

Features

This document describes the new and deprecated features for Version 6.2.3.

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

Upgrade Impact

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

Snort

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



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

Intrusion Rules and Keywords

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

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

FlexConfig

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

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

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

- FMC Features in Version 6.2.3, on page 2
- FDM Features in Version 6.2.3, on page 10

FMC Features in Version 6.2.3

Table 1: FMC Features in Version 6.2.3 Patches

Feature	Details
Version 6.2.3.13 Detection of rule conflicts in FTD NAT policies	After you upgrade to Version 6.2.3.13+, you can no longer create FTD NAT policies with conflicting rules (often referred to as *duplicate* or *overlapping* rules). This fixes an issue where conflicting NAT rules were applied out-of-order. If you currently have conflicting NAT rules, you will be able to deploy post-upgrade. However, your NAT rules will continue to be applied out-of-order. Therefore, we recommend that after the upgrade, you inspect your FTD NAT policies by editing (no changes are needed) then attempting to resave. If you have rule conflicts, the system will prevent you from saving. Correct the issues, save, and then deploy. **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. Supported platforms: FTD
Version 6.2.3.8 EMS extension support	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. **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. Supported platforms: Any

Feature	Details
Version 6.2.3.7 TLS v1.3 downgrade CLI command for FTD	A new CLI command allows you to specify when to downgrade TLS v1.3 connections to TLS v1.2. 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. For more information, see the **system support** commands in the Cisco Secure Firewall Threat Defense Command Reference. We recommend you use these commands only after consulting with Cisco TAC. Supported platforms: FTD
Version 6.2.3.3 Site-to-site VPN with clustering	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. Supported platforms: Firepower 4100/9300

Table 2: FMC Features in Version 6.2.3

Feature	Details
Platform	
FTD on the ISA 3000.	You can now run FTD on the ISA 3000 series. 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 FTD in this release.
Support for VMware ESXi 6.5.	You can now deploy FMCv, FTDv, and NGIPSv virtual appliances on VMware vSphere/VMware ESXi 6.5.
Firepower Threat Defense: Encryption and VPN	
SSL hardware acceleration for Firepower 4100/9300	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. **Note** This feature is renamed *TLS crypto acceleration* in Version 6.4.0+. Supported platforms: Firepower 4100/9300

Feature	Details
Certificate enrollment improvements	Non-blocking work flow for certificate enrollment operation allows certificate enrollment on multiple FTD devices in parallel: • 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. Supported platforms: FTD
Firepower Threat Defense: High Availability and Clustering	
Automatically rejoin the FTD cluster after an internal failure	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. New/modified command: **show cluster info auto-join** Supported platforms: Firepower 4100/9300

FTD High Availability Hardening	Version 6.2.3 introduces the following features for FTD devices in high availability:
	• Whenever active or standby FTD devices in a high availability pair restart, the FMC may not display accurate high availability status for either managed device. However, the status may not upgrade on the FMC because the communication between the device and the FMC 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 FMC 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:
	  • **DELETE ftddevicehapairs**
	  • **PUT ftddevicehapairs**
	  • **POST ftddevicehapairs**
	  • **GET ftddevicehapairs**

Administration and Troubleshooting	

Feature	Details
FMC High Availability Messaging	FMC high availability pairs have improved UI messaging. The UI now displays interim status messages while FMC pairs are being established and rephrased UI messaging to be more intuitive. Supported platforms: FMC
External Authentication added for FTD SSH Access	You can now configure external authentication for SSH access to FTD devices using LDAP or RADIUS. New/modified screen: **Devices** > **Platform Settings** > **External Authentication** Supported platforms: FTD
Enhanced Vulnerability Database (VDB) Installation	The FMC 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. These warnings can appear: • 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. Supported platforms: FMC
Upgrade Package Push	You can now copy (or push) an upgrade package from the FMC 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. 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. New/modified screens: **System** > **Updates** Supported platforms: FMC
FTD serviceability	Version 6.2.3 improves the **show fail over** CLI command. The new keyword, **-history**, details to help troubleshooting. • **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. **Note** This command includes fail over state changes and the reason for the state change for the peer unit. Supported platforms: FTD

Feature	Details
Device list sorting	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. Supported platforms: FMC
Audit log improvements	The audit log now denotes if a policy changed on the FTD Platform Settings **Devices** > **Platform Settings** page. Supported platforms: FMC with FTD
Updated FTD CLI commands	The **asa_mgmt_plane** and **asa_dataplane** options for FTD device CLI commands are renamed to **management-plane** and **data-plane** respectively. Supported platforms: FTD
Cisco Success Network	**Upgrade impact.** Cisco Success Network sends usage information and statistics to Cisco, which are essential to provide you with technical support. During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time. For more information, see Sharing Data with Cisco. Supported platforms: FMC
Web Analytics Tracking	**Upgrade impact.** Web analytics provides 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. 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. For more information, see Sharing Data with Cisco. Supported platforms: FMC
Performance	
Snort restarts reduced for FTD devices	In Version 6.2.3, fewer FTD configuration changes restart the Snort process on FTD devices. 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. Supported platforms: FTD

Feature	Details
Traffic Drop on Policy Apply	Version 6.2.3 adds the **configure snort preserve-connection {enable | disable}** command to the FTD 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. Note that you cannot permanently disable this command on a FTD device managed by FDM; existing connections may drop when the settings revert to default during the next configuration deployment.
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 FMC now discovers the new active pxGrid faster.
New result limits in reports.	**Upgrade can change report settings.** 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. For HTML/CSV report sections, the new limits are: • Bar and pie charts: 100 (top or bottom) • Table views: 400,000 • Detail views: 1,000 For PDF report sections, the new limits are: • Bar and pie charts: 100 (top or bottom) • Table views: 100,000 • Detail views: 500 If, before you upgrade the FMC, 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. 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.
Firepower Management Center REST API	

Feature	Details
FMC REST API Improvements	The new FMC 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 FTD. Newly introduced APIs for NAT: • NAT rules • FTD NAT policies • Auto NAT rules • Manual NAT rules When deploying FTD 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 FTD in ACI. Newly introduced APIs for Static Route: • IPv4 static routes • IPv6 static routes • SLA monitors
Deprecated Features	

Feature	Details
Expired CA certificates for dynamic analysis with AMP for Networks.	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 is the first major version with the new certificate. If you do not want to upgrade to Version 6.3+, you can patch to obtain the new certificate and reenable dynamic analysis, as follows: • Version 6.2.3 → patch to Version 6.2.3.4 • Version 6.2.2 → patch to Version 6.2.2.4 • Version 6.2.1 → no patches available • Version 6.2 → patch to Version 6.2.0.6 • Version 6.1 → patch to Version 6.1.0.7 • Version 6.0 → no patches available You can also apply a hotfix. For available hotfixes, see the Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes. Find the hotfix for your version and platform that applies to CSCvj07038*: Firepower devices need to trust Threat Grid certificate*. 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. Note that 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.
Deprecated: Geolocation details.	In May 2022 we split the GeoDB into two packages: a country code package that maps IP addresses to countries/continents, and an IP package that contains additional contextual data associated with routable IP addresses. The contextual data in the IP package can include additional location details, as well as connection information such as ISP, connection type, proxy type, domain name, and so on. The new country code package has the same file name as the old all-in-one package: Cisco_GEODB_Update-*date-build*. This allows deployments running Version 7.1 and earlier to continue to obtain GeoDB updates. If you manually download GeoDB updates—for example, in an air-gapped deployment—make sure you get the country code package and not the IP package. **Important** This split does not affect geolocation rules or traffic handling in any way—those rules rely only on the data in the country code package. However, because the country code package essentially replaces the all-in-one package, the contextual data is no longer updated and will grow stale. To obtain fresh data, upgrade or reimage the FMC to Version 7.2+ and update the GeoDB.

FDM Features in Version 6.2.3

Table 3: FDM Features in Version 6.2.3

Feature	Description
SSL/TLS decryption.	You can decrypt SSL/TLS connections so that you can inspect the contents of the connection. Without decryption, encrypted connections cannot be effectively inspected to identify intrusion and malware threats, or to enforce compliance with your URL and application usage polices. We added the **Policies** > **SSL Decryption** page and **Monitoring** > **SSL Decryption** dashboard. **Attention** Identity policies that implement active authentication automatically generate SSL decryption rules. If you upgrade from a release that does not support SSL decryption, the SSL decryption policy is automatically enabled if you have this type of rule. However, you must specify the certificate to use for Decrypt-Resign rules after completing the upgrade. Please edit the SSL decryption settings immediately after upgrade.
Security Intelligence blocking.	From the new **Policies** > **Security Intelligence** page you can configure a Security Intelligence policy, which you can use to drop unwanted traffic based on source/destination IP address or destination URL. Any allowed connections will still be evaluated by access control policies and might eventually be dropped. You must enable the Threat license to use Security Intelligence. We also renamed the **Policies** dashboard to **Access And SI Rules**, and the dashboard now includes Security Intelligence rule-equivalents as well as access rules.
Intrusion rule tuning.	You can change the action for intrusion rules within the pre-defined intrusion policies you apply with your access control rules. You can configure each rule to drop or generate events (alert) matching traffic, or disable the rule. You can change the action for enabled rules only (those set to drop or alert); you cannot enable a rule that is disabled by default. To tune intrusion rules, choose **Policies** > **Intrusion**.
Automatic network analysis policy (NAP) assignment based on intrusion policy.	In previous releases, the Balanced Security and Connectivity network analysis policy was always used for preprocessor settings, regardless of the intrusion policy assigned to a specific source/destination security zone and network object combination. Now, the system automatically generates NAP rules to assign the same-named NAP and intrusion policies to traffic based on those criteria. Note that if you use Layer 4 or 7 criteria to assign different intrusion policies to traffic that otherwise matches the same source/destination security zone and network object, you will not get perfectly matching NAP and intrusion policies. You cannot create custom network analysis policies.
Drill-down reports for the Threats, Attackers, and Targets dashboards.	You can now click into the Threats, Attackers, and Targets dashboards to view more detail about the reported items. These dashboards are available on the Monitoring page. Because of these new reports, you will lose reporting data for these dashboards when upgrading from a pre-6.2.3 release.
Web Applications dashboard.	The new Web Applications dashboard shows the top web applications, such as Google, that are being used in the network. This dashboard augments the Applications dashboard, which provides protocol-oriented information, such as HTTP usage.

Feature	Description
New Zones dashboard replaces the Ingress Zone and Egress Zone dashboards.	The new Zones dashboard shows the top security zone pairs for traffic entering and then exiting the device. This dashboard replaces the separate dashboards for Ingress and Egress zones.
New Malware dashboard.	The new Malware dashboard shows the top Malware action and disposition combinations. You can drill down to see information on the associated file types. You must configure file policies on access rules to see this information.
Self-signed internal certificates, and Internal CA certificates.	You can now generate self-signed internal identity certificates. You can also upload or generate self-signed internal CA certificates for use with SSL decryption policies. Configure these features on the **Objects** > **Certificates** page.
Ability to edit DHCP server settings when editing interface properties.	You can now edit settings for a DHCP server configured on an interface at the same time you edit the interface properties. This makes it easy to redefine the DHCP address pool if you need to change the interface IP address to a different subnet.
The Cisco Success Network sends usage and statistics data to Cisco to improve the product and provide effective technical support.	You can connect to the Cisco Success Network to send data to Cisco. By enabling Cisco Success Network, you are providing usage information and statistics to Cisco which are essential for Cisco to provide you with technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. You can enable the connection when you register the device with the Cisco Smart Software Manager, or later at your choice. You can disable the connection at any time. Cisco Success Network is a cloud service. The **Device** > **System Settings** > **Cloud Management** page is renamed **Cloud Services**. You can configure Cisco Defense Orchestrator from the same page.
FTDv for Kernel-based Virtual Machine (KVM) hypervisor device configuration.	You can configure Firepower Threat Defense on FTDv for KVM devices using FDM. Previously, only VMware was supported. **Note** You must install a new 6.2.3 image to get FDM support. You cannot upgrade an existing virtual machine from an older version and then switch to FDM.
Support for VMware ESXi 6.5.	You can now deploy FTDv on VMware vSphere/VMware ESXi 6.5.
ISA 3000 (Cisco 3000 Series Industrial Security Appliances) device configuration.	You can configure Firepower Threat Defense on ISA 3000 devices using FDM. 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.
Optional deployment on update of the rules database or VDB.	When you update the intrusion rules database or VDB, or configure an update schedule, you can prevent the immediate deployment of the update. Because the update restarts the inspection engines, there is a momentary traffic drop during the deployment. By not deploying automatically, you can choose to initiate the deployment at a time when traffic drops will be least disruptive. **Note** A VDB download can also restart Snort all by itself, and then again cause a restart on deployment. You cannot stop the restart on download.

Feature	Description
Improved messages that indicate whether a deployment restarts Snort. Also, a reduced need to restart Snort on deployment.	Before you start a deployment, FDM indicates whether the configuration updates require a Snort restart. Snort restarts result in the momentary dropping of traffic. Thus, you now know whether a deployment will not impact traffic and can be done immediately, or will impact traffic, so that you can deploy at a less disruptive time. In addition, in prior releases, Snort restarted on every deployment. Now, Snort restarts for the following reasons only: • you enable or disable SSL decryption policies • an updated rules database or VDB was downloaded • you changed the MTU on one or more physical interface (but not subinterface)
CLI console in FDM.	You can now open a CLI Console from FDM. The CLI Console mimics an SSH or console session, but allows a subset of commands only: **show**, **ping**, **traceroute**, and **packet-tracer**. Use the CLI Console for troubleshooting and device monitoring.
Support for blocking access to the management address.	You can now remove all management access list entries for a protocol to prevent access to the management IP address. Previously, if you removed all entries, the system defaulted to allowing access from all client IP addresses. On upgrade to 6.2.3, if you previously had an empty management access list for a protocol (HTTPS or SSH), the system creates the default allow rule for all IP addresses. You can then delete these rules as needed. In addition, FDM will recognize changes you make to the management access list from the CLI, including if you disable SSH or HTTPS access. Ensure that you enable HTTPS access for at least one interface, or you will not be able to configure and manage the device.
EMS extension support.	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. **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. Support is reintroduced in Version 6.3.0.1. Minimum FTD: Version 6.2.3.8
TLS v1.3 downgrade CLI command for FTD.	A new CLI command allows you to specify when to downgrade TLS v1.3 connections to TLS v1.2. 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. For more information, see the **system support** commands in the Cisco Secure Firewall Threat Defense Command Reference. We recommend you use these commands only after consulting with Cisco TAC. Minimum FTD: Version 6.2.3.7

Feature	Description
Smart CLI and FlexConfig for configuring features using the device CLI.	Smart CLI and FlexConfig allows you to configure features that are not yet directly supported through FDM policies and settings. FTD uses ASA configuration commands to implement some features. If you are a knowledgeable and expert user of ASA configuration commands, you can configure these features on the device using the following methods: • Smart CLI—(Preferred method.) A Smart CLI template is a pre-defined template for a particular feature. All of the commands needed for the feature are provided, and you simply need to select values for variables. The system validates your selection, so that you are more likely to configure a feature correctly. If a Smart CLI template exists for the feature you want, you must use this method. In this release, you can configure OSPFv2 using the Smart CLI. • FlexConfig—The FlexConfig policy is a collection of FlexConfig objects. The FlexConfig objects are more free-form than Smart CLI templates, and the system does no CLI, variable, or data validation. You must know ASA configuration commands and follow the ASA configuration guides to create a valid sequence of commands. **Caution** Cisco strongly recommends using Smart CLI and FlexConfig only if you are an advanced user with a strong ASA background and at your own risk. You may configure any commands that are not blacklisted. Enabling features through Smart CLI or FlexConfig may cause unintended results with other configured features.
FTD REST API, and an API Explorer.	You can use a REST API to programmatically interact with a Firepower Threat Defense device that you are managing locally through FDM. There is an API Explorer that you can use to view object models and test the various calls you can make from a client program. To open the API Explorer, log into FDM, and then change the path on the URL to /#/api-explorer, for example, https://ftd.example.com/#/api-explorer.