Features and Functionality

Patches contain new features, functionality, and behavior changes related to urgent or resolved issues.

Features for Firepower Management Center Deployments

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.

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.

New Features in FMC Version 6.2.3 Patches

Table 1:

Feature	Description
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: Firepower Threat Defense
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
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 Firepower Threat Defense Command Reference. We recommend you use these commands only after consulting with Cisco TAC. Supported platforms: Firepower Threat Defense
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

Deprecated Features in FMC Version 6.2.3 Patches

Table 2:

Feature	Upgrade Impact	Description
Versions 6.2.3.1–6.2.3.3 Expired CA certificates for dynamic analysis	None, but you should patch.	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.

Features for Firepower Device Manager Deployments

New Features in FDM Version 6.2.3 Patches

Table 3:

Feature	Description
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. Support is reintroduced in Version 6.3.0.1.
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 Firepower Threat Defense Command Reference. We recommend you use these commands only after consulting with Cisco TAC.

Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

Intrusion rule updates (SRUs) provide 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.

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.

Supported keywords depend on your Snort version:

- FMC: Choose Help > About.
- FTD with FDM: Use the show summary CLI command.
- ASA FirePOWER with ASDM: Choose ASA FirePOWER Configuration > System Information.

You can also find your Snort version in the Bundled Components section of the Cisco Firepower Compatibility Guide.

The Snort release notes contain details on new keywords. You can read the release notes on the Snort download page: https://www.snort.org/downloads.

Sharing Data with Cisco

Web Analytics tracking

In Version 6.2.3+, Web analytics tracking 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.

You are enrolled in web analytics tracking by default (by accepting the Version 6.5.0+ EULA you consent to web analytics tracking), but you can change your enrollment at any time after you complete initial setup.

Note Upgrades to Version 6.2.3 through 6.6.x can enroll you in web analytics tracking. This can occur even if you purposely unenrolled. If you do not want Cisco to collect this data, unenroll after upgrading.

Cisco Success Network

In Version 6.2.3+, 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.

Cisco Support Diagnostics

In Version 6.5.0+, Cisco Support Diagnostics (sometimes called Cisco Proactive Support) 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.

During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time.

Note This feature is supported on Firepower Management Centers and their managed Firepower Threat Defense devices. In Version 6.5.0 only, FTD support is restricted to the Firepower 4100/9300 with FTD and FTDv for Azure. This feature is not supported with Firepower Device Manager.