



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

First Published: 2022-11-29

Last Modified: 2025-08-12

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 Firewall in Security Cloud Control](#).

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.

The feature descriptions here include upgrade impact where appropriate. For a more complete list of features with upgrade impact by version, see [Upgrade Impact Features, on page 25](#).

Features in Maintenance Releases

Features, enhancements, and critical fixes included in maintenance releases (third-digit) and patches (fourth-digit) can skip future releases, depending on release date, release type (short term vs. long term), and other factors. Minimize upgrade and other impact by going directly to the latest maintenance release in your chosen version. See [Choosing your upgrade target, on page 28](#).

If you are using the web interface in a language other than English, features introduced in maintenance releases and patches may not be translated until the next major release.

Snort Features

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



Important

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

Intrusion Rules and Keywords

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

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

FlexConfig

Upgrades can add web interface or Smart CLI support for features that previously required FlexConfig. Although you cannot newly assign or create FlexConfig objects using deprecated commands, in most cases existing FlexConfigs continue to work and you can still deploy. However, sometimes, using deprecated

commands can cause deployment issues. The upgrade does not convert FlexConfigs. After upgrade, configure the newly supported features in the web interface or Smart CLI. When you are satisfied with the new configuration, delete the deprecated FlexConfigs.

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

Integrations and Logging

These integrations and logging facilities may have new features associated with threat defense and management center releases:

- Syslog: [Cisco Secure Firewall Threat Defense Syslog Messages](#)
- Cisco Success Network: [Cisco Success Network Telemetry Data Collected from Cisco Secure Firewall Management Center](#)
- REST API: [Secure Firewall Management Center REST API Quick Start Guide](#) and [Cisco Secure Firewall Threat Defense REST API Guide](#)

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 |
|---|---------------------------|------------------------|---|
| Features from Earlier Maintenance Releases | | | |
| Features from earlier maintenance releases. | Feature dependent | Feature dependent | Version 7.3.1.1 also has: <ul style="list-style-type: none"> • Smaller VDB for lower memory Snort 2 devices. (7.0.6) |

Table 3: Management Center Features in Version 7.3.1

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|-----------------------|---------------------------|------------------------|---|
| Secure Firewall 3105. | 7.3.1 7.4.0 | 7.3.1 7.4.0 | 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 |
|---|---------------------------|------------------------|--|
| Features from Earlier Maintenance Releases | | | |
| Features from earlier maintenance releases. | Feature dependent | Feature dependent | <p>Version 7.3.0 also has:</p> <ul style="list-style-type: none"> • ISA 3000 System LED support for shutting down. (7.0.5) • Automatically update CA bundles. Upgrade impact. (7.0.5) • Updated internet access requirements for Smart Licensing. Upgrade impact. (7.0.8) • Hardware bypass ("fail-to-wire") network modules for the Secure Firewall 3100. (7.2.1) • Intel Ethernet Network Adapter E810-CQDA2 driver with Firewall Threat Defense Virtual for KVM. (7.2.1) • Default Forward Error Correction (FEC) on Secure Firewall 3100 fixed ports changed to Clause 108 RS-FEC from Clause 74 FC-FEC for 25 GB+ SR, CSR, and LR transceivers. (7.2.4) • Select devices to upgrade from the Firewall Threat Defense upgrade wizard. (7.2.6) • Unattended Firewall Threat Defense upgrades. (7.2.6) • Simultaneous Firewall Threat Defense upgrade workflows by different users. (7.2.6) • Skip pre-upgrade troubleshoot generation for Firewall Threat Defense. (7.2.6) • Firewall Threat Defense Virtual for Megaport. (7.2.8) |
| 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 | <p>We introduced these network modules for the Firepower 4100:</p> <ul style="list-style-type: none"> • 2-port 100G network module (FPR4K-NM-2X100G) <p>Supported platforms: Firepower 4112, 4115, 4125, 4145</p> |

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|--|---------------------------|------------------------|--|
| New compute shapes for Firewall Threat Defense Virtual and Firewall Management Center Virtual for OCI. | 7.3.0 | 7.3.0 | <p>Firewall Threat Defense Virtual for OCI adds support for the following compute shapes:</p> <ul style="list-style-type: none"> • 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 <p>Firewall Management Center Virtual for OCI adds support for the following compute shapes:</p> <ul style="list-style-type: none"> • Intel VM.StandardB1.4 • Intel VM.Standard3.Flex • Intel VM.Optimized3.Flex • AMD VM.Standard.E4.Flex <p>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.</p> <p>For information on compatible compute shapes, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.</p> |

Interfaces

| | | | |
|--------------------------------------|-------|-------|---|
| IPv6 support for virtual appliances. | 7.3.0 | 7.3.0 | <p>Firewall Threat Defense Virtual and Firewall Management Center Virtual now support IPv6 in the following environments:</p> <ul style="list-style-type: none"> • AWS • Azure • OCI • KVM • VMware <p>For more information, see Cisco Secure Firewall Threat Defense Virtual Getting Started Guide and Cisco Secure Firewall Management Center Virtual Getting Started Guide.</p> |
|--------------------------------------|-------|-------|---|

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|--|---------------------------|------------------------|--|
| Loopback interface support for VTIs. | 7.3.0 | 7.3.0 | <p>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.</p> <p>New/modified screens: Devices > Device Management > Device > Interfaces > Add Interfaces > Add Loopback Interface</p> <p>For more information, see Configure Loopback Interfaces in the device configuration guide.</p> |
| Redundant manager access data interface. | 7.3.0 | 7.3.0 | <p>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.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Devices > Device Management > Device > Management • Devices > Device Management > Device > Interfaces > Manager Access <p>For more information, see Configure a Redundant Manager Access Data Interface in the device configuration guide.</p> |

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|---|---------------------------|------------------------|--|
| IPv6 DHCP. | 7.3.0 | 7.3.0 | <p>We now support the following features for IPv6 addressing:</p> <ul style="list-style-type: none"> • DHCPv6 Address client: Firewall Threat Defense obtains an IPv6 global address and optional default route from the DHCPv6 server. • DHCPv6 Prefix Delegation client: Firewall Threat Defense obtains delegated prefix(es) from a DHCPv6 server. It can then use these prefixes to configure other Firewall 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: Firewall Threat Defense provides other information such as the domain name to SLAAC clients when they send Information Request (IR) packets to Firewall Threat Defense. Firewall Threat Defense only accepts IR packets and does not assign addresses to the clients. <p>New/modified screens:</p> <ul style="list-style-type: none"> • Devices > Device Management > Device > Interfaces > Interface > IPv6 > DHCP • Objects > Object Management > DHCP IPv6 Pool <p>New/modified CLI commands: show bgp ipv6 unicast, show ipv6 dhcp, show ipv6 general-prefix</p> <p>For more information, see Configure the IPv6 Prefix Delegation Client, BGP, and Configure the DHCPv6 Stateless Server in the device configuration guide.</p> |
| Paired proxy VXLAN for the Firewall Threat Defense Virtual for the Azure Gateway Load Balancer. | 7.3.0 | 7.3.0 | <p>You can configure a paired proxy mode VXLAN interface for Firewall 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.</p> <p>New/modified screens: Devices > Device Management > Device > Interfaces > Add Interfaces > VNI Interface</p> <p>For more information, see Configure VXLAN Interfaces in the device configuration guide.</p> |
| High Availability/Scalability: Threat Defense | | | |
| Clustering for Firewall Threat Defense Virtual for Azure. | 7.3.0 | 7.3.0 | <p>You can now configure clustering for up to 16 nodes with Firewall Threat Defense Virtual for Azure.</p> <p>New/modified screens: Devices > Device Management</p> <p>For more information, see Clustering for Threat Defense Virtual in a Public Cloud in the device configuration guide.</p> |

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|---|---------------------------|------------------------|--|
| Autoscale for Firewall Threat Defense Virtual for Azure Gateway Load Balancers. | 7.3.0 | 7.3.0 | We now support autoscale for Firewall 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 | <p>You can now use the Firewall Management Center to back up device clusters, except in the public cloud. To restore, use the device CLI.</p> <p>New/modified screens: System > Tools > Backup/Restore > Managed Device Backup</p> <p>New/modified commands: restore remote-manager-backup</p> <p>For more information, see Backup/Restore in the administration guide.</p> |

High Availability: Management Center

| | | | |
|---|-------|-----|---|
| High availability for Firewall Management Center Virtual for KVM. | 7.3.0 | Any | <p>We now support high availability for Firewall Management Center Virtual for KVM.</p> <p>In a Firewall Threat Defense deployment, you need two identically licensed Firewall Management Centers, as well as one Firewall Threat Defense entitlement for each managed device. For example, to manage 10 devices with an FMCv10 high availability pair, you need two FMCv10 entitlements and 10 Firewall Threat Defense entitlements. If you are managing Classic devices only (NGIPSv or ASA FirePOWER), you do not need FMCv entitlements.</p> <p>Platform restrictions: Not supported with FMCv2</p> <p>For more information, see the Cisco Secure Firewall Management Center Virtual Getting Started Guide, as well as High Availability in the administration guide.</p> |
|---|-------|-----|---|

VPN: Remote Access

| | | | |
|-------------------|-------|-----|--|
| RA VPN dashboard. | 7.3.0 | Any | <p>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:</p> <ul style="list-style-type: none"> • 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. <p>New/modified screens: Overview > Dashboards > Remote Access VPN</p> <p>For more information, see Dashboards in the administration guide.</p> |
|-------------------|-------|-----|--|

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|--|---------------------------|------------------------|---|
| Encrypt RA VPN connections with TLS 1.3. | 7.3.0 | 7.3.0 | <p>You can now use TLS 1.3 to encrypt RA VPN connections with the following ciphers:</p> <ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 <p>Use the Firewall Threat Defense platform settings to set the TLS version: Devices > Platform Settings > Add/Edit Threat Defense Settings Policy > SSL > TLS Version.</p> <p>This feature requires Cisco Secure Client, Release 5 (formerly known as the AnyConnect Secure Mobility Client).</p> <p>For more information, see Configure SSL Settings in the device configuration guide.</p> |
| VPN: Site to Site | | | |
| Packet tracer in the site-to-site VPN dashboard. | 7.3.0 | Any | <p>We added packet tracer capabilities to the site-to-site VPN dashboard, to help you troubleshoot VPN tunnels between devices.</p> <p>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.</p> <p>For more information, see Monitoring the Site-to-Site VPNs in the device configuration guide.</p> |
| Support for dynamic VTIs with site-to-site VPN. | 7.3.0 | 7.3.0 | <p>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.</p> <p>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.</p> <p>New/modified screens: We updated the options when configuring hub-node endpoints for a route-based hub-and-spoke site-to-site VPN topology.</p> <p>For more information, see Configure Endpoints for a Hub and Spoke Topology in the device configuration guide.</p> |

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|--|---------------------------|------------------------|---|
| Improved Umbrella SIG integration. | 7.3.0 | 7.3.0 | <p>You can now easily deploy IPsec IKEv2 tunnels between a Firewall 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.</p> <p>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.</p> <p>For more information, see Deploy a SASE Tunnel on Umbrella in the device configuration guide.</p> |
| Routing | | | |
| Configure BFD for BGP from the Firewall Management Center web interface. | 7.3.0 | Any | <p>Upgrade impact. Redo related FlexConfigs after upgrade.</p> <p>You can now use the Firewall 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.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • 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 Firewall 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. <p>For more information, see Bidirectional Forwarding Detection Routing in the device configuration guide.</p> |
| Support for IPv4 and IPv6 OSPF routing for VTIs. | 7.3.0 | 7.3.0 | <p>We now support IPv4 and IPv6 OSPF routing for VTI interfaces.</p> <p>New/modified pages: You can add VTI interfaces to an OSPF routing process on Devices > Device Management > Device > Routing > OSPF/OSFPv3.</p> <p>For more information, see OSPF and Additional Configurations for VTI in the device configuration guide.</p> |
| Support for IPv4 EIGRP routing for VTIs. | 7.3.0 | 7.3.0 | <p>We now support IPv4 EIGRP routing for VTI interfaces.</p> <p>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.</p> <p>For more information, see EIGRP and Additional Configurations for VTI in the device configuration guide.</p> |

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|--|---------------------------|------------------------|---|
| 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 | <p>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.</p> <p>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.</p> <p>For more information, see Configure Policy-Based Routing Policy in the device configuration guide.</p> |
| Upgrade | | | |
| Choose and direct-download upgrade packages to the Firewall Management Center. | 7.3.x only | Any | <p>You can now choose which Firewall Threat Defense upgrade packages you want to direct download to the Firewall Management Center. Use the new Download Updates sub-tab on > Updates > Product Updates.</p> <p>Version restrictions: this feature is replaced by an improved package management system in Version 7.2.6/7.4.1.</p> <p>See: Download Upgrade Packages with the Management Center</p> |
| Upload upgrade packages to the Firewall Management Center from the Firewall Threat Defense wizard. | 7.3.x only | Any | <p>You now use the wizard to upload Firewall Threat Defense upgrade packages or specify their location. Previously (depending on version), you used System > Updates or System > Product Upgrades.</p> <p>Version restrictions: this feature is replaced by an improved package management system in Version 7.2.6/7.4.1.</p> <p>See: Upgrade Threat Defense</p> |
| Auto-upgrade to Snort 3 after successful Firewall Threat Defense upgrade is no longer optional. | 7.3.0 | Any | <p>Upgrade impact. All eligible devices upgrade to Snort 3 when you deploy.</p> <p>When you upgrade Firewall Threat Defense to Version 7.3+, you can no longer disable the Upgrade Snort 2 to Snort 3 option.</p> <p>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 is not supported on Firewall Threat Defense 7.7+. You should stop using it now.</p> <p>For devices that are ineligible for auto-upgrade because they use custom intrusion or network analysis policies, 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.</p> |

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|--|---------------------------|------------------------|---|
| Combined upgrade and install package for Secure Firewall 3100. | 7.3.0 | 7.3.0 | <p>Reimage Impact.</p> <p>In Version 7.3, we combined the Firewall Threat Defense install and upgrade package for the Secure Firewall 3100, as follows:</p> <ul style="list-style-type: none"> • Version 7.1–7.2 install package: <code>cisco-ftd-fp3k.version.SPA</code> • Version 7.1–7.2 upgrade package: <code>Cisco_FTD_SSP_FP3K_Upgrade-version-build.sh.REL.tar</code> • Version 7.3+ combined package: <code>Cisco_FTD_SSP_FP3K_Upgrade-version-build.sh.REL.tar</code> <p>Although you can upgrade Firewall Threat Defense without issue, you cannot reimage from older Firewall Threat Defense and ASA versions directly to Firewall 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.</p> <p>To get to Firewall Threat Defense Version 7.3+, your options are:</p> <ul style="list-style-type: none"> • Upgrade from Firewall Threat Defense Version 7.1 or 7.2 — use the normal upgrade process. See the appropriate Upgrade Guide. • Reimage from Firewall Threat Defense Version 7.1 or 7.2 — reimage to ASA 9.19+ first, then reimage to Firewall Threat Defense Version 7.3+. See <i>Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100</i> and then <i>ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100</i> 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 Firewall Threat Defense Version 7.3+. See the Cisco Secure Firewall ASA Upgrade Guide and then <i>ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100</i> in the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide. • Reimage from Firewall Threat Defense Version 7.3+ — use the normal reimage process. See <i>Reimage the System with a New Software Version</i> in the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense. |

Access Control: Threat Detection and Application Identification

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|---|---------------------------|------------------------|--|
| SSL policy renamed to decryption policy. | 7.3.0 | Any | <p>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.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • 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. <p>For more information, see Decryption Policies in the device configuration guide.</p> |
| Improvements to TLS server identity discovery with Snort 3 devices. | 7.3.0 | 7.3.0 | <p>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.</p> <p>For more information, see TLS 1.3 Decryption Best Practices in the device configuration guide.</p> |


| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|---|---------------------------|------------------------|--|
| URL filtering using cloud lookup results only. | 7.3.0 | 7.3.0 | <p>When you enable (or re-enable) URL filtering, the Firewall 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.</p> <p>To do this, we replaced the Query Cisco Cloud for Unknown URLs options with three new options:</p> <ul style="list-style-type: none"> • 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 <i>not</i> match rules with category or reputation-based URL conditions. You cannot assign categories or reputations to URLs manually. <p>For upgraded Firewall Management Centers, this option is enabled if the old Query Cisco Cloud for Unknown URLs was disabled.</p> <ul style="list-style-type: none"> • 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. <p>For upgraded Firewall Management Centers, this option is enabled if the old Query Cisco Cloud for Unknown URLs option was enabled.</p> <ul style="list-style-type: none"> • 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. <p>This option is the default on new and reimaged Version 7.3+ Firewall Management Centers. Note that it also requires Firewall Threat Defense Version 7.3+. If you enable this option, devices running earlier versions use the Local Database and Cisco Cloud option.</p> <p>New/modified screens: Integration > Other Integrations > Cloud Services > URL Filtering</p> <p>For more information, see URL Filtering Options in the device configuration guide.</p> |
| Detect HTTP/3 and SMB over QUIC using EVE (Snort 3 only). | 7.3.0 | 7.3.0 with Snort 3 | <p>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.</p> <p>For more information, see Encrypted Visibility Engine in the device configuration guide.</p> |

| 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 | <p>Snort 3 devices can now generate indications of compromise (IoC) connection events based on unsafe client applications detected by the encrypted visibility engine (EVE). These connection events have a Encrypted Visibility Threat Confidence of Very High.</p> <ul style="list-style-type: none"> • 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 <p>For more information, see Encrypted Visibility Engine in the device configuration guide.</p> |
| Improved JavaScript inspection for Snort 3 devices. | 7.3.0 | 7.3.0 with Snort 3 | <p>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.</p> <p>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.</p> |
| Nested rule groups, including MITRE ATT&CK, in Snort 3 intrusion policies. | 7.3.0 | 7.0 with Snort 3 | <p>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.</p> <p>We also group system-provided rules in a Talos-curated MITRE ATT&CK framework, so you can act on traffic based on those categories.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • 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 <p>For more information, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide.</p> |

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|--|---------------------------|------------------------|--|
| Access control rule conflict analysis. | 7.3.0 | Any | <p>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.</p> <p>For more information, see Analyzing Rule Conflicts and Warnings in the device configuration guide.</p> |
| Event Logging and Analysis | | | |
| NetFlow support for Snort 3 devices. | 7.3.0 | 7.3.0 with Snort 3 | <p>Upgrade impact. Devices may begin processing NetFlow records.</p> <p>Snort 3 devices now can consume NetFlow records (IPv4 and IPv6, NetFlow v5 and v9). Previously, only Snort 2 devices did this.</p> <p>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.</p> <p>For more information, see Network Discovery Policies in the device configuration guide.</p> |
| Integrations | | | |
| New remediation module for integration with the Cisco ACI Endpoint Update App | 7.3.0 | Any | <p>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:</p> <ul style="list-style-type: none"> • 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. <p>For more information, see APIC/Secure Firewall Remediation Module 3.0 in the device configuration guide.</p> |
| Health Monitoring | | | |
| Cluster health monitor settings in the Firewall Management Center web interface. | 7.3.0 | Any | <p>You can now use the Firewall 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.</p> <p>New/modified screens: Devices > Device Management > Edit Cluster > Cluster Health Monitor Settings</p> <p>For more information, see Edit Cluster Health Monitor Settings in the device configuration guide.</p> |

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|--|---------------------------|------------------------|--|
| Improved health monitoring for device clusters. | 7.3.0 | Any | <p>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.</p> <p>To view the dashboard for each cluster, choose System (⚙️) > Health > Monitor, then click the cluster.</p> <p>For more information, see Cluster Health Monitor in the administration guide.</p> |
| Monitor fan speed and temperature for the power supply on the hardware Firewall Management Center. | 7.3.0 | Any | <p>We added the Hardware Statistics health module that monitors fan speed and temperature for the power supply on the hardware Firewall Management Center. The upgrade process automatically adds and enables this module. After upgrade, apply the policy.</p> <p>To enable or disable the module and set threshold values, edit the Firewall Management Center health policy on System (⚙️) > Health > Policy.</p> <p>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.</p> <p>You can also view module status on the health monitor's Home page and in the Firewall 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.</p> <p>For more information, see Hardware Statistics on Management Center in the administration guide.</p> |
| Monitor temperature and power supply for the Firepower 4100/9300. | 7.3.0 | 7.3.0 | <p>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.</p> <p>To enable or disable this module and set threshold values, edit the Firewall Management Center health policy: System (⚙️) > Health > Policy > Device Policy.</p> <p>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.</p> <p>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.</p> <p>For more information, see Hardware/Environment Status Metrics in the administration guide.</p> |

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|---|---------------------------|------------------------|--|
| Licensing | | | |
| Changes to license names and support for the Carrier license. | 7.3.0 | Any | <p>We renamed licenses as follows:</p> <ul style="list-style-type: none"> • 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 <p>In addition, you can now apply the Carrier license, which allows you to configure GTP/GPRS, Diameter, SCTP, and M3UA inspections.</p> <p>New/modified screens: System (⚙️) > Licenses > Smart Licenses</p> <p>For more information, see Licenses in the administration guide.</p> |
| Administration | | | |
| Migrate configurations from FlexConfig to web interface management. | 7.3.0 | Feature dependent | <p>You can now easily migrate these configurations from FlexConfig to web interface management:</p> <ul style="list-style-type: none"> • 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 <p>After you migrate, you cannot deploy until you remove the deprecated FlexConfigs.</p> <p>New/modified screens: Devices > FlexConfig > Edit FlexConfig Policy > Migrate Config</p> <p>For more information, see Migrating FlexConfig Policies in the device configuration guide.</p> |

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|--------------------------|---------------------------|------------------------|--|
| Automatic VDB downloads. | 7.3.0 | Any | <p>The initial setup on the Firewall 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.</p> <p>New/modified screens: The Vulnerability Database check box is now enabled by default in the system-created Weekly Software Download scheduled task.</p> <p>For more information, see Vulnerability Database Update Automation in the administration guide.</p> |
| Install any VDB. | 7.3.0 | Any | <p>Starting with VDB 357, you can now install any VDB as far back as the baseline VDB for that Firewall Management Center.</p> <p>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.</p> <p>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.</p> <p>For more information, see Update the Vulnerability Database in the administration guide.</p> |

Usability, Performance, and Troubleshooting

| | | | |
|--|-------|-----|---|
| 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. |

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|---|---------------------------|------------------------|---|
| Performance profile for CPU core allocation on the Firepower 4100/9300 and Firewall Threat Defense Virtual. | 7.3.0 | 7.3.0 | <p>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).</p> <p>We added the Performance Profile page to the platform settings policy.</p> <p>For more information, see Configure the Performance Profile in the device configuration guide.</p> |

Deprecated Features

| | | | |
|--|-------|-------|--|
| End of support: Firepower 4110, 4120, 4140, 4150. | — | 7.3.0 | You cannot run Version 7.3+ on the Firepower 4110, 4120, 4140, or 4150. |
| End of support: 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 | <p>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.</p> <p>Note that this is a Snort 2 feature that is not available for Snort 3.</p> <p>You should redo your configurations after upgrade.</p> |
| Deprecated: Cluster health monitor settings with FlexConfig. | 7.3.0 | Any | <p>You can now edit cluster health monitor settings from the Firewall 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.</p> <p>You should redo your configurations after upgrade.</p> |
| Deprecated: BFD for BGP with FlexConfig. | 7.3.0 | Any | <p>You can now configure bidirectional forwarding detection (BFD) for BGP routing from the Firewall Management Center web interface. If you do this, you cannot deploy until you remove any deprecated FlexConfigs.</p> <p>You should redo your configurations after upgrade.</p> |
| Deprecated: ECMP zones with FlexConfig. | 7.3.0 | Any | <p>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.</p> <p>You should redo your configurations after upgrade.</p> |
| Deprecated: VXLAN interfaces with FlexConfig. | 7.3.0 | Any | <p>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.</p> |

Firewall Device Manager Features in Version 7.3.x

Table 5: Firewall 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 <p>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.</p> <p>See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide</p> |
| 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 |
|---|---|
| Firepower 1010E does not support Version 7.3. | <p>The Firepower 1010E, which was introduced in Version 7.2.3, does not support Version 7.3. Support returns in Version 7.4.</p> <p>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.</p> |

Firewall and IPS Features

| | |
|--|--|
| TLS 1.3 support in SSL decryption policies, and configurable behavior for undecryptable connections. | <p>Upgrade impact.</p> <p>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.</p> <p>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.</p> <p>See: Advanced Criteria for SSL Decryption Rules and Configure Advanced and Undecryptable Traffic Settings</p> |
| Refined URL filtering lookup. | <p>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.</p> <p>See: Configuring URL Filtering Preferences</p> |


Interface Features

| | |
|--------------------------------------|---|
| IPv6 support for virtual appliances. | <p>Threat defense virtual now supports IPv6 in the following environments:</p> <ul style="list-style-type: none"> • AWS • Azure • KVM • VMware <p>See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide</p> |
| DHCPv6 Client. | <p>You can now obtain an IPv6 address from DHCPv6.</p> <p>New/modified screens: Device > Interfaces > Edit Interface > Advanced</p> <p>See: Configure Advanced Interface Options</p> |

Administrative and Troubleshooting Features

| Feature | Description |
|---|--|
| Automatically update CA bundles. | <p>Upgrade impact. The system connects to Cisco for something new.</p> <p>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.</p> <p>New resources: https://cisco.com/security/pki/</p> <p>New/modified CLI commands: configure cert-update auto-update, configure cert-update run-now, configure cert-update test, show cert-update</p> <p>Version restrictions: Requires Version 7.0.5, 7.1.0.3, or 7.2.4+. Not supported with Version 7.0.0–7.0.4, 7.1.0–7.1.0.2, or 7.2.0–7.2.3.</p> <p>See: Cisco Secure Firewall Threat Defense Command Reference</p> |
| Skip Certificate Authority checking for trusted certificates. | <p>You can skip the check if you need to install a local CA certificate as the trusted CA certificate.</p> <p>We added the Skip CA Certificate Check option when uploading trusted CA certificates.</p> |

| Feature | Description |
|--|---|
| Combined upgrade and install package for Secure Firewall 3100. | <p>Reimage Impact.</p> <p>In Version 7.3, we combined the Firewall Threat Defense install and upgrade package for the Secure Firewall 3100, as follows:</p> <ul style="list-style-type: none"> • Version 7.1–7.2 install package: <code>cisco-ftd-fp3k.version.SPA</code> • Version 7.1–7.2 upgrade package: <code>Cisco_FTD_SSP_FP3K_Upgrade-version-build.sh.REL.tar</code> • Version 7.3+ combined package: <code>Cisco_FTD_SSP_FP3K_Upgrade-version-build.sh.REL.tar</code> <p>Although you can upgrade Firewall Threat Defense without issue, you cannot reimage from older Firewall Threat Defense and ASA versions directly to Firewall 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.</p> <p>To get to Firewall Threat Defense Version 7.3+, your options are:</p> <ul style="list-style-type: none"> • Upgrade from Firewall Threat Defense Version 7.1 or 7.2 — use the normal upgrade process. See the appropriate Upgrade Guide. • Reimage from Firewall Threat Defense Version 7.1 or 7.2 — reimage to ASA 9.19+ first, then reimage to Firewall Threat Defense Version 7.3+. <ul style="list-style-type: none"> See <i>Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100</i> and then <i>ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100</i> 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 Firewall Threat Defense Version 7.3+. <ul style="list-style-type: none"> See the Cisco Secure Firewall ASA Upgrade Guide and then <i>ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100</i> in the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide. • Reimage from Firewall Threat Defense Version 7.3+ — use the normal reimage process. See <i>Reimage the System with a New Software Version</i> in the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense. |

| Feature | Description |
|--|---|
| Firewall Threat Defense REST API version 6.4 (v6). | <p>The Firewall 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.</p> <p>Please re-evaluate all existing calls, as changes might have been made to the resource models you are using. To open the API Explorer, where you can view the resources, log into Firewall Device Manager, then click the more options button () and choose API Explorer.</p> <p>See: Cisco Secure Firewall Threat Defense REST API Guide</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 to avoid an undesirable outcome; for example, if you must change a configuration.



Important

Minimize upgrade and other impact by going directly to the latest maintenance release in your chosen version. See [Choosing your upgrade target, on page 28](#).

Upgrade Impact Features for Firewall Management Center

Table 6: Upgrade Impact Features for Firewall Management Center

| Target version | Features with upgrade impact |
|---------------------------------|---|
| 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 Firewall Management Center web interface. • Automatically update CA bundles. • Updated internet access requirements for Smart Licensing. |
| 7.2.0+ | <ul style="list-style-type: none"> • Configure VXLAN from the Firewall Management Center web interface. • Configure EIGRP from the Firewall Management Center web interface. |

| 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. |

Upgrade Impact Features for Firewall Threat Defense with Firewall Management Center

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

| Current version | Features with upgrade impact |
|---|--|
| 7.2.x and earlier | <ul style="list-style-type: none"> • Auto-upgrade to Snort 3 after successful Firewall Threat Defense upgrade is no longer optional. (7.3.0) • Combined upgrade and install package for Secure Firewall 3100. (7.3.0) • NetFlow support for Snort 3 devices. (7.3.0) |
| 7.2.0–7.2.3 7.1.0–7.1.0.2 7.0.4 and earlier | <ul style="list-style-type: none"> • Automatically update CA bundles. (7.0.5) |
| 7.1.x and earlier | <ul style="list-style-type: none"> • Autoscale for Firewall Threat Defense Virtual for GCP. (7.2.0) |
| 7.0.x and earlier | <ul style="list-style-type: none"> • Snort 3 support for inspection of DCE/RPC over SMB2. (7.1.0) • Snort 3 support for ssl_version and ssl_state keywords. (7.1.0) |
| 6.7.x and earlier | <ul style="list-style-type: none"> • End of support: VMware vSphere/VMware ESXi 6.0. (7.0.0) • FTDv performance tiered Smart Licensing. (7.0.0) • Deprecated: RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm. (7.0.0) • Deprecated: MD5 authentication algorithm and DES encryption for SNMPv3 users. (7.0.0) |

Upgrade Impact Features for Firewall Threat Defense with Firewall Device Manager

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

| Target version | Features |
|----------------|--|
| 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. • Firepower 1010E does not support Version 7.3. • 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. |

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—which can include interruptions to traffic flow and inspection—see the appropriate upgrade guide: [For Assistance, on page 43](#).

Upgrade Guidelines for Firewall Management Center

Table 9: Upgrade Guidelines for Firewall Management Center

| Current Version | Guideline | Details |
|-----------------|--|--|
| 7.2.6–7.2.x | Upgrade not recommended: Version 7.2.6–7.2.x to Version 7.3.x–7.4.0. | Upgrading is supported, but will remove critical fixes and enhancements that are included in your current version. Instead, upgrade to Version 7.4.1+. |

Upgrade Guidelines for Firewall Threat Defense with Firewall Device Manager

Table 10: Upgrade Guidelines for Firewall Threat Defense

| Current Version | Guideline | Details |
|-----------------|-----------|--|
| Any | — | There are no known issues for this version right now, but you should still check for open issues and features with upgrade impact. |

Upgrade Guidelines for Firewall Threat Defense with Firewall Management Center

Table 11: Upgrade Guidelines for Firewall Threat Defense

| Current Version | Guideline | Details |
|-----------------|-----------|--|
| Any | — | There are no known issues for this version right now, but you should still check for open issues and features with upgrade impact. |

Upgrade Guidelines for the Firepower 4100/9300 Chassis

In most cases, we recommend you use the latest build for your FXOS major version.

For release-specific FXOS upgrade warnings and guidelines, as well as features and bugs with upgrade impact, check all release notes between your current and target version: <http://www.cisco.com/go/firepower9300-rns>.

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 and order is especially important for large deployments, high availability/clustering, multi-hop upgrades, and situations where you need to coordinate chassis, hosting environment, or other upgrades. Those scenarios, as well as information on revert and uninstall, are covered in more detail in the upgrade guide: [For Assistance, on page 43](#).

Choosing your upgrade target

Go **directly to the latest maintenance release** to minimize upgrade and other impact.

Features, enhancements, and critical fixes can skip "future" releases that are ahead by version, but not by release date. For example, if you are up-to-date within major Version A, upgrading to dot-zero Version B can deprecate features and fixes.

If you cannot go to the latest release, at least make sure your current version was released on a date before your target version. In the following table, confirm your current version is listed next to your target version. If it is not, choose a later target.

Table 12: Released before Version 7.3.x, by date

| Target version | | Current version: confirm yours is listed. | | | |
|----------------|------------|---|-----|-----|-----|
| | | from 7.0 | 7.1 | 7.2 | 7.3 |
| to 7.3.1 * | 2022-11-29 | — | — | — | — |
| to 7.3.0 * | 2024-09-16 | — | — | — | — |

* Version 7.3.x removes significant features, enhancements, and critical fixes included in earlier versions. Upgrade to a later release.

Upgrading from a patched deployment

Critical fixes in patches (fourth-digit) releases can also skip future releases. If you depend on these critical fixes, verify that your target version contains them. For a full list of release dates, see [Cisco Secure Firewall Management Center New Features by Release](#) or [Cisco Secure Firewall Device Manager New Features by Release](#).

Supported upgrades and downgrades

This section summarizes upgrade and downgrade capability. For help with:

- Choosing an upgrade target, see [Choosing your upgrade target, on page 28](#).
- Upgrade and downgrade procedures, including general guidelines, best practices, and troubleshooting, see the upgrade guide for the version you are currently running: <https://www.cisco.com/go/ftd-upgrade>.

Supported upgrades

This table shows the supported direct upgrades for Firewall Management Center and Firewall Threat Defense software.



Note You can upgrade directly to any major (first and second-digit) or maintenance (third digit) release. Patches change the fourth digit only. You cannot upgrade directly to a patch from a previous major or maintenance release. Although a patched device (fourth-digit) can be managed with an unpatched Firewall Management Center, fully patched deployments undergo enhanced testing.

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

Table 13: Supported direct upgrades

| Current version | Target software version | | | | | | |
|-----------------|---|------|-------|------|------|------|------|
| | to 7.7 | 7.6 | 7.4 * | 7.3 | 7.2 | 7.1 | 7.0 |
| | FXOS version for Firepower 4100/9300 chassis upgrades | | | | | | |
| | to 2.17 | 2.16 | 2.14 | 2.13 | 2.12 | 2.11 | 2.10 |
| from 7.7 | YES | — | — | — | — | — | — |
| from 7.6 | YES | YES | — | — | — | — | — |
| from 7.4 | YES | YES | YES | — | — | — | — |
| from 7.3 | YES | YES | YES | YES | — | — | — |
| from 7.2 | YES | YES | YES | YES | YES | — | — |
| from 7.1 | — | YES | YES | YES | YES | YES | — |
| from 7.0 | — | — | YES | YES | YES | YES | YES |

| Current version | Target software version | | | | | | |
|-----------------|---|------|-------|------|------|------|------|
| | to 7.7 | 7.6 | 7.4 * | 7.3 | 7.2 | 7.1 | 7.0 |
| | FXOS version for Firepower 4100/9300 chassis upgrades | | | | | | |
| | to 2.17 | 2.16 | 2.14 | 2.13 | 2.12 | 2.11 | 2.10 |
| from 6.4 | — | — | — | — | — | — | YES |

* You cannot upgrade Firewall Threat Defense to Version 7.4.0, which is available as a fresh install on the Secure Firewall 4200 only, and is not supported with Firewall Device Manager. It removes significant features, enhancements, and critical fixes included in earlier versions. Upgrade to a later release.

Supported downgrades

If an upgrade or patch succeeds but the system does not function to your expectations, you may be able to revert (Firewall Threat Defense upgrades) or uninstall (Firewall Threat Defense and Firewall Management Center patches). For general information, particularly on common scenarios where returning to a previous version is not supported or recommended, see the upgrade guide: <https://cisco.com/go/fd-upgrade>.

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.



Important

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

Open Bugs in Version 7.3.0

Table last updated: 2024-04-08

Table 14: 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 |

| Bug ID | Headline |
|----------------------------|--|
| 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 times 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 15: 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 |
| 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. |

| Bug ID | Headline |
|----------------------------|--|
| CSCwh71358 | Unable to create VRF via FDM in Firepower 3105 device |
| CSCwi08392 | Configuring /32 make 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: 2025-02-25

Table 16: 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 |
| CSCwd66820 | Cisco Firepower Management Center Object Group Access Control List Bypass Vulnerability |
| 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 |
| CSCwe33819 | Snort2 ENH: Use a common pattern matcher list for CN and SNI patterns in apps |
| 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 |
| CSCwf71606 | Cisco ASA and FTD ACLs Not Installed upon Reload |

Resolved Bugs in Version 7.3.1

Table last updated: 2023-05-30

Table 17: 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 18: 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 |
| 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 |

| Bug ID | Headline |
|----------------------------|--|
| 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" |
| 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 |

| Bug ID | Headline |
|----------------------------|--|
| 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 |
| 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 |

| Bug ID | Headline |
|----------------------------|--|
| 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. |
| 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 |

| Bug ID | Headline |
|----------------------------|--|
| 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 |
| 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 |

| Bug ID | Headline |
|----------------------------|---|
| 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 extremely 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" |
| 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 |

| Bug ID | Headline |
|----------------------------|---|
| 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 |
| 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 |

| Bug ID | Headline |
|----------------------------|--|
| 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 permitted 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 |
| 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 |

| Bug ID | Headline |
|----------------------------|--|
| 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 generated 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. |
| 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 deployment |
| 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 |

| Bug ID | Headline |
|----------------------------|--|
| 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 |
| 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 |

| Bug ID | Headline |
|----------------------------|--|
| 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 Firewall Management Center deployments, the Firewall Management Center must run the same or newer maintenance (third-digit) release as its managed devices. Upgrade the Firewall Management Center first, then devices. Use the upgrade guide for the version you are *currently* running—not your target version.

Table 19: Upgrade Guides

| Platform | Upgrade Guide | Link |
|---|--|---|
| Firewall Management Center | Firewall Management Center version you are <i>currently</i> running. | https://cisco.com/go/fmc-upgrade |
| Firewall Threat Defense with Firewall Management Center | Firewall Management Center version you are <i>currently</i> running. | https://cisco.com/go/ftd-fmc-upgrade |
| Firewall Threat Defense with device manager | Firewall Threat Defense version you are <i>currently</i> running. | https://cisco.com/go/ftd-fdm-upgrade |
| Firewall Threat Defense with Cloud-Delivered Firewall Management Center | Cloud-Delivered Firewall Management Center. | https://cisco.com/go/ftd-cdfmc-upgrade |

Install Guides

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

Table 20: Install Guides

| Platform | Install Guide | Link |
|---|--|--|
| Firewall Management Center hardware | Getting started guide for your Firewall Management Center hardware model. | https://cisco.com/go/fmc-install |
| Firewall Management Center Virtual | Getting started guide for the Firewall Management Center Virtual. | https://cisco.com/go/fmcv-quick |
| Firewall Threat Defense hardware | Getting started or reimage guide for your device model. | https://cisco.com/go/ftd-quick |
| Firewall Threat Defense Virtual | Getting started guide for your Firewall Threat Defense Virtual version. | https://cisco.com/go/ftdv-quick |
| FXOS for the Firepower 4100/9300 | Configuration guide for your FXOS version, in the <i>Image Management</i> chapter. | https://cisco.com/go/firepower9300-config |
| FXOS for the Firepower 1000/2100 and Secure Firewall 3100 | 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: <https://cisco.com/go/threatdefense-73-docs>
- Cisco Support & Download site: <https://cisco.com/c/en/us/support/index.html>
- Cisco Bug Search Tool: <https://tools.cisco.com/bugsearch/>
- Cisco Notification Service: <https://cisco.com/cisco/support/notifications.html>

Access to most tools on the Cisco Support & Download site requires a Cisco.com user ID and password.

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): [Cisco Worldwide Support Contacts](#)

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

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

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

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

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

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

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

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

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

© 2022 –2025 Cisco Systems, Inc. All rights reserved.