Features

This document describes the new and deprecated features for Version 6.7.

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

Upgrade Impact

A feature has upgrade impact if upgrading and deploying can cause the system to process traffic or otherwise act differently without any other action on your part; this is especially common with new threat detection and application identification capabilities. A feature can also have upgrade impact if upgrading requires that you take action before or after upgrade; for example, if you must change a configuration. In the next sections, we indicate upgrade impact for Version 6.7 features.

Snort

Snort 3 is the default inspection engine for FTD starting in Version 6.7 (with FDM) and Version 7.0 (with FMC). Snort 3 features for FMC deployments also apply to FDM, even if they are not listed as new FDM features. However, keep in mind that the FMC may offer more configurable options than FDM.

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

Intrusion Rules and Keywords

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

The Snort release notes contain details on new keywords: https://www.snort.org/downloads.

FlexConfig

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

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

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

FMC Features

FMC Features in Version 6.7

Table 1: FMC Features in Version 6.7

Feature	Details
Platform	
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

Feature	Details
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	
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

Feature	Details
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
Firepower 1100/2100 series SFP interfaces now support disabling auto-negotiation.	**Upgrade impact.** 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. New/modified pages: **Devices > Device Management > Interfaces >** edit interface **> Hardware Configuration > Speed** Supported platforms: Firepower 1100/2100 series
Firepower Threat Defense: Clustering	

Feature	Details
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
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	

Feature	Details
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
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
FMC REST API	
FMC REST API.	We added the following FMC REST API services/operations to support new and existing features. Authorization services: • ssoconfig: GET and PUT operations to retrieve and modify FMC single-sign on. Health services: • metrics: GET operation to retrieve metrics for the health monitor. • alerts: GET operation to retrieve health alerts. • deploymentdetails: GET operation to retrieve deployment health details. Deployment services: • jobhistories: GET operation to retrieve deployment history. • rollbackrequests: POST operation to request a configuration rollback. Device services: • metrics: GET operation to retrieve device metrics. • virtualtunnelinterfaces: GET, PUT, POST, and DELETE operations to retrieve and modify virtual tunnel interfaces. Integration services: • externalstorage: GET, GET by ID, and PUT operations to retrieve and modify external event storage configuration. Policy services: • intrusionpolicies: POST and DELETE operations to modify intrusion policies. Update services: • cancelupgrades: POST operation to cancel a failed upgrade. • retryupgrades: POST operation to retry a failed upgrade. Supported platforms: FMC
Deprecated Features	

Feature	Details
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.

Feature	Details
Deprecated: Geolocation details.	In May 2022 we split the GeoDB into two packages: a country code package that maps IP addresses to countries/continents, and an IP package that contains additional contextual data associated with routable IP addresses. The contextual data in the IP package can include additional location details, as well as connection information such as ISP, connection type, proxy type, domain name, and so on. The new country code package has the same file name as the old all-in-one package: Cisco_GEODB_Update-*date-build*. This allows deployments running Version 7.1 and earlier to continue to obtain GeoDB updates. If you manually download GeoDB updates—for example, in an air-gapped deployment—make sure you get the country code package and not the IP package. **Important** This split does not affect geolocation rules or traffic handling in any way—those rules rely only on the data in the country code package. However, because the country code package essentially replaces the all-in-one package, the contextual data is no longer updated and will grow stale. To obtain fresh data, upgrade or reimage the FMC to Version 7.2+ and update the GeoDB.

FDM Features

FDM Features in Version 6.7.x

Table 2: FDM Features in Version 6.7.x

Feature	Description
Platform Features	
Support ends for the ASA 5525-X, 5545-X, and 5555-X. The last supported release is Firepower Threat Defense 6.6.	You cannot install Firepower Threat Defense 6.7 on an ASA 5525-X, 5545-X, or 5555-X. The last supported release for these models is Firepower Threat Defense 6.6.
Firewall and IPS Features	
TLS server identity discovery for access control rule matching.	TLS 1.3 certificates are encrypted. For traffic encrypted with TLS 1.3 to match access rules that use application or URL filtering, the system must decrypt the TLS 1.3 certificate. We recommend that you enable **TLS Server Identity Discovery** to ensure encrypted connections are matched to the right access control rule. The setting decrypts the certificate only; the connection remains encrypted. We added the **Access Control Settings** (⚙) button and dialog box to the **Policy** > **Access Control** page.

Feature	Description
External trusted CA certificate groups.	You can now customize the list of trusted CA certificates used by the SSL decryption policy. By default, the policy uses all system-defined trusted CA certificates, but you can create a custom group to add more certificates, or replace the default group with your own, more limited, group. We added certificate groups to the **Objects** > **Certificates** page, and modified the SSL decryption policy settings to allow the selection of certificate groups.
Active Directory realm sequences for passive identity rules.	You can create a realm sequence, which is an ordered list of Active Directory (AD) servers and their domains, and use them in a passive authentication identity rule. Realm sequences are useful if you support more than one AD domain and you want to do user-based access control. Instead of writing separate rules for each AD domain, you can write a single rule that covers all of your domains. The ordering of the AD realms within the sequence is used to resolve identity conflicts if any arise. We added the AD realm sequence object on the **Objects** > **Identity Sources** page, and the ability to select the object as a realm in a passive authentication identity rule. In the Firepower Threat Defense API, we added the **RealmSequence** resource, and in the **IdentityRule** resource, we added the ability to select a realm sequence object as the realm for a rule that uses passive authentication as the action.
FDM support for Trustsec security group tag (SGT) group objects and their use in access control rules.	In Firepower Threat Defense 6.5, support was added to the Firepower Threat Defense API to configure SGT group objects and use them as matching criteria in access control rules. In addition, you could modify the ISE identity object to listen to the SXP topic published by ISE. Now, you can configure these features directly in FDM. We added a new object, SGT groups, and updated the access control policy to allow their selection and display. We also modified the ISE object to include the explicit selection of topics to subscribe to.
Snort 3.0 support.	For new systems, Snort 3.0 is the default inspection engine. If you upgrade to 6.7 from an older release, Snort 2.0 remains the active inspection engine, but you can switch to Snort 3.0. For this release, Snort 3.0 does not support virtual routers, time-based access control rules, or the decryption of TLS 1.1 or lower connections. Enable Snort 3.0 only if you do not need these features. You can freely switch back and forth between Snort 2.0 and 3.0, so you can revert your change if needed. Traffic will be interrupted whenever you switch versions. We added the ability to switch Snort versions to the **Device** > **Updates** page, in the **Intrusion Rules** group. In the Firepower Threat Defense API, we added the IntrusionPolicy resource action/toggleinspectionengine. In addition, there is a new audit event, Rules Update Event, that shows which intrusion rules were added, deleted, or changed in a Snort 3 rule package update.

Feature	Description
Custom intrusion policies for Snort 3.	You can create custom intrusion policies when you are using Snort 3 as the inspection engine. In comparison, you could use the pre-defined policies only if you use Snort 2. With custom intrusion policies, you can add or remove groups of rules, and change the security level at the group level to efficiently change the default action (disabled, alert or drop) of the rules in the group. Snort 3 intrusion policies give you more control over the behavior of your IPS/IDS system without the need to edit the base Cisco Talos-provided policies. We changed the **Policies** > **Intrusion** page to list intrusion policies. You can create new ones, and view or edit existing policies, including adding/removing groups, assigning security levels, and changing the action for rules. You can also select multiple rules and change their actions. In addition, you can select custom intrusion policies in access control rules.
Multiple syslog servers for intrusion events.	You can configure multiple syslog servers for intrusion policies. Intrusion events are sent to each syslog server. We added the ability to select multiple syslog server objects to the intrusion policy settings dialog box.
URL reputation matching can include sites with unknown reputations.	When you configure URL category traffic-matching criteria, and select a reputation range, you can include URLs with unknown reputation in the reputation match. We added the **Include Sites with Unknown Reputation** check box to the URL reputation criteria in access control and SSL decyption rules.
VPN Features	
Virtual Tunnel Interface (VTI) and route-based site-to-site VPN.	You can now create route-based site-to-site VPNs by using a Virtual Tunnel Interface as the local interface for the VPN connection profile. With route-based site-to-site VPN, you manage the protected networks in a given VPN connection by simply changing the routing table, without altering the VPN connection profile at all. You do not need to keep track of remote networks and update the VPN connection profile to account for these changes. This simplifies VPN management for cloud service providers and large enterprises. We added the **Virtual Tunnel Interfaces** tab to the Interface listing page, and updated the site-to-site VPN wizard so that you can use a VTI as the local interface.
FTD API support for Hostscan and Dynamic Access Policy (DAP) for remote access VPN connections.	You can upload Hostscan packages and the Dynamic Access Policy (DAP) rule XML file, and configure DAP rules to create the XML file, to control how group policies are assigned to remote users based on attributes related to the status of the connecting endpoint. You can use these features to perform Change of Authorization if you do not have Cisco Identity Services Engine (ISE). You can upload Hostscan and configure DAP using the Firepower Threat Defense API only; you cannot configure them using FDM. See the AnyConnect documentation for information about Hostscan and DAP usage. We added or modified the following Firepower Threat Defense API object models: dapxml, hostscanpackagefiles, hostscanxmlconfigs, ravpns.

Feature	Description
Enabling certificate revocation checking for external CA certificates.	You can use the Firepower Threat Defense API to enable certificate revocation checking on a particular external CA certificate. Revocation checking is particularly useful for certificates used in remote access VPN. You cannot configure revocation checking on a certificate using FDM, you must use the Firepower Threat Defense API. We added the following attributes to the ExternalCACertificate resource: revocationCheck, crlCacheTime, oscpDisableNonce.
Support removed for less secure Diffie-Hellman groups, and encryption and hash algorithms.	**Upgrade impact. Can prevent post-upgrade deploy.** The following features were deprecated in 6.6 and they are now removed. If you are still using them in IKE proposals or IPsec policies, you must replace them after upgrade before you can deploy any configuration changes. We recommend that you change your VPN configuration prior to upgrade to supported DH and encryption algorithms to ensure the VPN works correctly. • 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.
Custom port for remote access VPN.	You can configure the port used for remote access VPN (RA VPN) connections. If you need to connect to FDM on the same interface used for RA VPN, you can change the port number for RA VPN connections. FDM uses port 443, which is also the default RA VPN port. We updated the global settings step of the RA VPN wizard to include port configuration.
SAML Server support for authenticating remote access VPN.	You can configure a SAML 2.0 server as the authentication source for a remote access VPN. Following are the supported SAML servers: Duo. We added SAML server as an identity source on the **Objects** > **Identity Sources** page, and updated remote access VPN connection profiles to allow its use.
FTD API Support for AnyConnect module profiles.	You can use the Firepower Threat Defense API to upload module profiles used with AnyConnect, such as AMP Enabler, ISE Posture, or Umbrella. You must create these profiles using the offline profile editors that you can install from the AnyConnect profile editor package. We added the anyConnectModuleType attribute to the AnyConnectClientProfile model. Although you can initially create AnyConnect Client Profile objects that use module profiles, you will still need to use the API to modify the objects created in FDM to specify the correct module type.
Routing Features	

Feature	Description
EIGRP support using Smart CLI.	**Upgrade impact. Can prevent post-upgrade deploy.** In previous releases, you configured EIGRP in the Advanced Configuration pages using FlexConfig. Now, you configure EIGRP using Smart CLI directly on the Routing page. If you configured EIGRP using FlexConfig, when you upgrade to release 6.7, you must remove the FlexConfig object from the FlexConfig policy, and then recreate your configuration in the Smart CLI object. You can retain your EIGRP FlexConfig object for reference until you have completed the Smart CLI updates. Your configuration is not automatically converted. We added the EIGRP Smart CLI object to the Routing pages.
Interface Features	
ISA 3000 hardware bypass persistence.	You can now enable hardware bypass for ISA 3000 interface pairs with the persistence option: after power is restored, hardware bypass remains enabled until you manually disable it. If you enable hardware bypass without persistence, hardware bypass is automatically disabled after power is restored. There may be a brief traffic interruption when hardware bypass is disabled. The persistence option lets you control when the brief interruption in traffic occurs. New/Modified screen: **Device** > **Interfaces** > **Hardware Bypass** > **Hardware Bypass Configuration**
Synchronization between the Firepower Threat Defense operational link state and the physical link state for the Firepower 4100/9300.	The Firepower 4100/9300 chassis can now synchronize the Firepower Threat Defense 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 Firepower Threat Defense application interface admin state is not considered. Without synchronization from Firepower Threat Defense, data interfaces can be in an Up state physically before the Firepower Threat Defense application has completely come online, for example, or can stay Up for a period of time after you initiate an Firepower Threat Defense shutdown. This feature is disabled by default, and can be enabled per logical device in FXOS. **Note** This feature is not supported for an Firepower Threat Defense with a Radware vDP decorator. New/Modified Firepower Chassis Manager screens: **Logical Devices > Enable Link State** New/Modified FXOS commands: **set link-state-sync enabled**, **show interface expand detail** Supported platforms: Firepower 4100/9300
Firepower 1100 and 2100 SFP interfaces now support disabling auto-negotiation.	You can now configure a Firepower 1100 and 2100 SFP interface to disable auto-negotiation. For 10GB interfaces, you can configure the speed down to 1GB without auto-negotiation; you cannot disable auto-negotiation for an interface with the speed set to 10GB. New/Modified screen: **Device > Interfaces > Edit Interface > Advanced Options > Speed** Supported platforms: Firepower 1100 and 2100

Feature	Description
Administrative and Troubleshooting Features	
Ability to cancel a failed Firepower Threat Defense software upgrade and to revert to the previous release.	If an Firepower Threat Defense major software upgrade fails or is otherwise not functioning correctly, you can revert to the state of the device as it was when you installed the upgrade. We added the ability to revert the upgrade to the System Upgrade panel in FDM. During an upgrade, the FDM login screen shows the upgrade status and gives you the option to cancel or revert in case of upgrade failure. In the Firepower Threat Defense API, we added the CancelUpgrade, RevertUpgrade, RetryUpgrade, and UpgradeRevertInfo resources. In the Firepower Threat Defense CLI, we added the following commands: **show last-upgrade status**, **show upgrade status**, **show upgrade revert-info**, **upgrade cancel**, **upgrade revert**, **upgrade cleanup-revert**, **upgrade retry**.
Custom HTTPS port for FDM/Firepower Threat Defense API access on data interfaces.	You can change the HTTPS port used for FDM or Firepower Threat Defense API access on data interfaces. By changing the port from the default 443, you can avoid conflict between management access and other features, such as remote access VPN, configured on the same data interface. Note that you cannot change the management access HTTPS port on the management interface. We added the ability to change the port to the **Device** > **System Settings** > **Management Access** > **Data Interfaces** page.
Low-touch provisioning for Cisco Defense Orchestrator on Firepower 1000 and 2100 series devices.	If you plan on managing a new Firepower Threat Defense device using Cisco Defense Orchestrator (CDO), you can now add the device without completing the device setup wizard or even logging into FDM. New Firepower 1000 and 2100 series devices are initially registered in the Cisco cloud, where you can easily claim them in CDO. Once in CDO, you can immediately manage the devices from CDO. This low-touch provisioning minimizes the need to interact directly with the physical device, and is ideal for remote offices or other locations where your employees are less experienced working with networking devices. We changed how Firepower 1000 and 2100 series devices are initially provisioned. We also added auto-enrollment to the **System Settings** > **Cloud Services** page, so that you can manually start the process for upgraded devices or other devices that you have previously managed using FDM.

Feature	Description
FTD API support for SNMP configuration.	**Upgrade impact. Can prevent post-upgrade deploy.** You can use the Firepower Threat Defense API to configure SNMP version 2c or 3 on an FDM or CDO managed Firepower Threat Defense device. We added the following API resources: SNMPAuthentication, SNMPHost, SNMPSecurityConfiguration, SNMPServer, SNMPUser, SNMPUserGroup, SNMPv2cSecurityConfiguration, SNMPv3SecurityConfiguration. **Note** If you used FlexConfig to configure SNMP, you must redo your configuration using the Firepower Threat Defense API SNMP resources. The commands for configuring SNMP are no longer allowed in FlexConfig. Simply removing the SNMP FlexConfig object from the FlexConfig policy will allow you to deploy changes; you can then use the object as reference while you use the API to reconfigure the feature.
Maximum backup files retained on the system is reduced from 10 to 3.	The system will retain a maximum of 3 backup files on the system rather than 10. As new backups are created, the oldest backup file is deleted. Please ensure that you download backup files to a different system so that you have the versions required to recover the system in case you need to.
Support ended for 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.
FTD API Version backward compatibility.	Starting with Firepower Threat Defense Version 6.7, if an API resource model for a feature does not change between releases, then the Firepower Threat Defense API can accept calls that are based on the older API version. Even if the feature model did change, if there is a logical way to convert the old model to the new model, the older call can work. For example, a v4 call can be accepted on a v5 system. If you use “latest” as the version number in your calls, these “older” calls are interpreted as a v5 call in this scenario, so whether you are taking advantage of backward compatibility depends on how you are structuring your API calls.
FTD REST API version 6 (v6).	The Firepower Threat Defense REST API for software version 6.7 is version 6. You can use v6 in the API URLs, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. Please re-evaluate all existing calls, as changes might have been mode to the resource models you are using. To open the API Explorer, where you can view the resources, log into FDM, then click the more options button (⋮) and choose **API Explorer**.