Features

This document describes the new and deprecated features for Version 6.6.

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.

Snort

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

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

Intrusion Rules and Keywords

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

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 6.6.x

Table 1: FMC Features in Version 6.6.3

Feature	Details
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 6.6.3+. It is not supported for upgrades *to* Version 6.6.3, unless you are upgrading from Version 6.4.0.10 or any later patch.
Appliance Configuration Resource Utilization health module.	**Upgrade impact for Version 6.7.0.** Version 6.6.3 improves device memory management and introduces a new health module: Appliance Configuration Resource Utilization. The module alerts when the size of your deployed configurations puts a device at risk of running out of memory. The alert shows you how much memory your configurations require, and by how much this exceeds the available memory. If this happens, re-evaluate your configurations. Most often you can reduce the number or complexity of access control rules or intrusion policies. For information on best practices for access control, see the configuration guide. The upgrade process automatically adds and enables this module in all health policies. After upgrade, apply health policies to managed devices to begin monitoring. **Note** This module requires Version 6.6.3 or later 6.6.x release or Version 7.0+ on both the FMC and managed devices. Version 6.7 *partially* and *temporarily* deprecates support for this module. For details, see Deprecated: Appliance Configuration Resource Utilization heath module (temporary). Full support returns in Version 7.0, where the module is renamed to Configuration Memory Allocation.

Table 2: FMC Features in Version 6.6.1

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

Table 3: FMC Features in Version 6.6.0

Feature	Description
Platform	
FTD on the Firepower 4112.	We introduced the Firepower 4112. You can also deploy ASA logical devices on this platform. Requires FXOS 2.8.1.
Larger instances for AWS deployments.	**Upgrade impact.** FTDv for AWS adds support for these larger instances: • C5.xlarge • C5.2xlarge • C5.4xlarge FMCv for AWS adds support for these larger instances: • C3.4xlarge • C4.4xlarge • C5.4xlarge All existing FMCv for AWS instance types are now deprecated (c3.xlarge, c3.2xlarge, c4.xlarge, c4.2xlarge). You must resize before you upgrade. For more information, see FMCv Requires 28 GB RAM for Upgrade.
Autoscale for cloud-based FTDv deployments.	We introduced support for AWS Auto Scale/Azure Autoscale. The serverless infrastructure in cloud-based deployments allow you to automatically adjust the number of FTDv instances in the Auto Scale group based on capacity needs. This includes automatic registering/unregistering to and from the managing FMC. Supported platforms: FTDv for AWS, FTDv for Azure
Firepower Threat Defense: Device Management	

Feature	Description
Obtain initial management interface IP address using DHCP.	For Firepower 1000/2000 series and ASA-5500-X series devices, the management interface now defaults to obtaining an IP address from DHCP. This change makes it easier for you to deploy a new device on your existing network. This feature is not supported for Firepower 4100/9300 chassis, where you set the IP address when you deploy the logical device. Nor is it supported for FTDv or the ISA 3000, which continue to default to 192.168.45.45. Supported platforms: Firepower 1000/2000 series, ASA-5500-X series
Configure MTU values in CLI.	You can now use the FTD CLI to configure MTU (maximum transmission unit) values for FTD device interfaces. The default is 1500 bytes. Maximum MTU values are: • Management interface: 1500 bytes • Eventing interface: 9000 bytes New FTD CLI commands: **configure network mtu** Modified FTD CLI commands: Added the **mtu-event-channel** and **mtu-management-channel** keyword to the **configure network management-interface** command. Supported platforms: FTD
Get threat defense upgrade packages from an internal web server.	FTD devices can now get upgrade packages from your own internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC. **Note** This feature is supported only for FTD devices running Version 6.6.0+. It is not supported for upgrades *to* Version 6.6.0, nor is it supported for the FMC or Classic devices. New/modified pages: **System** > **Updates** > **Upload Update** button > **Specify software update source** option Supported platforms: FTD
Connection-based troubleshooting enhancements.	We made the following enhancements to FTD CLI connection-based troubleshooting (debugging): • **debug packet-module trace**: Added to enable module level packet tracing. • **debug packet-condition**: Modified to support troubleshooting of ongoing connections. Supported platforms: FTD
Firepower Threat Defense: Clustering	

Feature	Description
Multi-instance clustering.	You can now create a cluster using container instances. On the Firepower 9300, you must include one container instance on each module in the cluster. You cannot add more than one container instance to the cluster per security engine/module. We recommend that you use the same security module or chassis model for each cluster instance. However, you can mix and match container instances on different Firepower 9300 security module types or Firepower 4100 models in the same cluster if required. You cannot mix Firepower 9300 and 4100 instances in the same cluster. New FXOS CLI commands: **set port-type cluster** New/modified Chassis Manager pages: • **Logical Devices** > **Add Cluster** • **Interfaces** > **All Interfaces** > **Add New** drop-down menu > **Subinterface** > **Type** field Supported platforms: Firepower 4100/9300
Parallel configuration sync to data units in FTD clusters.	The control unit in an FTD cluster now syncs configuration changes with slave units in parallel by default. Formerly, synching occurred sequentially. Supported platforms: Firepower 4100/9300
Messages for cluster join failure or eviction added to **show cluster history**.	We added new messages to the **show cluster history** command for when a cluster unit either fails to join the cluster or leaves the cluster. Supported platforms: Firepower 4100/9300
Firepower Threat Defense: Routing	
Virtual routers and VRF-Lite.	You can now create multiple virtual routers to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device. Virtual routers implement the "light" version of Virtual Routing and Forwarding, or VRF-Lite, which does not support Multiprotocol Extensions for BGP (MBGP). The maximum number of virtual routers you can create ranges from five to 100, and depends on the device model. For a full list, see the Virtual Routing for Firepower Threat Defense chapter in the *Firepower Management Center Configuration Guide*. New/modified pages: **Devices** > **Device Management** > edit device > **Routing** tab New FTD CLI commands: **show vrf**. Modified FTD CLI commands: Added the [**vrf** *name* | **all**] keyword set to the following CLI commands, and changed the output to indicate virtual router information where applicable: **clear ospf**, **clear route**, **ping**, **show asp table routing**, **show bgp**, **show ipv6 route**, **show ospf**, **show route**, **show snort counters**. Supported platforms: FTD, except Firepower 1010 and ISA 3000
Firepower Threat Defense: VPN	

Feature	Description
DTLS 1.2 in remote access VPN.	You can now use Datagram Transport Layer Security (DTLS) 1.2 to encrypt RA VPN connections. Use FTD platform settings to specify the minimum TLS protocol version that the FTD device uses when acting as a, RA VPN server. If you want to specify DTLS 1.2, you must also choose TLS 1.2 as the minimum TLS version. Requires Cisco AnyConnect Secure Mobility Client, Version 4.7+. New/modified pages: **Devices** > **Platform Settings** > add/edit Threat Defense policy > **SSL** > **DTLS Version** option Supported platforms: FTD, except ASA 5508-X and ASA 5516-X
Site-to-site VPN IKEv2 support for multiple peers.	You can now add a backup peer to a site-to-site VPN connection, for IKEv1 and IKEv2 point-to-point extranet and hub-and-spoke topologies. Previously, you could only configure backup peers for IKEv1 point-to-point topologies. New/modified pages: **Devices** > **VPN** > **Site to Site** > add or edit a point to point or hub and spoke FTD VPN topology > add endpoint > **IP Address** field now supports comma-separated backup peers Supported platforms: FTD
Security Policies	
Usability enhancements for security policies.	Version 6.6.0 makes it easier to work with access control and prefilter rules. You can now: • Edit certain attributes of multiple access control rules in a single operation: state, action, logging, intrusion policy, and so on. In the access control policy editor, select the relevant rules, right-click, and choose **Edit**. • Search access control rules by multiple parameters. In the access control policy editor, click the **Search Rules** text box to see your options. • View object details and usage in an access control or prefilter rule. In the access control or prefilter policy editor, right-click the rule and choose **Object Details**. Supported platforms: FMC
Object group search for access control policies.	While operating, FTD devices expand access control rules into multiple access control list entries based on the contents of any network objects used in the access rule. You can reduce the memory required to search access control rules by enabling object group search. With object group search enabled, the system does not expand network objects, but instead searches access rules for matches based on those group definitions. Object group search does not impact how your rules are defined or how they appear in the FMC. It impacts only how the device interprets and processes them while matching connections to access control rules. Object group search is disabled by default. New/modified pages: **Devices** > **Device Management** > edit device > **Device** tab > **Advanced Settings** > **Object Group Search** option Supported platforms: FTD

Feature	Description
Time-based rules in access control and prefilter policies.	You can now specify an absolute or recurring time or time range for a rule to be applied. The rule is applied based on the time zone of the device that processes the traffic. New/modified pages: • Access control and prefilter rule editors • **Devices** > **Platform Settings** > add/edit Threat Defense policy > **Time Zone** • **Objects** > **Object Management** > **Time Range** and **Time Zone** Supported platforms: FTD
Egress optimization re-enabled.	**Upgrade impact.** Version 6.6.0 fixes CSCvs86257. If egress optimization was: • Enabled but turned off, the upgrade turns it back on. (We turned off egress optimization in some Version 6.4.0.x and 6.5.0.x patches, even if the feature was enabled.) • Manually disabled, we recommend you reenable it post-upgrade: **asp inspect-dp egress-optimization**. Supported platforms: FTD
Event Logging and Analysis	
New datastore improves performance.	**Upgrade impact.** To improve performance, Version 6.6.0 uses a new datastore for connection and Security Intelligence events. After the upgrade finishes and the FMC reboots, historical connection and Security Intelligence events are migrated in the background, resource constrained. Depending on FMC model, system load, and how many events you have stored, this can take from a few hours up to a day. Historical events are migrated by age, newest events first. Events that have not been migrated do not appear in query results or dashboards. If you reach the connection event database limit before the migration completes, for example, because of post-upgrade events, the oldest historical events are not migrated. You can monitor event migration progress in the Message Center. Supported platforms: FMC
Wildcard support when searching connection and Security Intelligence events for URLs.	When searching connection and Security Intelligence events for URLs having the pattern **`example.com`**, you must now include wildcards. Specifically, use **`*example.com*`** for such searches. Supported platforms: FMC

Feature	Description
Monitor up to 300,000 concurrent user sessions with FTD devices.	In Version 6.6.0, some FTD device models support monitoring of additional concurrent user sessions (logins): • 300,000 sessions: Firepower 4140, 4145, 4150, 9300 • 150,000 sessions: Firepower 2140, 4112, 4115, 4120, 4125 All other devices continue to support the old limit of 64,000, except ASA FirePOWER which is limited to 2000. A new health module alerts you when the user identity feature's memory usage reaches a configurable threshold. You can also view a graph of the memory usage over time. New/modified pages: • **System** > **Health** > **Policy** > add or edit health policy > **Snort Identity Memory Usage** • **System** > **Health** > **Monitor** > select a device > **Graph** option for the Snort Identity Memory Usage module Supported platforms: FTD devices listed above
Integration with IBM QRadar.	You can use the new Cisco Firepower app for IBM QRadar as an alternate way to display event data and help you analyze, hunt for, and investigate threats to your network. Requires eStreamer. For more information, see the Integration Guide for the Cisco Firepower App for IBM QRadar. Supported platforms: FMC
Administration and Troubleshooting	

Feature	Description
New options for deploying configuration changes.	The **Deploy** button on the FMC menu bar is now a menu, with options that add the following functionality: • Status: For each device, the system displays whether changes need to be deployed; whether there are warnings or errors you should resolve before you deploy; and whether your last deploy is in process, failed, or completed successfully. • Preview: See all applicable policy and object changes you have made since you last deployed to the device. • Selective deploy: Choose from the policies and configurations you want to deploy to a managed device. • Deploy time estimate: Display an estimate of how long it will take to deploy to a particular device. You can display estimates for a full deploy, as well as for specific policies and configurations. • History: View details of previous deploys. New/modified pages: • **Deploy** > **Deployment** • **Deploy** > **Deployment History** Supported platforms: FMC
Initial configuration updates the VDB and schedules SRU updates.	On new and reimaged FMCs, the setup process now: • Downloads and installs the latest vulnerability database (VDB) update. • Enables daily intrusion rule (SRU) downloads. Note that the setup process does *not* enable auto-deploy after these downloads, although you can change this setting. Upgraded FMCs are not affected. New/modified pages: • **System** > **Updates** > **Product Updates** (VDB updates) • **System** > **Updates** > **Rule Updates** (SRU updates) Supported platforms: FMC
VDB match no longer required to restore FMC.	Restoring an FMC from backup no longer requires the same VDB on the replacement FMC. However, restoring does now replace the existing VDB with the VDB in the backup file. Supported platforms: FMC
HTTPS certificates with subject alternative name (SAN).	You can now request a HTTPS server certificate that secures multiple domain names or IP addresses by using SAN. For more information on SAN, see RFC 5280, section 4.2.1.6. New/modified pages: **System** > **Configuration** > **HTTPS Certificate** > **Generate New CSR** > **Subject Alternative Name** fields Supported platforms: FMC

Feature	Description
Real names associated with FMC user accounts.	You can now specify a real name when you create or modify an FMC user account. This can be a person's name, department, or other identifying attribute. New/modified pages: **System** > **Users** > **Users** > **Real Name** field. Supported platforms: FMC
Cisco Support Diagnostics on additional FTD platforms.	**Upgrade impact.** Cisco Support Diagnostics is now fully supported on all FMCs and FTD devices. Previously, support was limited to FMCs, Firepower 4100/9300 with FTD, and FTDv for Azure. For more information, see Sharing Data with Cisco. Supported platforms: FMC, FTD
Usability	
Light theme.	The FMC now defaults to the Light theme, which was introduced as a Beta feature in Version 6.5.0. Upgrading to Version 6.6.0 automatically switches you to the Light theme. You can switch back to the Classic theme in your user preferences. Although we cannot respond to everybody, we welcome feedback on the Light theme. Use the feedback link on the User Preferences page or contact us at fmc-light-theme-feedback@cisco.com. Supported platforms: FMC
Display time remaining for upgrades.	The FMC's Message Center now displays approximately how much time remains until an upgrade will complete. This does not include reboot time. New/modified pages: Message Center Supported platforms: FMC
Security and Hardening	
Default HTTPS server certificate renewals have 800 day lifespans.	**Upgrade impact.** Unless the current *default* HTTPS server certificate already has an 800-day lifespan, upgrading to Version 6.6.0 renews the certificate, which now expires 800 days from the date of the upgrade. All future renewals have an 800 day lifespan. Your old certificate was set to expire depending on when it was generated. Supported platforms: FMC
Firepower Management Center REST API	

Feature	Description
New REST API capabilities.	Added the following REST API services to support Version 6.6.0 features: • bgp, bgpgeneralsettings, ospfinterface, ospfv2routes, ospfv3interfaces, ospfv3routes, virtualrouters, routemaps, ipv4prefixlists, ipv6prefixlists, aspathlists, communitylists, extendedcommunitylists, standardaccesslists, standardcommunitylists, policylists: Routing • virtualrouters, virtualipv4staticroutes, virtualipv6staticroutes, virtualstaticroutes: Virtual routing • timeranges, globaltimezones, timezoneobjects: Time-based rules • commands: Run a limited set of CLI commands from the REST API • pendingchanges: Deploy improvements Added the following REST API services to support older features: • intrusionrules, intrusionpolicies: Intrusion policies Supported platforms: FMC
Changed REST API service name for extended access lists.	**Upgrade impact.** The extendedaccesslist (singular) service in the FMC REST API is now extendedaccesslist**s** (plural). Make sure you update your client. Using the old service name fails and returns an Invalid URL error. Request Type: GET URL to retrieve the extended access list associated with a specific ID: • Old: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist/{objectId} • New: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s**/{objectId} URL to retrieve a list of all extended access lists: • Old: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist • New: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s** Supported platforms: FMC
Deprecated Features	

Feature	Description
Deprecated: Lower-memory instances for cloud-based FMCv deployments.	For performance reasons, the following FMCv instances are no longer supported: • c3.xlarge on AWS • c3.2xlarge on AWS • c4.xlarge on AWS • c4.2xlarge on AWS • Standard_D3_v2 on Azure All existing FMCv for AWS instance types are now deprecated (c3.xlarge, c3.2xlarge, c4.xlarge, c4.2xlarge). You must resize before you upgrade. For more information, see FMCv Requires 28 GB RAM for Upgrade. Additionally, as of the Version 6.6 release, lower-memory instance types for cloud-based FMCv deployments are fully deprecated. You cannot create new FMCv instances using them, even for earlier Firepower versions. You can continue running existing instances.
Deprecated: e1000 Interfaces on FTDv for VMware.	**Prevents upgrade.** Version 6.6 ends support for e1000 interfaces on FTDv for VMware. You cannot upgrade until you switch to vmxnet3 or ixgbe interfaces. Or, you can deploy a new device. For more information, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.
Deprecated: Less secure Diffie-Hellman groups, and encryption and hash algorithms.	Version 6.6 deprecates the following FTD security features: • Diffie-Hellman groups: 2, 5, and 24. • Encryption algorithms for users who satisfy export controls for strong encryption: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continues to be supported (and is the only option) for users who do not satisfy export controls. • Hash algorithms: MD5. These features are removed in Version 6.7. Avoid configuring them in IKE proposals or IPSec policies for use in VPNs. Change to stronger options as soon as possible.
Deprecated: Custom tables for connection events.	Version 6.6 ends support for custom tables for connection and Security Intelligence events. After you upgrade, existing custom tables for those events are still 'available' but return no results. We recommend you delete them. There is no change to other types of custom tables. Deprecated options: • **Analysis** > **Advanced** > **Custom Tables** > click **Create Custom Table** > **Tables** drop-down list > **Connection Events** and **Security Intelligence Events**

Feature	Description
Deprecated: Ability to delete connection events from the event viewer.	Version 6.6 ends support for deleting connection and Security Intelligence events from the event viewer. To purge the database, select **System** > **Tools** > **Data Purge**. Deprecated options: • **Analysis** > **Connections** > **Events** > **Delete** and **Delete All** • **Analysis** > **Connections** > **Security Intelligence Events** > **Delete** and **Delete All**
Deprecated: Geolocation details.	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 6.6.x

Table 4: FDM Features in Version 6.6.x

Feature	Description
Platform Features	
FDM support for FTDv for the Amazon Web Services (AWS) Cloud.	You can configure Firepower Threat Defense on FTDv for the AWS Cloud using FDM.
FDM for the Firepower 4112.	We introduced Firepower Threat Defense for the Firepower 4112. **Note** Requires FXOS 2.8.1.
e1000 Interfaces on FTDv for VMware.	**Prevents upgrade.** Version 6.6 ends support for e1000 interfaces on FTDv for VMware. You cannot upgrade until you switch to vmxnet3 or ixgbe interfaces. Or, you can deploy a new device. For more information, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.
Firewall and IPS Features	

Feature	Description
Ability to enable intrusion rules that are disabled by default.	Each system-defined intrusion policy has a number of rules that are disabled by default. Previously, you could not change the action for these rules to alert or drop. You can now change the action for rules that are disabled by default. We changed the Intrusion Policy page to display all rules, even those that are disabled by default, and allow you to edit the action for these rules.
Intrusion Detection System (IDS) mode for the intrusion policy.	You can now configure the intrusion policy to operate in Intrusion Detection System (IDS) mode. In IDS mode, active intrusion rules issue alerts only, even if the rule action is Drop. Thus, you can monitor or test how an intrusion policy works before you make it an active prevention policy in the network. In FDM, we added an indication of the inspection mode to each intrusion policy on the **Policies** > **Intrusion** page, and an **Edit** link so that you can change the mode. In the Firepower Threat Defense API, we added the inspectionMode attribute to the IntrusionPolicy resource.
Support for manually uploading Vulnerability Database (VDB), Geolocation Database, and Intrusion Rule update packages.	You can now manually retrieve update packages for VDB, Geolocation Database, and Intrusion Rules, and then upload them from your workstation to the Firepower Threat Defense 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.
Firepower Threat Defense API support for access control rules that are limited based on time.	Using the Firepower Threat Defense API, you can create time range objects, which specify one-time or recurring time ranges, and apply these objects to access control rules. Using time ranges, you can apply an access control rule to traffic during certain times of day, or for certain periods of time, to provide flexibility to network usage. You cannot use FDM to create or apply time ranges, nor does FDM show you if an access control rule has a time range applied to it. The TimeRangeObject, Recurrence, TimeZoneObject, DayLightSavingDateRange, and DayLightSavingDayRecurrence resources were added to the Firepower Threat Defense API. The timeRangeObjects attribute was added to the accessrules resource to apply a time range to the access control rule. In addition, there were changes to the GlobalTimeZone and TimeZone resources.
Object group search for access control policies.	While operating, the Firepower Threat Defense device expands access control rules into multiple access control list entries based on the contents of any network objects used in the access rule. You can reduce the memory required to search access control rules by enabling object group search. With object group search enabled, the system does not expand network objects, but instead searches access rules for matches based on those group definitions. Object group search does not impact how your access rules are defined or how they appear in FDM. It impacts only how the device interprets and processes them while matching connections to access control rules. Object group search is disabled by default. In FDM, you must use FlexConfig to enable the **object-group-search access-control** command.

Feature	Description
VPN Features	
Backup peer for site-to-site VPN. (Firepower Threat Defense API only.)	You can use the Firepower Threat Defense API to add a backup peer to a site-to-site VPN connection. For example, if you have two ISPs, you can configure the VPN connection to fail over to the backup ISP if the connection to the first ISP becomes unavailable. Another main use of a backup peer is when you have two different devices on the other end of the tunnel, such as a primary-hub and a backup-hub. The system would normally establish the tunnel to the primary hub. If the VPN connection fails, the system automatically can re-establish the connection with the backup hub. We updated the Firepower Threat Defense API so that you can specify more than one interface for outsideInterface in the SToSConnectionProfile resource. We also added the BackupPeer resource, and the remoteBackupPeers attribute to the SToSConnectionProfile resource. You cannot configure a backup peer using FDM, nor will the existence of a backup peer be visible in FDM.
Support for Datagram Transport Layer Security (DTLS) 1.2 in remote access VPN.	You can now use DTLS 1.2 in remote access VPN. This can be configured using the Firepower Threat Defense API only, you cannot configure it using FDM. However, DTLS 1.2 is now part of the default SSL cipher group, and you can enable the general use of DTLS using FDM in the AnyConnect attributes of the group policy. Note that DTLS 1.2 is not supported on the ASA 5508-X or 5516-X models. We updated the protocolVersion attribute of the sslcipher resource to accept DTLSV1_2 as an enum value.
Deprecated support for less secure Diffie-Hellman groups, and encryption and hash algorithms.	The following features are deprecated and will be removed in a future release. You should avoid configuring these features in IKE proposals or IPSec policies for use in VPNs. Please transition away from these features and use stronger options as soon as is practical. • Diffie-Hellman groups: 2, 5, and 24. • Encryption algorithms for users who satisfy export controls for strong encryption: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continues to be supported (and is the only option) for users who do not satisfy export controls. • Hash algorithms: MD5.
Routing Features	

Feature	Description
Virtual routers and Virtual Routing and Forwarding (VRF)-Lite.	You can create multiple virtual routers to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device. Virtual routers implement the "light" version of Virtual Routing and Forwarding, or VRF-Lite, which does not support Multiprotocol Extensions for BGP (MBGP). We changed the **Routing** page so you can enable virtual routers. When enabled, the **Routing** page shows a list of virtual routers. You can configure separate static routes and routing processes for each virtual router. We also added the [**vrf** *name* | **all**] keyword set to the following CLI commands, and changed the output to indicate virtual router information where applicable: **clear ospf**, **clear route**, **ping**, **show asp table routing**, **show bgp**, **show ipv6 route**, **show ospf**, **show route**, **show snort counters**. We added the following command: **show vrf**.
OSPF and BGP configuration moved to the Routing pages.	In previous releases, you configured OSPF and BGP in the Advanced Configuration pages using Smart CLI. Although you still configure these routing processes using Smart CLI, the objects are now available directly on the Routing pages. This makes it easier for you to configure processes per virtual router. The OSPF and BGP Smart CLI objects are no longer available on the Advanced Configuration page. If you configured these objects before upgrading to 6.6, you can find them on the Routing page after upgrade.
High Availability Features	
The restriction for externally authenticated users logging into the standby unit of a high availability (HA) pair has been removed.	Previously, an externally-authenticated user could not directly log into the standby unit of an HA pair. The user first needed to log into the active unit, then deploy the configuration, before login to the standby unit was possible. This restriction has been removed. Externally-authenticated users can log into the standby unit even if they never logged into the active unit, so long as they provide a valid username/password.

Feature	Description
Change to how interfaces are handled by the BreakHAStatus resource in the Firepower Threat Defense API.	Previously, you could include the **clearIntfs** query parameter to control the operational status of the interfaces on the device where you break the high availability (HA) configuration. Starting with version 6.6, there is a new attribute, **interfaceOption**, which you should use instead of the clearIntfs query parameter. This attribute is optional when used on the active node, but required when used on a non-active node. You can choose from one of two options: • DISABLE_INTERFACES (the default)—All data interfaces on the standby device (or this device) are disabled. • ENABLE_WITH_STANDBY_IP—If you configured a standby IP address for an interface, the interface on the standby device (or this device) is reconfigured to use the standby address. Any interface that lacks a standby address is disabled. If you use break HA on the active node when the devices are in a healthy active/standby state, this attribute applies to the interfaces on the standby node. In any other state, such as active/active or suspended, the attribute applies to the node on which you initiate the break. If you do use the clearIntfs query parameter, clearIntfs=true will act like interfaceOption = DISABLE_INTERFACES. This means that breaking an active/standby pair with clearIntfs=true will no longer disable both devices; only the standby device will be disabled. When you break HA using FDM, the interface option is always set to DISABLE_INTERFACES. You cannot enable the interfaces with the standby IP address. Use the API call from the API Explorer if you want a different result.
The last failure reason for High Availability problems is now displayed on the High Availability page.	If High Availability (HA) fails for some reason, such as the active device becoming unavailable and failing over to the standby device, the last reason for failure is now shown below the status information for the primary and secondary device. The information includes the UTC time of the event.
Interface Features	
PPPoE support.	You can now configure PPPoE for routed interfaces. PPPoE is not supported on High Availability units. New/Modified screens: **Device** > **Interfaces** > **Edit** > **IPv4 Address** > **Type** > **PPPoE** New/Modified commands: **show vpdn group, show vpdn username, show vpdn session pppoe state**
Management interface acts as a DHCP client by default.	The Management interface now defaults to obtaining an IP address from DHCP instead of using the 192.168.45.45 IP address. This change makes it easier for you to deploy an Firepower Threat Defense in your existing network. This feature applies to all platforms except for the Firepower 4100/9300 (where you set the IP address when you deploy the logical device), and the FTDv and ISA 3000 (which still use the 192.168.45.45 IP address). The DHCP server on the Management interface is also no longer enabled. You can still connect to the default inside IP address by default (192.168.1.1).

Feature	Description
HTTP proxy support for FDM management connections.	You can now configure an HTTP proxy for the management interface for use with FDM connections. All management connections, including manual and scheduled database updates, go through the proxy. We added the **System Settings** > **HTTP Proxy** page to configure the setting. In addition, we added the HTTPProxy resource to the Firepower Threat Defense API.
Set the MTU for the Management interface.	You can now set the MTU for the Management interface up to 1500 bytes. The default is 1500 bytes. New/Modified commands: **configure network mtu, configure network management-interface mtu-management-channel** No modified screens.
Licensing Features	
Smart Licensing and Cloud Services enrollment are now separate, and you can manage your enrollments separately.	You can now enroll for cloud services using your security account rather than your Smart Licensing account. Enrolling using the security account is the recommended approach if you intend to manage the device using Cisco Defense Orchestrator. You can also unregister from cloud services without unregistering from Smart Licensing. We changed how the **System Settings** > **Cloud Services** page behaves, and added the ability to unregister from cloud services. In addition, the Web Analytics feature was removed from the page and you can now find it at **System Settings** > **Web Analytics**. In the Firepower Threat Defense API, the CloudServices resources were modified to reflect the new behavior.
Support for Permanent License Reservation.	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. ISA 3000 does not support Universal PLR. 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 Firepower Threat Defense API, there are new resources for PLRAuthorizationCode, PLRCode, PLRReleaseCode, PLRRequestCode, and actions for PLRRequestCode, InstallPLRCode, and CancelReservation.
Administrative and Troubleshooting Features	

Feature	Description
FDM direct support for Precision Time Protocol (PTP) configuration for ISA 3000 devices.	You can use FDM to configure the Precision Time Protocol (PTP) on ISA 3000 devices. PTP is a time-synchronization protocol developed to synchronize the clocks of various devices in a packet-based network. The protocol is designed specifically for industrial, networked measurement and control systems. In previous releases, you had to use FlexConfig to configure PTP. We grouped PTP with NTP on the same System Settings page, and renamed the **System Settings** > **NTP** page to **Time Services**. We also added the PTP resource to the Firepower Threat Defense API.
Trust chain validation for the FDM management web server certificate.	When you configure a non-self-signed certificate for the FDM web server, you now need to include all intermediate certificates, and the root certificate, in the trust chain. The system validates the entire chain. We added the ability to select the certificates in the chain on the **Management Web Server** tab on the **Device** > **System Settings** > **Management Access** page.
Support for encrypting backup files.	You can now encrypt backup files using a password. To restore an encrypted backup, you must supply the correct password. We added the ability to choose whether to encrypt backup files for recurring, scheduled, and manual jobs, and to supply the password on restore, to the **Device** > **Backup and Restore** page. We also added the encryptArchive and encryptionKey attributes to the BackupImmediate and BackupSchedule resources, and encryptionKey to the RestoreImmediate resource in the Firepower Threat Defense API.
Support for selecting which events to send to the Cisco cloud for use by cloud services.	When you configure the device to send events to the Cisco cloud, you can now select which types of events to send: intrusion, file/malware, and connection. For connection events, you can send all events or just the high-priority events, which are those related to connections that trigger intrusion, file, or malware events, or that match Security Intelligence blocking policies. We changed how the Send Events to the Cisco Cloud Enable button works. The feature is on the **System Settings** > **Cloud Services** page.
Firepower Threat Defense REST API version 5 (v5).	The Firepower Threat Defense REST API for software version 6.6 has been incremented to version 5. You must replace v1/v2/v3/v4 in the API URLs with v5, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. The v5 API includes many new resources that cover all features added in software version 6.6. Please re-evaluate all existing calls, as changes might have been mode to the resource models you are using. To open the API Explorer, where you can view the resources, log into FDM, then click the more options button (⋮) and choose **API Explorer**.