



Features and Functionality

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

- [Features for Firepower Management Center Deployments, on page 1](#)
- [Features for Firepower Device Manager Deployments, on page 1](#)
- [Intrusion Rules and Keywords, on page 1](#)
- [How-To Walkthroughs for the FMC, on page 2](#)
- [Sharing Data with Cisco, on page 3](#)

Features for Firepower Management Center Deployments

There are no new or deprecated features for Firepower Management Center deployments in Version 6.7.x patches.

Features for Firepower Device Manager Deployments

There are no new or deprecated features for Firepower Device Manager deployments in Version 6.7.x patches.

Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

Intrusion rule updates (SRUs/LSPs) 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/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.

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>.

How-To Walkthroughs for the FMC

FMC walkthroughs (also called how-tos) guide you through a variety of basic tasks such as device setup and policy configuration. Just click How To at the bottom of the browser window, choose a walkthrough, and follow the step-by-step instructions.



Note FMC walkthroughs are tested on the Firefox and Chrome browsers. If you encounter issues with a different browser, we ask that you switch to Firefox or Chrome. If you continue to encounter issues, contact Cisco TAC.

The following table lists some common problems and solutions. To end a walkthrough at any time, click the x in the upper right corner.

Table 1: Troubleshooting Walkthroughs

Problem	Solution
Cannot find the How To link to start walkthroughs.	Make sure walkthroughs are enabled. From the drop-down list under your username, select User Preferences then click How-To Settings. Version 6.7.0 discontinues walkthroughs for the Classic theme. You can switch themes in your user preferences.
Walkthrough appears when you do not expect it.	If a walkthrough appears when you do not expect it, end the walkthrough.
Walkthrough disappears or quits suddenly.	If a walkthrough disappears: <ul style="list-style-type: none"> • Move your pointer. Sometimes the FMC stops displaying an in-progress walkthrough. For example, pointing to a different top-level menu can make this happen. • Navigate to a different page and try again. If moving your pointer does not work, the walkthrough may have quit.

Problem	Solution
<p>Walkthrough is out of sync with the FMC:</p> <ul style="list-style-type: none"> • Starts on the wrong step. • Advances prematurely. • Will not advance. 	<p>If a walkthrough is out of sync, you can:</p> <ul style="list-style-type: none"> • Attempt to continue. <p>For example, if you enter an invalid value in a field and the FMC displays an error, the walkthrough can prematurely move on. You may need to go back and resolve the error to complete the task.</p> <ul style="list-style-type: none"> • End the walkthrough, navigate to a different page, and try again. <p>Sometimes you cannot continue. For example, if you do not click Next after you complete a step, you may need to end the walkthrough.</p>

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.
