New Features and Changed Behavior

Although mixed-version Firepower Management Center deployments are supported, new features and resolved issues often require the latest version on the Firepower Management Center *and* its managed devices.

New Features in Firepower Management Center/Firepower 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
Firepower Management Center High Availability Messaging	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.

Feature	Description
Firepower Threat Defense High Availability Hardening	Version 6.2.3 introduces the following features for Firepower Threat Defense devices in high availability: • 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: • **DELETE ftddevicehapairs** • **PUT ftddevicehapairs** • **POST ftddevicehapairs** • **GET ftddevicehapairs**
Firepower Management Center REST API Improvements	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. Newly introduced APIs for NAT: • NAT rules • Firepower Threat Defense NAT policies • Auto NAT rules • Manual NAT rules 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. Newly introduced APIs for Static Route: • IPv4 static routes • IPv6 static routes • SLA monitors

Feature	Description
Upgrade Package Push	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. 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. New/Modified screens: **System** > **Updates**
SSL Hardware Acceleration	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. The following hardware models support SSL acceleration: • Firepower 9300 Series • Cisco Firepower 4100 series
Cisco Success Network	Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to help improve the product and provide effective technical support.
Web Analytics Tracking	By default, in order to improve Firepower products, Cisco collects non-personally-identifiable usage data, including but not limited to pages viewed, the time spent on a page, browser versions, product versions, user location, and management IP addresses or hostnames of your Firepower Management Center appliances. You can opt out of this tracking on the **System** > **Configuration** page.
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 Support on ISA3000	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.
Firepower Threat Defense 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.

Feature	Description
Firepower Threat Defense VPN Improvement	Non-blocking work flow for certificate enrollment operation allows certificate enrollment on multiple Firepower Threat Defense 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.
Automatically rejoin the Firepower Threat Defense 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 Threat Defense on the Firepower 4100 • Firepower Threat Defense on the Firepower 9300
Cluster Control Available in FXOS	By default, the cluster control link uses the 127.2.0.0/16 subnet. Each unit receives an auto-generated address based on the chassis and slot number. For example, for chassis ID 1, slot 1, the Firepower chassis assigns 127.2.**1.1**. 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; the same auto-generation is used for each unit IP address. New/Modified FXOS command: **set ccl subnet** New/Modified Firepower Chassis Management screen: **Logical Devices** > **Add Device** Supported Platforms: • Firepower Threat Defense on the Firepower 4100 • Firepower Threat Defense on the Firepower 9300
External Authentication added for Firepower Threat Defense SSH Access	You can now configure external authentication for SSH access to the Firepower Threat Defense using LDAP or RADIUS. New/Modified screen: **Devices** > **Platform Settings** > **External Authentication** Supported platforms: • Firepower Threat Defense

Feature	Description
Enhanced Vulnerability Database (VDB) Installation	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. 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.
Policy Deploy Restart Improvements	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. Note that restart behavior is different for devices managed using the Firepower Device Manager. See the New Features in Firepower Device Manager/Firepower Threat Defense Version 6.2.3, on page 5 for more information.
Traffic Drop on Policy Apply	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. 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.

New Features in Firepower Device Manager/Firepower Threat Defense Version 6.2.3

Released: March 29, 2018

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

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 Blacklisting	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.

Feature	Description
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.
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.
Firepower Threat Defense Virtual for Kernel-based Virtual Machine (KVM) hypervisor device configuration	You can configure Firepower Threat Defense on Firepower Threat Defense Virtual for KVM devices using Firepower Device Manager. Previously, only VMware was supported. **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.
ISA 3000 (Cisco 3000 Series Industrial Security Appliances) device configuration	You can configure Firepower Threat Defense 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.

Feature	Description
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.
Improved messages that indicate whether a deployment restarts Snort. Also, a reduced need to restart Snort on deployment	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. 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 Firepower Device Manager	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**, **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, Firepower Device Manager 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.

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 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: • 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.
Firepower Threat Defense 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 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 /#/api-explorer, for example, https://ftd.example.com/#/api-explorer.

Changed Behavior in Version 6.2.3

Version 6.2.3 includes the following changed behavior:

- The audit log now denotes if a policy changed on the Firepower Threat Defense Platform Settings **Devices** > **Platform Settings** page. (CSCvg79176)
- If an ISE pxgrid deployed in high availability fails or becomes unreachable, the Firepower Management Center now discovers the new active pxgrid faster. (CSCve71562)
- 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.

- Version 6.2.2.2 increases the memory capacity for lower-end Firepower appliances and reduces the number of health alerts. (CSCvg34306)
- The **asa_mgmt_plane** and **asa_dataplane** options for Firepower Threat Defense device CLI commands are renamed to **management-plane** and **data-plane** respectively.
- Version 6.2.3 limits the number of results you can use or include in a report section, as follows. For table and detail views, you can include fewer records in a PDF report than in an HTML/CSV report.

Report Section Type	Max Records: HTML/CSV Report Section	Max Records: PDF Report Section
Bar chart Pie chart	100 (top or bottom)	100 (top or bottom)
Table view	400,000	100,000
Detail view	1,000	500

Where limits are lower for PDF output than for other output formats, if you enter a number of results that is above the PDF limit but below the limit for other formats, the field shows a yellow warning icon. To see the maximum number of results permitted for PDF output for that section format, hover your pointer over the icon. When you save the template, you are prompted to choose an output format. The PDF output format is unavailable if the PDF limit is exceeded.