnyConnect Apex is now Secure Client Premier • AnyConnect Plus is now Secure Client Advantage • AnyConnect VPN Only is now Secure Client VPN Only <p>In addition, you can now apply the Carrier license, which allows you to configure GTP/GPRS, Diameter, SCTP, and M3UA inspections. Use FlexConfig to configure these features.</p> <p>See: Licensing the System</p>
Administrative and Troubleshooting Features	
Default NTP server updated.	<p>Upgrade impact. The system connects to new resources.</p> <p>The default NTP servers have changed from sourcefire.pool.ntp.org to time.cisco.com. To use a different NTP server, select Device, then click Time Services in the System Settings panel.</p>
SAML servers for HTTPS management user access.	<p>You can configure a SAML server to provide external authentication for HTTPS management access. You can configure external users with the following types of authorization access: Administrator, Audit Admin, Cryptographic Admin, Read-Write User, Read-Only User. You can use Common Access Card (CAC) for login when using a SAML server.</p> <p>We updated the SAML identity source object configuration, and the System Settings > Management Access page to accept them.</p>
Detect configuration mismatches in threat defense high availability pairs.	<p>You can now use the CLI to detect configuration mismatches in threat defense high availability pairs.</p> <p>New/modified CLI commands: show failover config-sync error, show failover config-sync stats</p> <p>See: Cisco Secure Firewall Threat Defense Command Reference</p>
Capture dropped packets with the Secure Firewall 3100.	<p>Packet losses resulting from MAC address table inconsistencies can impact your debugging capabilities. The Secure Firewall 3100 can now capture these dropped packets.</p> <p>New/modified CLI commands: [drop { disable mac-filter }] in the capture command.</p> <p>See: Cisco Secure Firewall Threat Defense Command Reference</p>

Feature	Description
Firmware upgrades included in FXOS upgrades.	<p>Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.</p> <p>For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1+ now include firmware upgrades. If any firmware component on the device is older than the one included in the FXOS bundle, the FXOS upgrade also updates the firmware. If the firmware is upgraded, the device reboots twice—once for FXOS and once for the firmware.</p> <p>Just as with software and operating system upgrades, do not make or deploy configuration changes during firmware upgrade. Even if the system appears inactive, do not manually reboot or shut down during firmware upgrade.</p> <p>See: Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide</p>
Quick recovery after data plane failure for the Firepower 1000/2100 and Firepower 4100/9300.	<p>When the data plane process on the Firepower 1000/2100 or the Firepower 4100/9300 crashes, the system reloads the process instead of rebooting the device. Reloading the data plane also restarts other processes, including Snort. If the data plane crashes during bootup, the device follows the normal reload/reboot sequence; this avoids a reload loop.</p> <p>This feature is enabled by default for both new and upgraded devices. To disable it, use FlexConfig.</p> <p>New/modified ASA CLI commands: data-plane quick-reload, show data-plane quick-reload status</p> <p>New/modified threat defense CLI commands: show data-plane quick-reload status</p> <p>Supported platforms: Firepower 1000/2100, Firepower 4100/9300</p> <p>See: Cisco Secure Firewall Threat Defense Command Reference and Cisco Secure Firewall ASA Series Command Reference.</p>

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; for example, if you must change a configuration.

Upgrade Impact Features for Management Center

Check all releases between your current and target version.

Table 5: Upgrade Impact Features for Management Center

Target Version	Features with Upgrade Impact
7.4.1+	<ul style="list-style-type: none"> • Configure DHCP relay trusted interfaces from the management center web interface. • Health alerts for excessive disk space used by deployment history (rollback) files. • Health alerts for NTP sync issues. • Updated internet access requirements for direct-downloading software upgrades. • Scheduled tasks download patches and VDB updates only. • Chassis-level health alerts for the Firepower 4100/9300. • Improved management center memory usage calculation, alerting, and swap memory monitoring. • Updated web analytics provider.
7.4.0+	<ul style="list-style-type: none"> • Smaller VDB for lower memory Snort 2 devices. • Configure threat defense devices as NetFlow exporters from the management center web interface. • Access control performance improvements (object optimization).
7.3.1.1–7.3.1.x	<ul style="list-style-type: none"> • Smaller VDB for lower memory Snort 2 devices.
7.3.0+	<ul style="list-style-type: none"> • Configure BFD for BGP from the management center web interface.
7.2.6–7.2.x	<ul style="list-style-type: none"> • Configure DHCP relay trusted interfaces from the management center web interface. • Health alerts for excessive disk space used by deployment history (rollback) files. • Health alerts for NTP sync issues. • Updated internet access requirements for direct-downloading software upgrades. • Scheduled tasks download patches and VDB updates only. • Updated web analytics provider.
7.2.5–7.2.x	<ul style="list-style-type: none"> • Management center detects interface sync errors.
7.2.4–7.2.x	<ul style="list-style-type: none"> • Automatically update CA bundles.
7.2.4–7.2.5	<ul style="list-style-type: none"> • Access control performance improvements (object optimization).
7.2.0+	<ul style="list-style-type: none"> • Configure VXLAN from the management center web interface. • Configure EIGRP from the management center web interface.
7.1.0.3–7.1.0.x	<ul style="list-style-type: none"> • Automatically update CA bundles.

Target Version	Features with Upgrade Impact
7.1.0+	<ul style="list-style-type: none"> • Configure Equal-Cost-Multi-Path (ECMP) from the FMC web interface. • Configure policy based routing from the FMC web interface. • Send intrusion events and retrospective malware events to the Secure Network Analytics cloud from the FMC. • Deprecated (temporary): Improved SecureX integration, SecureX orchestration. • Deprecated: Intrusion incidents and the intrusion event clipboard. • Deprecated: Custom tables for intrusion events.
7.0.6–7.0.x	<ul style="list-style-type: none"> • Updated web analytics provider. • Smaller VDB for lower memory Snort 2 devices.
7.0.5-7.0.x	<ul style="list-style-type: none"> • Automatically update CA bundles.
7.0.0+	<ul style="list-style-type: none"> • End of support: VMware vSphere/VMware ESXi 6.0. • Deprecated: Port 32137 comms with AMP clouds.
6.7.0+	<ul style="list-style-type: none"> • Changes to PAT address allocation in clustering. • pxGrid 2.0 with ISE/ISE-PIC. • Improved preclassification of files for dynamic analysis. • National Vulnerability Database (NVD) replaces Bugtraq. • Pre-upgrade compatibility check. • Upgrades postpone scheduled tasks. • Upgrades remove PCAP files to save disk space. • Deprecated: Cisco Firepower User Agent software and identity source. • Deprecated: Cisco ISE Endpoint Protection Services (EPS) remediation. • Deprecated: Less secure Diffie-Hellman groups, and encryption and hash algorithms. • Deprecated: Appliance Configuration Resource Utilization health module (temporary).

Upgrade Impact Features for Threat Defense with Management Center

Check all releases between your current and target version.

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

Target Version	Features with Upgrade Impact
7.4.1+	<ul style="list-style-type: none"> • 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+	<ul style="list-style-type: none"> • 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.
7.2.4–7.2.x	<ul style="list-style-type: none"> • Automatically update CA bundles.
7.2.0+	<ul style="list-style-type: none"> • Autoscale for threat defense virtual for GCP.
7.1.0.3–7.1.0.x	<ul style="list-style-type: none"> • Automatically update CA bundles.
7.1.0+	<ul style="list-style-type: none"> • Snort 3 support for inspection of DCE/RPC over SMB2. • Snort 3 support for <code>ssl_version</code> and <code>ssl_state</code> keywords.
7.0.5+	<ul style="list-style-type: none"> • Automatically update CA bundles.
7.0.0+	<ul style="list-style-type: none"> • End of support: VMware vSphere/VMware ESXi 6.0. • FTDv performance tiered Smart Licensing. • Deprecated: RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm. • Deprecated: MD5 authentication algorithm and DES encryption for SNMPv3 users.
6.7.0+	<ul style="list-style-type: none"> • Firepower 1100/2100 series SFP interfaces now support disabling auto-negotiation. • ClientHello modification for Decrypt - Known Key TLS/SSL rules. • Pre-upgrade compatibility check. • Improved readiness checks. • Improved FTD upgrade status reporting and cancel/retry options. • Upgrades remove PCAP files to save disk space.

Upgrade Impact Features for Threat Defense with Device Manager

Check all releases between your current and target version.

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

Target Version	Features with Upgrade Impact
7.4.1+	<ul style="list-style-type: none"> Merged management and diagnostic interfaces. IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100. Sensitive data detection and masking. Firmware upgrades included in FXOS upgrades. Default NTP server updated.
7.3.0+	<ul style="list-style-type: none"> TLS 1.3 support in SSL decryption policies, and configurable behavior for undecryptable connections. Combined upgrade and install package for Secure Firewall 3100. No support for Firepower 1010E (temporary).
7.2.4–7.2.x	<ul style="list-style-type: none"> Automatically update CA bundles.
7.1.0.3–7.1.0.x	<ul style="list-style-type: none"> Automatically update CA bundles.
7.1.0+	<ul style="list-style-type: none"> Dynamic Domain Name System (DDNS) support for updating fully-qualified domain name (FQDN) to IP address mappings for system interfaces. Snort 3 support for inspection of DCE/RPC over SMB2. Snort 3 support for <code>ssl_version</code> and <code>ssl_state</code> keywords.
7.0.6–7.0.x	<ul style="list-style-type: none"> Smaller VDB for lower memory devices with Snort 2.
7.0.5–7.0.x	<ul style="list-style-type: none"> Automatically update CA bundles.
7.0.0+	<ul style="list-style-type: none"> End of support: VMware vSphere/VMware ESXi 6.0. DHCP relay configuration using the threat defense API.
6.7.0+	<ul style="list-style-type: none"> Support removed for less secure Diffie-Hellman groups, and encryption and hash algorithms. EIGRP support using Smart CLI. Threat Defense API support for SNMP configuration.

Upgrade Guidelines

The following sections contain release-specific upgrade warnings and guidelines. You should also check for features and bugs with upgrade impact. For general information on time/disk space requirements and on system behavior during upgrade, see the upgrade guide: [For Assistance, on page 91](#).

Upgrade Guidelines for Management Center

Check all releases between your current and target version.

Table 8: Upgrade Guidelines for Management Center

Target Version	Current Version	Guideline	Details
7.4.1.x	7.4.1	Migration failure: do not migrate to management center Version 7.4.1 if you are using Security Intelligence.	<p>Patch the target management center to Version 7.4.1.1 before you begin migration. The source management center can continue to run Version 7.4.1.</p> <p>Note Version 7.4.1 is not supported on the Firepower Management Center 1000/2500/4500, even during the migration process. To migrate to Secure Firewall Management Center 1700/2700/4700, use Version 7.4.0.</p> <p>For more information on model migration, see the Cisco Secure Firewall Management Center Model Migration Guide.</p>
7.3.x–7.4.0	7.2.6–7.2.x	Upgrade not recommended: Version 7.2.6–7.2.x to Version 7.3.x–7.4.0.	Upgrading is supported, but will remove critical fixes and enhancements that are included in your current version. Instead, upgrade to Version 7.4.1+.
7.2.6	6.6.0–7.2.5	Upgrade not recommended: Version 7.2.6.	Due to CSCwi63113 , Version 7.2.6 was deferred on 2024-04-29 and is no longer available for download. If you downloaded it, do not use it. If you are running this version, upgrade.
7.1.0	7.0.4–7.0.x	Upgrade prohibited: Version 7.0.4+ to Version 7.1.0.	Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4–7.0.x to Version 7.1.0. Instead, upgrade to Version 7.2.0+.

Target Version	Current Version	Guideline	Details
7.0.0–7.2.x	6.4.0–6.7.x	Reconnect with Threat Grid for high availability management centers.	<p>Version 7.0.0 fixes an issue with management center high availability and malware detection where, after failover, the system stopped submitting files for dynamic analysis (CSCvu35704). For the fix to take effect, you must reassociate with the Cisco Threat Grid public cloud after upgrading.</p> <p>After you upgrade the high availability pair to Version 7.0.0+, on the primary management center:</p> <ol style="list-style-type: none"> 1. Choose AMP > Dynamic Analysis Connections. 2. Click Associate in the table row corresponding to the public cloud. A portal window opens. You do not have to sign in. The reassociation happens in the background, within a few minutes.
6.7.0	6.6.5–6.6.x	Upgrade prohibited: management center Version 6.6.5+ to Version 6.7.0.	Due to datastore incompatibilities, you cannot upgrade the management center from Version 6.6.5–6.6.x to Version 6.7.0. Instead, upgrade to Version 7.0.0+.

Upgrade Guidelines for Threat Defense with Device Manager

Check all releases between your current and target version.

Table 9: Upgrade Guidelines for Threat Defense with Device Manager

Target Version	Current Version	Guideline	Details
7.2.6	6.6.0–7.2.5	Upgrade not recommended: Version 7.2.6.	Due to CSCwi63113 , Version 7.2.6 was deferred on 2024-04-29 and is no longer available for download. If you downloaded it, do not use it. If you are running this version, upgrade.
7.1.0	7.0.4–7.0.x	Upgrade prohibited: Version 7.0.4+ to Version 7.1.0.	Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4+ to Version 7.1.0. Instead, upgrade to Version 7.2.0+.
6.7.0–7.2.x	6.4.0–6.6.x	Upgrade failure: Firepower 1010 switch ports with invalid VLAN IDs.	For the Firepower 1010, threat defense upgrades to Version 6.7+ will fail if you configured switch ports with a VLAN ID in the 3968–4047 range. These IDs are for internal use only.

Upgrade Guidelines for Threat Defense with Management Center

Check all releases between your current and target version.

Table 10: Upgrade Guidelines for Threat Defense with Management Center

Target Version	Current Version	Guideline	Details
7.4.1	7.1.x 7.0.0–7.0.2	Unregister and reregister devices after reverting threat defense.	If you revert from Version 7.4.1 to Version 7.0.0–7.0.2 or to Version 7.1.x, unregister and reregister devices after the revert completes (CSCwi31680).
7.3.x	7.2.6–7.2.x	Upgrade not recommended: Version 7.2.6–7.2.x to Version 7.3.x.	Upgrading is supported, but will remove critical fixes and enhancements that are included in your current version. Instead, upgrade to Version 7.4.1+.
7.3.x	7.1.x 6.7.0–7.0.2	Unregister and reregister devices after reverting threat defense.	If you revert from Version 7.3.x to Version 6.7.0–7.0.2 or to Version 7.1.x, unregister and reregister devices after the revert completes (CSCwi31680).
7.2.6	6.6.0–7.2.5	Upgrade not recommended: Version 7.2.6.	Due to CSCwi63113, Version 7.2.6 was deferred on 2024-04-29 and is no longer available for download. If you downloaded it, do not use it. If you are running this version, upgrade.
7.2.0+	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.
7.2.0–7.2.6	7.1.x 6.6.0–7.0.2	Unregister and reregister devices after reverting threat defense.	If you revert from Version 7.2.0–7.2.6 to Version 6.6.0–7.0.2 or to Version 7.1.x, unregister and reregister devices after the revert completes (CSCwi31680).
7.1.0	7.0.4–7.0.x	Upgrade prohibited: Version 7.0.4+ to Version 7.1.0.	Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4+ to Version 7.1.0. Instead, upgrade to Version 7.2.0+.
6.7.0–7.2.x	6.4.0–6.6.x	Upgrade failure: Firepower 1010 switch ports with invalid VLAN IDs.	For the Firepower 1010, threat defense upgrades to Version 6.7+ will fail if you configured switch ports with a VLAN ID in the 3968–4047 range. These IDs are for internal use only.

Upgrade Guidelines for the Firepower 4100/9300 Chassis

FXOS Upgrade Guidelines

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.

Table 11: Cisco Firepower 4100/9300 FXOS Release Notes

Target Threat Defense	Target FXOS	Release Notes
7.4	2.14	Cisco Firepower 4100/9300 FXOS Release Notes, 2.14(1)
7.3	2.13	Cisco Firepower 4100/9300 FXOS Release Notes, 2.13

Target Threat Defense	Target FXOS	Release Notes
7.2	2.12	Cisco Firepower 4100/9300 FXOS Release Notes, 2.12(1)
7.1	2.11	Cisco Firepower 4100/9300 FXOS Release Notes, 2.11(1)
7.0	2.10	Cisco Firepower 4100/9300 FXOS Release Notes, 2.10(1)
6.7	2.9	Cisco Firepower 4100/9300 FXOS Release Notes, 2.9(1)
6.6	2.8	Cisco Firepower 4100/9300 FXOS Release Notes, 2.8(1)

Firmware Upgrade Guidelines

For firmware upgrade guidelines, see the firmware upgrade guide: [Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide](#).

Upgrade Path

Planning your upgrade path is especially important for large high availability deployments, multi-hop upgrades, and situations where you need to coordinate related upgrades—operating systems, firmware, chassis, hosting environments, and so on.

Upgrade Path for Management Center

This table lists the minimum version to upgrade management center. The management center must run the same or newer version as its managed 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 you will need to perform a three (or more) step upgrade: devices first, then the management center, then devices again.

Table 12: Minimum Version to Upgrade Management Center

Target Version	Minimum Version to Upgrade	Oldest Device You Can Manage
7.4	7.0	7.0
7.3	7.0	6.7
7.2	6.6	6.6

Upgrade Path for Threat Defense

This table lists the minimum version to upgrade threat defense. If you are not running the minimum version, you will need to perform a multi-step upgrade. If a chassis upgrade is required, threat defense upgrade is blocked; see [Upgrade Path for Threat Defense with Chassis Upgrade, on page 47](#).

Table 13: Minimum Version to Upgrade Threat Defense

Target Version	Minimum Version to Upgrade
7.4	7.0

Target Version	Minimum Version to Upgrade
7.3	7.0
7.2	6.6

Upgrade Path for Threat Defense with Chassis Upgrade

You may need to upgrade the chassis (FXOS and firmware) before you upgrade threat defense. 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 you will need to perform a three (or more) step upgrade: devices first, then the chassis, then devices again. In high availability or clustered deployments, upgrade one chassis at a time.

This table lists the minimum versions to upgrade when a chassis upgrade is required (usually major upgrades). Chassis upgrades to FXOS 2.14.1+ include firmware, otherwise, see the [Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide](#).

Table 14: Minimum Versions to Upgrade the Firepower 4100/9300

Target Versions	Minimum Versions to Upgrade
Threat Defense 7.4.1 on FXOS 2.14.1.131+	Threat Defense 7.0 on FXOS 2.10
Threat Defense 7.3 on FXOS 2.13.0.198+	Threat Defense 7.0 on FXOS 2.10
Threat Defense 7.2 on FXOS 2.12.0.31+	Threat Defense 6.6 on FXOS 2.8

Bugs

This document lists open and resolved bugs for threat defense and management center Version 7.4. For bugs in earlier releases, see the release notes for those versions. For cloud-delivered Firewall Management Center bugs, see the [Cisco Cloud-Delivered Firewall Management Center Release Notes](#).



Important We do not list open bugs for most 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 7.4.0

Table last updated: 2023-09-11

Table 15: Open Bugs in Version 7.4.0

Bug ID	Headline
CSCwd87510	Deploy failure when flow export destinations are swapped or port value changed
CSCwe36422	IDP SAML missing filter in Zero Trust Policy shows all groups have missing IDP data
CSCwf93776	New User activity page does not display events for Special Identities Realm
CSCwh00002	Azure AD sessions do not get removed after disabling subscription or changing ise configuration
CSCwh04354	Importing a realm with a proxy will fail
CSCwh38213	Editing CSDAC dynamic attribute filter throwing Internal Error
CSCwh41164	OSPFv3 BFD sessions not coming up for more than 7
CSCwh45488	PBR configuration using User Identity is not migrated during FTD migration to cdFMC
CSCwh46657	Save button disabled when updating Zero Trust Policy
CSCwh49918	New SRU is not immediately installed upon management center upgrade
CSCwh50221	4200 Series: Portchannel in cluster may stay down sometimes when LACP is in active mode
CSCwh50259	EventHandler should not log warning if it fails to open a unified file when the file doesn't exist

Resolved Bugs in Version 7.4.1.1

Table last updated: 2024-04-24

Table 16: Resolved Bugs in Version 7.4.1.1

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

Bug ID	Headline
CSCwj14832	SAML: Single sign-on AnyConnect token verification failure is seen after successful authentication

Resolved Bugs in Version 7.4.1

Table last updated: 2023-12-13

Table 17: Resolved Bugs in Version 7.4.1

Bug ID	Headline
CSCvc06888	FMC should monitor only named interfaces on FTD
CSCvq48086	ASA concatenates syslog event to other syslog event while sending to the syslog server
CSCvu22491	FMC fails to connect to SSM with error "Failed to send the message to the server"
CSCvx44261	SNMPv3: Special characters used in FXOS SNMPv3 configuration causes authentication errors
CSCvy31169	deployment failing with - Unable to load container
CSCvy50598	BGP table not removing connected route when interface goes down
CSCvz03407	IPTables.conf file is disappearing resulting in backup and restore failure.
CSCvz22945	ERROR: Deleted IDB found in in-use queue - message misleading
CSCvz34289	In some cases transition to lightweight proxy doesn't work for Do Not Decrypt flows
CSCvz36903	ASA traceback and reload while allocating a new block for cluster keepalive packet
CSCvz71215	FMC is pushing SLA monitor commands in an incorrect order causing deployment failure.
CSCvz71596	"Number of interfaces on Active and Standby are not consistent" should trigger warning syslog
CSCwa36535	Standby unit failed to join failover due to large config size.
CSCwa53186	FTD with Inline TAP re-writes frame with wrong MAC Address leading to connectivity problems.
CSCwa59907	LINA observed traceback on thread name "snmp_client_callback_thread"
CSCwa70323	Unable to push extra domains >1024 Character, as part of Custom Attribute under Anyconnect VPN
CSCwa72528	user-name from certificate feature does not work with SER option
CSCwa72929	SNMPv3 polling may fail using privacy algorithms AES192/AES256
CSCwa74063	Disable NLP rules installation workaround after mgmt-access into NLP is enabled

Bug ID	Headline
CSCwa82791	ENH: Support for snapshots of RX queues on InternalData interfaces when "Blocks free curr" goes low
CSCwa82850	ASA Failover does not detect context mismatch before declaring joining node as "Standby ready"
CSCwa97917	ISA3000 in boot loop after powercycle
CSCwb00871	ENH: Reduce latency in log_handler_file to reduce watchdog under scale or stress
CSCwb04000	ASA/FTD: DF bit is being set on packets routed into VTI
CSCwb17963	Unable to identify dynamic rate limiting mechanism & not following msg limit per/sec at syslog server.
CSCwb31551	When inbound packet contains SGT header, FPR2100 cannot distribute properly per 5 tuple
CSCwb53172	FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated
CSCwb53328	ASA/FTD Traceback and reload caused by Smart Call Home process sch_dispatch_to_url
CSCwb66382	ASAv - 9344 Block not created automatically after enabling JumboFrames, breaks OSPF MD5
CSCwb73248	FW traceback in timer infra / netflow timer
CSCwb74571	PBR not working on ASA routed mode with zone-members
CSCwb79062	FMC GUI not displaying correct count of unused network objects
CSCwb79812	RIP is advertising all connected Anyconnect users and not matching route-map for redistribution
CSCwb83691	ASA/FTD traceback and reload due to the initiated capture from FMC
CSCwb87498	Lina traceback and reload during EIGRP route update processing.
CSCwb89963	ASA Traceback & reload in thread name: Datapath
CSCwb90532	ASA/FTD traceback and reload on NAT related function nat_policy_find_location
CSCwb92320	Network Object not visible after Flex migration and unable to save interface change in EIGRP->Setup
CSCwb92709	We can't monitor the interface via "snmpwalk" once interface is removed from context.
CSCwb93932	ASA/FTD failover pair traceback and reload due to connection replication race condition
CSCwb94190	ASA graceful shut down when applying ACL's with forward reference feature and FIPS enabled.
CSCwb94312	Unable to apply SSH settings to ASA version 9.16 or later

Bug ID	Headline
CSCwb95784	cache and dump last 20 rmu request response packets in case failures/delays while reading registers
CSCwb95850	Snort down due to missing lua files because of disabled application detectors (PM side)
CSCwb97251	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCwc02488	ASA/FTD may traceback and reload in Thread Name 'None'
CSCwc03069	Interface internal data0/0 is up/up from cli but up/down from SNMP polling
CSCwc03507	No-buffer drops on Internal Data interfaces despite little evidence of CPU hog
CSCwc05375	AnyConnect SAML - Client Certificate Prompt incorrectly appears within External Browser
CSCwc07262	Standby ASA goes to booting loop during configuration replication after upgrade to 9.16(3).
CSCwc08646	User without password prompted to change password when logged in from SSH Client
CSCwc09414	ASA/FTD may traceback and reload in Thread Name 'ci/console'
CSCwc10145	FTDv Cluster unit not re-joining cluster with error msg "Failed to open NLP SSL listening socket"
CSCwc10241	Temporary HA split-brain following upgrade or device reboot
CSCwc10483	ASA/FTD - Traceback in Thread Name: appAgent_subscribe_nd_thread
CSCwc11511	FTD: SNMP failures after upgrade to 7.0.2
CSCwc11597	ASA tracebacks after SFR was upgraded to 6.7.0.3
CSCwc11663	ASA traceback and reload when modifying DNS inspection policy via CSM or CLI
CSCwc12322	Digitally signed ASDM image verification error on FPR3100 platforms
CSCwc13017	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
CSCwc13994	ASA - Restore not remove the new configuration for an interface setup after backup
CSCwc18312	"show nat pool cluster" commands run within EEM scripts lead to traceback and reload
CSCwc18524	ASA/FTD Voltage information is missing in the command "show environment"
CSCwc23356	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-20-7695'
CSCwc23695	ASA/FTD can not parse UPN from SAN field of user's certificate
CSCwc24422	AC SSLVPN with Certificate Authentication and DAP failure if client's machine cert has empty subject

Bug ID	Headline
CSCwc24906	ASA/FTD traceback and reload on Thread id: 1637
CSCwc26648	ASA/FTD Traceback and Reload in Thread name Lina or Datatath
CSCwc27846	Traceback and Reload while HA sync after upgrading and reloading.
CSCwc28532	9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwc28684	MI hangs and not repsonding when FTD container instance is reloaded
CSCwc28806	ASA Traceback and Reload on process name Lina
CSCwc28854	Incorrect IF-MIB response when failover is configured on multiple contexts
CSCwc28928	ASA: SLA debugs not showing up on VTY sessions
CSCwc32246	NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used
CSCwc35583	Snort leaking file descriptors with each u2 file created
CSCwc36905	ASA traceback and reload due to "Heap memory corrupted at slib_malloc.c
CSCwc37256	SSL AnyConnect access blocked after upgrade
CSCwc40352	Lina Netflow sending permitted events to Stealthwatch but they are block by snort afterwards
CSCwc40381	ASA : HTTPS traffic authentication issue with Cut-through Proxy enabled
CSCwc44289	FTD - Traceback and reload when performing IPv4 & IPv6 NAT translations
CSCwc45108	ASA/FTD: GTP inspection causing 9344 sized blocks leak
CSCwc45397	ASA HA - Restore in primary not remove new interface configuration done after backup
CSCwc45575	ASA/FTD traceback and reload when ssh using username with nopassword keyword
CSCwc48375	Inbound IPSEC SA stuck inactive - many inbound SPIs for one outbound SPI in "show crypto ipsec sa"
CSCwc49095	ASA/FTD 2100 platform traceback and reload when fragments are coalesced and sent to PDTS
CSCwc50887	FTD - Traceback and reload on NAT IPv4&IPv6 for UDP flow redirected over CCL link
CSCwc50891	MPLS tagging removed by FTD
CSCwc51326	FXOS-based Firepower platform showing 'no buffer' drops despite high values for RX ring watermarks

Bug ID	Headline
CSCwc52351	ASA/FTD Cluster Split Brain due to NAT with "any" and Global IP/range matching broadcast IP
CSCwc53280	ASA parser accepts incomplete network statement under OSPF process and is present in show run
CSCwc54217	syslog related to failover is not outputted in FPR2140
CSCwc54984	IKEv2 rekey - Responding Invalid SPI for the new SPI received right after Create_Child_SA response
CSCwc60037	ASA fails to rekey with IPSEC ERROR: Failed to allocate an outbound hardware context
CSCwc61912	ASA/FTD OSPFv3 does not generate messages Type 8 LSA for IPv6
CSCwc66757	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwc67031	vti hub with NAT-T enabled pinholes connections are looping and causing snort busy drops
CSCwc67886	ASA/FTD may traceback and reload in Thread Name 'lina_inotify_file_monitor_thread'
CSCwc70962	FTD/ASA "Write Standby" enables ECDSA ciphers causing AC SSLv3 handshake failure
CSCwc72155	ASA/FTD Traceback and reload on function "snp_cluster_trans_allocb"
CSCwc72284	TACACS Accounting includes an incorrect IPv6 address of the client
CSCwc73224	Call home configuration on standby device is lost after reload
CSCwc74103	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-11-32591'
CSCwc74858	FTD - Traceback in Thread Name: DATAPATH
CSCwc77680	FTD may traceback and reload in Thread Name 'DATAPATH-0-4948'
CSCwc77892	CGroups errors in ASA syslog after startup
CSCwc78781	ASA/FTD may traceback and reload during ACL changes linked to PBR config
CSCwc79366	During the deployment time, device got stuck processing the config request.
CSCwc80234	"inspect snmp" config difference between active and standby
CSCwc81184	ASA/FTD traceback and reload caused by SNMP process failure
CSCwc81945	Traffic on data unit gets dropped with "LU allocate xlate failed" on GCP cluster with interface NAT
CSCwc81960	Unable to configure 'match ip address' under route-map when using object-group in access list

Bug ID	Headline
CSCwc82188	FTD Traceback and reload when applying long commands from FMC UI or CLISH
CSCwc83346	ASA/FTD Traceback and reload in Threadname: IKE Daemon
CSCwc88897	ASA traceback and reload due to null pointer in Umbrella after modifying DNS inspection policy
CSCwc90091	ASA 9.12(4)47 with user-statistics, will affects the "policy-server xxxx global" visibility.
CSCwc93166	Using write standby in a user context leaves secondary firewall license status in an invalid state
CSCwc94085	Unable to establish DTLSv1.2 with FIPS enabled after upgrade from 6.6.5.
CSCwc94501	ASA/FTD memory leak and tracebacks due to ctm_n5 resets
CSCwc94547	Lina Traceback and reload when issuing 'debug menu fxos_parser 4'
CSCwc95290	ESP rule missing in vpn-context may cause IPSec traffic drop
CSCwc96805	traceback and reload due to tcp intercept stat in thread unicorn
CSCwc99242	ISA3000 LACP channel member SFP port suspended after reload
CSCwd00386	ASA/FTD may traceback and reload when clearing the configuration due to "snp_clear_acl_log_flow_all"
CSCwd00778	ifAdminStatus output is abnormal via snmp polling
CSCwd02864	logging/syslog is impacted by SNMP traps and logging history
CSCwd03793	FTD Traceback and reload
CSCwd03810	ASA Custom login page is not working through webvpn after an upgrade
CSCwd04135	Snort3 unexpectedly dropping packets after 4MB when using file inspection with detection mode NAP
CSCwd04436	User/group download may fail if a different realm is changed and saved
CSCwd04494	Unable to add on-board and netmod interfaces to the same port-channel on Firepower 3110
CSCwd05756	FTD traceback on Lina due to syslog component.
CSCwd06005	ASA/FTD Cluster Traceback and Reload during node leave
CSCwd07098	25G CU SFPs not working in Brentwood 8x25G netmod
CSCwd08098	ca-cert.pem on FMC expired and all the devices showing as disabled.
CSCwd10822	Failover trigger due to Inspection engine in other unit has failed due to disk failure

Bug ID	Headline
CSCwd11303	ASA might generate traceback in ikev2 process and reload
CSCwd11855	ASA/FTD may traceback and reload in Thread Name 'ikev2_fo_event'
CSCwd14972	ASA/FTD Traceback and Reload in Thread Name: pix_flash_config_thread
CSCwd16294	GTP inspection drops packets for optional IE Header Length being too short
CSCwd16689	ASA/FTD traceback due to block data corruption
CSCwd20627	ASA/FTD: NAT configuration deployment failure
CSCwd22349	ASA: Unable to connect AnyConnect Cert based Auth with "periodic-authentication certificate" enabled
CSCwd22907	ASA/FTD High CPU in SNMP Notify Thread
CSCwd23913	FTD in HA traceback multiple times after adding a BGP neighbour with prefix list.
CSCwd25201	ASA/FTD SNMP traps enqueued when no SNMP trap server configured
CSCwd25256	ASA/FTD Transactional Commit may result in mismatched rules and traffic loss
CSCwd26867	Device should not move to Active state once Reboot is triggered
CSCwd28037	TPK: No nameif during traffic causes the device traceback, lina core is generated.
CSCwd31181	Lina traceback and reload - VPN parent channel (SAL) has an invalid underlying channel
CSCwd31806	ASAv show crashinfo printing in loop continuously
CSCwd31960	Management access over VPN not working when custom NAT is configured
CSCwd33811	Cluster registration is failing because DATA_NODE isn't joining the cluster
CSCwd33962	3130 HA assert: mh->mh_mem_pool & MEMPOOL_UNDEFINED && mh->mh_mem_pool & MEMPOOL_MAX_TYPE
CSCwd34079	FTD: Traceback & reload in process name lina
CSCwd38583	ASA/FTD: Command "no snmp-server enable oid mempool" enabled by default or enforced during upgrades
CSCwd38805	Syslog 106016 is not rate-limited by default
CSCwd40260	Serviceability Enhancement - Unable to parse payload are silently drop by ASA/FTD
CSCwd41083	ASA traceback and reload due to DNS inspection
CSCwd41553	PIM register packets are not sent to Rendezvous Point (RP) due to PIM tunnel interface down state

Bug ID	Headline
CSCwd43622	Blade remains online for more than 600 secs after deleting Native logical device on 92.14.0
CSCwd45451	FMC: Script to change hostname/IP on FTD's when FMC's Ip/hostname is changed
CSCwd49402	Not able to ping Virtual IP of FTDv cluster
CSCwd54360	FP2100: FXOS side changes for HA is not resilient to unexpected lacp process termination issue
CSCwd66822	FDM FPR2k Network module interfaces are greyed out post 7.1.0 update
CSCwd68745	QEMU KVM console got stuck in "Booting the kernel" page
CSCwd73020	Fix Bootup Warning: Counter ID 'TLS13_DOWNSTREAM_CLIENT_CERTIFICATE_VERIFY' is too long
CSCwd79150	Device API healthStatus for cluster devices not aligned with health status on device listing
CSCwd85073	Snort3 stream core found init_tcp_packet_analysis
CSCwd89095	Stratix5950 and ISA3000 LACP channel member SFP port suspended after reload
CSCwd98070	Unable to register new devices to buildout FMC 2700 (FMC HA Active)
CSCwe04043	FTD-HA upgrade failed
CSCwe10872	Internal Error while editing PPPoE configurations
CSCwe12705	multimode-tmatch_df_hijack_walk traceback observed during shut/unshut on FO connected switch interfa
CSCwe15924	FMC-HA Sync loss for more then hr due to MariaDB replication is not in good state and recovered
CSCwe21301	Azure FMC not accessible after upgrading from 7.3.0 to 7.4.0
CSCwe25025	8x10Gb netmod fails to come online
CSCwe25342	ASA/FTD - SNMP related memory leak behavior when snmp-server is not configured
CSCwe25412	Azure D5v2 FTDv unable to send traffic - underruns and deplete DPDK buffers observed
CSCwe28912	FPR 4115- primary unit lost all HA config after ftd HA upgrade
CSCwe30359	Traffic drops for several minutes during deployment
CSCwe33282	FTD: The upgrade was unsuccessful because the httpd process was not running
CSCwe34664	The interface is deleted from interface group if the user change the name of it [API]

Bug ID	Headline
CSCwe37941	v1_message* and abp* files & sxp bookmark are not cleaned in user_enforcement on device registration
CSCwe38601	FMC search error: "Error Loading Data Search Service Please Try Again."
CSCwe38640	EventHandler warnings if syslog facility is CONSOLE
CSCwe41766	FTD may not reboot as expect post upgrade if bundled FXOS version is the same on old and new version
CSCwe42061	Deleting a BVI in FTD interfaces is causing packet drops in other BVIs
CSCwe42236	FMC: Domain creation fails with error "Index 'netmap_num' for table 'domain_control_info'"
CSCwe44571	FMC: GEOLOCATION size is causing upgrade failures
CSCwe45569	FTD upgrade from 7.0 to 7.2.x and beyond crashes due to management-access enabled
CSCwe48997	Cannot create two RA-VPN profiles with different SAML servers that have the same IDPâ€
CSCwe55308	Memory leak in the MessageService
CSCwe58635	Readiness Check Failed [ERROR] Fatal error: Enterprise Object integrity check failed with 7 errors
CSCwe58700	ASA/FTD: Revision of cluster event message "Health check detected that control left cluster"
CSCwe59889	Create Identity Services Engine via API returns 404 Client Error: Not Found
CSCwe63759	Cluster hardening fixes
CSCwe65492	KP Generating invalid core files which cannot be decoded 7.2.4-64
CSCwe65516	show xlate does not display xlate entries for internal interfaces (nlp_int_tap) after enabling ssh.
CSCwe67180	FTD HA app-sync failure, due to corruption in cache files.
CSCwe68840	add syslog ids the range 805003 ? 852002 for rate limit under fmc
CSCwe69824	validation check on FMC GUI causing issue and throwing error when adding new NAT objects
CSCwe70378	Connections not replicated to Standby FTD
CSCwe71220	FTD Crash in Thead Name: CP Processing
CSCwe73933	SNMPv3 polling may fail using privacy algorithms AES192/AES256
CSCwe75267	Cannot Force Break FTD HA Pair

Bug ID	Headline
CSCwe78674	User Group Download fetches less data than available or fails with "Size limit exceeded" error
CSCwe80273	FMC device search page removes FTD from the groups and put them back to ungrouped
CSCwe82704	PortChannel sub-interfaces configured as data/data-sharing, in multi-instance HA go into "waiting"
CSCwe83255	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe84079	asa_snmp.log is not rotated, resulting in large file size
CSCwe84695	FMC/FTD Dynamic VPN. Possibility to choose default preshared key from the dropdown list.
CSCwe85156	FTD: 10Gbps/full interfaces changed to 1Gbps/Auto after upgrade and going to down state
CSCwe87134	Lina core created during high traffic testing
CSCwe88802	FTD readiness and upgrade passed with exception log as ProgressReport' has no attribute 'KB_UNIT'
CSCwe90168	Unable to Access FMC GUI when using Certificate Authentication
CSCwe92723	Phase 2 NAP delay seen in 7.0.1 while deploying policy
CSCwe93137	KP - multimode: ASA traceback observed during HA node break and rejoin.
CSCwe97277	Observed ASA traceback and reload when performing hitless upgrade while VPN traffic running
CSCwe98435	Selective policy deploy with Identity Policy (captive-portal) and SSL Policy (dp-tcp-proxy) CLI
CSCwf00804	EventHandler occasional corrupt bundle record - SFDataCorrelator logs "Error deserializing"
CSCwf05295	FTD running on FP1000 series might drop packets on TLS flows after the "Client Hello" message.
CSCwf08790	FMC Restore of remote backup fails due to no space left on the device
CSCwf13674	Deployments can cause certain RAVPN users mapping to get removed.
CSCwf14031	Snort down due to missing lua files because of disabled application detectors (VDB side)
CSCwf14411	getting wrong destination zone on traffic causing traffic to match wrong AC rule
CSCwf15863	Very specific "vpn-idle-timeout" values cause continuous SSL session disconnects and reconnects

Bug ID	Headline
CSCwf16559	getReadinessStatusTaskList pjb request is very frequent when user in Upgrade sensor list page
CSCwf16679	HA Serviceability Enh: Maintain HA NLP client stats and HA CTL NLP counters for current App-sync
CSCwf17042	ASDM replaces custom policy-map with default map on class inspect options at backup restore.
CSCwf19621	Unable to edit name or inspection mode of intrusion policy
CSCwf21204	DBCheck shouldn't run against MonetDB if user is collecting config backup alone
CSCwf22045	MYSQL, or any TCP high traffic, getting blocked by snort3, with snort-block as Drop-reason
CSCwf22637	Network Object Group overrides not visible or be edited from FMC GUI
CSCwf24818	Unable to change admin user password after FMC migration if it had LOM access
CSCwf25402	FMC - Import SSL Certificate Pinning from a CSV file may result in a failure to deploy policy on FTD
CSCwf25563	Device list takes longer to load while creating new AC policy
CSCwf25642	High Disk Utilization and Performance issue due to large MariaDB Undo Logs
CSCwf26350	User is not informed of the dependent IPS when policy import fails.
CSCwf27337	KP: Cleanup/Reformat the second (MSP) disk on FTD reinstall
CSCwf31050	[IMS_7_5_MAIN]High CPU usage on multiple appliances
CSCwf35573	Traffic may be impacted if TLS Server Identity probe timeout is too long
CSCwf36563	The interface configuration is missing after the FTD upgrade
CSCwf36621	access-list: Cannot mix different types of access lists.
CSCwf39163	ASAv - High latency is experienced on Azure environment for ICMP ping packets while running snmpwalk
CSCwf39821	FTD: High-Availability unit struck at CD App Sync error due to error ngfwManager restart on peer
CSCwf41187	WINSCP and SFTP detectors do not work as expected
CSCwf41433	ASA/FTD client IP missing from TACACS+ request in SSH authentication
CSCwf42012	Improper load-balancing for traffic on ERSPAN interfaces on FPR 3100/4200
CSCwf42097	PSEQ (Power-Sequencer) firmware may not be upgraded with bundled FXOS upgrade
CSCwf42234	S2S dashboard SVTI tunnel details are missing after upgrade

Bug ID	Headline
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
CSCwf45091	Snort3 matches SMTP_RESPONSE_OVERFLOW (IPS rule 124:3) when SMTPS hosts exchange certificates
CSCwf47227	Priority-queue command causes silent egress packet drops on all port-channel interfaces
CSCwf49486	store_*list_history.pl task is created every 5min without getting closed causing FMC slowness.
CSCwf50497	DNS cache entry exhaustion leads to traceback
CSCwf52810	ASA SNMP polling not working and showing "Unable to honour this request now" on show commands
CSCwf54510	ASA traceback and reload on Thread Name: DHCPRA Monitor
CSCwf55236	Unable to delete custom rule group even when excluded from all the ips policies
CSCwf56386	vFTD runs out of memory and goes to failed state
CSCwf56811	ASA Traceback & reload on process name lina due to memory header validation
CSCwf59643	FTD: HA App sync failure due to fover interface flap on standby unit
CSCwf60590	"show route all summary" executed on transparent mode FTD is causing CLISH to become Sluggish.
CSCwf62820	Failover: standby unit traceback and reload during modifying access-lists
CSCwf63358	FTD Diskmanager.log is corrupt causing hm_du module to alert false high disk usage
CSCwf63872	FTD taking longer than expected to form OSPF adjacencies after a failover switchover
CSCwf64590	Units get kicked out of the cluster randomly due to HB miss ASA 9.16.3.220
CSCwf68335	vFMC: Scheduled deployment failing
CSCwf69313	Correlation events for Connection Tracker <, <=, or != rules show data for unrelated connections
CSCwf69880	FP3110 7.2.4 Unexpected reboot of Firepower 3110 Device
CSCwf69901	FTD: Traceback and reload during OSPF redistribution process execution
CSCwf71602	FMC not generating FTD S2S VPN alerts when down or idle
CSCwf72434	Add meaningful logs when the maximums system limit rules are hit
CSCwf73773	Dumping of last 20 rmu request response packets failed

Bug ID	Headline
CSCwf75214	ASA removes the IKEv2 Remote PSK if the Key String ends with a backslash "\" after reload
CSCwf75695	Duplicate FTD cluster has been created when multiple cluster events comes at same time
CSCwf76945	Packet data is still dropped after upgrade
CSCwf77994	False critical high CPU alerts for FTD device system cores running diskmanager/Pruner
CSCwf78321	ASA: Checkheaps traceback and reload due to Clientless WebVPN
CSCwf79372	after HA break, selected list shows both the devices when 1 device selected for upgrade
CSCwf80163	Critical Alert Smart Agent is not registered with Smart Licensing Cloud
CSCwf80183	Snort3 core in navl seen during traffic flow
CSCwf82279	Excessive logging of ssp-multi-instance-mode messages to /opt/cisco/platform/logs/messages
CSCwf82447	Editing identity nat rule disables "perform route lookup" silently
CSCwf82742	FTD: SNMP not working on management interface
CSCwf82970	Snort2 engine is crashing after enabling TLS Server Identity Discovery feature
CSCwf84200	Snort core while running IP Flow Statistics
CSCwf86519	FMC displays VPN status as unknown even if the status is up if one of the peer is extranet
CSCwf86557	Decrypting engine/ssl connections hang with PKI Interface Error seen
CSCwf87070	WM RM - SFP port status of 9 follows port of state of SFP 10 11 12
CSCwf88030	FMC pushes the "shutdown" command on the management interface for the logical device
CSCwf88124	switch ports in Trunk mode do not pass vlan traffic after power loss
CSCwf89959	ASA: ISA3000 does not respond to entPhySensorValue OID SNMP polls
CSCwf91282	import of .SFO to FMC failed due to included local/custom rules having a blank rule message field
CSCwf92135	ASA: Traceback and reload on Tread name "fover_FSM_thread" and ha_ntfy_prog_process_timer
CSCwf92646	ECDSA Self-signed certificate using SHA384 for EC521
CSCwf92661	ASA FTD: Traceback & reload due to a free buffer corruption
CSCwf92726	LDAP missing files after upgrade when the Vault token is corrupted

Bug ID	Headline
CSCwf94194	FMC: Should not be able to add the same interface to the same ECMP zone
CSCwf94450	FTD Lina traceback Thread Name: DATAPATH-3-11917 due to double free
CSCwf94677	"failover standby config-lock" config is lost after both HA units are reloaded simultaneously
CSCwf95147	OSPFv3 Traffic is Centralized in Transparent Mode
CSCwf96938	FMC: ACP Rule with UDP port 6081 is getting removed after subsequent deployment
CSCwh01673	FTD /ngfw disk space full from Snort3 url db files
CSCwh02457	Radius authentication stopped working after ASA v on AWS upgrade to any higher version than 9.18.2
CSCwh02561	Port-channel interface speed changes from 10G to 1G after a policy deployment
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 OSCP request if non-default port begins with 80
CSCwh06452	Interface speed mismatch in SNMP response using OID .1.3.6.1.2.1.2.2
CSCwh08481	ASA traceback on Lina process with FREEB and VPN functions
CSCwh08683	FTDv/AWS - NTP clock offset between Lina and FTD cluster
CSCwh09968	ASA/FTD: Traceback and reload due to NAT change and DVTI in use
CSCwh10087	core-compressor fails due to core filename with white space
CSCwh11411	Snort blacklisting traffic during deployment
CSCwh11764	ASA/FTD may traceback and reload in Thread Name "RAND_DRBG_bytes" and CTM function on n5 platforms
CSCwh13625	Encrypted Visibility Engine (EVE) FMC dashboard tab and widgets not renamed after 7.1 > 7.2+ upgrade
CSCwh13821	ASA/FTD may traceback and reload in when changing capture buffer size
CSCwh14467	File sizes bigger than 100MB for AnyConnect/Secure Client images cannot be uploaded on FMC
CSCwh14863	FTD 7.0.4 cluster drops Oracle's sqlnet packets due to tcp-not-syn

Bug ID	Headline
CSCwh15109	SRU installation gets stuck at 602_log_package.pl script, causing deployment failure
CSCwh15223	Lina crash in snp_fp_tcp_normalizer() when DAQ/Snort sends malformed L3 header
CSCwh16301	Incorrect Hit count statistics on ASA Cluster only for Cluster-wide output
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
CSCwh21141	The FMC preview deployment shows a wrong information.
CSCwh21360	741 - HA & AppAgent - Long term solution for avoiding momentary split-brain situations
CSCwh21420	ASA unexpected HA failover due to MIO blade heartbeat failure
CSCwh21474	ASA traceback when re-configuring access-list
CSCwh22348	sfdatacorrelator crashing due to table corruption 'rua_event_xxxxx'
CSCwh23567	PAC Key file missing on standby on reload
CSCwh24826	FMC upgrade stuck at 1039_fmc_rabbitmq_enable
CSCwh24901	'Frequent drain of events (not unprocessed events) to be removed from FMC
CSCwh25351	FTD VMWare: High disk utilization on /dev/sda8 partition caused by file system corruption
CSCwh25928	FMC userrole missing permissions may cause Tomcat to continuously restart after upgrade to 7.2.4
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.
CSCwh28007	While editing AC-policy rules, the rule order number becomes misaligned.
CSCwh28144	Specific OID 1.3.6.1.2.1.25 should not be responding
CSCwh28185	dl_task.pl tasks keep getting created every hour when a database query is blocked
CSCwh28206	Firewall Blocking packets after failover due to IP <-> SGT mappings
CSCwh28218	Syslog not updating when prefilter rule name changes
CSCwh29092	FTD (FDM) fails when executing script 800_post/100_ftd_onbox_data_import.sh
CSCwh30111	FTD - Upgrade triggers persistent VPN Tunnel health monitor alarm

Bug ID	Headline
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
CSCwh32118	ASDM management-sessions quota reached due to HTTP sessions stuck in CLOSE_WAIT
CSCwh34344	FTD not generating end of connection event after "Deleting Firewall session"
CSCwh36167	DAP: FMC adds  characters in a LUA script
CSCwh37475	Removal of msie-proxy commands during flexconfig rollback
CSCwh37733	FTD responding to UDP500 packet with a Mac Address of 0000.000.000
CSCwh37737	FMC7.2.x EIGRP flexconfig migration fails with internal error due to interface config mismatch
CSCwh38492	FMC Restore is stuck in vault clear stage after mysql restore completed
CSCwh38708	ASA "pager line 25" command doesn't work as expected on few terminal applications
CSCwh40106	FTD hosted on KP incorrectly dropping decoded ESP packets if pre-filter action is analyze
CSCwh41127	ASA/FTD: NAT64 error "overlaps with inside standby interface address" for Standalone ASA
CSCwh42077	Cisco_Firepower_GEODB_FMC_Update* are not included in diskmanager
CSCwh42412	FTD Block 9344 leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwh44479	Configuration archive creation failing and causing deployment preview to throw error
CSCwh45450	2100: Interfaces missing from FTD after removing interfaces as members of a port-channel
CSCwh47395	Extended Access List Object does not allow IP range configuration
CSCwh47701	ASA allows same BGP Dynamic routing process for Physical Data and management-only interfaces
CSCwh48844	FTD: Failover/High Availability disabled with Mate version 0.0 is not compatible
CSCwh49244	"show aaa-server" command always shows the Average round trip time 0ms.
CSCwh49483	ASA/FTD may traceback and reload while running show inventory all
CSCwh52420	AMP Cloud look up timeout frequently.
CSCwh52526	FMC SSO timesout when user session is active for more than 1 hr (idle timeout)

Bug ID	Headline
CSCwh53116	Initiator Country and Continent missing on Custom View on Event viewer
CSCwh53143	ASA:Management access via IPSec tunnel is NOT working
CSCwh54228	FMC: query_engine.log Growing More Quickly Than Expected, Resulting In High Disk Utilization
CSCwh54477	The FMC is showing "The password encryption key has not been set" alert for a 11xx/21xx/31xx device
CSCwh56218	ASA: Traceback and reload during 6 nodes cluster synchronization after CCL link failure/recovery
CSCwh56945	SFDataCorrelator crashing repeatedly in RNA_DB_InsertServiceInfo
CSCwh58999	Devices with classic licenses are failed to register with FMC running version 7.2.X
CSCwh59199	ASA/FTD traceback and reload with IPSec VPN, possibly involving upgrade
CSCwh59222	SNORT3 - FTD - TSID high cpu, daq polling when ssl enabled is not pulling enough packets
CSCwh59557	Source NAT Rule performing incorrect translation due to interface overload
CSCwh60604	ASA/FTD may traceback and reload in Thread Name 'lina' while processing DAP data
CSCwh60608	VPN Load Balancing Cluster IP address/host name is not on the same subnet as the public interface
CSCwh60631	Fragmented UDP packet via MPLS tunnel reassemble fail
CSCwh61690	Multicast through the box traffic causing high CPU with 1GBps traffic
CSCwh62080	additional command outputs needed in FTD troubleshoot for blocks and ssl cache
CSCwh62473	FMC HA: When logging into the standby FMC stacktraces are always present.
CSCwh63588	FTD SNMPv3 host configuration gets deleted from IPTABLES after adding host-group configuration
CSCwh63663	Cannot use .k12 domain on realm AD Primary Domain configuration
CSCwh64508	Fixing the regression caused while handling web UI is not getting FTDv Variable
CSCwh66359	ASDM can not see log timestamp after enable logging timestamp on cli
CSCwh66636	Configuring and unconfiguring "match ip address test" may lead to crash
CSCwh66991	sshd restarting during upgrade leading to have /new-root as default root partition
CSCwh68856	Configuration to disable TLS1.3
CSCwh68878	Diskmanager process terminated unexpectedly

Bug ID	Headline
CSCwh69209	Prefilter cannot add Tunnel Endpoints in Tunnel Rule on FMC
CSCwh69346	ASA: Traceback and reload when restore configuration using CLI
CSCwh69815	FTDs through put got changed to 100Kbps after upgrade
CSCwh70323	Timestamp entry missing for some syslog messages sent to syslog server
CSCwh70481	Community string sent from router is not matching ASA
CSCwh70628	spin lock and watch dog crash in kp 741-1146 - ctm_ipsec_get_sa_lock+112
CSCwh70905	Secondary lost failover communication on Inside, using IPv6, but next testing of Inside passes
CSCwh71050	FXOS : Duplication of NTP entry results in Error message : Unreachable Or Invalid Ntp Server
CSCwh71358	Unable to create VRF via FDM in Firepower 3105 device
CSCwh73727	Snort3 dropping IP protocol 51
CSCwh74870	Unexpected high values for DAQ outstanding counter
CSCwh76959	FMC does not save changes made on access list.
CSCwh77348	ASA: Traceback and reload when executing the command "show nat pool detail" on a cluster setup
CSCwh77527	FMC should report user whether it supports or not while configuring remote storage
CSCwh83328	SNMP fails to poll accurate hostname from FMC
CSCwh84833	Every HA sync attempts to disable URL filtering if already disabled.
CSCwh85824	eStreamer JSON parse error and memory leak
CSCwh89289	Snort is getting reloaded during deploy due to diff in timerange and nap conf contents in each run
CSCwh90693	FTD unregisters the standby FMC immediately after a successful registration
CSCwh90813	FDM Upgrade failure due to expired certificates
CSCwh93649	File copy via SCP using ciscossh stack fails with error "no such file or directory"
CSCwh95175	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwh98733	CPOC: 4245 ASA Crashed with CPS test
CSCwi03528	Cross ifc access: Revert PING to old non-cross ifc behavior
CSCwi06007	FMC missing validation for syslog port setting

Bug ID	Headline
CSCwi14896	Node kicked out of cluster while enabling or disabling rule profiling
CSCwi24880	ASA dropping IPSEC traffic incorrectly when "ip verify reverse-path" is configured
CSCwi31091	OSPF Redistribution route-map with prefix-list not working after upgrade

Resolved Bugs in Version 7.4.0

Table last updated: 2023-09-07

Table 18: Resolved Bugs in Version 7.4.0

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

Bug ID	Headline
CSCwa04262	Cisco ASA Software SSL VPN Client-Side Request Smuggling Vulnerability via "/"URI
CSCwa22766	FMC4500/4600 shows virtual license
CSCwa51867	FDM IKEv2 S2S PSK Not Deploying Correctly (Changing Asymmetric to Symmetric PSK)
CSCwa72481	API key corrupted for FMC with multiple interfaces
CSCwa80040	FMC NFS configuration failing after upgrade from 6.4.0.4 to 7.0.1
CSCwa93215	Primary node disconnected from VPN-Cluster when performed HA failover on Primary with DNS lookup
CSCwb02955	Modify /800_post/1027_ldap_external_auth_fix.pl to not fail FMC upgrade when objects are corrupt
CSCwb08189	Microsoft update traffic blocked with Snort version 3 Malware inspection
CSCwb20926	FDM: Policy deployment failure after upgrade due to unused IKEv1 policies
CSCwb44848	ASA/FTD Traceback and reload in Process Name: lina
CSCwb51821	Disk usage errors on Firepower Azure device due to large backup unified files under ngfw directory
CSCwb67464	FDM bootstrap could be skipped if device rebooted when bootstrap is not completed
CSCwb84677	FMC backup may fail due to monetdb backup failure with return code 102
CSCwb92583	upgrade with a large amount of unmonitored disk space used can cause failed upgrade and hung device
CSCwb94431	MFIB RPF failed counter instead of Other drops increments when outgoing interface list is Null
CSCwb95453	ASA: The timestamp for all logs generated by Admin context are the same
CSCwc03332	FTD on FP2100 can take over as HA active unit during reboot process
CSCwc13477	FMC Interface update Failed. Could not find source interface
CSCwc23844	ASAv high CPU and stack memory allocation errors despite over 30% free memory
CSCwc28660	Snort3: NFSv3 mount may fail for traffic through FTD
CSCwc30573	Deployment/Tasks Button not seen FMC_UI while doing upgrade tests configured in Light theme
CSCwc32245	FMC: Validation check to prevent exponential expansion of NAT rules
CSCwc44608	Selective deployment of IPS may cause outage due to incorrectly written FTD configuration files

Bug ID	Headline
CSCwc45298	Connection Events seen on FMC even though the rule is not configured to send events to FMC
CSCwc49655	FTPS getting ssl3_get_record:bad record type during connection for KK and DR rules
CSCwc49936	FMC 7.2.0 7.3.0 Integration > Identity Sources page does not load, keeps spinning
CSCwc50519	Excessive logging from hm_du.pm may lead to syslog-ng process restarts
CSCwc51588	Failing to generate FMC Backup/Restore via SMB/SSH
CSCwc52357	Estreamer page fails to load in ASDM
CSCwc59953	Snort3 crash with TLS 1.3
CSCwc61828	Fix multiple crash handler issues
CSCwc62215	FTD unable to sync HA due to snort validation failed
CSCwc64923	ASA/FTD may traceback and reload in Thread Name 'lina' ip routing ndbshr
CSCwc65814	sybase related modules should be removed
CSCwc65907	snort3 hangs in Crash handler which can lead to extended outage time during a snort crash
CSCwc67687	ASA HA failover triggers HTTP server restart failure and ASDM outage
CSCwc74099	FPR2140 ASA Clock Timezone reverts to UTC after appliance restart/reload
CSCwc74271	Auth-Daemon process is getting restarted continuously when SSO disabled
CSCwc74841	FMC RSS Feed broken because FeedBurner is no longer active - "Unable to parse feed"
CSCwc75082	25G-SR should default to RS-FEC (IEEE CL108) instead of FC-FEC
CSCwc76849	link state propagation stops working when performing full chassis reboot
CSCwc77519	FPR1000 ASA/FTD: Primary takes active role after reloading
CSCwc78296	Database may fail to shut down and/or start up properly during upgrade
CSCwc78689	Cannot save realm configuration unless AD Join Password is empty
CSCwc79520	Snort process may trace back in ssl_debug_log_config and generate core file
CSCwc81219	Intrusion events intermittently stop appearing in FMC when using snort3
CSCwc82205	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwc83037	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 36)
CSCwc87963	ASAv "Unable to retrieve license info. Please try again later"

Bug ID	Headline
CSCwc89661	FTD misses diagnostic data required for investigation of "Communication with NPU lost" error
CSCwc89924	FXOS ASA/FTD SNMP OID to poll Internal-data 'no buffer' interface counters
CSCwc93964	ASA using WebVPN tracebacks in Unicorn thread during memory tracking
CSCwc96016	Captive portal support in cross domain
CSCwc96780	FMC module specific health exclusion disables all health checks
CSCwd00583	SNMP 'Confirm Community String' string is not auto-populated after the FMC upgrade
CSCwd04210	ASA: ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT
CSCwd05814	PDTS write from Daq can fail when PDTS buffer is full eventually leads to block depletion
CSCwd07059	multiple snort3 crashes after upgrading FTD from 7.2.0 to 7.2.0.1
CSCwd07278	ASA/FTD tmatch compilation check when unit joins the cluster, when TCM is off
CSCwd09870	AnyConnect SAML using external browser and round robin DNS intermittently fails
CSCwd09967	Deployment Fails with stacktrace: Invalid type (LocalIdentitySource)
CSCwd10497	FTD sensor rules missing from ngfw.rules file after a sensor backup restore execution
CSCwd10880	critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on 2100/3100 devices
CSCwd11005	Missing fqdns_old.conf file causes FTD HA app sync failure
CSCwd13083	FMC - Unable to initiate deployment due to incorrect threat license validation
CSCwd13917	during download from file event on FMC, high CPU use on FMC for 20 minutes before download fails
CSCwd14688	FTD upgrade failure due to Syslog files getting generated/deleted rapidly
CSCwd14732	FTD Unable to bind to port 8305 after management IP change
CSCwd15197	ASA/FTD: Using Round Robin with PAT rules on two or more interfaces breaks IP stickiness
CSCwd16017	Object edit slowness when it is associated with NAT rules
CSCwd16517	GTP drops not always logged on buffer and syslog
CSCwd16902	File events show Action as "Malware Block" for files with correct disposition of unknown
CSCwd16906	ASA/FTD may traceback and reload in Thread Name 'lina' following policy deployment

Bug ID	Headline
CSCwd17940	HA did not failover due to misleading status updates from NDClient
CSCwd18744	FPR1K FTD fails to form HA due to reason "Other unit has different set of hwidb index"
CSCwd19053	ASA/FTD may traceback with large number of network objects deployment using distribute-list
CSCwd20900	HTTP Block Response and Interactive Block response pages not being displayed by Snort3
CSCwd22413	EIGRPv6 - Crashed with "mem_lock: Assertion mem_refcount' failed" on LINA.
CSCwd23188	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwd27186	All traffic blocked due to access-group command missing from FTD config
CSCwd28236	standby unit using both active and standby IPs causing duplicate IP issues due to nat "any"
CSCwd29835	log rotate failing to cycle files, resulting in large file sizes
CSCwd30298	FTD: FTPS Data Channel connection impacted by TLS Server Identity and Discovery Probe sent by FTD
CSCwd30774	FMC HA - files in tmp/Sync are left on secondary when synchronisation task fails
CSCwd32892	lost cac.conf after upgrade to 7.2.1 for FMC smart-card auth
CSCwd33054	DHCP Relay is looping back the DHCP offer packet causing dhcprelay to fail on the FTD/ASA
CSCwd33479	Duplicate SMB session id packets causing snort3 crash
CSCwd34662	LTS18 and LTS21 commit id update in CCM layer (seq 39)
CSCwd35726	Cisco FXOS Software Arbitrary File Write Vulnerability
CSCwd36246	Filtering of jobs in deploy history page is applying the criteria only on Top50 jobs
CSCwd37135	ASA/FTD traceback and reload on thread name fover_fail_check
CSCwd38196	Proxy is engaged even when we have a Definitive DND rule match
CSCwd38526	FMC can allow deployment of NAP in test mode with Decrypt policy
CSCwd39506	SSL Policy DND default Rule fails on error unsupported cipher suite and SKE error.
CSCwd40141	Firepower Management Center GUI view for Snort2 Local Intrusion Rules is missing
CSCwd40955	Very long validation time during Policy Deployment due to big network object in SSL policy
CSCwd41224	FMC HA webUI is not getting FTDv Variable tier assigned FTDv - Variable

Bug ID	Headline
CSCwd41466	Re-downloaded users from a forest with trusted domains may become unresolved/un-synchronized
CSCwd41806	deployment failed with OOM (out of memory) for policy_apply.pl process
CSCwd41986	Packet-Tracer interfaces not showing up in UI after updating interface name from lower to upper case
CSCwd42072	SRU installation failure.
CSCwd42347	FMC not showing any alerts/warnings when deploying changes of prefix list with same seq #
CSCwd42410	Expected snmp output is not found in 'show run in fxos snmp'
CSCwd42620	Deploying objects with escaped values in the description might cause all future deployments to fail
CSCwd43666	Analyze why there is no logrotate for /opt/cisco/config/var/log/ASAconsole.log
CSCwd43745	FTDv Cluster Health Monitor fails with "Error fetching live status of the cluster"
CSCwd44326	Object NAT edit is failing
CSCwd45048	Pre-login banner on FCM webUI shows extra characters on 92.14.0
CSCwd46061	FPR 2100: 10G interfaces with 1G SFP goes down post reload
CSCwd46182	Periodic sync failures are not reported to users
CSCwd46741	fxos log rotate failing to cycle files, resulting in large file sizes
CSCwd46780	ASA/FTD: Traceback and reload in Thread Name: appAgent_reply_processor_thread
CSCwd47340	FXOS: memory leak in svc_sam_envAG process
CSCwd47442	800_post/1027_ldap_external_auth_fix.pl upgrade error -- reference to missing authentication object
CSCwd47481	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 40)
CSCwd48633	ASA - traceback and reload when Webvpn Portal is used
CSCwd48776	Port-channel interface went down post deployment
CSCwd49636	FMC UI showing disabled/offline for multiple devices as health events are not processed
CSCwd49685	Missing SSL MEMCAP causes deployment failure due timeout waiting for snort detection engines
CSCwd49758	Pre-deployment failure seen in FMC due to huge number policies
CSCwd50131	Upgrades are not cleaning up mysql files leading to alert for 'High unmanaged disk usage on /ngfw'

Bug ID	Headline
CSCwd50218	ASA restore is not applying vlan configuration
CSCwd51757	Unable to get polling results using snmp GET for connection rate OID's
CSCwd51964	Add validation in lua detector api to check for empty patterns for service apps
CSCwd52995	FMC not opening deployment preview window
CSCwd53135	ASA/FTD: Object Group Search Syslog for flows exceeding threshold
CSCwd53340	FTD PDTS LINA RX queue can become stuck when snort send messages with 4085-4096 bytes size
CSCwd53635	AWS: SSL decryption failing with Geneve tunnel interface
CSCwd53863	Data migration from Sybase to MariaDB taking more time due to large data size of POLICY_SNAPSHOT
CSCwd54439	FMC gives an irrelevant error message for Snort2 to Snort3 rules conversion failure
CSCwd55642	Stale CPU core health events seen on FMC UI post upgrade to 7.0.0+.
CSCwd55673	Need corrections in log_handler_file watchdog crash fix
CSCwd55853	Deployment failure with localpool overlap error after upgrade
CSCwd56254	"show tech-support" generation does not include "show inventory" when run on FTD
CSCwd56296	FTD Lina traceback and reload in Thread Name 'IP Init Thread'
CSCwd56774	Misleading drop reason in "show asp drop"
CSCwd56995	Clientless Accessing Web Contents using application/octet-stream vs text/plain
CSCwd57698	Recursive panic under lina_duart_write
CSCwd57927	FMC UI may become unavailable and show "System processes are starting" message after upgrade
CSCwd58188	Inline-pair's state could not able to auto recover from hardware-bypass to standby mode.
CSCwd58337	allocate more cgroup memory for policy deployment subgroup
CSCwd58417	HA Periodic sync is failing due to cfg files are missing
CSCwd58430	At times AC Policy save takes longer time, may be around 10 or above mins
CSCwd59736	ASA/FTD: Traceback and reload due to SNMP group configuration during upgrade
CSCwd61016	ASA: Standby may get stuck in "Sync Config" status upon reboot when there is EEM is configured
CSCwd61082	FMC UI Showing inaccurate data in S2S VPN Monitoring page

Bug ID	Headline
CSCwd62025	FTDv: Policy Deployment failure due to interface setting on failover interface
CSCwd62138	ASA Connections stuck in idle state when DCD is enabled
CSCwd62915	Cross-domain users with non-ASCII characters are not resolved
CSCwd63580	FPR2100: Increase in failover convergence time with ASA in Appliance mode
CSCwd63722	FTDv Single-Arm Proxy behind AWS GWLB drops due to geneve-invalid-udp-checksum with all 0 checksum
CSCwd63961	AC clients fail to match DAP rules due to attribute value too large
CSCwd64480	Packets through cascading contexts in ASA are dropped in gateway context after software upgrade
CSCwd64919	FXOS is not rotating PoE logs
CSCwd66709	FP4125 2.10.1.166 FTD applications in HA went into not responding state
CSCwd66815	Lina changes to support - Snort3 traceback in daq-pdts while handling FQDN based traffic
CSCwd68088	ASA FTD: Implement different TLS diffie-hellman prime based on RFC recommendation
CSCwd69236	FMC Connection Event stop displaying latest event
CSCwd69454	Port-channel interfaces of secondary unit are in waiting status after reload
CSCwd70117	FMC should not accept carriage return in the interface description field of a managed device
CSCwd71254	ASA/FTD may traceback and reload in idfw fqdn hash lookup
CSCwd71274	S2S VPN dashboard shows ipv4 SVTI tunnel down between KP-HA and WA-HA after KP-HA Switch role.
CSCwd72680	FXOS: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
CSCwd72915	FMC 7.1.0.1 Doesn't throw warning that S2S VPN Configs contain deprecated MD5 Hash during deployment
CSCwd73981	FMC: Updates page takes more than 5 minutes to load
CSCwd74116	S2S Tunnels do not come up due to DH computation failure caused by DSID Leak
CSCwd74839	30+ seconds data loss when unit re-join cluster
CSCwd75738	Predefined FlexConfig Text Objects are not exported by Import-Export
CSCwd75782	FMC External Auth test error "Encryption method is configured but you did not upload a certificate."

Bug ID	Headline
CSCwd76622	FTD with Snort3 might have memory corruption BT in snort file with same IP traffic scaling
CSCwd76634	FMC import takes too long
CSCwd76930	FPR3110 Fans' SN in label are different from show inventory cli output
CSCwd77300	Snort crashes while reloading mercury library with any VDB install on 7.3.0 and 7.4.0
CSCwd78624	ASA configured with HA may traceback and reload with multiple input/output error messages
CSCwd79388	intrusion events fail to migrate from MariaDB to MonetDB following FMC upgrade from 7.0.3 to 7.1.0
CSCwd80284	Import/export fails with backend error
CSCwd80343	MI FTD running 7.0.4 is on High disk utilization
CSCwd80741	Snort drops Bomgar application packets with Early Application Detection enabled
CSCwd81538	FTD Traffic failure due to 9344 block depletion in peer_proxy_tx_q
CSCwd81897	Snort3 crash seen sometimes while processing a future flow connection after appid detectors reload
CSCwd82235	LINA Traceback on FPR-1010 under Thread Name: update_cpu_usage
CSCwd82801	Snort outputs massive volume of packet events - IPS event view may show "No Packet Information"
CSCwd83441	FMC should display the status of physical FTD interfaces bundled in port-channel
CSCwd83990	FTD -Snort match incorrect NAP id for traffic
CSCwd84046	Microsoft SCEP enrollment fails to get ASA identity cert - Unable to verify PKCS7
CSCwd84133	ASA/FTD may traceback and reload in Thread Name 'telnet/ci'
CSCwd84153	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwd84868	Observing some devcmd failures and checkheaps traceback when flow offload is not used.
CSCwd84942	Snort mem used alert should read the value from perfstats for snort instance rather than cgroups
CSCwd85178	AWS ASAv PAYG Licensing not working in GovCloud regions.
CSCwd85609	FTDs running 6.6.x show as disconnected on new HM (6.7+) but checks are running and updating
CSCwd85927	Traceback and reload when webvpn users match DAP access-list with 36k elements

Bug ID	Headline
CSCwd86313	Unable to access Dynamic Access policy
CSCwd86457	Number of objects are not getting updated under policies>>>Security intelligence >>>Block list
CSCwd86535	ASA/FTD: Traceback and Reload on Netflow timer infra
CSCwd86783	Disabling NAVL guides from userappid.conf doesn't work
CSCwd86929	Cut-Through Proxy does not work with HTTPS traffic
CSCwd87129	seeing error on access policies on FMC - "Error during policy validation"
CSCwd87438	Enhance logging mechanism for syslogs
CSCwd88585	ASA/FTD NAT Pool Cluster allocation and reservation discrepancy between units
CSCwd88641	Deployment changes to push VDB package based on Device model and snort engine
CSCwd89848	ASA/FTD failure due to heartbeat loss between chassis and blade
CSCwd90112	MariaDB crash (segmentation fault) related to netmap query
CSCwd90846	Software upgrade on FDM fails due to improper next-hop validation
CSCwd91013	FMC Deployment failure in csm_snapshot_error
CSCwd91421	ASA/FTD may traceback and reload in logging_cfg processing
CSCwd91932	Incorrect Paging and count value for Time Range Object Get API
CSCwd92804	FAN LED flashing amber on FPR2100
CSCwd93316	No Inspect Interruption warning when deploy after FMC upgrade
CSCwd93376	Clientless VPN users are unable to download large files through the WebVPN portal
CSCwd93792	SFDataCorrelator performance degradation involving hosts with many discovered MAC addresses
CSCwd94096	Anyconnect users unable to connect when ASA using different authentication and authorization server
CSCwd94183	Blade not coming up after FXOS update support on multi-instance due to ssp_ntp.log log rotation prob
CSCwd94670	Can't modify RA vpn group policy on FDM 7.3
CSCwd95436	Primary ASA traceback upon rebooting the secondary
CSCwd95908	ASA/FTD traceback and reload, Thread Name: rtcli async executor process
CSCwd96041	FMC SecureX via proxy stops working after upgrade to 7.x

Bug ID	Headline
CSCwd96493	Link Up seen for a few seconds on FPR1010 during bootup
CSCwd96500	FTD: Unable to configure WebVPN Keepout or Certificate Map on FPR3100
CSCwd96755	ASA is unexpected reload when doing backup
CSCwd96766	41xx: Blade does not capture or log a reboot signal
CSCwd96790	High FMC backup file size due to configurations snapshot for all managed devices
CSCwd97020	ASA/FTD: External IDP SAML authentication fails with Bad Request message
CSCwe00757	Summary status dashboard takes more than 3 mins to load upon login
CSCwe00828	Interactive Block action doesn't work when websites are redirected to https
CSCwe00864	License Commands go missing in Cluster data unit if the Cluster join fails.
CSCwe03529	FTD traceback and reload while deploying PAT POOL
CSCwe03631	Need to provide rate-limit on "logging history & mode;"
CSCwe04437	collection of top.log.gz in troubleshoot can be corrupt due to race condition
CSCwe04746	Unexpected "No Traffic" health alert on Standby HA Data Interface where no data flows
CSCwe05913	FTD traceback/reloads - Icmp error packet processing involves snp_nat_xlate_identity
CSCwe06562	FPR1K/FPR2K: Increase in failover time in Transparent Mode with high number of Sub-Interfaces
CSCwe06724	Database table optimization not working for some of the tables
CSCwe06826	Email alert incorrectly send for a successful database backup
CSCwe06828	FMC HA Synchronization can hang forever if no response from SendUserReloadSGTAndEndpointsEvent
CSCwe07103	FMC: Upgrade fails at DB Integrity check due to large number of EO warnings for "rule_comments"
CSCwe07722	Cluster data unit drops non-VPN traffic with ASP reason "VPN reclassify failure"
CSCwe07928	On a cloud-delivered FMC there is no way to send events to syslog without sending to SAL/CDO as well
CSCwe08729	FPR1120:connections are getting teardown after switchover in HA
CSCwe08908	Threatgrid integration configuration is not sync'd as part of the FMC HA Synchronisation
CSCwe09074	None option under trustpoint doesn't work when CRL check is failing

Bug ID	Headline
CSCwe09121	FTD Deployment failures due to "snort3.validation.lua:5: '=' expected near 'change'"
CSCwe09811	FTD traceback and reload during policy deployment adding/removing/editing of NAT statements.
CSCwe10290	FTD is dropping GRE traffic from WSA
CSCwe10548	ASA binding with LDAP as authorization method with missing configuration
CSCwe11119	ASA: Traceback and reload while processing SNMP packets
CSCwe11727	Purging of Config Archive failed for all the devices if one device has no versions
CSCwe12407	High Lina memory use due to leaked SSL handles
CSCwe13627	FMC Unable to fetch VPN troubleshooting logs.
CSCwe14174	FTD - 'show memory top-usage' providing improper value for memory allocation
CSCwe14417	FTD: IPSLA Pre-emption not working even when destination becomes reachable
CSCwe14514	ASA/FTD Traceback and reload of Standby Unit while removing capture configurations
CSCwe14590	FMC deployment preview showing full config instead of delta.
CSCwe15111	FMC is not taking BGP default originate configuration via API PUT request.
CSCwe16554	TLS sessions dropped under certain conditions after a fragmented Client Hello
CSCwe16620	FMC Health Monitor does not report alerts for the Interface Status module
CSCwe16730	Deployment failing - "Error while printing show-xml-response file contents" XML response too big
CSCwe17858	FMC HA info is not sync'ed reliably to FTD to support CLOUD_SERVICE
CSCwe18090	FMC deployment failure:"Validation failed: This is a slav*/ha standby device, rejecting deployment."
CSCwe18216	null connection error seen in logs
CSCwe18472	[FTD Multi-Instance][SNMP] - CPU OIDs return incomplete list of associated CPUs
CSCwe18974	ASA/FTD may traceback and reload in Thread Name: CTM Daemon
CSCwe19051	FTD High unmanaged disk usage alert is triggered due to stored files located on /ngfw/Volume/root1/
CSCwe19830	Policy deploy failure "error executing /*!40101 SET character_set_client = @saved_cs_client */; *"
CSCwe20043	256-byte memory block gets depleted on start if jumbo frame is enabled with FTD on ASA5516

Bug ID	Headline
CSCwe20714	Traffic drop when primary device is active
CSCwe21037	Snort mem used alert should be consistent with value from top.log
CSCwe21187	ASA/FTD may drop multicast packets due to no-mcast-intrf ASP drop reason until UDP timeout expires
CSCwe21280	Multicast connection built or teardown syslog messages may not always be generated
CSCwe21831	add warning to FTD platform settings when VPN Logging Settings logging level is informational
CSCwe21959	Snort3: Process in D state resulting in OOM with jemalloc memory manager
CSCwe22254	After disabling malware analysis, high disk usage on /dev/shm/snort
CSCwe22302	Partition "/opt/cisco/config" gets full due to wtmp file not getting logrotated
CSCwe22386	Unexpected firewalls reloads with traceback.
CSCwe22492	Slow UI loading for Table View of Hosts
CSCwe22980	Database integrity check takes several minutes to complete
CSCwe23039	NTP polling frequency changed from 5 minutes to 1 second causes large useless log files
CSCwe23801	FPR2100: Multiple snort3 & snort2 cores got generated and sensor goes down in KP platform
CSCwe24532	Multiple instances of nvram.out log rotated files under /opt/cisco/platform/logs/
CSCwe25187	FMC External authentication getting "Internal error"
CSCwe25391	rpc service detector causing snort traceback due to universal address being an empty string
CSCwe26342	ASA Traceback & reload citing thread name: asacli/0
CSCwe26612	FTD taking longer than expected to form OSPF adjacencies after a failover switchover
CSCwe28094	ASA/FTD may traceback and reload after executing 'clear counters all' when VPN tunnels are created
CSCwe28362	Copy and pasting rules is broken and give blank error message in ID policy
CSCwe28407	LINA traceback with icmp_thread
CSCwe28726	The command "app-agent heartbeat" is getting removed when deleting any created context
CSCwe29179	CLUSTER: ICMP reply arrives at director earlier than CLU add flow request from flow owner.

Bug ID	Headline
CSCwe29498	occasional failure to load light-modal-ac-rule-xx.css with a net::ERR_TOO_MANY_RETRIES error
CSCwe29529	FTD MI does not adjust PVID on vlans attached to BVI
CSCwe29583	ASA/FTD may traceback and reload in Thread Name 'None' at lua_getinfo
CSCwe29850	ASA/FTD Show chunkstat top command implementation
CSCwe29952	SFDataCorrelator cores due to stuck database query after 1 hour deadlock timeout
CSCwe30228	ASA/FTD might traceback in funtion "snp_fp_l2_capture_internal" due to cf_reinject_hide flag
CSCwe30867	Workaround to set hwclock from ntp logs on low end platforms
CSCwe32448	changing time window settings in FMC GUI event viewers may not work with FMC integrated with SecureX
CSCwe33130	Supervisor does not reboot unresponsive module/blade due to IERR with minor severity sensor ID 79
CSCwe34871	Active authentication sessions are showing in VPN dashboard
CSCwe36176	ASA/FTD: High failover delay with large number of (sub)interfaces and http server enabled
CSCwe37132	TLS Server Identity may cause certain clients to produce mangled Client Hello
CSCwe37453	Gateway is not reachable from standby unit in admin and user context with shared mgmt intf
CSCwe38029	Multiple traceback seen on standby unit.
CSCwe39425	2100: Power switch toggle leads to ungraceful shutdowns and "PowerCycleRequest" reset
CSCwe39431	FMC Upgrade: generation of sftunnel.json file per FTD does not check for duplicate names
CSCwe39546	FMC: Backup to an unavailable remote host results in the inability to restart the appliance.
CSCwe40463	Stale IKEv2 SA formed during simultaneous IKE SA handling when missing delete from the peer
CSCwe41336	FDM WM-HA ssh is not working after upgrading 7.2.3 beta with data interface as management
CSCwe41898	ASA: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.

Bug ID	Headline
CSCwe43965	Remove the limit of 30characters in the rule name which a rule is moved from ACP to Prefilter
CSCwe44311	FP2100:Update LINA asa.log files to avoid recursive messages-<date>.1.gz rotated filenames
CSCwe44620	Question mark in NAT description causes config mismatch on Data members of an FTD cluster
CSCwe44672	Syslog ASA-6-611101 is generated twice for a single ssh connection
CSCwe44766	IMS: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
CSCwe45211	Need to Warn the users before triggering a full deployment on FTD managed by FDM
CSCwe45222	Snort3 crashes are seen under Dce2Smb2FileTracker processing of data
CSCwe45779	ASA/FTD drops traffic to BVI if floating conn is not default value due to no valid adjacency
CSCwe45879	Frequent errors seen regarding failures to load bulkcsv files that don't exist
CSCwe48378	Remove FMC drop_cache trigger to prevent Disk I/O increase due to file cache thrashing
CSCwe48432	Unable to save Access Control Policy changes due to Internal error
CSCwe50946	Management interface link status not getting synced between FXOS and ASA
CSCwe50993	SNMP on SFR module goes down and won't come back up
CSCwe51286	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe51296	Not able to remove group policy from RAVPN via REST API
CSCwe51443	ASA Evaluation of OpenSSL vulnerability CVE-2022-4450
CSCwe52120	SSL decrypted conns fails when tx chksum-offload is enabled with the egress interface a pppoe.
CSCwe52499	NGIPsv syslog-tls.conf.tt needs filters removed when in CC mode
CSCwe53089	The user belonging to a subdomain, is unable to collect packet tracer
CSCwe54529	FTD on FPR2140 - Lina traceback and reload by TCP normalization
CSCwe54567	Manager gets unregistered on its own from the FTD, show manager shows 'No managers configured'
CSCwe56452	BGP IPv6 configuration : route-map association with neighbour not getting deployed
CSCwe57218	FMC: Incorrect FTD cluster role status leading to inability to upgrade FTD

Bug ID	Headline
CSCwe58207	Memory leak observed on ASA/FTD when logging history is enabled
CSCwe58576	FTD:Node not joining cluster with "Health check detected that control left cluster" due to SSL error
CSCwe58881	After FMC upgrade, SecureX ribbon redirects to US cloud region regardless of the set cloud region
CSCwe58980	/var/sf/QueryPoolData fills up with warehouse directories
CSCwe59380	FTD: "timeout floating-conn" not operating as expected for connections dependent on VRF routing
CSCwe59664	DAP policy created in FMC Gui, to detect a Windows OS with a hotfix, will not work as expected
CSCwe59737	ASA/FTD reboots due to traceback pointing to watchdog timeout on p3_tree_lookup
CSCwe59919	FTD Traceback and reload on Thread Name "NetSnmp Event mib process"
CSCwe60267	FXOS fault F0853 and F0855 seen despite keyring reporting renewed
CSCwe61599	FTD 2100 -Update daq-ioq mempool to help protect against buffer corruption
CSCwe61703	Unable to delete custom anyconnect attribute --dynamic-split-tunnel from group-policy
CSCwe61928	PIM register packets are not sent to RP after a reload if FTD uses a default gateway to reach the RP
CSCwe61969	ASA Multicontext 'management-only' interface attribute not synced during creation
CSCwe62361	ASA reboots due to heartbeat loss and "Communication with NPU lost"
CSCwe62703	New context subcommands are not replicated on HA standby when multiple sessions are opened.
CSCwe62927	DCCSM session authorization failure cause multiple issues across FMC
CSCwe62971	Policy Deploy Failing when trying to remove Umbrella DNS Connector Configuration
CSCwe62997	ASA/FTD traceback in snp_tracer_format_route
CSCwe63067	ASA/FTD may traceback and reload in Thread Name 'lina' due to due to tcp intercept stat
CSCwe63232	ASA/FTD: Ensure flow-offload states within cluster are the same
CSCwe63266	Need fault/error for invalid firmware MF-111-234949
CSCwe63316	Pri-Active FMC NOT triggering registration TASK for FTD to configure standby manager
CSCwe63493	Post backup restore multiple processes are not up. No errors are observed during backup or restore.

Bug ID	Headline
CSCwe64043	Cisco ASA and FTD ACLs Not Installed upon Reload
CSCwe64281	Deployment failed in snapshot generation after upgrading FMC to 7.3
CSCwe64404	ASA/FTD may traceback and reload after changing IP of authentication server
CSCwe64542	TID python processes stuck at 100% CPU
CSCwe64557	ASA: Prevent SFR module configuration on unsupported 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
CSCwe65634	ASA - Standby device may traceback and reload during synchronization of ACL DAP
CSCwe66132	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe67751	Last fragment from SIP IPv6 packets has MF equal to 1, flagging that more packets are expected
CSCwe67816	ASA / FTD Traceback and reload when removing isakmp capture
CSCwe68159	Failover fover_trace.log file is flooding and gets overwritten quickly
CSCwe68917	Snort3 fails to match SMTPS traffic to ACP rules
CSCwe69388	FMC should push the AnyConnect Custom attribute defer keyword as lowercase instead of capitalized
CSCwe70202	Multiple times the failover may be disabled by wrongly seeing a different "Mate operational mode".
CSCwe70558	FTD: unable to run any commands on CLISH prompt
CSCwe70665	Snort high memory alerts still seen despite fix for CSCwd84942
CSCwe70721	Deployment is blocked due to Pre-deploy Validation Error - Invalid endpoint
CSCwe71284	ASA/FTD may traceback and reload in Thread Name DATAPATH-3-21853
CSCwe71672	Selective deployment negating the route configs
CSCwe71673	Selective deployment removing the prefilter-configs
CSCwe71674	Selective deployment removing the Group policy
CSCwe72330	FTD LINA traceback and reload in Datapath thread after adding Static Routing
CSCwe72535	Unable to login to FTD using external authentication
CSCwe73116	Cross-interface-access: ICMP Ping to management access ifc over VPN is broken

Bug ID	Headline
CSCwe73240	FMC runs out of space when Snort sends massive numbers of packet logs
CSCwe74059	logrotate is not compressing files on 9.16 ASA or 7.0 FTD
CSCwe74089	ASA/FTD may traceback and reload in Thread Name DATAPATH-1-1656
CSCwe74290	SFDataCorrelator spam seen in /var/log/messages
CSCwe74328	AnyConnect - mobile devices are not able to connect when hostscan is enabled
CSCwe74899	CD App Sync error is App Config Apply Failed on Secondary/Standby after backup restore on RMA device
CSCwe74916	Interface remains DOWN in an Inline-set with propagate link state
CSCwe75018	Snort2 rule recommendations increases disabled rule count drastically
CSCwe75055	[FMC model migration] Health monitoring on FMC reporting errors
CSCwe75124	Upgraded FMC didn't mark FTD's with Hot Fix as light registered - failed FMC HA sync
CSCwe75207	High rate of network map updates can cause large delays and backlogs in event processing
CSCwe76036	ndclientd error message 'Local Disk is full' needs to provide mount details which is full
CSCwe76722	ASA/FTD: From-the-box ping fails when using a custom VRF
CSCwe77123	ASA/FTD : Degradation for TCP tput on FPR2100 via IPSEC VPN when there is delay between VPN peers
CSCwe77896	Improve Azure AD realm documentation
CSCwe78977	ASA/FTD may traceback and reload in Thread Name 'pix_flash_config_thread'
CSCwe79051	Deployment for eigrp / bgp change may cause temporary outage during policy apply
CSCwe79072	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe79954	LDAP External auth config fails to deploy to FTD if same LDAP server is added as Primary and backup
CSCwe80063	Default DLY value of port-channel sub interface mismatch with parent Portchannel
CSCwe81684	ASA: Standby failure on parsing of "management-only" not reported to parser/failover subsystem
CSCwe82107	health alert for [FSM:STAGE:FAILED]: external aaa server configuration
CSCwe82631	FMC isn't allowing to create more than 30 VLAN interfaces

Bug ID	Headline
CSCwe83061	FMC Upgrade from Active-Primary FMC is failed with "Installation failed: Peer Discovery incomplete."
CSCwe83069	Fix Snort3 Memory Utilisation Value
CSCwe83478	Prune target should account for the allocated memory from the thread pruned
CSCwe85432	ASA/FTD traceback and reload on thread DATAPATH-14-11344 when SIP inspection is enabled
CSCwe86029	FMC system restore authentication error during FMC re-image when using FTP/SCP protocol
CSCwe86225	ASA/FTD traceback and reload due citing thread name: cli_xml_server in tm_job_add
CSCwe86350	email alert to scheduled activity is not working after upgrading to 7.2
CSCwe88496	"Failed to convert snort 2 custom rules. Refer /var/sf/htdocs/ips/snort.rej for more details."
CSCwe88772	ASA traceback and reload with process name: cli_xml_request_process
CSCwe89030	Serial number attribute from the subject DN of certificate should be taken as the username
CSCwe89305	vFMC300 to FMC2600 migration failure with error "migration from R to N is not allowed"
CSCwe89731	Notification Daemon false alarm of Service Down
CSCwe89985	CVIM Console getting stuck in "Booting the kernel" page
CSCwe90095	Username-from-certificate feature cannot extract the email attribute
CSCwe90202	ASA: Standby failure on parsing of "management-only" for dynamic configuraiton changes
CSCwe90334	Missing Instance ID in unified_events-2.log
CSCwe90596	Elephant flow detection disabled on FMC, getting enabled on FTD after random deployment
CSCwe90720	ASA Traceback and reload in parse thread due ha_msg corruption
CSCwe91958	correlation events based on connection events do not contain Security Intelligence Category content
CSCwe92905	ngfwManager process continuously restarting leading to ZMQ Out of Memory traceback
CSCwe93061	FTD returns no output of "show elephant-flow status" when efd.lua file's content is empty
CSCwe93162	FP1140 7.0.4 Deployment keep failing with error "Can't use an undefined value as a HASH reference"

Bug ID	Headline
CSCwe93176	Snort2 rule assignments missing from ngfw.rules (assignment_data table) after FMC upgrade.
CSCwe93202	FXOS REST API: Unable to create a keyring with type "ecdasa"
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
CSCwe93566	need to turn off default TLS 1.1 (deprecated) support for the FDM GUI
CSCwe93736	ASA not updating Timezone despite taking commands
CSCwe94287	FTD DHCP Relay drops NACK if multiple DHCP Servers are configured
CSCwe94789	Umbrella DNS Negate of Bypass Domain Field is not generated from FMC
CSCwe95757	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe96023	ASa/FTD: SNMP related traceback and reload immediately after upgrade from 6.6.5 to 7.0.1
CSCwe96068	ASA: Configurable CLU for Large amount of under/overruns on CLU RX/TX queues
CSCwe96857	FMC error displaying users page due to wide characters in real name field
CSCwe97325	FDM Cannot create self-signed certificates due to Expiration Date format
CSCwe98430	AC policy deploy failing on 7.2.4 FMC to 6.7 FTD
CSCwe99040	traceback and reload thread datapath on process tcpmod_proxy_continue_bp
CSCwe99550	Add knob to pause/resume file specific logging in asa log infra.
CSCwe99945	DOC: Misleading Documentation of Cisco Firepower 2100 GLC-T and GLC-TE SFP Support
CSCwf00417	FTD: Unable to process a TLS1.2 website with TLS Server Identity with client generating SSL Errors
CSCwf00483	Found Orphaned SFTop10Cacher processes
CSCwf00865	FTD/ASA Hub and spoke (U-turn) VPN fails when one spoke is IPSec flow offloaded and the other isn't
CSCwf01051	standby in disabled state after QP-MI HA 7.0.3 to 7.2.4-126, APPLY_APP_CONFIG_APPLICATION_FAILURE
CSCwf01064	TCP ping is completely broken starting in 9.18.2
CSCwf01954	FTD: ADI.conf - send_s2s_vpn_events is set to 0, even after applying s2s vpn health policy

Bug ID	Headline
CSCwf02363	Snort3 Crash in SslServiceDetector after call from nss_passwd_lookup
CSCwf03011	Prune symmetric triggers that existed in sfsnort schema before FMC upgrade to 7.3 version or later
CSCwf04831	ASA/FTD may traceback and reload in Thread Name 'ci/console'
CSCwf04870	ASA: "Ping <ifc_name> x.x.x.x" is not working as expected starting 9.18.x
CSCwf06318	Readiness check needs to be allowed to run without pausing FMC HA
CSCwf06377	Setting heartbeat timeout to 6sec for BS and QP
CSCwf07030	Upgrade Device listing page is taking more than 15 mins to load page fully with 25 FTDs registered
CSCwf07791	ASA running out of SNMP PDU and SNMP VAR chunks
CSCwf08043	Lina traceback and reload due to fragmented packets
CSCwf08515	FPR3100: ASA/FTD High traffic impact on all data interfaces with high counter of "demux drops"
CSCwf10422	"Security Intelligence feed download failed" displayed even though it succeeded
CSCwf10486	ISE Integration Network filter not accepting multiple comma separated networks
CSCwf10910	FTD : Traceback in ZMQ running 7.3.0
CSCwf12005	ASA sends OCSP request without user-agent and host
CSCwf12408	ASA: After upgrade to 9.16.4 all type-8 passwords are lost on first reboot
CSCwf12521	Unable to load intrusion policy page on FMC GUI
CSCwf12985	FTDv: Traffic failure in VMware Deployments due to dpdk pool exhaustion and rx_buff_alloc_failure
CSCwf14126	ASA Traceback and reload citing process name 'lina'
CSCwf14257	FTD container restored from backup fails to register to FMC due to Peer send bad hash error
CSCwf14735	traceback and reload in Process Name: lina related to Nat/Pat
CSCwf14811	TCP normalizer needs stats that show actions like packet drops
CSCwf15858	LDAP authentication over SSL not working for users that send large authorisation profiles
CSCwf15902	ASAv in Hyper-V drops packets on management interface
CSCwf16108	When enabling backup peer ip on FMC 7.3.1 with a space the VPN IPSec profile would be removed

Bug ID	Headline
CSCwf17406	Failure to remove snort stat files older than 70 days
CSCwf17814	ASA/FTD may traceback and reload in Thread Name '19', free block checksum failure
CSCwf19562	Changes to lamplighter logs written to /var/log/tid_process.log
CSCwf19853	FATAL errors in DBCheck due to missing columns in eventdb table
CSCwf20215	admin user should be excluded from CLI shell access filter
CSCwf20338	ASA may traceback and reload in Thread Name 'DHCPv6 Relay'
CSCwf20958	No logrotate and max size is configured for Health.log file
CSCwf21106	ASA/FTD: Traceback on thread name: snmp_master_callback_thread during SNMP and interface changes
CSCwf22005	ASA Packet-tracer displays the first ACL rule always, though matches the right ACL
CSCwf22568	FTD HA Creation fails resulting in devices showing up in an inconsistent state on the FMC
CSCwf22854	Not able to add files with file names which has '\u' to clean list from Malware Summary page
CSCwf23564	Unable to establish BGP when using MD5 authentication over GRE TUNNEL and FTD as passthrough device
CSCwf24124	SFDataCorrelator process crashing very frequently on the FMC.
CSCwf24773	crashhandler running with test mode snort
CSCwf25144	FMC backup management page showing "Verifying Backup" for FTD sensors.
CSCwf26264	FMC backup restore page takes around 5 mins to load when remote storage is unreachable
CSCwf26407	FP2130- Unable to disassociate member from port channel, deployment fails, member is lost on FTD/FMC
CSCwf26534	ASA/FTD: Connection information in SIP-SDP header remains untranslated with destination static Any
CSCwf26939	FTD may fail to create a NAT rule with error: "IPv4 dst real obj address range is huge"
CSCwf28488	Inconsistent log messages seen when emblem is configured and buffer logging is set to debug
CSCwf28592	In some specific scenarios, object optimizer can cause incorrect rules to be deployed to the device
CSCwf30716	ASA in multi context shows standby device in failed stated even after MIO HB recovery.

Bug ID	Headline
CSCwf30727	ASA integration with umbrella does not work without validation-usage ssl-server.
CSCwf31701	ASA traceback and reload with the Thread name: **CP Crypto Result Processing**
CSCwf31820	Firewall may drop packets when routing between global or user VRFs
CSCwf32890	Standby FMC SSH connection getting disconnected frequently.
CSCwf33574	ASA access-list entries have the same hash after upgrade
CSCwf33904	Virtual FDM Upgrade fails: HA configStatus='OUT_OF_SYNC after UpgradeOnStandby
CSCwf34152	FMC Fails to deploy or register new FTDs due to SFTunnel Establishment Failure.
CSCwf34450	Snort3 crash after the consequent snort restart if duplicate custom apps are present
CSCwf34500	FTD: GRE traffic is load balanced between CPU cores
CSCwf35173	SFTunnel Fails to Properly Establish due to running_config.conf file misconfiguration
CSCwf35207	ASA: Traceback and reload while updating ACLs on ASA
CSCwf35346	FMC should handle error appropriately when ISE reports error during SXP download
CSCwf37160	AnyConnect Ikev2 Login Failed With certificate-group-map Configured
CSCwf39968	FMC UI related issue in Object management page
CSCwf42144	ASA/FTD may traceback and reload citing process name "lina"
CSCwf43247	NMAP Remediation scan tasks remain in pending state in action queue table, does not clear out
CSCwf43288	Traceback in Thread Name: ssh/client in a clustered setup
CSCwf43391	Adding verify check for networks added under network object group in FMC
CSCwf44915	Old LSP packages are not pruned causing high disk utilization
CSCwf47487	CSM backup failed due to modification of CSM audit log file while tar was reading it
CSCwf48599	VPN load-balancing cluster encryption using deprecated ciphers
CSCwf49573	ASA/FTD: Traceback and reload when issuing 'show memory webvpn all objects'
CSCwf51824	FXOS SNMP "property community of sys/svc-ext/snmp-svc is out of range" is unclear to users
CSCwf51933	FTD username with dot fails AAA-RADIUS external authentication login after upgrade
CSCwf54418	Reduce time taken to clear stale IKEv2 SAs formed after Duplicate Detection

Bug ID	Headline
CSCwf56291	FMC config archives retention reverts to default if ca_purge tool was used prior to 7.2.4 upgrade
CSCwf57850	TelemetryApp process keeps exiting every minute after upgrading the FMC
CSCwf58876	KP2140-HA, reloaded primary unit not able to detect the peer unit
CSCwf59571	FTD/Lina - ZMQ issue OUT OF MEMORY. due to less Msglyr pool memory in low end platforms
CSCwf60311	ASA generating traceback with thread-name: DATAPATH-53-18309 after upgrade to 9.16.4.19
CSCwf60584	Health Monitoring to NOT collect route stats for transparent mode FTD
CSCwf62103	FMC needs to properly validate QoS policy rules before allowing deployment to FTD
CSCwf62885	FTDv Single-Arm Proxy behind AWS GWLB drops due to geneve-invalid-udp-checksum.
CSCwf66271	Unable to list down the interface under the device exclude policy
CSCwf71606	Cisco ASA and FTD ACLs Not Installed upon Reload
CSCwf71812	FTD Lina engine may traceback, due to assertion, in datapath
CSCwf72510	Avoid both the devices in HA sends events to FMC
CSCwf73189	FTD is dropping GRE traffic from WSA due to NAT failure
CSCwf76970	Include a warning during break HA when secondary unit is active
CSCwf77191	ASA appliance mode - 'connect fxos [admin]' will get ERROR: failed to open connection.
CSCwf78950	FMC 1600 process ssp_snmp_trap_fwdr high memory utilization
CSCwf81058	FTD: Firepower 3100 Dynamic Flow Offload showing as Enabled
CSCwf81320	Unable to configure and deploy IPv6 DNS server for RAVPN in FMC 7.2.4
CSCwf82247	Policy deployment fails when a route same prefix/metric is configured in a separate VRF.
CSCwf84588	Disable TLS 1.1 permanently for sftunnel communication
CSCwf85307	[Snort 3] IPS Policy Overrides not working on Chained Intrusion Policies
CSCwf86860	FMC GUI ACP page gets blank and hang while doing search in rules and moving to last pages
CSCwf87761	Copy of Policy causes all devices to be marked as dirty
CSCwf88552	ASA/FTD: Traceback and reload due to NAT L7 inspection rewrite

Bug ID	Headline
CSCwh12009	EOSStore failed error is outputted after deleting shared rule layer.
CSCwh13551	Encrypted Visibility Engine (EVE) dashboard tab and widgets not added to FMC GUI upon upgrade
CSCwh14731	The authentication object names should not contain white spaces
CSCwh21337	FTD - Issue with the LSP package code during deploy rollback.
CSCwh28779	Unable to save intrusion policy after upgrade to 7.x as the name exceeds 40 characters
CSCwh30276	Rule update filter in Intrusion policy shows inconsistent results

For Assistance

Upgrade Guides

In 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 19: Upgrade Guides

Platform	Upgrade Guide	Link
Management center	Management center version you are <i>currently</i> running.	https://www.cisco.com/go/fmc-upgrade
Threat defense with management center	Management center version you are <i>currently</i> running.	https://www.cisco.com/go/ftd-fmc-upgrade
Threat defense with device manager	Threat defense version you are <i>currently</i> 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 20: 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 <i>Image Management</i> chapter.	https://www.cisco.com/go/firepower9300-config
FXOS for the Firepower 1000/2100 and Secure Firewall 3100/4200	Troubleshooting guide, in the <i>Reimage Procedures</i> 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-74-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](#)

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

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

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

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

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

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

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

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

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

© 2023–2024 Cisco Systems, Inc. All rights reserved.