



Features and Functionality

Major releases provide new features, functionality, and enhancements to the Firepower software. Major versions can include deprecated features and platforms, menu and terminology changes, changed behavior, and so on.

Because deprecated features are the most likely to cause upgrade issues when skipping versions, the release notes provide historical information for deprecated features. For historical information on new features, read the release notes for the versions you are skipping.

- [New Features in Firepower Management Center/Version 6.2.3, on page 1](#)
- [New Features in Firepower Device Manager/FTD Version 6.2.3, on page 6](#)
- [Deprecated Features, on page 10](#)
- [Deprecated FlexConfig Commands, on page 13](#)
- [Intrusion Rules and Keywords, on page 14](#)
- [Sharing Data with Cisco, on page 14](#)

New Features in Firepower Management Center/Version 6.2.3

The following table lists the new features available in Firepower Version 6.2.3 when configured using a Firepower Management Center.

Feature	Description
Hardware and Virtual Hardware	
FTD on ISA 3000	You can now run Firepower Threat Defense on the ISA 3000 series, using either the Firepower Device Manager or Firepower Management Center for management. 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.
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.

Feature	Description
Firepower Threat Defense: Encryption and VPN	
SSL Hardware Acceleration	<p>Certain Firepower managed device models 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>Supported Platforms: Firepower 4100/9300</p>
Firepower Threat Defense VPN Improvement	<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.
Firepower Threat Defense: High Availability and Clustering	
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>
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>

Feature	Description
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	
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.

Feature	Description
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/master/primary first, then to the standby/slave/secondary.</p> <p>New/Modified screens: System > Updates</p>
Firepower Threat Defense erviceability	<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>
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>
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>
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>
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 upgrade, you are asked to accept or decline participation. You can also opt in or out at any time.</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>Upgrading to Version 6.2.3 enables web analytics tracking. If you do not want Cisco to collect this data, you can opt out after the upgrade.</p>

Feature	Description
Performance	
Policy Deploy Restart Improvements	<p>As an enhancement in Version 6.2.3, the configurations that restart the Snort process have been reduced. For Firepower Threat Defense devices, the managing UI 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>Note that restart behavior is different for devices managed using the Firepower Device Manager. See the New Features in Firepower Device Manager/FTD Version 6.2.3, on page 6 for more information.</p>
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	<p>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.</p>
Faster ISE pxgrid discovery	<p>If an ISE pxgrid deployed in high availability fails or becomes unreachable, the Firepower Management Center now discovers the new active pxgrid faster.</p>
FMC REST API	

Feature	Description
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 Firepower Device Manager/FTD Version 6.2.3

Released: March 29, 2018

The following table lists the new features available in FTD 6.2.3 when configured using Firepower Device Manager.

Feature	Description
SSL/TLS Decryption	<p>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 policies. We added the Policies > SSL Decryption page and Monitoring > SSL Decryption dashboard.</p> <p>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.</p>

Feature	Description
Security Intelligence Blacklisting	<p>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.</p> <p>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.</p>
Intrusion Rule Tuning	<p>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.</p>
Automatic Network Analysis Policy (NAP) Assignment based on Intrusion Policy	<p>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.</p>
Drill-down reports for the Threats, Attackers, and Targets dashboards	<p>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.</p> <p>Because of these new reports, you will lose reporting data for these dashboards when upgrading from a pre-6.2.3 release.</p>
Web Applications Dashboard	<p>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.</p>
New Zones dashboard replaces the Ingress Zone and Egress Zone dashboards.	<p>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.</p>
New Malware Dashboard	<p>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.</p>
Self-signed internal certificates, and Internal CA certificates	<p>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.</p>

Feature	Description
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	<p>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.</p> <p>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.</p>
Firepower Threat Defense Virtual for Kernel-based Virtual Machine (KVM) hypervisor device configuration	<p>You can configure FTD on Firepower Threat Defense Virtual for KVM devices using Firepower Device Manager. Previously, only VMware was supported.</p> <p>Note You must install a new 6.2.3 image to get Firepower Device Manager support. You cannot upgrade an existing virtual machine from an older version and then switch to Firepower Device Manager.</p>
ISA 3000 (Cisco 3000 Series Industrial Security Appliances) device configuration	You can configure FTD on ISA 3000 devices using Firepower Device Manager. 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	<p>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.</p> <p>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.</p>

Feature	Description
Improved messages that indicate whether a deployment restarts Snort. Also, a reduced need to restart Snort on deployment	<p>Before you start a deployment, Firepower Device Manager 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.</p> <p>In addition, in prior releases, Snort restarted on every deployment. Now, Snort restarts for the following reasons only:</p> <ul style="list-style-type: none"> • 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 Firepower Device Manager	<p>You can now open a CLI Console from Firepower Device Manager. The CLI Console mimics an SSH or console session, but allows a subset of commands only: show, ping, tracert, and packet-tracer. Use the CLI Console for troubleshooting and device monitoring.</p>
Support for blocking access to the management address	<p>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.</p> <p>In addition, Firepower Device Manager will recognize changes you make to the management access list from the CLI, including if you disable SSH or HTTPS access.</p> <p>Ensure that you enable HTTPS access for at least one interface, or you will not be able to configure and manage the device.</p>

Feature	Description
Smart CLI and FlexConfig for configuring features using the device CLI	<p>Smart CLI and FlexConfig allows you to configure features that are not yet directly supported through Firepower Device Manager policies and settings. Firepower Threat Defense 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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
Firepower Threat Defense REST API, and an API Explorer	<p>You can use a REST API to programmatically interact with a Firepower Threat Defense device that you are managing locally through Firepower Device Manager. 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 Firepower Device Manager, and then change the path on the URL to <code>##/api-explorer</code>, for example, <code>https://ftd.example.com/##/api-explorer</code>.</p>

Deprecated Features

Deprecated features can prevent upgrade or require pre- or post-upgrade configuration changes. If your upgrade path skips versions, review the deprecated features for intermediate releases.



Note Version 6.6.0 is the last major release that will support the Cisco Firepower User Agent software as an identity source. You will not be able to further upgrade FMCs with user agent configurations. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC) now. This will also allow you to take advantage of features that are not available with the user agent. To convert your license, contact Sales.

For more information, see the appropriate *Cisco Firepower User Agent Configuration Guide* on the [Cisco Firepower Management Center Configuration Guides](#) page.

Version 6.2.3 Deprecated Features

These features were deprecated in Version 6.2.3.

Table 1: Version 6.2.3 Deprecated Features

Feature	Upgrade Impact	Platforms	Description
pager FlexConfig commands	You should redo your configurations after upgrade.	FTD with FDM	Version 6.2.3 blocks pager FlexConfig CLI commands for FTD with FDM.
Expired CA certificates for dynamic analysis	None, but you should patch or upgrade.	AMP for Networks	On June 15, 2018, some Firepower deployments stopped being able to submit files for dynamic analysis. See Expired CA Certificates for Dynamic Analysis, on page 13 .

Version 6.2.0 Deprecated Features

These features were deprecated in Version 6.2.0.

Table 2: Version 6.2.0 Deprecated Features

Feature	Upgrade Impact	Platforms	Description
Nested correlation rules	Upgrade can fail.	FMC	<p>Version 6.2.0 ends support for nested correlation rules. A correlation rule is nested if it serves as a trigger for <i>another correlation rule</i>. For example, if you create Rule A and Rule B, which both trigger on an intrusion event, you can use 'Rule A is true' as a constraint for Rule B. In this configuration, Rule A is nested inside Rule B.</p> <p>Automatic Configuration Changes</p> <p>The upgrade process "flattens" certain nested correlation rules by copying settings from the nested rule (Rule A) to the nesting rule (Rule B), then deleting the nested rule. The upgrade also copies the host profile/user qualifications and the snooze/inactive periods from the nested rule to the nesting rule.</p> <p>For all of these settings except inactive periods, the system can copy the settings from the nested rule to the nesting rule only if the settings are absent from the nesting rule. When the system copies inactive periods from the nested rule to the nesting rule, it retains inactive periods from the nesting rule, so that the resulting rule uses settings from both rules originally involved in the nesting configuration.</p> <p>Avoiding Upgrade Failure</p> <p>Before you upgrade, make sure that any nested correlation rules can be "flattened." Otherwise, the upgrade will fail. Note that the upgrade cannot flatten nested rules if the nested and nesting rule have specific conflicts. To avoid upgrade failure, modify your correlation rules before the upgrade:</p> <ul style="list-style-type: none"> • Remove the host profile qualification, user qualification, and snooze period settings from either the nested rule or the nesting rule, so that only one rule in the nested configuration specifies these settings. • Remove connection trackers from any nested rules. • Remove host profile qualifications, user qualifications, snooze periods, and inactive periods from nested rules that do not have to be true; that is, remove those elements from nested rules that are linked to other rule conditions using the OR operator, within the nesting rule.

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 reenable 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 3: 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.	

Deprecated FlexConfig Commands

The release notes list deprecated FlexConfig objects and commands along with the other deprecated features for each version, in [Deprecated Features, on page 10](#).

For a full list of prohibited commands, including those prohibited when FlexConfig was introduced, see your configuration guide.

**Caution**

In most cases, your existing FlexConfig configurations continue to work post-upgrade and you can still deploy. However, in some cases, using deprecated commands can cause deployment issues.

About FlexConfig

Some Firepower Threat Defense features are configured using ASA configuration commands. Beginning with Version 6.2.0 (FMC deployments) or Version 6.2.3 (FDM deployments), you can use Smart CLI or FlexConfig to manually configure various ASA features that are not otherwise supported in the web interface.

FTD upgrades can add GUI or Smart CLI support for features that you previously configured using FlexConfig. This can deprecate FlexConfig commands that you are currently using; your configurations are *not* automatically converted. After the upgrade, you cannot assign or create FlexConfig objects using the newly deprecated commands.

After the upgrade, examine your FlexConfig policies and objects. If any contain commands that are now deprecated, messages indicate the problem. We recommend you redo your configuration. When you are satisfied with the new configuration, you can delete the problematic FlexConfig objects or commands.

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 Firepower version, that rule is not imported when you update the SRU.

After you upgrade the Firepower software 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 the Snort version included with your Firepower software:

- 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

Some features involve sharing data with Cisco.

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 accept or decline participation. You can also opt in or out at any time.

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.

Web analytics tracking is on by default (and by accepting the Version 6.5.0+ EULA you consent to web analytics tracking), but you can opt out at any time after you complete initial setup.



Note Upgrades to Version 6.2.3 through 6.6.x can enable (or reenable) web analytics tracking. This can occur *even if your current setting is to opt out*. If you do not want Cisco to collect this data, opt out after upgrading.

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 accept or decline participation. You can also opt in or out at any time.

