Features and Functionality

Major releases contain new features, functionality, and enhancements. Major releases can also include deprecated features and platforms, menu and terminology changes, changed behavior, and so on.

Note These release notes list the new and deprecated features in *this* version, including any upgrade impact. If your upgrade skips versions, see Cisco Firepower Management Center New Features by Release and Cisco Firepower Device Manager New Features by Release for historical feature information and upgrade impact.

- Features for Firepower Management Center Deployments, on page 1
- Features for Firepower Device Manager Deployments, on page 13
- About Deprecated FlexConfig Commands, on page 19
- Intrusion Rules and Keywords, on page 19
- How-To Walkthroughs for the FMC, on page 20
- Sharing Data with Cisco, on page 21

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 6.3.0

Table 1:

Feature	Description
Hardware	
FMC models FMC 1600, 2600, and 4600	We introduced the Firepower Management Center models FMC 1600, 2600, and 4600.
ISA 3000 with FirePOWER Services	ISA 3000 with FirePOWER Services is supported in Version 6.3.0 (Protection license only). Although ISA 3000 with FirePOWER Services was also supported in Version 5.4.x, you cannot upgrade to Version 6.3.0. You must reimage.
Firepower Threat Defense: Device Management	
Hardware bypass support on the Firepower 2100 series for supported network modules	Firepower 2100 series devices now support hardware bypass functionality when using the hardware bypass network modules. New/modified pages: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** Supported platforms: Firepower 2100 series
Support for data EtherChannels in On mode	You can now set data and data-sharing EtherChannels to either Active LACP mode or to On mode. Other types of EtherChannels only support Active mode. New/modified Firepower Chassis Manager pages: **Interfaces** > **All Interfaces** > **Edit Port Channel** > **Mode** New/modified FXOS commands: **set port-channel-mode** Supported platforms: Firepower 4100/9300
Firepower Threat Defense: HA and Clustering	

Feature	Description
Multi-instance capability for Firepower 4100/9300 with FTD	You can now deploy multiple logical devices, each with a Firepower Threat Defense container instance, on a single security engine/module. Formerly, you could only deploy a single native application instance. To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances. Resource management lets you customize performance capabilities for each instance. You can use high availability using a container instance on 2 separate chassis. Clustering is not supported. **Note** Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode is not available for FTD. New/modified FMC pages: **Devices** > **Device Management >** edit device **> Interfaces** tab New/modified Firepower Chassis Manager pages: • **Overview** > **Devices** • **Interfaces** > **All Interfaces** > **Add New** drop-down menu **> Subinterface** • **Interfaces** > **All Interfaces** > **Type** • **Logical Devices** > **Add Device** • **Platform Settings** > **Mac Pool** • **Platform Settings** > **Resource Profiles** New/modified FXOS commands: **connect ftd***name*, **connect module telnet**, **create bootstrap-key PERMIT_EXPERT_MODE**,**create resource-profile**, **create subinterface**, **scope auto-macpool**, **set cpu-core-count**, **set deploy-type**, **set port-type data-sharing**, **set prefix**, **set resource-profile-name**, **set vlan**, **scope app-instance ftd** *name*, **show cgroups container**, **show interface**, **show mac-address**, **show subinterface**, **show tech-support module app-instance**, **show version** Supported platforms: Firepower 4100/9300

Feature	Description
Cluster control link customizable IP Address for the Firepower 4100/9300	By default, the cluster control link uses the 127.2.0.0/16 network. You can now set the network when you deploy the cluster in FXOS. The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: 127.2.*chassis_id*.*slot_id*. 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 except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses. New/modified Firepower Chassis Manager pages: **Logical Devices** > **Add Device** > **Cluster Information** New/modified options: **CCL Subnet IP** field New/modified FXOS commands: **set cluster-control-link network** Supported platforms: Firepower 4100/9300
Improved FTD cluster addition to the FMC	You can now add any unit of a cluster to the FMC, and the other cluster units are detected automatically. Formerly, you had to add each cluster unit as a separate device, and then group them into a cluster with the FMC. Adding a cluster unit is also now automatic. Note that you must delete a unit manually. New/modified pages: • **Devices** > **Device Management** > **Add** drop-down menu > **Device** > **Add Device** dialog box • **Devices** > **Device Management** > **Cluster** tab > **General** area > **Cluster Registration Status** > **Current Cluster Summary** link > **Cluster Status** dialog box Supported platforms: Firepower 4100/9300
Firepower Threat Defense: Encryption and VPN	
SSL hardware acceleration	Additional FTD devices now support SSL hardware acceleration. Also, this option is now enabled by default. Upgrading to Version 6.3.0 automatically enables SSL hardware acceleration on eligible devices. Using SSL hardware acceleration if you are not decrypting traffic can affect performance. We recommend you disable SSL hardware acceleration on devices that are not decrypting traffic. Supported platforms: Firepower 2100 series, Firepower 4100/9300
RA VPN: RADIUS Dynamic Authorization or Change of Authorization (CoA)	You can now use RADIUS servers for user authorization of RA VPN using dynamic access control lists (ACLs) or ACL names per user. Supported platforms: FTD

Feature	Description
RA VPN: Two-Factor Authentication	Firepower Threat Defense now supports two-factor authentication for RA VPN users using the Cisco AnyConnect Secure Mobility Client. For the two-factor authentication process, we support: • First factor: any RADIUS or LDAP/AD server • Second factor: RSA tokens or DUO passcodes pushed to mobile For more information on Duo multi-factor authentication (MFA) for FTD, see the Cisco Firepower Threat Defense (FTD) VPN with AnyConnect documentation on the Duo Security website. Supported platforms: FTD
Security Policies	
Firepower Threat Defense service policy	You can now configure a Firepower Threat Defense service policy as part of your access control policy advanced options. Use FTD service policies to apply services to specific traffic classes. Features supported include: • TCP State Bypass • Randomizing TCP sequence numbers • Decrementing the time-to-live (TTL) value on packets • Dead Connection Detection • Setting a limit on the maximum number of connections and embryonic connections per traffic class and per client. • Timeouts for embryonic, half closed, and idle connections **Note** Before Version 6.3.0, you could configure connection-related service rules using the TCP_Embryonic_Conn_Limit and TCP_Embryonic_Conn_Timeout predefined FlexConfig objects. You should remove those objects and redo your rules in the FTD service policy. If you created any custom FlexConfig objects to implement any of these connection-related features (that is, **set connection** commands), you should also remove those objects and implement the features through the FTD service policy. Failure to do so can cause deployment issues. The *Threat Defense Service Policies* chapter in the Firepower Management Center Configuration Guide has details on how service policies relate to FlexConfig and other features. New/modified pages: **Policies** > **Access Control** > edit/create policy > **Advanced** tab > **Threat Defense Service Policy** Supported platforms: FTD

Feature	Description
Update interval for URL category and reputation data	**Upgrade impact.** You can now force URL data to expire. There is a tradeoff between security and performance. A shorter interval means you use more current data, while a longer interval can make web browsing faster for your users. If you worked with Cisco TAC to specify a timeout value for the URL filtering cache, the upgrade may change that value. Otherwise, the setting defaults to disabled (the current behavior), meaning that cached URL data does not expire. New/modified pages: **System** > **Integration** > **Cisco CSI** > **Cached URLs Expire** setting Supported platforms: FMC
Event Logging and Analysis	
Cisco Security Packet Analyzer Integration	You can integrate with Cisco Security Packet Analyzer to examine events and display analysis results, or download results for further analysis. New/modified pages: • **System** > **Integration** > **Packet Analyzer** • **Analysis** > **Advanced** > **Packet Analyzer Queries** • **Query Packet Analyzer** when right-clicking on an event in the dashboard or event viewer Supported platforms: FMC
Contextual cross-launch	You can right-click an event in the dashboard or event viewer to look up related information in predefined or custom, public or private URL-based resources. New/modified pages: **Analysis** > **Advanced** > **Contextual Cross-Launch** Supported platforms: FMC

Feature	Description
Unified syslog configuration	**Upgrade impact.** Version 6.3.0 changes and centralizes the way the system logs connection and intrusion events via syslog. Previously, you configured event logging via syslog in multiple places, depending on the event type. You now configure syslog messaging in the access control policy. These configurations affect connection and intrusion event logging for the access control, SSL, prefilter, and intrusion policies, as well as for Security Intelligence. The upgrade does not change your existing settings for connection event logging. However, you may suddenly start receiving intrusion events you did not "expect" via syslog. This is because the intrusion policy now sends syslog events to the destination specified in the access control policy. (Before, you could configure syslog alerting in an intrusion policy to send events to the syslog on the managed device itself rather than to an external host.) For FTD devices, some syslog platform settings now apply to connection and intrusion event messages. For a list, see the *Platform Settings for Firepower Threat Defense* chapter in the Firepower Management Center Configuration Guide. For NGIPS devices (7000/8000 series, ASA FirePOWER, NGIPSv), messages now use the ISO 8601 timestamp format as specified in RFC 5425. Supported platforms: Any
Fully qualified syslog messages for connection and intrusion events	The format of syslog messages for connection, security intelligence, and intrusion events have the following changes: • Messages from FTD devices now include event type identification numbers. • Fields with empty or unknown values are no longer included, so messages are shorter and important data is less likely to be truncated. • Timestamps now use the ISO 8601 timestamp format as specified in the RFC 5425 syslog format (optional for FTD, required for Classic). Supported platforms: Any
Other syslog improvements for FTD devices	You can send all syslog messages from the same interface (data or management), using the same IP address, using TCP or UDP protocol. Note that secure syslog is supported on data ports only. You can also use the RFC 5424 format for message timestamps. Supported platforms: FTD
Administration and Troubleshooting	

Feature	Description
Export-controlled features for approved customers	Customers whose Smart Accounts are not otherwise eligible to use restricted functionality can purchase term-based licenses, with approval. New/modified pages: **System** > **Licenses** > **Smart Licenses** Supported platforms: FMC, FTD
Specific License Reservation for approved customers	Customers can use Specific License Reservation to deploy Smart Licensing in an air-gapped network. The FMC reserves licenses from your virtual account for a specified duration without accessing the Cisco Smart Software Manager or Smart Software Satellite Server. New/modified pages: **System** > **Licenses** > **Specific Licenses** Supported platforms: FMC, FTD (except ISA 3000)
IPv4 range, subnet, and IPv6 support for SNMP hosts	You can now use IPv4 range, IPv4 subnet, and IPv6 host network objects to specify the SNMP hosts that can access a Firepower Threat Defense device. New/modified pages: **Devices** > **Platform Settings** > create or edit FTD policy **> SNMP > Hosts** tab Supported platforms: FTD
Access control using fully qualified domain names (FQDN)	You can now create fully qualified domain name (FQDN) network objects and use them in access control and prefilter rules. To use FQDN objects, you must also configure DNS server groups and DNS platform settings, so that the system can resolve the domain names. New/modified pages: • **Objects** > **Object Management** > **Network** • **Objects** > **Object Management** > **DNS Server Group** • **Devices** > **Platform Settings** > create or edit FTD policy > **DNS** Supported platforms: FTD
CLI for the FMC	An CLI for the FMC supports a small set of basic commands (change password, show version, reboot/restart, and so on). By default the FMC CLI is disabled, and logging into FMC using SSH accesses the Linux shell. New/modified Classic CLI commands: The **system lockdown-sensor** command has changed to **system lockdown**. This command now works for both devices and FMCs. New/modified pages: **System** > **Configuration** > **Console Configuration** > **Enable CLI Access** check box Supported platforms: FMC, including FMCv

Feature	Description
Copy device configurations	You can copy device configurations and policies from one device to another. New/modified pages: **Devices** > **Device Management** > edit the device > **General** area > **Get/Push Device Configuration** icons. Supported platforms: FMC
Backup/restore FTD device configurations	You can use the FMC web interface to back up configurations for some FTD devices. New/modified pages: **System** > **Tools** > **Backup/Restore** New/modified CLI commands: **restore** Supported platforms: All physical FTD devices, FTDv for VMware
Skip deploying to up-to-date devices when you schedule deploy tasks	**Upgrade impact.** When you schedule a task to deploy configuration changes, you can now opt to **Skip Deployment for up-to-date devices**. This performance-enhancing setting is enabled by default. The upgrade process automatically enables this option on existing scheduled tasks. To continue to force a scheduled deploy to up-to-date devices, you must edit the scheduled task. New/modified pages: **System** > **Tools** > **Scheduling** > add or edit a task > choose **Job Type** of **Deploy Policies** Supported platforms: FMC
New health modules	New health modules alert you when: • **Threat Data Updates on Devices**: Threat identification data on managed devices fails to update. • **Realm**: A user is reported to the FMC without being downloaded, or a user logs into a domain that corresponds to a realm not known to the FMC. New/modified pages: • **System > Health > Policy** • **System > Health > Monitor** Supported platforms: FMC
Configurable packet capture size	You can now store up to 10 GB of packet captures. New/modified CLI commands: **file-size**, **show capture** Supported platforms: Firepower 4100/9300
Security and Hardening	

Feature	Description
HTTPS Certificates	The default HTTPS server certificate provided with the system now expires in three years. If your appliance uses a default server certificate that was generated before you upgraded to Version 6.3.0, the server certificate will expire 20 years from when it was first generated. If you are using the default HTTPS server certificate the system now provides the ability to renew it. New/modified pages: **System** > **Configuration** > **HTTPS Certificate** > **Renew HTTPS Certificate** button New/modified Classic CLI commands: **show http-cert-expire-date**, **system renew-http-cert***new_key* Supported platforms: Physical FMCs, 7000/8000 series devices
Improved login security	**Upgrade impact.** Added FMC user configuration settings to improve login security: • **Track Successful Logins**: Track the number of successful logins each FMC account has performed within a specific time period. • **Password Reuse Limit**: Track an FMC user's password history to prevent reuse. • **Max Number of Login Failures** and **Set Time in Minutes to Temporarily Lockout Users**: Limit the number of times in a row an FMC user can enter incorrect web interface login credentials before being temporarily blocked. We also updated the list of supported ciphers and cryptographic algorithms for secure SSH access. If your SSH client fails to connect with a Firepower appliance due to a cipher error, update your client to the latest version. New/modified pages: **System** > **Configuration > User Configuration** Supported platforms: FMC
Limit SSH login failures on devices	When a user accesses any device via SSH and fails three successive login attempts, the device terminates the SSH session. Supported platforms: Any device
Firepower Management Center REST API	

Feature	Description
New REST API services	Added REST API services to support these features: • Site-to-site VPN topology: ftds2svpns, endpoints, ipsecsettings, advancedsettings, ikesettings, ikev1ipsecproposals, ikev1policies, ikev2ipsecproposals, ikev2policies • HA device failover: failoverinterfacemacaddressconfigs, monitoredinterfaces Supported platforms: FMC
Bulk overrides	You can now perform bulk overrides on specific objects. For a full list, see the Cisco Firepower Management Center REST API Quick Start Guide.

Deprecated Features in FMC Version 6.3.0

Table 2:

Feature	Upgrade Impact	Description
EMS extension support for decryption	EMS extension support discontinued until you patch or upgrade.	Version 6.3.0 discontinues EMS extension support, which was introduced in Version 6.2.3.8/6.2.3.9. This means that the **Decrypt-Resign** and **Decrypt-Known Key** SSL policy actions no longer support the EMS extension during ClientHello negotiation, which would enable more secure communications. The EMS extension is defined by RFC 7627. In Firepower Management Center deployments, this feature depends on the *device* version. Upgrading the Firepower Management Center to Version 6.3.0 does not discontinue support, as long as the device is running a supported version. However, upgrading the device to Version 6.3.0 does discontinue support. Support is reintroduced in Version 6.3.0.1.
Decryption on passive and inline tap Interfaces	The system stops decrypting traffic in passive deployments.	Version 6.3.0 ends support for decrypting traffic on interfaces in passive or inline tap mode, even though the GUI allows you to configure it. Any inspection of encrypted traffic is necessarily limited.

Feature	Upgrade Impact	Description
Default DNS group FlexConfig objects	You should redo your configurations after upgrade.	Version 6.3.0 deprecates this FlexConfig object for Firepower Threat Defense with FMC: • Default_DNS_Configure And these associated text objects: • defaultDNSNameServerList • defaultDNSParameters These allowed you to configure the Default DNS group, which defines the DNS servers that can be used when resolving fully qualified domain names on the data interfaces. This allowed you to use commands in the CLI, such as **ping**, using host names rather than IP addresses. You can now configure DNS for the data interfaces in the FTD platform settings policy: **Devices** > **Platform Settings >** create or edit FTD policy **>** **DNS**.
Embryonic connection limit and timeout FlexConfig objects	Post-upgrade deployment issues. You should redo your configurations after upgrade.	Version 6.3.0 deprecates these FlexConfig objects for Firepower Threat Defense with FMC: • TCP_Embryonic_Conn_Limit • TCP_Embryonic_Conn_Timeout And these associated text objects: • tcp_conn_misc • tcp_conn_limit • tcp_conn_timeout These allowed you to configure embryonic connection limits and timeouts to protect against SYN Flood Denial of Service (DoS) attacks. You can now configure these features in the FTD service policy: **Policies** > **Access Control >** add/edit policy **>** **Advanced** tab **>** **Threat Defense Service Policy**. **Caution** If you used **set connection** commands to implement connection-related service rules, you should remove the associated objects and implement the features through the FTD service policy. Failure to do so can cause deployment issues.

Feature	Upgrade Impact	Description
Web interface changes	None.	Version 6.3.0 changes these menu options: **Analysis > Advanced > Whois** is now **Analysis > Lookup > Whois** **Analysis > Advanced > Geolocation** is now **Analysis > Lookup > Geolocation** **Analysis > Advanced > URL** is now **Analysis > Lookup > URL** **Analysis > Advanced > Custom Workflows** is now **Analysis > Custom > Custom Workflows** **Analysis > Advanced > Custom Tables** is now **Analysis > Custom > Custom Tables** **Analysis > Hosts > Vulnerabilities** is now **Analysis > Vulnerabilities > Vulnerabilities** **Analysis > Hosts > Third-Party Vulnerabilities** is now **Analysis > Vulnerabilities > Third-Party Vulnerabilities**
VMware 5.5 hosting	Upgrade the hosting environment before you upgrade the Firepower software.	Version 6.3.0+ virtual deployments have not been tested on VMware vSphere/VMware ESXi 5.5. This includes FMCv, FTDv, and NGIPSv for VMware.
ASA 5506-X series and ASA 5512-X devices with Firepower software	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.3.0+ of the Firepower software (both Firepower Threat Defense and ASA FirePOWER) on ASA 5506-X, 5506H-X, 5506W-X, and 5512-X devices.

Features for Firepower Device Manager Deployments

New Features in FDM Version 6.3.0

Feature	Description
High availability configuration.	You can configure two devices as an active/standby high availability pair. A high availability or failover setup joins two devices so that if the primary device fails, the secondary device can take over. This helps you keep your network operational in case of device failure. The devices must be of the same model, with the same number and type of interfaces, and they must run the same software version. You can configure high availability from the **Device** page.

Feature	Description
Support for passive user identity acquisition.	You can configure identity policies to use passive authentication. Passive authentication gathers user identity without prompting the user for username and password. The system obtains the mappings from the identity sources you specify, which can be Cisco Identity Services Engine (ISE)/Cisco Identity Services Engine Passive Identity Connector (ISE PIC), or logins from remote access VPN users. Changes include supporting passive authentication rules in **Policies** > **Identity**, and ISE configuration in **Objects** > **Identity Sources**.
Local user support for remote access VPN and user identity.	You can now create users directly through FDM. You can then use these local user accounts to authenticate connections to a remote access VPN. You can use the local user database as either the primary or fallback authentication source. In addition, you can configure passive authentication rules in the identity policy so that local usernames are reflected in the dashboards and so they are available for traffic matching in policies. We added the **Objects** > **Users** page, and updated the remote access VPN wizard to include a fallback option.
Changed default behavior for VPN traffic handling in the access control policy (**sysopt connection permit-vpn**).	The default behavior for how VPN traffic is handled by the access control policy has changed. Starting in 6.3, the default is that all VPN traffic will be processed by the access control policy. This allows you to apply advanced inspections, including URL filtering, intrusion protection, and file policies, to VPN traffic. You must configure access control rules to allow VPN traffic. Alternatively, you can use FlexConfig to configure the **sysopt connection permit-vpn** command, which tells the system to bypass the access control policy (and any advanced inspections) for VPN-terminated traffic
Support for FQDN-based network objects and data interface support for DNS lookup.	You can now create network objects (and groups) that specify a host by fully-qualified domain name (FQDN) rather than a static IP address. The system looks up the FQDN-to-IP address mapping periodically for any FQDN object that is used in an access control rule. You can use these objects in access control rules only. We added the DNS Group object to the objects page, changed the **System Settings** > **DNS Server** page to allow group assignment to data interfaces, and the access control rule to allow for FQDN network object selection. In addition, the DNS configuration for the management interface now uses DNS groups instead of a set list of DNS server addresses.

Feature	Description
Support for TCP syslog and the ability to send diagnostic syslog messages through the management interface.	In previous releases, diagnostic syslog messages (as opposed to connection and intrusion messages) always used a data interface. You can now configure syslog so that all messages use the management interface. The ultimate source IP address depends on whether you use the data interfaces as the gateway for the management interface, in which case the IP address will be the one from the data interface. You can also configure syslog to use TCP instead of UDP as the protocol. We made changes to the Add/Edit dialog box for syslog servers from **Objects** > **Syslog Servers**.
External Authentication and Authorization using RADIUS for FDM Users.	You can use an external RADIUS server to authenticate and authorize users logging into FDM. You can give external users administrative, read-write, or read-only access. FDM can support 5 simultaneous logins; the sixth session automatically logs off the oldest session. You can forcefully end a FDM user session if necessary. We added RADIUS server and RADIUS server group objects to the **Objects** > **Identity Sources** page for configuring the objects. We added the **AAA Configuration** tab to **Device** > **System Settings** > **Management Access**, for enabling use of the server groups. In addition, the **Monitoring** > **Sessions** page lists the active users and lets an administrative user end a session.
Pending changes view and deployment improvements.	The deployment window has changed to provide a clearer view of the pending changes that will be deployed. In addition, you now have the option to discard changes, copy changes to the clipboard, and download changes in a YAML formatted file. You can also name deployment jobs so they are easier to find in the audit log.
Audit Log.	You can view an audit log that records events such as deployments, system tasks, configuration changes, and administrative user login and logout. We added the **Device** > **Device Administration** > **Audit Log** page.
Ability to export the configuration.	You can download a copy of the device configuration for record keeping purposes. However, you cannot import this configuration into a device. This feature is not a replacement for backup/restore. We added the **Device** > **Device Administration** > **Download Configuration** page.
Improvements to URL filtering for unknown URLs.	If you perform category-based URL filtering in access control rules, users might access URLs whose category and reputation are not defined in the URL database. Previously, you needed to manually enable the option to look up the category and reputation for these URLs from Cisco Collective Security Intelligence (CSI). Now, that option is enabled by default. In addition, you can now set the time-to-live (TTL) for the lookup results, so that the system can refresh the category/reputation for each unknown URL. We updated the **Device** > **System Settings** > **URL Filtering Preferences** page.

Feature	Description
Security Intelligence logging is now enabled by default.	The Security Intelligence policy was introduced in 6.2.3, with logging disabled by default. Starting with 6.3.0, logging is enabled by default. If you upgrade from 6.2.3, your logging settings are preserved, either enabled or disabled. Enable logging if you want to see the results of policy enforcement.
Passive mode interfaces	You can configure an interface in passive mode. When acting passively, the interface simply monitors the traffic from the source ports in a monitoring session configured on the switch itself (for hardware devices) or on the promiscuous VLAN (for FTDv). You can use passive mode to evaluate how the FTDv device would behave if you deployed it as an active firewall. You can also use passive interfaces in a production network if you need IDS (intrusion detection system) services, where you want to know about threats, but you do not want the device to actively prevent the threats. You can select passive mode when editing physical interfaces and when you create security zones.
Smart CLI enhancements for OSPF, and support for BGP.	The Smart CLI OSPF configuration has been enhanced, including new Smart CLI object types for standard and extended ACLs, route maps, AS Path objects, IPv4 and IPv6 prefix lists, policy lists, and standard and expanded community lists. In addition, you can now use Smart CLI to configure BGP routing. You can find these features on the **Device** > **Advanced Configuration** page.
Enhancements for ISA 3000 devices.	You can now configure the following features for the ISA 3000: alarms, hardware bypass, and backup and restore using the SD card. You use FlexConfig to configure the alarms and hardware bypass. For the SD card, we updated the backup/restore pages in FDM.
Support for ASA 5506-X, 5506W-X, 5506H-X, and 5512-X removed starting with FTD 6.3.	You cannot install FTD 6.3 or subsequent releases on the ASA 5506-X, 5506W-X, 5506H-X, and 5512-X. The final supported FTD release for these platforms is 6.2.3.
FTD REST API version 2 (v2).	The FTD REST API for software version 6.3 has been incremented to version 2. You must replace v1 in the API URLs with v2. The v2 API includes many new resources that cover all features added in software version 6.3. Please re-evaluate all existing calls, as changes might have been mode to the resource models you are using. To open the API Explorer, where you can view the resources, change the end of the FDM URL to **/#/api-explorer** after logging in.
Web analytics for providing product usage information to Cisco.	You can enable web analytics, which provides anonymous product usage information to Cisco based on page hits. This information can help Cisco determine feature usage patterns and help Cisco improve the product. All usage data is anonymous and no sensitive data is transmitted. Web analytics is enabled by default. We added Web Analytics to the **Device** > **System Settings** > **Cloud Services** page.

Feature	Description
Installing a Vulnerability Database (VDB) update no longer restarts Snort.	When you install a VDB update, the installation itself no longer restarts Snort. However, Snort continues to restart during the next configuration deployment.
Deploying an Intrusion Rules (SRU) database update no longer restarts Snort.	After you install an intrusion rules (SRU) update, you must deploy the configuration to activate the new rules. The deployment of the SRU update no longer causes a Snort restart.

Deprecated Features in FDM Version 6.3.0

Table 3:

Feature	Upgrade Impact	Description
EMS extension support for decryption	EMS extension support discontinued until you patch or upgrade.	Version 6.3.0 discontinues EMS extension support, which was introduced in Version 6.2.3.8/6.2.3.9. This means that the **Decrypt-Resign** and **Decrypt-Known Key** SSL policy actions no longer support the EMS extension during ClientHello negotiation, which would enable more secure communications. The EMS extension is defined by RFC 7627. Support is reintroduced in Version 6.3.0.1.

Feature	Upgrade Impact	Description
FlexConfig commands	You should redo your configurations after upgrade.	Version 6.3.0 deprecates the following FlexConfig commands for Firepower Threat Defense with FDM: • **access-list**: You can now create **extended** and **standard** access lists using the Smart CLI Extended Access List or Standard Access List objects. You can then use them on FlexConfig-supported commands that refer to the ACL by object name, such as **match access-list** with an extended ACL for service policy traffic classes. • **as-path**: You can now create Smart CLI AS Path objects and use them in a Smart CLI BGP object to configure an autonomous system path filter. • **community-list**: You can now create Smart CLI Expanded Community List or Standard Community List objects and use them in a Smart CLI BGP object to configure a community list filter. • **dns-group**: You can now configure DNS groups using **Objects** > **DNS Groups**, and assign the groups using **Device** > **System Settings** > **DNS Server**. • **policy-list**: You can now create Smart CLI Policy List objects and use them in a Smart CLI BGP object to configure a policy list. • **prefix-list**: You can now create Smart CLI IPv4 Prefix List objects and use them in a Smart CLI OSPF or BGP object to configure prefix list filtering for IPv4. • **route-map**: You can now create Smart CLI Route Map objects and use them in a Smart CLI OSPF or BGP object to configure route maps. • **router bgp**: You can now use the Smart CLI templates for BGP.
VMware 5.5 hosting	Upgrade the hosting environment before you upgrade the Firepower software.	Version 6.3.0+ FTDv deployments have not been tested on VMware vSphere/VMware ESXi 5.5.
ASA 5506-X series and ASA 5512-X devices with Firepower Threat Defense	Upgrade prohibited.	You cannot upgrade to or freshly install Firepower Threat Defense Version 6.3.0+ on ASA 5506-X, 5506H-X, 5506W-X, and 5512-X devices.

About Deprecated FlexConfig Commands

This document lists any deprecated FlexConfig objects and commands along with the other deprecated features. 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.

Upgrades to FTD 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 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.

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 4: 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**.
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: • 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.
Walkthrough is out of sync with the FMC: • Starts on the wrong step. • Advances prematurely. • Will not advance.	If a walkthrough is out of sync, you can: • Attempt to continue. 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. • End the walkthrough, navigate to a different page, and try again. Sometimes you cannot continue. For example, if you do not click **Next** after you complete a step, you may need to end the walkthrough.

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.