



Cisco Firepower Management Center New Features by Release

First Published: 2021-03-26

Last Modified: 2021-12-15

New Features by Release

This document lists new and deprecated features for each release.

Suggested Release

Suggested Release: Version 6.6.5.1

To take advantage of new features and resolved issues, we recommend you upgrade all eligible appliances to at least the suggested release. On the Cisco Support & Download site, the suggested release is marked with a gold star.

Suggested Releases for Older Appliances

If an appliance is too old to run the suggested release and you do not plan to refresh the hardware right now, choose a major version then patch as far as possible. Some major versions are designated *long-term* or *extra long-term*, so consider one of those. For an explanation of these terms, see [Cisco NGFW Product Line Software Release and Sustaining Bulletin](#).

If you are interested in a hardware refresh, contact your Cisco representative or partner contact.

Version 7.1.0

New Features in FMC Version 7.1.0

Feature	Description
Hardware and Virtual Appliances	
FMCv300 for AWS FMCv300 for OCI	We introduced the FMCv300 for both AWS and OCI. The FMCv300 can manage up to 300 devices.

Feature	Description
FTDv for AWS instances.	<p>FTDv for AWS adds support for these instances:</p> <ul style="list-style-type: none"> • c5a.xlarge, c5a.2xlarge, c5a.4xlarge • c5ad.xlarge, c5ad.2xlarge, c5ad.4xlarge • c5d.xlarge, c5d.2xlarge, m c5d.4xlarge • i3en.xlarge, i3en.2xlarge, i3en.3xlarge • inf1.xlarge, inf1.2xlarge • m5.xlarge, m5.2xlarge, m5.4xlarge • m5a.xlarge, m5a.2xlarge, m5a.4xlarge • m5ad.xlarge, m5ad.2xlarge, m5ad.4xlarge • m5d.xlarge, m5d.2xlarge, m5d.4xlarge • m5dn.xlarge, m5dn.2xlarge, m5dn.4xlarge • m5n.xlarge, m5n.2xlarge, m5n.4xlarge • m5zn.xlarge, m5zn.2xlarge, m5zn.3xlarge • r5.xlarge, r5.2xlarge, r5.4xlarge • r5a.xlarge, r5a.2xlarge, r5a.4xlarge • r5ad.xlarge, r5ad.2xlarge, r5ad.4xlarge • r5b.xlarge, r5b.2xlarge, r5b.4xlarge • r5d.xlarge, r5d.2xlarge, r5d.4xlarge • r5dn.xlarge, r5dn.2xlarge, r5dn.4xlarge • r5n.xlarge, r5n.2xlarge, r5n.4xlarge • z1d.xlarge, z1d.2xlarge, z1d.3xlarge
FTDv for Azure instances.	<p>FTDv for Azure adds support for these instances:</p> <ul style="list-style-type: none"> • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2
Device Setup	

Feature	Description
Use FDM to configure the FTD for management by the FMC.	<p>When you perform initial setup using FDM, all interface configuration completed in FDM is retained when you switch to FMC for management, in addition to the Management and FMC access settings. Note that other default configuration settings, such as the access control policy or security zones, are not retained. When you use the FTD CLI, only the Management and FMC access settings are retained (for example, the default inside interface configuration is not retained).</p> <p>After you switch to FMC, you can no longer use FDM to manage the FTD.</p> <p>New/modified FDM screens: System Settings > Management Center</p>
Device Upgrade	
Revert a successful device upgrade.	<p>You can now revert major and maintenance upgrades to FTD. Reverting returns the software to its state just before the last upgrade, also called a <i>snapshot</i>. If you revert an upgrade after installing a patch, you revert the patch as well as the major and/or maintenance upgrade.</p> <p>Important If you think you might need to revert, you must use the System > Updates page to upgrade FTD. The System Updates page is the only place you can enable the Enable revert after successful upgrade option, which configures the system to save a revert snapshot when you initiate the upgrade. This is in contrast to our usual recommendation to use the wizard on the Devices > Device Upgrade page.</p> <p>This feature is not supported for container instances on the Firepower 4100/9300.</p>
Improvements to the upgrade workflow for clustered and high availability devices.	<p>We made the following improvements to the upgrade workflow for clustered and high availability devices:</p> <ul style="list-style-type: none"> • The upgrade wizard now correctly displays clustered and high availability units as groups, rather than as individual devices. The system can identify, report, and preemptively require fixes for group-related issues you might have. For example, you cannot upgrade a cluster on the Firepower 4100/9300 if you have made unsynced changes on Firepower Chassis Manager. • We improved the speed and efficiency of copying upgrade packages to clusters and high availability pairs. Previously, the FMC copied the package to each group member sequentially. Now, group members can get the package from each other as part of their normal sync process. • You can now specify the upgrade order of data units in a cluster. The control unit always upgrades last.

Feature	Description
Snort 3 backwards compatibility.	<p>For Snort 3, new features and resolved bugs require that you fully upgrade the FMC <i>and</i> its managed devices. Unlike Snort 2, you cannot update the inspection engine on an older device (for example, Version 7.0.0) by deploying from a newer FMC (for example, Version 7.1.0).</p> <p>When you deploy to an older device, the system lists any unsupported configurations and warns you that they will be skipped. We recommend you always update your entire deployment.</p>
Device Management	
Geneve interface support for an FTDv on AWS instances.	<p>Geneve encapsulation support was added to support single-arm proxy for the AWS Gateway Load Balancer (GWLB). The AWS GWLB combines a transparent network gateway (with a single entry and exit point for all traffic) and a load balancer that distributes traffic and scales FTDv to match the traffic demand.</p> <p>This support requires FMC with Snort 3 enabled and is available on the following performance tiers:</p> <ul style="list-style-type: none"> • FTDv20 • FTDv30 • FTDv50 • FTDv100
Single Root I/O Virtualization (SR-IOV) support for FTDv on OCI.	You can now implement Single Root Input/Output Virtualization (SR-IOV) for FTDv on OCI. SR-IOV can provide performance improvements for an FTDv. Mellanox 5 as vNICs are not supported in SR-IOV mode.
LLDP support for the Firepower 1100.	<p>You can now enable Link Layer Discovery Protocol (LLDP) for Firepower 1100 interfaces.</p> <p>New/modified screens: Devices > Device Management > Interfaces > Hardware Configuration > LLDP</p> <p>New/modified commands: show lldp status, show lldp neighbors, show lldp statistics</p> <p>Supported platforms: Firepower 1100 (1120, 1140, and 1150)</p>
Interface auto-negotiation is now set independently from speed and duplex, interface sync improved.	<p>Interface auto-negotiation is now set independently from speed and duplex. Also, when you sync the interfaces in FMC, hardware changes are detected more effectively.</p> <p>New/modified screens: Devices > Device Management > Interfaces > Hardware Configuration > Speed</p> <p>Supported platforms: Firepower 1000/2100</p>

Feature	Description
Support to specify trusted DNS servers.	You can use FTD platform settings to specify trusted DNS servers for DNS snooping. This helps detect applications on the first packet by mapping domains to IP addresses. By default, trusted DNS servers include those in DNS server objects, and those discovered by dhcp-pool, dhcp-relay, and dhcp-client.
Import and export device configurations.	<p>You can export the device-specific configuration, and you can then import the saved configuration for the same device in the following use cases:</p> <ul style="list-style-type: none"> • Moving the device to a different FMC. • Restore an old configuration. • Reregistering a device. <p>New/modified screens: Devices > Device Management > Device > General</p>
High Availability/Scalability	
High availability for: <ul style="list-style-type: none"> • FMCv for AWS • FMCv for OCI 	<p>We now support high availability on FMCv for AWS and FMCv for OCI.</p> <p>In an FTD deployment, you need two identically licensed FMCs, as well as one FTD entitlement for each managed device. For example, to manage 10 FTD devices with an FMCv10 high availability pair, you need two FMCv10 entitlements and 10 FTD entitlements. If you are managing Version 6.5.0–7.0.x Classic devices only (NGIPSv or ASA FirePOWER), you do not need FMCv entitlements.</p> <p>Supported platforms: FMCv10, FMCv25, FMCv300 (not supported for FMCv2)</p>
Autoscale on FTDv for OCI.	<p>We now support autoscaling on FTDv for OCI.</p> <p>The serverless infrastructure in cloud-based deployments allow you to automatically adjust the number of FTDv instances in an autoscale group based on capacity needs. This includes automatic registering/unregistering to and from the managing FMC.</p>
Cluster deployment for firewall changes completes faster.	<p>Cluster deployment for firewall changes now completes faster.</p> <p>Supported platforms: Firepower 4100/9300</p>
Clearing routes in a high availability group or cluster.	In previous releases, the clear route command cleared the routing table on the unit only. Now, when operating in a high availability group or cluster, the command is available on the active or control unit only, and clears the routing table on all units in the group or cluster.
NAT	
Manual NAT support for fully-qualified domain name (FQDN) objects as the translated destination.	You can use an FQDN network object, such as one specifying www.example.com, as the translated destination address in manual NAT rules. The system configures the rule based on the IP address returned from the DNS server.

Feature	Description
Routing	
BGP configuration to interconnect virtual routers.	<p>You can configure BGP settings to dynamically leak routes among user-defined virtual routers, and between global virtual router and user-defined virtual routers. The import and export routes feature was introduced to exchange routes among the virtual routers by tagging them with route targets and optionally, filtering the matched routes with route maps. This BGP feature is accessible only when you select a user-defined virtual router.</p> <p>New/modified screens: For a selected user-defined virtual router, Devices > Device Management > Routing > BGPv4/v6 > Route Import/Export</p>
BGPv6 support for user-defined virtual routers.	<p>FTD now supports configuring BGPv6 on user-defined virtual routers.</p> <p>New/modified screens: For a selected user-defined virtual router, Devices > Device Management > Routing > BGPv6</p>
Equal-Cost-Multi-Path (ECMP) zone support.	<p>You can now group interfaces in traffic zones and configure Equal-Cost-Multi-Path (ECMP) routing in FMC.</p> <p>ECMP routing was previously supported through FlexConfig policies.</p> <p>New/modified screens: Devices > Device Management > Routing > ECMP</p>
Direct Internet Access/Policy Based Routing	
Direct internet access with policy based routing.	<p>You can now configure policy based routing through the FMC to classify network traffic based on applications and to implement Direct Internet Access (DIA) to send traffic to the internet from a branch deployment. You can define a PBR policy and configure it on ingress interfaces, specifying match criteria and egress interfaces. Network traffic that matches the access control policy is forwarded through the egress interface based on priority or the order as configured in the policy.</p> <p>New/modified screens: New policy page for configuring the policy based routing policy: Devices > Device Management > Routing > Policy Based Routing</p> <p>Supported platforms: FTD</p>
FMC REST API enhancements for direct internet access and policy based routing.	<p>You can use the FMC REST API to configure Direct Internet Access through Policy Based Routing. The following enhancements have been made to the FMC REST API to support this:</p> <ul style="list-style-type: none"> • New APIs were added to enable you to create, view, edit, and delete your Policy Based Routing configuration • New parameters added to existing APIs for Extended Access Control Lists to define applications • New parameters added to existing APIs for device interfaces to define interface priority
Remote Access VPN	

Feature	Description
Copy RA VPN policies.	You can now create a new RA VPN policy by copying an existing policy. We added a copy button next to each policy on Devices > VPN > Remote Access .
AnyConnect VPN SAML external browser.	<p>You can now configure AnyConnect VPN SAML External Browser to enable additional authentication choices, such as passwordless authentication, WebAuthN, FIDO, SSO, U2F, and an improved SAML experience due to the persistence of cookies. When you use SAML as the primary authentication method for a remote access VPN connection profile, you can elect to have the AnyConnect client use the client's local browser instead of the AnyConnect embedded browser to perform the web authentication. This option enables single sign-on (SSO) between your VPN authentication and other corporate logins. Also choose this option if you want to support web authentication methods, such as biometric authentication and Yubikeys, that cannot be performed in the embedded browser.</p> <p>We updated the remote access VPN connection profile wizard to allow you to configure the SAML Login Experience.</p>
Multiple trustpoints for SAML identity providers on Microsoft Azure.	<p>You can now add multiple RA VPN trustpoints for SAML identity providers, as required by Microsoft Azure.</p> <p>In a Microsoft Azure network, Azure can support multiple applications for the same Entity ID. Each application (typically mapped to a different tunnel group) requires a unique certificate. This feature enables you to add multiple trustpoints for RA VPN in FTDv for Microsoft Azure.</p>
Site to Site VPN	
VPN filters.	<p>You can now configure site to site VPN filters with rules that determine whether to allow or reject tunneled data packets based on criteria such as source address, destination address, and protocol.</p> <p>The VPN filter is applied to post-decrypted traffic after it exits a tunnel and to pre-encrypted traffic before it enters a tunnel.</p>
Unique local tunnel ID for IKEv2.	<p>You can now configure a Local Tunnel ID per IKEv2 tunnel for both policy-based and route-based Site to Site VPNs. You can configure the local tunnel ID with the FMC web interface or from the REST API.</p> <p>This local tunnel ID configuration enables Umbrella SIG integration with FTD.</p>
Multiple IKE policies.	<p>You can now configure multiple IKE policies for both policy-based and route-based Site to Site VPNs.</p> <p>Multiple IKE policies can be configured through the FMC GUI and the REST API.</p>

Feature	Description
VPN monitoring dashboard.	<p>Beta.</p> <p>The Site to Site VPN Monitoring Dashboard provides:</p> <ul style="list-style-type: none"> • Visualization of tunnel status distribution across all devices • Visualization of network topology consisting of VPN tunnels • Ability to visually isolate and examine tunnels based on criteria like Topology, Device and Status <p>Note The Site to Site Monitoring Dashboard is a Beta feature and may not work as expected. Do not use it in production environments.</p>
Security Intelligence	
Snort 3 support for Security Intelligence on proxied traffic.	With Snort 3, you can now apply Security Intelligence to HTTP proxy traffic where the IP address is embedded into the HTTP request. For example, when a user uploads a Block list or an Allow list containing IP addresses or networks, the system matches on the destination server IP instead of proxy IP. As a result, traffic to the destination server can be blocked, monitored, or allowed (according to your Security Intelligence configuration).
Intrusion Detection and Prevention	
Snort 3 support for drop, reject, rewrite, and pass rule actions.	<p>Version 7.1.0 FMCs now support the following intrusion rule actions for FTD devices with Snort 3, including Version 7.0.0/7.0.x devices:</p> <ul style="list-style-type: none"> • Drop: Drops the matching packet, but does not block further traffic in this connection. Generates an intrusion event. • Reject: Drops the matching packet and blocks further traffic in this connection. For TCP traffic, sends a TCP reset. For UDP traffic, sends ICMP port unreachable to the source and destination hosts. Generates an intrusion event. • Rewrite: Overwrites the matching packet based on the replace option in the rule. Generates an intrusion event. • Pass: Allows matching packet to pass without further evaluation by any other intrusion rules. Does not generate an intrusion event. <p>To configure these new rule actions, edit the Snort 3 version of an intrusion policy and use the Rule Action drop-down for each rule.</p>
Snort 3 support for TLS-based intrusion rules.	You can now create TLS-based intrusion rules to inspect decrypted TLS traffic with Snort 3. This feature allows Snort 3 intrusion rules to use TLS information.

Feature	Description
Snort 3 support for inspection of DCE/RPC over SMB2.	<p>Upgrade impact.</p> <p>Version 7.1.0 with Snort 3 supports DCE/RPC inspection over SMB2.</p> <p>After the first post-upgrade deploy to Snort 3 devices, existing DCE/RPC rules begin inspecting DCE/RPC over SMB2; previously these rules only inspected DCE/RPC over SMB1.</p>
Snort 3 support for intrusion rule recommendations.	<p>Version 7.1.0 FMCs now support intrusion rule recommendations for FTD devices with Snort 3, including Version 7.0.0/7.0.x devices.</p> <p>To configure this feature, edit the Snort 3 version of an intrusion policy and click the Recommendations button (in the left pane, next to All Rules).</p>
Snort 3 support for ssl_version and ssl_state keywords.	<p>Upgrade impact.</p> <p>Version 7.1.0 with Snort 3 supports the ssl_version and ssl_state intrusion rule keywords.</p> <p>Cisco-provided intrusion policies include active rules using those keywords. You can also create, upload, and deploy custom/third party rules using them. In Version 7.0.x, we supported those keywords with Snort 2 only. With Snort 3, rules with those keywords did not match traffic, and thus could not generate alerts or affect traffic. There was no indication that the rules were not working as expected. After the first post-upgrade deploy to Version 7.1.0+ Snort 3 devices, existing rules with those keywords can match traffic.</p>

Identity Services and User Control

Snort 3 captive portal support for interception of HTTP/2 traffic.	<p>You can now intercept and redirect HTTP/2 traffic for user authentication with captive portal.</p> <p>When a redirect is received by the browser, the browser follows the redirect and authenticates with idhttpsd (Apache web server) using the same process as the HTTP/1 captive portal. After authentication, idhttpsd redirects the user back to the original URL.</p>
Snort 3 captive portal support for hostname-based redirect.	<p>You can configure active authentication for identity policy rules to redirect the user's authentication to a fully-qualified domain name (FQDN) rather than the IP address of the interface through which the user's connection enters the device.</p> <p>The FQDN must resolve to the IP address of one of the interfaces on the device. By using an FQDN, you can assign a certificate for active authentication that the client will recognize, thus avoiding the untrusted certificate warning users get when being redirected to an IP address. The certificate can specify the FQDN, a wildcard FQDN, or multiple FQDNs in the Subject Alternate Names (SAN) in the certificate.</p> <p>New/modified screens: We added the Redirect to Host Name option in the identity policy settings.</p>

Encrypted Traffic Handling (TLS/SSL)

Feature	Description
TLS certificate feeds.	You can now create TLS/SSL rules based on live TLS certificate feeds. Using live TLS certificate feeds, reduces the management overhead for TLS certificate fingerprints and allows rules to be based on more up-to-date information.
Advanced TLS/SSL policy options.	<p>You can now configure the following advanced TLS/SSL policy options in the Advanced Settings tab on the SSL Policy page:</p> <ul style="list-style-type: none"> • Block flows requesting ESNI (Encrypted Server Name Identification) • Disable HTTP/3 advertisement • Propagate untrusted server certificates to clients
Encrypted Visibility Engine for visibility into encrypted sessions.	<p>Beta.</p> <p>You can enable the Encrypted Visibility Engine to gain visibility into an encrypted session without needing to decrypt it. The engine fingerprints and analyzes encrypted traffic. In FMC 7.1, the Encrypted Visibility Engine provides more visibility into encrypted traffic, including protocols such as TLS and QUIC. It does not enforce any actions on that traffic.</p> <p>The Encrypted Visibility Engine is disabled by default. You can enable it on the Advanced tab of an access control policy in the Experimental Features section.</p> <p>New/modified screens: Policies > Access Control > Access Control Policy name > Advanced</p> <p>Note The Encrypted Visibility Engine is an experimental Beta feature provided for visibility. It may cause false positives.</p>
Service Policy	
Configure the maximum segment size (MSS) for embryonic connections.	<p>You can configure a service policy to set the server maximum segment size (MSS) for SYN-cookie generation for embryonic connections upon reaching the embryonic connections limit. This is meaningful for service policies where you are also setting embryonic connection maximums.</p> <p>New/modified screens: Connection Settings in the Add/Edit Service Policy wizard.</p>
Network Discovery	

Feature	Description
Improved Snort 3 support for network discovery (remote network access support).	<p>With improvements to network discovery and remote network access support, Snort 3 is now at parity with Snort 2 for those features. The improvements include:</p> <ul style="list-style-type: none"> • Discovery of hosts and applications for SMB traffic: For SMB traffic on your network, the host is discovered in the network map, and the SMB application protocol and associated operating system information are discovered. • Discovery of NetBIOS traffic: For NetBIOS traffic, the NetBIOS name is discovered as well as associated information related to applications, such as the client application and operating system. • Discovery of applications only for hosts/networks monitored by the network discovery policy: This enhancement to the filtering logic enables you to discover applications for networks that are being monitored based on a network discovery rule. <p>In Snort 3, application detection is always enabled for all networks by default.</p>
Event Logging and Analysis	
Snort 3 support for elephant flow identification and monitoring.	<p>With FTD running Snort 3, you can now identify <i>elephant flows</i>—single-session network connections that are large enough to affect overall system performance. By default, elephant flow detection is automatically enabled, and tracks and logs connections larger than 1GB/10 seconds.</p> <p>A new predefined search for connection events (Reason = Elephant Flow) allows you to quickly identify elephant flows. You can also use the health monitor to view active elephant flows on your devices, and to create a custom health dashboard to correlate elephant flow incidence with other device metrics such as CPU usage.</p> <p>To disable this feature or to configure the size and time thresholds, use the FTD CLI.</p> <p>New/modified FTD CLI commands:</p> <ul style="list-style-type: none"> • show elephant-flow status • show elephant-flow detection-config • system support elephant-flow-detection enable • system support elephant-flow-detection disable • system support elephant-flow-detection bytes-threshold <i>bytes-in-MB</i> • system support elephant-flow-detection time-threshold <i>time-in-seconds</i>

Feature	Description
Send intrusion events and retrospective malware events to the Secure Network Analytics cloud from the FMC.	<p>Upgrade impact.</p> <p>When you configure the system to send security events to the Stealthwatch cloud using Cisco Security Analytics and Logging (SaaS), the FMC now sends:</p> <ul style="list-style-type: none"> • Intrusion events. This allows remotely stored intrusion events to include impact flag data. Previously, these events were sent to the cloud by FTD and did not include the impact flag. • Retrospective malware events. These supplement the "original disposition" file and malware events that are still sent to the cloud by devices. <p>If you already enabled this feature, the FMC starts sending this information after a successful upgrade.</p>
New datastore for intrusion events improves performance.	<p>To improve performance, Version 7.1.0 uses a new datastore for intrusion events. After the upgrade finishes and the FMC reboots, historical events are migrated in the background, newest events first.</p> <p>As part of this migration, we deprecated intrusion incidents, the intrusion event clipboard, and custom tables for intrusion events. For more information, see Deprecated Features in FMC Version 7.1.0, on page 17.</p> <p>We also introduced two new fields in the intrusion event table: Source Host Criticality and Destination Host Criticality.</p>
NAT IP address and port information in connection and Security Intelligence events.	<p>For additional visibility into NAT translations, we added the following fields to connection and Security Intelligence events:</p> <ul style="list-style-type: none"> • NAT Source IP • NAT Destination IP • NAT Source Port • NAT Destination Port <p>In the table view of events, these fields are hidden by default. To change the fields that appear, click the x in any column name to display a field chooser.</p>

Feature	Description
Packet tracer enhancements.	<p>Version 7.1.0 updates the packet tracer interface for better usability. In addition, you can now:</p> <ul style="list-style-type: none"> • Access the packet tracer directly from the main menu: Devices > Troubleshoot > Packet Tracer. • Save packet traces. • Run parallel packet traces across multiple devices. • Replay PCAPs through a device. • For Snort 3 devices, view enhanced output that provides new details on the phases of traffic evaluation from L2 to L7 (application identification, file/malware detection, intrusion detection, Security Intelligence, and so on), as well as how long each phase takes. <p>New/modified FTD CLI commands:</p> <ul style="list-style-type: none"> • packet-tracer input<i>source_interface</i>pcapp<i>cap_filename</i>
Object Management	
Network object support for HTTP, ICMP, and SSH platform settings.	You can now use network object groups that contain network objects for hosts or networks when configuring the IP addresses in the Threat Defense Platform Settings policy.
Snort 3 support for network wildcard mask objects.	You can now create and manage network wildcard mask objects on the Object Management page. You can use network wildcard mask objects in access control, prefilter, and NAT policies.
Deployment preview enhancements for objects.	<p>You can now preview deployment changes to Geolocation, File List, and Security Intelligence objects.</p> <p>Updated screen: Deploy > Deployment. In the Preview column, click the Preview icon for a device to see the changes to the file list objects.</p>
Integrations	
Support for Cisco ACI Endpoint Update App, Version 2.0 and remediation module.	<p>Version 2.0 of the Cisco ACI Endpoint Update App has the following improvements over previous versions:</p> <ul style="list-style-type: none"> • The minimum update interval (how often the app updates the FMC) is now 10 seconds. Previously, it was 30 seconds. • The site prefix (a string that creates a network group object on the FMC associated with each APIC tenant) is now limited to 10 characters. Previously, it was 5 characters. <p>A new Cisco ACI Endpoint remediation module is also available with this update.</p>
Usability, Performance, and Troubleshooting	

Feature	Description
Health monitoring enhancements.	<p>We updated the health monitor as follows:</p> <ul style="list-style-type: none"> • The health policy editor now groups similar health modules. You can enable and disable entire module groups. • The health policy exclusion editor is updated for better usability. Also, when you exclude a device or health module from alerting, you can now specify a time period for the exclusion, from 15 minutes to permanently. • The health monitor alert editor is updated for better usability. • The health policy deployment interface is updated for better usability. <p>Note To use the updated health monitor, you must enable REST API access on System > Configuration > REST API Preferences.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • System > Health > Policy > Edit Policy • System > Health > Exclude • System > Health > Monitor Alerts • System > Health > Policy > Deploy Policy
Deployment history enhancements.	You can now bookmark a deployment job, edit the deployment notes for a job, and generate a report.
Global search enhancements.	<p>Global search now has the following capabilities:</p> <ul style="list-style-type: none"> • You can search the full text of FMC walkthroughs (<i>how-tos</i>). • You can search extended community list names or configured values. • You can restrict searches by domain.
New walkthroughs.	<p>We added the following walkthroughs:</p> <ul style="list-style-type: none"> • Create a Snort 3 intrusion policy. • Enable or disable Snort 3 on an individual device. • Create a Snort 3 network analysis policy. • View the network analysis policy mapping. • Upgrade FTD. • Create and manage a cluster. • Change the FMC access interface from Management to Data. • Change the FMC access interface from Data to Management.

Feature	Description
Snort memory usage telemetry sent to Cisco Success Network.	For improved serviceability, we now send telemetry on Snort memory and swap usage, including out-of-memory events, to Cisco Success Network. We send this information for both Snort 2 and Snort 3. You can change your Cisco Success Network enrollment at any time.
Snort 3 support for statistics on start-of-flow and end-of-flow events.	For FTD with Snort 3, the output of the show snort statistics command now reports statistics on start-of-flow and end-of-flow events.
FMC REST API	

Feature	Description
FMC REST API services/operations.	<p>We added multiple FMC REST API services/operations to support new and existing features. For more information, see the <i>Firepower Management Center REST API Quick Start Guide, Version 7.1</i>.</p> <p>The new FMC REST APIs include:</p> <ul style="list-style-type: none"> • Chassis Management: added Chassis Management APIs for managed chassis, chassis interfaces, network modules, and breakout interfaces • Deployment: added APIs for job histories • Device Clusters: added APIs to perform readiness checks and modify clustering • Devices: added APIs for the following: <ul style="list-style-type: none"> • Get FTD interface • Packet Tracer • Routing • Virtual LAN • Health: Added tunnel APIs • Object: Added APIs for the following: <ul style="list-style-type: none"> • Autonomous Service Paths • Expanded Community Lists • Extended Community Lists • Extended Access Lists • IPv4 Prefix Lists • IPv6 Prefix Lists • Policy Lists • Route Maps • Standard Access Lists • Standard Community Lists • Policy: Added APIs to modify automatic and manual NAT rules • Users: Added APIs to retrieve and modify Duo configurations • Troubleshoot: Added Packet Tracer PCAP functionality • Updates: Added API to revert upgrades • Network Map: Added APIs for hosts and vulnerabilities

Deprecated Features in FMC Version 7.1.0

Table 1: Deprecated Features in FMC Version 7.1.0

Feature	Upgrade Impact	Description
Intrusion incidents and the intrusion event clipboard.	<p>All data related to incidents is removed.</p> <p>Report templates sections that use the clipboard as a data source are deleted.</p>	<p>Version 7.1.0 removes the intrusion incidents feature and the related intrusion event clipboard.</p> <p>Deprecated screens/options:</p> <ul style="list-style-type: none"> • Analysis > Intrusions > Incidents • Analysis > Intrusions > Clipboard • Copy and Copy All on intrusion event workflow pages and packet views • When adding sections to a report template (Overview > Reporting > Report Templates), you can no longer choose the Clipboard table as a data source.
Custom tables for intrusion events	Custom tables that contain fields from the intrusion event table are deleted.	<p>Version 7.1.0 ends support for custom tables for intrusion events.</p> <p>When adding fields to a custom table (Analysis > Advanced > Custom Tables), you can no longer choose the Intrusion Events table as a data source.</p>
NGIPS software (ASA FirePOWER/NGIPSv)	Upgrade prohibited.	<p>Version 7.1.0 is supported on the FMC and on FTD devices only. It is not supported on ASA FirePOWER or NGIPSv devices.</p> <p>You can still use a Version 7.1.0 FMC to manage older devices — FTD as well as ASA FirePOWER and NGIPSv — that are running Version 6.5.0 through 7.0.x.</p>
ASA 5508-X and 5516-X	Upgrade prohibited.	You cannot run Version 7.1.0+ on the ASA 5508-X or 5516-X.
FMC 1000, 2500, 4500	Upgrade prohibited.	You cannot run Version 7.1.0+ on the FMC models FMC 1000, 2500, and 4500. You cannot manage Version 7.1.0+ devices with these FMCs.

Version 7.0.1

New Features in FMC Version 7.0.1

Table 2: New Features in FMC Version 7.0.1

Feature	Description
Snort 3 rate_filter inspector	<p>Version 7.0.1 introduces the Snort 3 rate_filter inspector.</p> <p>This allows you to change the action of an intrusion rule in response to excessive matches on that rule. You can block rate-based attacks for a specific length of time, then return to allowing matching traffic while still generating events. For more information, see the Snort 3 Inspector Reference.</p> <p>Note This feature requires Version 7.0.1+ on both the FMC and the device. Additionally, you must be running lsp-rel-20210816-1910 or later. You can check and update the LSP on System > Updates > Rule Updates.</p> <p>New/modified pages: Configure the inspector by editing the Snort 3 version of a custom network analysis policy.</p> <p>Supported platforms: FTD</p>
New default password for ISA 3000 with ASA FirePOWER Services	<p>For new devices, the default password for the admin account is now Adm!n123. Previously, the default admin password was Admin123.</p> <p>Upgrading or reimaging to Version 7.0.1+ does not change the password. However, we do recommend that all user accounts—especially those with Admin access—have strong passwords.</p> <p>Supported platforms: ISA 3000 with ASA FirePOWER Services</p>

Version 7.0.0

New Features in FMC Version 7.0.0

Table 3: New Features in FMC Version 7.0.0

Feature	Description
Hardware and Virtual Appliances	
VMware vSphere/VMware ESXi 7.0 support	<p>You can now deploy FMCv, FTDv, and NGIPSv virtual appliances on VMware vSphere/VMware ESXi 7.0.</p> <p>Note that Version 7.0.0 also discontinues support for VMware 6.0. Upgrade the hosting environment before you upgrade the Firepower software.</p>

Feature	Description
New virtual environments	<p>We introduced FMCv and FTDv for:</p> <ul style="list-style-type: none"> • Cisco HyperFlex • Nutanix Enterprise Cloud • OpenStack
FTDv performance tiered Smart Licensing	<p>Upgrade impact.</p> <p>FTDv now supports performance-tiered Smart Software Licensing, based on throughput requirements and RA VPN session limits. Options run from FTDv5 (100 Mbps/50 sessions) to FTDv100 (16 Gbps/10,000 sessions).</p> <p>Before you add a new device, make sure your account contains the licenses you need. To purchase additional licenses, contact your Cisco representative or partner contact.</p> <p>Upgrading FTDv to Version 7.0.0 automatically assigns the device to the FTDv50 tier. To continue using your legacy (non-tiered) license, after upgrade, change the tier to Variable.</p> <p>For more information on supported instances, throughputs, and other hosting requirements, see the appropriate Getting Started Guide.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • You can now specify a performance tier when adding or editing an FTDv device on the Device > Device Management page. • You can bulk-edit performance tiers on System > Licenses > Smart Licenses page.
Device Management	
FTD CLI show cluster history improvements	<p>New keywords allow you to customize the output of the show cluster history command.</p> <p>New/modified commands: show cluster history [brief] [latest] [reverse] [time]</p> <p>Supported platforms: Firepower 4100/9300</p>
FTD CLI command to permanently leave a cluster	<p>You can now use the FTD CLI to permanently remove a unit from the cluster, converting its configuration to a standalone device.</p> <p>New/modified commands: cluster reset-interface-mode</p> <p>Supported platforms: Firepower 4100/9300</p>
NAT	

Feature	Description
Prioritized system-defined NAT rules	<p>We added a new Section 0 to the NAT rule table. This section is exclusively for the use of the system. Any NAT rules that the system needs for normal functioning are added to this section, and these rules take priority over any rules you create. Previously, system-defined rules were added to Section 1, and user-defined rules could interfere with proper system functioning.</p> <p>You cannot add, edit, or delete Section 0 rules, but you will see them in show nat detail command output.</p> <p>Supported platforms: FTD</p>
Virtual Routing	
Virtual router support for the ISA 3000	<p>You can now configure up to 10 virtual routers on an ISA 3000 device.</p> <p>Supported platforms: ISA 3000</p>
Site to Site VPN	
Backup virtual tunnel interfaces (VTI) for route-based site-to-site VPN.	<p>When you configure a site-to-site VPN that uses virtual tunnel interfaces, you can select a backup VTI for the tunnel.</p> <p>Specifying a backup VTI provides resiliency, so that if the primary connection goes down, the backup connection might still be functional. For example, you could point the primary VTI to the endpoint of one service provider, and the backup VTI to the endpoint of a different service provider.</p> <p>New/modified pages: We added the ability to add a backup VTI to the site-to-site VPN wizard when you select Route-Based as the VPN type for a point-to-point connection.</p> <p>Supported platforms: FTD</p>
Remote Access VPN	
Load balancing	<p>We now support RA VPN load balancing. The system distributes sessions among grouped devices by number of sessions; it does not consider traffic volume or other factors.</p> <p>New/modified screens: We added load balancing options to the Advanced settings in an RA VPN policy.</p> <p>Supported platforms: FTD</p>

Feature	Description
Local authentication	<p>We now support local authentication for RA VPN users. You can use this as the primary or secondary authentication method, or as a fallback in case the configured remote server cannot be reached.</p> <ol style="list-style-type: none"> 1. Create a local realm. Local usernames and passwords are stored in local realms. When you create a realm (System > Integration > Realms) and select the new LOCAL realm type, the system prompts you to add one or more local users. 2. Configure RA VPN to use local authentication. Create or edit an RA VPN policy (Devices > VPN > Remote Access), create a connection profile within that policy, then specify LOCAL as the primary, secondary, or fallback authentication server in that connection profile. 3. Associate the local realm you created with an RA VPN policy. In the RA VPN policy editor, use the new Local Realm setting. Every connection profile in the RA VPN policy that uses local authentication will use the local realm you specify here. <p>Supported platforms: FTD</p>
Dynamic access policies	<p>The new dynamic access policy allows you to configure remote access VPN authorization that automatically adapts to a changing environment:</p> <ol style="list-style-type: none"> 1. Configure HostScan by uploading the AnyConnect HostScan package as an AnyConnect file (Objects > Object Management > VPN > AnyConnect File). There is a new HostScan Package option in the File Type drop-down list. This module runs on endpoints and performs a posture assessment that the dynamic access policy will use. 2. Create a dynamic access policy (Devices > Dynamic Access Policy). Dynamic access policies specify session attributes (such as group membership and endpoint security) that you want to evaluate each time a user initiates a session. You can then deny or grant access based on that evaluation. 3. Associate the dynamic access policy you created with an RA VPN policy. In the remote access VPN policy editor, use the new Dynamic Access Policy setting. <p>Supported platforms: FTD</p>

Feature	Description
Multi-certificate authentication	<p>We now support multi-certificate authentication for remote access VPN users. You can validate the machine or device certificate, to ensure the device is a corporate-issued device, in addition to authenticating the user's identity certificate to allow VPN access using the AnyConnect client during SSL or IKEv2 EAP phase.</p> <p>Supported platforms: FTD</p>
AnyConnect custom attributes	<p>We now support AnyConnect custom attributes, and provide an infrastructure to configure AnyConnect client features without adding explicit support for these features in the system.</p> <p>Supported platforms: FTD</p>
Access Control	

Feature	Description
Snort 3 for FTD	<p>For new Version 7.0.0+ FTD deployments, Snort 3 is the default inspection engine. Upgraded deployments continue to use Snort 2, but you can switch at any time.</p> <p>Advantages to using Snort 3 include, but are not limited to:</p> <ul style="list-style-type: none"> • Improved performance. • Improved SMBv2 inspection. • New script detection capabilities. • HTTP/2 inspection. • Custom rule groups. • Syntax that makes custom intrusion rules easier to write. • Reasons for 'would have dropped' inline results in intrusion events. • No Snort restarts when deploying changes to the VDB, SSL policies, custom application detectors, captive portal identity sources, and TLS server identity discovery. • Improved serviceability, due to Snort 3-specific telemetry data sent to Cisco Success Network, and to better troubleshooting logs. <p>A Snort 3 intrusion rule update is called an <i>LSP</i> (Lightweight Security Package) rather than an SRU. The system still uses SRUs for Snort 2; downloads from Cisco contain both the latest LSP and SRU. The system automatically uses the appropriate rule set for your configurations.</p> <p>A Version 7.0.0+ FMC can manage a deployment with both Snort 2 and Snort 3 devices, and will apply the correct policies to each device. However, unlike Snort 2, you cannot update Snort 3 on a device by upgrading the FMC only and then deploying. With Snort 3, new features and resolved bugs require you upgrade the software on the FMC <i>and</i> its managed devices. For information on the Snort included with each software version, see the <i>Bundled Components</i> section of the Cisco Firepower Compatibility Guide.</p> <p>Important Before you switch to Snort 3, we <i>strongly</i> recommend you read and understand the Firepower Management Center Snort 3 Configuration Guide. Pay special attention to feature limitations and migration instructions. Although upgrading to Snort 3 is designed for minimal impact, features do not map exactly. Careful planning and preparation can help you make sure that traffic handled as expected.</p> <p>You can also visit the Snort 3 website: https://snort.org/snort3.</p> <p>Supported platforms: FTD</p>

Feature	Description
Dynamic objects	<p>You can now use <i>dynamic objects</i> in access control rules.</p> <p>A dynamic object is just a list of IP addresses/subnets (no ranges, no FQDN). But unlike a network object, changes to dynamic objects take effect immediately, without having to redeploy. This is useful in virtual and cloud environments, where IP addresses often dynamically map to workload resources.</p> <p>To create and manage dynamic objects, we recommend the Cisco Secure Dynamic Attributes Connector. The connector is a separate, lightweight application that quickly and seamlessly updates firewall policies based on workload changes. To do this, it gets workload attributes from tagged resources in your environment, and compiles an IP list based on criteria you specify (a “dynamic attributes filter”). It then creates a dynamic object on the FMC and populates it with the IP list. When your workload changes, the connector updates the dynamic object and the system immediately starts handling traffic based on the new mappings. For more information, see the Cisco Secure Dynamic Attributes Connector Configuration Guide.</p> <p>After you create a dynamic object, you can add it to access control rules on the new Dynamic Attributes tab in the access control rule editor. This tab replaces the narrower-focus SGT/ISE Attributes tab; continue to configure rules with SGT attributes here.</p> <p>Note You can also create a dynamic object on the FMC: Objects > Object Management > External Attributes > Dynamic Objects. However, this creates the container only; you must then populate and manage it using the REST API. See the Firepower Management Center REST API Quick Start Guide, Version 7.0.</p> <p>Supported platforms: FMC</p> <p>Supported virtual/cloud workloads for Cisco Secure Dynamic Attributes Connector integration: Microsoft Azure, AWS, VMware</p>
Cross-domain trust for Active Directory domains	<p>You can now configure user identity rules with users from Microsoft Active Directory forests (groupings of AD domains that trust each other).</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> You now configure a realm and directories at the same time. A new Sync Results page (System > Integration > Realms > Sync Results) displays any errors related to downloading users and groups in a cross-domain trust relationship. <p>Supported platforms: FMC</p>
DNS filtering	<p>DNS filtering, which was introduced as a Beta feature in Version 6.7.0, is now fully supported and is enabled by default in new access control policies.</p> <p>Supported platforms: Any</p>
Event Logging and Analysis	

Feature	Description
Improved process for storing events in a Secure Network Analytics on-prem deployment	<p>A new Cisco Security Analytics and Logging (On Premises) app and a new FMC wizard make it easier to configure remote data storage for on-prem Secure Network Analytics solutions:</p> <ol style="list-style-type: none"> 1. Deploy hardware or virtual Stealthwatch appliances. You can use a Stealthwatch Management Console alone, or you can configure Stealthwatch Management Console, flow collector, and data store. 2. Install the new Cisco Security Analytics and Logging (On Premises) app on your Stealthwatch Management Console to configure Stealthwatch as a remote data store. 3. On the FMC, use one of the new wizards on the System > Logging > Security Analytics & Logging page to connect to your Stealthwatch deployment. Note that the wizards replace the narrower-focus page where you used to configure Stealthwatch contextual cross-launch; that is now a step in the wizard. <p>For upgraded deployments where you were using syslog to send Firepower events to Stealthwatch, disable those configurations before you use the wizard. Otherwise, you will get double events. To remove the syslog connection to Stealthwatch use FTD platform settings (Devices > Platform Settings); to disable sending events to syslog, edit your access control rules.</p> <p>For more information, including Stealthwatch hardware and software requirements, see Cisco Security Analytics and Logging (On Premises): Firepower Event Integration Guide.</p> <p>Supported platforms: FMC</p>

Feature	Description
Work with events stored remotely in a Secure Network Analytics on-prem deployment	<p>You can now use the FMC to work with connection events stored remotely in a Secure Network Analytics on-prem deployment.</p> <p>A new Data Source option on the connection events page (Analysis > Connections > Events) and in the unified event viewer (Analysis > Unified Events) allows you to choose which connection events you want to work with. The default is to display locally stored connection events, unless there are none in the time range. In that case, the system displays remotely stored events..</p> <p>We also added a data source option to report templates (Overview > Reporting > Report Templates), so that you can generate reports based on remotely stored connection events.</p> <p>Note This feature is supported for connection events only; cross-launch is still the only way to examine remotely stored Security Intelligence, intrusion, file and malware events. Even in the unified event viewer, the system only displays locally stored events of those types.</p> <p>However, note that for every Security Intelligence event, there is an identical connection event—these are the events with reasons such as 'IP Block' or 'DNS Block.' You can work with those duplicated events on the connection events page or in the unified event viewer, but not on the dedicated Security Intelligence events page.</p> <p>Supported platforms: FMC.</p>
Store all connection events in the Secure Network Analytics cloud	<p>You can now store all connection events in the Stealthwatch cloud using Cisco Security Analytics and Logging (SaaS). Previously, you were limited to security events: Security Intelligence, intrusion, file, and malware events, as well as their associated connection events.</p> <p>To change the events you send to the cloud, choose System > Integration. On the Cloud Services tab, edit the Cisco Cloud Event Configuration. The old option to send high priority connection events to the cloud has been replaced with a choice of All, None, or Security Events.</p> <p>Note These settings also control which events you send to SecureX. However, even if you choose to send all connection events to the cloud, SecureX consumes only the security (higher priority) connection events. Also note that you now configure the SecureX connection itself on Analysis > SecureX.</p> <p>Supported platforms: FMC</p>

Feature	Description
Unified event viewer	<p>The unified event viewer (Analysis > Unified Events) displays connection, Security Intelligence, intrusion, file, and malware events in a single table. This can help you look relationships between events of different types.</p> <p>A single search field allows you to dynamically filter the view based on multiple criteria, and a Go Live option displays events received from managed devices in real time.</p> <p>Supported platforms: FMC</p>
SecureX ribbon	<p>The SecureX ribbon on the FMC pivots into SecureX for instant visibility into the threat landscape across your Cisco security products.</p> <p>To connect with SecureX and enable the ribbon, use Analysis > SecureX. Note that you must still use System > Integration > Cloud Services to choose your cloud region and to specify which events to send to SecureX.</p> <p>For more information, see the Cisco Firepower and SecureX Integration Guide.</p> <p>Supported platforms: FMC</p>
Exempt all connection events from rate limiting when you turn off local storage	<p>Event rate limiting applies to all events sent to the FMC, with the exception of security events: Security Intelligence, intrusion, file, and malware events, as well as their associated connection events.</p> <p>In Version 7.0.0+, disabling local connection event storage exempts <i>all</i> connection events from rate limiting, not just security events. To do this, set the Maximum Connection Events to zero on the System > Configuration > Database page.</p> <p>Note Other than turning it off by setting it to zero, Maximum Connection Events does not govern connection event rate limiting. Any non-zero number in this field ensures that <i>all</i> lower-priority connection events are rate limited.</p> <p>Note that disabling local event storage does not affect remote event storage, nor does it affect connection summaries or correlation. The system still uses connection event information for features like traffic profiles, correlation policies, and dashboard displays.</p> <p>Supported platforms: FMC</p>
Port and protocol displayed together in file and malware event tables	<p>In file and malware event tables, the port field now displays the protocol, and you can search port fields for protocol. For events that existed before upgrade, if the protocol is not known, the system uses "tcp."</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Analysis > Files > Malware Events • Analysis > Files > File Events <p>Supported platforms: FMC</p>

Feature	Description
Upgrade	
Improved upgrade performance and status reporting	<p>FTD upgrades are now easier faster, more reliable, and take up less disk space. A new Upgrades tab in the Message Center provides further enhancements to upgrade status and error reporting.</p> <p>Supported platforms: FTD</p>
Upgrade wizard	<p>A new device upgrade page (Devices > Upgrade) on the Version 7.0.0 FMC provides an easy-to-follow wizard for upgrading Version 6.4.0+ FTD devices. It walks you through important pre-upgrade stages, including selecting devices to upgrade, copying the upgrade package to the devices, and compatibility and readiness checks.</p> <p>To begin, use the new Upgrade Firepower Software action on the Device Management page (Devices > Device Management > Select Action).</p> <p>As you proceed, the system displays basic information about your selected devices, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a device does not "pass" a stage in the wizard, it does not appear in the next stage.</p> <p>If you navigate away from wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the wizard.</p> <p>Note You must still use the System Updates page (System > Updates) page to upload or specify the location of FTD upgrade packages. You must also use the System Updates page to upgrade the FMC itself, as well as all non-FTD managed devices.</p> <p>Note In Version 7.0.0/7.0.x, the wizard does not correctly display devices in clusters or high availability pairs. Even though you must select and upgrade these devices as a unit, the wizard displays them as standalone devices. Device status and upgrade readiness are evaluated and reported on an individual basis. This means it is possible for one unit to appear to "pass" to the next stage while the other unit or units do not. However, these devices are still grouped. Running a readiness check on one, runs it on all. Starting the upgrade on one, starts it on all.</p> <p>To avoid possible time-consuming upgrade failures, <i>manually</i> ensure all group members are ready to move on to the next step of the wizard before you click Next.</p> <p>Supported platforms: FTD</p>

Feature	Description
Upgrade more devices at once	<p>The FTD upgrade wizard lifts the following restrictions:</p> <ul style="list-style-type: none"> • Simultaneous device upgrades. <p>The number of devices you can upgrade at once is now limited by your management network bandwidth—not the system's ability to manage simultaneous upgrades. Previously, we recommended against upgrading more than five devices at a time.</p> <p>Important Only upgrades to FTD Version 6.7.0+ see this improvement. If you are upgrading devices to an older FTD release—even if you are using the new upgrade wizard—we still recommend you limit to five devices at a time.</p> <ul style="list-style-type: none"> • Grouping upgrades by device model. <p>You can now queue and invoke upgrades for all FTD models at the same time, as long as the system has access to the appropriate upgrade packages.</p> <p>Previously, you would choose an upgrade package, then choose the devices to upgrade using that package. That meant that you could upgrade multiple devices at the same time <i>only</i> if they shared an upgrade package. For example, you could upgrade two Firepower 2100 series devices at the same time, but not a Firepower 2100 series and a Firepower 1000 series.</p> <p>Supported platforms: FTD</p>
Administration and Troubleshooting	
Zero-touch restore for the ISA 3000 using the SD card	<p>When you perform a local backup, the backup file is copied to the SD card if present. To restore the configuration on a replacement device, simply install the SD card in the new device, and depress the Reset button for 3 to 15 seconds during the device bootup.</p> <p>Supported platforms: ISA 3000</p>
Selectively deploy RA and site-to-site VPN policies	<p>Selective policy deployment, which was introduced in Version 6.6.0, now supports remote access and site-to-site VPN policies.</p> <p>New/modified pages: We added VPN policy options on the Deploy > Deployment page.</p> <p>Supported platforms: FTD</p>

Feature	Description
New health modules	<p>We added the following health modules:</p> <ul style="list-style-type: none"> • AMP Connection Status • AMP Threat Grid Status • ASP Drop • Advanced Snort Statistics • Chassis Status FTD • Event Stream Status • FMC Access Configuration Changes • FMC HA Status (replaces HA Status) • FTD HA Status • File System Integrity Check • Flow Offload • Hit Count • MySQL Status • NTP Status FTD • Rabbit MQ Status • Routing Statistics • SSE Connection Status • Sybase Status • Unresolved Groups Monitor • VPN Statistics • xTLS Counters <p>Additionally, full support returns for the Configuration Memory Allocation module, which was introduced in Version 6.6.3 as the Appliance Configuration Resource Utilization module, but was not fully supported in Version 6.7.0.</p> <p>Supported platforms: FMC</p>
Security and Hardening	
New default password for AWS deployments	<p>The default password for the admin account is now the AWS Instance ID, unless you define a default password with user data (Advanced Details > User Data) during the initial deployment.</p> <p>Previously, the default admin password was Admin123.</p> <p>Supported platforms: FMCv for AWS, FTDv for AWS</p>

Feature	Description
EST for certificate enrollment	<p>Support for Enrollment over Secure Transport for certificate enrollment was provided.</p> <p>New/modified pages: New enrollment options when configuring Objects > PKI > Cert Enrollment > CA Information tab.</p> <p>Supported platforms: FMC</p>
Support for EdDSA certificate type	<p>A new certificate key type- EdDSA was added with key size 256.</p> <p>New/modified pages: New certificate key options when configuring Objects > PKI > Cert Enrollment > Key tab.</p> <p>Supported platforms: FMC</p>
AES-128 CMAC authentication for NTP servers	<p>You can now use AES-128 CMAC keys to secure connections between the FMC and NTP servers.</p> <p>New/modified pages: System > Configuration > Time Synchronization.</p> <p>Supported platforms: FMC</p>
SNMPv3 users can authenticate using a SHA-224 or SHA-384 authorization algorithm	<p>SNMPv3 users can now authenticate using a SHA-224 or SHA-384 algorithm.</p> <p>New/modified pages: Devices > Platform Settings > SNMP > Users > Auth Algorithm Type</p> <p>Supported platforms: FTD</p>
Usability and Performance	
Global search for policies and objects	<p>You can now search for certain policies by name, and for certain objects by name and configured value. This feature is not available with the Classic theme.</p> <p>New/modified pages: We added capabilities to the Search icon and field on the FMC menu bar, to the left of the Deploy menu.</p> <p>Supported platforms: FMC</p>
Hardware crypto acceleration on FTDv using Intel QuickAssist Technology (QAT)	<p>We now support hardware crypto acceleration (CBC cipher only) on FTDv for VMware and FTDv for KVM. This feature requires a Intel QAT 8970 PCI adapter/Version 1.7+ driver on the hosting platform. After you reboot, hardware crypto acceleration is automatically enabled.</p> <p>Supported platforms: FTDv for VMware, FTDv for KVM</p>

Feature	Description
Improved CPU usage and performance for many-to-one and one-to-many connections.	<p>The system no longer creates local host objects and locks them when creating connections, except for connections that involve dynamic NAT/PAT and scanning threat detection and host statistics. This improves performance and CPU usage in situations where many connections are going to the same server (such as a load balancer or web server), or one endpoint is making connections to many remote hosts.</p> <p>We changed the following commands: clear local-host (deprecated), show local-host</p> <p>Supported platforms: FTD</p>
FMC REST API: New Services and Operations <p>We added the following FMC REST API services/operations to support new and existing features. For more information, see the Firepower Management Center REST API Quick Start Guide, Version 7.0.</p>	
Device	alerts: GET
Integration	fmchastatuses: GET securexconfigs: GET and PUT

Feature	Description
Object	<p>anyconnectcustomattributes, anyconnectpackages, anyconnectprofiles: GET</p> <p>anyconnectcustomattributes/overrides: GET</p> <p>applicationfilters: PUT, POST, and DELETE</p> <p>certificatemaps: GET</p> <p>dnsservergroups: GET</p> <p>dnsservergroups/overrides: GET</p> <p>dynamicobjectmappings: POST</p> <p>dynamicobjects: GET, PUT, POST, and DELETE</p> <p>dynamicobjects/mappings: GET and PUT</p> <p>geolocations: PUT, POST, and DELETE</p> <p>grouppolicies: GET</p> <p>hostscanpackages: GET</p> <p>intrusionrules, intrusionrulegroups: GET, PUT, POST, and DELETE</p> <p>intrusionrulesupload: POST</p> <p>ipv4addresspools, ipv6addresspools: GET</p> <p>ipv4addresspools/overrides, ipv6addresspools/overrides: GET</p> <p>localrealmusers: GET, PUT, POST, DELETE</p> <p>radiusservergroups: GET</p> <p>realms: PUT, POST, and DELETE</p> <p>sidnsfeeds, sidnslists, sinetworkfeeds, sinetworklists: GET</p> <p>sinkholes: GET</p> <p>ssoservers: GET</p> <p>ssoservers/overrides: GET</p> <p>usage: GET</p>

Feature	Description
Policy	<p>accesspolicies/securityintelligencepolicies: GET</p> <p>dnspolicies: GET</p> <p>dnspolicies/allowdnrules, dnspolicies/blockdnrules: GET</p> <p>dynamicaccesspolicies: GET, PUT, POST, and DELETE</p> <p>identitypolicies: GET</p> <p>intrusionpolicies: PUT, POST, and DELETE</p> <p>intrusionpolicies/intrusionrulegroups, intrusionpolicies/intrusionrules: GET and PUT</p> <p>networkanalysispolicies: GET, PUT, POST, and DELETE</p> <p>networkanalysispolicies/inspectorconfigs: GET</p> <p>networkanalysispolicies/inspectoroverrideconfigs: GET and PUT</p> <p>ravpns: GET</p> <p>ravpns/addressassignmentsettings, ravpns/certificatemapsettings, ravpns/connectionprofiles: GET</p>
Search	globalsearch: GET

Deprecated Features in FMC Version 7.0.0

Table 4: Deprecated Features in FMC Version 7.0.0

Feature	Upgrade Impact	Description
RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm	Prevents post-upgrade VPN connections through Firepower Threat Defense devices.	<p>Version 7.0.0 removes support for RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm.</p> <p>Before you upgrade, use the object manager to update your PKI certificate enrollments with stronger options: Objects > PKI > Cert Enrollment. Otherwise, although the upgrade preserves your current settings, VPN connections through the device will fail.</p> <p>To continue managing older Firepower Threat Defense devices only (Version 6.4.0–6.7.x) with these weaker options, select the new Enable Weak-Crypto option for each device on the Devices > Certificates page.</p>

Feature	Upgrade Impact	Description
MD5 authentication algorithm and DES encryption for SNMPv3 users (removed)	Prevents post-upgrade deploy.	<p>Version 7.0.0 removes support for the MD5 authentication algorithm and DES encryption for SNMPv3 users on Firepower Threat Defense devices.</p> <p>Upgrading Firepower Threat Defense to Version 7.0.0 deletes these users from the device, regardless of the configurations on the Firepower Management Center. If you are still using these options in your platform settings policy, change and verify your configurations before you upgrade Firepower Threat Defense.</p> <p>These options are in the Auth Algorithm Type and Encryption Type drop-downs when creating or editing an SNMPv3 user in a Threat Defense platform settings policy: Devices > Platform Settings.</p>
Port 32137 comms with AMP clouds	Prevents Firepower Management Center upgrade.	<p>Version 7.0.0 deprecates the Firepower Management Center option to use port 32137 to obtain file disposition data from public and private AMP clouds. Unless you configure a proxy, the Firepower Management Center now uses port 443/HTTPS.</p> <p>Before you upgrade, disable the Use Legacy Port 32137 for AMP for Networks option on the System > Integration > Cloud Services page. Do not proceed with upgrade until your AMP for Networks deployment is working as expected.</p>
HA Status health module	None.	Version 7.0.0 renames the HA Status health module. It is now the <i>FMC</i> HA Status health module. This is to distinguish it from the new FTD HA Status module.
VMware 6.0 hosting	Upgrade the hosting environment before you upgrade the Firepower software.	<p>Version 7.0.0 discontinues support for virtual deployments on VMware vSphere/VMware ESXi 6.0.</p> <p>This includes FMCv, FTDv, and NGIPSv for VMware.</p>
Web interface changes	None.	<p>Version 7.0.0 changes the following:</p> <ul style="list-style-type: none"> In the access control rule editor, the Dynamic Attributes tab replaces the narrower-focus SGT/ISE Attributes tab. Continue to configure rules with SGT attributes here. System > SecureX now configures SecureX integration. Previously, these configurations were on System > Integration > Cloud Services. Help > How-Tos now invokes walkthroughs. Previously, you clicked How-Tos at the bottom of the browser window.

Version 6.7.0

New Features in FMC Version 6.7.0

Table 5:

Feature	Description
Hardware and Virtual Appliances	
Oracle Cloud Infrastructure (OCI) virtual deployments	We introduced FMCv and FTDv for Oracle Cloud Infrastructure.
Google Cloud Platform (GCP) virtual deployments	We introduced FMCv and FTDv for Google Cloud Platform.
High availability support on FMCv for VMware	<p>FMCv for VMware now supports high availability. You use the FMCv web interface to establish HA, just as you would on hardware models.</p> <p>In an FTD deployment, you need two identically licensed FMCv's, as well as one FTD entitlement for each managed device. For example, to manage 10 FTD devices with an FMCv10 HA pair, you need two FMCv10 entitlements and 10 FTD entitlements. If you are managing Classic devices only (7000/8000 series, NGIPSv, ASA FirePOWER), you do not need FMCv entitlements.</p> <p>Note that this feature is not supported on FMCv 2 for VMware—that is, an FMCv licensed to manage only two devices.</p> <p>Supported platforms: FMCv 10, 25, and 300 for VMware</p>
Auto Scale improvements for FTDv for AWS	<p>Version 6.7.0 includes the following Auto Scale improvements for FTDv for AWS:</p> <ul style="list-style-type: none"> • Custom Metric Publisher. A new Lambda function polls the FMC every second minute for memory consumption of all FTDv instances in the Auto Scale group, then publishes the value to CloudWatch Metric. • A new scaling policy based on memory consumption is available. • FTDv private IP connectivity for SSH and Secure Tunnel to the FMC. • FMC configuration validation. • Support for opening more Listening ports on ELB. • Modified to Single Stack deployment. All Lambda functions and AWS resources are deployed from a single stack for a streamlined deployment. <p>Supported platforms: FTDv for AWS</p>

Feature	Description
Auto Scale improvements for FTDv for Azure	<p>The FTDv for Azure Auto Scale solution now includes support for scaling metrics based on CPU and memory (RAM), not just CPU.</p> <p>Supported platforms: FTDv for Azure</p>
Firepower Threat Defense: Device Management	
Manage FTD on a data interface	<p>You can now configure FMC management of the FTD on a data interface instead of using the dedicated management interface.</p> <p>This feature is useful for remote deployment when you want to manage the FTD at a branch office from an FMC at headquarters and need to manage the FTD on the outside interface. If the FTD receives a public IP address using DHCP, then you can optionally configure Dynamic DNS (DDNS) for the interface using the web type update method. DDNS ensures the FMC can reach the FTD at its Fully-Qualified Domain Name (FQDN) if the FTD's IP address changes.</p> <p>Note FMC access on a data interface is not supported with clustering or high availability.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Devices > Device Management > Device > Management section • Devices > Device Management > Interfaces > FMC Access • Devices > Device Management > DHCP > DDNS > DDNS Update Methods page <p>New/modified FTD CLI commands: configure network management-data-interface, configure policy rollback</p> <p>Supported platforms: FTD</p>
Update the FMC IP address on the FTD	<p>If you change the FMC IP address, you can now use the FTD CLI to update the device.</p> <p>New/modified FTD CLI commands: configure manager edit</p> <p>Supported platforms: FTD</p>

Feature	Description
Synchronization between the FTD operational link state and the physical link state for the Firepower 4100/9300	<p>The Firepower 4100/9300 chassis can now synchronize the FTD operational link state with the physical link state for data interfaces.</p> <p>Currently, interfaces will be in an Up state as long as the FXOS admin state is up and the physical link state is up. The FTD application interface admin state is not considered. Without synchronization from FTD, data interfaces can be in an Up state physically before the FTD application has completely come online, for example, or can stay Up for a period of time after you initiate an FTD shutdown. For inline sets, this state mismatch can result in dropped packets because external routers may start sending traffic to the FTD before the FTD can handle it.</p> <p>This feature is disabled by default, and can be enabled per logical device in FXOS.</p> <p>Note This feature is not supported for clustering, container instances, or an FTD with a Radware vDP decorator. It is also not supported for ASA.</p> <p>New/modified Firepower Chassis Manager pages: Logical Devices > Enable Link State</p> <p>New/modified FXOS commands: set link-state-sync enabled, show interface expand detail</p> <p>Supported platforms: Firepower 4100/9300</p>
Firepower 1100/2100 series SFP interfaces now support disabling auto-negotiation	<p>Upgrade impact.</p> <p>You can now configure a Firepower 1100/2100 series SFP interface to disable flow control and link status negotiation.</p> <p>Previously, when you set an SFP interface speed (1000 or 10000 Mbps) on these devices, flow control and link status negotiation was automatically enabled. You could not disable it.</p> <p>Now, you can select No Negotiate to disable flow control and link status negotiation. This also sets the speed to 1000 Mbps, regardless of whether you are configuring a 1 GB SFP or 10 GB SFP+ interface. You cannot disable negotiation at 10000 Mbps.</p> <p>New/modified pages: Devices > Device Management > Interfaces > edit interface > Hardware Configuration > Speed</p> <p>Supported platforms: Firepower 1100/2100 series</p>
Firepower Threat Defense: Clustering	

Feature	Description
New cluster management functionality on the FMC	<p>You can now use the FMC to perform the following cluster management tasks, where previously you had to use the CLI:</p> <ul style="list-style-type: none">• Enable and disable cluster units.• Show cluster status from the Device Management page, including History and Summary per unit.• Change the role to the control unit. <p>New/modified pages:</p> <ul style="list-style-type: none">• Devices > Device Management > More menu• Devices > Device Management > Cluster > General area > Cluster Live Status link > Cluster Status <p>Supported platforms: Firepower 4100/9300</p>
Faster cluster deployment	<p>Cluster deployment now completes faster. Also, for most deployment failures, it fails more quickly.</p> <p>Supported platforms: Firepower 4100/9300</p>

Feature	Description
Changes to PAT address allocation in clustering. The PAT pool Flat Port Range option is now enabled by default and it is not configurable.	<p>Upgrade impact.</p> <p>The way PAT addresses are distributed to the members of a cluster is changed.</p> <p>Previously, addresses were distributed to the members of the cluster, so your PAT pool would need a minimum of one address per cluster member. Now, the control instead divides each PAT pool address into equal-sized port blocks and distributes them across cluster members. Each member has port blocks for the same PAT addresses. Thus, you can reduce the size of the PAT pool, even to as few as one IP address, depending on the amount of connections you typically need to PAT.</p> <p>Port blocks are allocated in 512-port blocks from the 1024–65535 range. You can optionally include the reserved ports, 1–1023, in this block allocation when you configure PAT pool rules. For example, in a 4-node cluster, each node gets 32 blocks with which it will be able to handle 16384 connections per PAT pool IP address compared to a single node handling all 65535 connections per PAT pool IP address.</p> <p>As part of this change, PAT pools for all systems, whether standalone or operating in a cluster, now use a flat port range of 1024–65535. Previously, you could use a flat range by enabling the Flat Port Range option in a PAT pool rule (Pat Pool tab in an FTD NAT rule). The Flat Port Range option is now ignored: the PAT pool is now always flat. You can optionally select the Include Reserved Ports option to include the 1–1023 port range within the PAT pool.</p> <p>Note that if you configure port block allocation (the Block Allocation PAT pool option), your block allocation size is used rather than the default 512-port block. In addition, you cannot configure extended PAT for a PAT pool for systems in a cluster.</p> <p>This change takes effect automatically. You do not need to do anything before or after upgrade.</p> <p>Supported platforms: FTD</p>

Firepower Threat Defense: Encryption and VPN

Feature	Description
AnyConnect module support for RA VPN	<p>FTD RA VPN now supports AnyConnect modules.</p> <p>As part of your RA VPN group policy, you can now configure a variety of optional modules to be downloaded and installed when a user downloads the Cisco AnyConnect VPN client. These modules can provide services such as web security, malware protection, off-network roaming protection, and so on.</p> <p>You must associate each module with a profile containing your custom configurations, created in the AnyConnect Profile Editor and uploaded to the FMC as an AnyConnect File object.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Upload module profiles: We added new File Type options to Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File • Configure modules: We added Client Modules options to Objects > Object Management > VPN > Group Policy > add or edit a Group Policy object > AnyConnect settings <p>Supported platforms: FTD</p>
AnyConnect management VPN tunnels for RA VPN	<p>FTD RA VPN now supports an AnyConnect management VPN tunnel that allows VPN connectivity to endpoints when the corporate endpoints are powered on, not just when a VPN connection is established by the end user.</p> <p>This feature helps administrators perform patch management on out-of-the-office endpoints, especially devices that are infrequently connected by the user, via VPN, to the office network. Endpoint operating system login scripts which require corporate network connectivity also benefit.</p> <p>Supported platforms: FTD</p>
Single sign-on for RA VPN	<p>FTD RA VPN now supports single sign-on (SSO) for remote access VPN users configured at a SAML 2.0-compliant identity provider (IdP).</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Connect to an SSO server: Objects > Object Management > AAA Server > Single Sign-on Server • Configure SSO as part of RA VPN: We added SAML as an authentication method (AAA settings) when configuring an RA VPN connection profile. <p>Supported platforms: FTD</p>

Feature	Description
LDAP authorization for RA VPN	<p>FTD RA VPN now supports LDAP authorization using LDAP attribute maps.</p> <p>An LDAP attribute map equates attributes that exist in the Active Directory (AD) or LDAP server with Cisco attribute names. Then, when the AD or LDAP server returns authentication to the FTD device during remote access VPN connection establishment, the FTD device can use the information to adjust how the AnyConnect client completes the connection.</p> <p>Supported platforms: FTD</p>
Virtual Tunnel Interface (VTI) and route-based site-to-site VPN	<p>FTD site-to-site VPN now supports a logical interface called Virtual Tunnel Interface (VTI).</p> <p>As an alternative to policy-based VPN, a VPN tunnel can be created between peers with Virtual Tunnel Interfaces configured. This supports route-based VPN with IPsec profiles attached to the end of each tunnel. This allows dynamic or static routes to be used. Using VTI does away with the requirement of configuring static crypto map access lists and mapping them to interfaces. Traffic is encrypted using static route or BGP. You can create a routed security zone, add VTI interfaces to it, and define access control rules for the decrypted traffic control over the VTI tunnel.</p> <p>VTI-based VPNs can be created between:</p> <ul style="list-style-type: none"> • Two FTD devices • An FTD device and a public cloud • An FTD device and another FTD device with service provider redundancy <p>New/modified pages:</p> <ul style="list-style-type: none"> • Devices > Device Management > Interfaces > Add Interfaces > Virtual Tunnel Interface • Devices > VPN > Site To Site > Add VPN > Firepower Threat Defense Device > Route Based (VTI) <p>Supported platforms: FTD</p>
Dynamic RRI support for site-to-site VPN	<p>FTD site-to-site VPN now supports Dynamic Reverse Route Injection (RRI) supported with IKEv2-based static crypto maps in site-to-site VPN deployments. This allowed static routes to be automatically inserted into the routing process for networks and hosts protected by a remote tunnel endpoint.</p> <p>New/modified pages: We added the Enable Dynamic Reverse Route Injection advanced option when adding an endpoint to a site-to-site VPN topology.</p> <p>Supported platforms: FTD</p>

Feature	Description
Enhancements to manual certificate enrollment	<p>You can now obtain signed CA certificates and identity certificates from a CA authority independently of each other.</p> <p>We made the following changes to PKI certificate enrollment objects, which store enrollment parameters for creating Certificate Signing Requests (CSRs) and obtaining identity certificates:</p> <ul style="list-style-type: none"> • We added the CA Only option to the manual enrollment settings for PKI certificate enrollment objects. If you enable this option, you will receive only a signed CA certificate from the CA authority, and not the identity certificate. • You can now leave the CA Certificate field blank in the manual enrollment settings for PKI certificate enrollment objects. If you do this, you will receive only the identity certificate from the CA authority, and not the signed CA certificate. <p>New/modified pages: Objects > Object Management > PKI > Cert Enrollment > Add Cert Enrollment > CA Information > Enrollment Type > Manual</p> <p>Supported platforms: FTD</p>
Enhancements to FTD certificate management	<p>We made the following enhancements to FTD certificate management:</p> <ul style="list-style-type: none"> • You can now view the chain of certifying authorities (CAs) when viewing certificate contents. • You can now export certificates. <p>New/modified pages:</p> <ul style="list-style-type: none"> • Devices > Certificates > Status column > View icon (magnifying glass) • Devices > Certificates > Export icon <p>Supported platforms: FTD</p>
Access Control: URL Filtering, Application Control, and Security Intelligence	

Feature	Description
URL filtering and application control on traffic encrypted with TLS 1.3 (TLS Server Identity Discovery)	<p>You can now perform URL filtering and application control on traffic encrypted with TLS 1.3, by using information from the server certificate. You do not have to decrypt the traffic for this feature to work.</p> <p>Note We recommend enabling this feature if you want to perform URL filtering and application control on encrypted traffic. However, it can affect device performance, especially on lower-memory models.</p> <p>New/modified pages: We added a TLS Server Identity Discovery warning and option to the access control policy's Advanced tab.</p> <p>New/modified FTD CLI commands: We added the B flag to the output of the show conn detail command. On a TLS 1.3-encrypted connection, this flag indicates that we used the server certificate for application and URL detection.</p> <p>Supported platforms: FTD</p>
URL filtering on traffic to websites with unknown reputation	<p>You can now perform URL filtering for websites that have an unknown reputation.</p> <p>New/modified pages: We added an Apply to unknown reputation check box to the access control, QoS, and SSL rule editors.</p> <p>Supported platforms: FMC</p>
DNS filtering enhances URL filtering	<p>Beta.</p> <p><i>DNS filtering</i> enhances URL filtering by determining the category and reputation of requested domains earlier in the transaction, including in encrypted traffic—but without decrypting the traffic. You enable DNS filtering per access control policy, where it applies to all category/reputation URL rules in that policy.</p> <p>Note DNS filtering is a Beta feature and may not work as expected. Do not use it in production environments.</p> <p>New/modified pages: We added the Enable reputation enforcement on DNS traffic option to the access control policy's Advanced tab, under General Settings.</p> <p>Supported platforms: FMC</p>

Feature	Description
Shorter update frequencies for Security Intelligence feeds	<p>The FMC can now update Security Intelligence data every 5 or 15 minutes. Previously, the shortest update frequency was 30 minutes.</p> <p>If you configure one of these shorter frequencies on a custom feed, you must also configure the system to use an md5 checksum to determine whether the feed has updates to download.</p> <p>New/modified pages: We added new options to Objects > Object Management > Security Intelligence > Network Lists and Feeds > edit feed > Update Frequency</p> <p>Supported platforms: FMC</p>
Access Control: User Control	
pxGrid 2.0 with ISE/ISE-PIC	<p>Upgrade impact.</p> <p>Use pxGrid 2.0 when you connect the FMC to an ISE/ISE-PIC identity source. If you are still using pxGrid 1.0, switch now. That version is deprecated.</p> <p>For use with pxGrid 2.0, Version 6.7.0 introduces the Cisco ISE Adaptive Network Control (ANC) remediation, which applies or clears ISE-configured ANC policies involved in a correlation policy violation.</p> <p>If you used the Cisco ISE Endpoint Protection Services (EPS) remediation with pxGrid 1.0, configure and use the ANC remediation with pxGrid 2.0. ISE remediations will not launch if you are using the 'wrong' pxGrid. The ISE Connection Status Monitor health module alerts you to mismatches.</p> <p>For detailed compatibility information for all supported Firepower versions, including integrated products, see the Cisco Firepower Compatibility Guide.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Policies > Actions > Modules > Installed Remediation Modules list • Policies > Actions > Instances > Select a module type drop-down list <p>Supported platforms: FMC</p>
Realm sequences	<p>You can now group realms into ordered <i>realm sequences</i>.</p> <p>Add a realm sequence to an identity rule in the same way as you add a single realm. When applying the identity rule to network traffic, the system searches the Active Directory domains in the order specified. You cannot create realm sequences for LDAP realms.</p> <p>New/modified pages: System > Integration > Realm Sequences</p> <p>Supported platforms: FMC</p>

Feature	Description
ISE subnet filtering	<p>Especially useful on lower-memory devices, you can now use the CLI to exclude subnets from receiving user-to-IP and Security Group Tag (SGT)-to-IP mappings from ISE.</p> <p>The Snort Identity Memory Usage health module alerts when memory usage exceeds a certain level, which by default is 80%.</p> <p>New device CLI command: configure identity-subnet-filter {add remove}</p> <p>Supported platforms: FMC-managed devices</p>
Access Control: Intrusion and Malware Prevention	
Improved preclassification of files for dynamic analysis	<p>Upgrade impact.</p> <p>The system can now decide not to submit a suspected malware file for dynamic analysis, based on the static analysis results (for example, a file with no dynamic elements).</p> <p>After you upgrade, in the Captured Files table, these files will have a Dynamic Analysis Status of Rejected for Analysis.</p> <p>Supported platforms: FMC</p>
S7Commplus preprocessor	<p>The new S7Commplus preprocessor supports the widely accepted S7 industrial protocol. You can use it to apply corresponding intrusion and preprocessor rules, drop malicious traffic, and generate intrusion events.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Enable the preprocessor: In the network analysis policy editor, click Settings (you must <i>click</i> the word 'Settings'), and enable S7Commplus Configuration under SCADA Preprocessors. • Configure the preprocessor: In the network analysis policy editor, under Settings, click S7Commplus Configuration. • Configure S7Commplus preprocessor rules: In the intrusion policy editor, click Rules > Preprocessors > S7 Commplus Configurations. <p>Supported platforms: all FTD devices, including ISA 3000</p>

Feature	Description
Custom intrusion rule import warns when rules collide	<p>The FMC now warns you of rule collisions when you import custom (local) intrusion rules. Previously, the FMC would silently skip the rules that cause collisions—with the exception of Version 6.6.0.1, where a rule import with collisions would fail entirely.</p> <p>On the Rule Updates page, if a rule import had collisions, a warning icon is displayed in the Status column. For more information, hover your pointer over the warning icon and read the tooltip.</p> <p>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 Firepower Management Center Configuration Guide.</p> <p>New/modified pages: We added a warning icon to System > Updates > Rule Updates.</p> <p>Supported platforms: FMC</p>
Access Control: TLS/SSL Decryption	
ClientHello modification for Decrypt - Known Key TLS/SSL rules	<p>Upgrade impact.</p> <p>If you configure TLS/SSL decryption, when a managed device receives a ClientHello message, the system now attempts to match the message to TLS/SSL rules that have the Decrypt - Known Key action. Previously, the system only matched ClientHello messages to Decrypt - Resign rules.</p> <p>The match relies on data from the ClientHello message and from cached server certificate data. If the message matches, the device modifies the ClientHello message in specific ways; see the <i>ClientHello Message Handling</i> topic in the Firepower Management Center Configuration Guide.</p> <p>This behavior change occurs automatically after upgrade. If you use Decrypt - Known Key TLS/SSL rules, make sure that encrypted traffic is being handled as expected.</p> <p>Supported platforms: Any device</p>
Event Logging and Analysis	

Feature	Description
Remote data storage and cross-launch with an on-prem Stealthwatch solution	<p>You can now store large volumes of Firepower event data off-FMC, using an on-premises Stealthwatch solution: Cisco Security Analytics and Logging (On Premises).</p> <p>When viewing events in FMC, you can quickly cross-launch to view events in your remote data storage location. The FMC uses syslog to send connection, Security Intelligence, intrusion, file, and malware events.</p> <p>Note This on-prem solution is supported for FMCs running Version 6.4.0+. However, contextual cross-launch requires Firepower Version 6.7.0+. This solution also depends on availability of the Security Analytics and Logging On Prem app for the Stealthwatch Management Console (SMC), which must be running Stealthwatch Enterprise (SWE) version 7.3.</p> <p>Supported platforms: FMC</p>
Quickly add Stealthwatch contextual cross-launch resources	<p>A new page on the FMC allows you to quickly add contextual cross-launch resources for your Stealthwatch appliance.</p> <p>After you add Stealthwatch resources, you manage them on the general contextual cross-launch page. This is where you continue to manually create and manage non-Stealthwatch cross-launch resources.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Add Stealthwatch resources: System > Logging > Security Analytics and Logging • Manage resources: Analysis > Advanced > Contextual Cross-Launch <p>Supported platform: FMC</p>

Feature	Description
New cross-launch options field types	<p>You can now cross-launch into an external resource using the following additional types of event data:</p> <ul style="list-style-type: none"> • Access control policy • Intrusion policy • Application protocol • Client application • Web application • Username (including realm) <p>New/modified pages:</p> <ul style="list-style-type: none"> • New variables when creating or editing cross-launch query links: Analysis > Advanced > Contextual Cross-Launch. • New data types in the dashboard and event viewer now offer cross-launch on right click. <p>Supported platforms: FMC</p>
National Vulnerability Database (NVD) replaces Bugtraq	<p>Upgrade impact.</p> <p>Bugtraq vulnerability data is no longer available. Most vulnerability data now comes from the NVD. To support this change, we made the following changes:</p> <ul style="list-style-type: none"> • Added the CVE ID and Severity fields to the Vulnerabilities table. Right-clicking the CVE ID in the table view allows you to view details about the vulnerability on the NVD. • Renamed the Vulnerability Impact field to Impact (in the table view only). • Removed the obsolete/redundant Bugtraq ID, Title, Available Exploits, Technical Description, and Solution fields. • Removed the Bugtraq ID filtering option from the Hosts network map. <p>If you export vulnerability data, make sure any integrations are working as expected after the upgrade.</p> <p>Supported platforms: FMC</p>
Upgrade	

Feature	Description
Pre-upgrade compatibility check	<p>Upgrade impact.</p> <p>In FMC deployments, Firepower appliances must now pass pre-upgrade compatibility checks before you can run more complex readiness checks or attempt to upgrade. This check catches issues that <i>will</i> cause your upgrade to fail—but we now catch them earlier and block you from proceeding.</p> <p>The checks are as follows:</p> <ul style="list-style-type: none"> You cannot use the FMC to upgrade a Firepower 4100/9300 chassis to Version 6.7.0+ until you upgrade FXOS to the new release's companion FXOS version. <p>Upgrade is blocked as long as you are upgrading the device to Version 6.7.0 or later. For example, you are <i>not</i> blocked from attempting a Firepower 4100/9300 upgrade from 6.3 → 6.6.x, even if the device is running a version of FXOS that is too old for Firepower Version 6.6.x.</p> <ul style="list-style-type: none"> You cannot use the FMC to upgrade a device if that device has out-of-date configurations. <p>Upgrade is blocked as long as the FMC is running Version 6.7.0 or later, and you are upgrading a managed device to a valid target. For example, you <i>are</i> blocked from upgrading a device from 6.3.0 → 6.6.x if the device has outdated configurations.</p> <ul style="list-style-type: none"> You cannot upgrade an FMC <i>from</i> Version 6.7.0+ if its devices have out-of-date configurations. <p>Upgrade is blocked as long as the FMC is running Version 6.7.0 or later. For upgrades from earlier versions (including <i>to</i> Version 6.7.0), you must make sure you deploy yourself.</p> <p>When you select an upgrade package to install, the FMC displays compatibility check results for all eligible appliances. The new Readiness Check page also displays this information. You cannot upgrade until you fix the issues indicated.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> System > Update > Product Updates > Available Updates > Install icon for the upgrade package System > Update > Product Updates > Readiness Checks <p>Supported platforms: FMC, FTD</p>

Feature	Description
Improved readiness checks	<p>Upgrade impact.</p> <p>Readiness checks assess a Firepower appliance's preparedness for a software upgrade. These checks include database integrity, file system integrity, configuration integrity, disk space, and so on.</p> <p>After you upgrade the FMC to Version 6.7.0, you will see the following improvements to FTD upgrade readiness checks:</p> <ul style="list-style-type: none"> • Readiness checks are faster. • Readiness checks are now supported on high availability and clustered FTD devices, without having to log into the device CLI. • Readiness checks for FTD device upgrades to Version 6.7.0+ no longer require the upgrade package to reside on the device. Although we still recommend you push the upgrade package to the device before you begin the upgrade itself, you no longer have to do so before you run the readiness check. • When you select an upgrade package to install, the FMC now shows the readiness status for all applicable FTD devices. A new Readiness Checks page allows you to view the results of readiness checks for the FTD devices in your deployment. You can also re-run readiness checks from this page. • Readiness check results include the estimated upgrade time (but do not include reboot time). • Error messages are better. You can also download success/failure logs from the Message Center on the FMC. <p>Note that these improvements are supported for FTD upgrades from Version 6.3.0+, as long as the FMC is running Version 6.7.0+.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • System > Update > Product Updates > Available Updates > Install icon for the upgrade package • System > Update > Product Updates > Readiness Checks • Message Center > Tasks <p>Supported platforms: FTD</p>

Feature	Description
Improved FTD upgrade status reporting and cancel/retry options	<p>Upgrade impact.</p> <p>You can now view the status of device upgrades and readiness checks in progress on the Device Management page, as well as a 7-day history of upgrade success/failures. The Message Center also provides enhanced status and error messages.</p> <p>A new Upgrade Status pop-up, accessible from both Device Management and the Message Center with a single click, shows detailed upgrade information, including percentage/time remaining, specific upgrade stage, success/failure data, upgrade logs, and so on.</p> <p>Also on this pop-up, you can manually cancel failed or in-progress upgrades (Cancel Upgrade), or retry failed upgrades (Retry Upgrade). Canceling an upgrade reverts the device to its pre-upgrade state.</p> <p>Note To be able to manually cancel or retry a failed upgrade, you must disable the new auto-cancel option, which appears when you use the FMC to upgrade an FTD device: Automatically cancel on upgrade failure and roll back to the previous version. With the option enabled, the device automatically reverts to its pre-upgrade state upon upgrade failure.</p> <p>Auto-cancel is not supported for patches. In an HA or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • System > Update > Product Updates > Available Updates > Install icon for the FTD upgrade package • Devices > Device Management > Upgrade • Message Center > Tasks <p>New FTD CLI commands:</p> <ul style="list-style-type: none"> • show upgrade status detail • show upgrade status continuous • show upgrade status • upgrade cancel • upgrade retry <p>Supported platforms: FTD</p>

Feature	Description
Upgrades postpone scheduled tasks	<p>Upgrade impact.</p> <p>FMC upgrades now postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot.</p> <p>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.</p> <p>Note that this feature is supported for all upgrades <i>from</i> a supported version. This includes Version 6.4.0.10 and later patches, Version 6.6.3 and later maintenance releases, and Version 6.7.0+. This feature is not supported for upgrades <i>to</i> a supported version from an unsupported version.</p> <p>Supported platforms: FMC</p>
Upgrades remove PCAP files to save disk space	<p>Upgrade impact.</p> <p>To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. Upgrades now remove locally stored PCAP files.</p> <p>Supported platforms: Any</p>
Deployment and Policy Management	
Configuration rollback	<p>Beta.</p> <p>You can now "roll back" configurations on an FTD device, replacing them with the previously deployed configurations.</p> <p>Note Rollback is a Beta feature, and is not supported in all deployment types and scenarios. It is also a disruptive operation. Make sure you read and understand the guidelines and limitations in the <i>Policy Management</i> chapter of the Firepower Management Center Configuration Guide.</p> <p>New/modified pages: Deploy > Deployment History > Rollback column and icons.</p> <p>Supported platforms: FTD</p>
Back up and restore FTD container instances	<p>You can now use the FMC to back up FTD container instances.</p> <p>Supported platforms: Firepower 4100/9300</p>
Deploy intrusion and file policies independently of access control policies	<p>You can now select and deploy intrusion and file policies independently of access control policies, unless there are dependent changes.</p> <p>New/modified pages: Deploy > Deployment</p> <p>Supported platforms: FMC</p>

Feature	Description
Search access control rule comments	<p>You can now search within access control rules comments.</p> <p>New/modified pages: In the access control policy editor, we added the Comments field to the Search Rules drop-down dialog.</p> <p>Supported platforms: FMC</p>
Search and filter FTD NAT rules	<p>You can now search for rules in an FTD NAT policy to help you find rules based on IP addresses, ports, object names, and so forth. Search results include partial matches. Searching on criteria filters the rule table so only matching rules are displayed.</p> <p>New/modified pages: We added a search field above the rule table when you edit an FTD NAT policy.</p> <p>Supported platforms: FTD</p>
Copy and move rules between access control and prefilter policies	<p>You can copy access control rules from one access control policy to another. You can also move rules between an access control policy and its associated prefilter policy.</p> <p>New/modified pages: In the access control and prefilter policy editors, we added Copy and Move options to each rule's right-click menu.</p> <p>Supported platforms: FMC</p>
Bulk object import	<p>You can now bulk-import network, port, URL, VLAN tag, and distinguished name objects onto the FMC, using a comma-separated-values (CSV) file.</p> <p>For restrictions and specific formatting instructions, see the <i>Reusable Objects</i> chapter of the Firepower Management Center Configuration Guide.</p> <p>New/modified pages: Objects > Object Management > choose an object type > Add [Object Type] > Import Object</p> <p>Supported platforms: FMC</p>

Feature	Description
Interface object optimization for access control and prefilter policies	<p>You can now enable interface object optimization on specific FTD devices.</p> <p>During deployment, interface groups and security zones used in the access control and prefilter policies generate separate rules for each source/destination interface pair. If you enable interface object optimization, the system will instead deploy a single rule per access control/prefilter rule, which can simplify the device configuration and improve deployment performance.</p> <p>Interface object optimization is disabled by default. If you enable it, you should also enable Object Group Search—which now applies to interface objects in addition to network objects—to reduce memory usage on the device.</p> <p>New/modified pages: Devices > Device Management > Device > Advanced Settings section > Interface Object Optimization check box</p> <p>Supported platforms: FTD</p>
Administration and Troubleshooting	
FMC single sign-on	<p>The FMC now supports single sign-on (SSO) for external users configured at any third-party SAML 2.0-compliant identity provider (IdP). You can map user or group roles from the IdP to FMC user roles.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Login > Single Sign-On • System > Users > SSO <p>Supported platforms: FMC</p>
FMC logout delay	<p>When you log out of the FMC, there is an automatic five-second delay and countdown. You can click Log Out again to log out immediately.</p> <p>Supported platforms: FMC</p>

Feature	Description
Health monitoring enhancements	<p>We enhanced health monitoring as follows:</p> <ul style="list-style-type: none">• Health Status summary page that provides an at-a-glance view of the health of the Firepower Management Center and all of the devices that the FMC manages.• The Monitoring navigation pane allows you to navigate the device hierarchy.• Managed devices are listed individually, or grouped according to their geolocation, high availability, or cluster status where applicable.• You can view health monitors for individual devices from the navigation pane.• Custom dashboards to correlate interrelated metrics. Select from predefined correlation groups, such as CPU and Snort; or create a custom correlation dashboard by building your own variable set from the available metric groups. <p>Supported platforms: FMC</p>

Feature	Description
Health module updates	<p>We replaced the CPU Usage health module with four new modules:</p> <ul style="list-style-type: none"> • CPU Usage (per core): Monitors the CPU usage on all of the cores. • CPU Usage Data Plane: Monitors the average CPU usage of all data plane processes on the device. • CPU Usage Snort: Monitors the average CPU usage of the Snort processes on the device. • CPU Usage System: Monitors the average CPU usage of all system processes on the device. <p>We added the following health modules to track memory use:</p> <ul style="list-style-type: none"> • Memory Usage Data Plane: Monitors the percentage of allocated memory used by data plane processes. • Memory Usage Snort: Monitors the percentage of allocated memory used by the Snort process. <p>We added the following health modules to track statistics:</p> <ul style="list-style-type: none"> • Connection Statistics: Monitors connection statistics and NAT translation counts. • Critical Process Statistics: Monitors the state of critical processes, their resource consumption, and the restart counts. • Deployed Configuration Statistics: Monitors statistics about the deployed configuration, such as the number of ACEs and IPS rules. • Snort Statistics: Monitors Snort statistics for events, flows, and packets. <p>Supported platforms: FMC</p>
Search Message Center	<p>You can now filter the current view in the Message Center.</p> <p>New/modified pages: We added a Filter icon and field to the Message Center, under the Show Notifications slider.</p> <p>Supported platforms: FMC</p>
Usability and Performance	

Feature	Description
Dusk theme	<p>Beta.</p> <p>The FMC web interface defaults to the Light theme, but you can also choose a new Dusk theme.</p> <p>Note The Dusk theme is a Beta feature. If you encounter issues that prevent you from using a page or feature, switch to a different theme. Although we cannot respond to everybody, we also welcome feedback — please use the feedback link on the User Preferences page or contact us at fmc-light-theme-feedback@cisco.com.</p> <p>New/modified pages: User Preferences, from the drop-down list under your username</p> <p>Supported platforms: FMC</p>
Search FMC menus	<p>You can now search the FMC menus.</p> <p>New/modified pages: We added a Search icon and field to the FMC menu bar, to the left of the Deploy menu.</p> <p>Supported platforms: FMC</p>
Firepower Management Center REST API	

Feature	Description
New REST API services	<p>We added the following FMC REST API services/operations to support new and existing features.</p> <p>Authorization services:</p> <ul style="list-style-type: none"> • ssoconfig: GET and PUT operations to retrieve and modify FMC single-sign on. <p>Health services:</p> <ul style="list-style-type: none"> • metrics: GET operation to retrieve metrics for the health monitor. • alerts: GET operation to retrieve health alerts. • deploymentdetails: GET operation to retrieve deployment health details. <p>Deployment services:</p> <ul style="list-style-type: none"> • jobhistories: GET operation to retrieve deployment history. • rollbackrequests: POST operation to request a configuration rollback. <p>Device services:</p> <ul style="list-style-type: none"> • metrics: GET operation to retrieve device metrics. • virtualtunnelinterfaces: GET, PUT, POST, and DELETE operations to retrieve and modify virtual tunnel interfaces. <p>Integration services:</p> <ul style="list-style-type: none"> • externalstorage: GET, GET by ID, and PUT operations to retrieve and modify external event storage configuration. <p>Policy services:</p> <ul style="list-style-type: none"> • intrusionpolicies: POST and DELETE operations to modify intrusion policies. <p>Update services:</p> <ul style="list-style-type: none"> • cancelupgrades: POST operation to cancel a failed upgrade. • retryupgrades: POST operation to retry a failed upgrade. <p>Supported platforms: FMC</p>

Deprecated Features in FMC Version 6.7.0

Table 6:

Feature	Upgrade Impact	Description
Cisco Firepower User Agent software and identity source	Prevents Firepower Management Center upgrade.	<p>You cannot upgrade a Firepower Management Center with user agent configurations to Version 6.7.0+.</p> <p>Version 6.6.0/6.6.x is the last release to support the Cisco Firepower User Agent software as an identity source. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC). To convert your license, contact Sales.</p> <p>For more information, see the End-of-Life and End-of-Support for the Cisco Firepower User Agent announcement and the Firepower User Identity: Migrating from User Agent to Identity Services Engine TechNote.</p> <p>Deprecated FTD CLI commands: configure user agent</p>
Cisco ISE Endpoint Protection Services (EPS) remediation	ISE remediations can stop working.	<p>The Cisco ISE Endpoint Protection Services (EPS) remediation does not work with pxGrid 2.0. Configure and use the new Cisco ISE Adaptive Network Control (ANC) remediation instead.</p> <p>ISE remediations will not launch if you are using the 'wrong' pxGrid to connect the Firepower Management Center to an ISE/ISE-PIC identity source. The ISE Connection Status Monitor health module alerts you to mismatches.</p>

Feature	Upgrade Impact	Description
Less secure Diffie-Hellman groups, and encryption and hash algorithms	Prevents Firepower Management Center upgrade.	<p>You may not be able to upgrade a Firepower Management Center if you use any of the following Firepower Threat Defense features:</p> <ul style="list-style-type: none"> • Diffie-Hellman groups: 2, 5, and 24. Group 5 continues to be supported in Firepower Management Center deployments for IKEv1, but we recommend you change to a stronger option. • Encryption algorithms for users who satisfy export controls for strong encryption: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continues to be supported (and is the only option) for users who do not satisfy export controls. • The NULL "encryption algorithm" (authentication without encryption, for testing purposes) continues to be supported in Firepower Management Center deployments for both IKEv1 and IKEv2 IPsec proposals. However, it is no longer supported in IKEv2 policies. • Hash algorithms: MD5. <p>If you are still using these features in IKE proposals or IPsec policies, change and verify your VPN configuration before you upgrade.</p>

Feature	Upgrade Impact	Description
Appliance Configuration Resource Utilization health module (temporary deprecation)	Possible post-upgrade errors in the health monitor	<p>Version 6.7.0 <i>partially</i> and <i>temporarily</i> deprecates support for the Appliance Configuration Resource Utilization health module, which was introduced in Version 6.6.3 and is supported in all later 6.6.x releases.</p> <p>Version 6.7.0 support is as follows:</p> <ul style="list-style-type: none"> • Firepower Management Center upgraded to Version 6.7.0 from Version 6.6.3+ <p>Continues to support the module, but only if the devices remain at Version 6.6.3/6.6.x. If you upgrade the devices to Version 6.7.0, the module stops working and the health monitor displays an error. To resolve the error, use the Firepower Management Center to disable the module and reapply policies.</p> <ul style="list-style-type: none"> • Firepower Management Center upgraded to Version 6.7.0 from Version 6.3.0–6.6.1, <i>or</i> Firepower Management Center freshly installed to Version 6.7.0. <p>Does not support the module .</p> <p>In the rare case that you add a Version 6.6.3/6.6.x device that has the module enabled to a Firepower Management Center where the module is not supported, the health monitor displays an error that you cannot resolve. This error is safe to ignore.</p> <p>Full support returns in Version 7.0.0, where the module is renamed to Configuration Memory Allocation.</p>
Other health modules (permanent deprecation)	None.	<p>Version 6.7.0 deprecates the following health modules:</p> <ul style="list-style-type: none"> • CPU Usage: Replaced by four new modules; see New Features in FMC Version 6.7.0, on page 36. • Local Malware Analysis: This module was replaced by the Threat Data Updates on Devices module in Version 6.3.0. A Version 6.7.0+ Firepower Management Center can no longer manage any devices where the older module applies. • User Agent Status Monitor: Cisco Firepower User Agent is no longer supported.
Walkthroughs with the Classic theme	None.	Version 6.7.0 discontinues Firepower Management Center walkthroughs (<i>how-tos</i>) for the Classic theme. You can switch themes in your user preferences.

Feature	Upgrade Impact	Description
Bugtraq	If you export vulnerability data, make sure any integrations are working as expected after the upgrade.	Version 6.7.0 removes database fields and options for Bugtraq. Bugtraq vulnerability data is no longer available. Most vulnerability data now comes from the National Vulnerability Database (NVD). For more information, see New Features in FMC Version 6.7.0, on page 36 .
Microsoft Internet Explorer	You should switch browsers.	We no longer test Firepower web interfaces using Microsoft Internet Explorer. We recommend you switch to Google Chrome, Mozilla Firefox, or Microsoft Edge.
ASA 5525-X, 5545-X, and 5555-X devices with Firepower software	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.7.0+ of the Firepower software (both Firepower Threat Defense and ASA FirePOWER) on ASA 5525-X, 5545-X, and 5555-X devices.

Version 6.6.3

New Features in FMC Version 6.6.3

Table 7:

Feature	Description
Upgrades postpone scheduled tasks	<p>Upgrade impact.</p> <p>Upgrades now postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot.</p> <p>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.</p> <p>Note that this feature is supported for Firepower appliances running Version 6.6.3+. It is not supported for upgrades <i>to</i> Version 6.6.3, unless you are upgrading from Version 6.4.0.10 or any later patch.</p>

Feature	Description
Appliance Configuration Resource Utilization health module	<p>Upgrade impact for Version 6.7.0.</p> <p>Version 6.6.3 improves device memory management and introduces a new health module: Appliance Configuration Resource Utilization.</p> <p>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 Firepower Management Center Configuration Guide.</p> <p>The upgrade process automatically adds and enables this module in all health policies. After upgrade, apply health policies to managed devices to begin monitoring.</p> <p>Note This module requires Version 6.6.3 or later 6.6.x release, or Version 7.0.0+ on both the FMC and managed devices.</p> <p>Version 6.7.0 <i>partially</i> and <i>temporarily</i> deprecates support for this module. For details, see Deprecated Features in FMC Version 6.7.0, on page 60.</p> <p>Full support returns in Version 7.0.0, where the module is renamed to Configuration Memory Allocation.</p>

Version 6.6.1

Deprecated Features in FMC Version 6.6.1

Table 8:

Feature	Upgrade Impact	Description
Custom intrusion rule import does not fail when rules collide	None.	<p>In Version 6.6.0, the Firepower Management Center 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 6.6.0 behavior of silently skipping the rules that cause collisions.</p> <p>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 Firepower Management Center Configuration Guide.</p> <p>Version 6.7.0 adds a warning for rule collisions in a later release.</p>

Version 6.6.0

New Features in FMC Version 6.6.0

Table 9:

Feature	Description
Hardware and Virtual Appliances	
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	<p>Upgrade impact.</p> <p>FTDv for AWS adds support for these larger instances:</p> <ul style="list-style-type: none"> • C5.xlarge • C5.2xlarge • C5.4xlarge <p>FMCv for AWS adds support for these larger instances:</p> <ul style="list-style-type: none"> • C3.4xlarge • C4.4xlarge • C5.4xlarge <p>All existing FMCv for AWS instance types are now deprecated. You must resize before you upgrade. For more information, see the Version 6.6.0 upgrade guidelines.</p> <p>Supported platforms: FTDv for AWS, FTDv for AWS</p>
Autoscale for cloud-based FTDv deployments	<p>Version 6.6.0 introduces support for AWS Auto Scale/Azure Autoscale.</p> <p>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.</p> <p>Supported platforms: FTDv for AWS, FTDv for Azure</p>
Firepower Threat Defense: Device Management	

Feature	Description
Obtain initial management interface IP address using DHCP	<p>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.</p> <p>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.</p> <p>Supported platforms: Firepower 1000/2000 series, ASA-5500-X series</p>
Configure MTU values in CLI	<p>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:</p> <ul style="list-style-type: none"> • Management interface: 1500 bytes • Eventing interface: 9000 bytes <p>New FTD CLI commands: configure network mtu</p> <p>Modified FTD CLI commands: Added the mtu-event-channel and mtu-management-channel keyword to the configure network management-interface command.</p> <p>Supported platforms: FTD</p>
Get upgrade packages from an internal web server	<p>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.</p> <p>Note This feature is supported only for FTD devices running Version 6.6.0+. It is not supported for upgrades <i>to</i> Version 6.6.0, nor is it supported for the FMC or Classic devices.</p> <p>New/modified pages: System > Updates > Upload Update button > Specify software update source option</p> <p>Supported platforms: FTD</p>
Connection-based troubleshooting enhancements	<p>We made the following enhancements to FTD CLI connection-based troubleshooting (debugging):</p> <ul style="list-style-type: none"> • debug packet-module trace: Added to enable module level packet tracing. • debug packet-condition: Modified to support troubleshooting of ongoing connections. <p>Supported platforms: FTD</p>
Firepower Threat Defense: Clustering	

Feature	Description
Multi-instance clustering	<p>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.</p> <p>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.</p> <p>New FXOS CLI commands: set port-type cluster</p> <p>New/modified Firepower Chassis Manager pages:</p> <ul style="list-style-type: none"> • Logical Devices > Add Cluster • Interfaces > All Interfaces > Add New drop-down menu > Subinterface > Type field <p>Supported platforms: Firepower 4100/9300</p>
Parallel configuration sync to data units in FTD clusters	<p>The control unit in an FTD cluster now syncs configuration changes with slave units in parallel by default. Formerly, syncing occurred sequentially.</p> <p>Supported platforms: Firepower 4100/9300</p>
Messages for cluster join failure or eviction added to show cluster history	<p>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.</p> <p>Supported platforms: Firepower 4100/9300</p>

Firepower Threat Defense: Routing

Feature	Description
Virtual routers and VRF-Lite	<p>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.</p> <p>Virtual routers implement the “light” version of Virtual Routing and Forwarding, or VRF-Lite, which does not support Multiprotocol Extensions for BGP (MBGP).</p> <p>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 <i>Firepower Management Center Configuration Guide</i>.</p> <p>New/modified pages: Devices > Device Management > edit device > Routing tab</p> <p>New FTD CLI commands: show vrf.</p> <p>Modified FTD CLI commands: Added the <code>[vrf name all]</code> 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.</p> <p>Supported platforms: FTD, except Firepower 1010 and ISA 3000</p>
Firepower Threat Defense: VPN	
DTLS 1.2 in remote access VPN	<p>You can now use Datagram Transport Layer Security (DTLS) 1.2 to encrypt RA VPN connections.</p> <p>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.</p> <p>Requires Cisco AnyConnect Secure Mobility Client, Version 4.7+.</p> <p>New/modified pages: Devices > Platform Settings > add/edit Threat Defense policy > SSL > DTLS Version option</p> <p>Supported platforms: FTD, except ASA 5508-X and ASA 5516-X</p>
Site-to-site VPN IKEv2 support for multiple peers	<p>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.</p> <p>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</p> <p>Supported platforms: FTD</p>
Security Policies	

Feature	Description
Usability enhancements for security policies	<p>Version 6.6.0 makes it easier to work with access control and prefilter rules. You can now:</p> <ul style="list-style-type: none"> • 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. <p>Supported platforms: FMC</p>
Object group search for access control policies	<p>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.</p> <p>With object group search enabled, the system does not expand network objects, but instead searches access rules for matches based on those group definitions.</p> <p>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.</p> <p>New/modified pages: Devices > Device Management > edit device > Device tab > Advanced Settings > Object Group Search option</p> <p>Supported platforms: FTD</p>
Time-based rules in access control and prefilter policies	<p>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.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Access control and prefilter rule editors • Devices > Platform Settings > add/edit Threat Defense policy > Time Zone • Objects > Object Management > Time Range and Time Zone <p>Supported platforms: FTD</p>

Feature	Description
Egress optimization re-enabled	<p>Upgrade impact.</p> <p>Version 6.6.0 fixes CSCvs86257. If egress optimization was:</p> <ul style="list-style-type: none"> • 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. <p>Supported platforms: FTD</p>
Event Logging and Analysis	
New datastore improves performance	<p>Upgrade impact.</p> <p>To improve performance, Version 6.6.0 uses a new datastore for connection and Security Intelligence events.</p> <p>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.</p> <p>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.</p> <p>You can monitor event migration progress in the Message Center.</p> <p>Supported platforms: FMC</p>
Wildcard support when searching connection and Security Intelligence events for URLs	<p>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.</p> <p>Supported platforms: FMC</p>

Feature	Description
Monitor up to 300,000 concurrent user sessions with FTD devices	<p>In Version 6.6.0, some FTD device models support monitoring of additional concurrent user sessions (logins):</p> <ul style="list-style-type: none"> • 300,000 sessions: Firepower 4140, 4145, 4150, 9300 • 150,000 sessions: Firepower 2140, 4112, 4115, 4120, 4125 <p>All other devices continue to support the old limit of 64,000, except ASA FirePOWER which is limited to 2000.</p> <p>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.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • 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 <p>Supported platforms: FTD devices listed above</p>
Integration with IBM QRadar	<p>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.</p> <p>For more information, see the Integration Guide for the Cisco Firepower App for IBM QRadar</p> <p>Supported platforms: FMC</p>
Administration and Troubleshooting	

Feature	Description
New options for deploying configuration changes	<p>The Deploy button on the FMC menu bar is now a menu, with options that add the following functionality:</p> <ul style="list-style-type: none"> • 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. <p>New/modified pages:</p> <ul style="list-style-type: none"> • Deploy > Deployment • Deploy > Deployment History <p>Supported platforms: FMC</p>
Initial configuration updates the VDB and schedules SRU updates	<p>On new and reimaged FMCs, the setup process now:</p> <ul style="list-style-type: none"> • Downloads and installs the latest vulnerability database (VDB) update. • Enables daily intrusion rule (SRU) downloads. Note that the setup process does <i>not</i> enable auto-deploy after these downloads, although you can change this setting. <p>Upgraded FMCs are not affected.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • System > Updates > Product Updates (VDB updates) • System > Updates > Rule Updates (SRU updates) <p>Supported platforms: FMC</p>
VDB match no longer required to restore FMC	<p>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.</p> <p>Supported platforms: FMC</p>

Feature	Description
HTTPS certificates with subject alternative name (SAN)	<p>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.</p> <p>New/modified pages: System > Configuration > HTTPS Certificate > Generate New CSR > Subject Alternative Name fields</p> <p>Supported platforms: FMC</p>
Real names associated with FMC user accounts	<p>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.</p> <p>New/modified pages: System > Users > Users > Real Name field.</p> <p>Supported platforms: FMC</p>
Cisco Support Diagnostics on additional FTD platforms	<p>Upgrade impact.</p> <p>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.</p> <p>Supported platforms: FMC, FTD</p>
Usability	
Light theme	<p>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.</p> <p>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.</p> <p>Supported platforms: FMC</p>
Display time remaining for upgrades	<p>The FMC's Message Center now displays approximately how much time remains until an upgrade will complete. This does not include reboot time.</p> <p>New/modified pages: Message Center</p> <p>Supported platforms: FMC</p>
Security and Hardening	

Feature	Description
Default HTTPS server certificate renewals have 800 day lifespans	<p>Upgrade impact.</p> <p>Unless the current <i>default</i> 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.</p> <p>Your old certificate was set to expire depending on when it was generated.</p> <p>Supported platforms: FMC</p>
Firepower Management Center REST API	
New REST API capabilities	<p>Added the following REST API services to support Version 6.6.0 features:</p> <ul style="list-style-type: none"> • 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 <p>Added the following REST API services to support older features:</p> <ul style="list-style-type: none"> • intrusionrules, intrusionpolicies: Intrusion policies <p>Supported platforms: FMC</p>

Feature	Description
Changed REST API service name for extended access lists	<p>Upgrade impact.</p> <p>The extendedaccesslist (singular) service in the FMC REST API is now extendedaccesslists (plural). Make sure you update your client. Using the old service name fails and returns an Invalid URL error.</p> <p>Request Type: GET</p> <p>URL to retrieve the extended access list associated with a specific ID:</p> <ul style="list-style-type: none"> • Old: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist/{objectId} • New: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslists/{objectId} <p>URL to retrieve a list of all extended access lists:</p> <ul style="list-style-type: none"> • Old: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist • New: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslists <p>Supported platforms: FMC</p>

Deprecated Features in FMC Version 6.6.0

Table 10:

Feature	Upgrade Impact	Description
Lower-memory instances for cloud-based FMCv deployments	Upgrade prohibited.	<p>For performance reasons, the following FMCv instances are no longer supported:</p> <ul style="list-style-type: none"> • c3.xlarge on AWS • c3.2xlarge on AWS • c4.xlarge on AWS • c4.2xlarge on AWS • Standard_D3_v2 on Azure <p>You must resize before you upgrade to Version 6.6.0+. For more information, see the Version 6.6.0 upgrade guidelines.</p> <p>Additionally, as of the Version 6.6.0 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.</p>

Feature	Upgrade Impact	Description
e1000 Interfaces on FTDv for VMware	Prevents upgrade.	Version 6.6.0 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 Firepower Threat Defense Virtual for VMware Getting Started Guide .
Less secure Diffie-Hellman groups, and encryption and hash algorithms	None, but you should switch now.	Version 6.6.0 deprecates the following Firepower Threat Defense security features: <ul style="list-style-type: none">• 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 6.7.0. Avoid configuring them in IKE proposals or IPSec policies for use in VPNs. Change to stronger options as soon as possible.
Custom tables for connection events	You should delete unsupported custom tables.	Version 6.6.0 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: <ul style="list-style-type: none">• Analysis > Advanced > Custom Tables > click Create Custom Table > Tables drop-down list > Connection Events and Security Intelligence Events
Ability to delete connection events from the event viewer	None.	Version 6.6.0 ends support for deleting connection and Security Intelligence events from the event viewer. To purge the database, select System > Tools > Data Purge . Deprecated options: <ul style="list-style-type: none">• Analysis > Connections > Events > Delete and Delete All• Analysis > Connections > Security Intelligence Events > Delete and Delete All

Version 6.5.0

New Features in FMC Version 6.5.0

Table 11:

Feature	Description
Hardware and Virtual Appliances	
FTD on the Firepower 1150	We introduced the Firepower 1150.
Larger instances for FTDv for Azure	Firepower Threat Defense Virtual on Microsoft Azure now supports larger instances: D4_v2 and D5_v2.
FMCv 300 for VMware	<p>We introduced the FMCv 300, a larger Firepower Management Center Virtual for VMware. It can manage up to 300 devices, compared to 25 devices for other FMCv instances.</p> <p>You can use the FMC model migration feature to switch to the FMCv 300 from a less powerful platform.</p>
VMware vSphere/VMware ESXi 6.7 support	You can now deploy FMCv, FTDv, and NGIPSv virtual appliances on VMware vSphere/VMware ESXi 6.7.
Firepower Threat Defense	
Firepower 1010 hardware switch support	<p>The Firepower 1010 now supports setting each Ethernet interface to be a switch port or a firewall interface.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Devices > Device Management > Interfaces • Devices > Device Management > Interfaces > Edit Physical Interface • Devices > Device Management > Interfaces > Add VLAN Interface <p>Supported platforms: Firepower 1010</p>
Firepower 1010 PoE+ support on Ethernet 1/7 and Ethernet 1/8	<p>The Firepower 1010 now supports Power over Ethernet+ (PoE+) on Ethernet 1/7 and Ethernet 1/8.</p> <p>New/modified pages: Devices > Device Management > Interfaces > Edit Physical Interface > PoE</p> <p>Supported platforms: Firepower 1010</p>

Feature	Description
Carrier-grade NAT enhancements	<p>For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time (see RFC 6888).</p> <p>New/modified pages: Devices > NAT > add/edit FTD NAT policy > add/edit NAT rule > PAT Pool tab > Block Allocation option</p> <p>Supported platforms: FTD</p>
TLS crypto acceleration for multiple container instances on Firepower 4100/9300	<p>TLS crypto acceleration is now supported on multiple container instances (up to 16) on a Firepower 4100/9300 chassis. Previously, you could enable TLS crypto acceleration for only <i>one</i> container instance per module/security engine.</p> <p>New instances have this feature enabled by default. However, the upgrade does <i>not</i> enable acceleration on existing instances. Instead, use the create hw-crypto and scope hw-crypto CLI commands. For more information, see the Cisco Firepower 4100/9300 FXOS Command Reference.</p> <p>New FXOS CLI commands:</p> <ul style="list-style-type: none"> • create hw-crypto • delete hw-crypto • scope hw-crypto • show hw-crypto <p>Removed FXOS CLI commands:</p> <ul style="list-style-type: none"> • show hwCrypto (replaced by show hw-crypto) • config hwCrypto <p>Removed FTD CLI commands:</p> <ul style="list-style-type: none"> • show crypto accelerator status <p>Supported platforms: Firepower 4100/9300</p>
Security Policies	
Access control rule filtering	<p>You can now filter access control rules based on search criteria.</p> <p>New/modified pages: Policies > Access Control > Access Control > add/edit policy > filter button ('show only rules matching filter criteria')</p> <p>Supported platforms: FMC</p>

Feature	Description
Dispute URL category or reputation	<p>You can now dispute the category or reputation of a URL.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Analysis > Connection Events > right-click a category or reputation > Dispute. • Analysis > Advanced > URL > search for URL > Dispute button • System > Integration > Cloud Services > Dispute link <p>Supported platforms: FMC</p>
User control with destination-based Security Group Tags (SGT)	<p>You can now use ISE SGT tags for both source and destination matching criteria in access control rules. SGT tags are tag-to-host/network mappings obtained by ISE.</p> <p>New connection event fields:</p> <ul style="list-style-type: none"> • Destination SGT (syslog: DestinationSecurityGroupTag): SGT attribute for the connection responder. <p>Renamed connection event fields:</p> <ul style="list-style-type: none"> • Source SGT (syslog: SourceSecurityGroupTag): SGT attribute for the connection initiator. Replaces Security Group Tag (syslog: SecurityGroup). <p>New/modified pages: System > Integration > Identity Sources > Identity Services Engine > Subscribe to Session Directory Topic and SXP Topic options</p> <p>Supported platforms: Any</p>
Cisco Firepower User Agent Version 2.5 integration	<p>We released Version 2.5 of the Cisco Firepower User Agent, which you can integrate with Firepower Versions 6.4.0 through 6.6.x.</p> <p>Note Version 6.6.0/6.6.x is the last release to support the Cisco Firepower User Agent software as an identity source. You cannot upgrade a Firepower Management Center with user agent configurations to Version 6.7.0+. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC). This will also allow you to take advantage of features that are not available with the user agent. To convert your license, contact your Cisco representative or partner contact.</p> <p>For more information, see the End-of-Life and End-of-Support for the Cisco Firepower User Agent announcement and the Firepower User Identity: Migrating from User Agent to Identity Services Engine TechNote.</p> <p>New/modified FMC CLI commands: configure user-agent</p> <p>Supported platforms: FMC</p>



Feature	Description
Event Logging and Analysis	
Threat Intelligence Director priorities.	<p>TID blocking/monitoring observable actions now have priority over blocking/monitoring with Security Intelligence Block lists.</p> <p>If you configure the Block TID observable action, even if the traffic also matches a Security Intelligence Block list set to Block:</p> <ul style="list-style-type: none"> • The Security Intelligence category in the connection event is a variant of <code>TID Block</code>. • The system generates a TID incident with an action taken of <code>Blocked</code>. <p>If you configure the Monitor TID observable action, even if the traffic also matches a Security Intelligence Block list set to Monitor:</p> <ul style="list-style-type: none"> • The Security Intelligence category in the connection event is a variant of <code>TID Monitor</code> • The system generates a TID incident with an action taken of <code>Monitored</code>. <p>Previously, in each of these cases, the system reported the category by analysis and did not generate a TID incident.</p> <p>Note The system still effectively handles traffic as before. Traffic that was blocked before is still blocked, and monitored traffic is still monitored. This simply changes which component gets the 'credit.' You may also see more TID incidents generated.</p> <p>For complete information on system behavior when you enable both Security Intelligence and TID, see the <i>TID-Firepower Management Center Action Prioritization</i> information in the Firepower Management Center Configuration Guide.</p> <p>Supported platforms: FMC</p>
'Packet profile' CLI commands	<p>You can now use the FTD CLI to obtain statistics on how the device handled network traffic. That is, how many packets were fastpathed by a prefilter policy, offloaded as a large flow, fully evaluated by access control (Snort), and so on.</p> <p>New FTD CLI commands:</p> <ul style="list-style-type: none"> • asp packet-profile • no asp packet-profile • show asp packet-profile • clear asp packet-profile <p>Supported platforms: FTD</p>

Feature	Description
Additional event types for Cisco SecureX threat response	<p>Firepower can now send file and malware events to Cisco SecureX threat response, as well as high priority connection events — those related to intrusion, file, malware, and Security Intelligence events.</p> <p>Note that the FMC web interface refers to this offering as <i>Cisco Threat Response (CTR)</i>.</p> <p>New/modified pages: System > Integration > Cloud Services.</p> <p>Supported platforms: FTD (via syslog or direct integration) and Classic (via syslog) devices</p>
Administration and Troubleshooting	
Precision Time Protocol (PTP) configuration for ISA 3000 devices.	<p>You can use FlexConfig 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.</p> <p>We now allow you to include the ptp (interface mode) command, and the global commands ptp mode e2transparent and ptp domain, in FlexConfig objects.</p> <p>New/modified commands: show ptp</p> <p>Supported platforms: ISA 3000 with FTD</p>
Configure more domains (multitenancy)	<p>When implementing multitenancy (segment user access to managed devices, configurations, and events), you can create up to 100 subdomains under a top-level Global domain, in two or three levels. The previous maximum was 50 domains.</p> <p>Supported platforms: FMC</p>
ISE Connection Status Monitor enhancements	<p>The ISE Connection Status Monitor health module now alerts you to issues with TrustSec SXP (SGT Exchange Protocol) subscription status.</p> <p>Supported platforms: FMC</p>
Regional clouds	<p>Upgrade impact.</p> <p>If you use the Cisco Threat Response integration, Cisco Support Diagnostics, or Cisco Success Network features, you can now select a regional cloud.</p> <p>By default, the upgrade assigns you to the US (North America) region.</p> <p>New/modified pages: System > Integration > Cloud Services</p> <p>Supported platforms: FMC, FTD</p>

Feature	Description
Cisco Support Diagnostics	<p>Upgrade impact.</p> <p><i>Cisco Support Diagnostics</i> (sometimes called <i>Cisco Proactive Support</i>) sends configuration and operational health data to Cisco, and processes that data through our automated problem detection system, allowing us to proactively notify you of issues. This feature also allows Cisco TAC to collect essential information from your devices during the course of a TAC case.</p> <p>During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time.</p> <p>In Version 6.5.0, Cisco Support Diagnostics support is limited to select platforms.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • System > Smart Licenses • System > Smart Licenses > Register <p>Supported platforms: FMC, Firepower 4100/9300, FTDv for Azure</p>
FMC model migration	<p>You can now use the backup and restore feature to migrate configurations and events between FMCs, even if they are not the same model. This makes it easier to replace FMCs due to technical or business reasons such as a growing organization, migration from a physical to a virtual implementation, hardware refresh, and so on.</p> <p>In general, you can migrate from a lower-end to a higher-end FMC, but not the reverse. Migration from KVM and Microsoft Azure is not supported. You must also unregister and reregister with Cisco Smart Software Manager (CSSM).</p> <p>For details, including supported target and destination models, see the Firepower Management Center Model Migration Guide.</p> <p>Supported platforms: FMC</p>
Security and Hardening	
Secure erase for appliance components on FXOS-based FTD devices	<p>You can now use the FXOS CLI to securely erase a specified appliance component.</p> <p>New FXOS CLI commands: erase secure</p> <p>Supported platforms: Firepower 1000/2000 and Firepower 4100/9300</p>

Feature	Description
Stricter password requirements for FMC <code>admin</code> accounts during initial setup	<p>FMC initial setup now requires that you choose a ‘strong’ password for <code>admin</code> accounts. The setup process applies this strong password to both the FMC web interface and CLI <code>admin</code> accounts.</p> <p>Note Upgrading to Version 6.5.0+ does not force you to change weak passwords to strong passwords. With the exception of LOM users on physical FMCs (and this does include the <code>admin</code> user), you are not prohibited from choosing a new weak password. However, we do recommend that all Firepower user accounts — especially those with Admin access — have strong passwords.</p> <p>Supported platforms: FMC</p>
Concurrent user session limits	<p>You can now limit the number of users that can be logged into the FMC at the same time. You can limit concurrent sessions for users with read only roles, read/write roles, or both. Note that CLI users are limited by the read/write setting.</p> <p>New/modified pages: System > Configuration > User Configuration > Max Concurrent Sessions Allowed options</p> <p>Supported platforms: FMC</p>
Authenticated NTP servers	<p>You can now configure secure communications between the FMC and NTP servers using SHA1 or MD5 symmetric key authentication. For system security, we recommend using this feature.</p> <p>New/modified pages: System > Configuration > Time Synchronization</p> <p>Supported platforms: FMC</p>
Usability and Performance	

Feature	Description
Improved initial configuration experience	<p>On new and reimaged FMCs, a wizard replaces the previous initial setup process. If you use the GUI wizard, when initial setup completes, the FMC displays the device management page so that you can immediately begin licensing and setting up your deployment.</p> <p>The setup process also automatically schedules the following:</p> <ul style="list-style-type: none"> • Software downloads. The system creates a weekly scheduled task to download (but not install) software patches and publicly available hotfixes that apply to your deployment. • FMC configuration-only backups. The system creates a weekly scheduled task to back up FMC configurations and store them locally. • GeoDB updates. The system enables weekly geolocation database updates. <p>These tasks are scheduled in UTC, which means that when they occur <i>locally</i> depends on the date and your specific location. Also, because tasks are scheduled in UTC, they do not adjust for Daylight Saving Time, summer time, or any such seasonal adjustments that you may observe in your location. If you are affected, scheduled tasks occur one hour "later" in the summer than in the winter, according to local time.</p> <p>Note We <i>strongly</i> recommend you review the auto-scheduled tasks/GeoDB updates and adjust them if necessary.</p> <p>Upgraded FMCs are not affected. For details on the initial configuration wizard, see the <i>Getting Started Guide</i> for your FMC model; for details on scheduled tasks, see the Firepower Management Center Configuration Guide.</p> <p>Supported platforms: FMC</p>
Light theme	<p>Beta.</p> <p>The FMC web interface defaults to the Classic theme, but you can also choose a new Light theme.</p> <p>Note The Light theme is a Beta feature. You may see misaligned text or other UI elements. In some cases, you may also experience slower-than-normal response times. If you encounter issues that prevent you from using a page or feature, switch back to the Classic theme. Although we cannot respond to everybody, we also welcome feedback — please use the feedback link on the User Preferences page or contact us at fmc-light-theme-feedback@cisco.com.</p> <p>New/modified pages: User Preferences, from the drop-down list under your username</p> <p>Supported platforms: FMC</p>

Feature	Description
Usability enhancements for viewing objects	<p>We have enhanced 'view object' capabilities for network, port, VLAN, and URL objects, as follows:</p> <ul style="list-style-type: none"> • In the access control policy and while configuring FTD routing, you can right-click an object and choose View Objects to display details about that object. • When you are viewing details about an object, or when you are browsing objects in the object manager, clicking Find Usage () now allows you to drill down into object groups and nested objects. <p>New/modified pages:</p> <ul style="list-style-type: none"> • Objects > Object Management > choose a supported object type > Find Usage () • Policies > Access Control > Access Control > create or edit policy > create or edit rule > choose a supported condition type > right-click an object > View Objects • Devices > Device Management > edit FTD device > Routing > right-click a supported object > View Objects <p>Supported platforms: FMC</p>
Usability enhancements for deploying configuration changes	<p>We streamlined the display of errors and warnings related to deploying configuration changes. Instead of an immediate verbose view, you can now Click to view all details to see more information about a particular error or warning.</p> <p>New/modified pages: Errors and Warnings for Requested Deployment dialog box</p> <p>Supported platforms: FMC</p>
Usability enhancements to FTD NAT policy management	<p>When configuring FTD NAT, you can now:</p> <ul style="list-style-type: none"> • View warnings and errors in your NAT policy, by device. Warnings and errors mark configurations that could adversely affect traffic flow or prevent the policy from deploying. • Display up to 1000 NAT rules per page. The default is 100. <p>New/modified pages: Devices > NAT > create or edit FTD NAT policy > Show Warnings and Rules Per Page options</p> <p>Supported platforms: FTD</p>
Firepower Management Center REST API	

Feature	Description
New REST API capabilities	<p>Added the following REST API objects to support Version 6.5.0 features:</p> <ul style="list-style-type: none"> • cloudregions: Regional clouds <p>Added the following REST API objects to support older features:</p> <ul style="list-style-type: none"> • categories: Categories for access control rules • domain, inheritancesettings: Domains and policy inheritance • prefilterpolicies, prefilterrules, tunneltags: Prefilter policies • vlaninterfaces: VLAN interfaces <p>Supported platforms: FMC</p>

New Features in FMC Version 6.5.0 Patches

Table 12:

Feature	Description
Version 6.5.0.5 Default HTTPS server certificates	<p>Upgrade impact.</p> <p>Unless the FMC's current <i>default</i> HTTPS server certificate already has an 800-day lifespan, upgrading to Version 6.5.0.5+ renews the certificate, which now expires 800 days from the date of the upgrade. All future renewals have an 800 day lifespan.</p> <p>Your old certificate was set to expire depending on when it was generated, as follows:</p> <ul style="list-style-type: none"> • 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

Deprecated Features in FMC Version 6.5.0

Table 13:

Feature	Upgrade Impact	Description
Ability to disable the Firepower Management Center CLI	None.	<p>Version 6.3.0 introduced the Firepower Management Center CLI, which you had to explicitly enable. In Version 6.5.0, the CLI is automatically enabled, for both new and upgraded deployments. If you want to access the Linux shell (also called <i>expert mode</i>), you must log in to the CLI and then use the expert command.</p> <p>Caution We recommend you do not access Firepower appliances using the shell, unless directed by Cisco TAC.</p> <p>Deprecated options: System > Configuration > Console Configuration > Enable CLI access check box</p>
MD5 authentication algorithm and DES encryption for SNMPv3 users (deprecated)	None, but you should switch now.	<p>Version 6.5.0 deprecates the MD5 authentication algorithm and DES encryption for SNMPv3 users on Firepower Threat Defense.</p> <p>Although these configurations continue to work post-upgrade, the system displays a warning when you deploy. And, you cannot create new users or edit existing users with these options.</p> <p>Support will be removed in a future release. If you are still using these options in your platform settings policy, we recommend you switch to stronger options now.</p> <p>New/modified screens: Devices > Platform Settings > SNMP > Users</p>
TLS 1.0 & 1.1	Client may fail to connect with an upgraded appliance.	<p>To enhance security:</p> <ul style="list-style-type: none"> • Captive portal (active authentication) has removed support for TLS 1.0. • Host input has removed support for TLS 1.0 and TLS 1.1. <p>If your client fails to connect with a Firepower appliance, we recommend you upgrade your client to support TLS 1.2.</p>

Feature	Upgrade Impact	Description
TLS crypto acceleration FXOS CLI commands for Firepower 4100/9300	None.	<p>As part of allowing TLS crypto acceleration for multiple container instances on Firepower 4100/9300, we removed the following FXOS CLI commands:</p> <ul style="list-style-type: none"> • show hwCrypto • config hwCrypto <p>And this FTD CLI command:</p> <ul style="list-style-type: none"> • show crypto accelerator status <p>For information on their replacements, see the new feature documentation.</p>
Cisco Security Packet Analyzer integration	None, but integration is no longer supported.	<p>Version 6.5.0 ends support for Firepower Management Center integration with Cisco Security Packet Analyzer.</p> <p>Deprecated screens/options:</p> <ul style="list-style-type: none"> • System > Integration > Packet Analyzer • Analysis > Advanced > Packet Analyzer Queries • Query Packet Analyzer when right-clicking on an event in the dashboard or event viewer
Default HTTPS server certificates	None.	<p>If you are upgrading from Version 6.4.0.9+, the <i>default</i> HTTPS server certificate's lifespan-on-renew returns to 3 years, but this is again updated to 800 days in Version 6.6.0+.</p> <p>Your current default HTTPS server certificate is set to expire depending on when it was generated, as follows:</p> <ul style="list-style-type: none"> • 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
Firepower Management Center models FMC 750, 1500, 3500	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower Management Center software on the FMC 750, FMC 1500, and FMC 3500. You cannot manage Version 6.5.0+ devices with these Firepower Management Centers.
ASA 5515-X and ASA 5585-X series devices with Firepower software	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower software (both Firepower Threat Defense and ASA FirePOWER) on ASA 5515-X and ASA 5585-X series devices (SSP-10, -20, -40, and -60).

Feature	Upgrade Impact	Description
Firepower 7000/8000 series devices	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower software on Firepower 7000/8000 series devices, including AMP models.

Version 6.4.0

New Features in FMC Version 6.4.0

Table 14:

Feature	Description
Hardware and Virtual Appliances	
FMC models FMC 1600, 2600, and 4600	We introduced the Firepower Management Center models FMC 1600, 2600, and 4600.
FMCv on Azure	We introduced Firepower Management Center Virtual 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	
FTDv for VMware defaults to vmxnet3 interfaces	<p>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.</p> <p>Note Version 6.6.0 ends support for e1000 interfaces. You will not be able to upgrade to Version 6.6.0+ 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 Firepower Threat Defense Virtual for VMware Getting Started Guide.</p> <p>Supported platforms: FTDv for VMware</p>

Feature	Description
Firepower Threat Defense: Routing	
Rotating (keychain) authentication for OSPFv2 routing	<p>You can now use rotating (keychain) authentication when configuring OSPFv2 routing.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • 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 <p>Supported platforms: FTD</p>
Firepower Threat Defense: Encryption and VPN	
RA VPN: Secondary authentication	<p>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.</p> <p>RA VPN supports secondary authentication for the AAA Only and Client Certificate and AAA authentication methods.</p> <p>New/modified pages: Devices > VPN > Remote Access > add/edit configuration > Connection Profile > AAA area</p> <p>Supported platforms: FTD</p>
Site-to-site VPN: Dynamic IP addresses for extranet endpoints	<p>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.</p> <p>New/modified pages: Devices > VPN > Site To Site > add/edit FTD VPN topology > Endpoints tab > add endpoint > IP Address option</p> <p>Supported platforms: FTD</p>
Site-to-site VPN: Dynamic crypto maps for point-to-point topologies	<p>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.</p> <p>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.</p> <p>New/modified pages: Devices > VPN > Site To Site > add/edit FTD VPN topology > IPsec tab > Crypto Map Type option</p> <p>Supported platforms: FTD</p>

Feature	Description
TLS crypto acceleration	<p>Upgrade impact.</p> <p>SSL hardware acceleration has been renamed <i>TLS crypto acceleration</i>. 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.</p> <p>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 <i>one</i> container instance per module/security engine. Acceleration is disabled for other container instances, but enabled for native instances.</p> <p>New FXOS CLI commands for the Firepower 4100/9300 chassis:</p> <ul style="list-style-type: none"> • show hwCrypto • config hwCrypto <p>New FTD CLI commands:</p> <ul style="list-style-type: none"> • show crypto accelerator status (replaces system support ssl-hw-status) <p>Removed FTD CLI commands:</p> <ul style="list-style-type: none"> • system support ssl-hw-accel • system support ssl-hw-status <p>Supported platforms: Firepower 2100 series, Firepower 4100/9300</p>
Event Logging and Analysis	
Improvements to syslog messages for file and malware events	<p>Fully qualified file and malware event data can now be sent from managed devices via syslog.</p> <p>New/modified pages: Policies > Access Control > Access Control > add/edit policy > Logging tab > File and Malware Settings area</p> <p>Supported platforms: Any</p>
Search intrusion events by CVE ID	<p>You can now search for intrusion events generated as a result of a particular CVE exploit.</p> <p>New/modified pages: Analysis > Search</p> <p>Supported platforms: FMC</p>
IntrusionPolicy field is now included in syslog	<p>Intrusion event syslog messages now specify the intrusion policy that triggered the event.</p> <p>Supported platforms: Any</p>

Feature	Description
Cisco SecureX threat response integration	<p>Cisco SecureX threat response is a Cisco Cloud offering that helps you rapidly detect, investigate, and respond to threats.</p> <p>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 <i>Cisco Threat Response (CTR)</i>.</p> <p>See the Cisco Firepower and SecureX Integration Guide.</p> <p>New/modified pages: System > Integration > Cloud Services</p> <p>Supported platforms: FTD</p>
Splunk integration	<p>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.</p> <p>See Cisco Firepower App for Splunk User Guide.</p> <p>Supported platforms: FMC</p>
Cisco Security Analytics and Logging (SaaS) integration	<p>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.</p> <p>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.</p> <p>See Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide.</p> <p>Supported platforms: FTD with FMC</p>
Administration and Troubleshooting	
New licensing capabilities for ISA 3000	<p>For ASA FirePOWER and FTD deployments, the ISA 3000 now supports URL Filtering and Malware licenses and their associated features.</p> <p>For FTD only, the ISA 3000 also now supports Specific License Reservation for approved customers.</p> <p>Supported platforms: ISA 3000</p>

Feature	Description
Scheduled remote backups of managed devices	<p>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.</p> <p>New/modified pages: System > Tools > Scheduling > add/edit task > choose Job Type: Backup > choose a Backup Type</p> <p>Supported platforms: FTD physical platforms, FTDv for VMware, Firepower 7000/8000 series</p> <p>Exceptions: No support for FTD clustered devices or container instances</p>
Ability to disable Duplicate Address Detection (DAD) on management interfaces	<p>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.</p> <p>New/modified pages: System > Configuration > Management Interfaces > Interfaces area > edit interface > IPv6 DAD check box</p> <p>Supported platforms: FMC, Firepower 7000/8000 series</p>
Ability to disable ICMPv6 Echo Reply and Destination Unreachable messages on management interfaces	<p>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.</p> <p>New/modified pages: System > Configuration > Management Interfaces > ICMPv6</p> <p>New/modified commands:</p> <ul style="list-style-type: none"> • configure network ipv6 destination-unreachable • configure network ipv6 echo-reply <p>Supported platforms: FMC (web interface only), managed devices (CLI only)</p>
Support for the Service-Type attribute for FTD users defined on the RADIUS server	<p>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.</p> <p>New/modified pages: System > Users > External Authentication tab > add/edit external authentication object > Shell Access Filter</p> <p>Supported platforms: FTD</p>

Feature	Description
View object use	<p>The object manager now allows you to see the policies, settings, and other objects where a network, port, VLAN, or URL object is used.</p> <p>New/modified pages: Objects > Object Management > choose object type > Find Usage (binoculars) icon</p> <p>Supported platforms: FMC</p>
Hit counts for access control and prefilter rules	<p>You can now access hit counts for access control and prefilter rules on your FTD devices.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Policies > Access Control > Access Control > add/edit policy > Analyze Hit Counts • Policies > Access Control > Prefilter > add/edit policy > Analyze Hit Counts <p>New commands:</p> <ul style="list-style-type: none"> • show rule hits • clear rule hits • cluster exec show rule hits • cluster exec clear rule hits • show cluster rule hits <p>Modified commands: show failover</p> <p>Supported platforms: FTD</p>
URL Filtering health monitor improvements	<p>You can now configure time thresholds for URL Filtering Monitor alerts.</p> <p>New/modified pages: System > Health > Policy > add/edit policy > URL Filtering Monitor</p> <p>Supported platforms: Any</p>
Connection-based troubleshooting	<p>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.</p> <p>New/modified commands:</p> <ul style="list-style-type: none"> • clear packet debugs • debug packet start • debug packet stop • show packet debugs <p>Supported platforms: FTD</p>

Feature	Description
New Cisco Success Network monitoring capabilities	<p>Added the following Cisco Success Network monitoring capabilities:</p> <ul style="list-style-type: none"> • CSPA (Cisco Security Packet Analyzer) query information • Contextual cross-launch instances enabled on the FMC • TLS/SSL inspection events • Snort restarts <p>Supported platforms: FMC</p>
Security and Hardening	
Signed SRU, VDB, and GeoDB updates	<p>So Firepower can verify that you are using the correct update files, Version 6.4.0+ uses <i>signed</i> 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 the Cisco Support & Download site—for example, in an air-gapped deployment—you should not notice any difference in functionality.</p> <p>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:</p> <ul style="list-style-type: none"> • 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 <p>Update files for Version 5.x through 6.3 still use the old naming scheme:</p> <ul style="list-style-type: none"> • 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 <p>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.</p> <p>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.</p> <p>Supported platforms: Any</p>

Feature	Description
SNMPv3 users can authenticate using a SHA-256 authorization algorithm	<p>SNMPv3 users can now authenticate using a SHA-256 algorithm.</p> <p>New/modified screen: Devices > Platform Settings > SNMP > Users > Auth Algorithm Type</p> <p>Supported platforms: Firepower Threat Defense</p>
2048-bit certificate keys now required (security enhancement)	<p>Upgrade impact.</p> <p>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.</p> <p>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.</p> <p>Supported platforms: FMC</p>
Usability and Performance	
Snort restart improvements	<p>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.</p> <p>Supported platforms: Firepower 4100/9300</p>
Performance improvement for selected IPS traffic	<p>Upgrade impact.</p> <p>Egress optimization is a performance feature targeted for selected IPS traffic. The feature is enabled by default on all FTD platforms.</p> <p>The Version 6.4.0 upgrade process enables egress optimization on eligible devices. For more information, see the Cisco Firepower Threat Defense Command Reference. To troubleshoot issues with egress optimization, contact Cisco TAC.</p> <p>Supported platforms: FTD</p> <p>New/modified commands:</p> <ul style="list-style-type: none"> • asp inspect-dp egress optimization • show asp inspect-dp egress optimization • clear asp inspect-dp egress optimization • show conn state egress_optimization

Feature	Description
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	
New REST API capabilities	Added REST API objects to support Version 6.4.0 features: <ul style="list-style-type: none"> • cloudeventsconfigs: Manage Cisco SecureX threat response 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

New Features in FMC Version 6.4.0 Patches

Table 15:

Feature	Description
Version 6.4.0.10 Upgrades postpone scheduled tasks	<p>Upgrade impact.</p> <p>Upgrades now postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot.</p> <p>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.</p> <p>Note that this feature is supported for Firepower appliances <i>running</i> Version 6.4.0.10 or any later patch. It is not supported for upgrades <i>to</i> Version 6.4.0.10, or upgrades that skip Version 6.4.0.10.</p> <p>This feature is also not supported in Version 6.5.0, 6.6.0, or 6.6.1. It is reintroduced in Version 6.6.3 and Version 6.7.0.</p>
Version 6.4.0.9 Default HTTPS server certificates	<p>Upgrade impact.</p> <p>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 <i>default</i> HTTPS server certificate, which expires 800 days from the date of the upgrade. All future renewals have an 800 day lifespan.</p> <p>Your old certificate was set to expire depending on when it was generated, as follows:</p> <ul style="list-style-type: none"> • 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 <p>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.</p>
Version 6.4.0.4 New syslog fields	<p>These new syslog fields collectively identify a unique connection event:</p> <ul style="list-style-type: none"> • Sensor UUID • First Packet Time • Connection Instance ID • Connection Counter <p>These fields also appear in syslogs for intrusion, file, and malware events, allowing connection events to be associated with those events.</p>

Feature	Description
Version 6.4.0.2 Detection of rule conflicts in FTD NAT policies	<p>Upgrade impact.</p> <p>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 <i>duplicate</i> or <i>overlapping</i> rules). This fixes an issue where conflicting NAT rules were applied out-of-order.</p> <p>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.</p> <p>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.</p>
Version 6.4.0.2 ISE Connection Status Monitor health module	<p>A new health module, the <i>ISE Connection Status Monitor</i>, monitors the status of the server connections between the Cisco Identity Services Engine (ISE) and the FMC.</p>

Deprecated Features in FMC Version 6.4.0

Table 16:

Feature	Upgrade Impact	Description			
SSL hardware acceleration FTD CLI commands	None.	<p>As part of the TLS crypto acceleration feature, we removed the following FTD CLI commands:</p> <ul style="list-style-type: none"> • system support ssl-hw-accel enable • system support ssl-hw-accel disable • system support ssl-hw-status <p>For information on their replacements, see the new feature documentation.</p>			
Web interface changes	None.	<p>These pages have changed location in Version 6.4.0.</p> <table> <tr> <td>System > Integration > Cloud Services</td> <td>is now</td> <td>System > Integration > Cisco CSI</td> </tr> </table>	System > Integration > Cloud Services	is now	System > Integration > Cisco CSI
System > Integration > Cloud Services	is now	System > Integration > Cisco CSI			

Deprecated Features in FMC Version 6.4.0 Patches

Table 17:

Feature	Upgrade Impact	Description
Version 6.4.0.7 Egress optimization	Patching turns off egress optimization processing.	<p>To mitigate CSCvq34340, patching a Firepower Threat Defense to Version 6.4.0.7+ turns off egress optimization processing. This happens regardless of whether the egress optimization feature is enabled or disabled.</p> <p>Note We recommend you upgrade to Version 6.6.0+, where this issue is fixed. That will turn egress optimization back on, if you left the feature 'enabled.'</p> <p>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.</p> <p>For more information, see the software advisory: FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature.</p>

Version 6.3.0

New Features in FMC Version 6.3.0

Table 18:

Feature	Description
Hardware	
FMC models FMC 1600, 2600, and 4600	We introduced the Firepower Management Center models FMC 1600, 2600, and 4600.
ISA 3000 with FirePOWER Services	<p>ISA 3000 with FirePOWER Services is supported in Version 6.3.0 (Protection license only).</p> <p>Although ISA 3000 with FirePOWER Services was also supported in Version 5.4.x, you cannot upgrade to Version 6.3.0. You must reimaged.</p>
Firepower Threat Defense: Device Management	
Hardware bypass support on the Firepower 2100 series for supported network modules	<p>Firepower 2100 series devices now support hardware bypass functionality when using the hardware bypass network modules.</p> <p>New/modified pages: Devices > Device Management > Interfaces > Edit Physical Interface</p> <p>Supported platforms: Firepower 2100 series</p>

Feature	Description
Support for data EtherChannels in On mode	<p>You can now set data and data-sharing EtherChannels to either Active LACP mode or to On mode. Other types of EtherChannels only support Active mode.</p> <p>New/modified Firepower Chassis Manager pages: Interfaces > All Interfaces > Edit Port Channel > Mode</p> <p>New/modified FXOS commands: set port-channel-mode</p> <p>Supported platforms: Firepower 4100/9300</p>
Firepower Threat Defense: HA and Clustering	

Feature	Description
Multi-instance capability for Firepower 4100/9300 with FTD	<p>You can now deploy multiple logical devices, each with a Firepower Threat Defense container instance, on a single security engine/module. Formerly, you could only deploy a single native application instance.</p> <p>To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances. Resource management lets you customize performance capabilities for each instance.</p> <p>You can use high availability using a container instance on 2 separate chassis. Clustering is not supported.</p> <p>Note Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode is not available for FTD.</p> <p>New/modified FMC pages: Devices > Device Management > edit device > Interfaces tab</p> <p>New/modified Firepower Chassis Manager pages:</p> <ul style="list-style-type: none"> • Overview > Devices • Interfaces > All Interfaces > Add New drop-down menu > Subinterface • Interfaces > All Interfaces > Type • Logical Devices > Add Device • Platform Settings > Mac Pool • Platform Settings > Resource Profiles <p>New/modified FXOS commands: connect ftdname, connect module telnet, create bootstrap-key PERMIT_EXPERT_MODE, create resource-profile, create subinterface, scope auto-macpool, set cpu-core-count, set deploy-type, set port-type data-sharing, set prefix, set resource-profile-name, set vlan, scope app-instance ftd name, show cgroups container, show interface, show mac-address, show subinterface, show tech-support module app-instance, show version</p> <p>Supported platforms: Firepower 4100/9300</p>

Feature	Description
Cluster control link customizable IP Address for the Firepower 4100/9300	<p>By default, the cluster control link uses the 127.2.0.0/16 network. You can now set the network when you deploy the cluster in FXOS. The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: 127.2.<i>chassis_id.slot_id</i>. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. Therefore, you can now set a custom /16 subnet for the cluster control link in FXOS except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses.</p> <p>New/modified Firepower Chassis Manager pages: Logical Devices > Add Device > Cluster Information</p> <p>New/modified options: CCL Subnet IP field</p> <p>New/modified FXOS commands: set cluster-control-link network</p> <p>Supported platforms: Firepower 4100/9300</p>
Improved FTD cluster addition to the FMC	<p>You can now add any unit of a cluster to the FMC, and the other cluster units are detected automatically. Formerly, you had to add each cluster unit as a separate device, and then group them into a cluster with the FMC. Adding a cluster unit is also now automatic. Note that you must delete a unit manually.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Devices > Device Management > Add drop-down menu > Device > Add Device dialog box • Devices > Device Management > Cluster tab > General area > Cluster Registration Status > Current Cluster Summary link > Cluster Status dialog box <p>Supported platforms: Firepower 4100/9300</p>
Firepower Threat Defense: Encryption and VPN	
SSL hardware acceleration	<p>Additional FTD devices now support SSL hardware acceleration. Also, this option is now enabled by default.</p> <p>Upgrading to Version 6.3.0 automatically enables SSL hardware acceleration on eligible devices. Using SSL hardware acceleration if you are not decrypting traffic can affect performance. We recommend you disable SSL hardware acceleration on devices that are not decrypting traffic.</p> <p>Supported platforms: Firepower 2100 series, Firepower 4100/9300</p>
RA VPN: RADIUS Dynamic Authorization or Change of Authorization (CoA)	<p>You can now use RADIUS servers for user authorization of RA VPN using dynamic access control lists (ACLs) or ACL names per user.</p> <p>Supported platforms: FTD</p>

Feature	Description
RA VPN: Two-Factor Authentication	<p>Firepower Threat Defense now supports two-factor authentication for RA VPN users using the Cisco AnyConnect Secure Mobility Client. For the two-factor authentication process, we support:</p> <ul style="list-style-type: none"> • First factor: any RADIUS or LDAP/AD server • Second factor: RSA tokens or DUO passcodes pushed to mobile <p>For more information on Duo multi-factor authentication (MFA) for FTD, see the Cisco Firepower Threat Defense (FTD) VPN with AnyConnect documentation on the Duo Security website.</p> <p>Supported platforms: FTD</p>
Security Policies	
Firepower Threat Defense service policy	<p>You can now configure a Firepower Threat Defense service policy as part of your access control policy advanced options. Use FTD service policies to apply services to specific traffic classes.</p> <p>Features supported include:</p> <ul style="list-style-type: none"> • TCP State Bypass • Randomizing TCP sequence numbers • Decrementing the time-to-live (TTL) value on packets • Dead Connection Detection • Setting a limit on the maximum number of connections and embryonic connections per traffic class and per client. • Timeouts for embryonic, half closed, and idle connections <p>Note Before Version 6.3.0, you could configure connection-related service rules using the TCP_Embryonic_Conn_Limit and TCP_Embryonic_Conn_Timeout predefined FlexConfig objects. You should remove those objects and redo your rules in the FTD service policy. If you created any custom FlexConfig objects to implement any of these connection-related features (that is, set connection commands), you should also remove those objects and implement the features through the FTD service policy. Failure to do so can cause deployment issues.</p> <p>The <i>Threat Defense Service Policies</i> chapter in the Firepower Management Center Configuration Guide has details on how service policies relate to FlexConfig and other features.</p> <p>New/modified pages: Policies > Access Control > edit/create policy > Advanced tab > Threat Defense Service Policy</p> <p>Supported platforms: FTD</p>

Feature	Description
Update interval for URL category and reputation data	<p>Upgrade impact.</p> <p>You can now force URL data to expire. There is a tradeoff between security and performance. A shorter interval means you use more current data, while a longer interval can make web browsing faster for your users.</p> <p>If you worked with Cisco TAC to specify a timeout value for the URL filtering cache, the upgrade may change that value. Otherwise, the setting defaults to disabled (the current behavior), meaning that cached URL data does not expire.</p> <p>New/modified pages: System > Integration > Cisco CSI > Cached URLs Expire setting</p> <p>Supported platforms: FMC</p>
Event Logging and Analysis	
Cisco Security Packet Analyzer Integration	<p>You can integrate with Cisco Security Packet Analyzer to examine events and display analysis results, or download results for further analysis.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • System > Integration > Packet Analyzer • Analysis > Advanced > Packet Analyzer Queries • Query Packet Analyzer when right-clicking on an event in the dashboard or event viewer <p>Supported platforms: FMC</p>
Contextual cross-launch	<p>You can right-click an event in the dashboard or event viewer to look up related information in predefined or custom, public or private URL-based resources.</p> <p>New/modified pages: Analysis > Advanced > Contextual Cross-Launch</p> <p>Supported platforms: FMC</p>

Feature	Description
Unified syslog configuration	<p>Upgrade impact.</p> <p>Version 6.3.0 changes and centralizes the way the system logs connection and intrusion events via syslog.</p> <p>Previously, you configured event logging via syslog in multiple places, depending on the event type. You now configure syslog messaging in the access control policy. These configurations affect connection and intrusion event logging for the access control, SSL, prefilter, and intrusion policies, as well as for Security Intelligence.</p> <p>The upgrade does not change your existing settings for connection event logging. However, you may suddenly start receiving intrusion events you did not "expect" via syslog. This is because the intrusion policy now sends syslog events to the destination specified in the access control policy. (Before, you could configure syslog alerting in an intrusion policy to send events to the syslog on the managed device itself rather than to an external host.)</p> <p>For FTD devices, some syslog platform settings now apply to connection and intrusion event messages. For a list, see the <i>Platform Settings for Firepower Threat Defense</i> chapter in the Firepower Management Center Configuration Guide.</p> <p>For NGIPS devices (7000/8000 series, ASA FirePOWER, NGIPSv), messages now use the ISO 8601 timestamp format as specified in RFC 5425.</p> <p>Supported platforms: Any</p>
Fully qualified syslog messages for connection and intrusion events	<p>The format of syslog messages for connection, security intelligence, and intrusion events have the following changes:</p> <ul style="list-style-type: none"> • Messages from FTD devices now include event type identification numbers. • Fields with empty or unknown values are no longer included, so messages are shorter and important data is less likely to be truncated. • Timestamps now use the ISO 8601 timestamp format as specified in the RFC 5425 syslog format (optional for FTD, required for Classic). <p>Supported platforms: Any</p>
Other syslog improvements for FTD devices	<p>You can send all syslog messages from the same interface (data or management), using the same IP address, using TCP or UDP protocol. Note that secure syslog is supported on data ports only. You can also use the RFC 5424 format for message timestamps.</p> <p>Supported platforms: FTD</p>
Administration and Troubleshooting	

Feature	Description
Export-controlled features for approved customers	<p>Customers whose Smart Accounts are not otherwise eligible to use restricted functionality can purchase term-based licenses, with approval.</p> <p>New/modified pages: System > Licenses > Smart Licenses</p> <p>Supported platforms: FMC, FTD</p>
Specific License Reservation for approved customers	<p>Customers can use Specific License Reservation to deploy Smart Licensing in an air-gapped network. The FMC reserves licenses from your virtual account for a specified duration without accessing the Cisco Smart Software Manager or Smart Software Satellite Server.</p> <p>New/modified pages: System > Licenses > Specific Licenses</p> <p>Supported platforms: FMC, FTD (except ISA 3000)</p>
IPv4 range, subnet, and IPv6 support for SNMP hosts	<p>You can now use IPv4 range, IPv4 subnet, and IPv6 host network objects to specify the SNMP hosts that can access a Firepower Threat Defense device.</p> <p>New/modified pages: Devices > Platform Settings > create or edit FTD policy > SNMP > Hosts tab</p> <p>Supported platforms: FTD</p>
Access control using fully qualified domain names (FQDN)	<p>You can now create fully qualified domain name (FQDN) network objects and use them in access control and prefilter rules. To use FQDN objects, you must also configure DNS server groups and DNS platform settings, so that the system can resolve the domain names.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> • Objects > Object Management > Network • Objects > Object Management > DNS Server Group • Devices > Platform Settings > create or edit FTD policy > DNS <p>Supported platforms: FTD</p>
CLI for the FMC	<p>An CLI for the FMC supports a small set of basic commands (change password, show version, reboot/restart, and so on). By default the FMC CLI is disabled, and logging into FMC using SSH accesses the Linux shell.</p> <p>New/modified Classic CLI commands: The system lockdown-sensor command has changed to system lockdown. This command now works for both devices and FMCs.</p> <p>New/modified pages: System > Configuration > Console Configuration > Enable CLI Access check box</p> <p>Supported platforms: FMC, including FMCv</p>

Feature	Description
Copy device configurations	<p>You can copy device configurations and policies from one device to another.</p> <p>New/modified pages: Devices > Device Management > edit the device > General area > Get/Push Device Configuration icons.</p> <p>Supported platforms: FMC</p>
Backup/restore FTD device configurations	<p>You can use the FMC web interface to back up configurations for some FTD devices.</p> <p>New/modified pages: System > Tools > Backup/Restore</p> <p>New/modified CLI commands: restore</p> <p>Supported platforms: All physical FTD devices, FTDv for VMware</p>
Skip deploying to up-to-date devices when you schedule deploy tasks	<p>Upgrade impact.</p> <p>When you schedule a task to deploy configuration changes, you can now opt to Skip Deployment for up-to-date devices. This performance-enhancing setting is enabled by default.</p> <p>The upgrade process automatically enables this option on existing scheduled tasks. To continue to force a scheduled deploy to up-to-date devices, you must edit the scheduled task.</p> <p>New/modified pages: System > Tools > Scheduling > add or edit a task > choose Job Type of Deploy Policies</p> <p>Supported platforms: FMC</p>
New health modules	<p>New health modules alert you when:</p> <ul style="list-style-type: none"> • Threat Data Updates on Devices: Threat identification data on managed devices fails to update. • Realm: A user is reported to the FMC without being downloaded, or a user logs into a domain that corresponds to a realm not known to the FMC. <p>New/modified pages:</p> <ul style="list-style-type: none"> • System > Health > Policy • System > Health > Monitor <p>Supported platforms: FMC</p>
Configurable packet capture size	<p>You can now store up to 10 GB of packet captures.</p> <p>New/modified CLI commands: file-size, show capture</p> <p>Supported platforms: Firepower 4100/9300</p>
Security and Hardening	

Feature	Description
HTTPS Certificates	<p>The default HTTPS server certificate provided with the system now expires in three years.</p> <p>If your appliance uses a default server certificate that was generated before you upgraded to Version 6.3.0, the server certificate will expire 20 years from when it was first generated. If you are using the default HTTPS server certificate the system now provides the ability to renew it.</p> <p>New/modified pages: System > Configuration > HTTPS Certificate > Renew HTTPS Certificate button</p> <p>New/modified Classic CLI commands: show http-cert-expire-date, system renew-http-cert<i>new_key</i></p> <p>Supported platforms: Physical FMCs, 7000/8000 series devices</p>
Improved login security	<p>Upgrade impact.</p> <p>Added FMC user configuration settings to improve login security:</p> <ul style="list-style-type: none"> • Track Successful Logins: Track the number of successful logins each FMC account has performed within a specific time period. • Password Reuse Limit: Track an FMC user's password history to prevent reuse. • Max Number of Login Failures and Set Time in Minutes to Temporarily Lockout Users: Limit the number of times in a row an FMC user can enter incorrect web interface login credentials before being temporarily blocked. <p>We also updated the list of supported ciphers and cryptographic algorithms for secure SSH access. If your SSH client fails to connect with a Firepower appliance due to a cipher error, update your client to the latest version.</p> <p>New/modified pages: System > Configuration > User Configuration</p> <p>Supported platforms: FMC</p>
Limit SSH login failures on devices	<p>When a user accesses any device via SSH and fails three successive login attempts, the device terminates the SSH session.</p> <p>Supported platforms: Any device</p>
Firepower Management Center REST API	

Feature	Description
New REST API services	<p>Added REST API services to support these features:</p> <ul style="list-style-type: none"> • Site-to-site VPN topology: <code>ftds2svpn</code>s, endpoints, ipsecsettings, advancedsettings, ikesettings, ikev1ipsecproposals, ikev1policies, ikev2ipsecproposals, ikev2policies • HA device failover: <code>failoverinterfacemacaddressconfigs</code>, <code>monitoredinterfaces</code> <p>Supported platforms: FMC</p>
Bulk overrides	You can now perform bulk overrides on specific objects. For a full list, see the Cisco Firepower Management Center REST API Quick Start Guide .

New Features in FMC Version 6.3.0 Patches

Table 19:

Feature	Description
Version 6.3.0.4 Detection of rule conflicts in FTD NAT policies	<p>Upgrade impact.</p> <p>After you upgrade to Version 6.3.0.4 or later patch, you can no longer create FTD NAT policies with conflicting rules (often referred to as <i>duplicate</i> or <i>overlapping</i> rules). This fixes an issue where conflicting NAT rules were applied out-of-order.</p> <p>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.</p> <p>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.</p> <p>Note that upgrading to Version 6.4.0 deprecates this fix. It is fixed again in Version 6.4.0.2.</p>
Version 6.3.0.4 ISE Connection Status Monitor module	<p>A new module, the <i>ISE Connection Status Monitor</i>, monitors the status of the server connections between the Cisco Identity Services Engine (ISE) and the FMC.</p> <p>Note that upgrading to Version 6.4.0 deprecates this module. Support returns in Version 6.4.0.2.</p> <p>New/modified screens: System > > Policy > create or edit policy > ISE Connection Status Monitor</p>

Feature	Description
Version 6.3.0.3 2048-bit certificate keys now required (security enhancement)	<p>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.</p> <p>If you cannot connect, regenerate the server certificate on your data source. If necessary, reconfigure the FMC connection to the data source.</p>
Version 6.3.0.1 EMS extension support	<p>Upgrade impact.</p> <p>Version 6.3.0.1 reintroduces EMS extension support, which was introduced in Version 6.2.3.8/6.2.3.9 but was not included in Version 6.3.0.</p> <p>Both the Decrypt-Resign and Decrypt-Known Key SSL policy actions again support the EMS extension during ClientHello negotiation, enabling more secure communications. The EMS extension is defined by RFC 7627.</p> <p>In FMC deployments, this feature depends on the <i>device</i> version. Although best practice is to upgrade your whole deployment, this feature is supported even if you patch only the device.</p>

Deprecated Features in FMC Version 6.3.0

Table 20:

Feature	Upgrade Impact	Description
EMS extension support for decryption	EMS extension support discontinued until you patch or upgrade.	<p>Version 6.3.0 discontinues EMS extension support, which was introduced in Version 6.2.3.8/6.2.3.9. This means that the Decrypt-Resign and Decrypt-Known Key SSL policy actions no longer support the EMS extension during ClientHello negotiation, which would enable more secure communications. The EMS extension is defined by RFC 7627.</p> <p>In Firepower Management Center deployments, this feature depends on the <i>device</i> version. Upgrading the Firepower Management Center to Version 6.3.0 does not discontinue support, as long as the device is running a supported version. However, upgrading the device to Version 6.3.0 does discontinue support.</p> <p>Support is reintroduced in Version 6.3.0.1.</p>
Decryption on passive and inline tap Interfaces	The system stops decrypting traffic in passive deployments.	Version 6.3.0 ends support for decrypting traffic on interfaces in passive or inline tap mode, even though the GUI allows you to configure it. Any inspection of encrypted traffic is necessarily limited.

Feature	Upgrade Impact	Description
Default DNS group FlexConfig objects	You should redo your configurations after upgrade.	<p>Version 6.3.0 deprecates this FlexConfig object for Firepower Threat Defense with FMC:</p> <ul style="list-style-type: none"> • Default_DNS_Configure <p>And these associated text objects:</p> <ul style="list-style-type: none"> • defaultDNSNameServerList • defaultDNSParameters <p>These allowed you to configure the Default DNS group, which defines the DNS servers that can be used when resolving fully qualified domain names on the data interfaces. This allowed you to use commands in the CLI, such as ping, using host names rather than IP addresses.</p> <p>You can now configure DNS for the data interfaces in the FTD platform settings policy: Devices > Platform Settings > create or edit FTD policy > DNS.</p>
Embryonic connection limit and timeout FlexConfig objects	<p>Post-upgrade deployment issues.</p> <p>You should redo your configurations after upgrade.</p>	<p>Version 6.3.0 deprecates these FlexConfig objects for Firepower Threat Defense with FMC:</p> <ul style="list-style-type: none"> • TCP_Embryonic_Conn_Limit • TCP_Embryonic_Conn_Timeout <p>And these associated text objects:</p> <ul style="list-style-type: none"> • tcp_conn_misc • tcp_conn_limit • tcp_conn_timeout <p>These allowed you to configure embryonic connection limits and timeouts to protect against SYN Flood Denial of Service (DoS) attacks.</p> <p>You can now configure these features in the FTD service policy: Policies > Access Control > add/edit policy > Advanced tab > Threat Defense Service Policy.</p> <p>Caution If you used set connection commands to implement connection-related service rules, you should remove the associated objects and implement the features through the FTD service policy. Failure to do so can cause deployment issues.</p>

Feature	Upgrade Impact	Description																					
Web interface changes	None.	<p>Version 6.3.0 changes these menu options:</p> <table> <tr> <td>Analysis > Advanced > Whois</td><td>is now</td><td>Analysis > Lookup > Whois</td></tr> <tr> <td>Analysis > Advanced > Geolocation</td><td>is now</td><td>Analysis > Lookup > Geolocation</td></tr> <tr> <td>Analysis > Advanced > URL</td><td>is now</td><td>Analysis > Lookup > URL</td></tr> <tr> <td>Analysis > Advanced > Custom Workflows</td><td>is now</td><td>Analysis > Custom > Custom Workflows</td></tr> <tr> <td>Analysis > Advanced > Custom Tables</td><td>is now</td><td>Analysis > Custom > Custom Tables</td></tr> <tr> <td>Analysis > Hosts > Vulnerabilities</td><td>is now</td><td>Analysis > Vulnerabilities > Vulnerabilities</td></tr> <tr> <td>Analysis > Hosts > Third-Party Vulnerabilities</td><td>is now</td><td>Analysis > Vulnerabilities > Third-Party Vulnerabilities</td></tr> </table>	Analysis > Advanced > Whois	is now	Analysis > Lookup > Whois	Analysis > Advanced > Geolocation	is now	Analysis > Lookup > Geolocation	Analysis > Advanced > URL	is now	Analysis > Lookup > URL	Analysis > Advanced > Custom Workflows	is now	Analysis > Custom > Custom Workflows	Analysis > Advanced > Custom Tables	is now	Analysis > Custom > Custom Tables	Analysis > Hosts > Vulnerabilities	is now	Analysis > Vulnerabilities > Vulnerabilities	Analysis > Hosts > Third-Party Vulnerabilities	is now	Analysis > Vulnerabilities > Third-Party Vulnerabilities
Analysis > Advanced > Whois	is now	Analysis > Lookup > Whois																					
Analysis > Advanced > Geolocation	is now	Analysis > Lookup > Geolocation																					
Analysis > Advanced > URL	is now	Analysis > Lookup > URL																					
Analysis > Advanced > Custom Workflows	is now	Analysis > Custom > Custom Workflows																					
Analysis > Advanced > Custom Tables	is now	Analysis > Custom > Custom Tables																					
Analysis > Hosts > Vulnerabilities	is now	Analysis > Vulnerabilities > Vulnerabilities																					
Analysis > Hosts > Third-Party Vulnerabilities	is now	Analysis > Vulnerabilities > Third-Party Vulnerabilities																					
VMware 5.5 hosting	Upgrade the hosting environment before you upgrade the Firepower software.	Version 6.3.0+ virtual deployments have not been tested on VMware vSphere/VMware ESXi 5.5. This includes FMCv, FTDv, and NGIPSv for VMware.																					
ASA 5506-X series and ASA 5512-X devices with Firepower software	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.3.0+ of the Firepower software (both Firepower Threat Defense and ASA FirePOWER) on ASA 5506-X, 5506H-X, 5506W-X, and 5512-X devices.																					

Version 6.2.3

New Features in FMC Version 6.2.3

Table 21:

Feature	Description
Hardware and Virtual Appliances	

Feature	Description
FTD on ISA 3000	<p>You can now run Firepower Threat Defense on the ISA 3000 series, using either the Firepower Device Manager or Firepower Management Center for management.</p> <p>Note that the ISA 3000 supports the Threat license only. It does not support the URL Filtering or Malware licenses. Thus, you cannot configure features that require the URL Filtering or Malware licenses on an ISA 3000. Special features for the ISA 3000 that were supported with the ASA, such as Hardware Bypass, Alarm ports, and so on, are not supported with Firepower Threat Defense in this release.</p>
Support for VMware ESXi 6.5	Firepower Threat Defense Virtual, Firepower Management Center Virtual, and Firepower NGIPS Virtual are now supported on VMware ESXi 6.5.
Firepower Threat Defense: Encryption and VPN	
SSL hardware acceleration for Firepower 4100/9300	<p>Firepower 4100/9300 with FTD now support SSL encryption and decryption acceleration in hardware, greatly improving performance. SSL hardware acceleration is disabled by default for all appliances that support it.</p> <p>Note This feature is renamed <i>TLS crypto acceleration</i> in Version 6.4.0+.</p> <p>Supported platforms: Firepower 4100/9300</p>
Certificate enrollment improvements	<p>Non-blocking work flow for certificate enrollment operation allows certificate enrollment on multiple Firepower Threat Defense devices in parallel:</p> <ul style="list-style-type: none"> • The administrator can now choose to have the Remote Access VPN Policy wizard enroll certificates for all devices in the policy by checking Enroll the selected certificate object on the target devices check box in the Access & Certificate step. If this is chosen, only deployment needs to be done after the wizard finishes. This is selected by default. • Administrators no longer have to initiate Remote Access VPN certificate enrollment on devices one at a time. The enrollment process for each device is now independent and can be done in parallel. • In the event of a PKS12 certificate enrollment failure, the administrator no longer needs to re-upload the PKS12 file again to retry enrollment, since it is now stored in the certificate enrollment object. <p>Supported platforms: FTD</p>
Firepower Threat Defense: High Availability and Clustering	

Feature	Description
Automatically rejoin the Firepower Threat Defense cluster after an internal failure	<p>Formerly, many internal error conditions caused a cluster unit to be removed from the cluster, and you were required to manually rejoin the cluster after resolving the issue. Now, a unit will attempt to rejoin the cluster automatically at the following intervals: 5 minutes, 10 minutes, and then 20 minutes. Internal failures include: application sync timeout; inconsistent application statuses; and so on.</p> <p>New/modified command: show cluster info auto-join</p> <p>Supported platforms: Firepower 4100/9300</p>
Firepower Threat Defense High Availability Hardening	<p>Version 6.2.3 introduces the following features for Firepower Threat Defense devices in high availability:</p> <ul style="list-style-type: none"> • Whenever active or standby Firepower Threat Defense devices in a high availability pair restart, the Firepower Management Center may not display accurate high availability status for either managed device. However, the status may not upgrade on the Firepower Management Center because the communication between the Firepower Threat Defense and the Firepower Management Center is not established yet. The Refresh Node Status option on the Devices > Device Management page allows you to refresh the high availability node status to obtain accurate information about the active and standby device in a high availability pair. • The Devices > Device Management page of the Firepower Management Center UI has a new Switch Active Peer icon. • Version 6.2.3 includes a new REST API object, Device High Availability Pair Services, that contains four functions: <ul style="list-style-type: none"> • DELETE ftddevicehapairs • PUT ftddevicehapairs • POST ftddevicehapairs • GET ftddevicehapairs
Administration and Troubleshooting	
Firepower Management Center High Availability Messaging	<p>The Firepower Management Center high availability pairs have improved UI messaging. The UI now displays interim status messages while Firepower Management Center pairs are being established and rephrased UI messaging to be more intuitive.</p> <p>Supported platforms: FMC</p>

Feature	Description
External Authentication added for Firepower Threat Defense SSH Access	<p>You can now configure external authentication for SSH access to the Firepower Threat Defense using LDAP or RADIUS.</p> <p>New/modified screen: Devices > Platform Settings > External Authentication</p> <p>Supported platforms: FTD</p>
Enhanced Vulnerability Database (VDB) Installation	<p>The Firepower Management Center now warns you before you install a VDB that installing restarts the Snort process, interrupting traffic inspection and, depending on how the managed device handles traffic, possibly interrupting traffic flow. You can cancel the install until a more convenient time, such as during a maintenance window.</p> <p>These warnings can appear:</p> <ul style="list-style-type: none"> • After you download and manually install a VDB. • When you create a scheduled task to install the VDB. • When the VDB installs in the background, such as during a previously scheduled task or as part of a Firepower software upgrade. <p>Supported platforms: FMC</p>
Upgrade Package Push	<p>You can now copy (or push) an upgrade package from the Firepower Management Center to a managed device before you run the actual upgrade. This is useful because you can push during times of low bandwidth use, outside of the upgrade maintenance window.</p> <p>When you push to high availability, clustered, or stacked devices, the system sends the upgrade package to the active/control/primary first, then to the standby/data/secondary.</p> <p>New/modified screens: System > Updates</p> <p>Supported platforms: FMC</p>
Firepower Threat Defense serviceability	<p>Version 6.2.3 improves the show fail over CLI command. The new keyword, -history, details to help troubleshooting.</p> <ul style="list-style-type: none"> • Show fail over history displays failure reason along with its specific details. • Show fail over history details displays fail over history from the peer unit. <p>Note This command includes fail over state changes and the reason for the state change for the peer unit.</p> <p>Supported platforms: FTD</p>

Feature	Description
Device list sorting	<p>On the Devices > Devices Management page, you can use the View by drop-down list to sort and view the device list by any of the following categories: group, license, model, or access control policy. In a multidomain deployment, you can also sort and view by domain, which is the default display category in that deployment. Devices must belong to a leaf domain.</p> <p>Supported platforms: FMC</p>
Audit log improvements	<p>The audit log now denotes if a policy changed on the Firepower Threat Defense Platform Settings Devices > Platform Settings page.</p> <p>Supported platforms: FMC with FTD</p>
Updated FTD CLI commands	<p>The asa_mgmt_plane and asa_dataplane options for Firepower Threat Defense device CLI commands are renamed to management-plane and data-plane respectively.</p> <p>Supported platforms: FTD</p>
Cisco Success Network	<p>Upgrade impact.</p> <p><i>Cisco Success Network</i> sends usage information and statistics to Cisco, which are essential to provide you with technical support.</p> <p>During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time.</p> <p>Supported platforms: FMC</p>
Web Analytics Tracking	<p>Upgrade impact.</p> <p><i>Web analytics tracking</i> sends non-personally-identifiable usage data to Cisco, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your FMCs.</p> <p>Initial setup enrolls you in web analytics tracking by default, but you can change your enrollment at any time after that. Upgrades can also enroll or re-enroll you in web analytics tracking.</p> <p>Supported platforms: FMC</p>
Performance	
Snort restarts reduced for FTD devices	<p>In Version 6.2.3, fewer FTD configuration changes restart the Snort process on FTD devices.</p> <p>The FMC now warns you before you deploy if the configuration deployment restarts the Snort process, interrupting traffic inspection and, depending on how the managed device handles traffic, possibly interrupting traffic flow.</p> <p>Supported platforms: FTD</p>

Feature	Description
Traffic Drop on Policy Apply	<p>Version 6.2.3 adds the configure snort preserve-connection {enable disable} command to the Firepower Threat Defense CLI. This command determines whether to preserve existing connections on routed and transparent interfaces if the Snort process goes down. When disabled, all new or existing connections are dropped when Snort goes down and remain dropped until Snort resume. When enabled, connections that were already allowed remain established, but new connections cannot be established until Snort is again available.</p> <p>Note that you cannot permanently disable this command on a Firepower Threat Defense device managed by Firepower Device Manager; existing connections may drop when the settings revert to default during the next configuration deployment.</p>
Increased memory capacity for lower-end appliances	Versions 6.1.0.7, 6.2.0.5, 6.2.2.2, and 6.2.3 increase the memory capacity for lower-end Firepower appliances. This reduces the number of health alerts.
Faster ISE pxGrid discovery	If an ISE pxGrid deployed in high availability fails or becomes unreachable, the Firepower Management Center now discovers the new active pxGrid faster.
FMC REST API	
Firepower Management Center REST API Improvements	<p>The new Firepower Management Center REST APIs support the use of CRUD (create, retrieve, upgrade, and delete) operations for NAT rules, static routing configuration, and corresponding objects while migrating from ASA FirePOWER to Firepower Threat Defense.</p> <p>Newly introduced APIs for NAT:</p> <ul style="list-style-type: none"> • NAT rules • Firepower Threat Defense NAT policies • Auto NAT rules • Manual NAT rules <p>When deploying Firepower Threat Defense devices in Cisco ACI, APIs enable APIC controller to add proper static routes in place, along with other configuration settings that are needed for a particular service graph. It also enables PBR service graph insertion, which is currently the most flexible way of inserting Firepower Threat Defense in ACI.</p> <p>Newly introduced APIs for Static Route:</p> <ul style="list-style-type: none"> • IPv4 static routes • IPv6 static routes • SLA monitors

New Features in FMC Version 6.2.3 Patches

Table 22:

Feature	Description
Version 6.2.3.13 Detection of rule conflicts in FTD NAT policies	<p>After you upgrade to Version 6.2.3.13+, you can no longer create FTD NAT policies with conflicting rules (often referred to as <i>duplicate</i> or <i>overlapping</i> rules). This fixes an issue where conflicting NAT rules were applied out-of-order.</p> <p>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.</p> <p>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.</p> <p>Note Upgrading to Version 6.3.0 or 6.4.0 deprecates this fix. The issue is addressed in Version 6.3.0.4 and 6.4.0.2.</p> <p>Supported platforms: Firepower Threat Defense</p>
Version 6.2.3.8 EMS extension support	<p>Both the Decrypt-Resign and Decrypt-Known Key SSL policy actions now support the EMS extension during ClientHello negotiation, enabling more secure communications. The EMS extension is defined by RFC 7627.</p> <p>Note Version 6.2.3.8 was removed from the Cisco Support & Download site on 2019-01-07. Upgrading to Version 6.2.3.9 also enables EMS extension support. Version 6.3.0 discontinues EMS extension support. In FMC deployments, this feature depends on the device version. Upgrading the FMC to Version 6.3.0 does not discontinue support, but upgrading the device does. Support is reintroduced in Version 6.3.0.1.</p> <p>Supported platforms: Any</p>
Version 6.2.3.7 TLS v1.3 downgrade CLI command for FTD	<p>A new CLI command allows you to specify when to downgrade TLS v1.3 connections to TLS v1.2.</p> <p>Many browsers use TLS v1.3 by default. If you are using an SSL policy to handle encrypted traffic, and people in your monitored network use browsers with TLS v1.3 enabled, websites that support TLS v1.3 fail to load.</p> <p>For more information, see the system support commands in the Cisco Firepower Threat Defense Command Reference. We recommend you use these commands only after consulting with Cisco TAC.</p> <p>Supported platforms: Firepower Threat Defense</p>
Version 6.2.3.3 Site-to-site VPN with clustering	<p>You can now configure site-to-site VPN with clustering. Site-to-site VPN is a centralized feature; only the control unit supports VPN connections.</p> <p>Supported platforms: Firepower 4100/9300</p>

Deprecated Features in FMC Version 6.2.3

Table 23:

Feature	Upgrade Impact	Description
New result limits in reports	Upgrade can change settings in reports.	<p>Version 6.2.3 limits the number of results you can use or include in a report section. For table and detail views, you can include fewer records in a PDF report than in an HTML/CSV report.</p> <p>For HTML/CSV report sections, the new limits are:</p> <ul style="list-style-type: none"> • Bar and pie charts: 100 (top or bottom) • Table views: 400,000 • Detail views: 1,000 <p>For PDF report sections, the new limits are:</p> <ul style="list-style-type: none"> • Bar and pie charts: 100 (top or bottom) • Table views: 100,000 • Detail views: 500 <p>If, before you upgrade the Firepower Management Center, a section in a report template specifies a larger number of results than the HTML/CSV maximum, the upgrade process lowers the setting to the new maximum value.</p> <p>For report templates that generate PDF reports, if you exceed the PDF limit in any template section, the upgrade process changes the output format to HTML. To continue generating PDFs, lower the results limit to the PDF maximum. If you do this after the upgrade, set the output format back to PDF.</p>
Expired CA certificates for dynamic analysis with AMP for Networks	None, but you should patch or upgrade.	<p>On June 15, 2018, some AMP for Networks deployments stopped being able to submit files for dynamic analysis. See Expired CA Certificates for Dynamic Analysis, on page 121.</p>

Deprecated Features in FMC Version 6.2.3 Patches

Table 24:

Feature	Upgrade Impact	Description
<p>Versions 6.2.3.1–6.2.3.3</p> <p>Expired CA certificates for dynamic analysis</p>	None, but you should patch.	<p>On June 15, 2018, some AMP for Networks deployments stopped being able to submit files for dynamic analysis. See Expired CA Certificates for Dynamic Analysis, on page 121.</p>

Date-Based Features

Expired CA Certificates for Dynamic Analysis

Deployments: AMP for Networks (malware detection) deployments where you submit files for dynamic analysis

Affected Versions: Version 6.0+

Resolves: [CSCvj07038](#)

On June 15, 2018, some Firepower deployments stopped being able to submit files for dynamic analysis. This occurred due to an expired CA certificate that was required for communications with the AMP Threat Grid cloud. Version 6.3.0 is the first major version with the new certificate.



Note

If you do not want to upgrade to Version 6.3.0+, you must patch or hotfix to obtain the new certificate and reenale dynamic analysis. However, subsequently upgrading a patched or hotfixed deployment to either Version 6.2.0 or Version 6.2.3 reverts to the old certificate and you must patch or hotfix again.

If this is your first time installing the patch or hotfix, make sure your firewall allows outbound connections to `fmc.api.threatgrid.com` (replacing `panacea.threatgrid.com`) from both the FMC and its managed devices. Managed devices submit files to the cloud for dynamic analysis; the FMC queries for results.

This table lists the versions with the old certificates, as well as the patches and hotfixes that contain the new certificates, for each major version sequence and platform. Patches and hotfixes are available on the Cisco Support & Download site.

Table 25: Patches and Hotfixes with New CA Certificates

Versions with Old Cert	First Patch with New Cert	Hotfix with New Cert	
6.2.3 through 6.2.3.3	6.2.3.4	Hotfix G	FTD devices
		Hotfix H	FMC, NGIPS devices
6.2.2 through 6.2.2.3	6.2.2.4	Hotfix BN	All platforms
6.2.1	None. You must upgrade.	None. You must upgrade.	
6.2.0 through 6.2.0.5	6.2.0.6	Hotfix BX	FTD devices
		Hotfix BW	FMC, NGIPS devices
6.1.0 through 6.1.0.6	6.1.0.7	Hotfix EM	All platforms
6.0.x	None. You must upgrade.	None. You must upgrade.	

Release Dates

Table 26: Version 7.1.0 Dates

Version	Build	Date	Platforms
7.1.0	90	2021-12-01	All

Table 27: Version 7.0.0/7.0.x Dates

Version	Build	Date	Platforms
7.0.1	84	2021-10-07	All
7.0.0	94	2021-05-26	All

Table 28: Version 7.0.0/7.0.x Patch Dates

Version	Build	Date	Platforms
7.0.0.1	15	2021-07-15	All

Table 29: Version 6.7.0 Dates

Version	Build	Date	Platforms
6.7.0	65	2020-11-02	All

Table 30: Version 6.7.0 Patch Dates

Version	Build	Date	Platforms
6.7.0.2	24	2021-05-11	All
6.7.0.1	13	2021-03-24	All

Table 31: Version 6.6.0/6.6.x Dates

Version	Build	Date	Platforms
6.6.5	81	2021-08-03	All
6.6.4	64	2021-04-29	Firepower 1000 series
	59	2021-04-26	FMC/FMCv All devices except Firepower 1000 series
6.6.3	80	2020-03-11	All

Version	Build	Date	Platforms
6.6.1	91	2020-09-20	All
	90	2020-09-08	—
6.6.0	90	2020-05-08	Firepower 4112
		2020-04-06	FMC/FMCv All devices except Firepower 4112

Table 32: Version 6.6.0/6.6.x Patch Dates

Version	Build	Date	Platforms
6.6.5.1	15	2021-12-06	All
6.6.0.1	7	2020-07-22	All

Table 33: Version 6.5.0 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.5.0	123	2020-02-03	FMC/FMCv	FMC/FMCv
6.5.0	120	2019-10-08	—	—
6.5.0	115	2019-09-26	All devices	All devices

Table 34: Version 6.5.0 Patch Dates

Version	Build	Date	Platforms
6.5.0.5	95	2021-02-09	All
6.5.0.4	57	2020-03-02	All
6.5.0.3	30	2020-02-03	No longer available.
6.5.0.2	57	2019-12-19	All
6.5.0.1	35	2019-11-20	No longer available.

Table 35: Version 6.4.0 Dates

Version	Build	Date	Platforms
6.4.0	113	2020-03-03	FMC/FMCv

Version	Build	Date	Platforms
6.4.0	102	2019-06-20	Firepower 4115, 4125, 4145 Firepower 9300 with SM-40, SM-48, and SM-56 modules
		2019-06-13	Firepower 1010, 1120, 1140
		2019-04-24	Firepower 2110, 2120, 2130, 2140 Firepower 4110, 4120, 4140, 4150 Firepower 9300 with SM-24, SM-36, and SM-44 modules ASA 5508-X, 5515-X, 5516-X, 5525-X, 5545-X, 5555-X ASA 5585-X-SSP-10, -20, -40, -60 ISA 3000 FTDv Firepower 7000/8000 series NGIPSv

Table 36: Version 6.4.0 Patch Dates

Version	Build	Date	Platforms
6.4.0.13	57	2021-12-02	All
6.4.0.12	112	2021-05-12	All
6.4.0.11	11	2021-01-11	All
6.4.0.10	95	2020-10-21	All
6.4.0.9	62	2020-05-26	All
6.4.0.8	28	2020-01-29	All
6.4.0.7	53	2019-12-19	All
6.4.0.6	28	2019-10-16	No longer available.
6.4.0.5	23	2019-09-18	All
6.4.0.4	34	2019-08-21	All
6.4.0.3	29	2019-07-17	All

Version	Build	Date	Platforms
6.4.0.2	35	2019-07-03	FMC/FMCv FTD/FTDv, except Firepower 1000 series
	34	2019-06-27	—
		2019-06-26	Firepower 7000/8000 series ASA FirePOWER NGIPSv
6.4.0.1	17	2019-06-27	FMC 1600, 2600, 4600
		2019-06-20	Firepower 4115, 4125, 4145 Firepower 9300 with SM-40, SM-48, and SM-56 modules
		2019-05-15	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv Firepower 2110, 2120, 2130, 2140 Firepower 4110, 4120, 4140, 4150 Firepower 9300 with SM-24, SM-36, and SM-44 modules ASA 5508-X, 5515-X, 5516-X, 5525-X, 5545-X, 5555-X ASA 5585-X-SSP-10, -20, -40, -60 ISA 3000 FTDv Firepower 7000/8000 series NGIPSv

Table 37: Version 6.3.0 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.3.0	85	2019-01-22	Firepower 4100/9300	Firepower 4100/9300
6.3.0	84	2018-12-18	FMC/FMCv ASA FirePOWER	—
6.3.0	83	2019-06-27	—	FMC 1600, 2600, 4600
		2018-12-03	All FTD devices except Firepower 4100/9300 Firepower 7000/8000 NGIPSv	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices except Firepower 4100/9300

Table 38: Version 6.3.0 Patch Dates

Version	Build	Date	Platforms
6.3.0.5	35	2019-11-18	Firepower 7000/8000 series NGIPSv
	34	2019-11-18	FMC/FMCv All FTD devices ASA FirePOWER
6.3.0.4	44	2019-08-14	All
6.3.0.3	77	2019-06-27	FMC 1600, 2600, 4600
		2019-05-01	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices
6.3.0.2	67	2019-06-27	FMC 1600, 2600, 4600
		2019-03-20	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices
6.3.0.1	85	2019-06-27	FMC 1600, 2600, 4600
		2019-02-18	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices

Table 39: Version 6.2.3 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.2.3	113	2020-06-01	FMC/FMCv	FMC/FMCv
6.2.3	111	2019-11-25	—	FTDv: AWS, Azure
6.2.3	110	2019-06-14	—	—
6.2.3	99	2018-09-07	—	—
6.2.3	96	2018-07-26	—	—
6.2.3	92	2018-07-05	—	—
6.2.3	88	2018-06-11	—	—
6.2.3	85	2018-04-09	—	—

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.2.3	84	2018-04-09	Firepower 7000/8000 series NGIPSv	—
6.2.3	83	2018-04-02	FTD/FTDv ASA FirePOWER	FTD: Physical platforms FTDv: VMware, KVM Firepower 7000/8000 ASA FirePOWER NGIPSv
6.2.3	79	2018-03-29	—	—

Table 40: Version 6.2.3 Patch Dates

Version	Build	Date	Platforms
6.2.3.17	30	2021-06-21	All
6.2.3.16	59	2020-07-13	All
6.2.3.15	39	2020-02-05	FTD/FTDv
	38	2019-09-18	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
6.2.3.14	41	2019-07-03	All
	36	2019-06-12	All
6.2.3.13	53	2019-05-16	All
6.2.3.12	80	2019-04-17	All
6.2.3.11	55	2019-03-17	All
	53	2019-03-13	—
6.2.3.10	59	2019-02-07	All
6.2.3.9	54	2019-01-10	All
6.2.3.8	51	2019-01-02	No longer available.
6.2.3.7	51	2018-11-15	All
6.2.3.6	37	2018-10-10	All

Version	Build	Date	Platforms
6.2.3.5	53	2018-11-06	FTD/FTDv
	52	2018-12-09	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
6.2.3.4	42	2018-08-13	All
6.2.3.3	76	2018-07-11	All
6.2.3.2	46	2018-06-27	All
	42	2018-06-06	—
6.2.3.1	47	2018-06-28	All
	45	2018-06-21	—
	43	2018-05-02	—

Table 41: Version 6.2.2 Dates

Version	Build	Date	Platforms
6.2.2	81	2017-09-05	All

Table 42: Version 6.2.2 Patch Dates

Version	Build	Date	Platforms
6.2.2.5	57	2018-11-27	All
6.2.2.4	43	2018-09-21	FTD/FTDv
	34	2018-07-09	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
	32	2018-06-15	—
6.2.2.3	69	2018-06-19	All
	66	2018-04-24	—
6.2.2.2	109	2018-02-28	All

Version	Build	Date	Platforms
6.2.2.1	80	2017-12-05	Firepower 2100 series
	78	2017-11-20	—
	73	2017-11-06	FMC/FMCv All devices except Firepower 2100 series

