Cisco Secure Firewall Threat Defense Release Notes, Version 7.3.x

First Published: 2022-11-29

Last Modified: 2024-09-06

Cisco Secure Firewall Threat Defense Release Notes

This document contains release information for:

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

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

Release Dates

Table 1: Version 7.3 Dates

Version	Build	Date	Platforms
7.3.1.2	79	2024-05-09	All
7.3.1.1	83	2023-08-24	All
7.3.1	19	2023-03-14	All
7.3.0	69	2022-11-29	All

Compatibility

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

For compatibility information, see:

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

Features

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

Upgrade Impact

A feature has upgrade impact if upgrading and deploying can cause the system *to process traffic or otherwise act differently without any other action on your part*. This is especially common with new threat detection and application identification capabilities. A feature can also have upgrade impact if upgrading requires that you take action before or after upgrade to avoid an undesirable outcome; for example, if you must change a configuration. Having to enable a new setting or deploy a policy post-upgrade to take advantage of a new feature does not count as upgrade impact.

The feature descriptions below include upgrade impact where appropriate. For a more complete list of features with upgrade impact by version, see Upgrade Impact Features, on page 29.

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 7.3.1

Table 2: Management Center Features in Version 7.3.1.1

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

Table 3: Management Center Features in Version 7.3.1

Feature	Minimum Management Center	Minimum Threat Defense	Details
Secure Firewall 3105.	7.3.1	7.3.1	We introduced the Secure Firewall 3105.

Management Center Features in Version 7.3.0

Table 4: Management Center Features in Version 7.3.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Platform			
Management center virtual 300 for KVM.	7.3.0	Any	We introduced the FMCv300 for KVM. The FMCv300 can manage up to 300 devices. High availability is supported.
Network modules for the Firepower 4100.	7.3.0	7.3.0	We introduced these network modules for the Firepower 4100: • 2-port 100G network module (FPR4K-NM-2X100G) Supported platforms: Firepower 4112, 4115, 4125, 4145

Feature	Minimum Management Center	Minimum Threat Defense	Details
ISA 3000 System LED support for shutting down.	7.3.0	7.0.5 7.3.0	Support returns for this feature. When you shut down the ISA 3000, the System LED turns off. Wait at least 10 seconds after that before you remove power from the device. This feature was introduced in Version 7.0.5 but was temporarily deprecated in Version 7.1–7.2.
New compute shapes for threat defense virtual and management center virtual for OCI.	7.3.0	7.3.0	Threat defense virtual for OCI adds support for the following compute shapes: • Intel VM.DenseIO2.8 • Intel VM.StandardB1.4 • Intel VM.StandardB1.8 • Intel VM.Standard1.4 • Intel VM.Standard1.8 • Intel VM.Standard3.Flex • Intel VM.Optimized3.Flex • AMD VM.Standard.E4.Flex Management center virtual for OCI adds support for the following compute shapes: • Intel VM.StandardB1.4 • Intel VM.Standard3.Flex • Intel VM.Optimized3.Flex • AMD VM.Standard.E4.Flex Note that the VM.Standard2.4 and VM.Standard2.8 compute shapes reached end of orderability in February 2022. If you are deploying Version 7.3+, we recommend one of the above compute shapes. For information on compatible compute shapes, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.

Interfaces

Feature	Minimum Management Center	Minimum Threat Defense	Details
IPv6 support for virtual appliances.	7.3.0	7.3.0	Threat defense virtual and management center virtual now support IPv6 in the following environments: • AWS • Azure • OCI • KVM • VMware For more information, see Cisco Secure Firewall Threat Defense Virtual Getting Started Guide and Cisco Secure Firewall Management Center Virtual Getting Started Guide.
Loopback interface support for VTIs.	7.3.0	7.3.0	You can now configure a loopback interface for redundancy of static and dynamic VTI VPN tunnels. A loopback interface is a software interface that emulates a physical interface. It is reachable through multiple physical interfaces with IPv4 and IPv6 addresses. New/modified screens: **Devices** > **Device Management** > **Device** > **Interfaces** > **Add Interfaces** > **Add Loopback Interface** For more information, see Configure Loopback Interfaces in the device configuration guide.
Redundant manager access data interface.	7.3.0	7.3.0	When you use a data interface for manager access, you can configure a secondary data interface to take over management functions if the primary interface goes down. The device uses SLA monitoring to track the viability of the static routes and an ECMP zone that contains both interfaces so management traffic can use both interfaces. New/modified screens: • **Devices** > **Device Management** > **Device** > **Management** • **Devices** > **Device Management** > **Device** > **Interfaces** > **Manager Access** For more information, see Configure a Redundant Manager Access Data Interface in the device configuration guide.

Feature	Minimum Management Center	Minimum Threat Defense	Details
IPv6 DHCP.	7.3.0	7.3.0	We now support the following features for IPv6 addressing: • DHCPv6 Address client: Threat defense obtains an IPv6 global address and optional default route from the DHCPv6 server. • DHCPv6 Prefix Delegation client: Threat defense obtains delegated prefix(es) from a DHCPv6 server. It can then use these prefixes to configure other threat defense interface addresses so that StateLess Address Auto Configuration (SLAAC) clients can autoconfigure IPv6 addresses on the same network. • BGP router advertisement for delegated prefixes. • DHCPv6 stateless server: Threat defense provides other information such as the domain name to SLAAC clients when they send Information Request (IR) packets to threat defense. Threat defense only accepts IR packets and does not assign addresses to the clients. New/modified screens: • **Devices** > **Device Management** > **Device** > **Interfaces** > **Interface** > **IPv6** > **DHCP** • **Objects** > **Object Management** > **DHCP IPv6 Pool** New/modified CLI commands: **show bgp ipv6 unicast**, **show ipv6 dhcp**, **show ipv6 general-prefix** For more information, see Configure the IPv6 Prefix Delegation Client, BGP, and Configure the DHCPv6 Stateless Server in the device configuration guide.
Paired proxy VXLAN for the threat defense virtual for the Azure Gateway Load Balancer.	7.3.0	7.3.0	You can configure a paired proxy mode VXLAN interface for threat defense virtual for Azure for use with the Azure Gateway Load Balancer. The device defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy. New/modified screens: **Devices** > **Device Management** > **Device** > **Interfaces** > **Add Interfaces** > **VNI Interface** For more information, see Configure VXLAN Interfaces in the device configuration guide.
High Availability/Scalability			

Feature	Minimum Management Center	Minimum Threat Defense	Details
High availability for management center virtual for KVM.	7.3.0	Any	We now support high availability for management center virtual for KVM. In a threat defense deployment, you need two identically licensed management centers, as well as one threat defense entitlement for each managed device. For example, to manage 10 devices with an FMCv10 high availability pair, you need two FMCv10 entitlements and 10 threat defense entitlements. If you are managing Classic devices only (NGIPSv or ASA FirePOWER), you do not need FMCv entitlements. Platform restrictions: Not supported with FMCv2 For more information, see the Cisco Secure Firewall Management Center Virtual Getting Started Guide, as well as High Availability in the administration guide.
Clustering for threat defense virtual for Azure.	7.3.0	7.3.0	You can now configure clustering for up to 16 nodes with threat defense virtual for Azure. New/modified screens: **Devices** > **Device Management** For more information, see Clustering for Threat Defense Virtual in a Public Cloud in the device configuration guide.
Autoscale for threat defense virtual for Azure Gateway Load Balancers.	7.3.0	7.3.0	We now support autoscale for threat defense virtual for Azure Gateway Load Balancers. For more information, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.
Back up and restore device clusters.	7.3.0	Any	You can now use the management center to back up device clusters, except in the public cloud (threat defense virtual for AWS). To restore, use the device CLI. New/modified screens: **System** > **Tools** > **Backup/Restore** > **Managed Device Backup** New/modified commands: **restore remote-manager-backup** For more information, see Backup/Restore in the administration guide.
Remote Access VPN			

Feature	Minimum Management Center	Minimum Threat Defense	Details
RA VPN dashboard.	7.3.0	Any	We introduced a remote access VPN (RA VPN) dashboard that allows you to monitor real-time data from active RA VPN sessions on the devices. So that you can quickly determine problems related to user sessions and mitigate the problems for your network and users, the dashboard provides: • Visualization of active user sessions based on their location. • Detailed information about the active user sessions. • Mitigation of user session problems by terminating sessions, if required. • Distribution of active user sessions per device, encryption type, Secure Client version, operating system, and connection profile. • Device identity certificate expiration details of the devices. New/modified screens: **Overview** > **Dashboards** > **Remote Access VPN** For more information, see Dashboards in the administration guide.
Encrypt RA VPN connections with TLS 1.3.	7.3.0	7.3.0	You can now use TLS 1.3 to encrypt RA VPN connections with the following ciphers: • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 Use the threat defense platform settings to set the TLS version: **Devices** > **Platform Settings** > **Add/Edit Threat Defense Settings Policy** > **SSL** > **TLS Version**. This feature requires Cisco Secure Client, Release 5 (formerly known as the AnyConnect Secure Mobility Client). For more information, see Configure SSL Settings in the device configuration guide.
Site to Site VPN			
Packet tracer in the site-to-site VPN dashboard.	7.3.0	Any	We added packet tracer capabilities to the site-to-site VPN dashboard, to help you troubleshoot VPN tunnels between devices. Open the dashboard by choosing **Overview** > **Dashboards** > **Site to Site VPN**. Then, click **View** (👁) next to the tunnel you want to investigate, and **Packet Tracer** in the side pane that appears. For more information, see Monitoring the Site-to-Site VPNs in the device configuration guide.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Support for dynamic VTIs with site-to-site VPN.	7.3.0	7.3.0	We now support dynamic virtual tunnel interfaces (VTI) when you configure a route-based site-to-site VPN in a hub and spoke topology. Previously, you could use only a static VTI. This makes it easier to configure large hub and spoke deployments. A single dynamic VTI can replace several static VTI configurations on the hub. And, you can add new spokes to a hub without changing the hub configuration. New/modified screens: We updated the options when configuring hub-node endpoints for a route-based hub-and-spoke site-to-site VPN topology. For more information, see Configure Endpoints for a Hub and Spoke Topology in the device configuration guide.
Improved Umbrella SIG integration.	7.3.0	7.3.0	You can now easily deploy IPsec IKEv2 tunnels between a threat defense device and the Umbrella Secure Internet Gateway (SIG), which allows you to forward all internet-bound traffic to Umbrella for inspection and filtering. To configure and deploy these tunnels, create a SASE topology, a new type of static VTI-based site-to-site VPN topology: **Devices** > **VPN** > **Site To Site** > **SASE Topology**. For more information, see Deploy a SASE Tunnel on Umbrella in the device configuration guide.
Routing			
Configure BFD for BGP from the management center web interface.	7.3.0	Any	**Upgrade impact. Redo related FlexConfigs after upgrade.** You can now use the management center web interface to configure bidirectional forwarding detection (BFD) for BGP. Note that you can only enable BFD on interfaces belonging to virtual routers. If you have an existing BFD FlexConfig and redo your configurations in the web interface, you cannot deploy until you remove the deprecated FlexConfigs. New/modified screens: • **Devices** > **Device Management** > **Device** > **Routing** > **BFD** • **Objects** > **Object Management** > **BFD Template** • When configuring BGP neighbor settings, we replaced the **BFD Failover** check box with a menu where you choose the BFD type: single hop, multi hop, auto detect, or none (disabled). For upgraded management centers, **auto-detect hop** is selected if the old **BFD Failover** option was enabled and **none** is selected if the old option was disabled. For more information, see Bidirectional Forwarding Detection Routing in the device configuration guide.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Support for IPv4 and IPv6 OSPF routing for VTIs.	7.3.0	7.3.0	We now support IPv4 and IPv6 OSPF routing for VTI interfaces. New/modified pages: You can add VTI interfaces to an OSPF routing process on **Devices** > **Device Management** > **Device** > **Routing** > **OSPF/OSFPv3**. For more information, see OSPF and Additional Configurations for VTI in the device configuration guide.
Support for IPv4 EIGRP routing for VTIs.	7.3.0	7.3.0	We now support IPv4 EIGRP routing for VTI interfaces. New/modified screens: You can define a VTI as the static neighbor for an EIGRP routing process, configure a VTI's interface-specific EIGRP routing properties. and advertise a VTI's summary address on **Devices** > **Device Management** > **Device** > **Routing** > **EIGRP**. For more information, see EIGRP and Additional Configurations for VTI in the device configuration guide.
More network service groups for policy-based routing.	7.3.0	7.3.0	You can now configure up to 1024 network service groups (application groups in an extended ACL for use in policy-based routing). Previously, the limit was 256.
Support for multiple next-hops while configuring policy-based routing forwarding actions.	7.3.0	7.1	You can now configure multiple next-hops while configuring policy-based routing forwarding actions. When traffic matches the criteria for the route, the system attempts to forward traffic to the IP addresses in the order you specify, until it succeeds. New/modified screens: We added several options when you select **IP Address** from the **Send To** menu on **Devices** > **Device Management** > **Device** > **Routing** > **Policy Based Routing** > **Add Policy Based Route** > **Add Match Criteria and Egress Interface**. For more information, see Configure Policy-Based Routing Policy in the device configuration guide.
Upgrade			
Choose and direct-download upgrade packages to the management center from Cisco.	7.3..x only	Any	You can now choose which threat defense upgrade packages you want to direct download to the management center. Use the new **Download Updates** sub-tab on > **Updates** > **Product Updates**. Other version restrictions: this feature is replaced by an improved package management system in Version 7.2.6/7.4.1. See: Download Upgrade Packages with the Management Center

Feature	Minimum Management Center	Minimum Threat Defense	Details
Upload upgrade packages to the management center from the threat defense wizard.	7.3.x only	Any	You now use the wizard to upload threat defense upgrade packages or specify their location. Previously (depending on version), you used **System** (⚙) > **Updates** or **System** (⚙) > **Product Upgrades**. Other version restrictions: this feature is replaced by an improved package management system in Version 7.2.6/7.4.1. See: Upgrade Threat Defense
Auto-upgrade to Snort 3 after successful threat defense upgrade is no longer optional.	7.3.0	Any	**Upgrade impact. All eligible devices upgrade to Snort 3 when you deploy.** When you upgrade threat defense to Version 7.3+, you can no longer disable the **Upgrade Snort 2 to Snort 3** option. After the software upgrade, all eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. Although you can switch individual devices back, Snort 2 will be deprecated in a future release and we strongly recommend you stop using it now. For devices that are ineligible for auto-upgrade because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For migration assistance, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Combined upgrade and install package for Secure Firewall 3100.	7.3.0	7.3.0	**Reimage Impact.** In Version 7.3, we combined the threat defense install and upgrade package for the Secure Firewall 3100, as follows: • Version 7.1–7.2 install package: cisco-ftd-fp3k.*version*.SPA • Version 7.1–7.2 upgrade package: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • Version 7.3+ combined package: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar Although you can upgrade threat defense without issue, you cannot reimage from older threat defense and ASA versions directly to threat defense Version 7.3+. This is due to a ROMMON update required by the new image type. To reimage from those older versions, you must "go through" ASA 9.19+, which is supported with the old ROMMON but also updates to the new ROMMON. There is no separate ROMMON updater. To get to threat defense Version 7.3+, your options are: • Upgrade from threat defense Version 7.1 or 7.2 — use the normal upgrade process. See the appropriate Upgrade Guide. • Reimage from threat defense Version 7.1 or 7.2 — reimage to ASA 9.19+ first, then reimage to threat defense Version 7.3+. See *Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100* and then *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100* in the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide. • Reimage from ASA 9.17 or 9.18 — upgrade to ASA 9.19+ first, then reimage to threat defense Version 7.3+. See the Cisco Secure Firewall ASA Upgrade Guide and then *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100* in the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide. • Reimage from threat defense Version 7.3+ — use the normal reimage process. See *Reimage the System with a New Software Version* in the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense.
Access Control and Threat Detection			

Feature	Minimum Management Center	Minimum Threat Defense	Details
SSL policy renamed to decryption policy.	7.3.0	Any	We renamed the SSL policy to the decryption policy. We also added a policy wizard that makes it easier to create and configure decryption policies, including creating initial rules and certificates for inbound and outbound traffic. New/modified screens: • Add or edit a decryption policy: **Policies** > **Access Control** > **Decryption**. • Use a decryption policy: **Decryption Policy Settings** in an access control policy's advanced settings. For more information, see Decryption Policies in the device configuration guide.
Improvements to TLS server identity discovery with Snort 3 devices.	7.3.0	7.3.0	We now support improved performance and inspection with the TLS server identity discovery feature, which allows you to handle traffic encrypted with TLS 1.3 with information from the server certificate. Although we recommend you leave it enabled, you can disable this feature using the new **Enable adaptive TLS server identity probe** option in the decryption policy's advanced settings. For more information, see TLS 1.3 Decryption Best Practices in the device configuration guide.

Feature	Minimum Management Center	Minimum Threat Defense	Details
URL filtering using cloud lookup results only.	7.3.0	7.3.0	When you enable (or re-enable) URL filtering, the management center automatically queries Cisco for URL category and reputation data and pushes the dataset to managed devices. You now have more options on how the system uses this dataset to filter web traffic. To do this, we replaced the **Query Cisco Cloud for Unknown URLs** options with three new options: • **Local Database Only**: Uses the local URL dataset only. Use this option if you do not want to submit your uncategorized URLs (category and reputation not in the local dataset) to Cisco, for example, for privacy reasons. However, note that connections to uncategorized URLs do *not* match rules with category or reputation-based URL conditions. You cannot assign categories or reputations to URLs manually. For upgraded management centers, this option is enabled if the old **Query Cisco Cloud for Unknown URLs** was disabled. • **Local Database and Cisco Cloud**: Uses the local dataset when possible, which can make web browsing faster. When users browse to an URL whose category and reputation is not in the local dataset or a cache of previously accessed websites, the system submits it to the cloud for threat intelligence evaluation and adds the result to the cache. For upgraded management centers, this option is enabled if the old **Query Cisco Cloud for Unknown URLs** option was enabled. • **Cisco Cloud Only**: Does not use the local dataset. When users browse to an URL whose category and reputation is not in a local cache of previously accessed websites, the system submits it to the cloud for threat intelligence evaluation and adds the result to the cache. This option guarantees the most up-to-date category and reputation information. This option is the default on new and reimaged Version 7.3+ management centers. Note that it also requires threat defense Version 7.3+. If you enable this option, devices running earlier versions use the **Local Database and Cisco Cloud** option. New/modified screens: **Integration** > **Other Integrations** > **Cloud Services** > **URL Filtering** For more information, see URL Filtering Options in the device configuration guide.
Detect HTTP/3 and SMB over QUIC using EVE (Snort 3 only).	7.3.0	7.3.0 with Snort 3	Snort 3 devices can now use the encrypted visibility engine (EVE) to detect HTTP/3 and SMB over QUIC. You can then create rules to handle traffic based on these applications. For more information, see Encrypted Visibility Engine in the device configuration guide.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Generate IoC events based on unsafe client applications detected by EVE (Snort 3 only).	7.3.0	7.3.0 with Snort 3	Snort 3 devices can now generate indications of compromise (IoC) connection events based unsafe client applications detected by the encrypted visibility engine (EVE). These connection events have a Encrypted Visibility Threat Confidence of Very High. • View IoCs in the event viewer: **Analysis** > **Hosts/Users** > **Indications of Compromise** • View IoCs in the network map: **Analysis** > **Hosts** > **Indications of Compromise** • View IoC information in connection events: **Analysis** > **Connections** > **Events** > **Table View of Connection Events** > **IOC/Encrypted Visibility columns** For more information, see Encrypted Visibility Engine in the device configuration guide.
Improved JavaScript inspection for Snort 3 devices.	7.3.0	7.3.0 with Snort 3	We improved JavaScript inspection, which is done by normalizing the JavaScript and matching rules against the normalized content. The normalizer introduced in Version 7.2 now allows you to inspect within the unescape, decodeURI, and decodeURIComponent functions: %XX, %uXXXX, \uXX, \u{XXXX}\xXX, decimal code point, and hexadecimal code point. It also removes plus operations from strings and concatenates them. For more information, see HTTP Inspect Inspector in the Snort 3 Inspector Reference, as well as the Cisco Secure Firewall Management Center Snort 3 Configuration Guide.
Nested rule groups, including MITRE ATT&CK, in Snort 3 intrusion policies.	7.3.0	7.0 with Snort 3	You can now nest rule groups in a Snort 3 intrusion policy. This allows you to view and handle traffic in a more granular fashion; for example, you might group rules by vulnerability type, target system, or threat category. You can create custom nested rule groups and change the security level and rule action per rule group. We also group system-provided rules in a Talos-curated MITRE ATT&CK framework, so you can act on traffic based on those categories. New/modified screens: • View and use rule groups: **Policies** > **Intrusion** > **Edit Snort 3 Version** • View rule group information in the classic event view: **Analysis** > **Intrusion** > **Events** > **Table View of Intrusion Events** > **Rule Group and MITRE ATT&CK columns** • View rule group information in the unified event view: **Analysis** > **Unified Events** > **Rule Group and MITRE ATT&CK columns** For more information, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Access control rule conflict analysis.	7.3.0	Any	You can now enable rule conflict analysis to help identify redundant rules and objects, and shadowed rules that cannot be matched due to previous rules in the policy. For more information, see Analyzing Rule Conflicts and Warnings in the device configuration guide.
Event Logging and Analysis			
NetFlow support for Snort 3 devices.	7.3.0	7.3.0 with Snort 3	**Upgrade impact. Devices may begin processing NetFlow records.** Snort 3 devices now can consume NetFlow records (IPv4 and IPv6, NetFlow v5 and v9). Previously, only Snort 2 devices did this. After upgrade, if you have an existing NetFlow exporter and NetFlow rule configured in the network discovery policy, Snort 3 devices may begin processing NetFlow records, generating NetFlow connection events, and adding host and application protocol information to the database based on NetFlow data. For more information, see Network Discovery Policies in the device configuration guide.
Integrations			
New remediation module for integration with the Cisco ACI Endpoint Update App	7.3.0	Any	We introduced a new Cisco ACI Endpoint remediation module. To use it, you must remove the old module then add and configure the new one. This new module can: • Quarantine endpoints in an endpoint security group (ESG) deployment. • Allow traffic from a quarantined endpoint to a Layer 3 outside network (L3Out) for monitoring and analysis. • Run in audit-only mode, where it notifies you instead of quarantining. For more information, see APIC/Secure Firewall Remediation Module 3.0 in the device configuration guide.
Health Monitoring			
Cluster health monitor settings in the management center web interface.	7.3.0	Any	You can now use the management center web interface to edit cluster health monitor settings. If you configured these settings with FlexConfig in a previous version, the system allows you to deploy, but also warns you to redo your configurations—the FlexConfig settings take precedence. New/modified screens: **Devices > Device Management > Edit Cluster > Cluster Health Monitor Settings** For more information, see Edit Cluster Health Monitor Settings in the device configuration guide.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Improved health monitoring for device clusters.	7.3.0	Any	We added cluster dashboards to the health monitor where you can view overall cluster status, load distribution metrics, performance metrics, cluster control link (CCL) and data throughput, and so on. To view the dashboard for each cluster, choose **System** (⚙) > **Health** > **Monitor**, then click the cluster. For more information, see Cluster Health Monitor in the administration guide.
Monitor fan speed and temperature for the power supply on the hardware management center.	7.3.0	Any	We added the Hardware Statistics health module that monitors fan speed and temperature for the power supply on the hardware management center. The upgrade process automatically adds and enables this module. After upgrade, apply the policy. To enable or disable the module and set threshold values, edit the management center health policy on **System** (⚙) > **Health** > **Policy**. To view health status, create a custom health dashboard: **System** (⚙) > **Health** > **Monitor** > **Firewall Management Center** > **Add/Edit**. Select the **Hardware Statistics** metric group, then select the metric you want. You can also view module status on the health monitor's **Home** page and in the management center's alert summary (as **Hardware Alarms** and **Power Supply**). You can configure external alert responses and view health events based on module status. For more information, see Hardware Statistics on Management Center in the administration guide.
Monitor temperature and power supply for the Firepower 4100/9300.	7.3.0	7.3.0	We added the Chassis Environment Status health module to monitor the temperature and power supply on a Firepower 4100/9300 chassis. The upgrade process automatically adds and enables these modules in all device health policies. After upgrade, apply health policies to Firepower 4100/9300 chassis to begin monitoring. To enable or disable this module and set threshold values, edit the management center health policy: **System** (⚙) > **Health** > **Policy** > **Device Policy**. To view health status, create a custom health dashboard: **System** (⚙) > **Health** > **Monitor** > **Select Device** > **Add/Edit Dashboard** > **Custom Correlation Group**. Select the **Hardware/Environment Status** metric group, then select the **Thermal Status** metric to view temperature or select any of the **Power Supply** options to view power supply status. You can also view module status on the health monitor's **Home** page and in each device's alert summary. You can configure external alert responses and view health events based on module status. For more information, see Hardware/Environment Status Metrics in the administration guide.
Licensing			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Changes to license names and support for the Carrier license.	7.3.0	Any	We renamed licenses as follows: • Base is now Essentials • Threat is now IPS • Malware is now Malware Defense • RA VPN/AnyConnect License is now Cisco Secure Client • AnyConnect Plus is now Secure Client Advantage • AnyConnect Apex is now Secure Client Premier • AnyConnect Apex and Plus is now Secure Client Premier and Advantage • AnyConnect VPN Only is now Secure Client VPN Only In addition, you can now apply the Carrier license, which allows you to configure GTP/GPRS, Diameter, SCTP, and M3UA inspections. New/modified screens: **System** (⚙) > **Licenses** > **Smart Licenses** For more information, see Licenses in the administration guide.
Updated internet access requirements for Smart Licensing.	7.3.0	Any	**Upgrade impact. The system connects to new resources.** When communicating with the Cisco Smart Software Manager, the management center now connects to smartreceiver.cisco.com instead of tools.cisco.com.
Administration			
Migrate configurations from FlexConfig to web interface management.	7.3.0	Feature dependent	You can now easily migrate these configurations from FlexConfig to web interface management: • ECMP zones, supported in the Version 7.1+ web interface • EIGRP routing, supported in the Version 7.2+ web interface • VXLAN interfaces, supported in the Version 7.2+ web interface After you migrate, you cannot deploy until you remove the deprecated FlexConfigs. New/modified screens: **Devices** > **FlexConfig** > **Edit FlexConfig Policy** > **Migrate Config** For more information, see Migrating FlexConfig Policies in the device configuration guide.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Automatic VDB downloads.	7.3.0	Any	The initial setup on the management center schedules a weekly task to download the latest available software updates, which now includes the latest vulnerability database (VDB). We recommend you review this weekly task and adjust if necessary. Optionally, schedule a new weekly task to actually update the VDB and deploy configurations.
			New/modified screens: The **Vulnerability Database** check box is now enabled by default in the system-created **Weekly Software Download** scheduled task.
			For more information, see Vulnerability Database Update Automation in the administration guide.
Install any VDB.	7.3.0	Any	Starting with VDB 357, you can now install any VDB as far back as the baseline VDB for that management center.
			After you update the VDB, deploy configuration changes. If you based configurations on vulnerabilities, application detectors, or fingerprints that are no longer available, examine those configurations to make sure you are handling traffic as expected. Also, keep in mind a scheduled task to update the VDB can undo a rollback. To avoid this, change the scheduled task or delete any newer VDB packages.
			New/modified screens: On **System** (⚙) > **Updates** > **Product Updates** > **Available Updates**, if you upload an older VDB, a new **Rollback** icon appears instead of the **Install** icon.
			For more information, see Update the Vulnerability Database in the administration guide.
Usability, Performance, and Troubleshooting			

Feature	Minimum Management Center	Minimum Threat Defense	Details

New how-to walkthroughs.	7.3.0	Feature dependent	We added these how-tos:
			
			• Renew a certificate using manual re-enrollment.
			
			• Renew a certificate using Self-signed, SCEP, or EST enrollment.
			
			• Configure LDAP attribute map for remote access VPN.
			
			• Add SAML Single Sign-On server object.
			
			• Collect packet capture for threat defense device.
			
			• Collect packet trace to troubleshoot threat defense device.
			
			• Configure Dynamic Access Policy for remote access VPN.
			
			    • Create a Dynamic Access Policy.
			
			    • Create a Dynamic Access Policy record.
			
			    • Associate Dynamic Access Policy with remote access VPN.
			
			To launch a how-to, choose **System** (⚙) > **How-Tos**.

New access control policy user interface is now the default.	7.3.0	Any	The access control policy user interface introduced in Version 7.2 is now the default interface. The upgrade switches you, but you can switch back.
Maximum objects per match criteria per access control rule is now 200.	7.3.0	Any	We increased the objects per match criteria in a single access control rule from 50 to 200. For example, you can now use up to 200 network objects in a single access control rule.
Filter devices by version.	7.3.0	Any	You can now filter devices by version on **Devices** > **Device Management**.
Better status emails for scheduled tasks.	7.3.0	Any	Email notifications for scheduled tasks are now sent when the task completes—whether success or failure—instead of when the task begins. This means that they can now indicate whether the task failed or succeeded. For failures, they include the reason for the failure and remediations to fix the issue.
Performance profile for CPU core allocation on the Firepower 4100/9300 and threat defense virtual.	7.3.0	7.3.0	You can adjust the percentage of system cores assigned to the data plane and Snort to adjust system performance. The adjustment is based on your relative use of VPN and intrusion policies. If you use both, leave the core allocation to the default values. If you use the system primarily for VPN (without applying intrusion policies), or as an IPS (with no VPN configuration), you can skew the core allocation to the data plane (for VPN) or Snort (for intrusion inspection). We added the **Performance Profile** page to the platform settings policy. For more information, see Configure the Performance Profile in the device configuration guide.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cisco Success Network telemetry.	7.3.0	Any	For telemetry changes, see Cisco Success Network Telemetry Data Collected from Cisco Secure Firewall Management Center, Version 7.3.x.
Management Center REST API			
Management center REST API.	7.3.0	Feature dependent	For information on changes to the management center REST API, see What's New in 7.3 in the API quick start guide.
Deprecated Features			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Temporarily deprecated features.	7.3.0	Feature dependent	

Feature	Minimum Management Center	Minimum Threat Defense	Details
			Although upgrading to Version 7.3 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+.

From Version 7.2.3+, upgrading removes:

- Firepower 1010E.. You cannot upgrade a Version 7.2.x Firepower 1010E to Version 7.3, and you should not reimage there either. If you have a Firepower 1010E device running Version 7.3, reimage to a supported release. Do not use a Version 7.2.3 or Version 7.3.0 management center to manage the Firepower 1010E. Instead, use a Version 7.2.3.1+ or Version 7.3.1.1+ management center.

From Version 7.2.4+, upgrading removes:

- Access control performance improvements (object optimization). Upgrade impact.

From Version 7.2.5+, upgrading removes:

- Management center detects interface sync errors. Upgrade impact.

From Version 7.2.6+, upgrading removes:

- Updated web analytics provider. Upgrade impact.
- Reduced "false failovers" for threat defense high availability.)
- 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.
- Health alerts for NTP sync issues.
- 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.

Feature	Minimum Management Center	Minimum Threat Defense	Details
			• 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.
Support ends: Firepower 4110, 4120, 4140, 4150.	—	7.3.0	You cannot run Version 7.3+ on the Firepower 4110, 4120, 4140, or 4150.
Support ends: Firepower 9300: SM-24, SM-36, SM-44 modules.	—	7.3.0	You cannot run Version 7.3+ on the Firepower 9300 with SM-24, SM-36, or SM-44 modules.
Deprecated: YouTube EDU content restriction for Snort 2 devices.	7.3.0	Any	You can no longer enable YouTube EDU content restriction in new or existing access control rules. Your existing YouTube EDU rules will keep working, and you can edit those rules to disable YouTube EDU. Note that this is a Snort 2 feature that is not available for Snort 3. You should redo your configurations after upgrade.
Deprecated: Cluster health monitor settings with FlexConfig.	7.3.0	Any	You can now edit cluster health monitor settings from the management center web interface. If you do this, the system allows you to deploy but also warns you that any existing FlexConfig settings take precedence. You should redo your configurations after upgrade.
Deprecated: BFD for BGP with FlexConfig.	7.3.0	Any	You can now configure bidirectional forwarding detection (BFD) for BGP routing from the management center web interface. If you do this, you cannot deploy until you remove any deprecated FlexConfigs. You should redo your configurations after upgrade.
Deprecated: ECMP zones with FlexConfig.	7.3.0	Any	You can now easily migrate EMCP zone configurations from FlexConfig to web interface management. After you migrate, you cannot deploy until you remove any deprecated FlexConfigs. You should redo your configurations after upgrade.
Deprecated: VXLAN interfaces with FlexConfig.	7.3.0	Any	You can now easily migrate VXLAN interface configurations from FlexConfig to web interface management. After you migrate, you cannot deploy until you remove any deprecated FlexConfigs.

Device Manager Features in Version 7.3.x

Table 5: Device Manager Features in Version 7.3.x

Feature	Description
Platform Features	
Secure Firewall 3105.	We introduced the Secure Firewall 3105. Minimum threat defense: Version 7.3.1
Network modules for the Secure Firewall 4100.	We introduced these network modules for the Firepower 4100: • 2-port 100G network module (FPR4K-NM-2X100G) Supported platforms: Firepower 4112, 4115, 4125, 4145
ISA 3000 System LED support for shutting down.	Support returns for this feature. When you shut down the ISA 3000, the System LED turns off. Wait at least 10 seconds after that before you remove power from the device. This feature was introduced in Version 7.0.5 but was temporarily deprecated in Versions 7.1–7.2.

New compute shapes for threat defense virtual for OCI.	Threat defense virtual for OCI adds support for the following compute shapes:
	
	   • Intel VM.DenseIO2.8
	
	   • Intel VM.StandardB1.4
	
	   • Intel VM.StandardB1.8
	
	   • Intel VM.Standard1.4
	
	   • Intel VM.Standard1.8
	
	   • Intel VM.Standard3.Flex
	
	   • Intel VM.Optimized3.Flex
	
	   • AMD VM.Standard.E4.Flex
	
	Note that the VM.Standard2.4 and VM.Standard2.8 compute shapes reached end of orderability in February 2022. If you are deploying Version 7.3+, we recommend a different compute shape.
	
	See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide

Support ends: Firepower 4110, 4120, 4140, 4150.	You cannot run Version 7.3+ on the Firepower 4110, 4120, 4140, or 4150.
Support ends: Firepower 9300: SM-24, SM-36, SM-44 modules.	You cannot run Version 7.3+ on the Firepower 9300 with SM-24, SM-36, or SM-44 modules.

Feature	Description
No support for Firepower 1010E (temporary).	The Firepower 1010E, which was introduced in Version 7.2.3, does not support Version 7.3. Support returns in Version 7.4.
	You cannot upgrade a Version 7.2.x Firepower 1010E to Version 7.3, and you should not reimage there either. If you have a Firepower 1010E device running Version 7.3, reimage to a supported release.
Firewall and IPS Features	
TLS 1.3 support in SSL decryption policies, and configurable behavior for undecryptable connections.	**Upgrade impact.**
	You can configure SSL decryption rules for TLS 1.3 traffic. TLS 1.3 support is available when using Snort 3 only. You can also configure non-default behavior for undecryptable connections. If you are using Snort 3, upon upgrade, TLS 1.3 is automatically selected for any rules that have all SSL/TLS versions selected; otherwise, TLS 1.3 is not selected. The same behavior happens if you switch from Snort 2 to Snort 3.
	We added TLS 1.3 as an option on the advanced tab of the add/edit rule dialog box. We also redesigned the SSL decryption policy settings to include the ability to enable TLS 1.3 decryption, and to configure undecryptable connection actions.
	See: Advanced Criteria for SSL Decryption Rules and Configure Advanced and Undecryptable Traffic Settings
Refined URL filtering lookup.	You can now explicitly set how URL filtering lookups occur. You can select to use the local URL database only, both the local database and cloud lookup, or cloud lookup only. We augmented the URL Filtering system setting options.
	See: Configuring URL Filtering Preferences
Interface Features	
IPv6 support for virtual appliances.	Threat defense virtual now supports IPv6 in the following environments:
	• AWS
	• Azure
	• KVM
	• VMware
	See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
DHCPv6 Client.	You can now obtain an IPv6 address from DHCPv6.
	New/modified screens: **Device** > **Interfaces** > **Edit Interface** > **Advanced**
	See: Configure Advanced Interface Options
Administrative and Troubleshooting Features	

Feature	Description
Automatically update CA bundles.	**Upgrade impact. The system connects to Cisco for something new.** The local CA bundle contains certificates to access several Cisco services. The system now automatically queries Cisco for new CA certificates at a daily system-defined time. Previously, you had to upgrade the software to update CA certificates. You can use the CLI to disable this feature. New/modified CLI commands: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** Version restrictions: This feature is included in Versions 7.0.5+, 7.1.0.3+, and 7.2.4+. It is not supported in earlier 7.0, 7.1, or 7.2 releases. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco. See: Cisco Secure Firewall Threat Defense Command Reference
Skip Certificate Authority checking for trusted certificates.	You can skip the check if you need to install a local CA certificate as the trusted CA certificate. We added the **Skip CA Certificate Check** option when uploading trusted CA certificates.

Feature	Description
Combined upgrade and install package for Secure Firewall 3100.	**Reimage Impact.** In Version 7.3, we combined the threat defense install and upgrade package for the Secure Firewall 3100, as follows: • Version 7.1–7.2 install package: cisco-ftd-fp3k.*version*.SPA • Version 7.1–7.2 upgrade package: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • Version 7.3+ combined package: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar Although you can upgrade threat defense without issue, you cannot reimage from older threat defense and ASA versions directly to threat defense Version 7.3+. This is due to a ROMMON update required by the new image type. To reimage from those older versions, you must "go through" ASA 9.19+, which is supported with the old ROMMON but also updates to the new ROMMON. There is no separate ROMMON updater. To get to threat defense Version 7.3+, your options are: • Upgrade from threat defense Version 7.1 or 7.2 — use the normal upgrade process. See the appropriate Upgrade Guide. • Reimage from threat defense Version 7.1 or 7.2 — reimage to ASA 9.19+ first, then reimage to threat defense Version 7.3+. See *Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100* and then *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100* in the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide. • Reimage from ASA 9.17 or 9.18 — upgrade to ASA 9.19+ first, then reimage to threat defense Version 7.3+. See the Cisco Secure Firewall ASA Upgrade Guide and then *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100* in the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide. • Reimage from threat defense Version 7.3+ — use the normal reimage process. See *Reimage the System with a New Software Version* in the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense.

Feature	Description
Threat Defense REST API version 6.4 (v6).	The threat defense REST API for software version 7.3 is version 6.4. You can use v6 in the API URLs, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. Note that the URL version path element for 6.4 is the same as all other 6.x versions: v6.
	Please re-evaluate all existing calls, as changes might have been mode to the resource models you are using. To open the API Explorer, where you can view the resources, log into device manager, then click the more options button (⋮) and choose **API Explorer**.
	See: Cisco Secure Firewall Threat Defense REST API Guide

Upgrade Impact Features

A feature has upgrade impact if upgrading and deploying can cause the system *to process traffic or otherwise act differently without any other action on your part*. This is especially common with new threat detection and application identification capabilities. A feature can also have upgrade impact if upgrading requires that you take action before or after upgrade to avoid an undesirable outcome; for example, if you must change a configuration. Having to enable a new setting or deploy a policy post-upgrade to take advantage of a new feature does not count as upgrade impact.

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

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

Upgrade Impact Features for Management Center

Check all releases between your current and target version.

Table 6: Upgrade Impact Features for Management Center

Target Version	Features with Upgrade Impact
7.3.1.1+	• Smaller VDB for lower memory Snort 2 devices.
7.3.0+	• Configure BFD for BGP from the management center web interface.
	• Updated internet access requirements for Smart Licensing.
7.2.4+	• Automatically update CA bundles.

Target Version	Features with Upgrade Impact
7.2.0+	• Configure VXLAN from the management center web interface. • Configure EIGRP from the management center web interface.
7.1.0+	• Configure Equal-Cost-Multi-Path (ECMP) from the FMC web interface. • Configure policy based routing from the FMC web interface. • Send intrusion events and retrospective malware events to the Secure Network Analytics cloud from the FMC. • Deprecated (temporary): Improved SecureX integration, SecureX orchestration. • Deprecated: Intrusion incidents and the intrusion event clipboard. • Deprecated: Custom tables for intrusion events.

Upgrade Impact Features for Threat Defense with Management Center

Check all releases between your current and target version.

Table 7: Upgrade Impact Features for Threat Defense with Management Center

Target Version	Features with Upgrade Impact
7.3.0+	• Auto-upgrade to Snort 3 after successful threat defense upgrade is no longer optional. • Combined upgrade and install package for Secure Firewall 3100. • NetFlow support for Snort 3 devices.
7.2.4+	• Automatically update CA bundles.
7.2.0+	• Autoscale for threat defense virtual for GCP.
7.1.0.3–7.1.0.x	• Automatically update CA bundles.
7.1.0+	• Snort 3 support for inspection of DCE/RPC over SMB2. • Snort 3 support for **ssl_version** and **ssl_state** keywords.
7.0.5–7.0.x	• Automatically update CA bundles.
7.0.0+	• End of support: VMware vSphere/VMware ESXi 6.0. • FTDv performance tiered Smart Licensing. • Deprecated: RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm. • Deprecated: MD5 authentication algorithm and DES encryption for SNMPv3 users.

Upgrade Impact Features for Threat Defense with Device Manager

Check all releases between your current and target version.

Table 8: Upgrade Impact Features for Threat Defense with Device Manager

Target Version	Features with Upgrade Impact
7.3.0+	• TLS 1.3 support in SSL decryption policies, and configurable behavior for undecryptable connections. • Combined upgrade and install package for Secure Firewall 3100. • No support for Firepower 1010E (temporary).
7.2.4+	• Automatically update CA bundles.
7.1.0+	• Dynamic Domain Name System (DDNS) support for updating fully-qualified domain name (FQDN) to IP address mappings for system interfaces. • Snort 3 support for inspection of DCE/RPC over SMB2. • Snort 3 support for **ssl_version** and **ssl_state** keywords.

Upgrade Guidelines

The following sections contain release-specific upgrade warnings and guidelines. You should also check for features and bugs with upgrade impact. For general information on time/disk space requirements and on system behavior during upgrade, see the appropriate upgrade guide: For Assistance, on page 46.

Upgrade Guidelines for Management Center

Table 9: Upgrade Guidelines for Management Center

Target Version	Current Version	Guideline	Details
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+.

Upgrade Guidelines for Threat Defense with Device Manager

Table 10: Upgrade Guidelines for Threat Defense with Device Manager

Target Version	Current Version	Guideline	Details
7.3.x	7.0.x–7.3.x	There are no upgrade warnings or guidelines for this version right now, but you should still check for features and bugs with upgrade impact.	

Upgrade Guidelines for Threat Defense with Management Center

Table 11: Upgrade Guidelines for Threat Defense with Management Center

Target Version	Current Version	Guideline	Details
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).
7.2.0–7.6.x	6.7.0–7.1.x	Upgrade prohibited: threat defense virtual for GCP from Version 7.1.x and earlier to Version 7.2.0+.	You cannot upgrade threat defense virtual for GCP from Version 7.1.x and earlier to Version 7.2.0+. You must deploy a new instance.

Upgrade Guidelines for the Firepower 4100/9300 Chassis

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

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

Upgrade Path

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

Upgrading the Management Center

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

Upgrading Threat Defense with Chassis Upgrade

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

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

Supported Direct Upgrades

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

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

Table 12: Supported Direct Upgrades for Major and Maintenance Releases

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

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

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

Bugs

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

☞

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

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

Open Bugs in Version 7.3.0

Table last updated: 2024-04-08

Table 13: Open Bugs in Version 7.3.0

Bug ID	Headline
CSCwc33025	FTD initially comes up with tunnel tap interface ip and later gets mgmt interface IP
CSCwd13333	FMC proxy user password is stored in plain text
CSCwd21325	FPR 3100: the 'show local-user detail' with unexpected "Error opening the tally file"
CSCwd34079	stress/low memory causing segfault in cavium_get_extended at cn7xxx_drv.c:699
CSCwd41021	Import failed when cloud services (Cisco Defense Orchestrator) is enabled/registered
CSCwd41329	Fast pathed IP has intrusion applied to it
CSCwd42221	730 : SFDataCorrelator core seen in FMC active device while doing Baseline test with 730
CSCwd53448	FPR3100: 4x40 LEDs do not blink with traffic
CSCwd59000	adi crashed multiple timed on longevity upgraded FMC-HA
CSCwd62764	Azure vFTD cluster control node crashed after all nodes powered on after being shut for 3 days
CSCwd72782	[IMS_7_3_0] appid_navl.so and SSL_RULES_LOAD fail after upgrade if disk is full
CSCwe90095	Username-from-certificate feature cannot extract the email attribute

Resolved Bugs in Version 7.3.1.2

Table last updated: 2024-05-10

Table 14: Resolved Bugs in Version 7.3.1.2

Bug ID	Headline
CSCwc51588	Failing to generate FMC Backup/Restore via SMB/SSH
CSCwd27186	All traffic blocked due to access-group command missing from FTD config

Bug ID	Headline
CSCwe10872	Internal Error while editing PPPoE configurations
CSCwe19286	Cisco FTD SMB Protocol Snort 3 Detection Engine Bypass and Denial of Service Vulnerability
CSCwe25412	Azure D5v2 FTDv unable to send traffic - underruns and deplete DPDK buffers observed
CSCwe38029	Multiple traceback seen on standby unit.
CSCwe39546	FMC: Backup to an unavailable remote host results in the inability to restart the appliance.
CSCwe51893	Cisco Firepower Management Center Software Log API Denial of Service Vulnerability
CSCwe84079	asa_snmp.log is not rotated, resulting in large file size
CSCwe99040	traceback and reload thread datapath on process tcpmod_proxy_continue_bp
CSCwf78950	FMC process ssp_snmp_trap_fwdr high memory utilization
CSCwh19475	Intermittently flow is getting white-listed by the snort for the unknow app-id traffic.
CSCwh71358	Unable to create VRF via FDM in Firepower 3105 device
CSCwi08392	Configuring /32 makse PPoE address: "Invalid value of IPV4 address or subnet or network overlap"
CSCwi75111	Configuring MTU value via CLI does not apply
CSCwi90040	Cisco ASA and FTD Software Command Injection Vulnerability
CSCwi98284	Cisco ASA and FTD Software Persistent Local Code Execution Vulnerability
CSCwj09999	FP 3100 MTU change on management interface is NOT persistent across reboots (returns to default MTU)
CSCwj10955	Cisco ASA and FTD Software Web Services Denial of Service Vulnerability
CSCwj40124	FMC 7.3 Deployment failed due to OOM in PBR Configuration

Resolved Bugs in Version 7.3.1.1

Table last updated: 2024-05-22

Table 15: Resolved Bugs in Version 7.3.1.1

Bug ID	Headline
CSCwb08189	Microsoft update traffic blocked with Snort version 3 Malware inspection
CSCwd52995	FMC not opening deployment preview window

Bug ID	Headline
CSCwd88641	Deployment changes to push VDB package based on Device model and snort engine
CSCwe11727	Purging of Config Archive failed for all the devices if one device has no versions
CSCwe51286	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe64043	Cisco ASA and FTD ACLs Not Installed upon Reload
CSCwe72330	FTD LINA traceback and reload in Datapath thread after adding Static Routing
CSCwe88772	ASA traceback and reload with process name: cli_xml_request_process
CSCwf36563	The interface configuration is missing after the FTD upgrade
CSCwh22565	Snort 3 HTTP Intrusion Prevention System Rule Bypass Vulnerability

Resolved Bugs in Version 7.3.1

Table last updated: 2023-05-30

Table 16: Resolved Bugs in Version 7.3.1

Bug ID	Headline
CSCwd29835	log rotate failing to cycle files, resulting in large file sizes
CSCwd46741	fxos log rotate failing to cycle files, resulting in large file sizes
CSCwd87227	High disk usage due to process_stdout.log and process_stderr.log logrotate failure (no rotation)
CSCwe49127	log rotation for process_stderr.log and process_stdout.log files may fail due to race condition

Resolved Bugs in Version 7.3.0

Table last updated: 2022-11-29

Table 17: Resolved Bugs in Version 7.3.0

Bug ID	Headline
CSCvo17612	Return error messages when failing to retrieve objects from database
CSCvo54799	ssh to device fails due to corrupted devpts entry in fstab
CSCvq70838	Traceback in the output of tail-logs command
CSCvv82681	RTC unstable clock register read causes "watchdog: BUG: soft lockup - CPU#0 stuck" error on console
CSCvw23514	Update FXOS troubleshooting documentation to provide details on isolating potential SSD HW failures

Bug ID	Headline
CSCvw90399	FMC HA issues with too many open file descriptors for sfipproxy UDP conn
CSCvx21458	FMC shows error when editing prefix-list attached to active route-map within BGP protocol
CSCvx68173	Observed few snort instances stuck at 100%
CSCvx68586	Not able to login to UI/SSH on FMC, console login doesn't prompt for password
CSCvx99172	M500IT Model Solid State Drives on 4100/9300 may go unresponsive after 3.2 Years in service
CSCvy17030	FMC Connection Events page "Error: Unable to process this query. Please contact support."
CSCvy38650	Unable to download captured file from FMC Captured files UI
CSCvy45048	Subsystem query parameter not filtering records for "auditrecords" restapi
CSCvy95809	Crashinfo script is invoked on SFR running snort2 and device fails to upgrade to 7.0
CSCvy99348	Shutdown command reboots instead of shutting the FP1k device down.
CSCvz34289	In some cases transition to lightweight proxy doesn't work for Do Not Decrypt flows
CSCvz40586	Incorrect error when creating two RA-VPN profiles with different SAML servers that have the same IDP
CSCvz52785	Management interface flaps every 13mins post upgrade from 9.12 to 9.14.2.15
CSCvz68713	PLR license reservation for ASAv5 is requesting ASAv10
CSCvz69729	Unstable client processes may cause LINA zmqio traceback on FTD
CSCvz90712	9.17/Rare 256 block leak/exhaustion, 1550 block overallocation
CSCvz94217	App-instance startup version is ignored and set to running-version after copy config
CSCwa08640	MonetDB crashing due to file size error
CSCwa16257	failover is getting failed in secondary FTD when the loopback interface is configured
CSCwa38996	Big number of repetitive messages in snmpd.log leading to huge log size
CSCwa48169	ASA/FTD traceback and reload on netsnmp_handler_check_cache function
CSCwa52215	Uploading firmware triggers data port-channel to flap
CSCwa55404	Multiple Cisco Products Snort SMB2 Detection Engine Policy Bypass and DoS Vulnerability
CSCwa55772	FPR 4100 saw an unexpected reload with reason "Reset triggered due to HA policy of Reset"

Bug ID	Headline
CSCwa69303	ASA running on SSP platform generate critical error "[FSM:FAILED]: sam:dme:MgmtIfSwMgmtOobIfConfig"
CSCwa72641	URL incorrectly extracted for TLS v1.2 self signed URLs when "Early application detection" enabled
CSCwa76822	Tune throttling flow control on syslog-ng destinations
CSCwa77777	Adding more logs to watchdog infra
CSCwa82850	ASA Failover does not detect context mismatch before declaring joining node as "Standby ready"
CSCwa85297	Multi-instance internal portchannel VLANs may be misprogrammed causing traffic loss
CSCwa85492	URL lookup responding with two categories
CSCwa89347	Cannot add object to network group on FMC
CSCwa90735	FTD/FXOS - ASAconsole.log files fail to rotate causing excessive disk space used in /ngfw
CSCwa94440	syncd process exits due to invalid GID and database synchronization issue
CSCwa96920	ASA/FTD may traceback and reload in process Lina
CSCwa97423	Deployment rollback causes brief traffic drop due to order of operations
CSCwa99171	Chassis and application sets the time to Jan 1, 2010 after reboot
CSCwa99932	ASA/FTD stuck after crash and reboot
CSCwb00871	ENH: Reduce latency in log_handler_file to reduce watchdog under scale or stress
CSCwb01633	FXOS misses logs to diagnose root cause of module show-tech file generation failure
CSCwb01983	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb01990	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb02689	FXOS should check reference clock stratum instead of NTP server local clock stratum
CSCwb03704	ASA/FTD datapath threads may run into deadlock and generate traceback
CSCwb04000	ASA/FTD: DF bit is being set on packets routed into VTI
CSCwb04975	FTD Snort3 traceback in daq-pdts while handling FQDN based traffic
CSCwb05148	Cisco ASA Software and FTD Software SNMP Denial of Service Vulnerability
CSCwb06318	FTD - Unable to issue "configure manager edit" to FMC entries in Pending state
CSCwb08393	SSL policy deploy failing when using special characters on SSL rule names

Bug ID	Headline
CSCwb18602	crontab -e unable to find editor
CSCwb19664	Malware Block false positives triggered after upgrade to version 7.0.1
CSCwb20206	FTD: Logs and Debugs for SSL/TLS traffic drop due to NAP in Detection Mode
CSCwb22359	Portmanager/LACP improvement to avoid false restarts and increase of logging events
CSCwb25809	Single Pass - Traceback due to stale ifc
CSCwb27099	FXOS: Third-party interop between Ciena Waveserver with firepower chassis.
CSCwb28123	FTD HA deployment fails with error "Deployment failed due to major version change on device"
CSCwb31551	When inbound packet contains SGT header, FPR2100 cannot distribute properly per 5 tuple
CSCwb32107	FMC shows limited interfaces in policy-based routing config
CSCwb34240	Log rotation failure of files process_stdout.out and process_stderr.out - syslog-ng. High disk usage
CSCwb34970	External authentication with Radius server fail on a 2k platform
CSCwb38406	GeoDB updates on multi-domain environment requires a manual policy deployment
CSCwb38961	Bootstrap After Upgrade failed due to Duplicate Key of Network Object
CSCwb39431	FTD unified logs do not print the log as per rfc5424 standard
CSCwb40662	ENH: FCM should include option for modifying the interface 'link debounce time'
CSCwb41854	Cisco FTD Software and Cisco FXOS Software Command Injection Vulnerability
CSCwb43629	License and rule counts telemetry data incorrectly generated for HA managed devices
CSCwb44048	Event Rate on FMC Health Monitoring Dashboard shows extremely high values
CSCwb46481	SNMPv3 not working after upgrade of FMC
CSCwb48166	FXOS upgrade to 2.11 is stuck
CSCwb51821	Disk usage errors on Firepower Azure device due to large backup unified files under ngfw directory
CSCwb57213	FTD - Unable to resolve DNS when only diagnostic interface is used for DNS lookups
CSCwb57524	FTD upgrade fails - not enough disk space from old FXOS bundles in distributables partition
CSCwb57615	Configuring pbr access-list with line number failed.
CSCwb57988	The smConLogger traceback is caused by memory leak.

Bug ID	Headline
CSCwb58007	CVE-2022-28199: Evaluation for FTDv and ASAv
CSCwb58554	Resumed SSL sessions with uncached tickets may fail to complete
CSCwb58817	FMC Deploying negative and positive form of BGP password command across deployments
CSCwb59619	PM needs to restart the Disk Manager after creating ramdisk to make DM aware of the ramdisk
CSCwb60993	FDM Need to block the deployment when a Security zone object is not associated with an interface
CSCwb62059	Unable to login to FTD using external authentication after upgrade
CSCwb65447	FTD: AAB cores are not complete and not decoding
CSCwb65718	FMC is stuck on loading SI objects page
CSCwb66382	ASAv - 9344 Block not created automatically after enabling JumboFrames, breaks OSPF MD5
CSCwb66736	Multiple Cisco Products Snort SMB2 Detection Engine Policy Bypass and DoS Vulnerability
CSCwb68993	FTD/FDM: SSL connections to sites using RSA certs with 3072 bit keys may fail
CSCwb70030	MIO: No blade reboot during CATERR if fault severity is non-Severe or CATERR sensor is different
CSCwb73678	/var/tmp partition fullness warning on FXOS
CSCwb74498	Cisco FXOS and NX-OS Software CDP DoS and Arbitrary Code Execution Vulnerability
CSCwb78323	Update diskmanager to monitor cisco_uridb files in /ngfw/var/sf/cloud_download folder.
CSCwb82796	ASA/FTD firewall may traceback and reload when tearing down IKE tunnels
CSCwb83691	ASA/FTD traceback and reload due to the initiated capture from FMC
CSCwb84677	FMC backup may fail due to monetdb backup failure with return code 102
CSCwb85822	Deployment failing when collecting policies.
CSCwb86171	Breaking FMCv HA in AWS gives VTEP CONFIGURATION IS NOT SUPPORTED FOR CURRENT PERFORMANCE TIER alert
CSCwb86339	ACP Network Validation Failure - Unable to parse ip - Can't call method "binip" - Blank Space
CSCwb86565	FMC upgrade fails due Mismatch in number of entries between /etc/passwd and /etc/shadow

Bug ID	Headline
CSCwb87762	Multiple Cisco Products Snort SMB2 Detection Engine Policy Bypass and DoS Vulnerability
CSCwb88090	FXOS:after fxos config import new port-channel creation causing existing port-channel flap
CSCwb88406	FMC-HA upgrade failure due to presence of this file "update.status"
CSCwb89004	FMC DBcheck.pl hungs at "Checking mysql.rna_flow_stats_template against the current schema"
CSCwb89187	Flex Config allow - "timeout icmp-error hh:mm:ss"
CSCwb90074	ASA: Multiple Context Mixed Mode SFR Redirection Validation
CSCwb91598	copying FMC backup to remote storage will fail if FMC has never connected via SSH/SCP to remote host
CSCwb92376	FMC syslog-ng daemon fails to start if log facility is set to ALERT
CSCwb92583	upgrade with a large amount of unmonitored disk space used can cause failed upgrade and hung device
CSCwb94170	merovingian.log file extremly big size can fill the disk
CSCwb95112	Intrusion Policy shows last modified by admin even though changes are made by a different user
CSCwb95787	FPR1010 - No ARP on switchport VLAN interface after portmanager DIED event
CSCwb96471	Semantic Search is enabled for IP address from 7.0
CSCwb99509	Cisco Firepower Threat Defense Software SIP and Snort 3 Denial of Service Vulnerability
CSCwc00115	FTD registration fails on on-prem FMC
CSCwc02133	Cisco FTD Software and Cisco FXOS Software Command Injection Vulnerability
CSCwc02416	Not re-subscribing to ISE topics after certain ISE connectivity issues.
CSCwc03296	Upgrade fails when using DDNS Service with user and password
CSCwc03385	DOC: Changing admin password using expert mode passwd command not supported
CSCwc05132	Unable to disable "Retrieve to Management Center
CSCwc05434	FMC shows 'File Not Stored' after download a file
CSCwc06833	Deployment failure with ERROR Process Manager failed to verify LSP ICDB
CSCwc07015	snort3 crash due to NULL pointer in TLS Client Hello Evaluation
CSCwc07431	FMC	Error generating configuration for policy "QoS / Access Control Policy"

Bug ID	Headline
CSCwc08683	The interface's LED remains green blinking when the optical fiber is unplugged on FPR1150
CSCwc10145	FTDv Cluster unit not re-joining cluster with error msg "Failed to open NLP SSL listening socket"
CSCwc12652	Control-Plane ACL Non-Functional After Upgrade to 9.18(1) or 7.2.0-82 Firepower
CSCwc13017	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
CSCwc13382	DCERPC traffic is dropped after upgrade to snort3 due to Parent flow is closed
CSCwc18218	Database files on disk grow larger than expected for some frequently updated tables
CSCwc18668	Failed user login on FMC does not record entry in audit log when using external authentication
CSCwc18953	Deployment failure after migration of sub-interface
CSCwc19124	FMC Deployment does not start for cluster devices
CSCwc20153	IPv6 ICMP configuration is added and removed during policy deployment
CSCwc22170	Hmdeamon not starting after disk full reported
CSCwc24582	Update diskmanager to monitor deploy directories in /ngfw/var/cisco/deploy/db
CSCwc25275	AC Policy UI: Cannot search rules while the rules are loading
CSCwc26406	FMC: Slowness in Device management page
CSCwc27236	FMC Health Monitoring JSON error
CSCwc27424	Unable to removed not used SAL On-Premise FMC configuration
CSCwc27846	Observing Crash in QP(multicontext)-99.18(28)9 while HA sync after upgrading and reloading.
CSCwc28660	Snort3: NFSv3 mount may fail for traffic through FTD
CSCwc28806	ASA Traceback and Reload on process name Lina
CSCwc29591	Retrospective file disposition updates fail due to incorrect eventsecond values in fileevent tables
CSCwc29888	Monet DB stops processing connections due to failure in allocating virtual memory
CSCwc30487	High unmanaged disk usage on Firepower 2110 device
CSCwc31163	FPR1010 upgrade failed - Error running script 200_pre/100_get_snort_from_dc.pl
CSCwc31457	ASA process with cleartext token when not able to encrypt it

Bug ID	Headline
CSCwc33076	JOBS_TABLE not getting purged due to foreign Key constraint violation in policy_diff_main
CSCwc33323	FMC 7.0 - Receiving alert "health monitor process: no events received yet" for multiple devices
CSCwc34818	The device is unregistered when Rest API calls script.
CSCwc35181	OSPF template adds "default-information-originate" to area <area-id> nssa statement on hitting OK.
CSCwc35969	cannot add IP from event to global lists (block or do-not-block) if similar IP is already on list
CSCwc37061	SNMP: FMC doesn't reply to OID 1.3.6.1.2.1.25.3.3.1.2
CSCwc38361	Cisco FXOS Software Command Injection Vulnerability
CSCwc38500	FMC: Extended ACL object should support mixed protocols on different entries
CSCwc39525	FMC HA status alert "degraded - maintenance" seen periodically after upgrade to 7.0.2
CSCwc40263	Error running script 000_start/099_check_legacy_amp_port.pl due to json decode failure
CSCwc40322	Onboarding on-prem FMC to CDO using SecureX fails due to User Authentication Failed error
CSCwc40352	Lina Netflow sending permited events to Stealthwatch but they are block by snort afterwards
CSCwc40850	FMC authentication with SecureX Orchestration fails
CSCwc41592	False positives for Ultrasurf
CSCwc41661	FTD Multiple log files with zero byte size.
CSCwc41728	FMC - Cannot Edit Standard ACL with error regarding "Only Host objects allowed"
CSCwc42561	Deploy page listing takes 1.5 to 2 mins with 462 HA device
CSCwc44289	FTD - Traceback and reload when performing IPv4 <> IPv6 NAT translations
CSCwc44608	Selective deployment of IPS may cause outage due to incorrectly written FTD configuration files
CSCwc48375	Inbound IPSEC SA stuck inactive - many inbound SPIs for one outbound SPI in "show crypto ipsec sa"
CSCwc48853	SFDataCorrelator Discovery Event bottleneck can cause Connection Event delay and backlog
CSCwc49369	When searching IPv6 rule in the access-control policy, no result will show

Bug ID	Headline
CSCwc49952	Selective deploy enables interaction with SRU interdependent-policies due to FMC API timeout
CSCwc50098	show ssl-policy-config does not show the policy when countries are being used in source/dest network
CSCwc50846	FTD Upgrade Fail - Readiness Check Successful, but Readiness status never shown
CSCwc50887	FTD - Traceback and reload on NAT IPv4<>IPv6 for UDP flow redirected over CCL link
CSCwc50891	MPLS tagging removed by FTD
CSCwc54901	Scheduled tasks may not run on active FMC in HA after switchover or split-brain resolution
CSCwc56003	Trigger FTD backup with remote storage option enabled along with retrieval to FMC fails
CSCwc56048	AD username with trailing space causes download of users/groups to fail
CSCwc57575	FMC: Scheduled backups working fine, but FMC email alerts displaying it failed.
CSCwc59953	Snort3 crash with TLS 1.3
CSCwc60263	Identity Realm - Active Directory and FMC need to be as close as possible for best download times
CSCwc61106	Unable to configure domain\username under cfg-export-policy in FXOS
CSCwc62144	FMC does not use proxy with authentication when accessing AMP cloud services
CSCwc62384	Vulnerabilities on Cisco FTD Captive Portal on TCP port 885
CSCwc64333	FMC GUI timeout and issues with loading http page due to exceeded http connections
CSCwc65907	snort3 hangs in Crash handler which can lead to extended outage time during a snort crash
CSCwc66671	FMC ACP PDF report generared in blank/0 bytes using UI
CSCwc67687	ASA HA failover triggers HTTP server restart failure and ASDM outage
CSCwc68543	mismatch in the config pushed from FMC and running config on FTD
CSCwc69583	Portchannel configured from FDM breaks "Use the Data Interfaces as the Gateway" for Mgmt interface
CSCwc69992	Essentials licenses are not assigned to the device and Edit licenses also not working
CSCwc70962	FTD/ASA "Write Standby" enables ECDSA ciphers causing AC SSLv3 handshake failure
CSCwc73209	DOC:The default keying is only used by FCM on FXOS.

Bug ID	Headline
CSCwc76658	SFDataCorrelator fails to start after <7.1 to >=7.1.0 upgrade due to compliance.rules "session_both"
CSCwc77519	FPR1120-ASA:Primary takes active role after reloading
CSCwc77680	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-0-4948'
CSCwc77892	CGroups errors in ASA syslog after startup
CSCwc79682	FMC 7.1+ allows ECMP FlexConfig depoyment
CSCwc80234	"inspect snmp" config difference between active and standby
CSCwc80357	[Deploy Performance] degrade in deployment page on FMC
CSCwc81727	Default Domain in VPN group policy objects cannot be deleted
CSCwc88583	Deployment fails with error Invalid Snort3IntrusionPolicy mode. Supports only inline and inline-test
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.
CSCwc95731	Policy applied to devices are not displayed in policy page of CDO FMC
CSCwc98997	FMC - Deployment blocked when ECMP route configured via same interface
CSCwc99053	FDM: "failover replication http" command may disappear from FTD running config
CSCwc99242	ISA3000 LACP channel member SFP port suspended after reload
CSCwd00778	ifAdminStatus output is abnormal via snmp polling
CSCwd03113	FMC local backup fails cause of "Update Task: Database integrity check failed" - Syslog server issue
CSCwd03793	FTD Traceback and reload
CSCwd05443	Config-dispatcher to fail the deployment immediately when download fails, instead of failing later
CSCwd05756	FTD traceback on Lina due to syslog component.
CSCwd07059	multiple snort3 crashes after upgrading FTD from 7.2.0 to 7.2.0.1
CSCwd08430	Create a resiliency configuration option for SFTunnel to support HA and FTD connectivity
CSCwd09093	Access rule policy page takes longer time to load
CSCwd09341	Multiple log files have zero bytes on the FMC

Bug ID	Headline
CSCwd11165	"Move" option is greyed out on Backup-Restore in FMC
CSCwd12334	Deployment fails with Config Error -- proxy paired
CSCwd12724	interfaces.conf may be empty after FDM policy deployment after FTDv tier change
CSCwd13917	during download from file event on FMC, high CPU use on FMC for 20 minutes before download fails
CSCwd17037	SFDataCorrelator RNA-Stop action should not block when database operations are hung
CSCwd22349	ASA: Unable to connect AnyConnect Cert based Auth with "periodic-authentication certificate" enabled
CSCwd24639	Functional: FMCv patch upgrade is fails
CSCwd30977	FMC deleted some access-rules due to an incorrect delta generated during the policy deployment.
CSCwd31960	Management access over VPN not working when custom NAT is configured
CSCwd39039	FMC - Error message "The server response was not understood. Please contact support." on UI
CSCwd40260	Serviceability Enhancement - Unable to parse payload are silently drop by ASA/FTD
CSCwd50131	Upgrades are not cleaning up mysql files leading to alert for 'High unmanaged disk usage on /ngfw'
CSCwd51757	Unable to get polling results using snmp GET for connection rate OID's
CSCwd56431	Disable asserts in FTD production builds
CSCwe21301	Azure FMC not accessible after upgrading from 7.3.0 to 7.4.0

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 18: Upgrade Guides

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

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

Install Guides

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

Table 19: Install Guides

Platform	Install Guide	Link
Management center hardware	Getting started guide for your management center hardware model.	https://www.cisco.com/go/fmc-install
Management center virtual	Getting started guide for the management center virtual.	https://www.cisco.com/go/fmcv-quick
Threat defense hardware	Getting started or reimage guide for your device model.	https://www.cisco.com/go/ftd-quick
Threat defense virtual	Getting started guide for your threat defense virtual version.	https://www.cisco.com/go/ftdv-quick
FXOS for the Firepower 4100/9300	Configuration guide for your FXOS version, in the *Image Management* chapter.	https://www.cisco.com/go/firepower9300-config
FXOS for the Firepower 1000/2100 and Secure Firewall 3100	Troubleshooting guide, in the *Reimage Procedures* chapter.	Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense

More Online Resources

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

- Documentation: http://www.cisco.com/go/threatdefense-73-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