

Features

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

Upgrade Impact

A feature has upgrade impact if upgrading and deploying can cause the system to process traffic or otherwise act differently without any other action on your part. This is especially common with new threat detection and application identification capabilities. A feature can also have upgrade impact if upgrading requires that you take action before or after upgrade to avoid an undesirable outcome; for example, if you must change a configuration.

The feature descriptions here include upgrade impact where appropriate.

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 .

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

Snort Features

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



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

Intrusion Rules and Keywords

Upgrades can import and auto-enable new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. If a newer intrusion rule uses keywords that

are not supported in your current version, that rule is not imported when you update the SRU/LSP. After you upgrade and those keywords become supported, the new intrusion rules are imported and, depending on your IPS configuration, can become auto-enabled and thus start generating events and affecting traffic flow.

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

FlexConfig

Upgrades can add web interface or Smart CLI support for features that previously required FlexConfig. Although you cannot newly assign or create FlexConfig objects using deprecated commands, in most cases existing FlexConfigs continue to work and you can still deploy. However, sometimes, using deprecated commands can cause deployment issues. The upgrade does not convert FlexConfigs. After upgrade, configure the newly supported features in the web interface or Smart CLI. When you are satisfied with the new configuration, delete the deprecated FlexConfigs.

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

Integrations and Logging

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

- Syslog: *Cisco Secure Firewall Threat Defense Syslog Messages*
- Cisco Success Network: Cisco Success Network Telemetry Data Collected from Cisco Firepower Management Center
- REST API: *Secure Firewall Management Center REST API Quick Start Guide* and *Cisco Secure Firewall Threat Defense REST API Guide*

- FMC Features in Version 7.0.10, on page 2
- FMC Features in Version 7.0.9, on page 3
- FMC Features in Version 7.0.8, on page 3
- FMC Features in Version 7.0.7, on page 3
- FMC Features in Version 7.0.6, on page 5
- FMC Features in Version 7.0.5, on page 7
- FMC Features in Version 7.0.4, on page 7
- FMC Features in Version 7.0.3, on page 8
- FMC Features in Version 7.0.2, on page 8
- FMC Features in Version 7.0.1, on page 10
- FMC Features in Version 7.0.0, on page 11
- FDM Features in Version 7.0.x, on page 24

FMC Features in Version 7.0.10

There are no new features in this release. See Resolved Bugs in Version 7.0.10.

FMC Features in Version 7.0.9

There are no new features in this release. See Resolved Bugs in Version 7.0.9.

FMC Features in Version 7.0.8

Table 1: 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 2: FMC Features in Version 7.0.7

Feature	Minimum FMC	Minimum FTD	Details
Access Control: File and Malware			

Feature	Minimum FMC	Minimum FTD	Details
New Cisco AMP cloud connection method. Deprecated Cisco AMP Cloud connection backups.	7.0.7 7.2.10 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 replaces AMP private cloud connections with US public cloud connections. Pre-upgrade, the readiness check fails once if you have private AMP connections. **Tip** To avoid this, delete private cloud connections before upgrade and reconnect after upgrade. Use **Integration** > **AMP Management**. Other restrictions: Version 7.0.7 Firewall Management Centers are not listed on **Management** > **Computers** in the Secure Endpoint console. Although you can still integrate with Secure Endpoint, you cannot use the console to run diagnostics, see a risk score, quick-link to events and trajectories, apply policies, and so on.
Administration			
Cisco Security Cloud regions: India and Australia.	7.0.7 7.2.9 7.6.0	7.0.7 7.2.9 7.6.0	Cisco Security Cloud 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 3: 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.
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 4: 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 5: 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: Cloud-Delivered Firewall Management Center for Firewall Threat Defense*.

FMC Features in Version 7.0.2

Table 6: 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 7: 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 8: 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 (**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: **System** (⚙) > **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			
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**

Feature	Minimum FMC	Minimum FTD	Details
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.
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**.

Feature	Minimum FMC	Minimum FTD	Details
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 view contextual data have no effect, and are removed in later versions.

FDM Features in Version 7.0.x

Table 9: FDM Features in Version 7.0.x

Feature	Description
Platform Features	
FTDv for HyperFlex and Nutanix.	We introduced FTDv for Cisco HyperFlex and Nutanix Enterprise Cloud.
FTDv for VMware vSphere/VMware ESXi 7.0.	You can now deploy FTDv 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 FTD.
New default password for the Firewall Threat Defense Virtual on AWS.	On AWS, the default admin password for the Firewall Threat Defense Virtual is the AWS Instance ID, unless you define a default password with user data (**Advanced Details** > **User Data**) during the initial deployment.

Feature	Description
ISA 3000 support for shutting down.	In Version 7.0.2+, you can shut down the ISA 3000; previously, you could only reboot the device. In Version 7.0.5+, 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. Version restrictions: Version 7.1 temporarily deprecates support for this feature. Support returns in Version 7.2.
Firewall and IPS Features	
New Section 0 for system-defined NAT rules.	A new Section 0 has been added 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.
Custom intrusion rules for Snort 3.	You can use offline tools to create custom intrusion rules for use with Snort 3, and upload them into an intrusion policy. You can organize custom rules in your own custom rule groups, to make it easy to update them as needed. You can also create the rules directly in Firewall Device Manager, but the rules have the same format as uploaded rules. Firewall Device Manager does not guide you in creating the rules. You can duplicate existing rules, including system-defined rules, as a basis for a new intrusion rule. We added support for custom groups and rules to the **Policies** > **Intrusion** page, when you edit an intrusion policy.
Snort 3 new features for Firewall Device Manager-managed systems.	You can now configure the following additional features when using Snort 3 as the inspection engine on an Firewall Device Manager-managed system: • Time-based access control rules. (Firewall Threat Defense API only.) • Multiple virtual routers. • The decryption of TLS 1.1 or lower connections using the SSL Decryption policy. • The decryption of the following protocols using the SSL Decryption policy: FTPS, SMTPS, IMAPS, POP3S.
DNS request filtering based on URL category and reputation.	You can apply your URL filtering category and reputation rules to DNS lookup requests. If the fully-qualified domain name (FQDN) in the lookup request has a category and reputation that you are blocking, the system blocks the DNS reply. Because the user does not receive a DNS resolution, the user cannot complete the connection. Use this option to apply URL category and reputation filtering to non-web traffic. You must have the URL filtering license to use this feature. We added the **Reputation Enforcement on DNS Traffic** option to the access control policy settings.

Feature	Description
Smaller VDB for lower memory devices with Snort 2.	**Upgrade impact. Application identification on lower memory devices is affected.** For Version 7.0.6+ devices with Snort 2, 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-5508-X, ASA-5516-X Version restrictions: The smaller VDB is not supported in all versions. If you upgrade from a supported version to an unsupported version, you cannot install VDB 363+ on lower memory devices running Snort 2. For a list of affected releases, see CSCwd88641.
VPN Features	
Firewall Device Manager SSL cipher settings for remote access VPN.	You can define the TLS versions and encryption ciphers to use for remote access VPN connections in Firewall Device Manager. Previously, you needed to use the Firewall Threat Defense API to configure SSL settings. We added the following pages: **Objects** > **SSL Ciphers**; **Device** > **System Settings** > **SSL Settings**.
Support for Diffie-Hellman group 31.	You can now use Diffie-Hellman (DH) group 31 in IKEv2 proposals and policies.
The maximum number of Virtual Tunnel Interfaces on the device is 1024.	The maximum number of Virtual Tunnel Interfaces (VTI) that you can create is 1024. In previous versions, the maximum was 100 per source interface.
IPsec lifetime settings for site-to-site VPN security associations.	You can change the default settings for how long a security association is maintained before it must be re-negotiated. We added the **Lifetime Duration** and **Lifetime Size** options to the site-to-site VPN wizard.
Routing Features	
Virtual router support for the ISA 3000.	You can configure up to 10 virtual routers on an ISA 3000 device.
Equal-Cost Multi-Path (ECMP) routing.	You can configure ECMP traffic zones to contain multiple interfaces, which lets traffic from an existing connection exit or enter the Firewall Threat Defense device on any interface within the zone. This capability allows Equal-Cost Multi-Path (ECMP) routing on the Firewall Threat Defense device as well as external load balancing of traffic to the Firewall Threat Defense device across multiple interfaces. ECMP traffic zones are used for routing only. They are not the same as security zones. We added the **ECMP Traffic Zones** tab to the Routing pages. In the Firewall Threat Defense API, we added the ECMPZones resources.
Interface Features	
New default inside IP address.	The default IP address for the inside interface is being changed to **192.168.95.1** from 192.168.1.1 to avoid an IP address conflict when an address on 192.168.1.0/24 is assigned to the outside interface using DHCP.

Feature	Description
Default outside IP address now has IPv6 autoconfiguration enabled; new default IPv6 DNS server for Management.	The default configuration on the outside interface now includes IPv6 autoconfiguration, in addition to the IPv4 DHCP client. The default Management DNS servers now also include an IPv6 server: 2620:119:35::35.
EtherChannel support for the ISA 3000.	You can now use Firewall Device Manager to configure EtherChannels on the ISA 3000. New/modified screens: **Devices** > **Interfaces** > **EtherChannels**
Licensing Features	
Performance-Tiered Licensing for Firewall Threat Defense Virtual.	The Firewall Threat Defense Virtual now supports performance-tiered Smart Licensing based on throughput requirements and RA VPN session limits. When the Firewall Threat Defense Virtual is licensed with one of the available performance licenses, two things occur. First, a rate limiter is installed that limits the device throughput to a specified level. Second, the number of VPN sessions is capped to the level specified by the license.
Administrative and Troubleshooting Features	
DHCP relay configuration using the Firewall Threat Defense API.	**Upgrade impact. Can prevent post-upgrade deploy.** You can use the Firewall Threat Defense API to configure DHCP relay. Using DHCP relay on an interface, you can direct DHCP requests to a DHCP server that is accessible through the other interface. You can configure DHCP relay on physical interfaces, subinterfaces, EtherChannels, and VLAN interfaces. You cannot configure DHCP relay if you configure a DHCP server on any interface. Note that if you used FlexConfig in prior releases to configure DHCP relay (the **dhcprelay** command), you must re-do the configuration using the API, and delete the FlexConfig object, after you upgrade. We added the following model to the Firewall Threat Defense API: dhcprelayservices
Faster bootstrap processing and early login to Firewall Device Manager.	The process to initially bootstrap an Firewall Device Manager-managed system has been improved to make it faster. Thus, you do not need to wait as long after starting the device to log into Firewall Device Manager. In addition, you can now log in while the bootstrap is in progress. If the bootstrap is not complete, you will see status information on the process so you know what is happening on the device.
Improved CPU usage and performance for many-to-one and one-to-many connections.	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 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**
Upgrade readiness check for Firewall Device Manager-managed devices.	You can run an upgrade readiness check on an uploaded Firewall Threat Defense upgrade package before attempting to install it. The readiness check verifies that the upgrade is valid for the system, and that the system meets other requirements needed to install the package. Running an upgrade readiness check helps you avoid failed installations. A link to run the upgrade readiness check was added to the **System Upgrade** section of the **Device** > **Updates** page.

Feature	Description
Automatically update CA bundles.	**Upgrade impact. The system connects to Cisco for something new.** The local CA bundle contains certificates to access several Cisco services. The system now automatically queries Cisco for new CA certificates at a daily system-defined time. Previously, you had to upgrade the software to update CA certificates. You can use the CLI to disable this feature. New 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** Version restrictions: Requires Version 7.0.5, 7.1.0.3, or 7.2.4+. See: *Cisco Secure Firewall Threat Defense Command Reference*
Require the Message-Authenticator attribute in all RADIUS responses.	**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 **Require Message-Authenticator for all RADIUS Responses** 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 CLI commands: **message-authenticator-required** Version restrictions: Requires Version 7.0.7, 7.2.10, 7.4.3, 7.6.1, or 7.7+. For the Firepower 4100/9300, may require an FXOS upgrade; for minimum builds, see *Cisco Secure Firewall Threat Defense Compatibility Guide*.
Firewall Threat Defense REST API version 6.1 (v6).	The Firewall Threat Defense REST API for software version 7.0 is version 6.1 You can use v6 in the API URLs, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. Note that the URL version path element for 6.1 is the same as 6.0: v6. Please re-evaluate all existing calls, as changes might have been mode to the resource models you are using. To open the API Explorer, where you can view the resources, log into Firewall Device Manager, then click the more options button (⋮) and choose **API Explorer**.