What's New in Firepower Management Center version 6.6.0?

Feature	Description
Hardware and Virtual Hardware	
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. You *must* resize your existing FMCv instances before you upgrade. For more information, see FMCv Requires 28 GB RAM for Upgrade. Supported platforms: FMCv for AWS, FTDv for AWS
Autoscale for cloud-based FTDv deployments	Version 6.6.0 introduces 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	
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

Feature	Description
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 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 screens: 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	
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

Feature	Description
	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 Firepower Chassis Manager screens: • 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 screens: Devices > Device Management > edit device > Routing tab

Feature	Description
	New FTD CLI commands: show vrf . Modified FTD CLI commands: Added the [vrf *name* | all] keyword set to the following CLI commands, and changed the output to indicate virtual router information where applicable: clear ospf , clear route , ping , show asp table routing , show bgp , show ipv6 route , show ospf , show route , show snort counters . Supported platforms: FTD, except Firepower 1010 and ISA 3000
Firepower Threat Defense: VPN	
DTLS 1.2 in remote access VPN	You can now use Datagram Transport Layer Security (DTLS) 1.2 to encrypt RA VPN connections. Use FTD platform settings to specify the minimum TLS protocol version that the FTD device uses when acting as a, RA VPN server. If you want to specify DTLS 1.2, you must also choose TLS 1.2 as the minimum TLS version. Requires Cisco AnyConnect Secure Mobility Client, Version 4.7+. New/modified screens: 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 screens: 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.

Feature	Description
	• 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 screens: Devices > Device Management > edit device > Device tab > Advanced Settings > Object Group Search option Supported platforms: FTD
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 screens: • 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.**

Feature	Description
	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. For more information, see Events Temporarily Unavailable After FMC Upgrade. 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
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 screens:

Feature	Description
	• **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	
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 screens: • 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.

Feature	Description
	• 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 screens: • 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 screens: System > Configuration > HTTPS Certificate > Generate New CSR > Subject Alternative Name fields Supported platforms: FMC
Real names associated with FMC user accounts	You can now specify a real name when you create or modify an FMC user account. This can be a person's name, department, or other identifying attribute. New/modified screens: System > Users > Users > Real Name field. Supported platforms: FMC
Usability	
FMC web interface Light theme	The FMC now defaults to the Light theme, which was introduced as an experimental 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

Feature	Description
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 screens: 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	
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

Feature	Description
	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