Features

This document describes the new and deprecated features for Version 6.4.

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.

Intrusion Rules and Keywords

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

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

FlexConfig

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

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

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

FMC Features in Version 6.4.x

Table 1: FMC Features in Version 6.4.x Patches

Feature	Details
Version 6.4.0.17 Smaller VDB for lower memory devices.	For VDB 363+, the system now installs a smaller VDB (also called *VDB lite*) on lower memory devices. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Minimum threat defense: Any Lower memory devices: ASA 5506-X series, ASA-5508-X, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X Version restrictions: The ability to install a smaller VDB depends on the version of the FMC, not managed devices. If you upgrade the FMC from a supported version to an unsupported version, you cannot install VDB 363+ if your deployment includes even one lower memory device. For a list of affected releases, see CSCwd88641.
Version 6.4.0.10 Upgrades postpone scheduled tasks.	**Upgrade impact.** Upgrades now postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. **Note** Before you begin any upgrade, you must still make sure running tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Note that this feature is supported for Firepower appliances *running* Version 6.4.0.10 or any later patch. It is not supported for upgrades *to* Version 6.4.0.10, or upgrades that skip Version 6.4.0.10. This feature is temporarily deprecated in Versions 6.5.0–6.6.1, but returns in Version 6.6.3.
Version 6.4.0.9 Default HTTPS server certificates.	**Upgrade impact.** Upgrading an FMC or 7000/8000 series device from Version 6.4.0–6.4.0.8 to any later Version 6.4.0.x patch (or an FMC to Version 6.6.0+) renews the *default* HTTPS server certificate, which expires 800 days from the date of the upgrade. All future renewals have an 800 day lifespan. Your old certificate was set to expire depending on when it was generated, as follows: • 6.4.0 to 6.4.0.8: 3 years • 6.3.0 and all patches: 3 years • 6.2.3 and earlier: 20 years Note that in Version 6.5.0–6.5.0.4, the lifespan-on-renew returns to 3 years, but this is again updated to 800 days with Version 6.5.0.5 and 6.6.0.

Feature	Details
Version 6.4.0.4 New syslog fields.	These new syslog fields collectively identify a unique connection event: • Sensor UUID • First Packet Time • Connection Instance ID • Connection Counter These fields also appear in syslogs for intrusion, file, and malware events, allowing connection events to be associated with those events.
Version 6.4.0.2 Detection of rule conflicts in FTD NAT policies.	**Upgrade impact.** After you upgrade to Version 6.4.0.2 or later patch, you can no longer create FTD NAT policies with conflicting rules (often referred to as *duplicate* or *overlapping* rules). This fixes an issue where conflicting NAT rules were applied out-of-order. If you currently have conflicting NAT rules, you will be able to deploy post-upgrade. However, your NAT rules will continue to be applied out-of-order. Therefore, we recommend that after the upgrade, you inspect your FTD NAT policies by editing (no changes are needed) then attempting to resave. If you have rule conflicts, the system will prevent you from saving. Correct the issues, save, and then deploy.
Version 6.4.0.2 ISE Connection Status Monitor health module.	A new health module, the *ISE Connection Status Monitor*, monitors the status of the server connections between the Cisco Identity Services Engine (ISE) and the FMC.

Table 2: FMC Features in Version 6.4.0

Feature	Details
Platform	
FMC 1600, 2600, and 4600.	We introduced the FMC models FMC 1600, 2600, and 4600.
FMCv for Azure.	We introduced FMCv for Microsoft Azure.
FTD on the Firepower 1010, 1120, and 1140.	We introduced the Firepower 1010, 1120, and 1140.
FTD on the Firepower 4115, 4125, and 4145.	We introduced the Firepower 4115, 4125, and 4145.
Firepower 9300 SM-40, SM-48, and SM-56 support.	We introduced three new security modules: SM-40, SM-48, and SM-56. With FXOS 2.6.1, you can mix different types of security modules in the same chassis.
ASA and FTD on the same Firepower 9300.	With FXOS 2.6.1, you can now deploy ASA and FTD logical devices on the same Firepower 9300.
Firepower Threat Defense: Device Management	

Feature	Details
FTDv for VMware defaults to vmxnet3 interfaces.	FTDv for VMware now defaults to vmxnet3 interfaces when you create a virtual device. Previously, the default was e1000. The vmxnet3 device drivers and network processing are integrated with the ESXi hypervisor, so they use fewer resources and offer better network performance. **Note** Version 6.6 ends support for e1000 interfaces. You will not be able to upgrade to Version 6.6+ until you switch to vmxnet3 or ixgbe interfaces. We recommend you do this now. For more information, refer to the instructions on adding and configuring VMware interfaces in the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide. Supported platforms: FTDv for VMware
Firepower Threat Defense: Routing	
Rotating (keychain) authentication for OSPFv2 routing.	You can now use rotating (keychain) authentication when configuring OSPFv2 routing. New/modified pages: • **Objects** > **Object Management** > **Key Chain** object • **Devices** > **Device Management** > edit device > **Routing** tab > **OSPF** settings > **Interface** tab > add/edit interface > **Authentication** option • **Devices** > **Device Management** > edit device > **Routing** tab > **OSPF** settings > **Area** tab > add/edit area > **Virtual Link** sub-tab > add/edit virtual link > **Authentication** option Supported platforms: FTD
Firepower Threat Defense: Encryption and VPN	
RA VPN: Secondary authentication.	Secondary authentication, also called double authentication, adds an additional layer of security to RA VPN connections by using two different authentication servers. With secondary authentication enabled, AnyConnect VPN users must provide two sets of credentials to log in to the VPN gateway. RA VPN supports secondary authentication for the AAA Only and Client Certificate and AAA authentication methods. New/modified pages: **Devices** > **VPN** > **Remote Access** > add/edit configuration > **Connection Profile** > **AAA** area Supported platforms: FTD
Site-to-site VPN: Dynamic IP addresses for extranet endpoints.	You can now configure site to site VPNs to use a dynamic IP address for extranet endpoints. In hub-and-spoke deployments, you can use a hub as an extranet endpoint. New/modified pages: **Devices** > **VPN** > **Site To Site** > add/edit FTD VPN topology > **Endpoints** tab > add endpoint > **IP Address** option Supported platforms: FTD

Feature	Details
Site-to-site VPN: Dynamic crypto maps for point-to-point topologies.	You can now use dynamic crypto maps in point-to-point as well as in hub-and-spoke VPN topologies. Dynamic crypto maps are still not supported for full mesh topologies. You specify the crypto map type when you configure a topology. Make sure you also specify a dynamic IP address for one of the peers in the topology. New/modified pages: **Devices** > **VPN** > **Site To Site >** add/edit FTD VPN topology **> IPsec** tab **> Crypto Map Type** option Supported platforms: FTD
TLS crypto acceleration.	**Upgrade impact.** SSL hardware acceleration has been renamed *TLS crypto acceleration*. Depending on the device, TLS crypto acceleration might be performed in software or in hardware. The Version 6.4.0 upgrade process automatically enables acceleration on all eligible devices, even if you previously disabled the feature manually. In most cases you cannot configure this feature; it is automatically enabled and you cannot disable it. However, if you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can enable TLS crypto acceleration for *one* container instance per module/security engine. Acceleration is disabled for other container instances, but enabled for native instances. New FXOS CLI commands for the Firepower 4100/9300 chassis: • **show hwCrypto** • **config hwCrypto** New FTD CLI commands: • **show crypto accelerator status** (replaces **system support ssl-hw-status**) Removed FTD CLI commands: • **system support ssl-hw-accel** • **system support ssl-hw-status** Supported platforms: Firepower 2100 series, Firepower 4100/9300
Event Logging and Analysis	
Improvements to syslog messages for file and malware events.	Fully qualified file and malware event data can now be sent from managed devices via syslog. New/modified pages: **Policies** > **Access Control** > **Access Control >** add/edit policy **> Logging** tab **> File and Malware Settings** area Supported platforms: Any
Search intrusion events by CVE ID.	You can now search for intrusion events generated as a result of a particular CVE exploit. New/modified pages: **Analysis** > **Search** Supported platforms: FMC

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

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

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

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

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

Feature	Details
New REST API capabilities.	Added REST API objects to support Version 6.4.0 features: • cloudeventsconfigs: Manage SecureX integration. • ftddevicecluster: Manage chassis clustering. • hitcounts: Manage hit count statistics for access control and prefilter rules. • keychain: Manage key chain objects used for rotating authentication when configuring OSPFv2 routing. • loggingsettings: Manage logging settings for access control policies Supported platforms: FMC
API Explorer based on OAS.	Version 6.4.0 uses a new API Explorer, based on the OpenAPI Specification (OAS). As part of the OAS, you now use CodeGen to generate sample code. You can still access the legacy API Explorer if you prefer. Supported platforms: FMC
Deprecated Features	
Deprecated: SSL hardware acceleration FTD CLI commands.	As part of the TLS crypto acceleration feature, we removed the following FTD CLI commands: • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status**
Deprecated: Geolocation details.	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 in Version 6.4.x

Table 3: FDM Features in Version 6.4.x

Feature	Description
Firepower 1000 series device configuration.	You can configure Firepower Threat Defense on Firepower 1000 series devices using FDM. Note that you can configure and use the Power over Ethernet (PoE) ports as regular Ethernet ports, but you cannot enable or configure any PoE-related properties.
Hardware bypass for the ISA 3000.	You can now configure hardware bypass for the ISA 3000 on the **Device** > **Interfaces** page. In release 6.3, you needed to configure hardware bypass using FlexConfig. If you are using FlexConfig, please redo the configuring on the Interfaces page and remove the hardware bypass commands from FlexConfig. However, the portion of the FlexConfig devoted to disabling TCP sequence number randomization is still recommended.
Ability to reboot and shut down the system from the FDM CLI Console.	You can now issue the **reboot** and **shutdown** commands through the CLI Console in FDM. Previously, you needed to open a separate SSH session to the device to reboot or shut down the system. You must have Administrator privileges to use these commands.
External Authentication and Authorization using RADIUS for Firepower Threat Defense CLI Users.	You can use an external RADIUS server to authenticate and authorize users logging into the Firepower Threat Defense CLI. You can give external users config (administrator) or basic (read-only) access. We added the SSH configuration to the **AAA Configuration** tab on the **Device** > **System Settings** > **Management Access** page.
Support for network range objects and nested network group objects.	You can now create network objects that specify a range of IPv4 or IPv6 addresses, and network group objects that include other network groups (that is, nested groups). We modified the network object and network group object Add/Edit dialog boxes to include these features, and modified the various security policies to allow the use of these objects, contingent on whether address specifications of that type make sense within the context of the policy.
Full-text search options for objects and rules.	You can do a full-text search on objects and rules. By searching a policy or object list that has a large number of items, you can find all items that include your search string anywhere within the rule or object. We added a search box to all policies that have rules, and to all pages on the **Objects** list. In addition, you can use the **filter=fts~***search-string* option on GET calls for supported objects in the API to retrieve items based on a full-text search.
Obtaining a list of supported API versions for an FDM-managed Firepower Threat Defense device.	You can use the GET /api/versions (ApiVersions) method to get a list of the API versions that are supported on a device. You can use your API client to communicate and configure the device using commands and syntax valid for any of the supported versions.

Feature	Description
Hit counts for access control rules.	You can now view hit counts for access control rules. The hit counts indicate how often connections matched the rule. We updated the access control policy to include hit count information. In the Firepower Threat Defense API, we added the HitCounts resource and the **includeHitCounts** and **filter=fetchZeroHitCounts** options to the GET Access Policy Rules resource.
Site-to-Site VPN enhancements for dynamic addressing and certificate authentication.	You can now configure site-to-site VPN connections to use certificates instead of preshared keys to authenticate the peers. You can also configure connections where the remote peer has an unknown (dynamic) IP address. We added options to the Site-to-Site VPN wizard and the IKEv1 policy object.
Support for RADIUS servers and Change of Authorization in remote access VPN.	You can now use RADIUS servers for authenticating, authorizing, and accounting remote access VPN (RA VPN) users. You can also configure Change of Authentication (CoA), also known as dynamic authorization, to alter a user's authorization after authentication when you use a Cisco ISE RADIUS server. We added attributes to the RADIUS server and server group objects, and made it possible to select a RADIUS server group within an RA VPN connection profile.
Multiple connection profiles and group policies for remote access VPN.	You can configure more than one connection profile, and create group policies to use with the profiles. We changed the **Device** > **Remote Access VPN** page to have separate pages for connection profiles and group policies, and updated the RA VPN Connection wizard to allow the selection of group policies. Some items that were previously configured in the wizard are now configured in the group policy.
Support for certificate-based, second authentication source, and two-factor authentication in remote access VPN.	You can use certificates for user authentication, and configure secondary authentication sources so that users must authenticate twice before establishing a connection. You can also configure two-factor authentication using RSA tokens or Duo passcodes as the second factor. We updated the RA VPN Connection wizard to support the configuration of these additional options.
Support for IP address pools with multiple address ranges, and DHCP address pools, for remote access VPN.	You can now configure address pools that have more than one address range by selecting multiple network objects that specify subnets. In addition, you can configure address pools in a DHCP server and use the server to provide addresses to RA VPN clients. If you use RADIUS for authorization, you can alternatively configure the address pools in the RADIUS server. We updated the RA VPN Connection wizard to support the configuration of these additional options. You can optionally configure the address pool in the group policy instead of the connection profile.

Feature	Description
Active Directory realm enhancements.	You can now include up to 10 redundant Active Directory (AD) servers in a single realm. You can also create multiple realms and delete realms that you no longer need. In addition, the limit for downloading users in a realm is increased to 50,000 from the 2,000 limit in previous releases. We updated the **Objects** > **Identity Sources** page to support multiple realms and servers. You can select the realm in the user criteria of access control and SSL decryption rules, to apply the rule to all users within the realm. You can also select the realm in identity rules and RA VPN connection profiles.
Redundancy support for ISE servers.	When you configure Cisco Identity Services Engine (ISE) as an identity source for passive authentication, you can now configure a secondary ISE server if you have an ISE high availability setup. We added an attribute for the secondary server to the ISE identity object.
File/malware events sent to external syslog servers.	You can now configure an external syslog server to receive file/malware events, which are generated by file policies configured on access control rules. File events use message ID 430004, malware events are 430005. We added the File/Malware syslog server options to the **Device** > **System Settings** > **Logging Settings** page.
Logging to the internal buffer and support for custom event log filters.	You can now configure the internal buffer as a destination for system logging. In addition, you can create event log filters to customize which messages are generated for the syslog server and internal buffer logging destinations. We added the Event Log Filter object to the **Objects** page, and the ability to use the object on the **Device** > **System Settings** > **Logging Settings** page. The internal buffer options were also added to the **Logging Settings** page.
Certificate for the FDM Web Server.	You can now configure the certificate that is used for HTTPS connections to the FDM configuration interface. By uploading a certificate your web browsers already trust, you can avoid the Untrusted Authority message you get when using the default internal certificate. We added the **Device** > **System Settings** > **Management Access** > **Management Web Server** page.
Cisco Threat Response support.	You can configure the system to send intrusion events to the Cisco Threat Response cloud-based application. You can use Cisco Threat Response to analyze intrusions. We added Cisco Threat Response to the **Device** > **System Settings** > **Cloud Services** page.

Feature	Description
Manually upload VDB, GeoDB, and SRU updates.	You can now manually retrieve update packages for VDB, Geolocation Database, and Intrusion Rules, and then upload them from your workstation to the FTD device using FDM. For example, if you have an air-gapped network, where FDM cannot retrieve updates from the Cisco Cloud, you can now get the update packages you need. We updated the **Device > Updates** page to allow you to select and upload a file from your workstation. Minimum FTD: 6.4.0.10. Version restrictions: This feature is not available in Version 6.5. Support returns in Version 6.6.
Smaller VDB for lower memory devices devices.	For VDB 363+, the system now installs a smaller VDB (also called *VDB lite*) on lower memory devices. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Minimum FTD: 6.4.0.17 Lower memory devices: ASA-5508-X, ASA-5515-X, ASA-5516-X, ASA-5525-X, ASA-5545-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. For a list of affected releases, see CSCwd88641.
Universal Permanent License Reservation (PLR) mode.	If you have an air-gapped network, where there is no path to the internet, you cannot register directly with the Cisco Smart Software Manager (CSSM) for Smart Licensing. In this situation, you can now get authorization to use Universal Permanent License Reservation (PLR) mode, where you can apply a license that does not need direct communication with CSSM. If you have an air-gapped network, please contact your account representative and ask for authorization to use Universal PLR mode in your CSSM account, and to obtain the necessary licenses. We added the ability to switch to PLR mode, and to cancel and unregister a Universal PLR license, to the **Device > Smart License** page. In the FTD API, there are new resources for PLRAuthorizationCode, PLRCode, PLRReleaseCode, PLRRequestCode, and actions for PLRRequestCode, InstallPLRCode, and CancelReservation. Minimum FTD: 6.4.0.10. This feature is temporarily deprecated in Version 6.5 and returns in Version 6.6. If you are running Version 6.4.0.10 or later patch, we recommend you upgrade directly to Version 6.6+.

Feature	Description
Default HTTPS server certificates.	**Upgrade impact.** Patching may renew the device's current *default* HTTPS server certificate. Your certificate is set to expire depending on when it is generated, as follows: • 6.5.0.5+: 800 days • 6.5.0 to 6.5.0.4: 3 years • 6.4.0.9 and later patches: 800 days • 6.4.0 to 6.4.0.8: 3 years • 6.3.0 and all patches: 3 years • 6.2.3: 20 years
New syslog fields.	These new syslog fields collectively identify a unique connection event: • Sensor UUID • First Packet Time • Connection Instance ID • Connection Counter These fields also appear in syslogs for intrusion, file, and malware events, allowing connection events to be associated with those events. Minimum FTD: 6.4.0.4
FTD REST API version 3 (v3).	The Firepower Threat Defense REST API for software version 6.4 has been incremented to version 3. You must replace v1/v2 in the API URLs with v3. The v3 API includes many new resources that cover all features added in software version 6.4. 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, change the end of the FDM URL to **/#/api-explorer** after logging in.