Cisco Secure Firewall Management Center New Features by Release

First Published: 2021-03-26

Last Modified: 2026-10-07

New Features by Release

This document describes new and deprecated features for each release.

Device Management

Although you can manage older devices with a newer Firewall Management Center, we recommend you always update your entire deployment. New traffic-handling features usually require the latest release on both the Firewall Management Center *and* device. Features where devices are not obviously involved (cosmetic changes to the web interface, cloud integrations) may only require the latest version on the Firewall Management Center, but that is not guaranteed.

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.

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 the Release Notes for Secure Firewall Threat Defense.

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 with Firewall Management Center starting in Version 7.0.



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*

Suggested release: Version 7.6.6

The current suggested release is Version 7.6.6.

To take advantage of new features and resolved issues, we recommend you upgrade all eligible appliances to at least the suggested release, including the latest patch. On the Cisco Support & Download site, the suggested release is marked with a gold star. In Version 7.2.6+/7.4.1+, the Firewall Management Center notifies you when a new suggested release is available, and indicates suggested releases on its product upgrades page.

Suggested releases for older appliances

If an appliance is too old to run the suggested release and you do not plan to refresh the hardware right now, choose a major version then upgrade or patch as far as possible. Some major versions are designated *long-term* or *extra long-term*, so consider one of those. For an explanation of these terms, see *Cisco's Next Generation Firewall Product Line Software Release and Sustaining Bulletin*.

If you are interested in a hardware refresh, contact your Cisco representative or partner contact.

Firewall Management Center Features in Version 10.1.0

Deployment and policy management

Table 1: Deployment and policy management features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Access control rule expansion analysis	10.1.0	10.1.0	The system now identifies access control rules that expand significantly when deployed, which can consume device memory and prevent deployment. Warnings and filters in the access control policy help you identify high-expansion rules. You can also warn or block deployment when the resulting expansion would exceed device limits. These validations are enabled by default in new deployments, but upgrading does not enable them. To enable or disable validations, use the access control preferences, which apply to all access control policies on Firewall Management Center: **Administration** > **Configuration** > **Access Control Preferences**. Refer to Access control rule expansion.

Encrypted traffic handling

Table 2: Encrypted traffic handling features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
DNS inspection for DNS over HTTPS and DNS over QUIC	10.1.0	10.1.0	You can now use DNS policies to handle *decrypted* DNS over HTTPS (DoH) and DNS over QUIC (DoQ) traffic, including DoH over HTTP/1.1, HTTP/2, and HTTP/3. Sinkhole actions support only A and AAAA DNS record types. For DNS over HTTP/3 and DNS over QUIC, the Sinkhole and Domain Not Found actions cannot inject a sinkhole address or an NXDOMAIN response; those actions behave as Block. Refer to DNS over HTTPS and QUIC.
Enhanced encrypted traffic visibility for SSH and STUN	10.1.0	10.1.0	The encrypted visibility engine (EVE) can now derive fingerprints from SSH key exchange initiation and STUN binding request attributes, and identify client processes for SSH and STUN traffic. This information is available in connection events and EVE dashboards, and can be used for policy enforcement. Refer to View Encrypted Visibility Engine events.

Health monitoring

Table 3: Health monitoring features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Identity mapping limits monitoring for Secure Firewall 200	10.1.0	Any	The Identity Limits Monitor health module for the Secure Firewall 200 monitors two download limits and generates alerts when either limit is exceeded: • A cumulative limit of 10,000 user sessions, SXP/SGT mappings, endpoint profiles, and dynamic objects. • A separate limit of 10,000 user-group mappings. When a limit is reached, the device stops downloading objects for the affected category. Refer to Health alerts for the Secure Firewall 200.

High availability and scalability

Table 4: Firewall Management Center high availability features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
High availability for Firewall Management Center Virtual for Nutanix (FMCv25)	10.1.0	Any	Firewall Management Center Virtual for Nutanix with a 25-device license (FMCv25) now supports high availability. Platform restrictions: Not supported with FMCv2 or FMCv10. Refer to High Availability.

Identity

Table 5: Identity features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Higher identity mapping limits (Beta)	10.1.0	10.1.0	More efficient memory use allows most devices to support more identity mappings, which associate IP addresses with identity information. The native instance (application mode) limit is based on model. Except for the Secure Firewall 200, most devices at least doubled their previous limit. The container instance (multi-instance mode) limit depends on available memory and also increased for instances with 24 GB or less and 256 GB or more RAM. We also greatly increased the maximum number of user groups and dynamic objects you can use in an access control policy. The system uses two health modules to alert you to issues related to mappings. The Snort Identity Memory Usage health module alerts when identity memory use is high. The Identity Limits Monitor health module for the Secure Firewall 200 alerts when the device exceeds its mapping limits. Refer to Maximum mappings per device and Maximum user mappings in multi-instance devices for the new maximum values. **Note** This is a Beta feature in Version 10.1.0. Support may be limited. Taking full advantage of the new maximums can increase memory use on the device. Carefully evaluate and monitor memory use in larger deployments, and apply identity mapping filters if necessary.
Microsoft Entra ID RA VPN as an identity source (Beta)	10.1.0	10.1.0	You can now use Microsoft Entra ID-authenticated remote access VPN sessions for identity-based access control. When a user authenticates with Microsoft Entra ID using SAML, the system correlates the VPN session with user and group data from the corresponding Entra ID realm. You can then use this identity information in access control rules. You do not need to configure a separate identity policy. Deployment restrictions: Not supported with clustered devices. **Note** This is a Beta feature in Version 10.1.0. Support may be limited. Refer to Remote Access VPN for Microsoft Entra ID-authenticated users.
Passive identity without the dynamic attributes connector	10.1.0	Any	You can now configure the passive identity agent identity source without enabling the dynamic attributes connector. Refer to Identity Source: Passive Identity Agent.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Resynchronize identity information on managed devices	10.1.0	10.1.0	When a device's identity information is missing, incomplete, or out of sync with Firewall Management Center, rules with user conditions may not match traffic as expected. A new **Resynchronize identity** option on the Device Management page reinitializes the identity feed connections and resynchronizes user identities from Firewall Management Center to the device. Use this action only after standard troubleshooting, and generate troubleshooting files for Firewall Management Center and devices before you begin. The reinitialization may briefly interrupt ongoing user sessions. Refer to Resynchronize identities.

Integrations

Table 6: Integrations features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Air-gapped support for the dynamic attributes connector	10.1.0	Any	You can now use the dynamic attributes connector with an air-gapped Firewall Management Center. This allows you to get changing network attributes from supported local sources and use the resulting dynamic objects in access control policies. Air gap mode supports Cisco APIC, Cisco Cyber Vision, vCenter, and generic text. To install and update the dynamic attributes connector in an air-gapped deployment, use **Administration** > **Content Updates** > **Dynamic Attributes Connector Updates**. Refer to Air gap mode.

Logging and analysis

Table 7: Logging and analysis features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cluster syslog class	10.1.0	10.1.0	Firewall Threat Defense now provides a `cluster` syslog class for messages in the 747, 748, and 785 ranges. You can set the logging level and destination for all cluster-related messages as a group. Refer to Syslog message classes and associated message ID numbers.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Default logging for new access control rules	10.1.0	Any	By default, connection logging is disabled in new access control rules—except Monitor rules, which automatically log the ends of monitored connections. You can now change this default so that connection logging is enabled in new access control rules. Changing the default does not change existing rules, and logging remains configurable for individual rules. For rules with Block actions, you can enable default beginning-of-connection logging. For rules with Allow, Trust, and Interactive Block actions, you can enable default beginning- or end-of-connection logging. If you change a rule's action, the system replaces the rule's logging settings with the defaults for the new action. To configure this setting, use the access control preferences, which apply to all access control policies on Firewall Management Center: **Administration** > **Configuration** > **Access Control Preferences**. Refer to Configure access control preferences.

Model migration

Table 8: Firewall Threat Defense Model migration features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Migrate Firepower 1100 to Secure Firewall 1200	10.1.0	See feature details	You can now use Firewall Management Center to migrate configurations from the Firepower 1100 to the Secure Firewall 1200, with these version requirements: • Source device (Firepower 1100): Version 7.3+ • Target device (Secure Firewall 1210): Version 7.6+ • Target device (Secure Firewall 1230, 1240, and 1250): Version 7.7+ Refer to Cisco Secure Firewall Threat Defense Model Migration Guide.
Migrate Firepower 2100 to Secure Firewall 1200	10.1.0	See feature details	You can now use Firewall Management Center to migrate configurations from the Firepower 2100 to the Secure Firewall 1200, with these version requirements: • Source device (Firepower 2100): Version 7.4+ • Target device (Secure Firewall 1210): Version 7.6+ • Target device (Secure Firewall 1230, 1240, and 1250): Version 7.7+ Refer to Cisco Secure Firewall Threat Defense Model Migration Guide.

Performance and resiliency

Table 9: Performance and resiliency features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Memory buffer (MBUF) depletion monitoring for the Secure Firewall 200 and 1200	10.1.0	10.1.0	The Secure Firewall 200 and 1200 now monitor for memory buffer (MBUF) depletion, which can interrupt traffic flow. When depletion is detected, the device reports a critical fault, collects troubleshooting data, and reloads. This feature is automatically enabled on new and upgraded standalone devices. For high availability pairs, it is disabled by default; enabling it causes failover in case of depletion. To enable or disable monitoring, change the monitoring interval, or disable the automatic reload, use FlexConfig with the `fault-monitor mbuf-depletion` command. Refer to Memory buffer monitoring and fault-monitor mbuf-depletion.

Public and private cloud

Table 10: Public and private cloud features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firewall Threat Defense Virtual compute options for public clouds	10.1.0	10.1.0	We added support for these cloud compute options for Firewall Threat Defense Virtual: • Alibaba Cloud ECS instance families: c7nex, c8i, c8ine, and c9i • AWS EC2 instance families: C6id, C7a, C7i, C7i-flex, M5, M6a, M6i, M6in, M7a, M7i, M7i-flex, R6i, R6id, and R7i • Azure VM sizes: Standard_D8s_v6 and Standard_D16s_v6 • Google Cloud Compute Engine machine types: t2d-standard-4, t2d-standard-8, and t2d-standard-16 • OCI compute shapes: VM.Standard.E5.Flex and VM.Standard.E6.Flex Refer to Cisco Secure Firewall Threat Defense Virtual Getting Started Guide, Version 10.1.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firewall Management Center Virtual compute options for public clouds	10.1.0	Any	We added support for these cloud compute options for Firewall Management Center Virtual: • Alibaba Cloud ECS instance families: g9i, r8i, and r9i • AWS EC2 instance families: C5n, C6a, C6i, C6id, C7a, C7i, C7i-flex, M6in, M7a, M7i, R6i, and R6id • Azure VM size: Standard_F16s_v2 • Google Cloud Compute Engine machine types: n2d-standard-8, n2d-standard-16, t2d-standard-8, and t2d-standard-16 • OCI compute shapes: VM.Standard.E5.Flex and VM.Standard.E6.Flex Refer to *Cisco Secure Firewall Management Center Virtual Getting Started Guide*.
Unlimited performance tier (FTDvU) for AWS	10.1.0	10.1.0	Firewall Threat Defense Virtual for AWS now supports an unlimited performance tier (FTDvU). This tier does not rate limit and the remote access VPN session limit depends on the allocated resources: • 20,000 sessions with 32 vCPU and 64 GB RAM • 32,000 sessions with 64 vCPU and 128 GB RAM Refer to Deploy Firewall Threat Defense Virtual Unlimited.

Routing

Table 11: Routing features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Multicast routing over static virtual tunnel interfaces	10.1.0	10.1.0	You can securely deliver real-time multicast applications, such as video streaming, financial data feeds, and data replication, over your VPN infrastructure by using IPsec tunnels configured with static VTI. Refer to Multicast routing over static virtual tunnel interface tunnel.
Support for up to 250 virtual routers on the Secure Firewall 4200 and 6100	10.1.0	10.1.0	Secure Firewall 4200 and 6100 now support up to 250 virtual routers. Previously, the limit was 100. Refer to Maximum number of virtual routers by device model.

Threat detection and application identification

Table 12: Threat detection and application identification features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Expanded Snort ML inspection for web traffic	10.1.0	10.1.0	Expanding its coverage of web-based threats, the snort_ml inspector now examines URL queries, URL-encoded POST data, and multipart/form-data POST data in addition to the HTTP URI. Also, the inspector is now enabled in the security over connectivity default policies. Previously, it was only enabled in maximum detection. Refer to SnortML.

Troubleshooting and serviceability

Table 13: Troubleshooting and serviceability features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
BGP-4 MIB support for SNMP monitoring	10.1.0	10.1.0	You can now monitor BGP peer connections on Firewall Threat Defense devices using SNMP polling of the BGP-4 MIB. The supported objects provide BGP peer state, administrative status, total inbound and outbound messages, the number of transitions into the Established state, and the time since the peer entered—or was last in—the Established state. BGP over IPv6 and VRF- or context-specific data are not supported. Refer to Supported tables and objects in MIBs.
In-product support	10.1.0	Any	From **Help** > **Support**, you can open a Cisco TAC case and share troubleshooting files or screen recordings. Refer to Cisco in-product support in Firewall Management Center.
Unified connection and inspection data in `show conn detail`	10.1.0	10.1.0	The `show conn detail` command now provides a unified view of how Firewall Threat Defense handles and inspects each connection. Previously, the command displayed only connection-handling information. The expanded output correlates this information with traffic-inspection status and statistics, including idle time, uptime, timeout, TCP state, and client/server packet and byte counters. It also indicates when inspection information is unavailable for a connection. This makes it easier to troubleshoot differences between connection handling and traffic inspection from a single command. Refer to show conn.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Scheduled diagnostic data collection	10.1.0	10.1.0	Use the Firewall Threat Defense CLI to schedule diagnostic `show` commands to run in the background and log their output. New CLI commands are: • `system support monitor`: schedule tasks for data collection • `show monitor`: view active scheduled tasks or details for a specific task • `clear monitor`: stop an individual task or all tasks Platform restrictions: Not supported with Secure Firewall 200. Refer to system support monitor, show monitor, and clear monitor.

Upgrade

Table 14: Upgrade features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
All-or-none option for unattended device upgrade	10.1.0	Any	When you start an unattended upgrade, a new **Require all devices to be eligible to advance** option allows you to enforce an "all or none" requirement. If a selected device cannot upgrade for any reason, no devices upgrade. For example, if one device cannot get the upgrade package or pass required checks, the entire process stops. Disable this option to let eligible devices proceed independently. Refer to Upgrade Firewall Threat Defense in unattended mode.

URL filtering

Table 15: URL filtering features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Contextual information on HTTP response pages	10.1.0	Any	You can now include contextual information when you block a website to help your users understand why it happened. This includes basic information like the requested URL and its category and reputation, but can also include session details like username, application, protocol, source and destination addresses and ports, geolocation, and the matching access control rule. To use this feature, configure a custom HTTP response page in the access control policy. In the HTML, use variables to show the information you want. For example, use `{{REPUTATION}}` to show the URL reputation. For a full list of supported variables, see the online help. Refer to Display contextual information on HTTP response pages.

VPN

Table 16: Site-to-site VPN features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Secure branch traffic with Secure Access	10.1.0	Any	When you configure a site-to-site VPN, you can now select a SASE topology to establish IPsec IKEv2 tunnels between Firewall Threat Defense and Secure Access. Depending on your configuration, you can use these tunnels to send branch internet traffic to Secure Access for inspection or to provide remote universal ZTNA users with access to private applications. A wizard steps you through specifying the Secure Access region, Firewall Threat Defense endpoints, tunnel credentials, and routing options. When you finish, the system creates the virtual tunnel interfaces and SASE VPN topology and pushes the corresponding tunnel configuration to Secure Access. You must separately configure the access list, static route, and policy-based routing required to direct traffic through the tunnels. Deployment restrictions: Not supported with clustered devices. Refer to Secure traffic using Cisco Secure Access and Firewall Threat Defense devices.

Zero trust access

Table 17: Zero trust access features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Universal ZTNA enhancements	10.1.0	10.1.0	**Upgrade impact. Upgrading a universal ZTNA device interrupts traffic until the post-upgrade deploy.** Universal ZTNA has these enhancements: • Additional model support. Universal ZTNA no longer requires 16 cores and is now supported on all device models. • No reboots. To minimize disruption, enabling or disabling universal ZTNA requires only a deployment, not a device reboot. • IPv6 support. Universal ZTNA now supports IPv6 for connections to the device, and connections from the device to protected applications. The outer and inner connections can use different IP versions. IPv6 source NAT is also supported. • Automatic trustpoints. When you deploy universal ZTNA, the system automatically creates the trustpoints required for certificate-based authentication with Secure Access. **Note** Due to framework changes, upgrading a universal ZTNA device to Version 10.1+ from older versions disables the feature. Traffic is interrupted until you deploy from Firewall Management Center. Refer to Universal Zero Trust Network Access.

Deprecated features

Table 18: Deprecated features in Version 10.1.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: Walkthroughs	10.1.0	Any	Walkthroughs (how-tos) are no longer available. For a list of supported walkthroughs by version, see Walkthroughs in Secure Firewall Management Center.

Firewall Management Center Features in Version 10.0.2

There are no new features in this release.

Firewall Management Center Features in Version 10.0.1

There are no new features in this release.

Firewall Management Center Features in Version 10.0.0

Reintroduced features

These Version 10.0.0 features were actually introduced in earlier releases, but may be new to you depending on your current version:

- Umbrella integration with Firewall Management Center over a proxy. (7.4.3)
- DC power supply for the Secure Firewall 4200 (7.4.3)
- Migrate select Firepower 4100/9300 models to Secure Firewall 3100/4200. (7.6.1)
- High availability for Firewall Management Center Virtual for OpenStack. (7.6.4)
- Universal Zero Trust Network Access (universal ZTNA) (7.7.10)

Content updates

Table 19: Content updates features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Updated internet access requirements for security intelligence feeds	10.0.0	Any	**Upgrade impact. The system connects to new resources.** The system now gets Security Intelligence feeds from: • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com • Security Services Exchange regional cloud If you are using regular Smart Licensing, registering with Smart Software Manager (CSSM) sets up SSE integration. If you are using Specific License Reservation in a non-airgapped deployment, enable Security Cloud Control for access to the Security Services Exchange regional cloud. The system no longer requires access to intelligence.sourcefire.com.

Deployment and policy management

Table 20: Deployment and policy management features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Simultaneous editing of access control policies by multiple users	10.0.0	Any	In previous releases, if two or more users simultaneously edited an access control policy, the first user who saved would retain their changes, and all other users would immediately lose all of their edits. Now, these users have the ability to selectively merge their changes, and changes that do not conflict with the first user's saved changes will automatically be accepted. This improves collaboration between users and reduces the need to lock the policy during edits.

Encrypted traffic handling

Table 21: Encrypted traffic handling features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
New decryption policy user interface, including basic and advanced policy creation	10.0.0	Any	Easily create standard decryption policies using a new interface tailored to the most common and effective scenarios, with single-page certificate management. Or, stick with the legacy wizard and advanced rules-based policy editor. After Firewall Management Center upgrade, existing policies are labeled as legacy policies and continue to work as before. You can switch from a standard policy to legacy, but not from legacy to standard.
Change server certificates without impacting decryption by using an internal certificate to decrypt/reencrypt traffic	10.0.0	10.0.0	You can now use a certificate and key defined in the decryption rule to decrypt traffic. This certificate and key can be the internal server's certificate or it can be a different certificate; in addition, you can change the certificate and key at any time. You can replace the certificate using the API, a system like the Automated Certificate Management Environment (ACME), or using Object Management.

Hardware

Table 22: Hardware features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firewall Management Center 1800, 2800, 4800	10.0.0	Any	We introduced the Firewall Management Center 1800, 2800, and 4800, with better performance and more event storage than current models. For these new models, eth0 is the main management port. You can use eth1, eth2, and eth3 as secondary management ports. The SFP ports are eth0 and eth1. This is different from earlier models.
Secure Firewall 200	10.0.0	10.0.0	The Secure Firewall 200 is an affordable security appliance for branch offices and remote locations that balances cost and features. During deployment, the system alerts you to any unsupported configurations. Version restrictions: In Version 10.0.0, the Secure Firewall 220 is the only supported device in the Secure Firewall 200 series.
Secure Firewall 6100	10.0.0	10.0.0	The Secure Firewall 6100 is an ultra-high-end firewall for demanding data center and telecom networks. It has exceptional price-to-performance, modular capability, and high throughput. The Secure Firewall 6100 supports Spanned EtherChannel and Individual interface clustering for up to 4 nodes. You must manage these devices with a Firewall Management Center. They do not support Firewall Device Manager.
View field-replaceable memory module details for the Secure Firewall 6100	10.0.0	10.0.0	You can view details, including operational status, for the field-replaceable memory module on the Secure Firewall 6100. New/modified screens: Choose **Devices** > **Device Management**, then edit the device and select the **Device** tab. In the **System** section, click **View** next to **Inventory** > **Memory**. New/modified Firewall Threat Defense commands: **show inventory** New/modified FXOS commands: **show dimm detail**
Network module for the Secure Firewall 4200	10.0.0	10.0.0	The FPR4K-XNM-6X1SXF for the Secure Firewall 4200 is a 6-port 1-Gbps SFP hardware bypass network module that operates in SX multimode. This network module has built-in SFP transceivers.

Health monitoring

Table 23: Health monitoring features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Event datastore alerts when connections fail	10.0.0	Any	The MonetDB Statistics health module now alerts when there are no active connections to the event database, which can indicate connection failure.

High availability and scalability

Table 24: Firewall Threat Defense high availability and scalability features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
More container instances (21) on the Secure Firewall 4225 in multi-instance mode	10.0.0	10.0.0	The Secure Firewall 4225 in multi-instance mode now supports 21 container instances. The previous limit was 14.
Cluster redirect: flow offload support for the Secure Firewall 4200 asymmetric cluster traffic	10.0.0	10.0.0	For asymmetric flows, cluster redirect lets the forwarding node offload flows to hardware. This feature is enabled by default but can be configured using FlexConfig. When traffic for an existing flow is sent to a different node, then that traffic is redirected to the owner node over the cluster control link. Because asymmetric flows can create a lot of traffic on the cluster control link, letting the forwarder offload these flows can improve performance. Added/modified commands: **flow-offload cluster-redirect** (FlexConfig), **show conn**, **show flow-offload flow**, **show flow-offload info**
IPsec flow offload for traffic on the cluster control link on the Secure Firewall 4200 in distributed site-to-site VPN mode	10.0.0	10.0.0	For asymmetric flows in distributed site-to-site VPN mode, IPsec flow offload now lets the flow owner decrypt IPsec traffic in hardware that was forwarded over the cluster control link. This feature is not configurable and is always available with IPsec flow offload. Added/modified commands: **show crypto ipsec sa detail**

Identity

Table 25: Identity features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Identity-based dynamic access control	10.0.0	7.3.0 (AD realm) 7.4.0 (Azure AD realm)	Handle traffic based on real-time user posture and risk by correlating identity and device context (from Cisco ISE or pxGrid Cloud) with Cisco Identity Intelligence (from Microsoft Entra ID or Cisco Duo).
pxGrid Cloud identity source	10.0.0	7.3.0 (AD realm) 7.4.0 (Azure AD realm)	The Cisco Identity Services Engine (Cisco ISE) pxGrid Cloud Identity Source enables you to use subscription and user data from a Cisco ISE server or cluster Cisco ISE in access control rules.

Integrations

Table 26: Integrations features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Dynamic security policy enforcement with the Cisco ACI Endpoint Update App and Dynamic Attributes Connector	10.0.0	Any	The dynamic attributes connector enables you to send Cisco APIC dynamic endpoint group (EPG) and endpoint security group (ESG) data from Cisco APIC tenants to the Firewall Management Center. Cisco APIC defines endpoint groups (EPGs) and endpoint security groups (ESGs) that have network object groups. Create a connector in the dynamic attributes connector that pulls that data from Cisco APIC tenants to the Firewall Management Center on which you can use those objects in access control rules.

Logging and analysis

Table 27: Logging and analysis features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Send security events to Splunk or other SIEM via syslog	10.0.0	10.0.0	A new Splunk integration wizard (**Integrations** > **Splunk**) and updated logging options in access control make it easier to send security events to Splunk (or any other SIEM via syslog)..
Generate and send protocol-aware (enriched) inspector logs via syslog	10.0.0	10.0.0	You can generate protocol-aware (enriched) inspector logs for traffic that you specify. Send these logs via syslog to Splunk or to any syslog server configured as an alert. To use this feature, enable advanced logging in your access control policy's advanced settings. Then, use access control rules to pinpoint the traffic where you want advanced logs. In those rules, enable the protocols you want to inspect. To receive alerts when there are communication issues between devices and the syslog server, enable the Snort 3 Statistics module in the device health policy.
Packet data included with intrusion events sent to Security Cloud Control	10.0.0	10.0.0	Packet data is now included with intrusion events sent to Security Cloud Control.

Model migration

Table 28: Firewall Management Center model migration features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firewall Management Center model migration wizard	7.4.7 (source) 10.0.0 (target)	7.3.0	A new wizard allows you to easily migrate from one Firewall Management Center model to another. Version restrictions: Not supported from a Version 7.6.x or 7.7.x Firewall Management Center. See: *Cisco Secure Firewall Management Center Model Migration Guide*
Migrate Firewall Management Center without upgrading first	7.4.7 (source) 10.0.0 (target)	7.3.0	You can now migrate an older Firewall Management Center to a Version 10.0+ Firewall Management Center without first upgrading the source system to the target version. **Note** Think of this process as a migration plus upgrade. Just as with regular upgrades, minimize impact by going **directly to the latest maintenance release** in your target major version. For release-specific upgrade warnings and guidelines, and for information on features and bugs with upgrade impact, see the Release Notes for Secure Firewall Threat Defense for your target version. Version restrictions: Not supported from a Version 7.6.x or 7.7.x Firewall Management Center. See: *Cisco Secure Firewall Management Center Model Migration Guide*
Migrate Firewall Management Center 1600/2600/4600 to 1800/2800/4800	7.4.7 (source) 10.0.0 (target)	7.3.0	Migrate from Firepower Management Center 1600/2600/4600 to Firewall Management Center 1800/2800/4800. Version restrictions: Not supported from a Version 7.6.x or 7.7.x Firewall Management Center. See: *Cisco Secure Firewall Management Center Model Migration Guide*
Migrate Firewall Management Center 4600 to Firewall Management Center Virtual 300 for Azure	7.4.7 (source) 10.0.0 (target)	7.3.0	Migrate from Firepower Management Center 4600 to Secure Firewall Management Center Virtual 300 for Azure. Version restrictions: Not supported from a Version 7.6.x or 7.7.x Firewall Management Center. See: *Cisco Secure Firewall Management Center Model Migration Guide*

Table 29: Firewall Threat Defense model migration features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Migrate Firepower 4100/9300 to Secure Firewall 3100, 4200, and 6100	10.0.0	Any (source) 7.4.1 (target)	Migrate to the Secure Firewall 3100, 4200, and 6100 from: • Firepower 4112, 4115, 4125, 4145 • Firepower 9300: SM-40, SM-48, SM-56
Migrate Firepower 1010 to Secure Firewall 200 and 1200	10.0.0	Any (source) 7.6.0 (target)	Migrate the Firepower 1010 and 1010E to the Secure Firewall 200 and 1200.

Performance and resiliency

Table 30: Performance and resiliency features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Block depletion autorecovery for clusters	10.0.0	10.0.0	The firewall block depletion fault manager introduced in Version 7.7.0 now supports clustered devices. Fault monitoring is automatically enabled on new and upgraded devices. To disable, use FlexConfig.
Other performance and resiliency improvements	Feature dependent	Feature dependent	We made performance and resiliency improvements to: • Deploying configuration changes • Event datastore on the Firewall Management Center • Event logging to external servers such as syslog or Security Cloud Control, for the Secure Firewall 4200 and 6100 • Install and upgrade • High availability for Firewall Threat Defense • Snort ML • Zero-touch provisioning
Improved cluster control link health check with high CPU	10.0.0	Any	When a cluster node CPU usage is high, the health check will be suspended, and the node will not be marked as unhealthy. This feature is enabled by default when the CPU usage reaches 90% but can be configured using FlexConfig. New/modified FlexConfig commands: **cpu-healthcheck-threshold**

Feature	Minimum Management Center	Minimum Threat Defense	Details
Ensure temporarily unavailable nodes can rejoin an oversubscribed cluster	10.0.0	10.0.0	Prioritizing critical control traffic increases resiliency in high availability and clustered deployments, especially when forming high availability or rejoining a cluster during times of heavy load. New/modified commands: **show asp priority-polling**, **show cluster info trace**, **show failover trace** Deployment restrictions: Not supported with container instances Platform restrictions: Supported with Secure Firewall 3100, 4200, and 6100 only

Public and private cloud

Table 31: Public and private cloud features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firewall Threat Defense Virtual for Microsoft Hyper-V	10.0.0	10.0.0	Firewall Threat Defense Virtual now supports Microsoft Hyper-V.
Firewall Threat Defense Container for Docker and Kubernetes	10.0.0	10.0.0	Firewall Threat Defense Container (FTDc) is a containerized firewall that you can deploy using Docker or as a pod in Kubernetes, including Amazon Elastic Kubernetes Service (Amazon EKS). In Kubernetes deployments, CNI plugins attach the Firewall Threat Defense pod to separate management and data networks. See: Cisco Secure Firewall Threat Defense Container Getting Started Guide
Nutanix AOS 6.8 support	10.0.0	10.0.0	Firewall Management Center Virtual and Firewall Threat Defense Virtual for Nutanix now support Nutanix AOS 6.8. This includes Virtual Private Cloud (VPC) support, whose flexible and cloud-like network segmentation and isolation allows you to effectively design and scale secure multi-tenant architectures.
OpenStack Caracal support	10.0.0	10.0.0	Firewall Management Center Virtual and Firewall Threat Defense Virtual for OpenStack now support the Caracal release.
VMware vSphere/VMware ESXi 9.0 and 9.1 support	10.0.0	10.0.0	You can now deploy Secure Firewall Threat Defense Virtual and Firewall Management Center Virtual on VMware vSphere/VMware ESXi 9.0 and 9.1.
OCI Ampere Compute instances	10.0.0	10.0.0	Firewall Threat Defense Virtual for OCI now supports Flex instances powered by an Ampere ARM-based processor. ARM architecture provides high performance with lower power consumption, enabling cost-efficient scaling. Supported instances: VM.Standard.A1.Flex, VM.Standard.A2.Flex

Feature	Minimum Management Center	Minimum Threat Defense	Details
Azure MANA NIC support	10.0.0	10.0.0	Firewall Threat Defense Virtual for Microsoft Azure now supports MANA NIC hardware, which is optimized for enhanced networking performance. Supported instances: Standard_D8s_v5, Standard_D16s_v5
Unlimited performance tier (FTDvU) for VMware and KVM	10.0.0	10.0.0	Firewall Threat Defense Virtual for VMware and KVM now support an unlimited performance tier (FTDvU). This tier does not rate limit and the RA VPN session limit depends on the allocated resources: • 20,000 sessions with 32 vCPU and 64 GB RAM • 32,000 sessions with 64 vCPU and 128 GB RAM
AWS two-arm Multi-AZ cluster support	10.0.0	10.0.0	FTDv for AWS in two-arm-mode now supports Multi-AZ clustering. The GWLB in each AZ (availability zone) steers traffic to local firewalls for inspection and NAT. If one AZ or firewall fails, workloads in other AZs continue with minimal disruption, and you can scale throughput by adding members per AZ. Platform restrictions: Not supported with FTDv5 or FTDv10.
GCP autoscale with clustered devices	10.0.0	10.0.0	Firewall Threat Defense Virtual now supports GCP autoscale (dynamic scaling) with clustered devices, using a Terraform template.
Secure Boot and UEFI firmware support	10.0.0	10.0.0	**Upgrade impact. You cannot revert from Version 10+ to Version 7.7 or earlier.** Firewall Threat Defense Virtual is now compatible with UEFI-based virtual machines. This modern firmware interface replaces legacy BIOS, improves boot performance, and provides enhanced hardware/VM compatibility. Secure Boot ensures that only signed and trusted bootloaders, kernel modules, and drivers are executed when the VM starts. It improves the virtual appliances security. These changes mean that you cannot revert virtual firewalls from Version 10+ to Version 7.7 and earlier. After upgrade, we also recommend you migrate configurations to freshly deployed Version 10+ instances and decommission the old ones.
Larger default disk size and the ability to resize the disk post-deployment	10.0.0	10.0.0	Firewall Threat Defense Virtual supports dynamic disk expansion on all virtual platforms. This capability optimizes disk utilization on high-capacity systems (for example, systems with 64 vCPUs and 128 GB RAM), ensuring that large core dump files do not trigger disk-space alerts. The default disk size has also changed.

Routing

Table 32: Routing features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Use PBR to handle traffic based on custom application patterns.	10.0.0	10.0.0	You can now use policy based routing to handle traffic using custom application patterns (basic supported from Version 7.7.0). Create an advanced custom application detector by uploading a Lua file with your detection pattern. Then, use the detector in an extended ACL in your PBR policy. See: Policy Based Routing
IPv6 router advertisements assign RDNSS/DNSSL	10.0.0	10.0.0	You can now configure recursive DNS server (RDNSS) and DNS search list (DNSSL) options to provide DNS servers and domains to SLAAC clients using router advertisements. New/modified screens: **Devices** > **Device Management** > **Interfaces** > **Add/Edit Interfaces** > **IPv6** > **Settings** New/modified commands: **show ipv6 nd detail**, **show ipv6 nd ra dns-search-list**, **show ipv6 nd ra dns server**, **show ipv6 nd summary**

Threat detection and application identification

Table 33: Threat detection and application identification features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Encrypted visibility engine (EVE) improvements	10.0.0	10.0.0 (widgets) Any (all others)	**Upgrade impact. Upgrade merges exceptions, changes the blocking level, and begins using EVE for application detection.** Encrypted visibility engine (EVE) improvements include: • Configuration moved from the access control policy advanced settings to the main access control policy page (in the **More** drop-down list). • New monitor and protect modes. The monitor mode allows you to see verdicts without blocking. • Five-level threat confidence scale now only two levels: high and very high. Firewall Management Center upgrade changes very low, low, and medium blocking thresholds to high, in policies that block based on EVE threat confidence. • EVE is now automatically used for application detection when you enable EVE. Firewall Management Center upgrade enables EVE-based application detection in access control policies where EVE is enabled. • EVE exceptions are now objects, and are automatically shared across all access control policies. Firewall Management Center upgrade moves existing exceptions to object management. Access control policies that use EVE now use the merged set of exceptions. • Security-related connection events now include those for connections with malware processes detected by EVE at higher threat confidence levels. • New EVE widgets on the Summary Dashboard provide information on targeted resources, as well as on connections blocked over time. Note that new dashboard widgets only show data for Version 10+ devices.
Default ports in application-based access control rules	10.0.0	Any with Snort 3	For access control rules, a new **Application Default** option on the **Applications** tab lets you limit the rule to the application's default ports. You can also specify that the application be identified on **Any** port, which is the system's previous behavior. Note that any specification on the **Ports** tab overrides these options. You can use the **Ports** tab to limit the rule to one, multiple, or a range of ports. After Firewall Management Center upgrade, existing application-based rules that do not have manual port conditions are applied to **Any** port. To take advantage of this feature, edit the rules you want to limit.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Dynamic objects and security group tags in DNS rules	10.0.0	10.0.0	You can configure DNS rules in the DNS policy to use dynamic objects or security group tags (SGT). If you are using these types of objects in access control rules already, you can now extend their use to your DNS policy. We added the **Dynamic Attributes** tab to the add/edit DNS rule dialog box.
HTTP command line injection attack detection with Snort ML	10.0.0	10.0.0	Snort ML now detects HTTP command line injection attacks. The snort_ml inspector is currently disabled in all default policies except maximum detection. The intrusion rule that generates an event when the snort_ml detects an attack (GID:411 SID:1) is also currently disabled in all default policies except maximum detection.
Portscan detection for clusters	10.0.0	10.0.0	You can configure threat detection at the cluster level. For nodes in a cluster, detection and prevention happen at the cluster level. Portscans can be detected when they happen across nodes or in an individual node. Shunned hosts are shunned on all devices in the cluster. Shuns are released at the same time on all nodes. Statistics are available at the cluster level.
Unauthorized privacy technology (shadow traffic) detection	10.0.0	10.0.0	A new Shadow Traffic dashboard (**Insights & Reports** > **Dashboard** > **Shadow Traffic**) monitors unauthorized privacy technology such as encrypted DNS, evasive private VPNs, multi-hop proxies, domain fronting, and fake TLS. Also, connection and unified events now have a Shadow Traffic Type field. Shadow traffic monitoring is auto-enabled by the upgrade. To disable it, use the access control policy advanced settings.

Troubleshooting and serviceability

Table 34: Troubleshooting and serviceability features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
MTU ping test on cluster node join provides more information by trying smaller MTUs	10.0.0	Any	When a node joins the cluster, it checks MTU compatibility by sending a ping to the control node with a packet size matching the cluster control link MTU. If the ping fails, it tries the MTU divided by 2 and keeps dividing by 2 until an MTU ping is successful. A notification is generated so you can fix the MTU to a working value and try again. We recommend increasing the switch MTU size to the recommended value, but if you can't change the switch configuration, a working value for the cluster control link will let you form the cluster. New/modified commands: **show cluster history**
Use the packet tracer to modify PCAPs	10.0.0	Any	You can now use the packet tracer to modify the source and destination IP address, source and destination port, and VLAN ID of a PCAP. In transparent mode, you can also modify the destination MAC address. You can then run a trace with the modified PCAP.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Generate a kernel dump on demand, or automatically on crash	10.0.0	10.0.0	You can now use the CLI to configure most hardware devices to generate a Linux kernel dump on crash. After you enable this feature, the device must reboot for it to take effect. Using the **force** keyword reboots the device and generates a kernel dump immediately. Or, manually reboot the device later. The upgrade automatically enables this feature. New CLI command: **system support kernel-crash-dump** Platform restrictions: Supported on all hardware devices except the Secure Firewall 200 and ISA 3000.
Recovery-config mode support for NAT and other interface commands	10.0.0	10.0.0	Recovery-config mode now supports NAT and related object and object-group commands. It also supports the following interface commands: • **duplex** • **fec** • **negotiate-auto** • **speed** These interface commands, in addition to shutdown, are not supported in recovery-config mode on the cluster control link or failover link. New/modified diagnostic CLI (**system support diagnostic-cli**) command: **configure recovery-config** Platform restrictions: Not supported with the Firepower 4100/9300, ISA 3000, or virtual firewall. Not supported for the Secure Firewall 3100/4200 in multi-instance mode.
Minimal system logging	10.0.0	10.0.0	You can now configure minimal (notice and above) system logging. For most devices, the default is full logging. For the new Secure Firewall 220, the default is minimal logging. New/modified CLI commands: **system support logging-show**, **system support logging-full**, **system support logging-minimal**

Upgrade

Table 35: Upgrade features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
New device and chassis upgrade wizard	10.0.0	Any	A new, streamlined upgrade wizard makes it easier to select and prepare devices for upgrade, and to identify issues preventing upgrade. Note that the Firewall Threat Defense wizard takes advantage of a new prepare-only option for unattended mode. This means that while the wizard copies packages and checks readiness, you may see messages about unattended mode running even if you did not explicitly start it.
Prepare-only and skip-checks options for unattended Firewall Threat Defense upgrade	10.0.0	Any	With unattended Firewall Threat Defense upgrades: • Prepare for upgrade only—copy packages and check readiness, but do not perform the actual upgrade. • Skip readiness checks for devices that already passed. These new options are available when you start unattended mode.
New options for downloading upgrade packages	10.0.0	Any	You can now: • Prevent devices from downloading upgrade packages from the internet. That is, you can now require that devices get upgrade packages from the Firewall Management Center or an internal server, even if the devices have internet access. • Specify how long the system retries failed downloads from an internal server (devices only) or the internet. This setting does not apply to transfers between the Firewall Management Center and device. New/modified screens: **Administration** > **Product Upgrades** > **Global upgrade settings**
Auto-replace outdated Firewall Management Center upgrade scripts.	10.0.0	Any	The Firewall Management Center can get new upgrade scripts for itself from the internet, fixing late-breaking upgrade issues without replacing the whole upgrade package. If the Firewall Management Center cannot download new scripts for any reason, the upgrade proceeds as it would have without them. If you encounter issues with Firewall Management Center upgrade, including a failed upgrade or unresponsive system, contact Cisco TAC. Download location: cdo-ftd-images.s3-us-west-2.amazonaws.com

Usability

Table 36: Usability features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Redesigned menus for the Firewall Management Center	10.0.0	Any	We redesigned the Firewall Management Center menus to be more intuitive and consistent with the Security Cloud Control user interface. A main, single-column menu provides a subset of your most used items, while all items are visible in expanded mode. You can customize which items to include on the main menu to suit your priorities. Preferences are per user. Existing and renamed top-level menus include: • **Overview** is now **Insights & Reports** • **Analysis** is now **Events & Logs** • **Policies**, **Devices**, and **Objects** are the same • **Integration** is now **Integrations** • **System** is now **Administration** and appears in the left navigation New top-level menus include: • **Secure Connections** • **Troubleshooting** Some submenus were moved to new main menu locations.

VPN

Table 37: Remote access VPN features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
ACME-based TLS certificate management for remote access VPN	10.0.0	10.0.0	You can now use an ACME certificate to authenticate a managed device as an RA VPN gateway. New/modified screens: **Objects > PKI > Cert Enrollment > Add Cert Enrollment > Enrollment Type > ACME** New/modified commands: **crypto ca trustpoint**

Table 38: Site-to-site VPN features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Site-to-site VPN tunnels over IPsec VTIs preserve SGT metadata	10.0.0	10.0.0	Cisco TrustSec uses security group tags (SGTs) to control access and enforce traffic on a network. This option enables SGT propagation over SVTIs and DVTIs of route-based and SD-WAN VPN topologies. To enable SGT propagation on a specific SVTI or DVTI, configure it in individual devices. New/modified screens: • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **SD-WAN Topology** > **Advanced Settings** • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **Route-based VPN** > **Advanced** > **Tunnel**
Site-to-site VPN hub support for ECMP load balancing with dynamic VTIs	10.0.0	10.0.0	You can now enable Equal Cost Multi-Path (ECMP) on the dynamic VTIs of hub devices. All virtual access interfaces on the hub connecting to the same spoke are grouped into an ECMP zone. New/modified screens: • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **SD-WAN Topology** > **Add Hub** • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **Route-based VPN** > **Hub**
Site-to-site VPN support for BFD-based failover	10.0.0	10.0.0	You can now enable the BFD routing protocol on the SVTIs and DVTIs of route-based and SD-WAN VPN topologies. New/modified screens: • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **SD-WAN Topology** > **Advanced Settings** • **Secure Connections** > **Site-to-Site VPN & SD-WAN** > **Route-based VPN** > **Advanced** > **Tunnel**
Distributed site-to-site VPN with clustering for the Secure Firewall 4200	10.0.0	10.0.0	A cluster on the Secure Firewall 4200 supports site-to-site VPN in distributed mode. Distributed mode provides the ability to have many site-to-site IPsec IKEv2 VPN connections distributed across members of a cluster, not just on the control node (as in centralized mode). This significantly scales VPN support beyond centralized VPN capabilities and provides high availability. Added/modified commands: **cluster redistribute vpn-sessiondb**, **show cluster vpn-sessiondb**, **cluster vpn-mode**, **show cluster resource usage**, **show vpn-sessiondb**, **show conn detail**, **show crypto ikev2 stats**

Zero trust access

Table 39: Zero trust access features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
ACME trustpoint as identity certificate for zero trust access	10.0.0	10.0.0	You can choose an ACME certificate for authenticating a managed device as a SAML SP for a zero-trust application policy. ACME certificates automate the lifecycle management of SSL and TLS certificates, including their auto-renewal. New/modified screens: **Objects** > **PKI** > **Cert Enrollment** > **ACME** New/modified commands: **crypto ca trustpoint**
IPv6 support for zero trust access	10.0.0	10.0.0	Clientless ZTNA now provides secure access to applications connected over IPv6 networks. Limitations: IPv6 source NAT for applications is only for homogeneous scenarios such as NAT66 and NAT44. NAT64 and NAT46 are not supported. New/modified screens: **Policies** > **Zero Trust Application** > **Clientless Policy** > **Add Application** New/modified CLIs: **show running-config zero-trust**

Deprecated features

Table 40: Deprecated features in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: Legacy screens used to register a device with a registration key	10.0.0	Any	The legacy screens used to register a device with a registration key are deprecated. On the Device Management page, **Add** > **Device** now launches the wizard and **Add** > **Device (Wizard)** was removed.
Deprecated: Enable a DHCP server on the firewall management interface	10.0.0	10.0.0	We deprecated these firewall CLI commands: • **configure network ipv4 dhcp-server-enable** • **configure network ipv4 dhcp-server-disable** • **show network-dhcp-server** See: *Cisco Secure Firewall Threat Defense Command Reference*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: Secure Network Analytics manager-only deployments	10.0.0	Any	You can no longer configure a Secure Network Analytics manager-only deployment to store events. Note that manager-only deployments are deprecated in Secure Network Analytics Version 7.5.1. Although existing manager-only integrations continue to work, we recommend you switch to a single-node data store deployment with the latest supported version of Secure Network Analytics. This allows you to take advantage of new features, resolved issues, and performance improvements.
Deprecated: database access	10.0.0	Any	External access to the Firewall Management Center database is no longer supported. After upgrade, all integrations stop working. The option to enable database access is removed. The External Database User role and users remain, but cannot be used except to access the online help. We recommend you remove this role from existing users and do not enable it for new users.
End of support: VMware vSphere/VMware ESXi 6.5, 6.7, and 7.0	10.0.0	10.0.0	**. Upgrade VMware before you upgrade the software.** We discontinued support for virtual deployments on VMware vSphere/VMware ESXi 6.5, 6.7, and 7.0. Upgrade your hosting environment to Version 8.0 before you upgrade any virtual appliance. Version restrictions: Versions 7.3.x and 7.4.0–7.4.1 are not qualified on VMware 8.0. If you run any of these versions, upgrade to VMware 8.0 first. Move to the next step as soon as possible. For best results, perform a multi-step upgrade: first the virtual appliance to 7.4.2–7.7.x, then VMware, then the virtual appliances again.
Deprecated: Monitor device revert in the Message Center	10.0.0	Any	You can no longer monitor device revert from the Message Center. Instead, use the Device Management page (**Devices** > **Device Management**). On the **Upgrade** tab, click **View Details** next to the device you are reverting.
Deprecated: Legacy theme	10.0.0	Any	We deprecated the Legacy theme. If you were using the Legacy theme, the upgrade switches you to the Light theme.
Deprecated: Selected walkthroughs	10.0.0	Any	Some walkthroughs are no longer available. For a list of supported walkthroughs by version, see Walkthroughs in Secure Firewall Management Center.

Branding

Table 41: Branding in Version 10.0.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cisco Security Cloud is now Cisco Security Cloud Control	10.0.0	Any	Cisco Security Cloud is now Cisco Security Cloud Control. Integration allows you to leverage cloud-delivered intelligence, unified visibility, and simplified management.

Firewall Management Center Features in Version 7.7.13

There are no new features in this release.

Firewall Management Center Features in Version 7.7.12

There are no new features in this release.

Firewall Management Center Features in Version 7.7.11

There are no new features in this release.

Firewall Management Center Features in Version 7.7.10

Table 42: Firewall Management Center Features in Version 7.7.10

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.7.10 also has: • Umbrella integration with Firewall Management Center over a proxy. (7.4.3) • Migrate select Firepower 4100/9300 models to Secure Firewall 3100/4200. (7.6.1)
Zero Trust Access			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Universal Zero Trust Network Access (universal ZTNA).	7.7.10 10.0.0	7.7.10 10.0.0	Universal Zero Trust Network Access (universal ZTNA) is a comprehensive solution that provides secure access to internal network resources based on user identity, trust, and posture. It ensures that access to one application does not implicitly grant access to the entire network, as with remote access VPN. New/modified screens: **Policies** > **Security policies** > **Zero Trust Application** Requires Cisco Secure Access and Security Cloud Control. **Note** Due to framework changes, upgrading a universal ZTNA device to Version 10.1+ from older versions disables the feature. Traffic is interrupted until you deploy from the Firewall Management Center. Deployment restrictions: Not supported with clustered devices, container instances, or transparent mode. Supported platforms: Secure Firewall 1150, 3100, 4100, 4200, and Firewall Threat Defense Virtual. See: Zero Trust Access

Firewall Management Center Features in Version 7.7.0

Table 43: Firewall Management Center Features in Version 7.7.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.7.0 also has: • New Cisco AMP cloud connection method. Upgrade impact. (7.0.7) • Deprecated Cisco AMP Cloud connection backups. (7.0.7) • Require the Message-Authenticator attribute in all RADIUS responses. Upgrade impact. (7.0.7) • High-bandwidth encrypted application traffic bypasses unnecessary intrusion inspection. (7.2.10) • DC power supply for the Secure Firewall 4200 (7.4.3) • Independently configure health monitoring for physical and subinterfaces. (7.4.3) • View health status for devices in leaf domains while logged into the parent domain. (7.4.3) • Faster failover for high availability Firewall Threat Defense. (7.4.3) • Device backup storage is easier to configure. (7.4.5) Add device by registration key using basic initial configuration added to the Device (Wizard) (7.6.1) • BGP AS-Override. (7.6.1) • Devices with internet access download upgrade packages from the internet. (7.6.1)
Platform			
Secure Firewall 1230, 1240, and 1250 (rack-mount).	7.7.0	7.7.0	We introduced the Secure Firewall CSF-1230 and CSF-1240: • 8x1Gbps RJ-45 1000BASET/2.5BBASE-T copper • 4x1Gbps SFP+ optical And the Secure Firewall CSF-1250: • 8x2.5Gbps1000BASET/2.5BBASE-T copper • 4x2.5Gbps SFP28 optical See: *Cisco Secure Firewall 1230, 1240, and 1250 Hardware Installation Guide*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Optical transceivers for the Secure Firewall 4200.	7.7.0	7.7.0	The Secure Firewall 4200 now supports these optical transceivers on the FPR4K-X-NM-2X200/400G network module: QDD-400G-DR4-S, QDD-4x100G-FR-S, QDD-4x100G-LR-S, QDD-400G-SR4.2-BD, QDD-400G-FR4-S, QDD-400G-LR4-S, QDD-400-CUxM, QDD-400-AOCxM, QDD-2X100-LR4-S, QDD-2X100-SR4-S, QDD-4ZQ100-CUxM. See: *Cisco Secure Firewall 4200 Series Hardware Installation Guide*
Secure Firewall 1210CP IEEE 802.3bt support (PoE++ and Hi-PoE).	7.7.0	7.7.0	We made the following improvements related to support for IEEE 802.3bt: • PoE++ and Hi-PoE—Up to 90W per port. • Single- and dual-signature powered devices (PDs). • Power budgeting is done on a first-come, first-served basis. • Power budget fields were added to **show power inline**. New/modified screens: **Devices** > **Device ManagementInterfaces** > **PoE** New/modified commands: **show power inline** See: Regular Firewall Interfaces, *Cisco Secure Firewall Threat Defense Command Reference*
Instances for AWS, Azure, and GCP.	7.7.0	7.7.0	We added instances for Firewall Management Center Virtual and Firewall Threat Defense Virtual from the following families: • AWS (Amazon Web Services): C6i and C6a • Azure (Microsoft Azure): Dv4 and Dv5 • GCP (Google Cloud Platform): E2, N1, N2D, C2D See: *Cisco Secure Firewall Management Center Virtual Getting Started Guide*, Secure Firewall Threat Defense Virtual getting started guides
Unattended provisioning for Firewall Threat Defense Virtual for VMware using ISO-based cloud-init seeding.	7.7.0	7.7.0	You can now quickly deploy Firewall Threat Defense Virtual for VMware using a text file (day0.iso) that contains initial setup details such as hostname, password, management mode, firewall mode, network settings, and deployment type. See: Secure Firewall Threat Defense Virtual getting started guides
Platform Migration			
Migrate from Firepower Management Center 4600 to Secure Firewall Management Center Virtual 300 for VMware.	7.7.0	Any	You can migrate from Firepower Management Center 4600 to Secure Firewall Management Center Virtual for VMware with a 300-device license. See: *Cisco Secure Firewall Management Center Model Migration Guide*
Device Management			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Recovery-config mode for emergency on-device configuration and out-of-band configuration detection on the Firewall Management Center.	7.7.0	7.7.0	If you lose the management connection to your device, you can make select configuration changes directly at the device CLI to: • Restore the management connection if you are using a data interface for manager access. • Make select policy changes that can't wait until the connection is restored. After the management connection is restored, the Firewall Management Center will detect the configuration changes on the device. It does not automatically update the device configuration in the Firewall Management Center; you must view the configuration differences, acknowledge that the device configuration is different, and then manually make the same changes in the Firewall Management Center before you deploy. New/modified screens: **Devices** > **Device ManagementDevice** > **Health** > **Out of Band Status** New/modified diagnostic CLI (**system support diagnostic-cli**) command: **configure recovery-config** See: Device Settings, *Cisco Secure Firewall Threat Defense Command Reference*
Interfaces			
Sync Device is now **Sync Interfaces**.	7.7.0	7.7.0	**Sync Device** was changed to **Sync Interfaces** to indicate that this function is only for interface changes. This function no longer detects changes made to the manager access interface; see **Devices** > **Device ManagementDevice** > **Management** > **Manager Access Details: Configuration**. Other out-of-band configuration changes performed at the diagnostic CLI in recovery-config mode need to be discovered at **Devices** > **Device Management>Device** > **Health** > **Out of Band Status**. New/modified screens: **Devices** > **Device Management>Interfaces** See: Interfaces
High Availability/Scalability			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Management center high availability enhancements.	7.7.0	Any	It is now easier to: • Determine when the peers last synced. • Compare intrusion rule (SRU/LSP) and vulnerability database (VDB) versions on the peers. • Resolve a common device registration issue. When device registration fails on the standby peer when you establish high availability, it is often due to stale manager data on the device. Previously, you used the device CLI to resolve this issue. You can now use the Firewall Management Center web interface—click **Disable Manager**, then **Add Manager**. New/modified screens: **Administration** > **High Availability** See: High Availability
Threat defense high availability supported with redundant manager access data interfaces.	7.7.0	7.7.0	You can now use redundant manager access data interfaces with Firewall Threat Defense high availability. See: High Availability
Autoscale for Firewall Threat Defense Virtual for Azure clusters.	7.7.0	7.7.0	We now support autoscale for new Firewall Threat Defense Virtual for Azure clusters. You cannot convert upgraded deployments. Platform restrictions: Not supported with FTDv5 or FTDv10. See: Secure Firewall Threat Defense Virtual getting started guides
VPN: Remote Access			
Geolocation-based RA VPN.	7.7.0	7.7.0	You can now allow or block remote access VPN connections based on country or region. Connections that don't meet your location-based criteria are blocked before authentication and logged for auditing purposes. New/modified screens: **Objects** > **Access List** > **Service Access** See: Remote Access VPN
Easily configure posture assessment criteria for dynamic access policies.	7.7.0	Any	In dynamic access policies (DAP), you can now easily configure *posture assessment criteria*—that is, file, process, or registry endpoint attributes with unique endpoint IDs that you can then use to configure DAP records. New/modified screens: • **Devices** > **Dynamic Access Policy** > **Add/Edit Policy** > **Posture Assessment Criteria** • **Devices** > **Dynamic Access Policy** > **Add/Edit Policy** > **Add/Edit DAP Record** > **Advanced** > **Endpoint Criteria** See: Dynamic Access Policies

Feature	Minimum Management Center	Minimum Threat Defense	Details
Routing			
Use PBR to handle traffic based on user-defined domains.	7.7.0	7.7.0	You can now use policy based routing to handle traffic based on user-defined domains. Create a basic custom application detector (advanced supported in Version 10.0.0) with your domain patterns and the NSG (network service group) tag, then use it in an extended ACL in your PBR policy. See: Policy Based Routing
Access Control: Threat Detection and Application Identification			
Easily block traffic based on TLS version and server certificate status.	7.7.0	7.7.0	New options in the decryption policy wizard make it easier to block traffic based on TLS version and server certificate status. Enabling these options adds predefined rules that do this. After the policy is created, you can edit, reorder, or delete the rules. New/modified screens: **Policies** > **Decryption** > **Create Decryption Policy** > **Blocking** See: Decryption Policies, Decryption Rules
Bypass decryption for low-risk connections to trusted URLs with the encrypted visibility engine (EVE).	7.7.0	7.7.0	A new Client Threat decryption rule condition and a new option in the decryption policy wizard and make it easier to bypass decryption to trusted URLs for low risk (as identified by EVE) connections. New decryption policies now include predefined rules that do this, using Category (trusted) and Client Threat (low) conditions. The Client Threat condition is new and represents the EVE verdict. For outbound decryption, you enable/disable these rules as part of creating the policy. For inbound decryption, the rules are disabled by default. After the policy is created, you can edit, reorder, or delete the rules. New/modified screens: **Policies** > **Decryption** > **Create Decryption Policy** > **Decryption Exclusions** Version restrictions: You cannot deploy policies with Client Threat rules to older devices. See: Decryption Policies, Decryption Rules

Feature	Minimum Management Center	Minimum Threat Defense	Details
New encrypted visibility engine (EVE) exceptions.	7.7.0	7.7.0	You can now bypass EVE block verdicts based on source network and on destination dynamic attributes. And, when bypassing based on network, you can now use FQDN network objects. Previously, you could only block based on destination network or EVE process name and could not use FQDNs. New/modified screens: • To add an exception from the access control policy, in the advanced settings, edit and enable **Encrypted Visibility Engine**, enable **Block Traffic Based on EVE Score**, and **Add Exception Rule**. • To add an exception from the Unified Events viewer, right-click a connection that was blocked by EVE and select **Add EVE Exception**. See: *Custom Snort 3 Intrusion Policies for Access Control*
Encrypted visibility engine (EVE) dashboard enhancements.	7.7.0	7.7.0	The Summary dashboard (the default home page for the Firewall Management Center) now includes EVE information in its own tab, including widgets for discovered processes, threat confidence, malicious processes, and connections with detected process names. The widgets for malicious processes and connections with detected process names are new, and show data from Version 7.7+ devices only. The widgets for discovered processes and threat confidence were previously on the Application Statistics dashboard, and show data from all managed devices. Note that if you did modify the EVE tab on the Application Statistics dashboard, the upgrade retains your changes but does not add the new widgets. If you did not modify the tab, it is removed. See: Dashboards
Event Logging and Analysis			
SNI information from the ClientHello message in connection events.	7.7.0	7.7.0	Connection events now include the TLS Client SNI field, which shows the SNI (server name indication) information from the ClientHello message. This indicates the hostname a client is trying to connect to. See: Connection and Security-Related Connection Events
'Pending Rule Match' reason in connection events.	7.7.0	Any	A new connection event reason, Pending Rule Match, marks a connection that ended before it matched any access control role. See: Connection and Security-Related Connection Events
Health Monitoring			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Get alerts before service authentication certificates expire.	7.7.0	7.7.0	To help prevent unexpected service disruptions, a new Certificate Monitoring health module alerts you before service authentication certificates expire on the Firewall Management Center and managed devices. New/modified screens: **System** (⚙) > **Health** > **Policy** > **Health Modules** > **Certificate Monitoring** See: Health
Monitor the event database.	7.7.0	Any	The Firewall Management Center uses a MonetDB database for firewall events and event-related data like connection summaries. A new MonetDB Statistics health module collects database statistics that you can also see in the health monitor: database size, active connections, memory use, data requests processed, slow-running requests, and so on. This module is enabled for new and upgraded Firewall Management Centers. Troubleshooting best practice is to leave it enabled. New/modified screens: **System** (⚙) > **Health** > **Policy** > **Health Modules** > **MonetDB Statistics** See: Health
Upgrade			
Upgrade Firewall Threat Defense or chassis without a manual readiness check.	7.7.0	7.7.0	You no longer have to run time-consuming pre-upgrade readiness checks for Firewall Threat Defense or chassis upgrades. Instead, these checks are now regularly run by the system and reported in the health monitor. This allows you to preemptively fix any issues that will block upgrade. • The Database module, new for devices, manages monitors database schema and configuration data (*EO*) integrity. • The FXOS Health module, new for devices, monitors the FXOS httpd service on FXOS-based devices. • The Disk Status module is now more robust, alerting on disk health issues reported by daily running of smartctl (a Linux utility for monitoring reliability, predicting failures, and performing other self-tests). Version restrictions: This feature is supported for upgrades *from* Version 7.7+. Devices running earlier versions still require the in-upgrade readiness check. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center

Feature	Minimum Management Center	Minimum Threat Defense	Details
Upgrade Firewall Management Center without a manual readiness check.	7.7.0	Any	You no longer have to run time-consuming pre-upgrade readiness checks for Firewall Management Center upgrades. Instead, these checks are now regularly run by the system and reported in the health monitor. This allows you to preemptively fix any issues that will block upgrade. Version restrictions: This feature is supported for upgrades *from* Version 7.7+. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
Skip post-upgrade deploy for Firewall Management Center.	7.7.0	Any	In many cases, you no longer have to deploy to Snort 3 devices after you upgrade the Firewall Management Center. If deploy is required, affected devices are marked out of date (with a few exceptions). Reasons for needing to manually deploy include: • The upgrade updated the LSP and scheduled LSP updates are off. • The upgrade updated the LSP and scheduled LSP updates are on, but automatic redeploy is off. Devices may not be marked out of date in this case. Note that if automatic redeploy is on, the redeploy will take place on schedule and you do not need to do it manually. • Specific configurations changed by the upgrade require a deploy. • You need to upgrade managed devices immediately. After Firewall Management Center upgrade, you cannot upgrade managed devices until you redeploy, even if they are not marked out of date. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
SRU update moved out of Firewall Management Center upgrade.	7.7.0	Any	**Upgrade impact. After Firewall Management Center upgrades to Version 7.7+, wait for SRU to install.** Instead of upgrading the SRU as part of the upgrade, the system now updates intrusion rules for Snort 2 devices (the *SRU*) after the upgrade completes and the Firewall Management Center reboots. Although this makes the upgrade itself faster, you cannot update intrusion rules, add devices, or deploy configuration changes while the SRU is updating. This occurs regardless of whether you are managing any Snort 2 devices. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
Administration			
Cancel Firewall Threat Defense backups, view detailed backup status.	7.7.0	7.7.0	The Message Center now displays detailed backup status for the Firewall Management Center and its devices. You can also cancel in-progress device backups. See: Backup/Restore

Feature	Minimum Management Center	Minimum Threat Defense	Details
Restrict Firewall Management Center SAML SSO logins to a subdomain.	7.7.0	Any	In a multidomain deployment, you can now restrict Firewall Management Center SAML SSO logins to a subdomain. This can only be configured at the global domain level. See: Users
Clear disk space utility.	7.7.0	7.7.0	A new utility allows you to click to safely remove unneeded files such as old backups, content updates, and troubleshooting files. Low disk space can reduce performance, prevent upgrade, and increase the risk of accidentally deleting important files when trying to recover space. New/modified screens: We added a **Clear disk space** button to the Disk Usage widget on health dashboards: **System** (⚙) > **Health** > **Monitor**. See: Troubleshooting
New dark theme and theme name changes.	7.7.0	Any	There are now three themes available for the Firewall Management Center: • *Light* is a renamed New theme—the left-hand navigation theme introduced recently. • *Dark* is a new left-hand navigation theme that replaces the Dusk theme. If you were using the Dusk theme, you are switched to the Dark theme. • *Legacy* is a renamed Light theme. To change themes, click your username in the top right corner of the Firewall Management Center web interface. See: Users
Performance and Resiliency			
Dynamic flow offload for the Secure Firewall 3100/4200.	7.7.0	7.7.0	Dynamic flow offload is now supported on the Secure Firewall 3100/4200. Previously, it was only supported on the Firepower 4100/9300. This feature is enabled in new and upgraded deployments. Platform restrictions: Not supported with container instances. See: Prefiltering
Use a loopback interface on Firewall Threat Defense Virtual for GCP to receive health probes from the GCP load balancer.	7.7.0	7.7.0	You can now use a dedicated loopback interface on Firewall Threat Defense Virtual for GCP to receive health probes from the GCP load balancer in autoscale deployments. This allows the system to handle health probes more efficiently, improving performance. See: Secure Firewall Threat Defense Virtual getting started guides

Feature	Minimum Management Center	Minimum Threat Defense	Details
Configure Firewall Threat Defense autorecovery from block depletion using FlexConfig.	7.7.0	7.7.0	To reduce downtime due to service disruption, a new fault manager monitors block depletion and automatically reloads devices when necessary. In high availability deployments, this triggers failover. Fault monitoring is automatically enabled on new and upgraded devices. To disable, use FlexConfig. New/modified FlexConfig commands: • **fault-monitor block-depletion recovery-action** {**none** | **reload**} Specifying **none** turns off automatic reload, but does not turn off fault monitoring. For that, use **no fault-monitoring**. • **fault-monitor block-depletion monitor-interval** *seconds* You can configure how long (in seconds) before the device reloads. New/modified Firewall Threat Defense CLI commands: **show fault-monitor block-depletion** {**status** | **statistics**} Platform restrictions: Not supported for clustered devices. See: Troubleshooting
Troubleshooting			
CPU profiler includes application identification statistics.	7.7.0	7.7.0	The CPU profiler now includes application identification statistics. That is, you can now see the resources used by processing specific application traffic. After you enable CPU profiling, use the CLI to see results. New/modified CLI commands: **system support appid-cpu-profiling status**, **system support appid-cpu-profiling dump** See: Troubleshooting, *Cisco Secure Firewall Threat Defense Command Reference*
Processing statistics in connection events.	7.7.0	7.7.0	To help with performance troubleshooting, connection events now contain two new fields: Inspection Duration (microseconds) and Inspected Packets. See: Connection and Security-Related Connection Events
New IP flow statistics.	7.7.0	7.7.0	When collecting IP flow statistics from Firewall Threat Defense under the direction of Cisco TAC, a new **all** parameter logs additional statistics to the specified file: port, protocol, application, cumulative latency, and inspection time. New/modified commands: **system support flow-ip-profiling start flow-ip-file** *filename* **all** {**enable** | **disable**} See: *Cisco Secure Firewall Threat Defense Command Reference*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cisco RADKit integration.	7.7.0	7.7.0	Cisco RADKit integration allows Cisco TAC engineers to remotely connect with your deployment (including sudo access) for an enhanced troubleshooting experience. You control the appliances and duration of access. This also gives you and Cisco TAC access to diagnostic data and logs. New/modified screens: **Troubleshooting** > **Tools** > **Remote Diagnostics**then click **Enable the RADKit service** See: Troubleshooting
Security and Hardening			
Limited user privileges for Threat Defense CLI Basic user.	7.7.0	7.7.0	The scope of the Threat Defense CLI Basic user privilege is now limited to the following commands: dig, ping, traceroute. If you have created users with the Basic privilege, evaluate whether you need to change them to the Config privilege. You can change a user's privilege level using the **configure user access** command. See: *Cisco Secure Firewall Threat Defense Command Reference*
Deprecated Features			
Deprecated: Snort 2.	7.7.0	7.7.0	**Upgrade impact. Cannot upgrade Snort 2 devices.** Snort 2 is deprecated. You cannot upgrade a Snort 2 device to Version 7.7.0+. Although you can use a Version 7.7.0+ Firewall Management Center to manage older Snort 2 devices, you should still switch to Snort 3 for improved detection and performance. Deprecated CLI commands: **show snort counters**, **show snort preprocessor-memory-usage**. See: *Custom Snort 3 Intrusion Policies for Access Control*
Deprecated: Access control policy legacy interface.	7.7.0	Any	You can no longer use the legacy user interface for access control policies. If you were using it, you switch to the improved user interface introduced in Version 7.2. New/modified screens: **Switch to Legacy UI** toggle is removed

Firewall Management Center Features in Version 7.6.6

There are no new features in this release.

Firewall Management Center Features in Version 7.6.5

There are no new features in this release.

Firewall Management Center Features in Version 7.6.4

Table 44: Firewall Management Center Features in Version 7.6.4

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.6.4 also has: • DC power supply for the Secure Firewall 4200 (7.4.3) • Faster failover for high availability Firewall Threat Defense. (7.4.3)
Public and Private Cloud			
High availability for Firewall Management Center Virtual for OpenStack.	7.6.4	Any	Firewall Management Center Virtual for OpenStack now supports high availability. Platform restrictions: Not supported with FMCv2

Firewall Management Center Features in Version 7.6.3

There are no new features in this release.

Note Version 7.6.3 was released to address specific vulnerabilities. It is available for Firewall Management Center as an upgrade or fresh install, and for Firewall Threat Defense Virtual in the public cloud as a fresh install only. For exisiting deployments, Version 7.6.2.1 provides the same fixes.

Firewall Management Center Features in Version 7.6.2

There are no new features in this release.

Firewall Management Center Features in Version 7.6.1

Table 45: Firewall Management Center Features in Version 7.6.1

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.6.1 also has: • New Cisco AMP cloud connection method. Upgrade impact. (7.0.7) • Deprecated Cisco AMP Cloud connection backups. (7.0.7) • Require the Message-Authenticator attribute in all RADIUS responses. Upgrade impact. (7.0.7) • High-bandwidth encrypted application traffic bypasses unnecessary intrusion inspection. (7.2.10) • Independently configure health monitoring for physical and subinterfaces. (7.4.3) • View health status for devices in leaf domains while logged into the parent domain. (7.4.3) • Umbrella integration with Firewall Management Center over a proxy. (7.4.3) • Device backup storage is easier to configure. (7.4.5)
Platform Migration			
Migrate select Firepower 4100/9300 models to Secure Firewall 3100/4200.	7.6.1 7.7.10 10.0.0	Any	You can now easily migrate configurations to the Secure Firewall 3100/4200 from these devices: • Firepower 4110, 4120, 4140, 4150 • Firepower 9300: SM-24, SM-36, SM-44
Device Management			
Add device by registration key using basic initial configuration added to the Device (Wizard)	7.6.1 7.7.0	An y	You can now use the Device (Wizard) to add a device using a registration key with a basic initial configuration. This functionality is still present on the **Add** > **Device** screen as well. New/modified screens: **Devices** > **Device Management** > **Add** > **Device (Wizard)** See: Device Management
Routing			

Feature	Minimum Management Center	Minimum Threat Defense	Details
BGP AS-Override.	7.6.1 7.7.0	7.6.1 7.7.0	Firewall Threat Defense can now overwrite an ASN received from a peer with its own BGP ASN. This allows other routers peering with Firewall Threat Defense to accept advertised prefixes without detecting a loop based on the contents of the AS_PATH attribute. New/modified screens: **Devices** > **Device Management** > **Add/Edit Device** > **Routing** > **BGP IPv4 or IPv6** > **Add/Edit Neighbor** > **AS Override** See: BGP
Upgrade			
Devices with internet access download upgrade packages from the internet.	7.6.1 7.7.0	Any (some restrictions)	You can now begin device and chassis upgrades without the upgrade package. At the appropriate time, devices will get the package directly from the internet. This saves time and Firewall Management Center disk space. Devices without internet access can continue to get the package from the Firewall Management Center or an internal server. Note that devices try the internal server (if configured) before either the internet or the Firewall Management Center. If the internal server download fails, newer devices with internet access try the internet then the Firewall Management Center, while older devices and devices without internet access just try the Firewall Management Center. (In this context, "newer" means Firewall Threat Defense 7.6+ or chassis 7.4.1+.) Restrictions: Firewall Management Center and devices must be able to access the internet. There is no way to force a device with internet access to try the Firewall Management Center before it tries the internet. Not supported for hotfixes. Download location: https://cdo-ftd-images.s3-us-west-2.amazonaws.com/ See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center

Firewall Management Center Features in Version 7.6.0

Table 46: Firewall Management Center Features in Version 7.6.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.6.0 also has: • Security Cloud Control regions: India and Australia. (7.0.7) • VMware vSphere/VMware ESXi 8.0 support. (7.2.9) • Asymmetric traffic handling. Upgrade impact. (7.2.9) • Firewall Threat Defense and chassis upgrade wizards optimized for lower resolution screens. (7.2.10) • Firewall Management Center Virtual 300 for Azure. (7.4.2) • High availability for Firewall Management Center Virtual for Azure. (7.4.2) • IMDSv2 support for AWS deployments. (7.4.3)
Administration			
Allow Cisco Talos to conduct advanced threat hunting and intelligence gathering using your traffic.	7.6.0	7.6.0 with Snort 3	**Upgrade impact. Upgrade enables telemetry.** You can help Talos (Cisco's threat intelligence team) develop a more comprehensive understanding of the threat landscape by enabling threat hunting telemetry. With this feature, events from special intrusion rules are sent to Talos to help with threat analysis, intelligence gathering, and development of better protection strategies. This setting is enabled by default in new and upgraded deployments. New/modified screens: **System** (⚙) > **Configuration** > **Intrusion Policy Preferences** > **Talos Threat Hunting Telemetry** See: Intrusion Policy Preferences
Change management ticket takeover; more features in the approval workflow.	7.6.0	Any user	You can now take over another user's ticket. This is useful if a ticket is blocking other updates to a policy and the user is unavailable. These features are now included in the approval workflow: decryption policies, DNS policies, file and malware policies, network discovery, certificates and certificate groups, cipher suite lists, Distinguished Name objects, Sinkhole objects. See: Change Management
Cisco AI Assistant for Security.	7.6.0	Any	The Cisco AI Assistant for Security can answer questions about your devices and policies and query documentation and reference materials, streamlining your workflow and boosting overall efficiency. Requires Security Cloud Control. See: Use Cisco AI Assistant for Security to Manage Your Threat Defense Devices Effectively

Feature	Minimum Management Center	Minimum Threat Defense	Details
Security Cloud Control replaces SecureX.	7.6.0	Any	**Upgrade impact. Enable Security Cloud Control after upgrade. Remove the SecureX Firefox Extension.** Registering an on-prem Firewall Management Center to the Security Cloud Control gives you access to the latest services such as the Cisco AI Assistant for Security, Policy Analyzer & Optimizer, and Cisco XDR Automation (replaces SecureX orchestration). With a Security Cloud Control account, you also have a centralized view of your inventory, and can easily perform Zero-Touch Provisioning, establish consistent policies across Firewall Management Centers, send events to the cloud, and enrich your threat hunts and investigations. New/modified screens: **Integration** > **Cisco Security Cloud** Deprecated screens: • **Integration** > **SecureX** • SecureX ribbon. If you are using Mozilla Firefox, remove the Cisco SecureX Ribbon extension. See: Integrate Management Center with the Cisco Security Cloud
Security Services Exchange (SSE) integration required for some threat intelligence downloads.	7.6.0	Any	**Upgrade impact. Enable Security Cloud Control integration in non-airgapped SLR deployments.** Talos Cloud Services is now the source for intrusion rules, URL filtering data and lookups, and data for the new event enrichment feature. To maintain a secure cloud connection, Security Services Exchange (SSE) integration is required. If you are using regular Smart Licensing, registering with Smart Software Manager (CSSM) sets up SSE integration. But if you are using Specific License Reservation in a non-airgapped deployment, you must instead enable Security Cloud Control (**Integration** > **Cisco Security Cloud**). If you have concerns with data sharing, disable all sharing options including event storage, Cisco Success Network, and Cisco Support Diagnostics. But the Firewall Management Center still must be able to reach the regional cloud you choose: • US: api-sse.cisco.com • EU: api.eu.sse.itd.cisco.com • APJC: api.apj.sse.itd.cisco.com • Australia: api.au.sse.itd.cisco.com • India: api.in.sse.itd.cisco.com Note that in airgapped deployments, you update threat intelligence manually, with the exception of event enrichment, which is not supported.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cisco Success Network and Cisco Support Diagnostics are enabled by default.	7.6.0	Any	**Upgrade impact. Upgrade opts into Cisco Success Network and Cisco Support Diagnostics.** Cisco Success Network and Cisco Support Diagnostics are now opt-out, instead of opt-in. If you were previously opted out, upgrade changes that. Also, you can no longer opt out when you register the Firewall Management Center to the Cisco Smart Software Manager (CSSM). You can still opt out on **Integration** > **Cisco Security Cloud** > **Cisco Security Cloud Support**. See: Integrate Management Center with the Cisco Security Cloud
New theme for the Firewall Management Center.	7.6.0	Any	We introduced a new left-hand navigation theme for the Firewall Management Center. To try it, click your user name in the top right corner and select the **New** theme. We also deprecated the Classic theme. If you were using the Classic theme, the upgrade switches you to the Light theme. See: Change the Web Interface Appearance
Reporting usability improvements.	7.6.0	Any	When including a table in a report, it's now easier to add, delete, sort, and move columns. New/modified screens: • **Overview** > **Reporting** > **Report Templates** > **Create Report Template** > **Add Table View** > **Fields** > **Edit** • To create a report based on your current event view, you now click **Create Report** instead of **Reporting**. See: Modify Fields in the Report Template Table Format Sections
Subscribe to Cisco newsletters and other product-related communications.	7.6.0	Any	Provide an email address to receive sales and product renewal conversations, new release adoption newsletters, and other product-related communications from Cisco. Each Firewall Management Center internal user has their own email address. New/modified screens: **System** (⚙) > **Users** > **Edit** > **Email Address**. See: Add or Edit an Internal User

Feature	Minimum Management Center	Minimum Threat Defense	Details
Updated internet access requirements for intrusion rule updates.	7.6.0	Any	**Upgrade impact. The system connects to new resources.** The system now requires access to the following resources to download intrusion rules: • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com It no longer requires access to talosintelligence.com.
Updated internet access requirements for URL filtering.	7.6.0	Any	**Upgrade impact. The system connects to new resources.** The system now requires access to *.talos.cisco.com for URL filtering data. It no longer requires access to regsvc.sco.cisco.com. For a full list of resources required for this feature, see Internet Access Requirements.
Deployment and Policy Management			
Policy Analyzer & Optimizer for access control.	From mgmt. center: 7.6.0 From Security Cloud Control: 7.2.0	Any	The Policy Analyzer & Optimizer evaluates access control policies for anomalies such as redundant or shadowed rules, and can take action to fix discovered anomalies. You can launch the access control Policy Analyzer & Optimizer directly from a Version 7.6+ Firewall Management Center; this requires Security Cloud Control. For Versions 7.2–7.4 Firewall Management Centers, use Security Cloud Control. New/modified screens: • To enable: **Integration** > **Cisco Security Cloud** > **Enable Policy Analyzer & Optimizer** • To analyze policies: **Policies** > **Access Control**, select policies, click **Analyze Policies**. See: Identifying and Fixing Anomalies with Policy Analyzer & Optimizer
Device Management			

Feature	Minimum Management Center	Minimum Threat Defense	Details
AAA for user-defined VRF interfaces.	7.6.0	7.6.0	A device's authentication, authorization, and accounting (AAA) is now supported on user-defined Virtual Routing and Forwarding (VRF) interfaces. The default is to use the management interface. In device platform settings, you can now associate a security zone or interface group having the VRF interface, with a configured external authentication server. New/modified screens: **Devices** > **Platform Settings** > **External Authentication** See: Enable Virtual-Router-Aware Interface for External Authentication of Platform
Delete is now **Unregister** on the device management page.	7.6.0	Any	The **Delete** menu choice was renamed to **Unregister** to better indicate that the device, high-availability pair, or cluster is being unregistered from the Firewall Management Center and not deleted from the high availability pair or cluster or having its configuration erased. The device, high-availability pair, or cluster continues to pass traffic until it is re-registered. New/modified screens: **Devices** > **Device Management** > **More** See: Device Management
Device templates.	7.6.0	7.4.1	Device templates allow you to deploy multiple branch devices with pre-provisioned initial device configurations (zero-touch provisioning). You can also apply configuration changes to multiple devices with different interface configurations, and clone configuration parameters from existing devices. Restrictions: You can use device templates to configure a device as a spoke in a site-to-site VPN topology, but not as a hub. A device can be part of multiple hub-and-spoke site-to-site VPN topologies. New/modified screens: **Devices** > **Template Management** Supported platforms: Firepower 1000/2100, Secure Firewall 1200/3100. Note that Firepower 2100 support is for Firewall Threat Defense 7.4.1–7.4.x only; those devices cannot run Version 7.6.0. See: Device Management Using Templates

Feature	Minimum Management Center	Minimum Threat Defense	Details
Serial-number registration (zero-touch provisioning) supported from an on-prem Firewall Management Center.	7.6.0	Mgmt. center must be publicly reachable: 7.2.0 Restriction removed: 7.2.4/7.4.0	You can now register a device using its serial number from an on-prem Firewall Management Center. With templates (requires Firewall Threat Defense 7.4.1+ on the device), you can register multiple devices at once. This feature was previously known as low-touch provisioning. Requires Security Cloud Control. For upgraded Firewall Management Centers, your existing Security Cloud Control integration continues to work until you enable Security Cloud Control. New/modified screens: **Devices** > **Device Management** > **Add** > **Device (Wizard)** Supported platforms: Firepower 1000/2100, Secure Firewall 1200/3100. Note that Firepower 2100 support is for Firewall Threat Defense 7.4.1–7.4.x only; those devices cannot run Version 7.6.0. See: Device Management
Encrypted traffic handling			
Easily bypass decryption for sensitive and undecryptable traffic.	7.6.0	Any	It is now easier to bypass decryption for sensitive and undecryptable traffic, which protects users and improves performance. New decryption policies now include predefined rules that, if enabled, can automatically bypass decryption for sensitive URL categories (such as finance or medical), undecryptable distinguished names, and undecryptable applications. Distinguished names and applications are undecryptable typically because they use TLS/SSL certificate pinning, which is itself not decryptable. For outbound decryption, you enable/disable these rules as part of creating the policy. For inbound decryption, the rules are disabled by default. After the policy is created, you can edit, reorder, or delete the rules entirely. New/modified screens: **Policies** > **Access Control** > **Decryption** > **Create Decryption Policy** See: Create a Decryption Policy
QUIC decryption.	7.6.0	7.6.0 with Snort 3	You can configure the decryption policy to apply to sessions running on the QUIC protocol. QUIC decryption is disabled by default. You can selectively enable QUIC decryption per decryption policy and write decryption rules to apply to QUIC traffic. By decrypting QUIC connections, the system can then inspect the connections for intrusion, malware, or other issues. You can also apply granular control and filtering of decrypted QUIC connections based on specific criteria in the access control policy. We modified the decryption policy Advanced Settings to include the option to enable QUIC decryption. See: Decryption Policy Advanced Options
Hardware			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200.	7.6.0	7.6.0	You can now disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200. By default, the port is enabled. New/modified Firewall Threat Defense CLI commands: **system support usb show**, **system support usb port disable**, **system support usb port enable** New/modified FXOS CLI commands for the Secure Firewall 3100/4200 in multi-instance mode: **show usb-port**, **disable USB port**, **enable usb-port** See: *Cisco Secure Firewall Threat Defense Command Reference* and *Cisco Firepower 4100/9300 FXOS Command Reference*
Network module for the Secure Firewall 4200.	7.6.0	7.6.0	We introduced this network module for the Secure Firewall 4200: • 2-port 400G network module (FPR-X-NM-2X400G) The module is also designed to support 200-Gb, 100-Gb, and 40-Gb per port. It provides full-duplex Ethernet traffic per port. The 400-Gb network module supports two QSFP-DD transceivers and is designed to also support 200-Gb QSFP56, 100-Gb QSFP28, and 40-Gb QSFP+ transceivers. See: *Cisco Secure Firewall 4200 Series Hardware Installation Guide*
Secure Firewall 1200.	7.6.0	7.6.0	We introduced the Secure Firewall 1200, which includes these models: • Secure Firewall 1210CX, with 8x1000BASE-T ports • Secure Firewall 1210CP, with 8x1000BASE-T ports, where ports 1/5-1/8 support power over Ethernet (PoE) • Secure Firewall 1220CX, with 8x1000BASE-T ports and two SFP+ ports See: *Cisco Secure Firewall 1210CE, 1210CP, and 1220CX Hardware Installation Guide*
Health Monitoring			
Apply a default health policy upon device registration.	7.6.0	Any	You can now choose a default health policy to apply upon device registration. On the health policy page, the policy name indicates which is the default. If you want to use a different policy for a specific device post-registration, change it there. You cannot delete the default device health policy. New/modified screens: **System** (⚙) > **Health** > **Policy** > **More** (⋮) > **Set as Default** See: Set a Default Health Policy

Feature	Minimum Management Center	Minimum Threat Defense	Details
Collect health data without alerting.	7.6.0	Any	You can now disable health alerts/health alert sub-types for ASP Drop, CPU, and Memory health modules, while continuing to collect health data. This allows you to minimize health alert noise and focus on the most critical issues. New/modified screens: In any health policy (**System** (⚙) > **Health** > **Policy**), there are now checkboxes that enable and disable ASP Drop (Firewall Threat Defense only), CPU, and Memory health alert sub-types. See: Health
High Availability/Scalability: Firewall Threat Defense			
16-node clusters for the Secure Firewall 3100/4200.	7.6.0	7.6.0	For the Secure Firewall 3100 and 4200, the maximum nodes were increased from 8 to 16. See: Clustering for the Secure Firewall 3100/4200
Firewall Threat Defense high availability automatically resumes after restoring from backup.	Any	7.6.0	When replacing a failed unit in a high availability pair, you no longer have to manually resume high availability after the restore completes and the device reboots. You should still confirm that high availability has resumed before you deploy. See: Restoring Management Centers and Managed Devices
Individual interface mode for Secure Firewall 3100/4200 clusters.	7.6.0	7.6.0	Individual interfaces are normal routed interfaces, each with their own local IP address used for routing. The main cluster IP address for each interface is a fixed address that always belongs to the control node. When the control node changes, the main cluster IP address moves to the new control node, so management of the cluster continues seamlessly. Load balancing must be configured separately on the upstream switch. Restrictions: Not supported for container instances. New/modified screens: • **Devices** > **Device Management** > **Add Cluster** • **Devices** > **Device Management** > **Cluster** > **Interfaces / EIGRP / OSPF / OSPFv3 / BGP** • **Objects** > **Object Management** > **Address Pools** > **MAC Address Pool** See: Clustering for the Secure Firewall 3100/4200 and Address Pools

Feature	Minimum Management Center	Minimum Threat Defense	Details
MTU ping test from data node on node join	7.6.0	7.6.0	When a node joins the cluster, it checks MTU compatibility by sending a ping to the control node with a packet size twice the cluster control link MTU. Previously, only the control node sent a ping. If the ping fails, a notification is generated so you can fix the MTU mismatch on connecting switches and try again. Added/modified commands: **show cluster history**. See: Clustering for the Secure Firewall 3100/4200, Clustering for Threat Defense Virtual in a Private Cloud, Clustering for Threat Defense Virtual in a Public Cloud, Clustering for the Firepower 4100/9300
Multi-instance mode conversion in the Firewall Management Center for the Secure Firewall 3100/4200.	7.6.0	7.6.0	You can now register an application-mode device to the Firewall Management Center and then convert it to multi-instance mode without having to use the CLI. New/modified screens: • **Devices** > **Device Management**, then for a device, click **More** (⋮) > **Convert to Multi-Instance** • **Devices** > **Device Management**, then select multiple devices and choose **Select Bulk Action** > **Convert to Multi-Instance** See: Convert a Device to Multi-Instance Mode
Multi-instance mode for the Secure Firewall 4200.	7.6.0	7.6.0	Multi-instance mode is now supported on the Secure Firewall 4200. See: Multi-Instance Mode for the Secure Firewall 3100/4200
Identity			
Easily configure an ISE identity source.	7.6.0	7.6.0	The system can use External RESTful Services (ERS) Operator user credentials to log into a Cisco ISE Primary Authentication Node (PAN), download certificates, and configure the identity source. Restrictions: Not supported for ISE-PIC. See: Cisco ISE Quick Configuration

Feature	Minimum Management Center	Minimum Threat Defense	Details
Microsoft Azure AD realms for active or passive authentication.	7.6.0	Active: 7.6.0 with Snort 3 Passive: 7.4.0 with Snort 3	You can now use Microsoft Azure Active Directory (AD) realms for active and passive authentication: • Active authentication using Azure AD: Use Azure AD as a captive portal. • Passive authentication using Cisco ISE (introduced in Version 7.4.0): The Firewall Management Center gets groups from Azure AD and logged-in user session data from ISE. We use SAML (Security Assertion Markup Language) to establish a trust relationship between a service provider (the devices that handle authentication requests) and an identity provider (Azure AD). **Upgrade impact**. If you had a Microsoft Azure AD realm configured before the upgrade, it is displayed as a SAML - Azure AD realm configured for passive authentication. All previous user session data is preserved. New/modified screens: **Integration** > **Other Integrations** > **Realms** > **Add Realm** > **SAML - Azure AD** New/modified CLI commands: none See: Create a Microsoft Azure AD (SAML) Realm.
New connectors for Dynamic Attributes Connector.	7.6.0	Any	Dynamic Attributes Connector now supports AWS security groups, AWS service tags, and Cisco Cyber Vision. Version restrictions: For on-prem Dynamic Attributes Connector integrations, requires Version 3.0. See: AWS service groups connector, AWS service tags connector, Cisco Cyber Vision connector

Feature	Minimum Management Center	Minimum Threat Defense	Details
Passive identity agent for Microsoft AD.	7.6.0	Any	This feature is introduced. Passive identity agent version 1.1 is compatible with 7.6.0 and later and adds the following: • You can use either FQDN, IPv4, or IPv6 to connect from the Passive Identity Agent to the Secure Firewall Management Center or Security Cloud Control. • Sends both IPv4 and IPv6 user sessions from Microsoft Active Directory (AD) to the Firewall Management Center. • You can zip troubleshooting logs. • When you start the passive identity agent software, a list of prerequisites is displayed. The passive identity agent identity source sends session data from Microsoft Active Directory (AD) to the Firewall Management Center. Passive identity agent software is supported on: • Microsoft AD server (Windows Server 2008 or later) • Microsoft AD domain controller (Windows Server 2008 or later) • Any client connected to the domain you want to monitor (Windows 8 or later) See: User Control With the Passive Identity Agent.
Logging and Analysis			
Easily filter unified events by event type.	7.6.0	Any	The unified events viewer now has buttons under the Search field that allow you to quickly filter by event type. See: Unified Events

Feature	Minimum Management Center	Minimum Threat Defense	Details
MITRE and other enrichment information in connection events.	7.6.0	7.6.0 with Snort 3	MITRE and other enrichment information in connection events makes it easy to access contextual information for detected threats. This includes information from Talos and from the encrypted visibility engine (EVE). For EVE enrichment, you must enable EVE. Connection events have two new fields, available in both the unified and classic event viewers: • **MITRE ATT&CK**: Click the progression graph to see an expanded view of threat details, including tactics and techniques. • **Other Enrichment**: Click to see any other available enrichment information, including from EVE. The new Talos Connectivity Status health module monitors Firewall Management Center connectivity with Talos, which is required for this feature. For the specific internet resources required, see Internet Access Requirements. See: Connection and Security-Related Connection Event Fields
Performance and Resiliency			
Hardware DTLS 1.2 crypto acceleration for the Secure Firewall 3100/4200.	7.6.0	7.6.0 with Snort 3	The Secure Firewall 3100/4200 now supports DTLS 1.2 cryptographic acceleration and egress optimization, which improves throughput of DTLS-encrypted and decrypted traffic. This is automatically enabled on new and upgraded devices. To disable, use FlexConfig. New/modified FlexConfig commands: **flow-offload-dtls**, **flow-offload-dtls egress-optimization**, **show flow-offload-dtls** See: DTLS Crypto Acceleration
Object group search performance enhancements.	7.6.0	Any	Object group search is now faster and uses fewer CPU resources. New CLI commands: **clear asp table network-object**, **show asp table network-object**, **debug acl ogs** Modified CLI comments (enhanced output): , **packet-tracer**, **show access-list**, **show object-group** See: Configure Object Group Search and *Cisco Secure Firewall Threat Defense Command Reference*
Public and Private Cloud			
Deploy Firewall Threat Defense Virtual for AWS in two-arm-mode with GWLB.	7.6.0	7.6.0	You can now deploy Firewall Threat Defense Virtual for AWS in two-arm-mode with GWLB. This allows you to directly forward internet-bound traffic after traffic inspection, while also performing network address translation (NAT). Two-arm mode is supported in single and multi-VPC environments. Restrictions: Not supported with clustering. See: Secure Firewall Threat Defense Virtual getting started guides

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deploy virtual firewall clusters across multiple AWS availability zones.	7.6.0 fault	7.6.0	You can now deploy Firewall Threat Defense Virtual clusters across multiple availability zones in an AWS region. This enables continuous traffic inspection and dynamic scaling (AWS Auto Scaling) during disaster recovery. See: *Deploy a Threat Defense Virtual Cluster on AWS*
SD-WAN			
SD-WAN wizard.	7.6.0	Hub: 7.6.0 Spoke: 7.3.0	A new wizard allows you to easily configure VPN tunnels between your centralized headquarters and remote branch sites. New/modified screens: **Devices** > **VPN** > **Site To Site** > **Add** > **SD-WAN Topology** See: Configure an SD-WAN Topology Using the SD-WAN Wizard
Security and Hardening			
TLS 1.3 support for the Firewall Management Center management interface.	7.6.0	Any	The Firewall Management Center web server now supports TLS 1.3 for HTTPS connections to the management interface. TLS 1.2 remains supported when clients use modern, secure cipher suites, including AES256-GCM-SHA384 and AES128-GCM-SHA256.
Threat Detection and Application Identification			
Bypass encrypted visibility engine (EVE) block verdict for trusted traffic.	7.6.0	Any with Snort 3	You can now bypass EVE block verdicts for known trusted traffic, based on destination network or EVE process name. Connections that bypass EVE in this way have the new **EVE Exempted** reason. New/modified screens: • To add an exception from the access control policy, in the advanced settings, edit and enable **Encrypted Visibility Engine**, enable **Block Traffic Based on EVE Score**, and **Add Exception Rule**. • To add an exception from the Unified Events viewer, right-click a connection that was blocked by EVE and select **Add EVE Exception**. See: Encrypted Visibility Engine
Snort ML: neural network-based exploit detector.	7.6.0	7.6.0 with Snort 3	A new Snort 3 inspector, snort_ml, uses neural network-based machine learning (ML) to detect known and 0-day attacks without needing multiple preset rules. The inspector subscribes to HTTP events and looks for the HTTP URI, which in turn is used by a neural network to detect exploits (currently limited to SQL injections). The new inspector is currently disabled in all default policies except maximum detection. A new intrusion rule, GID:411 SID:1, generates an event when the snort_ml detects an attack. This rule is also currently disabled in all default policies except maximum detection. See: *Snort 3 Inspector Reference*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Troubleshooting and Serviceability			
Application detection debug logs in connection-based troubleshooting.	7.6.0	7.6.0 with Snort 3	For connection-based troubleshooting, you can now collect debug logs from application detectors. New/modified CLI commands: **debug packet-module appid** enables and sets the severity level for application detector debug logs. You can choose 3 (error), 4 (warning), or 7 (debug). See: Connection-Based Troubleshooting and *Cisco Secure Firewall Threat Defense Command Reference*
Packet tracer improvements.	7.6.0	Varies.	Packet tracker improvements allow you to: • Capture and replay identity trace data (requires Firewall Threat Defense 7.6.0 with Snort 3). • Replay packet trace data on NAT-configured devices. • Replay packet trace data that imitates the actual timing of the packets, for a more realistic simulation. • Save packet trace data as PCAP file, which can be viewed using third-party tools like Wireshark. New/modified commands: • To enable the timestamp option, use the **honor-timestamp** keyword in the **packet-tracer** command: **packet-tracer input***ifc_name* **pcap***pcap_filename* [**honor-timestamp**] • To store the device-generated packet trace data as part of the PCAP file, use the **export-pcapng** keyword in the **show packet tracer** command: **show packet-tracer pcap trace** [**export-pcapng**] See: Packet Tracer and *Cisco Secure Firewall Threat Defense Command Reference*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Receive additional Firewall Threat Defense troubleshooting syslogs, and view them as unified events. VPN troubleshooting syslogs moved.	7.6.0	Any with Snort 3	You can now configure Firewall Threat Defense to send all device troubleshooting syslogs (instead of just VPN troubleshooting syslogs) to the Firewall Management Center. New/modified screens: • To send device troubleshooting syslogs to the Firewall Management Center, use Firewall Threat Defense platform settings: **Devices** > **Platform Settings** > **Syslog** > **Logging to Secure Firewall Management Center** • To view all device troubleshooting syslogs, **Devices** > **Troubleshooting Logs** replaces **Devices** > **VPN** > **Troubleshooting**. • To view device troubleshooting syslogs in context with other events, use **Analysis** > **Unified Events**, where we added a **Troubleshoot Events** type. See: Configure Syslog Logging for Threat Defense Devices and View Troubleshooting Syslogs in the Secure Firewall Management Center
Troubleshoot Snort 3 performance issues with a CPU and rule profiler.	7.6.0	7.6.0 with Snort 3	New CPU and rule profilers help you troubleshoot Snort 3 performance issues. You can now monitor: • CPU time taken by Snort 3 modules/inspectors to process packets. • CPU resources each module is consuming, relative to the total CPU consumed by the Snort 3 process. • Modules with unsatisfactory performance when Snort 3 is consuming high CPU. • Intrusion rules with unsatisfactory performance. New/modified screens: **Devices** > **Troubleshoot** > **Snort 3 Profiling** Platform restrictions: Not supported for container instances. See: Advanced Troubleshooting for the Secure Firewall Threat Defense Device
Upgrade			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Generate and download post-upgrade configuration change reports from the Firewall Threat Defense and chassis upgrade wizards.	7.6.0	Any	You can now generate and download post-upgrade configuration change reports from the Firewall Threat Defense and chassis upgrade wizards, as long as you have not cleared your upgrade workflow. Previously, you used the Advanced Deploy screens to generate the reports and the Message Center to download them. Note that you can still use this method, which is useful if you want to quickly generate change reports for multiple devices, or if you cleared your workflow. New/modified screens: • **Devices** > **Threat Defense Upgrade** > **Configuration Changes** • **Devices** > **Chassis Upgrade** > **Configuration Changes** See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
Improved upgrade process for high availability Firewall Management Centers.	7.6.0	Any	Upgrading high availability Firewall Management Centers is now easier: • You no longer have to manually copy the upgrade package to both peers. Depending on your setup, you can have each peer get the package from the support site, or you can copy the package between peers. • You no longer have to manually run the readiness check on both peers. Running it on one runs it on both. • If you do not have enough disk space to run the upgrade, a new **Clean Up Disk Space** option can help. • You no longer have to manually pause synchronization before upgrade, or resolve split brain after the upgrade; the system now does this automatically. Also, your original active/standby roles are preserved. Note that although you can complete most of the upgrade process from one peer (we recommend the standby), you do have to log into the second peer to actually initiate its upgrade. New/modified screens: **System** (⚙) > **Product Upgrades** Version restrictions: This feature applies to upgrades *from* Version 7.6.0 and later, not *to* 7.6.0. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
Deprecated Features			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: Copy upgrade packages ("peer-to-peer sync") from device to device.	7.6.0	7.6.0	You can no longer use the Firewall Threat Defense CLI to copy upgrade packages between devices over the management network. If you have limited bandwidth between the Firewall Management Center and its devices, configure devices to get upgrade packages directly from an internal web server. Deprecated CLI commands: **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status**
End of management support: ASA FirePOWER and NGIPSv.	7.6.0	—	You cannot manage Classic devices (ASA FirePOWER and NGIPSv) with a Version 7.6+ Firewall Management Center. This is because Classic devices cannot be upgraded past Version 7.0, and a Version 7.6 Firewall Management Center can only manage devices as far back as Version 7.1. New/modified screens: For new and upgraded Firewall Management Centers, Classic-specific configurations and screens are removed. This includes platform settings, NAT, syslog logging, licensing, and so on. In some cases, creating Firewall Threat Defense configurations is quicker because you do not have to begin by selecting a device type.
Deprecated: backup of locally stored reports on the Firewall Management Center.	7.6.0	Any	Locally stored reports are no longer backed up. You should store reports in a secure remote location.
End of support: analytics-only capabilities with the full range of Firewall Threat Defense devices supported with Cloud-Delivered Firewall Management Center.	Any	7.2.0	If you are co-managing Version 7.0.x devices with Cloud-Delivered Firewall Management Center and an on-prem analytics-only Firewall Management Center, you cannot upgrade the analytics Firewall Management Center to Version 7.6 (which would allow you to add Version 7.6 devices) until you upgrade the older devices to 7.2+, or replace or remove them. See: *Cisco Secure Firewall Management Center Compatibility Guide*
Deprecated: Legacy and insecure TLS 1.2 cipher suites on the Firewall Management Center management interface.	7.6.0	Any	**Upgrade impact. Integrations running on Microsoft Windows Server 2012 that rely on legacy TLS 1.2 cipher suites fail after upgrade.** The Firewall Management Center web server configuration no longer includes older, insecure TLS 1.2 cipher suites, such as CBC-mode suites. TLS 1.2 itself remains fully supported with modern cipher suites, including AES256-GCM-SHA384 and AES128-GCM-SHA256. TLS 1.3 is also supported. If you use TSAgent or another integration on Windows Server 2012, migrate it to Windows Server 2016 or later, or to Windows Server 2012 R2 with applicable updates, before upgrading. Windows Server 2012 is end-of-life.

Feature	Minimum Management Center	Minimum Threat Defense	Details
End of support: Firepower 2110, 2120, 2130, 2140.	—	7.6.0	You cannot run Version 7.6+ on the Firepower 2110, 2120, 2130, or 2140. Although a newer Firewall Management Center can manage older devices, the Version 7.6 documentation only includes features supported in Version 7.6 Firewall Threat Defense. For features that are only supported with older devices, refer to the Firewall Management Center guide that matches your Firewall Threat Defense version.

Firewall Management Center Features in Version 7.4.8

There are no new features in this release.

Firewall Management Center Features in Version 7.4.7

Table 47: Firewall Management Center Features in Version 7.4.7

Feature	Minimum Management Center	Minimum Threat Defense	Details
Model Migration			
Migrate Firewall Management Center without upgrading first	7.4.7 (source) 7.6.6 (source) 10.0.0 (target)	7.3.0	You can now migrate an older Firewall Management Center to a Version 10.0+ Firewall Management Center without first upgrading the source system to the target version. **Note** Think of this process as a migration plus upgrade. Just as with regular upgrades, minimize impact by going **directly to the latest maintenance release** in your target major version. For release-specific upgrade warnings and guidelines, and for information on features and bugs with upgrade impact, see the Release Notes for Secure Firewall Threat Defense for your target version. Version restrictions: Not supported from a Version 7.6.x or 7.7.x Firewall Management Center. See: *Cisco Secure Firewall Management Center Model Migration Guide*

Firewall Management Center Features in Version 7.4.6

There are no new features in this release.

Firewall Management Center Features in Version 7.4.5

There are no new features in this release.

Firewall Management Center Features in Version 7.4.4

Due to CSCws69719, Version 7.4.4 for the Firewall Management Center was deferred on 202-10-13 and is no longer available for download. If you downloaded it, do not use it. If you are running this version, upgrade.

There are no new features in this release.

Firewall Management Center Features in Version 7.4.3

Table 48: Firewall Management Center Features in Version 7.4.3

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.4.3 also has: • New Cisco AMP cloud connection method. Upgrade impact. (7.0.7) • Deprecated Cisco AMP Cloud connection backups. (7.0.7) • Security Cloud Control regions: India and Australia. (7.0.7) • Require the Message-Authenticator attribute in all RADIUS responses. Upgrade impact. (7.0.7) • High-bandwidth encrypted application traffic bypasses unnecessary intrusion inspection. (7.2.10) • Firewall Threat Defense and chassis upgrade wizards optimized for lower resolution screens. (7.2.10)
Platform			
DC power supply for the Secure Firewall 4200	7.4.3 7.6.2 7.7.0	7.4.3 7.6.2 7.7.0	The FPR4200-PWR-DC for Secure Firewall 4200 is a 1500 W DC power supply. The dual power supply modules can supply up to 1500 W power across the input voltage range (48 VDC to 60 VDC). The load is shared when both power supply modules are plugged in and running at the same time.
Device Management			

Feature	Minimum Management Center	Minimum Threat Defense	Details
IMDSv2 support for AWS deployments.	7.4.3 7.6.0	7.4.3 7.6.0	Firewall Threat Defense and Firewall Management Center virtual for AWS now support Instance Metadata Service Version 2 (IMDSv2), a security improvement over IMDSv1. When you enable the instance metadata service on AWS, IMDSv2 Optional mode is still the default, but we recommend you choose IMDSv2 Required. We also recommend you switch your upgraded instances. Platform restrictions: Not available for Firewall Management Center Virtual 300 See: Secure Firewall Threat Defense Virtual getting started guides and *Cisco Secure Firewall Management Center Virtual Getting Started Guide*
Health Monitoring			
Independently configure health monitoring for physical and subinterfaces.	7.4.3 7.6.1 7.7.0	Any	You can now disable health monitoring for a physical interface while continuing to monitor and receive health alerts for its subinterfaces. You can disable alerts permanently or temporarily. To do this, configure the device for health monitoring exclusion, edit that configuration to enable module-level exclusion, and finally configure exclusion settings for the Interface Settings health module. New/modified screens: **System** (⚙) > **Health** > **Exclude** See: Health
View health status for devices in leaf domains while logged into the parent domain.	7.4.3 7.6.1 7.7.0	Any	In a multidomain deployment, you can now view health status for devices in leaf domains while logged into the parent domain. See: Health
Performance			
Faster failover for high availability Firewall Threat Defense.	7.4.3 7.6.4 7.7.0	7.4.3 7.6.4 7.7.0	With Firewall Threat Defense high availability failover, the new active device generates multicast packets for each MAC address entry and sends them to all bridge group interfaces, which prompts the upstream switches to update their routing tables. This task now runs asynchronously in the data plane, privileging critical failover tasks in the control plane. This makes failover faster, reducing downtime. See: High Availability
Integrations			
Umbrella integration with Firewall Management Center over a proxy.	7.4.3 7.6.1 7.7.10 10.0.0	Any	Umbrella integration with Firewall Management Center now works over a proxy. See: Configuring the Umbrella DNS Connector for Cisco Secure Firewall Management Center

Firewall Management Center Features in Version 7.4.2

Table 49: Firewall Management Center Features in Version 7.4.2

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.4.2 also has: • VMware vSphere/VMware ESXi 8.0 support. (7.2.9) • Asymmetric traffic handling. Upgrade impact. (7.2.9)
Platform			
Firewall Management Center Virtual 300 for Azure.	7.4.2 7.6.0	Any	We introduced the Firewall Management Center Virtual 300 for Azure. It can manage up to 300 devices, and high availability is supported. Migration from the FMCv25 for Azure is also supported. See: *Cisco Secure Firewall Management Center Virtual Getting Started Guide* and *Cisco Secure Firewall Management Center Model Migration Guide*
High Availability: Management Center			
High availability for Firewall Management Center Virtual for Azure.	7.4.2 7.6.0	Any	We now support high availability for Firewall Management Center Virtual for Azure. 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 Version 7.0.x Classic devices only (NGIPSv or ASA FirePOWER), you do not need FMCv entitlements. Platform restrictions: Not supported with FMCv2 See: *Cisco Secure Firewall Management Center Virtual Getting Started Guide* and High Availability

Firewall Management Center Features in Version 7.4.1

Table 50: Firewall Management Center Features in Version 7.4.1

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.4.1 also has: • Support for Firewall Threat Defense on all device platforms supported in Version 7.3, and also on the Firepower 1010E (last supported in 7.2). • Updated web analytics provider. Upgrade impact. (7.0.6) • Management center detects interface sync errors. Upgrade impact. (7.2.5) • Configure DHCP relay trusted interfaces from the Firewall Management Center web interface. Upgrade impact. (7.2.6) • Create network groups while editing NAT rules. (7.2.6) • Single backup file for high availability Firewall Management Centers. (7.2.6) • Open the packet tracer from the unified event viewer. (7.2.6) • Health alerts for excessive disk space used by deployment history (rollback) files. (7.2.6) • Health alerts for NTP sync issues. (7.2.6) • View and generate reports on configuration changes since your last deployment. (7.2.6) • Set the number of deployment history files to retain for device rollback. (7.2.6) • Improved upgrade starting page and package management. (7.2.6) • Enable revert from the Firewall Threat Defense upgrade wizard. (7.2.6) • View detailed upgrade status from the Firewall Threat Defense upgrade wizard. (7.2.6) • Suggested release notifications. (7.2.6) • New upgrade wizard for the Firewall Management Center. (7.2.6) • Hotfix high availability Firewall Management Centers without pausing synchronization. (7.2.6) • Updated internet access requirements for direct-downloading software upgrades. Upgrade impact. (7.2.6) • Enable/disable access control object optimization. (7.2.6) • Cluster control link ping tool. (7.2.6) • Set the frequency of Snort 3 core dumps. (7.2.6) • Capture dropped packets with the Secure Firewall 3100/4200. (7.2.6)

Feature	Minimum Management Center	Minimum Threat Defense	Details
Platform			
Network modules for the Secure Firewall 3130 and 3140.	7.4.1	7.4.1	The Secure Firewall 3130 and 3140 now support these network modules: • 2-port 100G QSFP+ network module (FPR3K-XNM-2X100G) See: *Cisco Secure Firewall 3100 Series Hardware Installation Guide*
Optical transceivers for Firepower 9300 network modules.	7.4.1	7.4.1	The Firepower 9300 now supports these optical transceivers: • QSFP-40/100-SRBD • QSFP-100G-SR1.2 • QSFP-100G-SM-SR On these network modules: • FPR9K-NM-4X100G • FPR9K-NM-2X100G • FPR9K-DNM-2X100G See: *Cisco Firepower 9300 Hardware Installation Guide*
Performance profile support for the Secure Firewall 3100.	7.4.1	7.4.1	The performance profile settings available in the platform settings policy now apply to the Secure Firewall 3100. Previously, this feature was supported on the Firepower 4100/9300, the Secure Firewall 4200, and on Firewall Threat Defense Virtual. See: Platform Settings
Interfaces			
Deploy without the diagnostic interface on Firewall Threat Defense Virtual for Azure and GCP.	7.4.1	7.4.1	You can now deploy without the diagnostic interface on Firewall Threat Defense Virtual for Azure and GCP. Previously, we required one management, one diagnostic, and at least two data interfaces. New interface requirements are: • Azure: one management, two data (max eight) • GCP: one management, three data (max eight) Restrictions: This feature is supported for new deployments only. It is not supported for upgraded devices. See: Secure Firewall Threat Defense Virtual getting started guides
Device Management			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Inspect and protect traffic through an Azure Virtual WAN hub.	7.4.1	7.4.1	You can now use Firewall Threat Defense Virtual for Azure to inspect and protect traffic through a Microsoft Azure Virtual WAN hub. This integration allows you to consistently and easily apply security policies and configurations across all spokes in the hub, and to leverage built-in scalability and load balancer capabilities for optimal performance. See: Secure Firewall Threat Defense Virtual getting started guides
Device management services supported on user-defined VRF interfaces.	7.4.1	Any	Device management services configured in the Firewall Threat Defense platform settings (NetFlow, SSH access, SNMP hosts, syslog servers) are now supported on user-defined Virtual Routing and Forwarding (VRF) interfaces. Platform restrictions: Not supported with container instances or clustered devices. See: Platform Settings
High Availability/Scalability: Firewall Threat Defense			
Multi-instance mode for the Secure Firewall 3100.	7.4.1	7.4.1	You can deploy the Secure Firewall 3100 as a single device (*appliance mode*) or as multiple container instances (*multi-instance mode*). In multi-instance mode, you can deploy multiple container instances on a single chassis that act as completely independent devices. Note that in multi-instance mode, you upgrade the operating system and the firmware (*chassis upgrade*) separately from the container instances (*Firewall Threat Defense upgrade*). New/modified screens: • **Devices** > **Device Management** > **Add** > **Chassis** • **Devices** > **Device Management** > **Device** > **Chassis Manager** • **Devices** > **Platform Settings** > **New Policy** > **Chassis Platform Settings** • **Devices** > **Chassis Upgrade** New/modified Firewall Threat Defense CLI commands: **configure multi-instance network ipv4**, **configure multi-instance network ipv6** New/modified FXOS CLI commands: **create device-manager**, **set deploymode** Platform restrictions: Not supported on the Secure Firewall 3105. See: Multi-Instance Mode for the Secure Firewall 3100 and Secure Firewall Threat Defense upgrade guides for Firewall Management Center
16-node clusters for Firewall Threat Defense Virtual for VMware and KVM.	7.4.1	7.4.1	You can now configure 16-node clusters for Firewall Threat Defense Virtual for VMware and Firewall Threat Defense Virtual for KVM. See: Clustering for Firewall Threat Defense Virtual in a Private Cloud

Feature	Minimum Management Center	Minimum Threat Defense	Details
Target failover for clustered Firewall Threat Defense Virtualdevices for AWS.	7.4.1	7.4.1	You can now configure target failover for clustered Firewall Threat Defense Virtual for AWS using the AWS Gateway Load Balancer (GWLB). Platform restrictions: Not available with five and ten-device licenses. See: Clustering for Firewall Threat Defense Virtual in a Public Cloud
Detect configuration mismatches in Firewall Threat Defense high availability pairs.	7.4.1	7.4.1	You can now use the CLI to detect configuration mismatches in Firewall Threat Defense high availability pairs. New/modified CLI commands: **show failover config-sync error**, **show failover config-sync stats** See: High Availability and *Cisco Secure Firewall Threat Defense Command Reference*
High Availability: Management Center			
Firewall Management Center high availability synchronization enhancements.	7.4.1	Any	Firewall Management Center high availability (HA) includes the following synchronization enhancements: • Large configuration history files can cause synchronization to fail in high-latency networks. To prevent this from happening, the device configuration history files are now synchronized in parallel with other configuration data. This enhancement also reduces the synchronization time. • The Firewall Management Center now monitors the configuration history file synchronization process and displays a health alert if the synchronization times out. New/modified screens: You can view these alerts on the following screens: • **Notifications** > **Message Center** > **Health** • **Integration** > **Other Integrations** > **High Availability** > **Status** (under **Summary**) See: High Availability
SD-WAN			
Application monitoring on the SD-WAN Summary dashboard.	7.4.1	7.4.1	You can now monitor WAN interface application performance on the SD-WAN Summary dashboard. New/modified screens: **Overview** > **SD-WAN Summary** > **Application Monitoring** See: VPN Monitoring and Troubleshooting
VPN			

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

Feature	Minimum Management Center	Minimum Threat Defense	Details
Zero trust access enhancements.	7.4.1	7.4.1 with Snort 3	Firewall Management Center now includes the following zero trust access enhancements: • You can configure source NAT for an application. The configured network object or object group translates the incoming request's public network source IP address to a routable IP address inside the application network. • You can troubleshoot the zero trust configuration issues using the diagnostics tool. New/modified screens: **Policies** > **Access Control** > **Zero Trust Application** New/modified CLI commands: **show running-config zero-trust**, **show zero-trust statistics** See: Zero Trust Access, *Cisco Secure Firewall Threat Defense Command Reference*
CIP detection.	7.4.1	7.4.1 with Snort 3	You can now detect and handle Common Industrial Protocol (CIP) by using CIP and Ethernet/IP (ENIP) application conditions in your security policies. See: Access Control Rules
CIP safety detection.	7.4.1	7.4.1 with Snort 3	CIP Safety is a CIP extension that enables the safe operation of industrial automation applications. The CIP inspector can now detect the CIP Safety segments in the CIP traffic. To detect and take action on the CIP Safety segments, enable the CIP inspector in the Firewall Management Center's network Analysis policy and assign it to an access control policy. New/modified screens: **Policies** > **Access Control** > Edit a policy > **Add Rule** > **Applications** tab > Search for CIP Safety in the search box. See: Cisco Secure Firewall Management Center Snort 3 Configuration Guide
Access Control: Identity			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Captive portal support for multiple Active Directory realms (realm sequences).	7.4.1	7.4.1	**Upgrade impact. Update custom authentication forms.** You can configure active authentication for either an LDAP realm; or a Microsoft Active Directory realm or a realm sequence. In addition, you can configure a passive authentication rule to fall back to active authentication using either a realm or a realm sequence. You can optionally share sessions between managed devices that share the same identity policy in access control rules. In addition, you have the option to require users to authenticate again when they access the system using a different managed device than they accessed previously. If you use the HTTP Response Page authentication type, after you upgrade Firewall Threat Defense, you must add **`<select name="realm" id="realm"></select>`** to your custom authentication form. This allows the user to choose between realms. Restrictions: Not supported with Microsoft Azure Active Directory. New/modified screens: • **Policies** > **Identity** > **(edit policy)** > **Active Authentication** > **Share active authentication sessions across firewalls** • **Identity policy** > **(edit)** > **Add Rule** > **Passive Authentication** > **Realms & Settings** > **Use active authentication if passive or VPN identity cannot be established** • **Identity policy** > **(edit)** > **Add Rule** > **Active Authentication** > **Realms & Settings** > **Use active authentication if passive or VPN identity cannot be established** See: User Control with Captive Portal
Share captive portal active authentication sessions across firewalls.	7.4.1	7.4.1	Determines whether or not users are required to authenticate when their authentication session is sent to a different managed device than one they previously connected to. If your organization requires users to authenticate every time they change locations or sites, you should *disable* this option. • (Default.) Enable to allow users to authenticate with any managed device associated with the active authentication identity rule. • Disable to require the user to authenticate with a different managed device, even if they have already authenticated with another managed device to which the active authentication rule is deployed. New/modified screens: **Policies** > **Identity** > **(edit policy)** > **Active Authentication** > **Share active authentication sessions across firewalls** See: User Control with Captive Portal

Feature	Minimum Management Center	Minimum Threat Defense	Details
Merge downloadable access control list with a Cisco attribute-value pair ACL for RADIUS identity sources, using the Firewall Management Center web interface.	7.4.1	Any	**Upgrade impact. Redo any related FlexConfigs after upgrade.** New/modified screens: **Objects** > **Object Management** > **AAA Server** > **RADIUS Server Group** > **Add RADIUS Server Group** > **Merge Downloadable ACL with Cisco AV Pair ACL** New CLI commands: • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl after-avpair** • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl before-avpair** See: Object Management
Health Monitoring			
Chassis-level health alerts for the Firepower 4100/9300.	7.4.1	Any with FXOS 2.14.1	You can now view chassis-level health alerts for Firepower 4100/9300 by registering the chassis to the Firewall Management Center as a read-only device. You must also enable the Firewall Threat Defense Platform Faults health module and apply the health policy. The alerts appear in the Message Center, the health monitor (in the left pane, under Devices, select the chassis), and in the health events view. You can also add a chassis (and view health alerts for) the Secure Firewall 3100 in multi-instance mode. For those devices, you use the Firewall Management Center to manage the chassis. But for the Firepower 4100/9300 chassis, you still must use the chassis manager or the FXOS CLI. New/modified screens: **Devices** > **Device Management** > **Add** > **Chassis** See: Device Management

Feature	Minimum Management Center	Minimum Threat Defense	Details
Improved Firewall Management Center memory usage calculation, alerting, and swap memory monitoring.	7.4.1	Any	**Upgrade impact. Memory usage alert thresholds may be lowered.** We improved the accuracy of Firewall Management Center memory usage and have lowered the default alert thresholds to 88% warning/90% critical. If your thresholds were higher than the new defaults, the upgrade lowers them automatically—you do not have to apply health policies for this change to take place. Note that the Firewall Management Center may now reboot in extremely critical system memory condition if terminating high-memory processes does not work. You can also add new swap memory usage metrics to a new or existing Firewall Management Center health dashboard. Make sure you choose the **Memory** metric group. New/modified screens: • **System** (⚙) > **Health** > **Monitoring** > **Firewall Management Center** > **Add/Edit Dashboard** > **Memory** • **System** (⚙) > **Health** > **Policy** > **Management Center Health Policy** > **Memory** See: Health
Deployment and Policy Management			
Change management.	7.4.1	Any	You can enable change management if your organization needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed. We added the **System**(⚙) > **Configuration** > **Change Management** page to enable the feature. When enabled, there is a **System**(⚙) > **Change Management Workflow** page, and a new **Ticket**(📋) quick access icon in the menu. See: Change Management
Upgrade			
Firmware upgrades included in FXOS upgrades.	7.4.1	Any	**Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.** For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1 now include firmware upgrades. If any firmware component on the device is older than the one included in the FXOS bundle, the FXOS upgrade also updates the firmware. If the firmware is upgraded, the device reboots twice—once for FXOS and once for the firmware. Just as with software and operating system upgrades, do not make or deploy configuration changes during firmware upgrade. Even if the system appears inactive, do not manually reboot or shut down during firmware upgrade. See: *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Automatically generate configuration change reports after Firewall Management Center upgrade.	7.4.1	Any	You can automatically generate reports on configuration changes after major and maintenance Firewall Management Center upgrades. This helps you understand the changes you are about to deploy. After the system generates the reports, you can download them from the Tasks tab in the Message Center. Version restrictions: Only supported for Firewall Management Center upgrades from Version 7.4.1+. Not supported for upgrades to Version 7.4.1 or any earlier version. New/modified screens: **System** > **Configuration** > **Upgrade Configuration** > **Enable Post-Upgrade Report** See: System Configuration
Administration			
Erase the hard drives on a hardware Firewall Management Center.	7.4.1	Any	You can use the Firewall Management Center CLI to reboot and permanently erase its own hard drive data. After the erase is completed, you can install a fresh software image. New/modified CLI commands: **secure erase** See: Secure Firewall Management Center Command Line Reference
Troubleshooting			
Troubleshooting file generation and download available from Device and Cluster pages.	7.4.1	7.4.1	You can generate and download troubleshooting files for each device on the Device page and also for all cluster nodes on the Cluster page. For a cluster, you can download all files as a single compressed file. You can also include cluster logs for the cluster for cluster nodes. You can alternatively trigger file generation from the **Devices** > **Device Management** > **More** > **Troubleshoot Files** menu. New/modified screens: • **Devices** > **Device Management** > **Device** > **General** • **Devices** > **Device Management** > **Cluster** > **General** See: Device Management
Automatic generation of a troubleshooting file on a node when it fails to join the cluster.	7.4.1	7.4.1	If a node fails to join the cluster, a troubleshooting file is automatically generated for the node. You can download the file from **Tasks** or from the **Cluster** page.
View CLI output for a device or device cluster.	7.4.1	Any	You can view a set of pre-defined CLI outputs that can help you troubleshoot the device or cluster. You can also enter any **show** command and see the output. New/modified screens: **Devices** > **Device Management** > **Cluster** > **General** See: Device Management

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

Firewall Management Center Features in Version 7.4.0

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

Table 51: Firewall Management Center Features in Version 7.4.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.4.0 also has: • Smaller VDB for lower memory Snort 2 devices. (7.0.6) • Access control performance improvements (object optimization). Upgrade impact. (7.0.6) • Deprecated: `high unmanaged disk usage` alerts. (7.0.6) • Reduced "false failovers" for Firewall Threat Defense high availability. (7.2.6) • Secure Firewall 3105. (7.3.1)
Platform			
Firewall Management Center 1700, 2700, 4700.	7.4.0	Any	We introduced the Firewall Management Center 1700, 2700, and 4700, which can manage up to 300 devices. Firewall Management Center high availability is supported. See: *Cisco Secure Firewall Management Center 1700, 2700, and 4700 Getting Started Guide*
Firewall Management Center Virtual for Microsoft Hyper-V.	7.4.0	Any	We introduced Firewall Management Center Virtual for Microsoft Hyper-V, which can manage up to 25 devices. Firewall Management Center high availability is supported. See: *Cisco Secure Firewall Management Center Virtual Getting Started Guide*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Secure Firewall 4200.	7.4.0 m	7.4.0	We introduced the Secure Firewall 4215, 4225, and 4245. These devices support the following new network modules: • 2-port 100G QSFP+ network module (FPR4K-XNM-2X100G) • 4-port 200G QSFP+ network module (FPR4K-XNM-4X200G) See: *Cisco Secure Firewall 4200 Series Hardware Installation Guide*
Performance profile support for the Secure Firewall 4200.	7.4.0	7.4.0	The performance profile settings available in the platform settings policy now apply to the Secure Firewall 4200. Previously, this feature was supported only on the Firepower 4100/9300 and on Firewall Threat Defense Virtual. See: Platform Settings
Platform Migration			
Migrate Firepower 1000/2100 to Secure Firewall 3100.	7.4.0	Any	You can now easily migrate configurations from the Firepower 1000/2100 to the Secure Firewall 3100. New/modified screens: **Devices** > **Device Management** > **Migrate** Platform restrictions: Migration not supported from the Firepower 1010 or 1010E. See: Device Management
Migrate Firepower Management Center 4600 to Secure Firewall Management Center for AWS.	7.4.0	Any	You can migrate from Firepower Management Center 4600 to Secure Firewall Management Center Virtual for AWS with a 300-device license. See: *Cisco Secure Firewall Management Center Model Migration Guide*
Migrate Firepower Management Center 1600/2600/4600 to Secure Firewall Management Center 1700/2700/4700.	7.4.0	Any	You can migrate from Firepower Management Center 1600/2600/4600 to Secure Firewall Management Center 1700/2700/4700. See: *Cisco Secure Firewall Management Center Model Migration Guide*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Migrate Firepower Management Center 1000/2500/4500 to Secure Firewall Management Center 1700/2700/4700.	7.4.0 only	7.0.0	You can migrate a Firepower Management Center 1000/2500/4500 to a Version 7.4.0 Secure Firewall Management Center 1700/2700/4700. To migrate, you must *temporarily* upgrade the old Firewall Management Center from Version 7.0 to Version 7.4.0. **Important** Migration is supported to/from Version 7.4.0 only, and Version 7.4.0 is only supported on the 1000/2500/4500 during the migration process. Do not upgrade the source or target to later maintenance releases. You should minimize the time between Firewall Management Center upgrade and device migration. To summarize the migration process: **1.** Prepare for upgrade and migration. Read, understand, and meet all the prerequisites outlined in the release notes, upgrade guides, and migration guide. Make sure the old Firewall Management Center is ready to go: freshly deployed, fully backed up, all appliances in good health, etc. You should also set up the new Firewall Management Center. **2.** Upgrade the old Firewall Management Center and all its managed devices to at least Version 7.0.0 (7.0.5 recommended). If you are already running the minimum version, you can skip this step. **3.** Upgrade the old Firewall Management Center to Version 7.4.0. Unzip (but do not untar) the upgrade package before uploading it to the Firewall Management Center. Download from: Special Release. **4.** Migrate the Firewall Management Center as described in the model migration guide. **5.** Verify migration success. If the migration does not function to your expectations and you want to switch back, note that Version 7.4 is unsupported for general operations on the 1000/2500/4500. To return the old Firewall Management Center to a supported version you must reimage back to Version 7.0, restore from backup, and reregister devices. See: • Release Notes for Secure Firewall Threat Defense • Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 • *Cisco Secure Firewall Management Center Model Migration Guide* If you have questions or need assistance at any point in the migration process, contact Cisco TAC.

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

Feature	Minimum Management Center	Minimum Threat Defense	Details
			You can migrate devices from Firepower Management Center 1000/2500/4500 to . To migrate devices, you must *temporarily* upgrade the on-prem Firewall Management Center from Version 7.0.3 (7.0.5 recommended) to Version 7.4.0. This temporary upgrade is required because Version 7.0 Firewall Management Centers do not support device migration to the cloud. Additionally, only standalone and high availability Firewall Threat Defense running Version 7.0.3+ (7.0.5 recommended) are eligible for migration. Cluster migration is not supported at this time. **Important** Version 7.4.0 is only supported on the 1000/2500/4500 during the migration process. You should minimize the time between Firewall Management Center upgrade and device migration. To summarize the migration process: **1.** Prepare for upgrade and migration. Read, understand, and meet all the prerequisites outlined in the release notes, upgrade guides, and migration guide. Before you upgrade, it is especially important that the on-prem Firewall Management Center is "ready to go," that is, managing only the devices you want to migrate, configuration impact assessed (such as VPN impact), freshly deployed, fully backed up, all appliances in good health, and so on. You should also provision, license, and prepare the cloud tenant. This must include a strategy for security event logging; you cannot retain the on-prem Firewall Management Center for analytics because it will be running an unsupported version. **2.** Upgrade the on-prem Firewall Management Center and all its managed devices to at least Version 7.0.3 (Version 7.0.5 recommended). If you are already running the minimum version, you can skip this step. **3.** Upgrade the on-prem Firewall Management Center to Version 7.4.0. Unzip (but do not untar) the upgrade package before uploading it to the Firewall Management Center. Download from: Special Release. **4.** Onboard the on-prem Firewall Management Center to CDO. **5.** Migrate all devices from the on-prem Firewall Management Center to the as described in the migration guide. When you select devices to migrate, make sure you choose **Delete FTD from On-Prem FMC**. Note that the device is not fully deleted unless you commit the changes or 14 days pass. **6.** Verify migration success. If the migration does not function to your expectations, you have 14 days

Feature	Minimum Management Center	Minimum Threat Defense	Details
			to switch back or it is committed automatically. However, note that Version 7.4.0 is unsupported for general operations. To return the on-prem Firewall Management Center to a supported version you must remove the re-migrated devices, re image back to Version 7.0.x, restore from backup, and reregister the devices. See: • Release Notes for Secure Firewall Threat Defense • Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 • Migrate On-Premises Management Center Managed Secure Firewall Threat Defense to Cloud-Delivered Firewall Management Center If you have questions or need assistance at any point in the migration process, contact Cisco TAC.
Device Management			
Zero-Touch Provisioning to register the Firepower 1000/2100 and Secure Firewall 3100 to the Firewall Management Center using a serial number.	7.4.0	Mgmt. center *is* publicly reachable: 7.2.0 Mgmt. center *is not* publicly reachable: 7.2.4, 7.4.1	Zero-Touch Provisioning (also called low-touch provisioning) lets you register Firepower 1000/2100 and Secure Firewall 3100 devices to the Firewall Management Center by serial number without having to perform any initial setup on the device. The Firewall Management Center integrates with SecureX and Security Cloud Control for this functionality. New/modified screens: **Devices** > **Device Management** > **Add** > **Device** > **Serial Number** See: Add a Device to the Management Center Using the Serial Number (Low-Touch Provisioning)
Interfaces			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Merged management and diagnostic interfaces.	7.4.0	7.4.0	**Upgrade impact. Merge interfaces after upgrade.** For new devices using 7.4 and later, you cannot use the legacy diagnostic interface. Only the merged management interface is available. If you upgraded to 7.4 or later and: • You did not have any configuration for the diagnostic interface, then the interfaces will merge automatically. • You have configuration for the diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate diagnostic interface. Note that support for the diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including Management) in the configuration. For platform settings, this means: • You can no longer enable HTTP, ICMP, or SMTP for diagnostic. • For SNMP, you can allow hosts on management instead of diagnostic. • For Syslog servers, you can reach them on management instead of diagnostic. • If Platform Settings for syslog servers or SNMP hosts specify the diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices. • DNS lookups no longer fall back to the management-only routing table if you do not specify interfaces. New/modified screens: **Devices** > **Device Management** > **Interfaces** New/modified commands: **show management-interface convergence** See: Interface Overview

Feature	Minimum Management Center	Minimum Threat Defense	Details
VXLAN VTEP IPv6 support.	7.4.0	7.4.0	You can now specify an IPv6 address for the VXLAN VTEP interface. IPv6 is not supported for the Firewall Threat Defense Virtual cluster control link or for Geneve encapsulation. New/modified screens: • **Devices** > **Device Management** > **Edit Device** > **VTEP** > **Add VTEP** • **Devices** > **Device Management** > **Edit Devices** > **Interfaces** > **Add Interfaces** > **VNI Interface** See: Regular Firewall Interfaces
Loopback interface support for BGP and management traffic.	7.4.0	7.4.0	You can now use loopback interfaces for AAA, BGP, DNS, HTTP, ICMP, IPsec flow offload, NetFlow, SNMP, SSH, and syslog. New/modified screens: **Devices** > **Device Management** > Edit device > **Interfaces** > **Add Interfaces** > **Loopback Interface** See: Regular Firewall Interfaces
Loopback and management type interface group objects.	7.4.0	7.4.0	You can create interface group objects with only management-only or loopback interfaces. You can use these groups for management features such as DNS servers, HTTP access, or SSH. Loopback groups are available for any feature that can utilize loopback interfaces. However, it's important to note that DNS does not support management interfaces. New/modified screens: **Objects** > **Object Management** > **Interface** > **Add** > **Interface Group** See: Object Management
High Availability/Scalability: Threat Defense			
Manage Firewall Threat Defense high availability pairs using a data interface.	7.4.0	7.4.0	Firewall Threat Defense high availability now supports using a regular data interface for communication with the Firewall Management Center. Previously, only standalone devices supported this feature. See: Device Management
SD-WAN			
WAN summary dashboard.	7.4.0	7.2.0	The WAN Summary dashboard provides a snapshot of your WAN devices and their interfaces. It provides insight into your WAN network and information about device health, interface connectivity, application throughput, and VPN connectivity. You can monitor the WAN links and take proactive and prompt recovery measures. New/modified screens: **Overview** > **WAN Summary** See: VPN Monitoring and Troubleshooting

Feature	Minimum Management Center	Minimum Threat Defense	Details
Policy-based routing using HTTP path monitoring.	7.4.0	7.2.0	Policy-based routing (PBR) can now use the performance metrics (RTT, jitter, packet-lost, and MOS) collected by path monitoring through HTTP client on the application domain rather than the metrics on a specific destination IP. HTTP-based application monitoring option is enabled by default for the interface. You can configure a PBR policy with match ACL having the monitored applications and interface ordering for path determination. New/modified screens: **Devices** > **Device Management** > Edit device > Edit interface > **Path Monitoring** > **Enable HTTP based Application Monitoring** check box. Platform restrictions: Not supported for clustered devices. See: Policy Based Routing
Policy-based routing with user identity and SGTs.	7.4.0	7.4.0	**Upgrade impact. Check SGT propagation before device upgrade.** You can now classify network traffic based on users, user groups, and SGTs in PBR policies. Select the identity and SGT objects while defining the extended ACLs for the PBR policies. Note that as a result of how this feature was implemented, Firewall Threat Defense can now add egress SGTs to traffic if the egress interface is configured to propagate SGTs. This can happen with ISE integration even if you do not configure policy-based routing. Starting with Version 7.4.0, the **Propagate Security Group Tag** option is disabled by default for new interfaces. But because upgrade respects your current settings, this option may be enabled for existing interfaces. **Important** If you have configured an ISE identity source, before you upgrade, check the **Propagate Security Group Tag** option on your devices' physical, redundant, and subinterfaces and disable it if necessary. If downstream devices are not configured to handle the tags, you could experience traffic loss. New/modified screens: **Objects** > **Object Management** > **Access List** > **Extended** > Add/Edit Extended Access List > Add/Edit Extended Access List Entry > **Users** and **Security Group Tag** See: Object Management
VPN			
IPsec flow offload on the VTI loopback interface for the Secure Firewall 4200.	7.4.0	7.4.0	On the Secure Firewall 4200, qualifying IPsec connections through the VTI loopback interface are offloaded by default. Previously, this feature was supported for physical interfaces on the Secure Firewall 3100. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command. Other requirements: FPGA firmware 6.2+ See: VPN Overview

Feature	Minimum Management Center	Minimum Threat Defense	Details
Crypto debugging enhancements for the Secure Firewall 4200.	7.4.0	7.4.0	We made the following enhancements to crypto debugging: • The crypto archive is now available in text and binary formats. • Additional SSL counters are available for debugging. • Remove stuck encrypt rules from the ASP table without rebooting the device. New/modified CLI commands: **show counters** See: Decryption Rules
VPN: Remote Access			
Customize Secure Client messages, icons, images, and connect/disconnect scripts.	7.4.0	7.1.0	You can now customize Secure Client and deploy these customizations to the VPN headend. The following are the supported Secure Client customizations: • GUI text and messages • Icons and images • Scripts • Binaries • Customized Installer Transforms • Localized Installer Transforms Firewall Threat Defense distributes these customizations to the endpoint when an end user connects from the Secure Client. New/modified screens: • **Objects** > **Object Management** > **VPN** > **Secure Client Customization** • **Devices** > **Remote Access** > Edit VPN policy > **Advanced** > **Secure Client Customization** See: Remote Access VPN
VPN: Site to Site			
Easily view IKE and IPsec session details for VPN nodes.	7.4.0	Any	You can view the IKE and IPsec session details of VPN nodes in a user-friendly format in the Site-to-Site VPN dashboard. New/modified screens: **Overview** > **Site to Site VPN** > Under the Tunnel Status widget, hover over a topology, click **View**, and then click the **CLI Details** tab. See: Site-to-Site VPNs

Feature	Minimum Management Center	Minimum Threat Defense	Details
Site-to-site VPN information in connection events.	7.4.0	7.4.0 with Snort 3	Connection events now contain three new fields: Encrypt Peer, Decrypt Peer, and VPN Action. For policy-based and route-based site-to-site VPN traffic, these fields indicate whether a connection was encrypted or decrypted (or both, for transiting connections), and who by. New/modified screens: **Analysis** > **Connections** > **Events** > **Table View of Events** See: VPN Monitoring and Troubleshooting
Easily exempt site-to-site VPN traffic from NAT translation.	7.4.0	Any	We now make it easier to exempt site-to-site VPN traffic from NAT translation. New/modified screens: • Enable NAT exemptions for an endpoint: **Devices** > **VPN** > **Site To Site** > **Add/Edit Site to Site VPN** > **Add/Edit Endpoint** > **Exempt VPN traffic from network address translation** • View NAT exempt rules for devices that do not have a NAT policy: **Devices** > **NAT** > **NAT Exemptions** • View NAT exempt rules for a single device: **Devices** > **NAT** > **Threat Defense NAT Policy** > **NAT Exemptions** See: Network Address Translation
Routing			
Configure graceful restart for BGP on IPv6 networks.	7.4.0	7.3.0	You can now configure BGP graceful restart for IPv6 networks on managed devices version 7.3 and later. New/modified screens: **Devices** > **Device Management** > Edit device > **Routing** > **BGP** > **IPv6** > **Neighbor** > Add/Edit Neighbor. See: BGP
Virtual routing with dynamic VTI.	7.4.0	7.4.0	You can now configure a virtual router with a dynamic VTI for a route-based site-to-site VPN. New/modified screens: **Devices** > **Device management** > **Edit Device** > **Routing** > **Virtual Router Properties** > **Dynamic VTI interfaces under Available Interfaces** Platform restrictions: Supported only on native mode standalone or high availability devices. Not supported for container instances or clustered devices. See: Virtual Routers
Access Control: Threat Detection and Application Identification			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Clientless zero-trust access.	7.4.0	7.4.0 with Snort 3	Zero Trust Access allows you to authenticate and authorize access to protected web based resources, applications, or data from inside (on-premises) or outside (remote) the network using an external SAML Identity Provider (IdP) policy. The configuration consists of a Zero Trust Application Policy (ZTAP), Application Group, and Applications. New/modified screens: • **Policies** > **Zero Trust Application** • **Analysis** > **Connections** > **Events** • **Overview** > **Dashboard** > **Zero Trust** New/modified CLI commands: • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics** See: Zero Trust Access
Encrypted visibility engine (EVE) enhancements.	7.4.0	7.4.0 with Snort 3	You can now use EVE to: • Block malicious communications in encrypted traffic based on threat score. • Determine client applications based on EVE-detected processes. • Reassemble fragmented Client Hello packets for detection purposes. New/modified screens: Use the access control policy's advanced settings to enable EVE and configure these settings. See: *Custom Snort 3 Intrusion Policies for Access Control*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Exempt specific networks and ports from bypassing or throttling elephant flows.	7.4.0	7.4.0 with Snort 3	You can now exempt specific networks and ports from bypassing or throttling elephant flows. New/modified screens: • When you configure elephant flow detection in the access control policy's advanced settings, if you enable the **Elephant Flow Remediation** option, you can now click **Add Rule** and specify traffic that you want to exempt from bypass or throttling. • When the system detects an elephant flow that is exempted from bypass or throttling, it generates a mid-flow connection event with the reason **Elephant Flow Exempted**. Platform restrictions: Not supported on the Firepower 2100 series. See: *Custom Snort 3 Intrusion Policies for Access Control*
First-packet application identification using custom application detectors.	7.4.0	7.4.0 with Snort 3	A new Lua detector API is now introduced, which maps the IP address, port, and protocol on the very first packet of a TCP session to application protocol (service AppID), client application (client AppID), and web application (payload AppID). This new Lua API *addHostFirstPktApp* is used for performance improvements, reinspection, and early detection of attacks in the traffic. To use this feature, you must upload the Lua detector by specifying the detection criteria in advanced detectors in your custom application detector. See: Application Detection
Sensitive data detection and masking.	7.4.0	7.4.0 with Snort 3	**Upgrade impact. New rules in default policies take effect.** Sensitive data such as social security numbers, credit card numbers, emails, and so on may be leaked onto the internet, intentionally or accidentally. Sensitive data detection is used to detect and generate events on possible sensitive data leakage and generates events only if there is a transfer of significant amount of Personally Identifiable Information (PII) data. Sensitive data detection can mask PII in the output of events, using built-in patterns. Disabling data masking is not supported. See: Custom Rules in Snort 3
Improved JavaScript inspection.	7.4.0	7.4.0 with Snort 3	We improved JavaScript inspection, which is done by normalizing the JavaScript and matching rules against the normalized content. See: HTTP Inspect Inspector and Cisco Secure Firewall Management Center Snort 3 Configuration Guide

Feature	Minimum Management Center	Minimum Threat Defense	Details
MITRE information in file and malware events.	7.4.0	7.4.0	The system now includes MITRE information (from local malware analysis) in file and malware events. Previously, this information was only available for intrusion events. You can view MITRE information in both the classic and unified events views. Note that the MITRE column is hidden by default in both event views. See: Network Malware Protection and File Policies and File/Malware Events and Network File Trajectory
Access Control: Identity			
Cisco Secure Dynamic Attributes Connector on the Firewall Management Center.	7.4.0	Any	You can now configure the Cisco Secure Dynamic Attributes Connector on the Firewall Management Center. Previously, it was only available as a standalone application. See: Cisco Secure Dynamic Attributes Connector
Microsoft Azure AD as a user identity source.	7.4.0	7.4.0	You can use a Microsoft Azure Active Directory (Azure AD) realm with ISE to authenticate users and get user sessions for user control. New/modified screens: • **Integration** > **Other Integrations** > **Realms** > **Add Realm** > **Azure AD** • **Integration** > **Other Integrations** > **Realms** > Actions, such as downloading users, copying, editing, and deleting Supported ISE versions: 3.0 patch 5+, 3.1 (any patch level), 3.2 (any patch level) See: Realms
Event Logging and Analysis			
Configure Firewall Threat Defense devices as NetFlow exporters from the Firewall Management Center web interface.	7.4.0	Any	**Upgrade impact. Redo FlexConfigs after upgrade.** NetFlow is a Cisco application that provides statistics on packets flows. You can now use the Firewall Management Center web interface to configure Firewall Threat Defense devices as NetFlow exporters. If you have an existing NetFlow FlexConfig and redo your configurations in the web interface, you cannot deploy until you remove the deprecated FlexConfigs. New/modified screens: **Devices** > **Platform Settings** > **Threat Defense Settings Policy** > **NetFlow** See: Platform Settings

Feature	Minimum Management Center	Minimum Threat Defense	Details
More information about "unknown" SSL actions in logged encrypted connections.	7.4.0	7.4.0	Serviceability improvements to the event reporting and decryption rule matching. • New **SSL Status** to indicate if the SSL handshake is not complete for an encrypted connection. The **SSL Status** column of the connection event displays “Unknown (Incomplete Handshake)” when the SSL handshake of the logged connection is not complete. • Subject Alternative Names (SANs) for certificates are now used when matching Certificate Authority (CA) names for improved decryption rule matching. New/modified screens: • **Analysis** > **Connections** > **Events** > **SSL Status** • **Analysis** > **Connections** > **Security-Related Events** > **SSL Status** See: Connection and Security-Related Connection Events
Health Monitoring			
Stream telemetry to an external server using OpenConfig.	7.4.0	7.4.0	You can now send metrics and health monitoring information from your Firewall Threat Defense devices to an external server (gNMI collector) using OpenConfig. You can configure either Firewall Threat Defense or the collector to initiate the connection, which is encrypted by TLS. New/modified screens: **System** (⚙) > **Health** > **Policy** > **Firewall Threat Defense Policies** > **Settings** > **OpenConfig Streaming Telemetry** See: Health
New asp drop metrics.	7.4.0	7.4.0	You can add over 600 new asp (accelerated security path) drop metrics to a new or existing device health dashboard. Make sure you choose the **ASP Drops** metric group. New/modified screens: **System** (⚙) > **Health** > **Monitor** > **Device** See: show asp drop Command Usage
Administration			
Send detailed Firewall Management Center audit logs to syslog.	7.4.0	Any	You can stream configuration changes as part of audit log data to syslog by specifying the configuration data format and the hosts. The Firewall Management Center supports backup and restore of the audit configuration log. New/modified screens: **System** (⚙) > **Configuration** > **Audit Log** > **Send Configuration Changes** See: System Configuration

Feature	Minimum Management Center	Minimum Threat Defense	Details
Granular permissions for modifying access control policies and rules.	7.4.0	Any	You can define custom user roles to differentiate between the intrusion configuration in access control policies and rules and the rest of the access control policy and rules. Using these permissions, you can separate the responsibilities of your network administration team and your intrusion administration teams. When defining user roles, you can select the **Policies** > **Access Control** > **Access Control Policy** > **Modify Access Control Policy** > **Modify Threat Configuration** option to allow the selection of intrusion policy, variable set, and file policy in a rule, the configuration of the advanced options for Network Analysis and Intrusion Policies, the configuration of the Security Intelligence policy for the access control policy, and intrusion actions in the policy default action. You can use the **Modify Remaining Access Control Policy Configuration** to control the ability to edit all other aspects of the policy. The existing pre-defined user roles that included the Modify Access Control Policy permission continue to support all sub-permissions; you need to create your own custom roles if you want to apply granular permissions. See: Users
Support for IPv6 URLs when checking certificate revocation.	7.4.0	7.4.0	Previously, Firewall Threat Defense supported only IPv4 OCSP URLs. Now, Firewall Threat Defense supports both IPv4 and IPv6 OCSP URLs. See: System Configuration and Object Management
Default NTP server updated.	7.4.0	Any	The default NTP server for new Firewall Management Center deployments changed from sourcefire.pool.ntp.org to time.cisco.com. We recommend you use the Firewall Management Center to serve time to its own devices. You can update the Firewall Management Center's NTP server on **System** (⚙) > **Configuration** > **Time Synchronization**. See: Security, Internet Access, and Communication Ports
Usability, Performance, and Troubleshooting			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Usability enhancements.	7.4.0	Any	You can now: • Manage Smart Licensing for Firewall Threat Defense clusters from **System** (⚙) > **Smart Licenses**. Previously, you had to use the Device Management page. See: Licensing • Download a report of Message Center notifications. In the Message Center, click the new **Download Report** icon, next to the **Show Notifications** slider. See: Troubleshooting • Download a report of all registered devices. On **Devices** > **Device Management**, click the new **Download Device List Report** link, at the top right of the page. See: Device Management • Clone network and port objects. In the object manager (**Objects** > **Object Management**), click the new **Clone** icon next to a port or network object. You can then change the new object's properties and save it using a new name. See: Object Management • Easily create custom health monitoring dashboards, and easily edit existing dashboards. See: Health
Specify the direction of traffic to be captured with packet capture for the Secure Firewall 4200.	7.4.0	7.4.0	On the Secure Firewall 4200, you can use a new **direction** keyword with the **capture** command. New/modified CLI commands: **capture***capture_name* **switch interface** *interface_name* [**direction** { **both** | **egress** | **ingress** }] See: *Cisco Secure Firewall Threat Defense Command Reference*

Feature	Minimum Management Center	Minimum Threat Defense	Details
Snort 3 restarts when it becomes unresponsive, which can trigger HA failover.	7.4.0	7.4.0 with Snort 3	To improve continuity of operations, an unresponsive Snort can now trigger high availability failover. This happens because Snort 3 now restarts if the process becomes unresponsive. Restarting the Snort process briefly interrupts traffic flow and inspection on the device, and in high availability deployments can trigger failover. (In a standalone deployment, interface configurations determine whether traffic drops or passes without inspection during the interruption.) This feature is enabled by default. You can use the CLI to disable it, or configure the time or number of unresponsive threads before Snort restarts. New/modified CLI commands: **configure snort3-watchdog** See: *Cisco Secure Firewall Threat Defense Command Reference*
Deprecated Features			
Deprecated: NetFlow with FlexConfig.	7.4.0	Any	You can now configure Firewall Threat Defense devices as NetFlow exporters from the Firewall Management Center web interface. If you do this, you cannot deploy until you remove any deprecated FlexConfigs. See: Platform Settings

Firewall Management Center Features in Version 7.3.1

Table 52: Firewall 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: • Smaller VDB for lower memory Snort 2 devices. (7.0.6)

Table 53: Firewall 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.

Firewall Management Center Features in Version 7.3.0

Table 54: Firewall 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	Version 7.3.0 also has: • 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			
Firewall Management Center Virtual 300 for KVM.	7.3.0	Any	We introduced the FMCv300 for KVM. The FMCv300 can manage up to 300 devices. High availability is supported.
Network modules for the Firepower 4100.	7.3.0	7.3.0	We introduced these network modules for the Firepower 4100: • 2-port 100G network module (FPR4K-NM-2X100G) Supported platforms: Firepower 4112, 4115, 4125, 4145

Feature	Minimum Management Center	Minimum Threat Defense	Details
New compute shapes for Firewall Threat Defense Virtual and Firewall Management Center Virtual for OCI.	7.3.0	7.3.0	Firewall Threat Defense Virtual for OCI adds support for the following compute shapes: • Intel VM.DenseIO2.8 • Intel VM.StandardB1.4 • Intel VM.StandardB1.8 • Intel VM.Standard1.4 • Intel VM.Standard1.8 • Intel VM.Standard3.Flex • Intel VM.Optimized3.Flex • AMD VM.Standard.E4.Flex Firewall Management Center Virtual for OCI adds support for the following compute shapes: • Intel VM.StandardB1.4 • Intel VM.Standard3.Flex • Intel VM.Optimized3.Flex • AMD VM.Standard.E4.Flex Note that the VM.Standard2.4 and VM.Standard2.8 compute shapes reached end of orderability in February 2022. If you are deploying Version 7.3+, we recommend one of the above compute shapes. For information on compatible compute shapes, see the Secure Firewall Threat Defense Virtual getting started guides.
Interfaces			
IPv6 support for virtual appliances.	7.3.0	7.3.0	Firewall Threat Defense Virtual and Firewall Management Center Virtual now support IPv6 in the following environments: • AWS • Azure • OCI • KVM • VMware For more information, see Secure Firewall Threat Defense Virtual getting started guides and *Cisco Secure Firewall Management Center Virtual Getting Started Guide*.

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

Feature	Minimum Management Center	Minimum Threat Defense	Details
IPv6 DHCP.	7.3.0	7.3.0	We now support the following features for IPv6 addressing: • DHCPv6 Address client: 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. New/modified screens: • **Devices** > **Device Management** > **Device** > **Interfaces** > **Interface** > **IPv6** > **DHCP** • **Objects** > **Object Management** > **DHCP IPv6 Pool** New/modified CLI commands: **show bgp ipv6 unicast**, **show ipv6 dhcp**, **show ipv6 general-prefix** For more information, see Configure the IPv6 Prefix Delegation Client, BGP, and Configure the DHCPv6 Stateless Server in the device configuration guide.
Paired proxy VXLAN for the Firewall Threat Defense Virtual for the Azure Gateway Load Balancer.	7.3.0	7.3.0	You can configure a paired proxy mode VXLAN interface for 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. New/modified screens: **Devices** > **Device Management** > **Device** > **Interfaces** > **Add Interfaces** > **VNI Interface** For more information, see Configure VXLAN Interfaces in the device configuration guide.
High Availability/Scalability: Firewall Threat Defense			
Clustering for Firewall Threat Defense Virtual for Azure.	7.3.0	7.3.0	You can now configure clustering for up to 16 nodes with Firewall Threat Defense Virtual for Azure. New/modified screens: **Devices** > **Device Management** For more information, see Clustering for Threat Defense Virtual in a Public Cloud in the device configuration guide.

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 Secure Firewall Threat Defense Virtual getting started guides.
Back up and restore device clusters.	7.3.0	Any	You can now use the Firewall Management Center to back up device clusters, except in the public cloud. To restore, use the device CLI. New/modified screens: **System** > **Tools** > **Backup/Restore** > **Managed Device Backup** New/modified commands: **restore remote-manager-backup** For more information, see Backup/Restore in the administration guide.
High Availability: Firewall Management Center			
High availability for Firewall Management Center Virtual for KVM.	7.3.0	Any	We now support high availability for Firewall Management Center Virtual for KVM. 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. Platform restrictions: Not supported with FMCv2 For more information, see the *Cisco Secure Firewall Management Center Virtual Getting Started Guide*, as well as High Availability in the administration guide.
VPN: Remote Access			
RA VPN dashboard.	7.3.0	Any	We introduced a remote access VPN (RA VPN) dashboard that allows you to monitor real-time data from active RA VPN sessions on the devices. So that you can quickly determine problems related to user sessions and mitigate the problems for your network and users, the dashboard provides: • Visualization of active user sessions based on their location. • Detailed information about the active user sessions. • Mitigation of user session problems by terminating sessions, if required. • Distribution of active user sessions per device, encryption type, Secure Client version, operating system, and connection profile. • Device identity certificate expiration details of the devices. New/modified screens: **Overview** > **Dashboards** > **Remote Access VPN** For more information, see Dashboards in the administration guide.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Encrypt RA VPN connections with TLS 1.3.	7.3.0	7.3.0	You can now use TLS 1.3 to encrypt RA VPN connections with the following ciphers: • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 Use the Firewall Threat Defense platform settings to set the TLS version: **Devices** > **Platform Settings** > **Add/Edit Threat Defense Settings Policy** > **SSL** > **TLS Version**. This feature requires Cisco Secure Client, Release 5 (formerly known as the AnyConnect Secure Mobility Client). For more information, see Configure SSL Settings in the device configuration guide.
VPN: Site to Site			
Packet tracer in the site-to-site VPN dashboard.	7.3.0	Any	We added packet tracer capabilities to the site-to-site VPN dashboard, to help you troubleshoot VPN tunnels between devices. Open the dashboard by choosing **Overview** > **Dashboards** > **Site to Site VPN**. Then, click **View** ( ) next to the tunnel you want to investigate, and **Packet Tracer** in the side pane that appears. For more information, see Monitoring the Site-to-Site VPNs in the device configuration guide.
Support for dynamic VTIs with site-to-site VPN.	7.3.0	7.3.0	We now support dynamic virtual tunnel interfaces (VTI) when you configure a route-based site-to-site VPN in a hub and spoke topology. Previously, you could use only a static VTI. This makes it easier to configure large hub and spoke deployments. A single dynamic VTI can replace several static VTI configurations on the hub. And, you can add new spokes to a hub without changing the hub configuration. New/modified screens: We updated the options when configuring hub-node endpoints for a route-based hub-and-spoke site-to-site VPN topology. For more information, see Configure Endpoints for a Hub and Spoke Topology in the device configuration guide.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Improved Umbrella SIG integration.	7.3.0	7.3.0	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. To configure and deploy these tunnels, create a SASE topology, a new type of static VTI-based site-to-site VPN topology: **Devices** > **VPN** > **Site To Site** > **SASE Topology**. For more information, see Deploy a SASE Tunnel on Umbrella in the device configuration guide.
Routing			
Configure BFD for BGP from the Firewall Management Center web interface.	7.3.0	Any	**Upgrade impact. Redo related FlexConfigs after upgrade.** 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. New/modified screens: • **Devices** > **Device Management** > **Device** > **Routing** > **BFD** • **Objects** > **Object Management** > **BFD Template** • When configuring BGP neighbor settings, we replaced the **BFD Failover** check box with a menu where you choose the BFD type: single hop, multi hop, auto detect, or none (disabled). For upgraded 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. For more information, see Bidirectional Forwarding Detection Routing in the device configuration guide.
Support for IPv4 and IPv6 OSPF routing for VTIs.	7.3.0	7.3.0	We now support IPv4 and IPv6 OSPF routing for VTI interfaces. New/modified pages: You can add VTI interfaces to an OSPF routing process on **Devices** > **Device Management** > **Device** > **Routing** > **OSPF/OSFPv3**. For more information, see OSPF and Additional Configurations for VTI in the device configuration guide.
Support for IPv4 EIGRP routing for VTIs.	7.3.0	7.3.0	We now support IPv4 EIGRP routing for VTI interfaces. New/modified screens: You can define a VTI as the static neighbor for an EIGRP routing process, configure a VTI's interface-specific EIGRP routing properties. and advertise a VTI's summary address on **Devices** > **Device Management** > **Device** > **Routing** > **EIGRP**. For more information, see EIGRP and Additional Configurations for VTI in the device configuration guide.

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	You can now configure multiple next-hops while configuring policy-based routing forwarding actions. When traffic matches the criteria for the route, the system attempts to forward traffic to the IP addresses in the order you specify, until it succeeds. New/modified screens: We added several options when you select **IP Address** from the **Send To** menu on **Devices** > **Device Management** > **Device** > **Routing** > **Policy Based Routing** > **Add Policy Based Route** > **Add Match Criteria and Egress Interface**. For more information, see Configure Policy-Based Routing Policy in the device configuration guide.
Upgrade			
Choose and direct-download upgrade packages to the Firewall Management Center.	7.3.x only	Any	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**. Version restrictions: this feature is replaced by an improved package management system in Version 7.2.6/7.4.1. See: Download Upgrade Packages with the Management Center
Upload upgrade packages to the Firewall Management Center from the Firewall Threat Defense wizard.	7.3.x only	Any	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**. Version restrictions: this feature is replaced by an improved package management system in Version 7.2.6/7.4.1. See: Upgrade Threat Defense
Auto-upgrade to Snort 3 after successful Firewall Threat Defense upgrade is no longer optional.	7.3.0	Any	**Upgrade impact. All eligible devices upgrade to Snort 3 when you deploy.** When you upgrade Firewall Threat Defense to Version 7.3+, you can no longer disable the **Upgrade Snort 2 to Snort 3** option. After the software upgrade, all eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. Although you can switch individual devices back, Snort 2 is not supported on Firewall Threat Defense 7.7+. You should stop using it now. 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 *Custom Snort 3 Intrusion Policies for Access Control* for your version.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Combined upgrade and install package for Secure Firewall 3100.	7.3.0	7.3.0	**Reimage Impact.** In Version 7.3, we combined the Firewall Threat Defense install and upgrade package for the Secure Firewall 3100, as follows: • Version 7.1–7.2 install package: cisco-ftd-fp3k.*version*.SPA • Version 7.1–7.2 upgrade package: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • Version 7.3+ combined package: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar Although you can upgrade 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. To get to Firewall Threat Defense Version 7.3+, your options are: • 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 *Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100* and then *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100* in the *Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide*. • Reimage from ASA 9.17 or 9.18 — upgrade to ASA 9.19+ first, then reimage to Firewall Threat Defense Version 7.3+. See the *Cisco Secure Firewall ASA Upgrade Guide* and then *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100* in the *Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide*. • Reimage from Firewall Threat Defense Version 7.3+ — use the normal reimage process. See *Reimage the System with a New Software Version* in the *Cisco FXOS Troubleshooting Guide for the Firewall 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	We renamed the SSL policy to the decryption policy. We also added a policy wizard that makes it easier to create and configure decryption policies, including creating initial rules and certificates for inbound and outbound traffic. New/modified screens: • Add or edit a decryption policy: **Policies** > **Access Control** > **Decryption**. • Use a decryption policy: **Decryption Policy Settings** in an access control policy's advanced settings. For more information, see Decryption Policies in the device configuration guide.
Improvements to TLS server identity discovery with Snort 3 devices.	7.3.0	7.3.0	We now support improved performance and inspection with the TLS server identity discovery feature, which allows you to handle traffic encrypted with TLS 1.3 with information from the server certificate. Although we recommend you leave it enabled, you can disable this feature using the new **Enable adaptive TLS server identity probe** option in the decryption policy's advanced settings. For more information, see TLS 1.3 Decryption Best Practices in the device configuration guide.

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

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

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

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

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

Feature	Minimum Management Center	Minimum Threat Defense	Details
Automatic VDB downloads.	7.3.0	Any	The initial setup on the 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. New/modified screens: The **Vulnerability Database** check box is now enabled by default in the system-created **Weekly Software Download** scheduled task. For more information, see Vulnerability Database Update Automation in the administration guide.
Install any VDB.	7.3.0	Any	Starting with VDB 357, you can now install any VDB as far back as the baseline VDB for that Firewall Management Center. After you update the VDB, deploy configuration changes. If you based configurations on vulnerabilities, application detectors, or fingerprints that are no longer available, examine those configurations to make sure you are handling traffic as expected. Also, keep in mind a scheduled task to update the VDB can undo a rollback. To avoid this, change the scheduled task or delete any newer VDB packages. New/modified screens: On **System**(⚙) > **Updates** > **Product Updates** > **Available Updates**, if you upload an older VDB, a new **Rollback** icon appears instead of the **Install** icon. For more information, see Update the Vulnerability Database in the administration guide.
Usability, Performance, and Troubleshooting			
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	You can adjust the percentage of system cores assigned to the data plane and Snort to adjust system performance. The adjustment is based on your relative use of VPN and intrusion policies. If you use both, leave the core allocation to the default values. If you use the system primarily for VPN (without applying intrusion policies), or as an IPS (with no VPN configuration), you can skew the core allocation to the data plane (for VPN) or Snort (for intrusion inspection). We added the **Performance Profile** page to the platform settings policy. For more information, see Configure the Performance Profile in the device configuration guide.
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: Scheduled software upgrades.	7.3.0	Any	**Upgrade impact. Scheduled software upgrade tasks stop working.** The **Download Latest Update**, **Push Latest Update**, and **Install Latest Update** scheduled tasks are no longer supported for software updates, although the web interface allows configuration. (Exception: Version 7.3.1.2) You can still use the **Download Latest Update** and **Install Latest Update** tasks to schedule VDB updates. See: Scheduling
Deprecated: YouTube EDU content restriction for Snort 2 devices.	7.3.0	Any	You can no longer enable YouTube EDU content restriction in new or existing access control rules. Your existing YouTube EDU rules will keep working, and you can edit those rules to disable YouTube EDU. Note that this is a Snort 2 feature that is not available for Snort 3. You should redo your configurations after upgrade.
Deprecated: Cluster health monitor settings with FlexConfig.	7.3.0	Any	You can now edit cluster health monitor settings from the 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. You should redo your configurations after upgrade.
Deprecated: BFD for BGP with FlexConfig.	7.3.0	Any	You can now configure bidirectional forwarding detection (BFD) for BGP routing from the Firewall Management Center web interface. If you do this, you cannot deploy until you remove any deprecated FlexConfigs. You should redo your configurations after upgrade.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: ECMP zones with FlexConfig.	7.3.0	Any	You can now easily migrate EMCP zone configurations from FlexConfig to web interface management. After you migrate, you cannot deploy until you remove any deprecated FlexConfigs. You should redo your configurations after upgrade.
Deprecated: VXLAN interfaces with FlexConfig.	7.3.0	Any	You can now easily migrate VXLAN interface configurations from FlexConfig to web interface management. After you migrate, you cannot deploy until you remove any deprecated FlexConfigs.

Firewall Management Center Features in Version 7.2.12

There are no new features in this release.

Firewall Management Center Features in Version 7.2.11

There are no new features in this release.

Firewall Management Center Features in Version 7.2.10

Table 55: Firewall Management Center Features in Version 7.2.10

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.2.10 also has: • New Cisco AMP cloud connection method. Upgrade impact. (7.0.7) • Deprecated Cisco AMP Cloud connection backups. (7.0.7) • Require the Message-Authenticator attribute in all RADIUS responses. Upgrade impact. (7.0.7) • Updated internet access requirements for Smart Licensing. Upgrade impact. (7.0.8)
Upgrade			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firewall Threat Defense and chassis upgrade wizards optimized for lower resolution screens.	7.2.10 7.4.3 7.6.0	Any	We optimized the Firewall Threat Defense and chassis upgrade wizards for lower resolution screens (and smaller browser windows). Text appears smaller and certain screen elements are hidden. If you change your resolution or window size mid-session, you may need to refresh the page for the web interface to adjust. Note that the minimum screen resolution to use the Firewall Management Center is 1280 x 720. New/modified screens: • **Devices** > **Threat Defense Upgrade** • **Devices** > **Chassis Upgrade**
Performance			
High-bandwidth encrypted application traffic bypasses unnecessary intrusion inspection.	7.2.10 7.4.3 7.6.1 7.7.0	7.2.10 with Snort 3 7.4.3 with Snort 3 7.6.1 with Snort 3 7.7.0	Specific high-bandwidth encrypted application traffic now bypasses unncessary intrusion inspection even if the connection matches an Allow rule. Intrusion rule (LSP) and vulnerability database (VDB) updates can change the applications bypassed but right now they are: AnyConnect, IPsec, iCloud Private Relay, QUIC (including HTTP/3), Webex Media, Secure RTCP.

Firewall Management Center Features in Version 7.2.9

Table 56: Firewall Management Center Features in Version 7.2.9

Feature	Minimum Mnagement Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.2.9 also has: • Security Cloud Control regions: India and Australia. (7.0.7)
Public and Private Cloud			
VMware vSphere/VMware ESXi 8.0 support.	7.2.9 7.4.2 7.6.0	7.2.9 7.4.2 7.6.0	You can now deploy Secure Firewall Threat Defense Virtual and Firewall Management Center Virtual on VMware vSphere/VMware ESXi 8.0. See: Secure Firewall Threat Defense Virtual getting started guides
Access Control: Threat Detection and Application Identification			

Feature	Minimum Mnagement Center	Minimum Threat Defense	Details
Asymmetric traffic handling.	7.2.9 7.4.2 7.6.0	7.2.9 with Snort 3 7.4.2 with Snort 3 7.6.0 with Snort 3	**Upgrade impact. Qualifying connections are now inspected and handled.** In asymmetric routing deployments, Firewall Threat Defense now inspects the side of the connection it sees. No additional configurations are required.

Firewall Management Center Features in Version 7.2.8

Table 57: Firewall Management Center Features in Version 7.2.8

Feature	Minimum Management Center	Minimum Threat Defense	Details
Platform			
Firewall Threat Defense Virtual for Megaport.	7.2.8 7.3.0	7.2.8 7.3.0	We introduced Firewall Threat Defense Virtual for Megaport (Megaport Virtual Edge). High availability is supported. Clustering is not supported. Version restrictions: Initially, you may not be able to freshly deploy Versions 7.3.x or 7.4.x. Instead, deploy Version 7.2.8–7.2.x and upgrade. See: Secure Firewall Threat Defense Virtual getting started guides

Firewall Management Center Features in Version 7.2.7

There are no new features in this release.

Firewall Management Center Features in Version 7.2.6

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

Table 58: Firewall Management Center Features in Version 7.2.6

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.2.6 also has: • Updated web analytics provider. Upgrade impact. (7.0.6)
Interfaces			
Configure DHCP relay trusted interfaces from the Firewall Management Center web interface.	7.2.6 7.4.1	Any	**Upgrade impact. Redo any related FlexConfigs after upgrade.** You can now use the Firewall Management Center web interface to configure interfaces as trusted interfaces to preserve DHCP Option 82. If you do this, these settings override any existing FlexConfigs, although you should remove them. DHCP Option 82 is used by downstream switches and routers for DHCP snooping and IP Source Guard. Normally, if the Firewall Threat Defense DHCP relay agent receives a DHCP packet with Option 82 already set, but the giaddr field (which specifies the DHCP relay agent address that is set by the relay agent before it forwards the packet to the server) is set to 0, then Firewall Threat Defense will drop that packet by default. You can preserve Option 82 and forward the packet by identifying an interface as a trusted interface. New/modified screens: **Devices** > **Device Management** > **Add/Edit Device** > **DHCP** > **DHCP Relay** See: Configure the DHCP Relay Agent
NAT			
Create network groups while editing NAT rules.	7.2.6 7.4.1	Any	You can now create network groups in addition to network objects while editing a NAT rule. See: Customizing NAT Rules for Multiple Devices
High Availability/Scalability: Threat Defense			
Reduced "false failovers" for Firewall Threat Defense high availability.	7.2.6 7.4.0	7.2.6 7.4.0	See: Heartbeat Module Redundancy
High Availability: Management Center			
Single backup file for high availability Firewall Management Centers.	7.2.6 7.4.1	Any	When performing a configuration-only backup of the active Firewall Management Center in a high availability pair, the system now creates a single backup file which you can use to restore either unit. See: Unified Backup of Management Centers in High Availability
Event Logging and Analysis			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Open the packet tracer from the unified event viewer.	7.2.6 7.4.1	Any	You can now open the packet tracer from the unified event view (**Analysis** > **Unified Events**). Click the ellipsis icon (**...**) next to the desired event and click **Open in Packet Tracer**. Version restrictions: In Version 7.2.x, use the Expand icon (>) icon instead of the ellipsis icon. See: Working with the Unified Event Viewer
Health Monitoring			
Health alerts for excessive disk space used by deployment history (rollback) files.	7.2.6 7.4.1	Any	The Disk Usage health module now alerts if deployment history (rollback) files are using excessive disk space on the Firewall Management Center. Deploy the Firewall Management Center health policy after upgrade. See: Disk Usage for Device Configuration History Files Health Alert
Health alerts for NTP sync issues.	7.2.6 7.4.1	Any	A new Time Server Status health module reports issues with NTP synchronization. Deploy the Firewall Management Center health policy after upgrade. See: Time Synchronization and Health Modules
Deployment and Policy Management			
View and generate reports on configuration changes since your last deployment.	7.2.6 7.4.1	Any	You can generate, view, and download the reports as a zip file on configuration changes since your last deployment: • A *policy changes* report for each device that previews the additions, changes, or deletions in the policy, or the objects that are to be deployed on the device. • A *consolidated* report that categorizes each device based on the status of policy changes report generation. This is especially useful after you upgrade either the Firewall Management Center or Firewall Threat Defense, so that you can see the changes made by the upgrade before you deploy. New/modified screens: **Deploy** > **Advanced Deploy**. See: Download Policy Changes Report for Multiple Devices
Set the number of deployment history files to retain for device rollback.	7.2.6 7.4.1	Any	You can now set the number of deployment history files to retain for device rollback, up to ten (the default). This can help you save disk space on the Firewall Management Center. New/modified screens: **Deploy** > **Deployment History** > **Deployment Setting** > **Configuration Version Setting** See: Set the Number of Configuration Versions
Upgrade			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Improved upgrade starting page and package management.	7.2.6 7.4.1	Any	A new upgrade page makes it easier to choose, download, manage, and apply upgrades to your entire deployment. This includes the Firewall Management Center, Firewall Threat Defense, and any older NGIPSv/ASA FirePOWER devices. The page lists all upgrade packages that apply to your current deployment, with suggested releases specially marked. You can easily choose and direct-download packages from Cisco, as well as manually upload and delete packages. Internet access is required to retrieve the list/direct download upgrade packages. Otherwise, you are limited to manual management. Patches are not listed unless you have at least one appliance at the appropriate maintenance release (or you manually uploaded the patch). You must manually upload hotfixes. New/modified screens: • **System**(⚙) > **Product Upgrades** is now where you upgrade the Firewall Management Center and all managed devices, as well as manage upgrade packages. • **System**(⚙) > **Content Updates** is now where you update intrusion rules, the VDB, and the GeoDB. • **Devices** > **Threat Defense Upgrade** takes you directly to the Firewall Threat Defense upgrade wizard. • **System**(⚙) > **Users** > **User Role** > **Create User Role** > **Menu-Based Permissions** allows you to grant access to **Content Updates** (VDB, GeoDB, intrusion rules) without allowing access to **Product Upgrades** (system software). Deprecated screens/options: • **System**(⚙) > **Updates** is deprecated. All Firewall Threat Defense upgrades now use the wizard. • The **Add Upgrade Package** button on the Firewall Threat Defense upgrade wizard has been replaced by a **Manage Upgrade Packages** link to the new upgrade page. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
Enable revert from the Firewall Threat Defense upgrade wizard.	7.2.6 7.4.1	Any, if upgrading to 7.1+	You can now enable revert from the Firewall Threat Defense upgrade wizard. Version restrictions: You must be upgrading Firewall Threat Defense to Version 7.1+. Not supported with Firewall Management Center Version 7.3.x or 7.4.0. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center

Feature	Minimum Management Center	Minimum Threat Defense	Details
Select devices to upgrade from the Firewall Threat Defense upgrade wizard.	7.2.6 7.3.0	Any	Use the wizard to select devices to upgrade. You can now use the Firewall Threat Defense upgrade wizard to select or refine the devices to upgrade. On the wizard, you can toggle the view between selected devices, remaining upgrade candidates, ineligible devices (with reasons why), devices that need the upgrade package, and so on. Previously, you could only use the Device Management page and the process was much less flexible. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
View detailed upgrade status from the Firewall Threat Defense upgrade wizard.	7.2.6 7.4.1	Any	The final page of the Firewall Threat Defense upgrade wizard now allows you to monitor upgrade progress. This is in addition to the existing monitoring capability on the Upgrade tab on the Device Management page, and on the Message Center. Note that as long as you have not started a new upgrade flow, **Devices** > **Threat Defense Upgrade** brings you back to this final wizard page, where you can view the detailed status for the current (or most recently complete) device upgrade. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
Unattended Firewall Threat Defense upgrades.	7.2.6 7.3.0	Any	The Firewall Threat Defense upgrade wizard now supports unattended upgrades, using a new **Unattended Mode** menu. You just need to select the target version and the devices you want to upgrade, specify a few upgrade options, and step away. You can even log out or close the browser. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
Simultaneous Firewall Threat Defense upgrade workflows by different users.	7.2.6 7.3.0	Any	We now allow simultaneous upgrade workflows by different users, as long as you are upgrading different devices. The system prevents you from upgrading devices already in someone else's workflow. Previously, only one upgrade workflow was allowed at a time across all users. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
Skip pre-upgrade troubleshoot generation for Firewall Threat Defense.	7.2.6 7.3.0	Any	You can now skip the automatic generating of troubleshooting files before major and maintenance upgrades by disabling the new **Generate troubleshooting files before upgrade begins** option. This saves time and disk space. To manually generate troubleshooting files for a Firewall Threat Defense device, choose **System**(⚙) > **Health** > **Monitor**, click the device in the left panel, then **View System & Troubleshoot Details**, then **Generate Troubleshooting Files**. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center

Feature	Minimum Management Center	Minimum Threat Defense	Details
Suggested release notifications.	7.2.6 7.4.1	Any	The Firewall Management Center now notifies you when a new suggested release is available. If you don't want to upgrade right now, you can have the system remind you later, or defer reminders until the next suggested release. The new upgrade page also indicates suggested releases.
New upgrade wizard for the Firewall Management Center.	7.2.6 7.4.1	Any	A new upgrade starting page and wizard make it easier to perform Firewall Management Center upgrades. After you use **System**(⚙) > **Product Upgrades** to get the appropriate upgrade package onto the Firewall Management Center, click **Upgrade** to begin. Version restrictions: Only supported for Firewall Management Center upgrades from Version 7.2.6+/7.4.1+. Not supported for upgrades from Version 7.3.x or 7.4.0. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
Hotfix high availability Firewall Management Centers without pausing synchronization.	7.2.6 7.4.1	Any	Unless otherwise indicated by the hotfix release notes or Cisco TAC, you do not have to pause synchronization to install a hotfix on high availability Firewall Management Centers. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
Administration			
Updated internet access requirements for direct-downloading software upgrades.	7.2.6 7.4.1	Any	**Upgrade impact. The system connects to new resources.** The Firewall Management Center has changed its direct-download location for software upgrade packages from sourcefire.com to amazonaws.com. See: Security, Internet Access, and Communication Ports
Usability, Performance, and Troubleshooting			
Enable/disable access control object optimization.	7.2.6 7.4.1	Any	You can now enable and disable access control object optimization from the Firewall Management Center web interface. New/modified screens: **System**(⚙) > **Configuration** > **Access Control Preferences** > **Object Optimization** Version restrictions: Access control object optimization is automatically enabled on all Firewall Management Centers upgraded or reimaged to Versions 7.2.4–7.2.5 and 7.4.0, and automatically disabled on all Firewall Management Centers upgraded or reimaged to Version 7.3.x. It is configurable and enabled by default for Firewall Management Centers reimaged to Version 7.2.6+/7.4.1+, but respects your current setting when you upgrade to those releases.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cluster control link ping tool.	7.2.6 7.4.1	Any	You can check to make sure all the cluster nodes can reach each other over the cluster control link by performing a ping. One major cause for the failure of a node to join the cluster is an incorrect cluster control link configuration; for example, the cluster control link MTU may be set higher than the connecting switch MTUs. New/modified screens: **Devices** > **Device Management** > **More** > **Cluster Live Status.** See: Perform a Ping on the Cluster Control Link
Snort 3 restarts when it uses too much memory, which can trigger HA failover.	7.2.6 7.4.1	7.2.6 with Snort 3 7.4.1 with Snort 3	To improve continuity of operations, excessive memory use by Snort can now trigger high availability failover. This happens because Snort 3 now restarts if the process uses too much memory. Restarting the Snort process briefly interrupts traffic flow and inspection on the device, and in high availability deployments can trigger failover. (In a standalone deployment, interface configurations determine whether traffic drops or passes without inspection during the interruption.) This feature is enabled by default. You can use the CLI to disable it, or configure the memory threshold. Platform restrictions: Not supported with clustered devices. New/modified CLI commands: **configure snort3 memory-monitor**, **show snort3 memory-monitor-status** See: *Cisco Secure Firewall Threat Defense Command Reference*
Set the frequency of Snort 3 core dumps.	7.2.6 7.4.1	7.2.6 with Snort 3 7.4.1 with Snort 3	You can now set the frequency of Snort 3 core dumps. Instead of generating a core dump every time Snort crashes, you can generate one the next time Snort crashes only. Or, generate one if a crash has not occurred in the last day, or week. Snort 3 core dumps are disabled by default for standalone devices. For high availability and clustered devices, the default frequency is now once per day instead of every time. New/modified CLI commands: **configure coredump snort3**, **show coredump** See: *Cisco Secure Firewall Threat Defense Command Reference*
Capture dropped packets with the Secure Firewall 3100/4200.	7.2.6 7.4.1	7.2.6 (no 4200) 7.4.1	Packet losses resulting from MAC address table inconsistencies can impact your debugging capabilities. The Secure Firewall 3100/4200 can now capture these dropped packets. New/modified CLI commands: [**drop** { **disable** | **mac-filter** }] in the **capture** command. See: *Cisco Secure Firewall Threat Defense Command Reference*
Deprecated Features			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: DHCP relay trusted interfaces with FlexConfig.	7.2.6 7.4.1	Any	**Upgrade impact. Redo any related FlexConfigs after upgrade.** You can now use the Firewall Management Center web interface to configure interfaces as trusted interfaces to preserve DHCP Option 82. If you do this, these settings override any existing FlexConfigs, although you should remove them. See: Configure the DHCP Relay Agent

Firewall Management Center Features in Version 7.2.5

Table 59: Firewall Management Center Features in Version 7.2.5

Feature	Minimum Management Center	Minimum Threat Defense	Details
Interfaces			
Management center detects interface sync errors.	7.2.5 7.4.1	Any	**Upgrade impact. You may need to sync interfaces after upgrade.** In some cases, the Firewall Management Center can be missing a configuration for an interface even though the interface is correctly configured and functioning on the device. If this happens, and your Firewall Management Center is running: • Version 7.2.5: Deploy is blocked until you edit the device and sync from the Interfaces page • Version 7.2.6+/7.4.1+: Deploy is allowed with a warning, but you cannot edit interface settings without syncing first. See: Sync Interface Changes with the Management Center

Firewall Management Center Features in Version 7.2.4

Table 60: Firewall Management Center Features in Version 7.2.4

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.2.4 also has: • Automatically update CA bundles. Upgrade impact. (7.0.5) • Smaller VDB for lower memory Snort 2 devices. (7.0.6) • Deprecated: `high unmanaged disk usage` alerts. (7.0.6)
Interfaces			
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 7.3.0	Any	When you set the FEC to Auto on the Secure Firewall 3100 fixed ports, the default type is now set to Clause 108 RS-FEC instead of Clause 74 FC-FEC for 25 GB+ SR, CSR, and LR transceivers. See: Interface Overview.
Performance			
Access control performance improvements (object optimization).	7.2.4 7.4.0	Any	**Upgrade impact. First deployment after Firewall Management Center upgrade to 7.2.4–7.2.5 or 7.4.0 can take a long time and increase CPU use on managed devices.** Access control object optimization improves performance and consumes fewer device resources when you have access control rules with overlapping networks. The optimizations occur on the *managed device* on the first deploy after the feature is enabled on the Firewall Management Center (including if it is enabled by an upgrade). If you have a high number of rules, the system can take several minutes to an hour to evaluate your policies and perform object optimization. During this time, you may also see higher CPU use on your devices. A similar thing occurs on the first deploy after the feature is disabled (including if it is disabled by upgrade). After this feature is enabled or disabled, we recommend you deploy when it will have the least impact, such as a maintenance window or a low-traffic time. New/modified screens (requires Version 7.2.6/7.4.1): **System**(⚙) > **Configuration** > **Access Control Preferences** > **Object-group optimization**. See: Access Control Preferences

Firewall Management Center Features in Version 7.2.3

Table 61: Firewall Management Center Features in Version 7.2.3

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firepower 1010E.	7.2.3.1 7.3.1.1 7.4.1	7.2.3 7.4.1	We introduced the Firepower 1010E, which does not support power over Ethernet (PoE). Do not use a Version 7.2.3 or Version 7.3.0 Firewall Management Center to manage the Firepower 1010E. Instead, use a Version 7.2.3.1+ or Version 7.3.1.1+ Firewall Management Center. See: Regular Firewall Interfaces

Firewall Management Center Features in Version 7.2.2

There are no new features in this release.

Firewall Management Center Features in Version 7.2.1

Table 62: Firewall Management Center Features in Version 7.2.1

Feature	Minimum Management Center	Minimum Threat Defense	Details
Hardware bypass ("fail-to-wire") network modules for the Secure Firewall 3100.	7.2.1 7.3.0	7.2.1	We introduced these hardware bypass network modules for the Secure Firewall 3100: • 6-port 1G SFP Hardware Bypass Network Module, SX (multimode) (FPR-X-NM-6X1SX-F) • 6-port 10G SFP Hardware Bypass Network Module, SR (multimode) (FPR-X-NM-6X10SR-F) • 6-port 10G SFP Hardware Bypass Network Module, LR (single mode) (FPR-X-NM-6X10LR-F) • 6-port 25G SFP Hardware Bypass Network Module, SR (multimode) (FPR-X-NM-X25SR-F) • 6-port 25G Hardware Bypass Network Module, LR (single mode) (FPR-X-NM-6X25LR-F) • 8-port 1G Copper Hardware Bypass Network Module, RJ45 (copper) (FPR-X-NM-8X1G-F) New/modified screens: **Devices > Device Management > Interfaces > Edit Physical Interface** For more information, see Inline Sets and Passive Interfaces.
Intel Ethernet Network Adapter E810-CQDA2 driver with Firewall Threat Defense Virtual for KVM.	7.2.1 7.3.0	7.2.1	We now support the Intel Ethernet Network Adapter E810-CQDA2 driver with Firewall Threat Defense Virtual for KVM. For more information, see Getting Started with Secure Firewall Threat Defense Virtual and KVM.

Firewall Management Center Features in Version 7.2.0

Table 63: Firewall Management Center Features in Version 7.2.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from Earlier Maintenance Releases			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Features from earlier maintenance releases.	Feature dependent	Feature dependent	Version 7.2.0 also has: • ISA 3000 support for shutting down. (7.0.2) • Improved SecureX integration, SecureX orchestration. Upgrade impact. (7.0.2) • Web interface changes: SecureX, threat intelligence, and other integrations. (7.0.2) • Threat defense support for Cloud-Delivered Firewall Management Center. (7.0.3)
Platform			
Management center virtual for Alibaba.	7.2.0	Any	We introduced Secure Firewall Management Center Virtual for Alibaba Cloud.
Threat defense virtual for Alibaba.	7.2.0	7.2.0	We introduced Secure Firewall Threat Defense for Alibaba Cloud. You must use Firewall Management Center; device manager is not supported. Note that due to underlying issues in the Alibaba infrastructure, the Firewall Threat Defense Virtual instance type ecs.g5ne.4xLarge has low performance, especially in terms of connections per second (CPS). We recommend the 2xlarge or 4xlarge.
Snapshots allow quick deploy of Firewall Threat Defense Virtual for AWS and Azure.	7.2.0	7.2.0	You can now take a snapshot of a Firewall Threat Defense Virtual for AWS or Azure instance, then use that snapshot to quickly deploy new instances. This feature also improves the performance of the autoscale solutions for AWS and Azure. For more information, see the Secure Firewall Threat Defense Virtual getting started guides.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Analytics mode for cloud-managed Firewall Threat Defense.	7.2.0	7.0.3 7.2.0	Concurrently with Version 7.2, we introduced the Cloud-Delivered Firewall Management Center, which uses the Security Cloud Control platform and unites management across multiple Cisco security solutions. We take care of feature updates. On-prem hardware and virtual Firewall Management Centers running Version 7.2+ can "co-manage" cloud-managed Firewall Threat Defense, but for event logging and analytics purposes only. You cannot deploy policy to these devices from an on-prem Firewall Management Center. New/modified screens: • When you add a cloud-managed device to an on-prem Firewall Management Center, use the new **CDO Managed Device** check box to specify that it is analytics-only. • View which devices are analytics-only on **Devices > Device Management**. New/modified CLI commands: **configure manager add**, **configure manager delete**, **configure manager edit**, **show managers** For more information, see *Cisco Security Cloud Control: Secure Firewall Threat Defense Management*.
High Availability/Scalability: Threat Defense			
Clustering for Firewall Threat Defense Virtual in both public and private clouds.	7.2.0	7.2.0	You can now configure clustering for the following Firewall Threat Defense Virtual platforms: • Threat defense virtual for AWS: 16-node clusters • Threat defense virtual for GCP: 16-node clusters • Threat defense virtual for KVM: 4-node clusters • Threat defense virtual for VMware: 4-node clusters New/modified screens: • **Devices > Device Management > Add Cluster** • **Devices > Device Management > More** menu • **Devices > Device Management > Cluster** For more information, see Clustering for Threat Defense Virtual in a Public Cloud (AWS, GCP) or Clustering for Threat Defense Virtual in a Private Cloud (KVM, VMware).

Feature	Minimum Management Center	Minimum Threat Defense	Details
16-node clusters for the Firepower 4100/9300, and for Firewall Threat Defense Virtual for AWS and GCP.	7.2.0	7.2.0	You can now configure 16-node clusters for the Firepower 4100/9300, and for Firewall Threat Defense Virtual for AWS and GCP. Note that the Secure Firewall 3100 still only supports 8 nodes. For more information, see Clustering for the Firepower 4100/9300 or Clustering for Threat Defense Virtual in a Public Cloud.
High availability for Firewall Threat Defense Virtual for Nutanix.	7.2.0	7.2.0	We now support high availability for Firewall Threat Defense Virtual for Nutanix. For more information, see the Secure Firewall Threat Defense Virtual getting started guides.
Autoscale for Firewall Threat Defense Virtual for AWS gateway load balancers.	7.2.0	7.2.0	We now support autoscale for Firewall Threat Defense Virtual for AWS gateway load balancers, using a CloudFormation template. For more information, see the Secure Firewall Threat Defense Virtual getting started guides.
Autoscale for Firewall Threat Defense Virtual for GCP.	7.2.0	7.2.0	**Upgrade impact. Threat defense virtual for GCP cannot upgrade across Version 7.2.0.** We now support autoscale for Firewall Threat Defense Virtual for GCP, by positioning a Firewall Threat Defense Virtual instance group between a GCP internal load balancer (ILB) and a GCP external load balancer (ELB). Version restrictions: Due to interface changes required to support this feature, Firewall Threat Defense Virtual for GCP upgrades cannot cross Version 7.2.0. That is, you cannot upgrade to Version 7.2.0+ from Version 7.1.x and earlier. You must deploy a new instance and redo any device-specific configurations. For more information, see the Secure Firewall Threat Defense Virtual getting started guides.
Interfaces			
LLDP support for the Firepower 2100 and Secure Firewall 3100.	7.2.0	7.2.0	You can now enable Link Layer Discovery Protocol (LLDP) for Firepower 2100 and Secure Firewall 3100 series interfaces. New/modified screens: **Devices** > **Device Management** > **Interfaces** > > **Hardware Configuration** > **LLDP** New/modified commands: **show lldp status**, **show lldp neighbors**, **show lldp statistics** For more information, see Interface Overview.

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

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

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

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

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

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

Feature	Minimum Management Center	Minimum Threat Defense	Details
Improved SMB 3 inspection.	7.2.0	7.2.0 with Snort 3	We now support inspection of SMB 3 traffic in the following situations: • During file server node failover for clusters configured for SMB Transparent Failover. • In multiple file server nodes for clusters using SMB Scale-Out. • Through directory information changes due to SMB Directory Leasing. • Spread across multiple connections due to SMB Multichannel. For more information, see the *Snort 3 Inspector Reference* and the Cisco Secure Firewall Management Center Snort 3 Configuration Guide.
Event Logging and Analysis			
Log security events to multiple Secure Network Analytics on-prem data stores.	7.2.0	7.0.0	When you configure a Secure Network Analytics Data Store (multi-node) integration, you can now add multiple flow collectors for security events. You assign each flow collector to one or more Firewall Threat Defense devices running Version 7.0+. New/modified screens: • Setup: **Integration** > **Security Analytics & Logging** > **Secure Network Analytics Data Store** • Modify: **Integration** > **Security Analytics & Logging** > **Update Device Assignments** This feature requires Secure Network Analytics Version 7.1.4. For more information, see the *Cisco Security Analytics and Logging (On Premises): Firewall Event Integration Guide*.
Database access changes.	7.2.0	Any	We added ten new tables, deprecated one table, and prohibited joins in six tables. We also added fields to various tables for Snort 3 support and to provide timestamps and IP addresses in human-readable format. For more information, see the *What's New* topic in the Cisco Secure Firewall Management Center Database Access Guide, Version 7.2.
eStreamer changes.	7.2.0	Any	A new Python-based reference client has been added to the SDK. Also, you can now request fully qualified events. For more information, see the *What's New* topic in the Cisco Secure Firewall Management Center Event Streamer Integration Guide, Version 7.2.
Deployment and Policy Management			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Auto rollback of a deployment that causes a loss of management connectivity.	7.2.0	7.2.0	You can now enable auto rollback of the configuration if a deployment causes the management connection between the Firewall Management Center and Firewall Threat Defense to go down. Previously, you could only manually roll back a configuration using the **configure policy rollback** command. New/modified screens: • **Devices > Device Management > Device > Deployment Settings** • **Deploy > Advanced Deploy > Preview** • **Deploy > Deployment History > Preview** For more information, see Device Management.
Generate and email a report when you deploy configuration changes.	7.2.0	Any	You can now generate a report for any deploy task. The report contains details about the deployed configuration. New/modified pages: **Deploy** > **Deployment History** ( ) **icon > More** ( )**Generate Report** For more information, see Configuration Deployment.
Access control policy locking.	7.2.0	Any	You can now lock an access control policy to prevent other administrators from editing it. Locking the policy ensures that your changes will not be invalidated if another administrator edits the policy and saves changes before you save your changes. Any user who has permission to modify the access control policy has permission to lock it. We added an icon to lock or unlock a policy next to the policy name while editing the policy. In addition, there is a new permission to allow users to unlock policies locked by other administrators: Override Access Control Policy Lock. This permission is enabled by default in the Administrator, Access Admin, and Network Admin roles. For more information, see Access Control Policies.
Object group search is enabled by default.	7.2.0	Any	The **Object Group Search** setting is now enabled by default when you add a device to the Firewall Management Center. New/modified screens: **Devices** > **Device Management** > **Device** > **Advanced Settings** For more information, see Device Management.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Access control rule hit counts persist over reboot.	7.2.0	7.2.0	Rebooting a managed device no longer resets access control rule hit counts to zero. Hit counts are reset only if you actively clear the counters. In addition, counts are maintained by each unit in an HA pair or cluster separately. You can use the **show rule hits** command to see cumulative counters across the HA pair or cluster, or see the counts per node. New/modified CLI commands: **show rule hits** For more information, see the *Cisco Secure Firewall Threat Defense Command Reference*.
New user interface for the access control policy.	7.2.0	Any	There is a new experimental user interface available for the access control policy. You can continue to use the legacy user interface, or you can try out the new user interface. The new interface has both a table and a grid view for the rules list, the ability to show or hide columns, enhanced search, infinite scroll, a clearer view of the packet flow related to policies associated with the access control policy, and a simplified add/edit dialog box for creating rules. You can freely switch back and forth between the legacy and new user interfaces while editing an access control policy. **Note** The new interface does not have all the features available in the legacy interface, and may have performance issues when displaying a large number of rules. If you experience issues with the new UI, switch back to the legacy UI. Additionally, Cisco TAC welcomes your feedback. If your organization allows it, you can help us improve this feature by making sure web analytics is enabled: **System** (⚙) > **Configuration** > **Web Analytics**. For more information, see Access Control Policies.
Upgrade			

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

Feature	Minimum Management Center	Minimum Threat Defense	Details
Upgrade for single-node clusters.	7.2.0	Any	You can now use the device upgrade page (**Devices** > **Device Upgrade**) to upgrade clusters with only one active node. Any deactivated nodes are also upgraded. Previously, this type of upgrade would fail. This feature is not supported from the system updates page (**System** > **Updates**). Hitless upgrades are also not supported in this case. Interruptions to traffic flow and inspection depend on the interface configurations of the lone active unit, just as with standalone devices. Supported platforms: Firepower 4100/9300, Secure Firewall 3100
Administration			
Multiple DNS server groups for resolving DNS requests.	7.2.0	Any	You can configure multiple DNS groups for the resolution of DNS requests from client systems. You can use these DNS server groups to resolve requests for different DNS domains. For example, you could have a catch-all default group that uses public DNS servers, for use with connections to the Internet. You could then configure a separate group to use internal DNS servers for internal traffic, for example, any connection to a machine in the example.com domain. Thus, connections to an FQDN using your organization's domain name would be resolved using your internal DNS servers, whereas connections to public servers use external DNS servers. New/modified screens: **Platform Settings** > **DNS** For more information, see Platform Settings.
Configure certificate validation with Firewall Threat Defense by usage type.	7.2.0	7.2.0	You can now specify the usage types where validation is allowed with the trustpoint (the Firewall Threat Defense device): IPsec client connections, SSL client connections, and SSL server certificates. New/modified screens: We added a **Validation Usage** option to certificate enrollment objects: **Objects** > **Object Manager** > **PKI** > **Cert Enrollment**. For more information, see Object Management.
French language option for web interface.	7.2.0	Any	You can now switch the Firewall Management Center web interface to French. New/modified screens: **System** (⚙) **> Configuration > Language** For more information, see System Configuration.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Web interface changes: deployment and user activity integrations.	7.2.0	Any	Version 7.2 changes these Firewall Management Center menu options in all cases. **Deploy > Deployment History** is now **Deploy > Deployment History** (bottom right corner) **Deploy > Deployment** is now **Deploy > Advanced Deploy** **Analysis > Users > Active Sessions** is now **Integration > Users > Active Sessions** **Analysis > Users > Users** is now **Integration > Users > Users** **Analysis > Users > User Activity** is now **Integration > Users > User Activity**
Troubleshooting			
Dropped packet statistics for the Secure Firewall 3100.	7.2.0	7.2.0	The new **show packet-statistics** Firewall Threat Defense CLI command displays comprehensive information about non-policy related packet drops. Previously this information required using several commands. For more information, see the *Cisco Secure Firewall Threat Defense Command Reference*.
Deprecated Features			
Deprecated: EIGRP with FlexConfig.	7.2.0	Any	You can now configure EIGRP routing from the Firewall Management Center web interface. You no longer need these FlexConfig objects: Eigrp_Configure, Eigrp_Interface_Configure, Eigrp_Unconfigure, Eigrp_Unconfigure_all. And these associated text objects: eigrpAS, eigrpNetworks, eigrpDisableAutoSummary, eigrpRouterId, eigrpStubReceiveOnly, eigrpStubRedistributed, eigrpStubConnected, eigrpStubStatic, eigrpStubSummary, eigrpIntfList, eigrpAS, eigrpAuthKey, eigrpAuthKeyId, eigrpHelloInterval, eigrpHoldTime, eigrpDisableSplitHorizon. The system does allow you to deploy post-upgrade, but also warns you to redo your EIGRP configurations. To help you with this process, we provide a command-line migration tool. For details, see Migrating FlexConfig Policies .

Feature	Minimum Management Center	Minimum Threat Defense	Details
Deprecated: VXLAN with FlexConfig.	7.2.0	Any	You can now configure VXLAN interfaces from the Firewall Management Center web interface. You no longer need these FlexConfig objects: VxLAN_Clear_Nve, VxLAN_Clear_Nve_Only, VxLAN_Configure_Port_And_Nve, VxLAN_Make_Nve_Only, VxLAN_Make_Vni. And these associated text objects: vxlan_Port_And_Nve, vxlan_Nve_Only, vxlan_Vni. If you configured VXLAN interfaces with FlexConfig in a previous version, they continue to work. In fact, FlexConfig takes precedence in this case—if you redo your VXLAN configurations in the web interface, remove the FlexConfig settings.
Deprecated: Automatic pre-upgrade troubleshooting.	7.2.0	Any	To save time and disk space, the Firewall Management Center upgrade process no longer automatically generates troubleshooting files before the upgrade begins. Note that device upgrades are unaffected and continue to generate troubleshooting files. To manually generate troubleshooting files for the Firewall Management Center, choose **System**(⚙) > **Health** > **Monitor**, click **Firewall Management Center** in the left panel, then **View System & Troubleshoot Details**, then **Generate Troubleshooting Files**.
Deprecated: Geolocation details.	Any	Any	We no longer provide the geolocation IP package, which contained contextual data associated with routable IP addresses. This saves disk space and does not affect geolocation rules or traffic handling in any way. Any contextual data is now stale, and upgrading to most later versions deletes the IP package. Options to download the IP package or view contextual data have no effect, and are removed in later versions.

FMC Features in Version 7.1.0

Note You cannot manage a Version 7.1 device with Cloud-Delivered Firewall Management Center. If your cloud-managed devices are running Version 7.0.x, upgrade directly to Version 7.2.0+ to take advantage of the features listed here.

Table 64: FMC Features in Version 7.1.0.3

Feature	Details
Features from earlier maintenance releases	

Feature	Details
Features from earlier maintenance releases.	Version 7.1.0.3 also has: • Automatically update CA bundles. Upgrade impact. (7.0.5)

Table 65: FMC Features in Version 7.1.0

Feature	Details
Platform	
Secure Firewall 3100.	We introduced the Secure Firewall 3110, 3120, 3130, and 3140. You can hot swap a network module of the same type while the firewall is powered up without having to reboot; making other module changes requires a reboot. Secure Firewall 3100 25 Gbps interfaces support Forward Error Correction as well as speed detection based on the SFP installed. The SSDs are self-encrypting drives (SEDs), and if you have 2 SSDs, they form a software RAID. These devices support up to 8 units for Spanned EtherChannel clustering. Note that the Version 7.1.0 release does not include online help for these devices; new online help is included in Version 7.1.0.2. New/modified screens: • **Devices** > **Device Management** > **Add Cluster** • **Devices** > **Device Management** > **More** • **Devices** > **Device Management** > **Cluster** • **Devices** > **Device Management** > **Chassis Operations** • **Devices** > **Device Management** > **Interfaces** > edit physical interface > **Hardware Configuration** • **Devices** > **Device Management** New/modified FTD CLI commands: **configure network speed**, **configure raid**, **show raid**, **show ssd**
FMCv300 for AWS FMCv300 for OCI	We introduced the FMCv300 for both AWS and OCI. The FMCv300 can manage up to 300 devices.

Feature	Details
FTDv for AWS instances.	FTDv for AWS adds support for these instances: • c5a.xlarge, c5a.2xlarge, c5a.4xlarge • c5ad.xlarge, c5ad.2xlarge, c5ad.4xlarge • c5d.xlarge, c5d.2xlarge, c5d.4xlarge • c5n.xlarge, c5n.2xlarge, c5n.4xlarge • i3en.xlarge, i3en.2xlarge, i3en.3xlarge • inf1.xlarge, inf1.2xlarge • m5.xlarge, m5.2xlarge, m5.4xlarge • m5a.xlarge, m5a.2xlarge, m5a.4xlarge • m5ad.xlarge, m5ad.2xlarge, m5ad.4xlarge • m5d.xlarge, m5d.2xlarge, m5d.4xlarge • m5dn.xlarge, m5dn.2xlarge, m5dn.4xlarge • m5n.xlarge, m5n.2xlarge, m5n.4xlarge • m5zn.xlarge, m5zn.2xlarge, m5zn.3xlarge • r5.xlarge, r5.2xlarge, r5.4xlarge • r5a.xlarge, r5a.2xlarge, r5a.4xlarge • r5ad.xlarge, r5ad.2xlarge, r5ad.4xlarge • r5b.xlarge, r5b.2xlarge, r5b.4xlarge • r5d.xlarge, r5d.2xlarge, r5d.4xlarge • r5dn.xlarge, r5dn.2xlarge, r5dn.4xlarge • r5n.xlarge, r5n.2xlarge, r5n.4xlarge • z1d.xlarge, z1d.2xlarge, z1d.3xlarge
FTDv for Azure instances.	FTDv for Azure adds support for these instances: • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2

Feature	Details
Use FDM to configure the FTD for management by the FMC.	When you perform initial setup using FDM, all interface configuration completed in FDM is retained when you switch to FMC for management, in addition to the Management and FMC access settings. Note that other default configuration settings, such as the access control policy or security zones, are not retained. When you use the FTD CLI, only the Management and FMC access settings are retained (for example, the default inside interface configuration is not retained). After you switch to FMC, you can no longer use FDM to manage the FTD. New/modified FDM screens: **System Settings** > **Management Center**
Threat Defense Upgrade	
Revert a successful device upgrade.	You can now revert major and maintenance upgrades to FTD. Reverting returns the software to its state just before the last upgrade, also called a *snapshot*. If you revert an upgrade after installing a patch, you revert the patch as well as the major and/or maintenance upgrade. **Important** If you think you might need to revert, you must use **System** > **Updates** to upgrade FTD. The System Updates page is the only place you can enable the **Enable revert after successful upgrade** option, which configures the system to save a revert snapshot when you initiate the upgrade. This is in contrast to our usual recommendation to use the wizard on the **Devices** > **Device Upgrade** page. This feature is not supported for container instances. Minimum FTD: 7.1
Improvements to the upgrade workflow for clustered and high availability devices.	We made the following improvements to the upgrade workflow for clustered and high availability devices: • The upgrade wizard now correctly displays clustered and high availability units as groups, rather than as individual devices. The system can identify, report, and preemptively require fixes for group-related issues you might have. For example, you cannot upgrade a cluster on the Firepower 4100/9300 if you have made unsynced changes on Firepower Chassis Manager. • We improved the speed and efficiency of copying upgrade packages to clusters and high availability pairs. Previously, the FMC copied the package to each group member sequentially. Now, group members can get the package from each other as part of their normal sync process. • You can now specify the upgrade order of data units in a cluster. The control unit always upgrades last.
Snort 3 backwards compatibility.	For Snort 3, new features and resolved bugs require that you fully upgrade the FMC *and* its managed devices. Unlike Snort 2, you cannot update the inspection engine on an older device (for example, Version 7.0) by deploying from a newer FMC (for example, Version 7.1). When you deploy to an older device, the system lists any unsupported configurations and warns you that they will be skipped. We recommend you always update your entire deployment.
Device Management	

Feature	Details
Geneve interface support for an FTDv on AWS instances.	Geneve encapsulation support was added to support single-arm proxy for the AWS Gateway Load Balancer (GWLB). The AWS GWLB combines a transparent network gateway (with a single entry and exit point for all traffic) and a load balancer that distributes traffic and scales FTDv to match the traffic demand. This support requires FMC with Snort 3 enabled and is available on the following performance tiers: • FTDv20 • FTDv30 • FTDv50 • FTDv100
Single Root I/O Virtualization (SR-IOV) support for FTDv on OCI.	You can now implement Single Root Input/Output Virtualization (SR-IOV) for FTDv on OCI. SR-IOV can provide performance improvements for an FTDv. Mellanox 5 as vNICs are not supported in SR-IOV mode.
LLDP support for the Firepower 1100.	You can now enable Link Layer Discovery Protocol (LLDP) for Firepower 1100 interfaces. New/modified screens: **Devices** > **Device Management** > **Interfaces** > **Hardware Configuration** > **LLDP** New/modified commands: **show lldp status**, **show lldp neighbors**, **show lldp statistics** Supported platforms: Firepower 1100 (1120, 1140, and 1150)
Interface auto-negotiation is now set independently from speed and duplex, interface sync improved.	Interface auto-negotiation is now set independently from speed and duplex. Also, when you sync the interfaces in FMC, hardware changes are detected more effectively. New/modified screens: **Devices** > **Device Management** > **Interfaces** > **Hardware Configuration** > **Speed** Supported platforms: Firepower 1000/2100, Secure Firewall 3100
Support to specify trusted DNS servers.	You can use FTD platform settings to specify trusted DNS servers for DNS snooping. This helps detect applications on the first packet by mapping domains to IP addresses. By default, trusted DNS servers include those in DNS server objects, and those discovered by dhcp-pool, dhcp-relay, and dhcp-client.
Import and export device configurations.	You can export the device-specific configuration, and you can then import the saved configuration for the same device in the following use cases: • Moving the device to a different FMC. • Restore an old configuration. • Reregistering a device. New/modified screens: **Devices** > **Device Management** > **Device** > **General**
High Availability/Scalability	

Feature	Details
High availability for: • FMCv for AWS • FMCv for OCI	We now support high availability on FMCv for AWS and FMCv for OCI. In an FTD deployment, you need two identically licensed FMCs, as well as one FTD entitlement for each managed device. For example, to manage 10 FTD devices with an FMCv10 high availability pair, you need two FMCv10 entitlements and 10 FTD entitlements. If you are managing Version 6.5.0–7.0.x Classic devices only (NGIPSv or ASA FirePOWER), you do not need FMCv entitlements. Supported platforms: FMCv10, FMCv25, FMCv300 (not supported for FMCv2)
Autoscale on FTDv for OCI.	We now support autoscaling on FTDv for OCI. The serverless infrastructure in cloud-based deployments allow you to automatically adjust the number of FTDv instances in an autoscale group based on capacity needs. This includes automatic registering/unregistering to and from the managing FMC.
Cluster deployment for firewall changes completes faster.	Cluster deployment for firewall changes now completes faster. Supported platforms: Firepower 4100/9300, Secure Firewall 3100
Clearing routes in a high availability group or cluster.	In previous releases, the **clear route** command cleared the routing table on the unit only. Now, when operating in a high availability group or cluster, the command is available on the active or control unit only, and clears the routing table on all units in the group or cluster.
NAT	
Manual NAT support for fully-qualified domain name (FQDN) objects as the translated destination.	You can use an FQDN network object, such as one specifying www.example.com, as the translated destination address in manual NAT rules. The system configures the rule based on the IP address returned from the DNS server.
Routing	
BGP configuration to interconnect virtual routers.	You can configure BGP settings to dynamically leak routes among user-defined virtual routers, and between global virtual router and user-defined virtual routers. The import and export routes feature was introduced to exchange routes among the virtual routers by tagging them with route targets and optionally, filtering the matched routes with route maps. This BGP feature is accessible only when you select a user-defined virtual router. New/modified screens: For a selected user-defined virtual router, **Devices** > **Device Management** > **Routing** > **BGPv4/v6** > **Route Import/Export**
BGPv6 support for user-defined virtual routers.	FTD now supports configuring BGPv6 on user-defined virtual routers. New/modified screens: For a selected user-defined virtual router, **Devices** > **Device Management** > **Routing** > **BGPv6**
Configure Equal-Cost-Multi-Path (ECMP) from the FMC web interface.	**Upgrade impact. Redo FlexConfigs after upgrade.** You can now group interfaces in traffic zones and configure Equal-Cost-Multi-Path (ECMP) routing in FMC. ECMP routing was previously supported through FlexConfig policies. New/modified screens: **Devices** > **Device Management** > **Routing** > **ECMP**

Feature	Details
Configure policy based routing from the FMC web interface.	**Upgrade impact. Redo FlexConfigs after upgrade.** You can now configure policy based routing (PBR) from the FMC web interface. This allows you to classify network traffic based on applications and to implement direct internet access (DIA) to send traffic to the internet from a branch deployment. You can define a PBR policy and configure it on ingress interfaces, specifying match criteria and egress interfaces. Network traffic that matches the access control policy is forwarded through the egress interface based on priority or the order as configured in the policy. This feature requires Version 7.1+ on both the FMC and the device. When you upgrade the FMC to Version 7.1+, existing policy based routing FlexConfigs are removed. After you upgrade your devices to Version 7.1+, redo your policy based routing configurations in the FMC web interface. For devices that you do not upgrade to Version 7.1+, redo the FlexConfigs and configure them to deploy "every time." New/modified screens: **Devices** > **Device Management** > **Routing** > **Policy Based Routing**
Remote Access VPN	
Copy RA VPN policies.	You can now create a new RA VPN policy by copying an existing policy. We added a copy button next to each policy on **Devices** > **VPN** > **Remote Access**.
AnyConnect VPN SAML external browser.	You can now configure AnyConnect VPN SAML External Browser to enable additional authentication choices, such as passwordless authentication, WebAuthN, FIDO, SSO, U2F, and an improved SAML experience due to the persistence of cookies. When you use SAML as the primary authentication method for a remote access VPN connection profile, you can elect to have the AnyConnect client use the client's local browser instead of the AnyConnect embedded browser to perform the web authentication. This option enables single sign-on (SSO) between your VPN authentication and other corporate logins. Also choose this option if you want to support web authentication methods, such as biometric authentication and Yubikeys, that cannot be performed in the embedded browser. We updated the remote access VPN connection profile wizard to allow you to configure the **SAML Login Experience**.
Multiple trustpoints for SAML identity providers on Microsoft Azure.	You can now add multiple RA VPN trustpoints for SAML identity providers, as required by Microsoft Azure. In a Microsoft Azure network, Azure can support multiple applications for the same Entity ID. Each application (typically mapped to a different tunnel group) requires a unique certificate. This feature enables you to add multiple trustpoints for RA VPN in FTDv for Microsoft Azure.
Site to Site VPN	
VPN filters.	You can now configure site to site VPN filters with rules that determine whether to allow or reject tunneled data packets based on criteria such as source address, destination address, and protocol. The VPN filter is applied to post-decrypted traffic after it exits a tunnel and to pre-encrypted traffic before it enters a tunnel.
Unique local tunnel ID for IKEv2.	You can now configure a Local Tunnel ID per IKEv2 tunnel for both policy-based and route-based site to site VPNs. This local tunnel ID configuration enables Umbrella SIG integration with FTD.

Feature	Details
Multiple IKE policies.	You can now configure multiple IKE policies for both policy-based and route-based site to site VPNs.
VPN monitoring dashboard.	**Beta.** The Site to Site VPN Monitoring Dashboard provides: • Visualization of tunnel status distribution across all devices • Visualization of network topology consisting of VPN tunnels • Ability to visually isolate and examine tunnels based on criteria like Topology, Device and Status **Note** This is a Beta feature and may not work as expected. Do not use it in production environments.
Security Intelligence	
Snort 3 support for Security Intelligence on proxied traffic.	With Snort 3, you can now apply Security Intelligence to HTTP proxy traffic where the IP address is embedded into the HTTP request. For example, when a user uploads a Block list or an Allow list containing IP addresses or networks, the system matches on the destination server IP instead of proxy IP. As a result, traffic to the destination server can be blocked, monitored, or allowed (according to your Security Intelligence configuration).
Intrusion Detection and Prevention	
Snort 3 support for drop, reject, rewrite, and pass rule actions.	Version 7.1 FMCs now support the following intrusion rule actions for FTD devices with Snort 3, including Version 7.0 devices: • Drop: Drops the matching packet, but does not block further traffic in this connection. Generates an intrusion event. • Reject: Drops the matching packet and blocks further traffic in this connection. For TCP traffic, sends a TCP reset. For UDP traffic, sends ICMP port unreachable to the source and destination hosts. Generates an intrusion event. • Rewrite: Overwrites the matching packet based on the replace option in the rule. Generates an intrusion event. • Pass: Allows matching packet to pass without further evaluation by any other intrusion rules. Does not generate an intrusion event. To configure these new rule actions, edit the Snort 3 version of an intrusion policy and use the **Rule Action** drop-down for each rule.
Snort 3 support for TLS-based intrusion rules.	You can now create TLS-based intrusion rules to inspect decrypted TLS traffic with Snort 3. This feature allows Snort 3 intrusion rules to use TLS information.
Snort 3 support for inspection of DCE/RPC over SMB2.	**Upgrade impact.** Version 7.1 with Snort 3 supports DCE/RPC inspection over SMB2. After the first post-upgrade deploy to Snort 3 devices, existing DCE/RPC rules begin inspecting DCE/RPC over SMB2; previously these rules only inspected DCE/RPC over SMB1.

Feature	Details
Snort 3 support for intrusion rule recommendations.	Version 7.1 FMCs now support intrusion rule recommendations for FTD devices with Snort 3, including Version 7.0 devices. To configure this feature, edit the Snort 3 version of an intrusion policy and click the **Recommendations** button (in the left pane, next to All Rules).
Snort 3 support for **ssl_version** and **ssl_state** keywords.	**Upgrade impact.** Version 7.1 with Snort 3 supports the **ssl_version** and **ssl_state** intrusion rule keywords. Cisco-provided intrusion policies include active rules using those keywords. You can also create, upload, and deploy custom/third party rules using them. In Version 7.0.x, we supported those keywords with Snort 2 only. With Snort 3, rules with those keywords did not match traffic, and thus could not generate alerts or affect traffic. There was no indication that the rules were not working as expected. After the first post-upgrade deploy to Version 7.1+ Snort 3 devices, existing rules with those keywords can match traffic.
Identity Services and User Control	
Snort 3 captive portal support for interception of HTTP/2 traffic.	You can now intercept and redirect HTTP/2 traffic for user authentication with captive portal. When a redirect is received by the browser, the browser follows the redirect and authenticates with idhttpsd (Apache web server) using the same process as the HTTP/1 captive portal. After authentication, idhttpsd redirects the user back to the original URL.
Snort 3 captive portal support for hostname-based redirect.	You can configure active authentication for identity policy rules to redirect the user's authentication to a fully-qualified domain name (FQDN) rather than the IP address of the interface through which the user's connection enters the device. The FQDN must resolve to the IP address of one of the interfaces on the device. By using an FQDN, you can assign a certificate for active authentication that the client will recognize, thus avoiding the untrusted certificate warning users get when being redirected to an IP address. The certificate can specify the FQDN, a wildcard FQDN, or multiple FQDNs in the Subject Alternate Names (SAN) in the certificate. New/modified screens: We added the **Redirect to Host Name** option in the identity policy settings.
Encrypted Traffic Handling (TLS/SSL)	
Advanced TLS/SSL policy options.	You can now configure the following advanced TLS/SSL policy options in the **Advanced Settings** tab on the SSL Policy page: • Block flows requesting ESNI (Encrypted Server Name Identification) • Disable HTTP/3 advertisement • Propagate untrusted server certificates to clients

Feature	Details
Encrypted Visibility Engine for visibility into encrypted sessions.	**Beta.** You can enable the Encrypted Visibility Engine to gain visibility into an encrypted session without needing to decrypt it. The engine fingerprints and analyzes encrypted traffic. In FMC 7.1, the Encrypted Visibility Engine provides more visibility into encrypted traffic, including protocols such as TLS and QUIC. It does not enforce any actions on that traffic. The Encrypted Visibility Engine is disabled by default. You can enable it on the **Advanced** tab of an access control policy in the **Experimental Features** section. New/modified screens: **Policies** > **Access Control** > ***Access Control Policy name*** > **Advanced** **Note** The Encrypted Visibility Engine is an experimental Beta feature provided for visibility. It may cause false positives.
Service Policy	
Configure the maximum segment size (MSS) for embryonic connections.	You can configure a service policy to set the server maximum segment size (MSS) for SYN-cookie generation for embryonic connections upon reaching the embryonic connections limit. This is meaningful for service policies where you are also setting embryonic connection maximums. New/modified screens: **Connection Settings** in the Add/Edit Service Policy wizard.
Network Discovery	
Improved Snort 3 support for network discovery (remote network access support).	With improvements to network discovery and remote network access support, Snort 3 is now at parity with Snort 2 for those features. The improvements include: • Discovery of hosts and applications for SMB traffic: For SMB traffic on your network, the host is discovered in the network map, and the SMB application protocol and associated operating system information are discovered. • Discovery of NetBIOS traffic: For NetBIOS traffic, the NetBIOS name is discovered as well as associated information related to applications, such as the client application and operating system. • Discovery of applications only for hosts/networks monitored by the network discovery policy: This enhancement to the filtering logic enables you to discover applications for networks that are being monitored based on a network discovery rule. In Snort 3, application detection is always enabled for all networks by default.
Event Logging and Analysis	

Feature	Details
Snort 3 support for elephant flow identification and monitoring.	With FTD running Snort 3, you can now identify *elephant flows*—single-session network connections that are large enough to affect overall system performance. By default, elephant flow detection is automatically enabled, and tracks and logs connections larger than 1GB/10 seconds. A new predefined search for connection events (Reason = Elephant Flow) allows you to quickly identify elephant flows. You can also use the health monitor to view active elephant flows on your devices, and to create a custom health dashboard to correlate elephant flow incidence with other device metrics such as CPU usage. To disable this feature or to configure the size and time thresholds, use the FTD CLI. New/modified FTD CLI commands: • **show elephant-flow status** • **show elephant-flow detection-config** • **system support elephant-flow-detection enable** • **system support elephant-flow-detection disable** • **system support elephant-flow-detection bytes-threshold** *bytes-in-MB* • **system support elephant-flow-detection time-threshold** *time-in-seconds*
Send intrusion events and retrospective malware events to the Secure Network Analytics cloud from the FMC.	**Upgrade impact.** When you configure the system to send security events to the Stealthwatch cloud using Cisco Security Analytics and Logging (SaaS), the FMC now sends: • Intrusion events. This allows remotely stored intrusion events to include impact flag data. Previously, these events were sent to the cloud by FTD and did not include the impact flag. • Retrospective malware events. These supplement the "original disposition" file and malware events that are still sent to the cloud by devices. If you already enabled this feature, the FMC starts sending this information after a successful upgrade.
New datastore for intrusion events improves performance.	To improve performance, Version 7.1 uses a new datastore for intrusion events. After the upgrade finishes and the FMC reboots, historical events are migrated in the background, newest events first. As part of this migration, we deprecated intrusion incidents, the intrusion event clipboard, and custom tables for intrusion events. We also introduced two new fields in the intrusion event table: Source Host Criticality and Destination Host Criticality.

Feature	Details
NAT IP address and port information in connection and Security Intelligence events.	For additional visibility into NAT translations, we added the following fields to connection and Security Intelligence events: • NAT Source IP • NAT Destination IP • NAT Source Port • NAT Destination Port In the table view of events, these fields are hidden by default. To change the fields that appear, click the **x** in any column name to display a field chooser.
Packet tracer enhancements.	Version 7.1 updates the packet tracer interface for better usability. In addition, you can now: • Access the packet tracer directly from the main menu: **Devices** > **Troubleshoot** > **Packet Tracer**. • Save packet traces. • Run parallel packet traces across multiple devices. • Replay PCAPs through a device. • For Snort 3 devices, view enhanced output that provides new details on the phases of traffic evaluation from L2 to L7 (application identification, file/malware detection, intrusion detection, Security Intelligence, and so on), as well as how long each phase takes. New/modified FTD CLI commands: • **packet-tracer input***source_interface***pcap***pcap_filename*
Object Management	
Network object support for HTTP, ICMP, and SSH platform settings.	You can now use network object groups that contain network objects for hosts or networks when configuring the IP addresses in the Threat Defense Platform Settings policy.
Snort 3 support for network wildcard mask objects.	You can now create and manage network wildcard mask objects on the **Object Management** page. You can use network wildcard mask objects in access control, prefilter, and NAT policies.
Deployment preview enhancements for objects.	You can now preview deployment changes to Geolocation, File List, and Security Intelligence objects. Updated screen: **Deploy** > **Deployment**. In the **Preview** column, click the **Preview** icon for a device to see the changes to the file list objects.
Integrations	

Feature	Details
Support for Cisco ACI Endpoint Update App, Version 2.0 and remediation module.	Version 2.0 of the Cisco ACI Endpoint Update App has the following improvements over previous versions: • The minimum update interval (how often the app updates the FMC) is now 10 seconds. Previously, it was 30 seconds. • The site prefix (a string that creates a network group object on the FMC associated with each APIC tenant) is now limited to 10 characters. Previously, it was 5 characters. A new Cisco ACI Endpoint remediation module is also available with this update.
Usability, Performance, and Troubleshooting	
Health monitoring enhancements.	We updated the health monitor as follows: • The health policy editor now groups similar health modules. You can enable and disable entire module groups. • The health policy exclusion editor is updated for better usability. Also, when you exclude a device or health module from alerting, you can now specify a time period for the exclusion, from 15 minutes to permanently. • The health monitor alert editor is updated for better usability. • The health policy deployment interface is updated for better usability. **Note** To use the updated health monitor, you must enable REST API access on **System** (⚙) > **Configuration** > **REST API Preferences**. New/modified screens: • **System** (⚙) > **Health** > **Policy** > **Edit Policy** • **System** (⚙) > **Health** > **Exclude** • **System** (⚙) > **Health** > **Monitor Alerts** • **System** (⚙) > **Health** > **Policy** > **Deploy Policy**
Deployment history enhancements.	You can now bookmark a deployment job, edit the deployment notes for a job, and generate a report.
Global search enhancements.	Global search now has the following capabilities: • You can search the full text of FMC walkthroughs (*how-tos*). • You can search extended community list names or configured values. • You can restrict searches by domain.
Snort 3 support for statistics on start-of-flow and end-of-flow events.	For FTD with Snort 3, the output of the **show snort statistics** command now reports statistics on start-of-flow and end-of-flow events.

Feature	Details
Deprecated Features	
End of support: FMC 1000, 2500, 4500.	You cannot run Version 7.1+ on the FMC models FMC 1000, 2500, and 4500. You cannot manage Version 7.1+ devices with these FMCs.
End of support: ASA 5508-X and 5516-X.	You cannot run Version 7.1+ on the ASA 5508-X or 5516-X.
End of support: NGIPS software (ASA FirePOWER/NGIPSv).	Version 7.1 is supported on the FMC and on FTD devices only. It is not supported on ASA FirePOWER or NGIPSv devices. You can still use a Version 7.1 FMC to manage older devices — FTD as well as ASA FirePOWER and NGIPSv — that are running Version 6.5 through 7.0.
Deprecated (temporary): Improved SecureX integration, SecureX orchestration.	**Upgrade impact. Cannot upgrade to Version 7.1.0 with new SecureX integration.** This feature is included in Versions 7.0.2+ and 7.2+. It is not supported in Version 7.1. If you use the new method to enable SecureX integration in Version 7.0.x, you cannot upgrade to Version 7.1 unless you disable the feature. We recommend you upgrade to Version 7.2+.
Deprecated: Intrusion incidents and the intrusion event clipboard.	**Upgrade impact. Data and configurations can be deleted.** We removed the intrusion incidents feature and the related intrusion event clipboard. The upgrade removes all data related to incidents, and deletes report templates sections that use the clipboard as a data source. Deprecated screens/options: • **Analysis > Intrusions > Incidents** • **Analysis > Intrusions > Clipboard** • **Copy** and **Copy All** on intrusion event workflow pages and packet views • When adding sections to a report template (**Overview > Reporting > Report Templates)**, you can no longer choose the **Clipboard** table as a data source.
Deprecated: Custom tables for intrusion events.	**Upgrade impact. Custom tables can be deleted.** Version 7.1 ends support for custom tables for intrusion events. The upgrade deletes custom tables that contain fields from the intrusion event table. When adding fields to a custom table (**Analysis > Advanced > Custom Tables**), you can no longer choose the **Intrusion Events** table as a data source.
Deprecated: ECMP zones with FlexConfig.	**Upgrade impact. Redo FlexConfigs after upgrade.** You can now group interfaces in traffic zones and configure Equal-Cost-Multi-Path (ECMP) routing in the FMC web interface. After upgrade, the system ignores ECMP zones configured with FlexConfig. You cannot deploy with equal-cost static routes exist and must assign their interfaces to an ECMP zone.

Feature	Details
Deprecated: Policy based routing with FlexConfig.	**Upgrade impact. Redo FlexConfigs after upgrade.** You can now configure policy based routing (PBR) from the FMC web interface. This feature requires Version 7.1+ on both the FMC and the device. When you upgrade the FMC to Version 7.1+, existing policy based routing FlexConfigs are removed. After you upgrade your devices to Version 7.1+, redo your policy based routing configurations in the FMC web interface. For devices that you do not upgrade to Version 7.1+, redo the FlexConfigs and configure them to deploy "every time."
Deprecated: Geolocation details.	We no longer provide the geolocation IP package, which contained contextual data associated with routable IP addresses. This saves disk space and does not affect geolocation rules or traffic handling in any way. Any contextual data is now stale, and upgrading to most later versions deletes the IP package. Options to download the IP package or view contextual data have no effect, and are removed in later versions.

FMC Features in Version 7.0.9

There are no new features in this release.

FMC Features in Version 7.0.9

There are no new features in this release.

FMC Features in Version 7.0.8

Table 66: FMC Features in Version 7.0.8

Feature	Minimum FMC	Minimum FTD	Details
Licensing			
Updated internet access requirements for Smart Licensing.	7.0.8 7.2.10 7.3.0	Any	**Upgrade impact. The system connects to new resources.** When communicating with the Cisco Smart Software Manager, the Firewall Management Center now connects to smartreceiver.cisco.com instead of tools.cisco.com.

FMC Features in Version 7.0.7

Table 67: FMC Features in Version 7.0.7

Feature	Minimum FMC	Minimum FTD	Details
Access Control: File and Malware			
New Cisco AMP cloud connection method. Deprecated Cisco AMP Cloud connection backups.	7.0.7 7.2.10 7.4.3 7.6.1 7.7.0	Any	**Upgrade impact. The system connects to new resources. US public cloud connections replace AMP private cloud connections.** We replaced the AMP cloud connection method with one that is more secure, as well as easier to maintain and enhance. As a result of these changes: • The system connects to new resources. Success is reported in the Message Center (as Update Legacy AMP Public Cloud Connections). See the section for *Secure Firewall (AMP For Networks)* on Required Server Addresses for Proper Cisco Secure Endpoint & Malware Analytics Operations. • AMP cloud connections, both public and private, are no longer included in Firewall Management Center configuration backups. You must reconfigure them after restore. • Upgrade to any supported version replaces AMP private cloud connections with US public cloud connections. Pre-upgrade, the readiness check fails once if you have private AMP connections. Except in Version 7.0.x, the AMP for Endpoints Status and AMP for Network Status health modules alert you if any connections were deleted. **Tip** To avoid this, delete private cloud connections before upgrade and reconnect after upgrade. Use **Integration** > **AMP Management**.
Administration			
Security Cloud Control regions: India and Australia.	7.0.7 7.2.9 7.4.3 7.6.0	7.0.7 7.2.9 7.4.3 7.6.0	Security Cloud Control integration now supports the India and Australia regional clouds. New/modified screens: • Version 7.6.0+ : **Integration** > **Cisco Security Cloud** > **Current Region** • Version 7.4.x and earlier: **Integration** > **SecureX** > **Current Region**
Security and Hardening			

Feature	Minimum FMC	Minimum FTD	Details
Require the Message-Authenticator attribute in all RADIUS responses.	7.0.7 7.2.10 7.4.3 7.6.1 7.7.0	7.0.7 7.2.10 7.4.3 7.6.1 7.7.0	**Upgrade impact. For the Firepower 4100/9300, check FXOS compatibility before you upgrade Firewall Threat Defense. After Firewall Threat Defense upgrade, enable the option for existing servers.** You can now require the Message-Authenticator attribute in all RADIUS responses, ensuring that the Firewall Threat Defense VPN gateway securely verifies every response from the RADIUS server, whether for RA VPN or access to the device itself. The **RADIUS Server-Enabled Message Authenticator** option is enabled by default for new RADIUS servers. We also recommend you enable it for existing servers. Disabling it may expose firewalls to potential attacks. New/modified screens: • **Objects** > **AAA Server** > **RADIUS Server Group** > **Add RADIUS Server Group** > **Add RADIUS Server** • **System** (⚙) > **Users** > **External Authentication** > **Add External Authentication Object (RADIUS)** New CLI commands: **message-authenticator-required** Version restrictions: For the Firepower 4100/9300, this feature may require an FXOS upgrade. For minimum builds, see *Cisco Secure Firewall Threat Defense Compatibility Guide*. Other restrictions: This feature introduced a login bug where the Firewall Management Center treats the RADIUS Class attribute (25) as octets instead of a string, which can break role mapping and cause login failures. For a list of fixed releases, or a workaround if you cannot upgrade, see CSCwq03404.

FMC Features in Version 7.0.6

Table 68: FMC Features in Version 7.0.6

Feature	Minimum FMC	Minimum FTD	Details
Access Control: Threat Detection and Application Identification			

Feature	Minimum FMC	Minimum FTD	Details
Smaller VDB for lower memory Snort 2 devices.	6.4.0.17 7.0.6 7.2.4 7.3.1.1 7.4.0	Any with Snort 2	**Upgrade impact. Application identification on lower memory devices is affected.** For VDB 363+, the system now installs a smaller VDB (also called *VDB lite*) on lower memory devices running Snort 2. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Lower memory devices: ASA 5506-X series, ASA-5508-X, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X Version restrictions: The ability to install a smaller VDB depends on the version of the Firewall Management Center, not managed devices. If you upgrade the Firewall Management Center from a supported version to an unsupported version, you cannot install VDB 363+ if your deployment includes even one lower memory device. For a list of affected releases, see CSCwd88641.
Administration			
Updated web analytics provider.	7.0.6 7.2.6 7.4.1	Any	**Upgrade impact. Your browser connects to new resources.** While using the Firewall Management Center, your browser now contacts Amplitude (amplitude.com) instead of Google (google.com) for web analytics. Web analytics provides non-personally-identifiable usage data to Cisco, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your Firewall Management Centers. You are enrolled in web analytics by default but you can change your enrollment at any time after you complete initial setup. Note that ad blockers can block web analytics, so if you choose to remain enrolled, please disable ad blocking for the hostnames/IP addresses of your Cisco appliances.
Deprecated Features			
Deprecated: `high unmanaged disk usage` alerts.	7.0.6 7.2.4 7.4.0	7.0.6 7.2.4 7.4.0	The Disk Usage health module no longer alerts with `high unmanaged disk usage`. After FMC upgrade, you may continue to see these alerts until you either deploy health policies to managed devices (stops the display of alerts) or upgrade the devices (stops the sending of alerts). **Note** Versions 7.0–7.0.5, 7.1.x, 7.2.0–7.2.3, and 7.3.x continue to support these alerts. If your Firewall Management Center is running any of these versions, you may also continue to see alerts. For information on the remaining Disk Usage alerts, see Disk Usage and Drain of Events Health Monitor Alerts.

FMC Features in Version 7.0.5

Table 69: FMC Features in Version 7.0.5

Feature	Minimum FMC	Minimum FTD	Details
ISA 3000 System LED support for shutting down.	Any	7.0.5 7.3.0	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.
Automatically update CA bundles.	7.0.5 7.1.0.3 7.2.4 7.3.0	7.0.5 7.1.0.3 7.2.4 7.3.0	**Upgrade impact. The system connects to new resources.** The local CA bundle contains certificates to access several Cisco services. The system now automatically queries Cisco for new CA certificates at a daily system-defined time. Previously, you had to upgrade the software to update CA certificates. You can use the CLI to disable this feature. New resources: https://cisco.com/security/pki/ New/modified CLI commands: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** See: Firepower Management Center Command Line Reference and *Cisco Secure Firewall Threat Defense Command Reference*

FMC Features in Version 7.0.4

There are no new features in this release.

FMC Features in Version 7.0.3

Table 70: FMC Features in Version 7.0.3

Feature	Minimum FMC	Minimum FTD	Details
Threat defense support for Cloud-Delivered Firewall Management Center.	7.2.0 for analytics-only support	7.0.3 7.2.0	Version 7.0.3–7.0.x and 7.2.0+ threat defense devices support management by the Cloud-Delivered Firewall Management Center in Security Cloud Control. cannot manage Firewall Threat Defense devices running Version 7.1, or Classic devices running any version. You cannot upgrade a cloud-managed device from Version 7.0.x to Version 7.1 unless you unregister and disable cloud management. We recommend you upgrade directly to a later version. **Important** ended support for Version 7.0.x Firewall Threat Defense devices on December 15, 2025. For more information, see FAQ and Support. New/modified CLI commands: **configure manager add**, **configure manager delete**, **configure manager edit**, **show managers** For more information, see *Cisco Security Cloud Control: Secure Firewall Threat Defense Management*.

FMC Features in Version 7.0.2

Table 71: FMC Features in Version 7.0.2

Feature	Minimum FMC	Minimum FTD	Details
ISA 3000 support for shutting down.	Any	7.0.2 7.2.0	You can now shut down the ISA 3000; previously, you could only reboot the device.
Dynamic object names now support the dash character.	7.0.2 7.1.0	7.0.2 7.1.0	Dynamic object names now support the dash character. This is especially useful if you are using the ACI endpoint update app (where the dash character is allowed), to create dynamic objects on the FMC that represent tenant endpoint groups.

Feature	Minimum FMC	Minimum FTD	Details
Improved SecureX integration, SecureX orchestration.	7.0.2 7.2.0	Any	**Upgrade impact. Cannot upgrade Version 7.0.x → 7.1 with feature enabled.** We have streamlined the SecureX integration process. Now, as long as you already have a SecureX account, you just choose your cloud region on the new **Integration > SecureX** page, click **Enable SecureX**, and authenticate to SecureX. The option to send events to the cloud, as well as to enable Cisco Success Network and Cisco Support Diagnostics, are also moved to this new page. When you enable SecureX integration on this new page, licensing and management for the system's cloud connection switches from Cisco Smart Licensing to SecureX. If you already enabled SecureX the "old" way, you must disable and re-enable to get the benefits of this cloud connection management. Note that this page also governs the cloud region for and event types sent to the Secure Network Analytics (Stealthwatch) cloud using Security Analytics and Logging (SaaS), even though the web interface does not indicate this. Previously, these options were on **System**(⚙) **> Integration > Cloud Services**. Enabling SecureX does not affect communications with the Secure Network Analytics cloud; you can send events to both. The Firewall Management Center also now supports SecureX orchestration—a powerful drag-and-drop interface you can use to automate workflows across security tools. After you enable SecureX, you can enable orchestration. As part of this feature, you can no longer use the REST API to configure SecureX integration. You must use the FMC web interface. Version restrictions: Not supported with Version 7.0.0-7.0.1, 7.1.x. If you use the new method to enable SecureX integration in Version 7.0.x, you cannot upgrade to Version 7.1 unless you disable the feature. We recommend you upgrade to Version 7.2+. See: *Cisco Secure Firewall Threat Defense and SecureX Integration Guide*

Feature	Minimum FMC	Minimum FTD	Details
Web interface changes: SecureX, threat intelligence, and other integrations.	7.0.2 7.2.0	Any	We changed these FMC menu options. **AMP > AMP Management** is now **Integration > AMP > AMP Management** **AMP > Dynamic Analysis Connections** is now **Integration > AMP > Dynamic Analysis Connections** **Intelligence > Sources** is now **Integration > Intelligence > Sources** **Intelligence > Elements** is now **Integration > Intelligence > Elements** **Intelligence > Settings** is now **Integration > Intelligence > Settings** **Intelligence > Incidents** is now **Integration > Intelligence > Incidents** **System (⚙) > Integration** is now **Integration > Other Integrations** **System (⚙) > Logging > Security Analytics & Logging** is now **Integration > Security Analytics & Logging** **System (⚙) > SecureX** is now **Integration > SecureX**

FMC Features in Version 7.0.1

Table 72: FMC Features in Version 7.0.1

Feature	Minimum FMC	Minimum FTD	Details
Device Management			
New default password for ISA 3000 with ASA FirePOWER Services.	7.0.1 7.1.0	7.0.1 7.1.0	For new devices, the default password for the admin account is now Adm!n123. Previously, the default admin password was Admin123. Upgrading or reimaging to Version 7.0.1+ does not change the password. However, we do recommend that all user accounts—especially those with Admin access—have strong passwords.
Access Control: Threat Detection and Application Identification			

Feature	Minimum FMC	Minimum FTD	Details
Snort 3 rate_filter inspector.	7.0.1 7.1.0	7.0.1 7.1.0	We introduced the Snort 3 rate_filter inspector. This allows you to change the action of an intrusion rule in response to excessive matches on that rule. You can block rate-based attacks for a specific length of time, then return to allowing matching traffic while still generating events. For more information, see the Snort 3 Inspector Reference. New/modified pages: Configure the inspector by editing the Snort 3 version of a custom network analysis policy. Version restrictions: Requires lsp-rel-20210816-1910 or later.

FMC Features in Version 7.0.0

Table 73: FMC Features in Version 7.0.0

Feature	Minimum FMC	Minimum FTD	Details
Platform			
VMware vSphere/VMware ESXi 7.0 support.	7.0	7.0	You can now deploy FMCv, FTDv, and NGIPSv virtual appliances on VMware vSphere/VMware ESXi 7.0. Note that Version 7.0 also discontinues support for VMware 6.0. Upgrade the hosting environment to a supported version before you upgrade the Firepower software.
FMCv for HyperFlex, Nutanix, and OpenStack.	7.0	Any	We now support FMCv2, v10, and v25 for Cisco HyperFlex, Nutanix Enterprise Cloud, and OpenStack. FMCv for HyperFlex supports high availability with FMCv10 and v25. If you are managing FTD devices, you need two identically licensed FMCs, as well as one FTD entitlement for each managed device. For example, to manage 10 devices with an FMCv10 high availability pair, you need two FMCv10 entitlements and 10 FTD entitlements. If you are managing Classic devices only (NGIPSv or ASA FirePOWER), you do not need FMCv entitlements.
FTDv for HyperFlex, Nutanix, and OpenStack.	7.0	7.0	We now support FTDv for Cisco HyperFlex, Nutanix Enterprise Cloud, and OpenStack.

Feature	Minimum FMC	Minimum FTD	Details
FTDv performance tiered Smart Licensing.	7.0	7.0	**Upgrade impact. Upgrading automatically assigns devices to the FTDv Variable tier.** FTDv now supports performance-tiered Smart Software Licensing, based on throughput requirements and RA VPN session limits. Options run from FTDv5 (100 Mbps/50 sessions) to FTDv100 (16 Gbps/10,000 sessions). Before you add a new device, make sure your account contains the licenses you need. To purchase additional licenses, contact your Cisco representative or partner contact. Upgrading FTDv to Version 7.0 automatically assigns the device to the FTDv Variable tier, although you can change this later. For more information on changing performance tiers, supported instances, throughputs, and other hosting requirements, see the appropriate *Getting Started Guide*. New/modified pages: • You can now specify a performance tier when adding or editing an FTDv device on the **Device > Device Management** page. • You can bulk-edit performance tiers on **System** (⚙) > **Licenses** > **Smart Licenses** > page.
FTD Clustering			
Improved PAT port block allocation for clustering	7.0	7.0	The improved PAT port block allocation ensures that the control unit keeps ports in reserve for joining nodes, and proactively reclaims unused ports. To best optimize the allocation, you can set the maximum nodes you plan to have in the cluster using the **cluster-member-limit** command using FlexConfig. The control unit can then allocate port blocks to the planned number of nodes, and it will not have to reserve ports for extra nodes you don't plan to use. The default is 16 nodes. You can also monitor syslog 747046 to ensure that there are enough ports available for a new node. New/modified commands: **cluster-member-limit** (FlexConfig), **show nat pool cluster [summary]**, **show nat pool ip detail** Supported platforms: Firepower 4100/9300
FTD CLI **show cluster history** improvements.	7.0	7.0	New keywords allow you to customize the output of the **show cluster history** command. New/modified commands: **show cluster history** [**brief**] [**latest**] [**reverse**] [**time**] Supported platforms: Firepower 4100/9300
FTD CLI command to permanently leave a cluster.	7.0	7.0	You can now use the FTD CLI to permanently remove a unit from the cluster, converting its configuration to a standalone device. New/modified commands: **cluster reset-interface-mode** Supported platforms: Firepower 4100/9300

Feature	Minimum FMC	Minimum FTD	Details
FTD NAT			
Prioritized system-defined NAT rules for FTD.	7.0	7.0	We added a new Section 0 to the NAT rule table. This section is exclusively for the use of the system. Any NAT rules that the system needs for normal functioning are added to this section, and these rules take priority over any rules you create. Previously, system-defined rules were added to Section 1, and user-defined rules could interfere with proper system functioning. You cannot add, edit, or delete Section 0 rules, but you will see them in **show nat detail** command output.
FTD Routing			
Virtual router support for the ISA 3000.	7.0	7.0	You can now configure up to 10 virtual routers on an ISA 3000 device.
FTD VPN: Site to Site			
Backup virtual tunnel interfaces (VTI) for route-based site-to-site VPN.	7.0	6.7	When you configure a site-to-site VPN that uses virtual tunnel interfaces, you can select a backup VTI for the tunnel. Specifying a backup VTI provides resiliency, so that if the primary connection goes down, the backup connection might still be functional. For example, you could point the primary VTI to the endpoint of one service provider, and the backup VTI to the endpoint of a different service provider. New/modified pages: We added the ability to add a backup VTI to the site-to-site VPN wizard when you select Route-Based as the VPN type for a point-to-point connection.
FTD VPN: Remote Access			
Load balancing.	7.0	7.0	We now support RA VPN load balancing. The system distributes sessions among grouped devices by number of sessions; it does not consider traffic volume or other factors. New/modified screens: We added load balancing options to the Advanced settings in an RA VPN policy.

Feature	Minimum FMC	Minimum FTD	Details
Local authentication.	7.0	7.0	We now support local authentication for RA VPN users. You can use this as the primary or secondary authentication method, or as a fallback in case the configured remote server cannot be reached. **1.** Create a local realm. Local usernames and passwords are stored in local realms. When you create a realm (**System** (⚙) > **Integration** > **Realms**) and select the new **LOCAL** realm type, the system prompts you to add one or more local users. **2.** Configure RA VPN to use local authentication. Create or edit an RA VPN policy (**Devices > VPN > Remote Access**), create a connection profile within that policy, then specify **LOCAL** as the primary, secondary, or fallback authentication server in that connection profile. **3.** Associate the local realm you created with an RA VPN policy. In the RA VPN policy editor, use the new **Local Realm** setting. Every connection profile in the RA VPN policy that uses local authentication will use the local realm you specify here.
Dynamic access policies.	7.0	Any	The new dynamic access policy allows you to configure remote access VPN authorization that automatically adapts to a changing environment: **1.** Configure HostScan by uploading the AnyConnect HostScan package as an AnyConnect file (**Objects > Object Management > VPN > AnyConnect File**). There is a new **HostScan Package** option in the **File Type** drop-down list. This module runs on endpoints and performs a posture assessment that the dynamic access policy will use. **2.** Create a dynamic access policy (**Devices > Dynamic Access Policy**). Dynamic access policies specify session attributes (such as group membership and endpoint security) that you want to evaluate each time a user initiates a session. You can then deny or grant access based on that evaluation. **3.** Associate the dynamic access policy you created with an RA VPN policy. In the remote access VPN policy editor, use the new **Dynamic Access Policy** setting.
Multi-certificate authentication.	7.0	7.0	We now support multi-certificate authentication for remote access VPN users. You can validate the machine or device certificate, to ensure the device is a corporate-issued device, in addition to authenticating the user's identity certificate to allow VPN access using the AnyConnect client during SSL or IKEv2 EAP phase.

Feature	Minimum FMC	Minimum FTD	Details
AnyConnect custom attributes.	7.0	7.0	We now support AnyConnect custom attributes, and provide an infrastructure to configure AnyConnect client features without adding explicit support for these features in the system.
Access Control: Threat Detection and Application Identification			
Snort 3 for FTD.	7.0	7.0	For new FTD deployments, Snort 3 is now the default inspection engine. Upgraded deployments continue to use Snort 2, but you can switch at any time. Advantages to using Snort 3 include, but are not limited to: • Improved performance. • Improved SMBv2 inspection. • New script detection capabilities. • HTTP/2 inspection. • Custom rule groups. • Syntax that makes custom intrusion rules easier to write. • Reasons for 'would have dropped' inline results in intrusion events. • No Snort restarts when deploying changes to the VDB, SSL policies, custom application detectors, captive portal identity sources, and TLS server identity discovery. • Improved serviceability, due to Snort 3-specific telemetry data sent to Cisco Success Network, and to better troubleshooting logs. A Snort 3 intrusion rule update is called an *LSP* (Lightweight Security Package) rather than an SRU. The system still uses SRUs for Snort 2; downloads from Cisco contain both the latest LSP and SRU. The system automatically uses the appropriate rule set for your configurations. The FMC can manage a deployment with both Snort 2 and Snort 3 devices, and will apply the correct policies to each device. However, unlike Snort 2, you cannot update Snort 3 on a device by upgrading the FMC only and then deploying. With Snort 3, new features and resolved bugs require you upgrade the software on the FMC *and* its managed devices. For information on the Snort included with each software version, see the *Bundled Components* section of the Cisco Firepower Compatibility Guide. **Important** Before you switch to Snort 3, we *strongly* recommend you read and understand the Firepower Management Center Snort 3 Configuration Guide. Pay special attention to feature limitations and migration instructions. Although upgrading to Snort 3 is designed for minimal impact, features do not map exactly. Careful planning and preparation can help you make sure that traffic handled as expected. You can also visit the Snort 3 website: https://snort.org/snort3.

Feature	Minimum FMC	Minimum FTD	Details
Access Control: Identity			
Cross-domain trust for Active Directory domains.	7.0	Any	You can now configure user identity rules with users from Microsoft Active Directory forests (groupings of AD domains that trust each other). New/modified pages: • You now configure a realm and directories at the same time. • A new Sync Results page (**System** (⚙) > **Integration** > **Sync Results**) displays any errors related to downloading users and groups in a cross-domain trust relationship.
Event Logging and Analysis			
Improved process for storing events in a Secure Network Analytics on-prem deployment.	7.0	7.0	A new Cisco Security Analytics and Logging (On Premises) app and a new FMC wizard make it easier to configure remote data storage for on-prem Secure Network Analytics solutions: **1.** Deploy hardware or virtual Stealthwatch appliances. You can use a Stealthwatch Management Console alone, or you can configure Stealthwatch Management Console, flow collector, and data store. **2.** Install the new Cisco Security Analytics and Logging (On Premises) app on your Stealthwatch Management Console to configure Stealthwatch as a remote data store. **3.** On the FMC, use one of the new wizards on **System** (⚙) > **Logging** > **Security Analytics & Logging** to connect to your Stealthwatch deployment. Note that the wizards replace the narrower-focus page where you used to configure Stealthwatch contextual cross-launch; that is now a step in the wizard. For upgraded deployments where you were using syslog to send Firepower events to Stealthwatch, disable those configurations before you use the wizard. Otherwise, you will get double events. To remove the syslog connection to Stealthwatch use FTD platform settings (**Devices > Platform Settings**); to disable sending events to syslog, edit your access control rules. For more information, including Stealthwatch hardware and software requirements, see *Cisco Security Analytics and Logging (On Premises): Firewall Event Integration Guide*.

Feature	Minimum FMC	Minimum FTD	Details
Work with events stored remotely in a Secure Network Analytics on-prem deployment.	7.0	Any	You can now use the FMC to work with connection events stored remotely in a Secure Network Analytics on-prem deployment. A new **Data Source** option on the connection events page (**Analysis > Connections > Events**) and in the unified event viewer (**Analysis > Unified Events**) allows you to choose which connection events you want to work with. The default is to display locally stored connection events, unless there are none in the time range. In that case, the system displays remotely stored events.. We also added a data source option to report templates (**Overview > Reporting > Report Templates**), so that you can generate reports based on remotely stored connection events. **Note** This feature is supported for connection events only; cross-launch is still the only way to examine remotely stored Security Intelligence, intrusion, file and malware events. Even in the unified event viewer, the system only displays locally stored events of those types. However, note that for every Security Intelligence event, there is an identical connection event—these are the events with reasons such as 'IP Block' or 'DNS Block.' You can work with those duplicated events on the connection events page or in the unified event viewer, but not on the dedicated Security Intelligence events page.
Store all connection events in the Secure Network Analytics cloud.	7.0	Any	You can now store all connection events in the Stealthwatch cloud using Cisco Security Analytics and Logging (SaaS). Previously, you were limited to security events: Security Intelligence, intrusion, file, and malware events, as well as their associated connection events. To change the events you send to the cloud, choose **System** (⚙) **> Integration**. On the **Cloud Services** tab, edit the **Cisco Cloud Event Configuration**. The old option to send high priority connection events to the cloud has been replaced with a choice of **All**, **None**, or **Security Events**. **Note** These settings also control which events you send to SecureX. However, even if you choose to send all connection events to the cloud, SecureX consumes only the security (higher priority) connection events. Also note that you now configure the SecureX connection itself on **Analysis > SecureX**.
Unified event viewer.	7.0	Any	The unified event viewer (**Events & Logs** > **Analysis** > **Unified Events**) displays connection, Security Intelligence, intrusion, file, and malware events in a single table. This can help you look relationships between events of different types. A single search field allows you to dynamically filter the view based on multiple criteria, and a **Go Live** option displays events received from managed devices in real time.

Feature	Minimum FMC	Minimum FTD	Details
SecureX ribbon.	7.0	Any	The SecureX ribbon on the FMC pivots into SecureX for instant visibility into the threat landscape across your Cisco security products. To connect with SecureX and enable the ribbon, use **System** (⚙) > **SecureX**. Note that you must still use **System** (⚙) > **Integration** > **Cloud Services** to choose your cloud region and to specify which events to send to SecureX. For more information, see the *Cisco Secure Firewall Threat Defense and SecureX Integration Guide*.
Exempt all connection events from rate limiting when you turn off local storage.	7.0	Any	Event rate limiting applies to all events sent to the FMC, with the exception of security events: Security Intelligence, intrusion, file, and malware events, as well as their associated connection events. Now, disabling local connection event storage exempts *all* connection events from rate limiting, not just security events. To do this, set the **Maximum Connection Events** to zero on **System** (⚙) > **Configuration** > **Database**. **Note** Other than turning it off by setting it to zero, **Maximum Connection Events** does not govern connection event rate limiting. Any non-zero number in this field ensures that *all* lower-priority connection events are rate limited. Note that disabling local event storage does not affect remote event storage, nor does it affect connection summaries or correlation. The system still uses connection event information for features like traffic profiles, correlation policies, and dashboard displays.
Port and protocol displayed together in file and malware event tables.	7.0	Any	In file and malware event tables, the port field now displays the protocol, and you can search port fields for protocol. For events that existed before upgrade, if the protocol is not known, the system uses "tcp." New/modified pages: • **Analysis** > **Files** > **Malware Events** • **Analysis** > **Files** > **File Events**
Health Monitoring			

Feature	Minimum FMC	Minimum FTD	Details
New health modules.	7.0	Module dependent	We added the following health modules: • AMP Connection Status • AMP Threat Grid Status • ASP Drop • Advanced Snort Statistics • Chassis Status FTD • Event Stream Status • FMC Access Configuration Changes • FMC HA Status (replaces HA Status) • FTD HA Status • File System Integrity Check • Flow Offload • Hit Count • MySQL Status • NTP Status FTD • Rabbit MQ Status • Routing Statistics • SSE Connection Status • Sybase Status • Unresolved Groups Monitor • VPN Statistics • xTLS Counters Additionally, full support returns for the Configuration Memory Allocation module, which was introduced in Version 6.6.3 as the Appliance Configuration Resource Utilization module, but was not fully supported in Version 6.7.
Deployment and Policy Management			

Feature	Minimum FMC	Minimum FTD	Details
Dynamic objects.	7.0	7.0	You can now use *dynamic objects* in access control rules. A dynamic object is just a list of IP addresses/subnets (no ranges, no FQDN). But unlike a network object, changes to dynamic objects take effect immediately, without having to redeploy. This is useful in virtual and cloud environments, where IP addresses often dynamically map to workload resources. To create and manage dynamic objects, we recommend the Cisco Secure Dynamic Attributes Connector. The connector is a separate, lightweight application that quickly and seamlessly updates firewall policies based on workload changes. To do this, it gets workload attributes from tagged resources in your environment, and compiles an IP list based on criteria you specify (a "dynamic attributes filter"). It then creates a dynamic object on the FMC and populates it with the IP list. When your workload changes, the connector updates the dynamic object and the system immediately starts handling traffic based on the new mappings. For more information, see the *Cisco Secure Dynamic Attributes Connector Configuration Guide*. After you create a dynamic object, you can add it to access control rules on the new **Dynamic Attributes** tab in the access control rule editor. This tab replaces the narrower-focus **SGT/ISE Attributes** tab; continue to configure rules with SGT attributes here. **Note** You can also create a dynamic object on the FMC: **Objects > Object Management > External Attributes > Dynamic Objects**. However, this creates the container only; you must then populate and manage it using the REST API. See the Firepower Management Center REST API Quick Start Guide, Version 7.0. Supported virtual/cloud workloads for Cisco Secure Dynamic Attributes Connector integration: Microsoft Azure, AWS, VMware
Global search for policies and objects.	7.0	Any	You can now search for certain policies by name, and for certain objects by name and configured value. This feature is not available with the Classic theme. New/modified pages: We added capabilities to the **Search** icon and field on the FMC menu bar, to the left of the **Deploy** menu.
Selectively deploy RA and site-to-site VPN policies.	7.0	Any	Selective policy deployment, which was introduced in Version 6.6, now supports remote access and site-to-site VPN policies for FTD. New/modified pages: We added VPN policy options on the **Deploy > Deployment** page.
FTD Upgrade			
Improved FTD upgrade performance and status reporting.	7.0	7.0	FTD upgrades are now easier faster, more reliable, and take up less disk space. A new **Upgrades** tab in the Message Center provides further enhancements to upgrade status and error reporting.

Feature	Minimum FMC	Minimum FTD	Details
Upgrade wizard for FTD.	7.0	Any	A new device upgrade page (**Devices** > **Device Upgrade**) on the FMC provides an easy-to-follow wizard for upgrading Version 6.4+ FTD devices. It walks you through important pre-upgrade stages, including selecting devices to upgrade, copying the upgrade package to the devices, and compatibility and readiness checks. To begin, use the new **Upgrade Firepower Software** action on the Device Management page **Devices** > **Device Management** > **Selection**. As you proceed, the system displays basic information about your selected devices, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a device does not "pass" a stage in the wizard, it does not appear in the next stage. If you navigate away from wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the wizard. **Note** You must still use **System** > **Updates** to upload or specify the location of FTD upgrade packages. You must also use the System Updates page to upgrade the FMC itself, as well as all non-FTD managed devices. **Note** In Version 7.0, the wizard does not correctly display devices in clusters or high availability pairs. Even though you must select and upgrade these devices as a unit, the wizard displays them as standalone devices. Device status and upgrade readiness are evaluated and reported on an individual basis. This means it is possible for one unit to appear to "pass" to the next stage while the other unit or units do not. However, these devices are still grouped. Running a readiness check on one, runs it on all. Starting the upgrade on one, starts it on all. To avoid possible time-consuming upgrade failures, *manually* ensure all group members are ready to move on to the next step of the wizard before you click **Next**.
Upgrade more FTD devices at once.	7.0	Upgrades to 6.7+	The number of devices you can upgrade at once is now limited by your management network bandwidth—not the system's ability to manage simultaneous upgrades. Previously, we recommended against upgrading more than five devices at a time. **Important** Only upgrades to FTD Version 6.7+ using the FTD upgrade wizard see this improvement. If you are upgrading devices to an older FTD release—even if you are using the new upgrade wizard—we still recommend you limit to five devices at a time.

Feature	Minimum FMC	Minimum FTD	Details
Upgrade different device models together.	7.0	Any	You can now use the FTD upgrade wizard to queue and invoke upgrades for all FTD models at the same time, as long as the system has access to the appropriate upgrade packages. Previously, you would choose an upgrade package, then choose the devices to upgrade using that package. That meant that you could upgrade multiple devices at the same time *only* if they shared an upgrade package. For example, you could upgrade two Firepower 2100 series devices at the same time, but not a Firepower 2100 series and a Firepower 1000 series.
Administration and Troubleshooting			
Zero-touch restore for the ISA 3000 using the SD card.	7.0	7.0	When you perform a local backup, the backup file is copied to the SD card if present. To restore the configuration on a replacement device, simply install the SD card in the new device, and depress the Reset button for 3 to 15 seconds during the device bootup.
Security and Hardening			
New default password for AWS deployments.	7.0	7.0	For FMCv/FTDv for AWS, the default password for the admin account is now the AWS Instance ID, unless you define a default password with user data (**Advanced Details > User Data**) during the initial deployment. Previously, the default admin password was Admin123.
EST for certificate enrollment.	7.0	7.0	Support for Enrollment over Secure Transport for certificate enrollment was provided. New/modified pages: New enrollment options when configuring **Objects > PKI > Cert Enrollment > CA Information** tab.
Support for EdDSA certificate type.	7.0	7.0	A new certificate key type- EdDSA was added with key size 256. New/modified pages: New certificate key options when configuring **Objects > PKI > Cert Enrollment > Key** tab.
AES-128 CMAC authentication for NTP servers.	7.0	Any	You can now use AES-128 CMAC keys to secure connections between the FMC and NTP servers. New/modified pages: **Administration** > **Configuration** > **Time Synchronization**.
SNMPv3 users can authenticate using a SHA-224 or SHA-384 authorization algorithm.	7.0	7.0	SNMPv3 users can now authenticate using a SHA-224 or SHA-384 algorithm. New/modified pages: **Devices > Platform Settings > SNMP > Users > Auth Algorithm Type**
Usability			

Feature	Minimum FMC	Minimum FTD	Details
Report appearance has changed.	7.0	Any	To make reports appear cleaner and easier to read, we changed red color accents to gray and blue, removed background shading on table and chart titles, and removed alternating row colors in tables. New/modified pages: **Overview** > **Reporting**
How-to location has changed.	7.0	Any	**Help** > **How-Tos** now invokes walkthroughs. Previously, you clicked **How-Tos** at the bottom of the browser window.
Performance			
Hardware crypto acceleration on FTDv using Intel QuickAssist Technology (QAT).	7.0	7.0	We now support hardware crypto acceleration (CBC cipher only) on FTDv for VMware and FTDv for KVM. This feature requires a Intel QAT 8970 PCI adapter/Version 1.7+ driver on the hosting platform. After you reboot, hardware crypto acceleration is automatically enabled.
Improved CPU usage and performance for many-to-one and one-to-many connections.	7.0	7.0	The system no longer creates local host objects and locks them when creating connections, except for connections that involve dynamic NAT/PAT and scanning threat detection and host statistics. This improves FTD performance and CPU usage in situations where many connections are going to the same server (such as a load balancer or web server), or one endpoint is making connections to many remote hosts. We changed the following commands: **clear local-host** (deprecated), **show local-host**
Deprecated Features			
End of support: VMware vSphere/VMware ESXi 6.0.	7.0	7.0	We discontinued support for virtual deployments on VMware vSphere/VMware ESXi 6.0. Upgrade the hosting environment to a supported version before you upgrade the Firepower software.
Deprecated: RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm.	7.0	7.0	**Prevents post-upgrade VPN connections through FTD devices.** We removed support for RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm. Before you upgrade, use the object manager to update your PKI certificate enrollments with stronger options: **Objects > PKI > Cert Enrollment**. Otherwise, although the upgrade preserves your current settings, VPN connections through the device will fail. To continue managing older FTD devices only (Version 6.4–6.7.x) with these weaker options, select the new **Enable Weak-Crypto** option for each device on the **Devices > Certificates** page.

Feature	Minimum FMC	Minimum FTD	Details
Deprecated: MD5 authentication algorithm and DES encryption for SNMPv3 users.	7.0	7.0	**Deletes Users. Prevents post-upgrade deploy.** We removed support for the MD5 authentication algorithm and DES encryption for SNMPv3 users on FTD devices. Upgrading FTD to Version 7.0+ deletes these users from the device, regardless of the configurations on the FMC. If you are still using these options in your platform settings policy, change and verify your configurations before you upgrade FTD. These options are in the **Auth Algorithm Type** and **Encryption Type** drop-downs when creating or editing an SNMPv3 user in a Threat Defense platform settings policy: **Devices > Platform Settings**.
Deprecated: Port 32137 comms with AMP clouds.	7.0	Any	**Prevents FMC upgrade.** We deprecated the FMC option to use port 32137 to obtain file disposition data from public and private AMP clouds. Unless you configure a proxy, the FMC now uses port 443/HTTPS. Before you upgrade, disable the **Use Legacy Port 32137 for AMP for Networks** option on the **System** (⚙) > **Integration** > **Cloud Services** page. Do not proceed with upgrade until your AMP for Networks deployment is working as expected.
Deprecated: HA Status health module.	7.0	Any	We renamed the HA Status health module to the *FMC* HA Status health module. This is to distinguish it from the new FTD HA Status module.
Deprecated: Legacy API Explorer.	7.0	Any	We removed support for the FMC REST API legacy API Explorer.
Deprecated: Geolocation details.	Any	Any	We no longer provide the geolocation IP package, which contained contextual data associated with routable IP addresses. This saves disk space and does not affect geolocation rules or traffic handling in any way. Any contextual data is now stale, and upgrading to most later versions deletes the IP package. Options to download the IP package or view contextual data have no effect, and are removed in later versions.

FMC Features in Version 6.7.x

Table 74: FMC Features in Version 6.7.0

Feature	Details
Platform	

Feature	Details
FMCv and FTDv for OCI and GCP.	We introduced FMCv and FTDv for: • Oracle Cloud Infrastructure (OCI) • Google Cloud Platform (GCP)
High availability support on FMCv for VMware.	FMCv for VMware now supports high availability. You use the FMCv web interface to establish HA, just as you would on hardware models. In an FTD deployment, you need two identically licensed FMCv's, as well as one FTD entitlement for each managed device. For example, to manage 10 FTD devices with an FMCv10 HA pair, you need two FMCv10 entitlements and 10 FTD entitlements. If you are managing Classic devices only (7000/8000 series, NGIPSv, ASA FirePOWER), you do not need FMCv entitlements. Note that this feature is not supported on FMCv 2 for VMware—that is, an FMCv licensed to manage only two devices. Supported platforms: FMCv 10, 25, and 300 for VMware
Auto Scale improvements for FTDv for AWS.	Version 6.7.0 includes the following Auto Scale improvements for FTDv for AWS: • Custom Metric Publisher. A new Lambda function polls the FMC every second minute for memory consumption of all FTDv instances in the Auto Scale group, then publishes the value to CloudWatch Metric. • A new scaling policy based on memory consumption is available. • FTDv private IP connectivity for SSH and Secure Tunnel to the FMC. • FMC configuration validation. • Support for opening more Listening ports on ELB. • Modified to Single Stack deployment. All Lambda functions and AWS resources are deployed from a single stack for a streamlined deployment. Supported platforms: FTDv for AWS
Auto Scale improvements for FTDv for Azure.	The FTDv for Azure Auto Scale solution now includes support for scaling metrics based on CPU and memory (RAM), not just CPU. Supported platforms: FTDv for Azure
Firepower Threat Defense: Device Management	

Feature	Details
Manage FTD on a data interface.	You can now configure FMC management of the FTD on a data interface instead of using the dedicated management interface. This feature is useful for remote deployment when you want to manage the FTD at a branch office from an FMC at headquarters and need to manage the FTD on the outside interface. If the FTD receives a public IP address using DHCP, then you can optionally configure Dynamic DNS (DDNS) for the interface using the web type update method. DDNS ensures the FMC can reach the FTD at its Fully-Qualified Domain Name (FQDN) if the FTD's IP address changes. **Note** FMC access on a data interface is not supported with clustering or high availability. New/modified pages: • **Devices** > **Device Management** > **Device** > **Management** section • **Devices** > **Device Management** > **Interfaces** > **FMC Access** • **Devices** > **Device Management** > **DHCP** > **DDNS** > **DDNS Update Methods** page New/modified FTD CLI commands: **configure network management-data-interface**, **configure policy rollback** Supported platforms: FTD
Update the FMC IP address on the FTD.	If you change the FMC IP address, you can now use the FTD CLI to update the device. New/modified FTD CLI commands: **configure manager edit** Supported platforms: FTD
Synchronization between the FTD operational link state and the physical link state for the Firepower 4100/9300.	The Firepower 4100/9300 chassis can now synchronize the FTD operational link state with the physical link state for data interfaces. Currently, interfaces will be in an Up state as long as the FXOS admin state is up and the physical link state is up. The FTD application interface admin state is not considered. Without synchronization from FTD, data interfaces can be in an Up state physically before the FTD application has completely come online, for example, or can stay Up for a period of time after you initiate an FTD shutdown. For inline sets, this state mismatch can result in dropped packets because external routers may start sending traffic to the FTD before the FTD can handle it. This feature is disabled by default, and can be enabled per logical device in FXOS. **Note** This feature is not supported for clustering, container instances, or an FTD with a Radware vDP decorator. It is also not supported for ASA. New/modified Firepower Chassis Manager pages: **Logical Devices > Enable Link State** New/modified FXOS commands: **set link-state-sync enabled**, **show interface expand detail** Supported platforms: Firepower 4100/9300

Feature	Details
Firepower 1100/2100 series SFP interfaces now support disabling auto-negotiation.	**Upgrade impact. Check autonegotiation settings after the upgrade.** You can now configure a Firepower 1100/2100 series SFP interface to disable flow control and link status negotiation. Previously, when you set an SFP interface speed (1000 or 10000 Mbps) on these devices, flow control and link status negotiation was automatically enabled. You could not disable it. Now, you can select **No Negotiate** to disable flow control and link status negotiation. This also sets the speed to 1000 Mbps, regardless of whether you are configuring a 1 GB SFP or 10 GB SFP+ interface. You cannot disable negotation at 10000 Mbps. Note that upgrade can change your auto-negotiation settings, which may cause you to lose link. The post-upgrade deploy should re-enable it. We recommend you check interface settings before you deploy. New/modified pages: **Devices > Device Management > Interfaces >** edit interface **> Hardware Configuration > Speed** Supported platforms: Firepower 1100/2100 series
Firepower Threat Defense: Clustering	
New cluster management functionality on the FMC.	You can now use the FMC to perform the following cluster management tasks, where previously you had to use the CLI: • Enable and disable cluster units. • Show cluster status from the Device Management page, including History and Summary per unit. • Change the role to the control unit. New/modified pages: • **Devices > Device Management > More** menu • **Devices > Device Management > Cluster > General** area **> Cluster Live Status** link **> Cluster Status** Supported platforms: Firepower 4100/9300
Faster cluster deployment.	Cluster deployment now completes faster. Also, for most deployment failures, it fails more quickly. Supported platforms: Firepower 4100/9300

Feature	Details
Changes to PAT address allocation in clustering.	**Upgrade impact.** The way PAT addresses are distributed to the members of a cluster is changed. Previously, addresses were distributed to the members of the cluster, so your PAT pool would need a minimum of one address per cluster member. Now, the control instead divides each PAT pool address into equal-sized port blocks and distributes them across cluster members. Each member has port blocks for the same PAT addresses. Thus, you can reduce the size of the PAT pool, even to as few as one IP address, depending on the amount of connections you typically need to PAT. Port blocks are allocated in 512-port blocks from the 1024-65535 range. You can optionally include the reserved ports, 1-1023, in this block allocation when you configure PAT pool rules. For example, in a 4-node cluster, each node gets 32 blocks with which it will be able to handle 16384 connections per PAT pool IP address compared to a single node handling all 65535 connections per PAT pool IP address. As part of this change, PAT pools for all systems, whether standalone or operating in a cluster, now use a flat port range of 1024–65535. Previously, you could use a flat range by enabling the **Flat Port Range** option in a PAT pool rule (Pat Pool tab in an FTD NAT rule). The **Flat Port Range** option is now ignored: the PAT pool is now always flat. You can optionally select the **Include Reserved Ports** option to include the 1–1023 port range within the PAT pool. Note that if you configure port block allocation (the **Block Allocation** PAT pool option), your block allocation size is used rather than the default 512-port block. In addition, you cannot configure extended PAT for a PAT pool for systems in a cluster. This change takes effect automatically. You do not need to do anything before or after upgrade. Supported platforms: FTD
Firepower Threat Defense: Encryption and VPN	
AnyConnect module support for RA VPN.	FTD RA VPN now supports AnyConnect modules. As part of your RA VPN group policy, you can now configure a variety of optional modules to be downloaded and installed when a user downloads the Cisco AnyConnect VPN client. These modules can provide services such as web security, malware protection, off-network roaming protection, and so on. You must associate each module with a profile containing your custom configurations, created in the AnyConnect Profile Editor and uploaded to the FMC as an AnyConnect File object. New/modified pages: • Upload module profiles: We added new **File Type** options to **Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File** • Configure modules: We added **Client Modules** options to **Objects > Object Management > VPN > Group Policy >** add or edit a Group Policy object **> AnyConnect** settings Supported platforms: FTD

Feature	Details
AnyConnect management VPN tunnels for RA VPN.	FTD RA VPN now supports an AnyConnect management VPN tunnel that allows VPN connectivity to endpoints when the corporate endpoints are powered on, not just when a VPN connection is established by the end user. This feature helps administrators perform patch management on out-of-the-office endpoints, especially devices that are infrequently connected by the user, via VPN, to the office network. Endpoint operating system login scripts which require corporate network connectivity also benefit. Supported platforms: FTD
Single sign-on for RA VPN.	FTD RA VPN now supports single sign-on (SSO) for remote access VPN users configured at a SAML 2.0-compliant identity provider (IdP). New/modified pages: • Connect to an SSO server: **Objects > Object Management > AAA Server > Single Sign-on Server** • Configure SSO as part of RA VPN: We added **SAML** as an authentication method (AAA settings) when configuring an RA VPN connection profile. Supported platforms: FTD
LDAP authorization for RA VPN.	FTD RA VPN now supports LDAP authorization using LDAP attribute maps. An LDAP attribute map equates attributes that exist in the Active Directory (AD) or LDAP server with Cisco attribute names. Then, when the AD or LDAP server returns authentication to the FTD device during remote access VPN connection establishment, the FTD device can use the information to adjust how the AnyConnect client completes the connection. Supported platforms: FTD

Feature	Details
Virtual Tunnel Interface (VTI) and route-based site-to-site VPN.	FTD site-to-site VPN now supports a logical interface called Virtual Tunnel Interface (VTI). As an alternative to policy-based VPN, a VPN tunnel can be created between peers with Virtual Tunnel Interfaces configured. This supports route-based VPN with IPsec profiles attached to the end of each tunnel. This allows dynamic or static routes to be used. Using VTI does away with the requirement of configuring static crypto map access lists and mapping them to interfaces. Traffic is encrypted using static route or BGP. You can create a routed security zone, add VTI interfaces to it, and define access control rules for the decrypted traffic control over the VTI tunnel. VTI-based VPNs can be created between: • Two FTD devices • An FTD device and a public cloud • An FTD device and another FTD device with service provider redundancy New/modified pages: • **Devices** > **Device Management** > **Interfaces** > **Add Interfaces** > **Virtual Tunnel Interface** • **Devices** > **VPN** > **Site To Site** > **Add VPN** > **Firepower Threat Defense Device** > **Route Based (VTI)** Supported platforms: FTD
Dynamic RRI support for site-to-site VPN.	FTD site-to-site VPN now supports Dynamic Reverse Route Injection (RRI) supported with IKEv2-based static crypto maps in site-to-site VPN deployments. This allowed static routes to be automatically inserted into the routing process for networks and hosts protected by a remote tunnel endpoint. New/modified pages: We added the **Enable Dynamic Reverse Route Injection** advanced option when adding an endpoint to a site-to-site VPN topology. Supported platforms: FTD
Enhancements to manual certificate enrollment.	You can now obtain signed CA certificates and identity certificates from a CA authority independently of each other. We made the following changes to PKI certificate enrollment objects, which store enrollment parameters for creating Certificate Signing Requests (CSRs) and obtaining identity certificates: • We added the **CA Only** option to the manual enrollment settings for PKI certificate enrollment objects. If you enable this option, you will receive only a signed CA certificate from the CA authority, and not the identity certificate. • You can now leave the **CA Certificate** field blank in the manual enrollment settings for PKI certificate enrollment objects. If you do this, you will receive only the identity certificate from the CA authority, and not the signed CA certificate. New/modified pages: **Objects > Object Management > PKI > Cert Enrollment > Add Cert Enrollment > CA Information > Enrollment Type > Manual** Supported platforms: FTD

Feature	Details
Enhancements to FTD certificate management.	We made the following enhancements to FTD certificate management: • You can now view the chain of certifying authorities (CAs) when viewing certificate contents. • You can now export certificates. New/modified pages: • **Devices** > **Certificates** > **Status** column > **View** icon (magnifying glass) • **Devices** > **Certificates** > **Export** icon Supported platforms: FTD
Access Control: URL Filtering, Application Control, and Security Intelligence	
URL filtering and application control on traffic encrypted with TLS 1.3 (TLS Server Identity Discovery).	You can now perform URL filtering and application control on traffic encrypted with TLS 1.3, by using information from the server certificate. You do not have decrypt the traffic for this feature to work. **Note** We recommend enabling this feature if you want to perform URL filtering and application control on encrypted traffic. However, it can affect device performance, especially on lower-memory models. New/modified pages: We added a **TLS Server Identity Discovery** warning and option to the access control policy's Advanced tab. New/modified FTD CLI commands: We added the B flag to the output of the **show conn detail** command. On a TLS 1.3-encrypted connection, this flag indicates that we used the server certificate for application and URL detection. Supported platforms: FTD
URL filtering on traffic to websites with unknown reputation.	You can now perform URL filtering for websites that have an unknown reputation. New/modified pages: We added an **Apply to unknown reputation** check box to the access control, QoS, and SSL rule editors. Supported platforms: FMC
DNS filtering enhances URL filtering.	**Beta.** *DNS filtering* enhances URL filtering by determining the category and reputation of requested domains earlier in the transaction, including in encrypted traffic—but without decrypting the traffic. You enable DNS filtering per access control policy, where it applies to all category/reputation URL rules in that policy. **Note** DNS filtering is a Beta feature and may not work as expected. Do not use it in production environments. New/modified pages: We added the **Enable reputation enforcement on DNS traffic** option to the access control policy's Advanced tab, under General Settings. Supported platforms: FMC

Feature	Details
Shorter update frequencies for Security Intelligence feeds.	The FMC can now update Security Intelligence data every 5 or 15 minutes. Previously, the shortest update frequency was 30 minutes. If you configure one of these shorter frequencies on a custom feed, you must also configure the system to use an md5 checksum to determine whether the feed has updates to download. New/modified pages: We added new options to **Objects > Object Management > Security Intelligence > Network Lists and Feeds** > edit feed > **Update Frequency** Supported platforms: FMC
Access Control: User Control	
pxGrid 2.0 with ISE/ISE-PIC.	**Upgrade impact.** Use pxGrid 2.0 when you connect the FMC to an ISE/ISE-PIC identity source. If you are still using pxGrid 1.0, switch now. That version is deprecated. For use with pxGrid 2.0, Version 6.7.0 introduces the Cisco ISE Adaptive Network Control (ANC) remediation, which applies or clears ISE-configured ANC policies involved in a correlation policy violation. If you used the Cisco ISE Endpoint Protection Services (EPS) remediation with pxGrid 1.0, configure and use the ANC remediation with pxGrid 2.0. ISE remediations will not launch if you are using the 'wrong' pxGrid. The ISE Connection Status Monitor health module alerts you to mismatches. For detailed compatibility information for all supported Firepower versions, including integrated products, see the Cisco Firepower Compatibility Guide. New/modified pages: • **Policies > Actions > Modules > Installed Remediation Modules** list • **Policies > Actions > Instances > Select a module type** drop-down list Supported platforms: FMC
Realm sequences.	You can now group realms into ordered *realm sequences*. Add a realm sequence to an identity rule in the same way as you add a single realm. When applying the identity rule to network traffic, the system searches the Active Directory domains in the order specified. You cannot create realm sequences for LDAP realms. New/modified pages: **System > Integration > Realm Sequences** Supported platforms: FMC
ISE subnet filtering.	Especially useful on lower-memory devices, you can now use the CLI to exclude subnets from receiving user-to-IP and Security Group Tag (SGT)-to-IP mappings from ISE. The Snort Identity Memory Usage health module alerts when memory usage exceeds a certain level, which by default is 80%. New device CLI command: **configure identity-subnet-filter** {**add** | **remove**} Supported platforms: FMC-managed devices

Feature	Details
Access Control: Intrusion and Malware Prevention	
Improved preclassification of files for dynamic analysis.	**Upgrade impact.** The system can now decide not to submit a suspected malware file for dynamic analysis, based on the static analysis results (for example, a file with no dynamic elements). After you upgrade, in the Captured Files table, these files will have a Dynamic Analysis Status of Rejected for Analysis. Supported platforms: FMC
S7Commplus preprocessor.	The new S7Commplus preprocessor supports the widely accepted S7 industrial protocol. You can use it to apply corresponding intrusion and preprocessor rules, drop malicious traffic, and generate intrusion events. New/modified pages: • Enable the preprocessor: In the network analysis policy editor, click **Settings** (you must *click* the word 'Settings'), and enable **S7Commplus Configuration** under SCADA Preprocessors. • Configure the preprocessor: In the network analysis policy editor, under **Settings**, click **S7Commplus Configuration**. • Configure S7Commplus preprocessor rules: In the intrusion policy editor, click **Rules > Preprocessors > S7 Commplus Configurations**. Supported platforms: all FTD devices, including ISA 3000
Custom intrusion rule import warns when rules collide.	The FMC now warns you of rule collisions when you import custom (local) intrusion rules. Previously, the FMC would silently skip the rules that cause collisions—with the exception of Version 6.6.0.1, where a rule import with collisions would fail entirely. On the Rule Updates page, if a rule import had collisions, a warning icon is displayed in the Status column. For more information, hover your pointer over the warning icon and read the tooltip. Note that a collision occurs when you try to import an intrusion rule that has the same SID/revision number as an existing rule. You should always make sure that updated versions of custom rules have new revision numbers. We recommend you read the best practices for importing local intrusion rules in the FMC configuration guide. New/modified pages: We added a warning icon to **System** > **Updates** > **Rule Updates**. Supported platforms: FMC
Access Control: TLS/SSL Decryption	

Feature	Details
ClientHello modification for Decrypt - Known Key TLS/SSL rules.	**Upgrade impact.** If you configure TLS/SSL decryption, when a managed device receives a ClientHello message, the system now attempts to match the message to TLS/SSL rules that have the Decrypt - Known Key action. Previously, the system only matched ClientHello messages to Decrypt - Resign rules. The match relies on data from the ClientHello message and from cached server certificate data. If the message matches, the device modifies the ClientHello message in specific ways; see the *ClientHello Message Handling* topic in the FMC configuration guide. This behavior change occurs automatically after upgrade. If you use Decrypt - Known Key TLS/SSL rules, make sure that encrypted traffic is being handled as expected. Supported platforms: Any device
Event Logging and Analysis	
Remote data storage and cross-launch with an on-prem Stealthwatch solution.	You can now store large volumes of Firepower event data off-FMC, using an on-premises Stealthwatch solution: Cisco Security Analytics and Logging (On Premises). When viewing events in FMC, you can quickly cross-launch to view events in your remote data storage location. The FMC uses syslog to send connection, Security Intelligence, intrusion, file, and malware events. **Note** This on-prem solution is supported for FMCs running Version 6.4.0+. However, contextual cross-launch requires Firepower Version 6.7.0+. This solution also depends on availability of the Security Analytics and Logging On Prem app for the Stealthwatch Management Console (SMC), which must be running Stealthwatch Enterprise (SWE) version 7.3. Supported platforms: FMC
Quickly add Stealthwatch contextual cross-launch resources.	A new page on the FMC allows you to quickly add contextual cross-launch resources for your Stealthwatch appliance. After you add Stealthwatch resources, you manage them on the general contextual cross-launch page. This is where you continue to manually create and manage non-Stealthwatch cross-launch resources. New/modified pages: • Add Stealthwatch resources: **System > Logging > Security Analytics and Logging** • Manage resources: **Analysis > Advanced > Contextual Cross-Launch** Supported platform: FMC

Feature	Details
New cross-launch options field types.	You can now cross-launch into an external resource using the following additional types of event data: • Access control policy • Intrusion policy • Application protocol • Client application • Web application • Username (including realm) New/modified pages: • New variables when creating or editing cross-launch query links: **Analysis > Advanced > Contextual Cross-Launch**. • New data types in the dashboard and event viewer now offer cross-launch on right click. Supported platforms: FMC
National Vulnerability Database (NVD) replaces Bugtraq.	**Upgrade impact.** Bugtraq vulnerability data is no longer available. Most vulnerability data now comes from the NVD. To support this change, we made the following changes: • Added the **CVE ID** and **Severity** fields to the Vulnerabilities table. Right-clicking the CVE ID in the table view allows you to view details about the vulnerability on the NVD. • Renamed the **Vulnerability Impact** field to **Impact** (in the table view only). • Removed the obsolete/redundant **Bugtraq ID**, **Title**, **Available Exploits**, **Technical Description**, and **Solution** fields. • Removed the **Bugtraq ID** filtering option from the Hosts network map. If you export vulnerability data, make sure any integrations are working as expected after the upgrade. Supported platforms: FMC
Upgrade	

Feature	Details
Pre-upgrade compatibility check.	**Upgrade impact.** In FMC deployments, Firepower appliances must now pass pre-upgrade compatibility checks before you can run more complex readiness checks or attempt to upgrade. This check catches issues that *will* cause your upgrade to fail—but we now catch them earlier and block you from proceeding. The checks are as follows: • You cannot use the FMC to upgrade a Firepower 4100/9300 chassis to Version 6.7.0+ until you upgrade FXOS to the new release's companion FXOS version. Upgrade is blocked as long as you are upgrading the device to Version 6.7.0 or later. For example, you are *not* blocked from attempting a Firepower 4100/9300 upgrade from 6.3 → 6.6.x, even if the device is running a version of FXOS that is too old for Firepower Version 6.6.x. • You cannot use the FMC to upgrade a device if that device has out-of-date configurations. Upgrade is blocked as long as the FMC is running Version 6.7.0 or later, and you are upgrading a managed device to a valid target. For example, you *are* blocked from upgrading a device from 6.3.0 → 6.6.x if the device has outdated configurations. • You cannot upgrade an FMC *from* Version 6.7.0+ if its devices have out-of-date configurations. Upgrade is blocked as long as the FMC is running Version 6.7.0 or later. For upgrades from earlier versions (including *to* Version 6.7.0), you must make sure you deploy yourself. When you select an upgrade package to install, the FMC displays compatibility check results for all eligible appliances. The new Readiness Check page also displays this information. You cannot upgrade until you fix the issues indicated. New/modified pages: • **System** > **Update** > **Product Updates** > **Available Updates** > **Install** icon for the upgrade package • **System** > **Update** > **Product Updates** > **Readiness Checks** Supported platforms: FMC, FTD

Feature	Details
Improved readiness checks.	**Upgrade impact.** Readiness checks assess a Firepower appliance's preparedness for a software upgrade. These checks include database integrity, file system integrity, configuration integrity, disk space, and so on. After you upgrade the FMC to Version 6.7.0, you will see the following improvements to FTD upgrade readiness checks: • Readiness checks are faster. • Readiness checks are now supported on high availability and clustered FTD devices, without having to log into the device CLI. • Readiness checks for FTD device upgrades to Version 6.7.0+ no longer require the upgrade package to reside on the device. Although we still recommend you push the upgrade package to the device before you begin the upgrade itself, you no longer have to do so before you run the readiness check. • When you select an upgrade package to install, the FMC now shows the readiness status for all applicable FTD devices. A new Readiness Checks page allows you to view the results of readiness checks for the FTD devices in your deployment. You can also re-run readiness checks from this page. • Readiness check results include the estimated upgrade time (but do not include reboot time). • Error messages are better. You can also download success/failure logs from the Message Center on the FMC. Note that these improvements are supported for FTD upgrades from Version 6.3.0+, as long as the FMC is running Version 6.7.0+. New/modified pages: • **System** > **Update** > **Product Updates** > **Available Updates** > **Install** icon for the upgrade package • **System** > **Update** > **Product Updates** > **Readiness Checks** • **Message Center > Tasks** Supported platforms: FTD

Feature	Details
Improved FTD upgrade status reporting and cancel/retry options.	**Upgrade impact.** You can now view the status of device upgrades and readiness checks in progress on the Device Management page, as well as a 7-day history of upgrade success/failures. The Message Center also provides enhanced status and error messages. A new Upgrade Status pop-up, accessible from both Device Management and the Message Center with a single click, shows detailed upgrade information, including percentage/time remaining, specific upgrade stage, success/failure data, upgrade logs, and so on. Also on this pop-up, you can manually cancel failed or in-progress upgrades (**Cancel Upgrade**), or retry failed upgrades (**Retry Upgrade**). Canceling an upgrade reverts the device to its pre-upgrade state. **Note** To be able to manually cancel or retry a failed upgrade, you must disable the new auto-cancel option, which appears when you use the FMC to upgrade an FTD device: **Automatically cancel on upgrade failure and roll back to the previous version**. With the option enabled, the device automatically reverts to its pre-upgrade state upon upgrade failure. Auto-cancel is not supported for patches. In an HA or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. New/modified pages: • **System** > **Update** > **Product Updates** > **Available Updates** > **Install** icon for the FTD upgrade package • **Devices** > **Device Management** > **Upgrade** • **Message Center > Tasks** New FTD CLI commands: • **show upgrade status detail** • **show upgrade status continuous** • **show upgrade status** • **upgrade cancel** • **upgrade retry** Supported platforms: FTD

Feature	Details
Upgrades postpone scheduled tasks.	**Upgrade impact.** FMC upgrades now postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. **Note** Before you begin any upgrade, you must still make sure running tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Note that this feature is supported for all upgrades *from* a supported version. This includes Version 6.4.0.10 and later patches, Version 6.6.3 and later maintenance releases, and Version 6.7.0+. This feature is not supported for upgrades *to* a supported version from an unsupported version. Supported platforms: FMC
Upgrades remove PCAP files to save disk space.	**Upgrade impact.** To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. Upgrades now remove locally stored PCAP files. Supported platforms: Any
Deployment and Policy Management	
Configuration rollback.	**Beta.** You can now "roll back" configurations on an FTD device, replacing them with the previously deployed configurations. **Note** Rollback is a Beta feature, and is not supported in all deployment types and scenarios. It is also a disruptive operation. Make sure you read and understand the guidelines and limitations in the *Policy Management* chapter of the FMC configuration guide. New/modified pages: **Deploy > Deployment History > Rollback** column and icons. Supported platforms: FTD
Deploy intrusion and file policies independently of access control policies.	You can now select and deploy intrusion and file policies independently of access control policies, unless there are dependent changes. New/modified pages: **Deploy > Deployment** Supported platforms: FMC
Search access control rule comments.	You can now search within access control rules comments. New/modified pages: In the access control policy editor, we added the **Comments** field to the **Search Rules** drop-down dialog. Supported platforms: FMC

Feature	Details
Search and filter FTD NAT rules.	You can now search for rules in an FTD NAT policy to help you find rules based on IP addresses, ports, object names, and so forth. Search results include partial matches. Searching on criteria filters the rule table so only matching rules are displayed. New/modified pages: We added a search field above the rule table when you edit an FTD NAT policy. Supported platforms: FTD
Copy and move rules between access control and prefilter policies.	You can copy access control rules from one access control policy to another. You can also move rules between an access control policy and its associated prefilter policy. New/modified pages: In the access control and prefilter policy editors, we added **Copy** and **Move** options to each rule's right-click menu. Supported platforms: FMC
Bulk object import.	You can now bulk-import network, port, URL, VLAN tag, and distinguished name objects onto the FMC, using a comma-separated-values (CSV) file. For restrictions and specific formatting instructions, see the *Reusable Objects* chapter of the FMC configuration guide. New/modified pages: **Objects > Object Management >** choose an object type **> Add [Object Type] > Import Object** Supported platforms: FMC
Interface object optimization for access control and prefilter policies.	You can now enable interface object optimization on specific FTD devices. During deployment, interface groups and security zones used in the access control and prefilter policies generate separate rules for each source/destination interface pair. If you enable interface object optimization, the system will instead deploy a single rule per access control/prefilter rule, which can simplify the device configuration and improve deployment performance. Interface object optimization is disabled by default. If you enable it, you should also enable **Object Group Search**—which now applies to interface objects in addition to network objects—to reduce memory usage on the device. New/modified pages: **Devices** > **Device Management** > **Device** > **Advanced Settings** section **> Interface Object Optimization** check box Supported platforms: FTD
Administration and Troubleshooting	
FMC single sign-on.	The FMC now supports single sign-on (SSO) for external users configured at any third-party SAML 2.0-compliant identity provider (IdP). You can map user or group roles from the IdP to FMC user roles. New/modified pages: • **Login** > **Single Sign-On** • **System** > **Users** > **SSO** Supported platforms: FMC

Feature	Details
FMC logout delay.	When you log out of the FMC, there is an automatic five-second delay and countdown. You can click **Log Out** again to log out immediately. Supported platforms: FMC
Backup and restore for FTD container instances.	You can now use the FMC to back up and restore Version 6.7.0+ FTD container instances. Supported platforms: Firepower 4100/9300
Health monitoring enhancements.	We enhanced health monitoring as follows: • Health Status summary page that provides an at-a-glance view of the health of the Firepower Management Center and all of the devices that the FMC manages. • The Monitoring navigation pane allows you to navigate the device hierarchy. • Managed devices are listed individually, or grouped according to their geolocation, high availability, or cluster status where applicable. • You can view health monitors for individual devices from the navigation pane. • Custom dashboards to correlate interrelated metrics. Select from predefined correlation groups, such as CPU and Snort; or create a custom correlation dashboard by building your own variable set from the available metric groups. Supported platforms: FMC

Feature	Details
Health module updates.	We replaced the CPU Usage health module with four new modules: • CPU Usage (per core): Monitors the CPU usage on all of the cores. • CPU Usage Data Plane: Monitors the average CPU usage of all data plane processes on the device. • CPU Usage Snort: Monitors the average CPU usage of the Snort processes on the device. • CPU Usage System: Monitors the average CPU usage of all system processes on the device. We added the following health modules to track memory use: • Memory Usage Data Plane: Monitors the percentage of allocated memory used by data plane processes. • Memory Usage Snort: Monitors the percentage of allocated memory used by the Snort process. We added the following health modules to track statistics: • Connection Statistics: Monitors connection statistics and NAT translation counts. • Critical Process Statistics: Monitors the state of critical processes, their resource consumption, and the restart counts. • Deployed Configuration Statistics: Monitors statistics about the deployed configuration, such as the number of ACEs and IPS rules. • Snort Statistics: Monitors Snort statistics for events, flows, and packets. Supported platforms: FMC
Search Message Center.	You can now filter the current view in the Message Center. New/modified pages: We added a **Filter** icon and field to the Message Center, under the **Show Notifications** slider. Supported platforms: FMC
Usability and Performance	
Dusk theme.	**Beta.** The FMC web interface defaults to the Light theme, but you can also choose a new Dusk theme. **Note** The Dusk theme is a Beta feature. If you encounter issues that prevent you from using a page or feature, switch to a different theme. Although we cannot respond to everybody, we also welcome feedback — please use the feedback link on the User Preferences page or contact us at fmc-light-theme-feedback@cisco.com. New/modified pages: **User Preferences**, from the drop-down list under your username Supported platforms: FMC

Feature	Details
Search FMC menus.	You can now search the FMC menus. New/modified pages: We added a **Search** icon and field to the FMC menu bar, to the left of the **Deploy** menu. Supported platforms: FMC
Deprecated Features	
End of support: ASA 5525-X, 5545-X, and 5555-X devices with Firepower software.	You cannot run Version 6.7+ on the ASA 5525-X, 5545-X, and 5555-X.
Deprecated: Cisco Firepower User Agent software and identity source.	**Prevents FMC upgrade.** You cannot upgrade an FMC with user agent configurations to Version 6.7+. Version 6.6 is the last release to support the Cisco Firepower User Agent software as an identity source. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC). To convert your license, contact Sales. For more information, see the End-of-Life and End-of-Support for the Cisco Firepower User Agent announcement and the Firepower User Identity: Migrating from User Agent to Identity Services Engine TechNote. Deprecated FTD CLI commands: **configure user agent**
Deprecated: Cisco ISE Endpoint Protection Services (EPS) remediation.	**ISE remediations can stop working.** The Cisco ISE Endpoint Protection Services (EPS) remediation does not work with pxGrid 2.0. Configure and use the new Cisco ISE Adaptive Network Control (ANC) remediation instead. ISE remediations will not launch if you are using the 'wrong' pxGrid to connect the FMC to an ISE/ISE-PIC identity source. The ISE Connection Status Monitor health module alerts you to mismatches.
Deprecated: Less secure Diffie-Hellman groups, and encryption and hash algorithms.	**Prevents FMC upgrade.** You may not be able to upgrade an FMC if you use any of the following FTD features: • Diffie-Hellman groups: 2, 5, and 24. Group 5 continues to be supported in FMC deployments for IKEv1, but we recommend you change to a stronger option. • Encryption algorithms for users who satisfy export controls for strong encryption: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continues to be supported (and is the only option) for users who do not satisfy export controls. • The NULL "encryption algorithm" (authentication without encryption, for testing purposes) continues to be supported in FMC deployments for both IKEv1 and IKEv2 IPsec proposals. However, it is no longer supported in IKEv2 policies. • Hash algorithms: MD5. If you are still using these features in IKE proposals or IPsec policies, change and verify your VPN configuration before you upgrade.

Feature	Details
Deprecated: Appliance Configuration Resource Utilization heath module (temporary).	**Possible post-upgrade errors in the health monitor.** Version 6.7 *partially* and *temporarily* deprecates support for the Appliance Configuration Resource Utilization health module, which was introduced in Version 6.6.3 and is supported in all later 6.6.x releases. Version 6.7 support is as follows: • FMC upgraded to Version 6.7 from Version 6.6.3+ Continues to support the module, but only if the devices remain at Version 6.6.x. If you upgrade the devices to Version 6.7, the module stops working and the health monitor displays an error. To resolve the error, use the FMC to disable the module and reapply policies. • FMC upgraded to Version 6.7 from Version 6.3–6.6.1, *or* FMC freshly installed to Version 6.7. Does not support the module. In the rare case that you add a Version 6.6.x device that has the module enabled to an FMC where the module is not supported, the health monitor displays an error that you cannot resolve. This error is safe to ignore. Full support returns in Version 7.0, where the module is renamed to Configuration Memory Allocation.
Deprecated: Other health modules (permanent).	Version 6.7 deprecates the following health modules: • CPU Usage: Replaced by four new modules; see the new features table above. • Local Malware Analysis: This module was replaced by the Threat Data Updates on Devices module in Version 6.3. A Version 6.7+ FMC can no longer manage any devices where the older module applies. • User Agent Status Monitor: Cisco Firepower User Agent is no longer supported.
Deprecated: Walkthroughs with the Classic theme.	Version 6.7 discontinues FMC walkthroughs (*how-tos*) for the Classic theme. You can switch themes in your user preferences.
Deprecated: Bugtraq	Version 6.7 removes database fields and options for Bugtraq. Bugtraq vulnerability data is no longer available. Most vulnerability data now comes from the National Vulnerability Database (NVD). If you export vulnerability data, make sure any integrations are working as expected after the upgrade.
Deprecated: Microsoft Internet Explorer	We no longer test Firepower web interfaces using Microsoft Internet Explorer. We recommend you switch to Google Chrome, Mozilla Firefox, or Microsoft Edge.
Deprecated: Geolocation details.	We no longer provide the geolocation IP package, which contained contextual data associated with routable IP addresses. This saves disk space and does not affect geolocation rules or traffic handling in any way. Any contextual data is now stale, and upgrading to most later versions deletes the IP package. Options to download the IP package or view contextual data have no effect, and are removed in later versions.

FMC Features in Version 6.6.x

Table 75: FMC Features in Version 6.6.3

Feature	Details
Upgrades postpone scheduled tasks.	**Upgrade impact. Scheduled tasks may run after upgrade.** Upgrades now postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. **Note** Before you begin any upgrade, you must still make sure running tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Note that this feature is supported for Firepower appliances running Version 6.6.3+. It is not supported for upgrades *to* Version 6.6.3, unless you are upgrading from Version 6.4.0.10 or any later patch.
Appliance Configuration Resource Utilization health module.	Version 6.6.3 improves device memory management and introduces a new health module: Appliance Configuration Resource Utilization. The module alerts when the size of your deployed configurations puts a device at risk of running out of memory. The alert shows you how much memory your configurations require, and by how much this exceeds the available memory. If this happens, re-evaluate your configurations. Most often you can reduce the number or complexity of access control rules or intrusion policies. For information on best practices for access control, see the configuration guide. The upgrade process automatically adds and enables this module in all health policies. After upgrade, apply health policies to managed devices to begin monitoring. **Note** This module requires Version 6.6.3 or later 6.6.x release or Version 7.0+ on both the FMC and managed devices. Version 6.7 *partially* and *temporarily* deprecates support for this module. For details, see Deprecated: Appliance Configuration Resource Utilization heath module (temporary). Full support returns in Version 7.0, where the module is renamed to Configuration Memory Allocation.

Table 76: FMC Features in Version 6.6.1

Feature	Details
Deprecated Features	

Feature	Details
Deprecated: Custom intrusion rule import failure when rules collide.	In Version 6.6.0, the FMC began rejecting custom (local) intrusion rule imports entirely if there were rule collisions. Version 6.6.1 deprecates this feature, and returns to the pre-Version 6.6 behavior of silently skipping the rules that cause collisions. Note that a collision occurs when you try to import an intrusion rule that has the same SID/revision number as an existing rule. You should always make sure that updated versions of custom rules have new revision numbers. We recommend you read the best practices for importing local intrusion rules in the FMC configuration guide. Version 6.7 adds a warning for rule collisions.

Table 77: FMC Features in Version 6.6.0

Feature	Description
Platform	
Firepower 4112.	We introduced the Firepower 4112. You can also deploy ASA logical devices on this platform. Requires FXOS 2.8.1.
Larger instances for AWS deployments.	**Upgrade impact. Resize AWS instances before you upgrade.** FTDv for AWS adds support for these larger instances: • C5.xlarge • C5.2xlarge • C5.4xlarge FMCv for AWS adds support for these larger instances: • C3.4xlarge • C4.4xlarge • C5.4xlarge All existing FMCv for AWS instance types are now deprecated (c3.xlarge, c3.2xlarge, c4.xlarge, c4.2xlarge). You must resize before you upgrade. For more information, see the upgrade guidelines for Version 6.6 in the release notes.
Device Management	
Obtain initial FTD management interface IP address using DHCP.	For the Firepower 1000/2000 and ASA-5500-X, the management interface now defaults to obtaining an IP address from DHCP. This change makes it easier for you to deploy a new device on your existing network. Supported platforms: Firepower 1000/2000 and ASA-5500-X only. On the Firepower 4100/9300, you set the IP address when you deploy the logical device. The ISA 3000 and FTDv continue to default to 192.168.45.45.

Feature	Description
SNMP polling and trap support on the FTD Management interface.	FTD devices now support SNMP configuration on the Management interface and unifies the FXOS and FTD MIBs over a single interface. Previously, SNMP was available only from the Diagnostic interface or Data interfaces. And, the Firepower 1000/2000 required additional SNMP configuration on the Device Management page. New/modified screens: • New: **Devices** > **Platform Settings** > **SNMP** > **Hosts** • Deprecated: **Devices** > **Device Management** > **SNMP** Supported platforms: FTD
Interfaces	
Configure FTD MTU values in CLI.	You can now use the FTD CLI to configure MTU (maximum transmission unit) values. The default is 1500 bytes. Maximum MTU values are: • Management interface: 1500 bytes • Eventing interface: 9000 bytes New FTD CLI commands: **configure network mtu** Modified FTD CLI commands: Added the **mtu-event-channel** and **mtu-management-channel** keyword to the **configure network management-interface** command. Supported platforms: FTD
Firepower Threat Defense: High Availability/Scalability	
Autoscale for FTDv for Azure and FTDv for AWS deployments.	We introduced support for AWS Auto Scale/Azure Autoscale. The serverless infrastructure in cloud-based deployments allow you to automatically adjust the number of FTDv instances in the Auto Scale group based on capacity needs. This includes automatic registering/unregistering to and from the managing FMC.
Multi-instance FTD clustering.	You can now create a cluster using container instances. On the Firepower 9300, you must include one container instance on each module in the cluster. You cannot add more than one container instance to the cluster per security engine/module. We recommend that you use the same security module or chassis model for each cluster instance. However, you can mix and match container instances on different Firepower 9300 security module types or Firepower 4100 models in the same cluster if required. You cannot mix Firepower 9300 and 4100 instances in the same cluster. New FXOS CLI commands: **set port-type cluster** New/modified Chassis Manager pages: • **Logical Devices** > **Add Cluster** • **Interfaces** > **All Interfaces** > **Add New** drop-down menu **> Subinterface > Type** field Supported platforms: Firepower 4100/9300

Feature	Description
Parallel configuration sync to data units in FTD clusters.	The control unit in an FTD cluster now syncs configuration changes with data units in parallel by default. Formerly, synching occurred sequentially. Supported platforms: Firepower 4100/9300
Messages for FTD cluster join failure or eviction added to **show cluster history**.	We added new messages to the **show cluster history** command for when a cluster unit either fails to join the cluster or leaves the cluster. Supported platforms: Firepower 4100/9300
Firepower Threat Defense: Routing	
Virtual routers and VRF-Lite.	You can now create multiple virtual routers to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device. Virtual routers implement the "light" version of Virtual Routing and Forwarding, or VRF-Lite, which does not support Multiprotocol Extensions for BGP (MBGP). The maximum number of virtual routers you can create ranges from five to 100, and depends on the device model. New/modified pages: **Devices > Device Management** > edit device > **Routing** tab New FTD CLI commands: **show vrf**. Modified FTD CLI commands: Added the [**vrf** *name* | **all**] keyword set to the following CLI commands, and changed the output to indicate virtual router information where applicable: **clear ospf**, **clear route**, **ping**, **show asp table routing**, **show bgp**, **show ipv6 route**, **show ospf**, **show route**, **show snort counters**. Supported platforms: FTD, except Firepower 1010 and ISA 3000
Firepower Threat Defense: VPN	
DTLS 1.2 in remote access VPN.	You can now use Datagram Transport Layer Security (DTLS) 1.2 to encrypt RA VPN connections. Use FTD platform settings to specify the minimum TLS protocol version that the FTD device uses when acting as a, RA VPN server. If you want to specify DTLS 1.2, you must also choose TLS 1.2 as the minimum TLS version. Requires Cisco AnyConnect Secure Mobility Client, Version 4.7+. New/modified pages: **Devices > Platform Settings >** add/edit Threat Defense policy **> SSL > DTLS Version** option Supported platforms: FTD, except ASA 5508-X and ASA 5516-X
Site-to-site VPN IKEv2 support for multiple peers.	You can now add a backup peer to a site-to-site VPN connection, for IKEv1 and IKEv2 point-to-point extranet and hub-and-spoke topologies. Previously, you could only configure backup peers for IKEv1 point-to-point topologies. New/modified pages: **Devices > VPN > Site to Site >** add or edit a point to point or hub and spoke FTD VPN topology > add endpoint > **IP Address** field now supports comma-separated backup peers Supported platforms: FTD

Feature	Description
Security Policies	
Time-based rules in access control and prefilter policies.	You can now specify an absolute or recurring time or time range for a rule to be applied. The rule is applied based on the time zone of the device that processes the traffic. New/modified pages: • Access control and prefilter rule editors • **Devices** > **Platform Settings** > add/edit Threat Defense policy > **Time Zone** • **Objects** > **Object Management** > **Time Range** and **Time Zone** Supported platforms: FTD
Usability enhancements for security policies.	Version 6.6.0 makes it easier to work with access control and prefilter rules. You can now: • Edit certain attributes of multiple access control rules in a single operation: state, action, logging, intrusion policy, and so on. In the access control policy editor, select the relevant rules, right-click, and choose **Edit**. • Search access control rules by multiple parameters. In the access control policy editor, click the **Search Rules** text box to see your options. • View object details and usage in an access control or prefilter rule. In the access control or prefilter policy editor, right-click the rule and choose **Object Details**. Supported platforms: FMC
Event Logging and Analysis	
Wildcard support when searching connection and Security Intelligence events for URLs.	When searching connection and Security Intelligence events for URLs having the pattern `example.com`, you must now include wildcards. Specifically, use `*example.com*` for such searches. Supported platforms: FMC
Integration with IBM QRadar.	You can use the new Cisco Firepower app for IBM QRadar as an alternate way to display event data and help you analyze, hunt for, and investigate threats to your network. Requires eStreamer. For more information, see the *Integration Guide for the Cisco Firepower App for IBM QRadar*. Supported platforms: FMC
Upgrade	

Feature	Description
Get FTD upgrade packages from an internal web server.	FTD devices can now get upgrade packages from your own internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC. **Note** This feature is supported only for FTD devices running Version 6.6.0+. It is not supported for upgrades *to* Version 6.6.0, nor is it supported for the FMC or Classic devices. New/modified pages: **System > Updates > Upload Update** button > **Specify software update source** option Supported platforms: FTD
Display time remaining for upgrades.	The Message Center on the FMC now displays approximately how much time remains until an upgrade will complete. This does not include reboot time. Supported platforms: FMC
Administration	
New options for deploying configuration changes.	The **Deploy** button on the FMC menu bar is now a menu, with options that add the following functionality: • Status: For each device, the system displays whether changes need to be deployed; whether there are warnings or errors you should resolve before you deploy; and whether your last deploy is in process, failed, or completed successfully. • Preview: See all applicable policy and object changes you have made since you last deployed to the device. • Selective deploy: Choose from the policies and configurations you want to deploy to a managed device. • Deploy time estimate: Display an estimate of how long it will take to deploy to a particular device. You can display estimates for a full deploy, as well as for specific policies and configurations. • History: View details of previous deploys. New/modified pages: • **Deploy > Deployment** • **Deploy > Deployment History** Supported platforms: FMC

Feature	Description
Initial configuration updates the VDB and schedules SRU updates.	On new and reimaged FMCs, the setup process now: • Downloads and installs the latest vulnerability database (VDB) update. • Enables daily intrusion rule (SRU) downloads. Note that the setup process does *not* enable auto-deploy after these downloads, although you can change this setting. Upgraded FMCs are not affected. New/modified pages: • **System > Updates > Product Updates** (VDB updates) • **System > Updates > Rule Updates** (SRU updates) Supported platforms: FMC
VDB match no longer required to restore FMC.	Restoring an FMC from backup no longer requires the same VDB on the replacement FMC. However, restoring does now replace the existing VDB with the VDB in the backup file. Supported platforms: FMC
Real names associated with FMC user accounts.	You can now specify a real name when you create or modify an FMC user account. This can be a person's name, department, or other identifying attribute. New/modified pages: **System > Users > Users > Real Name** field. Supported platforms: FMC
FMC defaults to the Light theme.	The FMC now defaults to the Light theme, which was introduced as a Beta feature in Version 6.5.0. Upgrading to Version 6.6.0 automatically switches you to the Light theme. You can switch back to the Classic theme in your user preferences. Although we cannot respond to everybody, we welcome feedback on the Light theme. Use the feedback link on the User Preferences page or contact us at fmc-light-theme-feedback@cisco.com. Supported platforms: FMC
Security and Hardening	
HTTPS certificates with subject alternative name (SAN).	You can now request a HTTPS server certificate that secures multiple domain names or IP addresses by using SAN. For more information on SAN, see RFC 5280, section 4.2.1.6. New/modified pages: **System > Configuration > HTTPS Certificate > Generate New CSR > Subject Alternative Name** fields Supported platforms: FMC
Performance and Resiliency	

Feature	Description
Monitor up to 300,000 concurrent user sessions with FTD devices.	In Version 6.6.0, some FTD device models support monitoring of additional concurrent user sessions (logins): • 300,000 sessions: Firepower 4140, 4145, 4150, 9300 • 150,000 sessions: Firepower 2140, 4112, 4115, 4120, 4125 All other devices continue to support the old limit of 64,000, except ASA FirePOWER which is limited to 2000. A new health module alerts you when the user identity feature's memory usage reaches a configurable threshold. You can also view a graph of the memory usage over time. New/modified pages: • **System** > **Health** > **Policy** > add or edit health policy > **Snort Identity Memory Usage** • **System** > **Health** > **Monitor** > select a device > **Graph** option for the Snort Identity Memory Usage module Supported platforms: FTD devices listed above
Object group search for access control policies.	While operating, FTD devices expand access control rules into multiple access control list entries based on the contents of any network objects used in the access rule. You can reduce the memory required to search access control rules by enabling object group search. With object group search enabled, the system does not expand network objects, but instead searches access rules for matches based on those group definitions. Object group search does not impact how your rules are defined or how they appear in the FMC. It impacts only how the device interprets and processes them while matching connections to access control rules. Object group search is disabled by default. New/modified pages: **Devices** > **Device Management** > edit device > **Device** tab > **Advanced Settings** > **Object Group Search** option Supported platforms: FTD
Egress optimization re-enabled.	Version 6.6.0 fixes CSCvs86257. If egress optimization was: • Enabled but turned off, the upgrade turns it back on. (We turned off egress optimization in some Version 6.4.0.x and 6.5.0.x patches, even if the feature was enabled.) • Manually disabled, we recommend you reenable it post-upgrade: **asp inspect-dp egress-optimization**. Supported platforms: FTD

Feature	Description
New datastore on the FMC.	**Upgrade impact. Old events migrate after upgrade.** To improve performance, Version 6.6.0 uses a new datastore for connection and Security Intelligence events. After the upgrade finishes and the FMC reboots, historical connection and Security Intelligence events are migrated in the background, resource constrained. Depending on FMC model, system load, and how many events you have stored, this can take from a few hours up to a day. Historical events are migrated by age, newest events first. Events that have not been migrated do not appear in query results or dashboards. If you reach the connection event database limit before the migration completes, for example, because of post-upgrade events, the oldest historical events are not migrated. You can monitor event migration progress in the Message Center. Supported platforms: FMC
Troubleshooting	
Connection-based troubleshooting enhancements.	We made the following enhancements to FTD CLI connection-based troubleshooting (debugging): • **debug packet-module trace**: Added to enable module level packet tracing. • **debug packet-condition**: Modified to support troubleshooting of ongoing connections. Supported platforms: FTD
Cisco Support Diagnostics on additional FTD platforms.	**Upgrade impact. The system may connect to new resources.** Cisco Support Diagnostics is now fully supported on all FMCs and FTD devices. Previously, support was limited to FMCs, Firepower 4100/9300 with FTD, and FTDv for Azure. Supported platforms: FMC, FTD
Security and Hardening	
Default HTTPS server certificate renewals have 800 day lifespans.	Unless the current *default* HTTPS server certificate already has an 800-day lifespan, upgrading to Version 6.6.0 renews the certificate, which now expires 800 days from the date of the upgrade. All future renewals have an 800 day lifespan. Your old certificate was set to expire depending on when it was generated. Supported platforms: FMC
Firepower Management Center REST API	

Feature	Description
Changed REST API service name for extended access lists.	**Upgrade impact. Update your client after upgrade.** The extendedaccesslist (singular) service in the FMC REST API is now extendedaccesslist**s** (plural). Make sure you update your client. Using the old service name fails and returns an Invalid URL error. Request Type: GET URL to retrieve the extended access list associated with a specific ID: • Old: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist/{objectId} • New: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s**/{objectId} URL to retrieve a list of all extended access lists: • Old: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist • New: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s** Supported platforms: FMC
Deprecated Features	
Deprecated: Lower-memory instances for cloud-based FMCv deployments.	**Upgrade impact. Prevents upgrade.** For performance reasons, the following FMCv instances are no longer supported: • c3.xlarge on AWS • c3.2xlarge on AWS • c4.xlarge on AWS • c4.2xlarge on AWS • Standard_D3_v2 on Azure You must resize before you upgrade to Version 6.6.0+. For more information, see the upgrade guidelines for Version 6.6 in the release notes. Additionally, as of the Version 6.6 release, lower-memory instance types for cloud-based FMCv deployments are fully deprecated. You cannot create new FMCv instances using them, even for earlier Firepower versions. You can continue running existing instances.
Deprecated: e1000 Interfaces on FTDv for VMware.	**Upgrade impact. Prevents upgrade.** Version 6.6 ends support for e1000 interfaces on FTDv for VMware. You cannot upgrade until you switch to vmxnet3 or ixgbe interfaces. Or, you can deploy a new device. For more information, see the Secure Firewall Threat Defense Virtual getting started guides.

Feature	Description
Deprecated: Less secure Diffie-Hellman groups, and encryption and hash algorithms.	Version 6.6 deprecates the following FTD security features: • Diffie-Hellman groups: 2, 5, and 24. • Encryption algorithms for users who satisfy export controls for strong encryption: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continues to be supported (and is the only option) for users who do not satisfy export controls. • Hash algorithms: MD5. These features are removed in Version 6.7. Avoid configuring them in IKE proposals or IPSec policies for use in VPNs. Change to stronger options as soon as possible.
Deprecated: Custom tables for connection events.	Version 6.6 ends support for custom tables for connection and Security Intelligence events. After you upgrade, existing custom tables for those events are still 'available' but return no results. We recommend you delete them. There is no change to other types of custom tables. Deprecated options: • **Analysis > Advanced > Custom Tables >** click **Create Custom Table > Tables** drop-down list **> Connection Events** and **Security Intelligence Events**
Deprecated: Ability to delete connection events from the event viewer.	Version 6.6 ends support for deleting connection and Security Intelligence events from the event viewer. To purge the database, select **System** > **Tools** > **Data Purge**. Deprecated options: • **Analysis** > **Connections** > **Events > Delete** and **Delete All** • **Analysis** > **Connections** > **Security Intelligence Events > Delete** and **Delete All**
Deprecated: Geolocation details.	We no longer provide the geolocation IP package, which contained contextual data associated with routable IP addresses. This saves disk space and does not affect geolocation rules or traffic handling in any way. Any contextual data is now stale, and upgrading to most later versions deletes the IP package. Options to download the IP package or view contextual data have no effect, and are removed in later versions.

FMC Features in Version 6.5.x

Table 78: FMC Features in Version 6.5.x Patches

Feature	Details
Administration and Troubleshooting	

Feature	Details
Version 6.5.0.5 Default HTTPS server certificates	**Upgrade impact.** Unless the FMC's current *default* HTTPS server certificate already has an 800-day lifespan, upgrading to Version 6.5.0.5+ renews the certificate, which now expires 800 days from the date of the upgrade. All future renewals have an 800 day lifespan. Your old certificate was set to expire depending on when it was generated, as follows: • 6.5.0 to 6.5.0.4: 3 years • 6.4.0.9 and later patches: 800 days • 6.4.0 to 6.4.0.8: 3 years • 6.3.0 and all patches: 3 years • 6.2.3: 20 years
Deprecated Features	
Version 6.5.0.2 Deprecated: Egress optimization (temporary).	**Upgrade impact.** Egress optimization is a performance feature targeted for selected IPS traffic. It is enabled by default on all FTD platforms, and the Version 6.5.0 upgrade process enables egress optimization on eligible devices. However, to mitigate CSCvq34340, patching FTD to Version 6.5.0.2+ turns off egress optimization processing. This happens regardless of whether the egress optimization feature is enabled or disabled. **Note** We recommend you upgrade to Version 6.6+, where this issue is fixed. That will turn egress optimization back on, if you left the feature 'enabled.' If you remain at Version 6.5.0 or 6.5.0.1, you should manually disable egress optimization from the FTD CLI: **no asp inspect-dp egress-optimization**. For more information, see the software advisory: FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature. Supported platforms: FTD

Table 79: FMC Features in Version 6.5.0

Feature	Details
Platform	
FTD on the Firepower 1150.	We introduced the Firepower 1150.
Larger instances for FTDv for Azure.	FTDv for Microsoft Azure now supports larger instances: D4_v2 and D5_v2.

Feature	Details
FMCv 300 for VMware.	We introduced the FMCv 300, a larger FMCv for VMware. It can manage up to 300 devices, compared to 25 devices for other FMCv instances. You can use the FMC model migration feature to switch to the FMCv 300 from a less powerful platform.
VMware vSphere/VMware ESXi 6.7 support	You can now deploy FMCv, FTDv, and NGIPSv virtual appliances on VMware vSphere/VMware ESXi 6.7.
Firepower Threat Defense	
Firepower 1010 hardware switch support	The Firepower 1010 now supports setting each Ethernet interface to be a switch port or a firewall interface. New/modified pages: • **Devices > Device Management > Interfaces** • **Devices > Device Management > Interfaces > Edit Physical Interface** • **Devices > Device Management > Interfaces > Add VLAN Interface** Supported platforms: Firepower 1010
Firepower 1010 PoE+ support on Ethernet 1/7 and Ethernet 1/8	The Firepower 1010 now supports Power over Ethernet+ (PoE+) on Ethernet 1/7 and Ethernet 1/8. New/modified pages: **Devices > Device Management > Interfaces > Edit Physical Interface > PoE** Supported platforms: Firepower 1010
Carrier-grade NAT enhancements	For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time (see RFC 6888). New/modified pages: **Devices** > **NAT** > add/edit FTD NAT policy > add/edit NAT rule > **PAT Pool** tab > **Block Allocation** option Supported platforms: FTD

Feature	Details
TLS crypto acceleration for multiple container instances on Firepower 4100/9300	TLS crypto acceleration is now supported on multiple container instances (up to 16) on a Firepower 4100/9300 chassis. Previously, you could enable TLS crypto acceleration for only *one* container instance per module/security engine. New instances have this feature enabled by default. However, the upgrade does *not* enable acceleration on existing instances. Instead, use the **create hw-crypto** and **scope hw-crypto** CLI commands. For more information, see the *Cisco Secure Firewall Threat Defense Command Reference*. New FXOS CLI commands: • **create hw-crypto** • **delete hw-crypto** • **scope hw-crypto** • **show hw-crypto** Removed FXOS CLI commands: • **show hwCrypto** (replaced by **show hw-crypto**) • **config hwCrypto** Removed FTD CLI commands: • **show crypto accelerator status** Supported platforms: Firepower 4100/9300
Security Policies	
Access control rule filtering	You can now filter access control rules based on search criteria. New/modified pages: **Policies** > **Access Control** > **Access Control** > add/edit policy > filter button ('show only rules matching filter criteria') Supported platforms: FMC
Dispute URL category or reputation	You can now dispute the category or reputation of a URL. New/modified pages: • **Analysis** > **Connection Events** > right-click a category or reputation > **Dispute**. • **Analysis** > **Advanced** > **URL** > search for URL > **Dispute** button • **System** > **Integration** > **Cloud Services** > **Dispute** link Supported platforms: FMC

Feature	Details
User control with destination-based Security Group Tags (SGT)	You can now use ISE SGT tags for both source and destination matching criteria in access control rules. SGT tags are tag-to-host/network mappings obtained by ISE. New connection event fields: • Destination SGT (syslog: DestinationSecurityGroupTag): SGT attribute for the connection responder. Renamed connection event fields: • Source SGT (syslog: SourceSecurityGroupTag): SGT attribute for the connection initiator. Replaces Security Group Tag (syslog: SecurityGroup). New/modified pages: **System > Integration > Identity Sources > Identity Services Engine >** Subscribe to **Session Directory Topic** and **SXP Topic** options Supported platforms: Any
Cisco Firepower User Agent Version 2.5 integration	We released Version 2.5 of the Cisco Firepower User Agent, which you can integrate with Firepower Versions 6.4.0 through 6.6.x. **Note** Version 6.6 is the last release to support the Cisco Firepower User Agent software as an identity source. You cannot upgrade an FMC with user agent configurations to Version 6.7+. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC). This will also allow you to take advantage of features that are not available with the user agent. To convert your license, contact your Cisco representative or partner contact. For more information, see the End-of-Life and End-of-Support for the Cisco Firepower User Agent announcement and the Migrate from User Agent to Identity Services Engine TechNote. New/modified FMC CLI commands: **configure user-agent** Supported platforms: FMC
Event Logging and Analysis	

Feature	Details
Threat Intelligence Director priorities.	TID blocking/monitoring observable actions now have priority over blocking/monitoring with Security Intelligence Block lists. If you configure the **Block** TID observable action, even if the traffic also matches a Security Intelligence Block list set to **Block**: • The Security Intelligence category in the connection event is a variant of `TID Block`. • The system generates a TID incident with an action taken of `Blocked`. If you configure the **Monitor** TID observable action, even if the traffic also matches a Security Intelligence Block list set to **Monitor**: • The Security Intelligence category in the connection event is a variant of `TID Monitor` • The system generates a TID incident with an action taken of `Monitored`. Previously, in each of these cases, the system reported the category by analysis and did not generate a TID incident. **Note** The system still effectively handles traffic as before. Traffic that was blocked before is still blocked, and monitored traffic is still monitored. This simply changes which component gets the 'credit.' You may also see more TID incidents generated. For complete information on system behavior when you enable both Security Intelligence and TID, see the *TID-Firepower Management Center Action Prioritization* information in the FMC configuration guide. Supported platforms: FMC
'Packet profile' CLI commands	You can now use the FTD CLI to obtain statistics on how the device handled network traffic. That is, how many packets were fastpathed by a prefilter policy, offloaded as a large flow, fully evaluated by access control (Snort), and so on. New FTD CLI commands: • **asp packet-profile** • **no asp packet-profile** • **show asp packet-profile** • **clear asp packet-profile** Supported platforms: FTD
Additional event types for Cisco SecureX	Firepower can now send file and malware events to Cisco SecureX, as well as high priority connection events — those related to intrusion, file, malware, and Security Intelligence events. Note that the FMC web interface refers to this offering as *Cisco Threat Response (CTR)*. New/modified pages: **System > Integration > Cloud Services**. Supported platforms: FTD (via syslog or direct integration) and Classic (via syslog) devices
Administration and Troubleshooting	

Feature	Details
Precision Time Protocol (PTP) configuration for ISA 3000 devices.	You can use FlexConfig to configure the Precision Time Protocol (PTP) on ISA 3000 devices. PTP is a time-synchronization protocol developed to synchronize the clocks of various devices in a packet-based network. The protocol is designed specifically for industrial, networked measurement and control systems. We now allow you to include the **ptp** (interface mode) command, and the global commands **ptp mode e2etransparent** and **ptp domain**, in FlexConfig objects. New/modified commands: **show ptp** Supported platforms: ISA 3000 with FTD
Configure more domains (multitenancy)	When implementing multitenancy (segment user access to managed devices, configurations, and events), you can create up to 100 subdomains under a top-level Global domain, in two or three levels. The previous maximum was 50 domains. Supported platforms: FMC
ISE Connection Status Monitor enhancements	The ISE Connection Status Monitor health module now alerts you to issues with TrustSec SXP (SGT Exchange Protocol) subscription status. Supported platforms: FMC
Regional clouds	**Upgrade impact.** If you use the Cisco Threat Response integration, Cisco Support Diagnostics, or Cisco Success Network features, you can now select a regional cloud. By default, the upgrade assigns you to the US (North America) region. New/modified pages: **System** > **Integration** > **Cloud Services** Supported platforms: FMC, FTD
Cisco Support Diagnostics	**Upgrade impact.** Cisco Support Diagnostics (sometimes called *Cisco Proactive Support*) sends configuration and operational health data to Cisco, and processes that data through our automated problem detection system, allowing us to proactively notify you of issues. This feature also allows Cisco TAC to collect essential information from your devices during the course of a TAC case. During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time. New/modified pages: • **System > Smart Licenses** • **System > Smart Licenses > Register** Supported platforms: FMC, Firepower 4100/9300, FTDv for Azure

Feature	Details
FMC model migration	You can now use the backup and restore feature to migrate configurations and events between FMCs, even if they are not the same model. This makes it easier to replace FMCs due to technical or business reasons such as a growing organization, migration from a physical to a virtual implementation, hardware refresh, and so on. In general, you can migrate from a lower-end to a higher-end FMC, but not the reverse. Migration from KVM and Microsoft Azure is not supported. You must also unregister and reregister with Cisco Smart Software Manager (CSSM). For details, including supported target and destination models, see the *Cisco Secure Firewall Management Center Model Migration Guide*. Supported platforms: FMC
Default HTTPS server certificates.	If you are upgrading from Version 6.4.0.9+, the *default* HTTPS server certificate's lifespan-on-renew returns to 3 years, but this is again updated to 800 days in Version 6.5.0.5+ and 6.6+. Your current default HTTPS server certificate is set to expire depending on when it was generated, as follows: • 6.4.0.9 and later patches: 800 days • 6.4.0 to 6.4.0.8: 3 years • 6.3.0 and all patches: 3 years • 6.2.3: 20 years
Security and Hardening	
Secure erase for appliance components on FXOS-based FTD devices	You can now use the FXOS CLI to securely erase a specified appliance component. New FXOS CLI commands: **erase secure** Supported platforms: Firepower 1000/2000 and Firepower 4100/9300
Stricter password requirements for FMC `admin` accounts during initial setup	FMC initial setup now requires that you choose a 'strong' password for `admin` accounts. The setup process applies this strong password to both the FMC web interface and CLI `admin` accounts. **Note** Upgrading to Version 6.5.0+ does not force you to change weak passwords to strong passwords. With the exception of LOM users on physical FMCs (and this does include the `admin` user), you are not prohibited from choosing a new weak password. However, we do recommend that all Firepower user accounts — especially those with Admin access — have strong passwords. Supported platforms: FMC
Concurrent user session limits	You can now limit the number of users that can be logged into the FMC at the same time. You can limit concurrent sessions for users with read only roles, read/write roles, or both. Note that CLI users are limited by the read/write setting. New/modified pages: **System > Configuration > User Configuration > Max Concurrent Sessions Allowed** options Supported platforms: FMC

Feature	Details
Authenticated NTP servers	You can now configure secure communications between the FMC and NTP servers using SHA1 or MD5 symmetric key authentication. For system security, we recommend using this feature. New/modified pages: **System > Configuration > Time Synchronization** Supported platforms: FMC
Usability and Performance	
Improved initial configuration experience	On new and reimaged FMCs, a wizard replaces the previous initial setup process. If you use the GUI wizard, when initial setup completes, the FMC displays the device management page so that you can immediately begin licensing and setting up your deployment. The setup process also automatically schedules the following: • Software downloads. The system creates a weekly scheduled task to download (but not install) software patches and publicly available hotfixes that apply to your deployment. • FMC configuration-only backups. The system creates a weekly scheduled task to back up FMC configurations and store them locally. • GeoDB updates. The system enables weekly geolocation database updates. These tasks are scheduled in UTC, which means that when they occur *locally* depends on the date and your specific location. Also, because tasks are scheduled in UTC, they do not adjust for Daylight Saving Time, summer time, or any such seasonal adjustments that you may observe in your location. If you are affected, scheduled tasks occur one hour "later" in the summer than in the winter, according to local time. **Note** We *strongly* recommend you review the auto-scheduled tasks/GeoDB updates and adjust them if necessary. Upgraded FMCs are not affected. For details on the initial configuration wizard, see the *Getting Started Guide* for your FMC model; for details on scheduled tasks, see the FMC configuration guide. Supported platforms: FMC
Light theme	**Beta.** The FMC web interface defaults to the Classic theme, but you can also choose a new Light theme. **Note** The Light theme is a Beta feature. You may see misaligned text or other UI elements. In some cases, you may also experience slower-than-normal response times. If you encounter issues that prevent you from using a page or feature, switch back to the Classic theme. Although we cannot respond to everybody, we also welcome feedback — please use the feedback link on the User Preferences page or contact us at fmc-light-theme-feedback@cisco.com">. New/modified pages: **User Preferences**, from the drop-down list under your username Supported platforms: FMC

Feature	Details
Usability enhancements for viewing objects	We have enhanced 'view object' capabilities for network, port, VLAN, and URL objects, as follows: • In the access control policy and while configuring FTD routing, you can right-click an object and choose **View Objects** to display details about that object. • When you are viewing details about an object, or when you are browsing objects in the object manager, clicking **Find Usage** ( ) now allows you to drill down into object groups and nested objects. New/modified pages: • **Objects > Object Management >** choose a supported object type > **Find Usage** ( ) • **Policies > Access Control > Access Control >** create or edit policy > create or edit rule > choose a supported condition type > right-click an object > **View Objects** • **Devices > Device Management >** edit FTD device > **Routing >** right-click a supported object > **View Objects** Supported platforms: FMC
Usability enhancements for deploying configuration changes	We streamlined the display of errors and warnings related to deploying configuration changes. Instead of an immediate verbose view, you can now **Click to view all details** to see more information about a particular error or warning. New/modified pages: **Errors and Warnings for Requested Deployment** dialog box Supported platforms: FMC
Usability enhancements to FTD NAT policy management	When configuring FTD NAT, you can now: • View warnings and errors in your NAT policy, by device. Warnings and errors mark configurations that could adversely affect traffic flow or prevent the policy from deploying. • Display up to 1000 NAT rules per page. The default is 100. New/modified pages: **Devices > NAT >** create or edit FTD NAT policy > **Show Warnings** and **Rules Per Page** options Supported platforms: FTD
Deprecated Features	
End of support: FMC 750, 1500, 3500.	You cannot run Version 6.5+ on the FMC models FMC 1000, 2500, and 4500. You cannot manage Version 6.5+ devices with these FMCs.
End of support: ASA 5515-X and ASA 5585-X series	You cannot run Version 6.5+ on the ASA 5515-X and ASA 5585-X series devices (SSP-10, -20, -40, and -60).
End of support: Firepower 7000/8000 series.	You cannot run Version 6.5+ on Firepower 7000/8000 series devices, including AMP models.

Feature	Details
Deprecated: Ability to disable the FMC CLI.	Version 6.3 introduced the FMC CLI, which you had to explicitly enable. In Version 6.5, the CLI is automatically enabled, for both new and upgraded deployments. If you want to access the Linux shell (also called *expert mode*), you must log in to the CLI and then use the **expert** command. **Caution** We recommend you do not access Firepower appliances using the shell, unless directed by Cisco TAC. Deprecated options: **System > Configuration > Console Configuration > Enable CLI access** check box
Deprecated: MD5 authentication algorithm and DES encryption for SNMPv3 users.	Version 6.5 deprecates the MD5 authentication algorithm and DES encryption for SNMPv3 users on FTD. Although these configurations continue to work post-upgrade, the system displays a warning when you deploy. And, you cannot create new users or edit existing users with these options. Support is removed in Version 7.0. If you are still using these options in your platform settings policy, we recommend you switch to stronger options now. New/modified screens: **Devices > Platform Settings > SNMP > Users**
Deprecated: TLS 1.0 & 1.1.	**Upgrade impact.** To enhance security: • Captive portal (active authentication) has removed support for TLS 1.0. • Host input has removed support for TLS 1.0 and TLS 1.1. If your client fails to connect with a Firepower appliance, we recommend you upgrade your client to support TLS 1.2.
Deprecated: TLS crypto acceleration FXOS CLI commands for Firepower 4100/9300.	As part of allowing TLS crypto acceleration for multiple container instances on Firepower 4100/9300, we removed the following FXOS CLI commands: • **show hwCrypto** • **config hwCrypto** And this FTD CLI command: • **show crypto accelerator status** For information on their replacements, see the new feature documentation.
Deprecated: Cisco Security Packet Analyzer integration.	Version 6.5 ends support for FMC integration with Cisco Security Packet Analyzer. Deprecated screens/options: • **System > Integration > Packet Analyzer** • **Analysis > Advanced > Packet Analyzer Queries** • **Query Packet Analyzer** when right-clicking on an event in the dashboard or event viewer

Feature	Details
Deprecated: Geolocation details.	We no longer provide the geolocation IP package, which contained contextual data associated with routable IP addresses. This saves disk space and does not affect geolocation rules or traffic handling in any way. Any contextual data is now stale, and upgrading to most later versions deletes the IP package. Options to download the IP package or view contextual data have no effect, and are removed in later versions.

FMC Features in Version 6.4.x

Table 80: FMC Features in Version 6.4.x Patches

Feature	Details
Version 6.4.0.17 Smaller VDB for lower memory devices.	For VDB 363+, the system now installs a smaller VDB (also called *VDB lite*) on lower memory devices. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Minimum threat defense: Any Lower memory devices: ASA 5506-X series, ASA-5508-X, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X Version restrictions: The ability to install a smaller VDB depends on the version of the FMC, not managed devices. If you upgrade the FMC from a supported version to an unsupported version, you cannot install VDB 363+ if your deployment includes even one lower memory device. For a list of affected releases, see CSCwd88641.
Version 6.4.0.10 Upgrades postpone scheduled tasks.	**Upgrade impact.** Upgrades now postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. **Note** Before you begin any upgrade, you must still make sure running tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Note that this feature is supported for Firepower appliances *running* Version 6.4.0.10 or any later patch. It is not supported for upgrades *to* Version 6.4.0.10, or upgrades that skip Version 6.4.0.10. This feature is temporarily deprecated in Versions 6.5.0–6.6.1, but returns in Version 6.6.3.

Feature	Details
Version 6.4.0.9 Default HTTPS server certificates.	**Upgrade impact.** Upgrading an FMC or 7000/8000 series device from Version 6.4.0–6.4.0.8 to any later Version 6.4.0.x patch (or an FMC to Version 6.6.0+) renews the *default* HTTPS server certificate, which expires 800 days from the date of the upgrade. All future renewals have an 800 day lifespan. Your old certificate was set to expire depending on when it was generated, as follows: • 6.4.0 to 6.4.0.8: 3 years • 6.3.0 and all patches: 3 years • 6.2.3 and earlier: 20 years Note that in Version 6.5.0–6.5.0.4, the lifespan-on-renew returns to 3 years, but this is again updated to 800 days with Version 6.5.0.5 and 6.6.0.
Version 6.4.0.4 New syslog fields.	These new syslog fields collectively identify a unique connection event: • Sensor UUID • First Packet Time • Connection Instance ID • Connection Counter These fields also appear in syslogs for intrusion, file, and malware events, allowing connection events to be associated with those events.
Version 6.4.0.2 Detection of rule conflicts in FTD NAT policies.	**Upgrade impact.** After you upgrade to Version 6.4.0.2 or later patch, you can no longer create FTD NAT policies with conflicting rules (often referred to as *duplicate* or *overlapping* rules). This fixes an issue where conflicting NAT rules were applied out-of-order. If you currently have conflicting NAT rules, you will be able to deploy post-upgrade. However, your NAT rules will continue to be applied out-of-order. Therefore, we recommend that after the upgrade, you inspect your FTD NAT policies by editing (no changes are needed) then attempting to resave. If you have rule conflicts, the system will prevent you from saving. Correct the issues, save, and then deploy.
Version 6.4.0.2 ISE Connection Status Monitor health module.	A new health module, the *ISE Connection Status Monitor*, monitors the status of the server connections between the Cisco Identity Services Engine (ISE) and the FMC.

Table 81: FMC Features in Version 6.4.0

Feature	Details
Platform	
FMCv for Azure.	We introduced FMCv for Microsoft Azure.

Feature	Details
FTD on the Firepower 1010, 1120, and 1140.	We introduced the Firepower 1010, 1120, and 1140.
FTD on the Firepower 4115, 4125, and 4145.	We introduced the Firepower 4115, 4125, and 4145.
Firepower 9300 SM-40, SM-48, and SM-56 support.	We introduced three new security modules: SM-40, SM-48, and SM-56. With FXOS 2.6.1, you can mix different types of security modules in the same chassis.
ASA and FTD on the same Firepower 9300.	With FXOS 2.6.1, you can now deploy ASA and FTD logical devices on the same Firepower 9300.
Firepower Threat Defense: Device Management	
FTDv for VMware defaults to vmxnet3 interfaces.	FTDv for VMware now defaults to vmxnet3 interfaces when you create a virtual device. Previously, the default was e1000. The vmxnet3 device drivers and network processing are integrated with the ESXi hypervisor, so they use fewer resources and offer better network performance. **Note** Version 6.6 ends support for e1000 interfaces. You will not be able to upgrade to Version 6.6+ until you switch to vmxnet3 or ixgbe interfaces. We recommend you do this now. For more information, refer to the instructions on adding and configuring VMware interfaces in the Secure Firewall Threat Defense Virtual getting started guides. Supported platforms: FTDv for VMware
Firepower Threat Defense: Routing	
Rotating (keychain) authentication for OSPFv2 routing.	You can now use rotating (keychain) authentication when configuring OSPFv2 routing. New/modified pages: • **Objects** > **Object Management** > **Key Chain** object • **Devices** > **Device Management** > edit device > **Routing** tab > **OSPF** settings > **Interface** tab > add/edit interface > **Authentication** option • **Devices** > **Device Management** > edit device > **Routing** tab > **OSPF** settings > **Area** tab > add/edit area > **Virtual Link** sub-tab > add/edit virtual link > **Authentication** option Supported platforms: FTD
Firepower Threat Defense: Encryption and VPN	

Feature	Details
RA VPN: Secondary authentication.	Secondary authentication, also called double authentication, adds an additional layer of security to RA VPN connections by using two different authentication servers. With secondary authentication enabled, AnyConnect VPN users must provide two sets of credentials to log in to the VPN gateway. RA VPN supports secondary authentication for the AAA Only and Client Certificate and AAA authentication methods. New/modified pages: **Devices** > **VPN** > **Remote Access >** add/edit configuration **> Connection Profile > AAA** area Supported platforms: FTD
Site-to-site VPN: Dynamic IP addresses for extranet endpoints.	You can now configure site to site VPNs to use a dynamic IP address for extranet endpoints. In hub-and-spoke deployments, you can use a hub as an extranet endpoint. New/modified pages: **Devices** > **VPN** > **Site To Site >** add/edit FTD VPN topology **> Endpoints** tab **>** add endpoint **> IP Address** option Supported platforms: FTD
Site-to-site VPN: Dynamic crypto maps for point-to-point topologies.	You can now use dynamic crypto maps in point-to-point as well as in hub-and-spoke VPN topologies. Dynamic crypto maps are still not supported for full mesh topologies. You specify the crypto map type when you configure a topology. Make sure you also specify a dynamic IP address for one of the peers in the topology. New/modified pages: **Devices** > **VPN** > **Site To Site >** add/edit FTD VPN topology **> IPsec** tab **> Crypto Map Type** option Supported platforms: FTD

Feature	Details
TLS crypto acceleration.	**Upgrade impact.** SSL hardware acceleration has been renamed *TLS crypto acceleration*. Depending on the device, TLS crypto acceleration might be performed in software or in hardware. The Version 6.4.0 upgrade process automatically enables acceleration on all eligible devices, even if you previously disabled the feature manually. In most cases you cannot configure this feature; it is automatically enabled and you cannot disable it. However, if you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can enable TLS crypto acceleration for *one* container instance per module/security engine. Acceleration is disabled for other container instances, but enabled for native instances. New FXOS CLI commands for the Firepower 4100/9300 chassis: • **show hwCrypto** • **config hwCrypto** New FTD CLI commands: • **show crypto accelerator status** (replaces **system support ssl-hw-status**) Removed FTD CLI commands: • **system support ssl-hw-accel** • **system support ssl-hw-status** Supported platforms: Firepower 2100 series, Firepower 4100/9300
Event Logging and Analysis	
Improvements to syslog messages for file and malware events.	Fully qualified file and malware event data can now be sent from managed devices via syslog. New/modified pages: **Policies** > **Access Control** > **Access Control >** add/edit policy **> Logging** tab **> File and Malware Settings** area Supported platforms: Any
Search intrusion events by CVE ID.	You can now search for intrusion events generated as a result of a particular CVE exploit. New/modified pages: **Analysis** > **Search** Supported platforms: FMC
IntrusionPolicy field is now included in syslog.	Intrusion event syslog messages now specify the intrusion policy that triggered the event. Supported platforms: Any

Feature	Details
Cisco SecureX integration.	Cisco SecureX is a cloud offering that helps you rapidly detect, investigate, and respond to threats. This feature lets you analyze incidents using data aggregated from multiple products, including Firepower Threat Defense. Note that the FMC web interface refers to this offering as *Cisco Threat Response (CTR)*. See the *Cisco Secure Firewall Threat Defense and SecureX Integration Guide*. New/modified pages: **System** > **Integration** > **Cloud Services** Supported platforms: FTD
Splunk integration.	Splunk users can use a new, separate Splunk app, Cisco Secure Firewall (f.k.a. Firepower) app for Splunk, to analyze events. Available functionality is affected by your Firepower version. See *Cisco Secure Firewall App for Splunk User Guide*. Supported platforms: FMC
Cisco Security Analytics and Logging (SaaS) integration.	You can send Firepower events to the Stealthwatch Cloud for storage, and optionally make your Firepower event data available for security analytics using Stealthwatch Cloud. Using Cisco Security Analytics and Logging (SaaS), also known as SAL (SaaS), your Firepower devices send events as syslog messages to a Security Events Connector (SEC) installed on a virtual machine on your network, and this SEC forwards the events to the Stealthwatch cloud for storage. You view and work with your events using the web-based Cisco Defense Orchestrator (CDO) portal. Depending on the license you purchase, you can also use the Stealthwatch portal to access that product's analytics features. See *Cisco Secure Firewall Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide*. Supported platforms: FTD with FMC
Administration and Troubleshooting	
New licensing capabilities for ISA 3000.	For ASA FirePOWER and FTD deployments, the ISA 3000 now supports URL Filtering and Malware licenses and their associated features. For FTD only, the ISA 3000 also now supports Specific License Reservation for approved customers. Supported platforms: ISA 3000
Scheduled remote backups of managed devices.	You can now use the FMC to schedule remote backups of certain managed devices. Previously, only Firepower 7000/8000 series devices supported scheduled backups, and you had to use the device's local GUI. New/modified pages: **System** > **Tools** > **Scheduling** > add/edit task > choose **Job Type: Backup** > choose a **Backup Type** Supported platforms: FTD physical platforms, FTDv for VMware, Firepower 7000/8000 series Exceptions: No support for FTD clustered devices or container instances

Feature	Details
Ability to disable Duplicate Address Detection (DAD) on management interfaces.	When you enable IPv6, you can disable DAD. You might want to disable DAD because using DAD opens up the possibility of denial of service attacks. If you disable this setting, you need check manually that this interface is not using an already-assigned address. New/modified pages: **System** > **Configuration** > **Management Interfaces** > **Interfaces** area > edit interface > **IPv6 DAD** check box Supported platforms: FMC, Firepower 7000/8000 series
Ability to disable ICMPv6 Echo Reply and Destination Unreachable messages on management interfaces.	When you enable IPv6, you can now disable ICMPv6 Echo Reply and Destination Unreachable messages. You might want to disable these packets to guard against potential denial of service attacks. Disabling Echo Reply packets means you cannot use IPv6 ping to the device management interfaces for testing purposes. New/modified pages: **System** > **Configuration** > **Management Interfaces** > **ICMPv6** New/modified commands: • **configure network ipv6 destination-unreachable** • **configure network ipv6 echo-reply** Supported platforms: FMC (web interface only), managed devices (CLI only)
Support for the Service-Type attribute for FTD users defined on the RADIUS server.	For RADIUS authentication of FTD CLI users, you used to have to predefine the usernames in the RADIUS external authentication object and manually make sure that the list matched usernames defined on the RADIUS server. You can now define CLI users on the RADIUS server using the Service-Type attribute and also define both Basic and Config user roles. To use this method, be sure to leave the shell access filter blank in the external authentication object. New/modified pages: **System** > **Users** > **External Authentication** tab > add/edit external authentication object > **Shell Access Filter** Supported platforms: FTD
View object use.	The object manager now allows you to see the policies, settings, and other objects where a network, port, VLAN, or URL object is used. New/modified pages: **Objects > Object Management >** choose object type > Find Usage (binoculars) icon Supported platforms: FMC

Feature	Details
Hit counts for access control and prefilter rules.	You can now access hit counts for access control and prefilter rules on your FTD devices. New/modified pages: • **Policies** > **Access Control** > **Access Control >** add/edit policy **> Analyze Hit Counts** • **Policies** > **Access Control** > **Prefilter >** add/edit policy **> Analyze Hit Counts** New commands: • **show rule hits** • **clear rule hits** • **cluster exec show rule hits** • **cluster exec clear rule hits** • **show cluster rule hits** Modified commands: **show failover** Supported platforms: FTD
URL Filtering health monitor improvements.	You can now configure time thresholds for URL Filtering Monitor alerts. New/modified pages: **System** > **Health** > **Policy >** add/edit policy **> URL Filtering Monitor** Supported platforms: Any
Connection-based troubleshooting.	Connection-based troubleshooting or debugging provides uniform debugging across modules to collect appropriate logs for a specific connection. It also supports level-based debugging up to 7 levels and enables uniform log collection mechanism for lina and Snort logs. New/modified commands: • **clear packet debugs** • **debug packet start** • **debug packet stop** • **show packet debugs** Supported platforms: FTD
New Cisco Success Network monitoring capabilities	Added the following Cisco Success Network monitoring capabilities: • CSPA (Cisco Security Packet Analyzer) query information • Contextual cross-launch instances enabled on the FMC • TLS/SSL inspection events • Snort restarts Supported platforms: FMC
Security and Hardening	

Feature	Details
Signed SRU, VDB, and GeoDB updates.	So Firepower can verify that you are using the correct update files, Version 6.4.0+ uses *signed* updates for intrusion rules (SRU), the vulnerability database (VDB), and the geolocation database (GeoDB). Earlier versions continue to use unsigned updates. Unless you manually download updates from Cosco—for example, in an air-gapped deployment—you should not notice any difference in functionality. If, however, you do manually download and install SRU, VDB, and GeoDB updates, make sure you download the correct package for your current version. Signed update files for Version 6.4.0+ begin with 'Cisco' instead of 'Sourcefire,' and terminate in .sh.REL.tar instead of .sh: • SRU: Cisco_Firepower_SRU-*date-build*-vrt.sh.REL.tar • VDB: Cisco_VDB_Fingerprint_Database-4.5.0-*version*.sh.REL.tar • GeoDB: Cisco_GEODB_Update-*date-build*.sh.REL.tar Update files for Version 5.x through 6.3 still use the old naming scheme: • SRU: Sourcefire_Rule_Update-*date-build*-vrt.sh • VDB: Sourcefire_VDB_Fingerprint_Database-4.5.0-*version*.sh • GeoDB: Sourcefire_Geodb_Update-*date-build*.sh We will provide both signed and unsigned updates until the end-of-support for versions that require unsigned updates. Do not untar signed (.tar) packages. **Note** If you accidentally upload a signed update to an older FMC or ASA FirePOWER device, you must manually delete it. Leaving the package takes up disk space, and also may cause issues with future upgrades. Supported platforms: Any
SNMPv3 users can authenticate using a SHA-256 authorization algorithm.	SNMPv3 users can now authenticate using a SHA-256 algorithm. New/modified screen: **Devices > Platform Settings > SNMP > Users > Auth Algorithm Type** Supported platforms: Firepower Threat Defense
2048-bit certificate keys now required (security enhancement).	**Upgrade impact.** When making secure connections to external data sources, such as AMP for Endpoints or Cisco Threat Intelligence Detector (TID), the FMC now requires that the server certificate be generated with keys that are at least 2048 bits long. Certificates previously generated with 1024-bit keys will no longer work. Note that this security enhancement was introduced in Version 6.3.0.3. If you are upgrading from Version 6.1.0 through 6.3.0.2, you may be affected. If you cannot connect, regenerate the server certificate on your data source. If necessary, reconfigure the FMC connection to the data source. Supported platforms: FMC
Usability and Performance	

Feature	Details
Snort restart improvements.	Before Version 6.4.0, during Snort restarts, the system dropped encrypted connections that matched a 'Do not decrypt' SSL rule or default policy action. Now, routed/transparent traffic passes without inspection instead of dropping, as long as you did not disable large flow offload or Snort preserve-connection. Supported platforms: Firepower 4100/9300
Performance improvement for selected IPS traffic.	**Upgrade impact.** Egress optimization is a performance feature targeted for selected IPS traffic. It is enabled by default on all FTD platforms, and the Version 6.4.0 upgrade process enables egress optimization on eligible devices. New/modified commands: • **asp inspect-dp egress optimization** • **show asp inspect-dp egress optimization** • **clear asp inspect-dp egress optimization** • **show conn state egress_optimization** For more information, see the *Cisco Secure Firewall Threat Defense Command Reference*. To troubleshoot issues with egress optimization, contact Cisco TAC. **Note** To mitigate CSCvq34340, patching FTD device to Version 6.4.0.7+ turns off egress optimization processing. This happens regardless of whether the egress optimization feature is enabled or disabled. We recommend you upgrade to Version 6.6+, where this issue is fixed. That will turn egress optimization back on, if you left the feature 'enabled.' If you remain at Version 6.4.0–6.4.0.6, you should manually disable egress optimization from the FTD CLI: **no asp inspect-dp egress-optimization**. For more information, see the software advisory: FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature. Supported platforms: FTD
Faster SNMP event logging.	Performance improvements when sending intrusion and connection events to an external SNMP trap server. Supported platforms: Any
Faster deploy.	Improvements to appliance communications and deploy framework. Supported platforms: FTD
Faster upgrade.	Improvements to the event database. Supported platforms: Any
Firepower Management Center REST API	

Feature	Details
API Explorer based on OAS.	Version 6.4.0 uses a new API Explorer, based on the OpenAPI Specification (OAS). As part of the OAS, you now use CodeGen to generate sample code. You can still access the legacy API Explorer if you prefer. Supported platforms: FMC
Deprecated Features	
Deprecated: SSL hardware acceleration FTD CLI commands.	As part of the TLS crypto acceleration feature, we removed the following FTD CLI commands: • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status**
Deprecated: Geolocation details.	We no longer provide the geolocation IP package, which contained contextual data associated with routable IP addresses. This saves disk space and does not affect geolocation rules or traffic handling in any way. Any contextual data is now stale, and upgrading to most later versions deletes the IP package. Options to download the IP package or view contextual data have no effect, and are removed in later versions.

FMC Features in Version 6.3.x

Table 82: FMC Features in Version 6.3.x Patches

Feature	Details
Version 6.3.0.4 Detection of rule conflicts in FTD NAT policies	**Upgrade impact.** After you upgrade to Version 6.3.0.4 or later patch, you can no longer create FTD NAT policies with conflicting rules (often referred to as *duplicate* or *overlapping* rules). This fixes an issue where conflicting NAT rules were applied out-of-order. If you currently have conflicting NAT rules, you will be able to deploy post-upgrade. However, your NAT rules will continue to be applied out-of-order. Therefore, we recommend that after the upgrade, you inspect your FTD NAT policies by editing (no changes are needed) then attempting to resave. If you have rule conflicts, the system will prevent you from saving. Correct the issues, save, and then deploy. Note that upgrading to Version 6.4.0 deprecates this fix. It is fixed again in Version 6.4.0.2.
Version 6.3.0.4 ISE Connection Status Monitor module	A new module, the *ISE Connection Status Monitor*, monitors the status of the server connections between the Cisco Identity Services Engine (ISE) and the FMC. Note that upgrading to Version 6.4.0 deprecates this module. Support returns in Version 6.4.0.2. New/modified screens: **System** > > **Policy** > create or edit policy > **ISE Connection Status Monitor**

Feature	Details
Version 6.3.0.3 2048-bit certificate keys now required (security enhancement)	When making secure connections to external data sources, such as AMP for Endpoints or Cisco Threat Intelligence Detector (TID), the FMC now requires that the server certificate be generated with keys that are at least 2048 bits long. Certificates previously generated with 1024-bit keys will no longer work. If you cannot connect, regenerate the server certificate on your data source. If necessary, reconfigure the FMC connection to the data source.
Version 6.3.0.1 EMS extension support	**Upgrade impact.** Version 6.3.0.1 reintroduces EMS extension support, which was introduced in Version 6.2.3.8/6.2.3.9 but was not included in Version 6.3.0. Both the **Decrypt-Resign** and **Decrypt-Known Key** SSL policy actions again support the EMS extension during ClientHello negotiation, enabling more secure communications. The EMS extension is defined by RFC 7627. In FMC deployments, this feature depends on the *device* version. Although best practice is to upgrade your whole deployment, this feature is supported even if you patch only the device.

Table 83: FMC Features in Version 6.3.0

Feature	Details
Platform	
FMC 1600, 2600, and 4600.	We introduced the FMC models FMC 1600, 2600, and 4600.
ISA 3000 with FirePOWER Services.	ISA 3000 with FirePOWER Services is supported in Version 6.3 (Protection license only). Although ISA 3000 with FirePOWER Services was also supported in Version 5.4.x, you cannot upgrade to Version 6.3 You must reimage.
Hardware bypass support for the Firepower 2100.	Firepower 2100 series devices now support hardware bypass functionality when using the hardware bypass network modules. New/modified pages: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** Supported platforms: Firepower 2100 series
Support for data EtherChannels in On mode for the Firepower 4100/9300.	You can now set data and data-sharing EtherChannels to either Active LACP mode or to On mode. Other types of EtherChannels only support Active mode. New/modified Firepower Chassis Manager pages: **Interfaces** > **All Interfaces** > **Edit Port Channel** > **Mode** New/modified FXOS commands: **set port-channel-mode** Supported platforms: Firepower 4100/9300
Firepower Threat Defense: HA and Clustering	

Feature	Details
Multi-instance capability for Firepower 4100/9300.	You can now deploy multiple logical devices, each with a Firepower Threat Defense container instance, on a single security engine/module. Formerly, you could only deploy a single native application instance. To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances. Resource management lets you customize performance capabilities for each instance. You can use high availability using a container instance on 2 separate chassis. Clustering is not supported. **Note** Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode is not available for FTD. New/modified FMC pages: **Devices** > **Device Management >** edit device **> Interfaces** tab New/modified Firepower Chassis Manager pages: • **Overview** > **Devices** • **Interfaces** > **All Interfaces** > **Add New** drop-down menu **> Subinterface** • **Interfaces** > **All Interfaces** > **Type** • **Logical Devices** > **Add Device** • **Platform Settings** > **Mac Pool** • **Platform Settings** > **Resource Profiles** New/modified FXOS commands: **connect ftd***name*, **connect module telnet**, **create bootstrap-key PERMIT_EXPERT_MODE**,**create resource-profile**, **create subinterface**, **scope auto-macpool**, **set cpu-core-count**, **set deploy-type**, **set port-type data-sharing**, **set prefix**, **set resource-profile-name**, **set vlan**, **scope app-instance ftd** *name*, **show cgroups container**, **show interface**, **show mac-address**, **show subinterface**, **show tech-support module app-instance**, **show version** Supported platforms: Firepower 4100/9300
Cluster control link customizable IP Address for the Firepower 4100/9300	By default, the cluster control link uses the 127.2.0.0/16 network. You can now set the network when you deploy the cluster in FXOS. The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: 127.2.*chassis_id*.*slot_id*. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. Therefore, you can now set a custom /16 subnet for the cluster control link in FXOS except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses. New/modified Firepower Chassis Manager pages: **Logical Devices** > **Add Device** > **Cluster Information** New/modified options: **CCL Subnet IP** field New/modified FXOS commands: **set cluster-control-link network** Supported platforms: Firepower 4100/9300

Feature	Details
Improved FTD cluster addition to the FMC	You can now add any unit of a cluster to the FMC, and the other cluster units are detected automatically. Formerly, you had to add each cluster unit as a separate device, and then group them into a cluster with the FMC. Adding a cluster unit is also now automatic. Note that you must delete a unit manually. New/modified pages: • **Devices** > **Device Management** > **Add** drop-down menu > **Device** > **Add Device** dialog box • **Devices** > **Device Management** > **Cluster** tab > **General** area > **Cluster Registration Status** > **Current Cluster Summary** link > **Cluster Status** dialog box Supported platforms: Firepower 4100/9300
Firepower Threat Defense: Encryption and VPN	
SSL hardware acceleration	Additional FTD devices now support SSL hardware acceleration. Also, this option is now enabled by default. Upgrading to Version 6.3.0 automatically enables SSL hardware acceleration on eligible devices. Using SSL hardware acceleration if you are not decrypting traffic can affect performance. We recommend you disable SSL hardware acceleration on devices that are not decrypting traffic. Supported platforms: Firepower 2100 series, Firepower 4100/9300
RA VPN: RADIUS Dynamic Authorization or Change of Authorization (CoA)	You can now use RADIUS servers for user authorization of RA VPN using dynamic access control lists (ACLs) or ACL names per user. Supported platforms: FTD
RA VPN: Two-Factor Authentication	Firepower Threat Defense now supports two-factor authentication for RA VPN users using the Cisco AnyConnect Secure Mobility Client. For the two-factor authentication process, we support: • First factor: any RADIUS or LDAP/AD server • Second factor: RSA tokens or DUO passcodes pushed to mobile For more information on Duo multi-factor authentication (MFA) for FTD, see the Cisco Firepower Threat Defense (FTD) VPN with AnyConnect documentation on the Duo Security website. Supported platforms: FTD
Security Policies	

Feature	Details
Firepower Threat Defense service policy	You can now configure a Firepower Threat Defense service policy as part of your access control policy advanced options. Use FTD service policies to apply services to specific traffic classes. Features supported include: • TCP State Bypass • Randomizing TCP sequence numbers • Decrementing the time-to-live (TTL) value on packets • Dead Connection Detection • Setting a limit on the maximum number of connections and embryonic connections per traffic class and per client. • Timeouts for embryonic, half closed, and idle connections **Note** Before Version 6.3.0, you could configure connection-related service rules using the TCP_Embryonic_Conn_Limit and TCP_Embryonic_Conn_Timeout predefined FlexConfig objects. You should remove those objects and redo your rules in the FTD service policy. If you created any custom FlexConfig objects to implement any of these connection-related features (that is, **set connection** commands), you should also remove those objects and implement the features through the FTD service policy. Failure to do so can cause deployment issues. The *Threat Defense Service Policies* chapter in the FMC configuration guide has details on how service policies relate to FlexConfig and other features. New/modified pages: **Policies** > **Access Control >** edit/create policy **> Advanced** tab **> Threat Defense Service Policy** Supported platforms: FTD
Update interval for URL category and reputation data	**Upgrade impact.** You can now force URL data to expire. There is a tradeoff between security and performance. A shorter interval means you use more current data, while a longer interval can make web browsing faster for your users. If you worked with Cisco TAC to specify a timeout value for the URL filtering cache, the upgrade may change that value. Otherwise, the setting defaults to disabled (the current behavior), meaning that cached URL data does not expire. New/modified pages: **System** > **Integration** > **Cisco CSI** > **Cached URLs Expire** setting Supported platforms: FMC
Event Logging and Analysis	

Feature	Details
Cisco Security Packet Analyzer Integration	You can integrate with Cisco Security Packet Analyzer to examine events and display analysis results, or download results for further analysis. New/modified pages: • **System** > **Integration** > **Packet Analyzer** • **Analysis** > **Advanced** > **Packet Analyzer Queries** • **Query Packet Analyzer** when right-clicking on an event in the dashboard or event viewer Supported platforms: FMC
Contextual cross-launch	You can right-click an event in the dashboard or event viewer to look up related information in predefined or custom, public or private URL-based resources. New/modified pages: **Analysis** > **Advanced** > **Contextual Cross-Launch** Supported platforms: FMC
Unified syslog configuration	**Upgrade impact.** Version 6.3.0 changes and centralizes the way the system logs connection and intrusion events via syslog. Previously, you configured event logging via syslog in multiple places, depending on the event type. You now configure syslog messaging in the access control policy. These configurations affect connection and intrusion event logging for the access control, SSL, prefilter, and intrusion policies, as well as for Security Intelligence. The upgrade does not change your existing settings for connection event logging. However, you may suddenly start receiving intrusion events you did not "expect" via syslog. This is because the intrusion policy now sends syslog events to the destination specified in the access control policy. (Before, you could configure syslog alerting in an intrusion policy to send events to the syslog on the managed device itself rather than to an external host.) For FTD devices, some syslog platform settings now apply to connection and intrusion event messages. For a list, see the *Platform Settings for Firepower Threat Defense* chapter in the FMC configuration guide. For NGIPS devices (7000/8000 series, ASA FirePOWER, NGIPSv), messages now use the ISO 8601 timestamp format as specified in RFC 5425. Supported platforms: Any
Fully qualified syslog messages for connection and intrusion events	The format of syslog messages for connection, security intelligence, and intrusion events have the following changes: • Messages from FTD devices now include event type identification numbers. • Fields with empty or unknown values are no longer included, so messages are shorter and important data is less likely to be truncated. • Timestamps now use the ISO 8601 timestamp format as specified in the RFC 5425 syslog format (optional for FTD, required for Classic). Supported platforms: Any

Feature	Details
Other syslog improvements for FTD devices	You can send all syslog messages from the same interface (data or management), using the same IP address, using TCP or UDP protocol. Note that secure syslog is supported on data ports only. You can also use the RFC 5424 format for message timestamps. Supported platforms: FTD
Administration and Troubleshooting	
Export-controlled features for approved customers	Customers whose Smart Accounts are not otherwise eligible to use restricted functionality can purchase term-based licenses, with approval. New/modified pages: **System** > **Licenses** > **Smart Licenses** Supported platforms: FMC, FTD
Specific License Reservation for approved customers	Customers can use Specific License Reservation to deploy Smart Licensing in an air-gapped network. The FMC reserves licenses from your virtual account for a specified duration without accessing the Cisco Smart Software Manager or Smart Software Satellite Server. New/modified pages: **System** > **Licenses** > **Specific Licenses** Supported platforms: FMC, FTD (except ISA 3000)
IPv4 range, subnet, and IPv6 support for SNMP hosts	You can now use IPv4 range, IPv4 subnet, and IPv6 host network objects to specify the SNMP hosts that can access a Firepower Threat Defense device. New/modified pages: **Devices** > **Platform Settings** > create or edit FTD policy > **SNMP** > **Hosts** tab Supported platforms: FTD
Access control using fully qualified domain names (FQDN)	You can now create fully qualified domain name (FQDN) network objects and use them in access control and prefilter rules. To use FQDN objects, you must also configure DNS server groups and DNS platform settings, so that the system can resolve the domain names. New/modified pages: • **Objects** > **Object Management** > **Network** • **Objects** > **Object Management** > **DNS Server Group** • **Devices** > **Platform Settings** > create or edit FTD policy > **DNS** Supported platforms: FTD
CLI for the FMC	An CLI for the FMC supports a small set of basic commands (change password, show version, reboot/restart, and so on). By default the FMC CLI is disabled, and logging into FMC using SSH accesses the Linux shell. New/modified Classic CLI commands: The **system lockdown-sensor** command has changed to **system lockdown**. This command now works for both devices and FMCs. New/modified pages: **System** > **Configuration** > **Console Configuration** > **Enable CLI Access** check box Supported platforms: FMC, including FMCv

Feature	Details
Copy device configurations	You can copy device configurations and policies from one device to another. New/modified pages: **Devices** > **Device Management** > edit the device > **General** area > **Get/Push Device Configuration** icons. Supported platforms: FMC
Backup/restore FTD device configurations	You can use the FMC web interface to back up configurations for some FTD devices. New/modified pages: **System** > **Tools** > **Backup/Restore** New/modified CLI commands: **restore** Supported platforms: All physical FTD devices, FTDv for VMware
Skip deploying to up-to-date devices when you schedule deploy tasks	**Upgrade impact.** When you schedule a task to deploy configuration changes, you can now opt to **Skip Deployment for up-to-date devices**. This performance-enhancing setting is enabled by default. The upgrade process automatically enables this option on existing scheduled tasks. To continue to force a scheduled deploy to up-to-date devices, you must edit the scheduled task. New/modified pages: **System** > **Tools** > **Scheduling** > add or edit a task > choose **Job Type** of **Deploy Policies** Supported platforms: FMC
New health modules	New health modules alert you when: • **Threat Data Updates on Devices**: Threat identification data on managed devices fails to update. • **Realm**: A user is reported to the FMC without being downloaded, or a user logs into a domain that corresponds to a realm not known to the FMC. New/modified pages: • **System > Health > Policy** • **System > Health > Monitor** Supported platforms: FMC
Configurable packet capture size	You can now store up to 10 GB of packet captures. New/modified CLI commands: **file-size**, **show capture** Supported platforms: Firepower 4100/9300

Feature	Details
Web interface changes.	Version 6.3 changes these menu options: **Analysis > Advanced > Whois** is now **Analysis > Lookup > Whois** **Analysis > Advanced > Geolocation** is now **Analysis > Lookup > Geolocation** **Analysis > Advanced > URL** is now **Analysis > Lookup > URL** **Analysis > Advanced > Custom Workflows** is now **Analysis > Custom > Custom Workflows** **Analysis > Advanced > Custom Tables** is now **Analysis > Custom > Custom Tables** **Analysis > Hosts > Vulnerabilities** is now **Analysis > Vulnerabilities > Vulnerabilities** **Analysis > Hosts > Third-Party Vulnerabilities** is now **Analysis > Vulnerabilities > Third-Party Vulnerabilities**
Security and Hardening	
HTTPS Certificates	The default HTTPS server certificate provided with the system now expires in three years. If your appliance uses a default server certificate that was generated before you upgraded to Version 6.3.0, the server certificate will expire 20 years from when it was first generated. If you are using the default HTTPS server certificate the system now provides the ability to renew it. New/modified pages: **System** > **Configuration** > **HTTPS Certificate** > **Renew HTTPS Certificate** button New/modified Classic CLI commands: **show http-cert-expire-date**, **system renew-http-cert***new_key* Supported platforms: Physical FMCs, 7000/8000 series devices
Improved login security	**Upgrade impact.** Added FMC user configuration settings to improve login security: • **Track Successful Logins**: Track the number of successful logins each FMC account has performed within a specific time period. • **Password Reuse Limit**: Track an FMC user's password history to prevent reuse. • **Max Number of Login Failures** and **Set Time in Minutes to Temporarily Lockout Users**: Limit the number of times in a row an FMC user can enter incorrect web interface login credentials before being temporarily blocked. We also updated the list of supported ciphers and cryptographic algorithms for secure SSH access. If your SSH client fails to connect with a Firepower appliance due to a cipher error, update your client to the latest version. New/modified pages: **System** > **Configuration** > **User Configuration** Supported platforms: FMC

Feature	Details
Limit SSH login failures on devices	When a user accesses any device via SSH and fails three successive login attempts, the device terminates the SSH session. Supported platforms: Any device
Usability and Performance	
How-to walkthroughs	FMC walkthroughs (also called *how-tos*) guide you through a variety of basic tasks such as device setup and policy configuration. Just click **How To** at the bottom of the browser window, choose a walkthrough, and follow the step-by-step instructions. To end a walkthrough at any time, click the **x** in the upper right corner. **Note** FMC walkthroughs are tested on the Firefox and Chrome browsers. If you encounter issues with a different browser, we ask that you switch to Firefox or Chrome. If you continue to encounter issues, contact Cisco TAC. The following are some common problems and solutions: • **Problem:** Cannot find the link to start walkthroughs. **Solution:** Make sure walkthroughs are enabled. From the drop-down list under your username, select **User Preferences** then click **How-To Settings**. • **Problem:** Walkthrough appears when you do not expect it. **Solution:** End the walkthrough. • **Problem:** Walkthrough disappears or quits suddenly. **Solution:** Move your pointer, or navigate to a different page and try again. • **Problem:** Walkthrough is out of sync with the FMC (starts on the wrong step, advances prematurely, will not advance). **Solution:** Attempt to continue. For example, if you enter an invalid value in a field and the FMC displays an error, the walkthrough can prematurely move on. You may need to go back and resolve the error to complete the task. However, sometimes you cannot continue. For example, if you do not click **Next** after you complete a step, you may need to end the walkthrough, navigate to a different page, and try again.
Firepower Management Center REST API	
Bulk overrides	You can now perform bulk overrides on specific objects. For a full list, see the Cisco Firepower Management Center REST API Quick Start Guide.
Deprecated Features	
End of support: VMware vSphere/VMware ESXi 5.5.	Version 6.3 discontinues support for virtual deployments on VMware vSphere/VMware ESXi 6.0. Upgrade the hosting environment to a supported version before you upgrade the Firepower software.
End of support: ASA 5512-X and 5506-X series.	You cannot run Version 6.3+ on the ASA 5506-X, 5506H-X, 5506W-X, and 5512-X.

Feature	Details
Deprecated: EMS extension support for decryption (temporary).	**Upgrade impact.** Version 6.3.0 temporarily discontinues EMS extension support, which was introduced in Version 6.2.3.8/6.2.3.9. This means that the **Decrypt-Resign** and **Decrypt-Known Key** SSL policy actions no longer support the EMS extension during ClientHello negotiation, which would enable more secure communications. The EMS extension is defined by RFC 7627. In FMC deployments, this feature depends on the *device* version. Upgrading the FMC to Version 6.3.0 does not discontinue support, as long as the device is running a supported version. However, upgrading the device to Version 6.3.0 does discontinue support. Support is reintroduced in Version 6.3.0.1.
Deprecated: Decryption on passive and inline tap interfaces.	**Upgrade impact.** Version 6.3 ends support for decrypting traffic on interfaces in passive or inline tap mode, even though the GUI allows you to configure it. Any inspection of encrypted traffic is necessarily limited.
Deprecated: Default DNS group with FlexConfig.	Version 6.3 deprecates this FlexConfig object for FTD with FMC: • Default_DNS_Configure And these associated text objects: • defaultDNSNameServerList • defaultDNSParameters These allowed you to configure the Default DNS group, which defines the DNS servers that can be used when resolving fully qualified domain names on the data interfaces. This allowed you to use commands in the CLI, such as **ping**, using host names rather than IP addresses. You can now configure DNS for the data interfaces in the FTD platform settings policy: **Devices** > **Platform Settings** > create or edit FTD policy > **DNS**.

Feature	Details
Deprecated: Embryonic connection limit and timeout with FlexConfig.	**Can cause post-upgrade deployment issues.** Version 6.3 deprecates these FlexConfig objects for FTD with FMC: • TCP_Embryonic_Conn_Limit • TCP_Embryonic_Conn_Timeout And these associated text objects: • tcp_conn_misc • tcp_conn_limit • tcp_conn_timeout These allowed you to configure embryonic connection limits and timeouts to protect against SYN Flood Denial of Service (DoS) attacks. You can now configure these features in the FTD service policy: **Policies** > **Access Control** > add/edit policy > **Advanced** tab > **Threat Defense Service Policy**. **Caution** If you used **set connection** commands to implement connection-related service rules, you should remove the associated objects and implement the features through the FTD service policy. Failure to do so can cause deployment issues.
Deprecated: Geolocation details.	We no longer provide the geolocation IP package, which contained contextual data associated with routable IP addresses. This saves disk space and does not affect geolocation rules or traffic handling in any way. Any contextual data is now stale, and upgrading to most later versions deletes the IP package. Options to download the IP package or view contextual data have no effect, and are removed in later versions.

FMC Features in Version 6.2.3

Table 84: FMC Features in Version 6.2.3 Patches

Feature	Details
Version 6.2.3.13 Detection of rule conflicts in FTD NAT policies.	After you upgrade to Version 6.2.3.13+, you can no longer create FTD NAT policies with conflicting rules (often referred to as *duplicate* or *overlapping* rules). This fixes an issue where conflicting NAT rules were applied out-of-order. If you currently have conflicting NAT rules, you will be able to deploy post-upgrade. However, your NAT rules will continue to be applied out-of-order. Therefore, we recommend that after the upgrade, you inspect your FTD NAT policies by editing (no changes are needed) then attempting to resave. If you have rule conflicts, the system will prevent you from saving. Correct the issues, save, and then deploy. **Note** Upgrading to Version 6.3.0 or 6.4.0 deprecates this fix. The issue is addressed in Version 6.3.0.4 and 6.4.0.2. Supported platforms: FTD
Version 6.2.3.8 EMS extension support.	Both the **Decrypt-Resign** and **Decrypt-Known Key** SSL policy actions now support the EMS extension during ClientHello negotiation, enabling more secure communications. The EMS extension is defined by RFC 7627. **Note** Version 6.2.3.8 was removed from the Cisco Support & Download site on 2019-01-07. Upgrading to Version 6.2.3.9 also enables EMS extension support. Version 6.3.0 discontinues EMS extension support. In FMC deployments, this feature depends on the device version. Upgrading the FMC to Version 6.3.0 does not discontinue support, but upgrading the device does. Support is reintroduced in Version 6.3.0.1. Supported platforms: Any
Version 6.2.3.7 TLS v1.3 downgrade CLI command for FTD.	A new CLI command allows you to specify when to downgrade TLS v1.3 connections to TLS v1.2. Many browsers use TLS v1.3 by default. If you are using an SSL policy to handle encrypted traffic, and people in your monitored network use browsers with TLS v1.3 enabled, websites that support TLS v1.3 fail to load. For more information, see the **system support** commands in the *Cisco Secure Firewall Threat Defense Command Reference*. We recommend you use these commands only after consulting with Cisco TAC. Supported platforms: FTD
Version 6.2.3.3 Site-to-site VPN with clustering	You can now configure site-to-site VPN with clustering. Site-to-site VPN is a centralized feature; only the control unit supports VPN connections. Supported platforms: Firepower 4100/9300

Table 85: FMC Features in Version 6.2.3

Feature	Details
Platform	
FTD on the ISA 3000.	You can now run FTD on the ISA 3000 series. Note that the ISA 3000 supports the Threat license only. It does not support the URL Filtering or Malware licenses. Thus, you cannot configure features that require the URL Filtering or Malware licenses on an ISA 3000. Special features for the ISA 3000 that were supported with the ASA, such as Hardware Bypass, Alarm ports, and so on, are not supported with FTD in this release.
Support for VMware ESXi 6.5.	You can now deploy FMCv, FTDv, and NGIPSv virtual appliances on VMware vSphere/VMware ESXi 6.5.
Firepower Threat Defense: Encryption and VPN	
SSL hardware acceleration for Firepower 4100/9300.	Firepower 4100/9300 with FTD now support SSL encryption and decryption acceleration in hardware, greatly improving performance. SSL hardware acceleration is disabled by default for all appliances that support it. **Note** This feature is renamed *TLS crypto acceleration* in Version 6.4.0+. Supported platforms: Firepower 4100/9300
Certificate enrollment improvements.	Non-blocking work flow for certificate enrollment operation allows certificate enrollment on multiple FTD devices in parallel: • The administrator can now choose to have the Remote Access VPN Policy wizard enroll certificates for all devices in the policy by checking **Enroll the selected certificate object on the target devices** check box in the **Access & Certificate** step. If this is chosen, only deployment needs to be done after the wizard finishes. This is selected by default. • Administrators no longer have to initiate Remote Access VPN certificate enrollment on devices one at a time. The enrollment process for each device is now independent and can be done in parallel. • In the event of a PKS12 certificate enrollment failure, the administrator no longer needs to re-upload the PKS12 file again to retry enrollment, since it is now stored in the certificate enrollment object. Supported platforms: FTD
Firepower Threat Defense: High Availability and Clustering	
Automatically rejoin the FTD cluster after an internal failure.	Formerly, many internal error conditions caused a cluster unit to be removed from the cluster, and you were required to manually rejoin the cluster after resolving the issue. Now, a unit will attempt to rejoin the cluster automatically at the following intervals: 5 minutes, 10 minutes, and then 20 minutes. Internal failures include: application sync timeout; inconsistent application statuses; and so on. New/modified command: **show cluster info auto-join** Supported platforms: Firepower 4100/9300

Feature	Details
FTD high availability hardening.	Version 6.2.3 introduces the following features for FTD devices in high availability: • Whenever active or standby FTD devices in a high availability pair restart, the FMC may not display accurate high availability status for either managed device. However, the status may not upgrade on the FMC because the communication between the device and the FMC is not established yet. The **Refresh Node Status** option on the **Devices** > **Device Management** page allows you to refresh the high availability node status to obtain accurate information about the active and standby device in a high availability pair. • The **Devices** > **Device Management** page of the FMC UI has a new **Switch Active Peer** icon.
Administration and Troubleshooting	
FMC high availability messaging.	FMC high availability pairs have improved UI messaging. The UI now displays interim status messages while FMC pairs are being established and rephrased UI messaging to be more intuitive. Supported platforms: FMC
External authentication added for FTD SSH access.	You can now configure external authentication for SSH access to FTD devices using LDAP or RADIUS. New/modified screen: **Devices** > **Platform Settings** > **External Authentication** Supported platforms: FTD
Enhanced vulnerability database (VDB) installation.	The FMC now warns you before you install a VDB that installing restarts the Snort process, interrupting traffic inspection and, depending on how the managed device handles traffic, possibly interrupting traffic flow. You can cancel the install until a more convenient time, such as during a maintenance window. These warnings can appear: • After you download and manually install a VDB. • When you create a scheduled task to install the VDB. • When the VDB installs in the background, such as during a previously scheduled task or as part of a Firepower software upgrade. Supported platforms: FMC
Upgrade package push.	You can now copy (or push) an upgrade package from the FMC to a managed device before you run the actual upgrade. This is useful because you can push during times of low bandwidth use, outside of the upgrade maintenance window. When you push to high availability, clustered, or stacked devices, the system sends the upgrade package to the active/control/primary first, then to the standby/data/secondary. New/modified screens: **System** > **Updates** Supported platforms: FMC

Feature	Details
FTD serviceability.	Version 6.2.3 improves the **show fail over** CLI command. The new keyword, **-history**, details to help troubleshooting. • **Show fail over history** displays failure reason along with its specific details. • **Show fail over history details** displays fail over history from the peer unit. **Note** This command includes fail over state changes and the reason for the state change for the peer unit. Supported platforms: FTD
Device list sorting.	On the **Devices** > **Devices Management** page, you can use the **View by** drop-down list to sort and view the device list by any of the following categories: group, license, model, or access control policy. In a multidomain deployment, you can also sort and view by domain, which is the default display category in that deployment. Devices must belong to a leaf domain. Supported platforms: FMC
Audit log improvements.	The audit log now denotes if a policy changed on the FTD Platform Settings **Devices** > **Platform Settings** page. Supported platforms: FMC with FTD
Updated FTD CLI commands.	The **asa_mgmt_plane** and **asa_dataplane** options for FTD device CLI commands are renamed to **management-plane** and **data-plane** respectively. Supported platforms: FTD
Cisco Success Network.	**Upgrade impact.** Cisco Success Network sends usage information and statistics to Cisco, which are essential to provide you with technical support. During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time. Supported platforms: FMC
Web analytics tracking.	**Upgrade impact.** Web analytics provides non-personally-identifiable usage data to Cisco, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your Firewall Management Centers. Initial setup enrolls you in web analytics tracking by default, but you can change your enrollment at any time after that. Upgrades can also enroll or re-enroll you in web analytics tracking. Supported platforms: FMC
Performance	

Feature	Details
Snort restarts reduced for FTD devices.	In Version 6.2.3, fewer FTD configuration changes restart the Snort process on FTD devices. The FMC now warns you before you deploy if the configuration deployment restarts the Snort process, interrupting traffic inspection and, depending on how the managed device handles traffic, possibly interrupting traffic flow. Supported platforms: FTD
Traffic drop on policy apply.	Version 6.2.3 adds the **configure snort preserve-connection {enable | disable}** command to the FTD CLI. This command determines whether to preserve existing connections on routed and transparent interfaces if the Snort process goes down. When disabled, all new or existing connections are dropped when Snort goes down and remain dropped until Snort resume. When enabled, connections that were already allowed remain established, but new connections cannot be established until Snort is again available. Note that you cannot permanently disable this command on a FTD device managed by FDM; existing connections may drop when the settings revert to default during the next configuration deployment.
Increased memory capacity for lower-end appliances.	Versions 6.1.0.7, 6.2.0.5, 6.2.2.2, and 6.2.3 increase the memory capacity for lower-end Firepower appliances. This reduces the number of health alerts.
Faster ISE pxGrid discovery.	If an ISE pxGrid deployed in high availability fails or becomes unreachable, the FMC now discovers the new active pxGrid faster.
New result limits in reports.	**Upgrade can change report settings.** Version 6.2.3 limits the number of results you can use or include in a report section. For table and detail views, you can include fewer records in a PDF report than in an HTML/CSV report. For HTML/CSV report sections, the new limits are: • Bar and pie charts: 100 (top or bottom) • Table views: 400,000 • Detail views: 1,000 For PDF report sections, the new limits are: • Bar and pie charts: 100 (top or bottom) • Table views: 100,000 • Detail views: 500 If, before you upgrade the FMC, a section in a report template specifies a larger number of results than the HTML/CSV maximum, the upgrade process lowers the setting to the new maximum value. For report templates that generate PDF reports, if you exceed the PDF limit in any template section, the upgrade process changes the output format to HTML. To continue generating PDFs, lower the results limit to the PDF maximum. If you do this after the upgrade, set the output format back to PDF.
Deprecated Features	

Feature	Details
Expired CA certificates for dynamic analysis with AMP for Networks.	On June 15, 2018, some Firepower deployments stopped being able to submit files for dynamic analysis. This occurred due to an expired CA certificate that was required for communications with the AMP Threat Grid cloud. Version 6.3 is the first major version with the new certificate. If you do not want to upgrade to Version 6.3+, you can patch to obtain the new certificate and reenable dynamic analysis, as follows: • Version 6.2.3 → patch to Version 6.2.3.4 • Version 6.2.2 → patch to Version 6.2.2.4 • Version 6.2.1 → no patches available • Version 6.2 → patch to Version 6.2.0.6 • Version 6.1 → patch to Version 6.1.0.7 • Version 6.0 → no patches available You can also apply a hotfix. For available hotfixes, see the Release Notes for Cisco Secure Firewall Threat Defense and Firepower Hotfixes. Find the hotfix for your version and platform that applies to CSCvj07038*: Firepower devices need to trust Threat Grid certificate*. If this is your first time installing the patch or hotfix, make sure your firewall allows outbound connections to `fmc.api.threatgrid.com` (replacing `panacea.threatgrid.com`) from both the FMC and its managed devices. Note that upgrading a patched or hotfixed deployment to either Version 6.2.0 or Version 6.2.3 reverts to the old certificate and you must patch or hotfix again.
Deprecated: Geolocation details.	We no longer provide the geolocation IP package, which contained contextual data associated with routable IP addresses. This saves disk space and does not affect geolocation rules or traffic handling in any way. Any contextual data is now stale, and upgrading to most later versions deletes the IP package. Options to download the IP package or view contextual data have no effect, and are removed in later versions.

Release Dates

Table 86: Version 10 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
10.1.0	160	2026-09-21	Firewall Management Center All devices except Secure Firewall 200	Firewall Management Center All devices except Secure Firewall 200
	681	2026-09-21	Secure Firewall 200	Secure Firewall 200

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
10.0.2	79	2026-09-15	Firewall Management Center All devices except Secure Firewall 200	Firewall Management Center All devices except Secure Firewall 200
	564	2026-09-15	Secure Firewall 200	Secure Firewall 200
10.0.1	1	2026-02-18	Firewall Management Center	Firewall Management Center
10.0.0	141	2025-12-23	Firewall Management Center	Firewall Management Center
	140	2025-12-03	All devices except Secure Firewall 200	All devices except Secure Firewall 200
	637	2025-12-03	Secure Firewall 200	Secure Firewall 200

Table 87: Version 7.7 Dates

Version	Build	Date	Platforms
7.7.13	69	2026-09-15	All
7.7.12	3	2026-02-17	Firewall Management Center Firewall Threat Defense Virtual for GCP
7.7.11	1061	2025-12-01	All
7.7.10.1	6	2025-09-26	Firewall Management Center
	5	2025-09-25	All devices
7.7.10	3200	2025-08-18	All devices
	3089	2025-08-11	Firewall Management Center
7.7.0	91	2025-03-14	Firewall Management Center
	89	2025-03-05	All devices

Table 88: Version 7.6 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
7.6.6	115	2026-09-15	All	All
7.6.5	106	2026-02-17	Firewall Management Center	Firewall Management Center
7.6.4	69	2026-01-07	All	All
7.6.3	113	2025-10-23	Firewall Management Center	Firewall Management Center Firewall Threat Defense Virtual in the public cloud

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
7.6.2.1	3	2025-09-25	All	All
7.6.2	329	2025-08-11	All	All
7.6.1	291	2025-06-02	All	All
7.6.0	113	2024-09-16	All	All
	41	2024-06-27	—	No longer available.

Table 89: Version 7.4 Dates

Version	Build	Date	Platforms
7.4.8	79	2026-09-15	All
7.4.7	50	2026-04-15	All
7.4.6	7	2026-02-17	Firewall Management Center
7.4.5	2	2026-01-14	Firewall Management Center
7.4.4	462	2026-01-05	All devices
7.4.3	315	2025-10-13	All
7.4.2.4	9	2025-09-25	All
7.4.2.3	4	2025-06-17	All
7.4.2.2	28	2025-03-03	All
7.4.2.1	30	2024-10-09	All
7.4.2	172	2024-07-31	All
7.4.1.1	12	2024-04-15	All
7.4.1	172	2023-12-13	All
7.4.0	81	2023-09-07	Firewall Management Center Secure Firewall 4200 series

Table 90: 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

Version	Build	Date	Platforms
7.3.0	69	2022-11-29	All

Table 91: Version 7.2 Dates

Version	Build	Date	Platforms
7.2.12	90	2026-09-15	All
7.2.11	313	2026-02-17	All
7.2.10.2	2	2025-09-25	All
7.2.10.1	10	2025-09-4	Firewall Management Center
7.2.10	210	2025-05-22	All
7.2.9	44	2024-10-22	All
7.2.8.1	17	2024-08-26	All
7.2.8	25	2024-06-24	All
7.2.7	500	2024-04-29	All
7.2.6	168	2024-04-22	No longer available.
	167	2024-03-19	No longer available.
7.2.5.2	4	2024-05-06	All
7.2.5.1	29	2023-11-14	All
7.2.5	208	2023-07-27	All
7.2.4.1	43	2023-07-27	All
7.2.4	169	2023-05-10	Firewall Management Center
	165	2023-05-03	Devices
7.2.3.1	13	2023-04-18	Firewall Management Center
7.2.3	77	2023-02-27	All
7.2.2	54	2022-11-29	All
7.2.1	40	2022-10-03	All
7.2.0.1	12	2022-08-10	All
7.2.0	82	2022-06-06	All

Table 92: Version 7.1 Dates

Version	Build	Date	Platforms
7.1.0.3	108	2023-03-15	All
7.1.0.2	28	2022-08-03	Firewall Management Center, including virtual Secure Firewall 3100 series
7.1.0.1	28	2022-02-24	Firewall Management Center, including virtual All devices except Secure Firewall 3100 series
7.1.0	90	2021-12-01	All

Table 93: Version 7.0 Dates

Version	Build	Date	Platforms
7.0.10	63	2026-09-15	All
7.0.9	25	2026-02-17	All
7.0.8.1	4	2025-09-25	All
7.0.8	174	2025-08-12	All
7.0.7	519	2025-02-14	Firewall Threat Defense
	518	2025-01-29	Firewall Management Center, including virtual ASA FirePOWER NGIPSv
7.0.6.3	50	2024-09-10	All
7.0.6.2	65	2024-04-15	All
7.0.6.1	36	2023-11-13	All
7.0.6	236	2023-07-18	All
7.0.5.1	5	2023-04-26	NGIPSv For devices with security certifications compliance enabled (CC/UCAPL mode). Use with a Version 7.0.5 FMC.
7.0.5	72	2022-11-17	All
7.0.4	55	2022-08-10	All
7.0.3	37	2022-06-30	All
7.0.2.1	10	2022-06-27	All
7.0.2	88	2022-05-05	All

Version	Build	Date	Platforms
7.0.1.1	11	2022-02-17	All
7.0.1	84	2021-10-07	All
7.0.0.1	15	2021-07-15	All
7.0.0	94	2021-05-26	All

Table 94: Version 6.7 Dates

Version	Build	Date	Platforms
6.7.0.3	105	2022-02-17	All
6.7.0.2	24	2021-05-11	All
6.7.0.1	13	2021-03-24	All
6.7.0	65	2020-11-02	All

Table 95: Version 6.6 Dates

Version	Build	Date	Platforms
6.6.7.2	11	2024-04-24	All
6.6.7.1	42	2023-01-26	All
6.6.7	223	2022-07-14	All
6.6.5.2	14	2022-03-24	All
6.6.5.1	15	2021-12-06	All
6.6.5	81	2021-08-03	All
6.6.4	64	2021-04-29	Firepower 1000 series
	59	2021-04-26	Firewall Management Center, including virtual All devices except Firepower 1000 series
6.6.3	80	2021-03-11	All
6.6.1	91	2020-09-20	All
	90	2020-09-08	—
6.6.0.1	7	2020-07-22	All

Version	Build	Date	Platforms
6.6.0	90	2020-05-08	Firepower 4112
		2020-04-06	Firewall Management Center, including virtual All devices except Firepower 4112

Table 96: Version 6.5 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.5.0.5	95	2021-02-09	All	—
6.5.0.4	57	2020-03-02	All	—
6.5.0.3	30	2020-02-03	No longer available.	—
6.5.0.2	57	2019-12-19	All	—
6.5.0.1	35	2019-11-20	No longer available.	—
6.5.0	123	2020-02-03	Firewall Management Center, including virtual	Firewall Management Center, including virtual
	120	2019-10-08	—	—
	115	2019-09-26	All devices	All devices

Table 97: Version 6.4 Dates

Version	Build	Date	Platforms
6.4.0.18	24	2024-04-24	All
6.4.0.17	26	2023-09-28	All
6.4.0.16	50	2022-11-21	All
6.4.0.15	26	2022-05-31	All
6.4.0.14	67	2022-02-18	All
6.4.0.13	57	2021-12-02	All
6.4.0.12	112	2021-05-12	All
6.4.0.11	11	2021-01-11	All
6.4.0.10	95	2020-10-21	All
6.4.0.9	62	2020-05-26	All
6.4.0.8	28	2020-01-29	All
6.4.0.7	53	2019-12-19	All

Version	Build	Date	Platforms
6.4.0.6	28	2019-10-16	No longer available.
6.4.0.5	23	2019-09-18	All
6.4.0.4	34	2019-08-21	All
6.4.0.3	29	2019-07-17	All
6.4.0.2	35	2019-07-03	Firewall Management Center, including virtual Firewall Threat Defense, except Firepower 1000 series
	34	2019-06-27	—
		2019-06-26	Firepower 7000/8000 series ASA FirePOWER NGIPSv
6.4.0.1	17	2019-06-27	FMC 1600, 2600, 4600
		2019-06-20	Firepower 4115, 4125, 4145 Firepower 9300 with SM-40, SM-48, and SM-56 modules
		2019-05-15	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv Firepower 2110, 2120, 2130, 2140 Firepower 4110, 4120, 4140, 4150 Firepower 9300 with SM-24, SM-36, and SM-44 modules ASA 5508-X, 5515-X, 5516-X, 5525-X, 5545-X, 5555-X ASA 5585-X-SSP-10, -20, -40, -60 ISA 3000 Firewall Threat Defense Virtual Firepower 7000/8000 series NGIPSv

Version	Build	Date	Platforms
6.4.0	113	2020-03-03	Firewall Management Center, including virtual
	102	2019-06-20	Firepower 4115, 4125, 4145 Firepower 9300 with SM-40, SM-48, and SM-56 modules
		2019-06-13	Firepower 1010, 1120, 1140
		2019-04-24	Firepower 2110, 2120, 2130, 2140 Firepower 4110, 4120, 4140, 4150 Firepower 9300 with SM-24, SM-36, and SM-44 modules ASA 5508-X, 5515-X, 5516-X, 5525-X, 5545-X, 5555-X ASA 5585-X-SSP-10, -20, -40, -60 ISA 3000 Firewall Threat Defense Virtual Firepower 7000/8000 series NGIPSv

Table 98: Version 6.3 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.3.0.5	35	2019-11-18	Firepower 7000/8000 series NGIPSv	—
	34	2019-11-18	Firewall Management Center, including virtual Firewall Threat Defense ASA FirePOWER	—
6.3.0.4	44	2019-08-14	All	—
6.3.0.3	77	2019-06-27	FMC 1600, 2600, 4600	—
		2019-05-01	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices	—

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.3.0.2	67	2019-06-27	FMC 1600, 2600, 4600	—
		2019-03-20	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices	—
6.3.0.1	85	2019-06-27	FMC 1600, 2600, 4600	—
		2019-02-18	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices	—
6.3.0	85	2019-01-22	Firepower 4100/9300	Firepower 4100/9300
	84	2018-12-18	Firewall Management Center, including virtual ASA FirePOWER	—
	83	2019-06-27	—	FMC 1600, 2600, 4600
		2018-12-03	Firewall Threat Defense except Firepower 4100/9300 Firepower 7000/8000 NGIPSv	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices except Firepower 4100/9300

Table 99: Version 6.2.3 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.2.3.18	50	2022-02-16	All	—
6.2.3.17	30	2021-06-21	All	—
6.2.3.16	59	2020-07-13	All	—
6.2.3.15	39	2020-02-05	Firewall Threat Defense	—
	38	2019-09-18	Firewall Management Center, including virtual Firepower 7000/8000 ASA FirePOWER NGIPSv	—

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.2.3.14	41	2019-07-03	All	—
	36	2019-06-12	All	—
6.2.3.13	53	2019-05-16	All	—
6.2.3.12	80	2019-04-17	All	—
6.2.3.11	55	2019-03-17	All	—
	53	2019-03-13	—	—
6.2.3.10	59	2019-02-07	All	—
6.2.3.9	54	2019-01-10	All	—
6.2.3.8	51	2019-01-02	No longer available.	—
6.2.3.7	51	2018-11-15	All	—
6.2.3.6	37	2018-10-10	All	—
6.2.3.5	53	2018-11-06	Firewall Threat Defense	—
	52	2018-09-12	Firewall Management Center, including virtual Firepower 7000/8000 ASA FirePOWER NGIPSv	—
6.2.3.4	42	2018-08-13	All	—
6.2.3.3	76	2018-07-11	All	—
6.2.3.2	46	2018-06-27	All	—
	42	2018-06-06	—	—
6.2.3.1	47	2018-06-28	All	—
	45	2018-06-21	—	—
	43	2018-05-02	—	—

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.2.3	113	2020-06-01	Firewall Management Center, including virtual	Firewall Management Center, including virtual
	111	2019-11-25	—	Firewall Threat Defense Virtual: AWS, Azure
	110	2019-06-14	—	—
	99	2018-09-07	—	—
	96	2018-07-26	—	—
	92	2018-07-05	—	—
	88	2018-06-11	—	—
	85	2018-04-09	—	—
	84	2018-04-09	Firepower 7000/8000 series NGIPSv	—
	83	2018-04-02	Firewall Threat Defense ASA FirePOWER	Firewall Threat Defense hardware Firewall Threat Defense Virtual: VMware, KVM Firepower 7000/8000 ASA FirePOWER NGIPSv
	79	2018-03-29	—	—

Table 100: Version 6.2.2 Dates

Version	Build	Date	Platforms
6.2.2.5	57	2018-11-27	All
6.2.2.4	43	2018-09-21	Firewall Threat Defense
	34	2018-07-09	Firewall Management Center, including virtual Firepower 7000/8000 ASA FirePOWER NGIPSv
	32	2018-06-15	—

Version	Build	Date	Platforms
6.2.2.3	69	2018-06-19	All
	66	2018-04-24	—
6.2.2.2	109	2018-02-28	All
6.2.2.1	80	2017-12-05	Firepower 2100 series
	78	2017-11-20	—
	73	2017-11-06	Firewall Management Center, including virtual All devices except Firepower 2100 series
6.2.2	81	2017-09-05	All

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)

© 2021–2026 Cisco Systems, Inc. All rights reserved.