Cisco Secure Firewall Device Manager New Features by Release

First Published: 2021-01-19

Last Modified: 2024-03-19

New Features by Release

This document describes new and deprecated features for each release, including upgrade impact.

A feature has upgrade impact if upgrading and deploying will cause the system to process traffic or otherwise act differently without any other action on your part. This is especially common with new threat detection and application identification capabilities. Or, sometimes the upgrade process has a special requirement; for example, in some cases you must perform a non-standard task before or after upgrade (edit or delete a specific configuration, apply health policies, redo FlexConfig commands in the web interface, and so on).

For information on Snort enhancements by version, keeping in mind that the management center may offer more configurable options than device manager, see Cisco Secure Firewall Management Center New Features by Release. Snort is the main inspection engine for threat defense regardless of whether you are using device manager or management center.

Note that if you are using the web interface in a language other than English, features introduced in maintenance releases and patches may not be translated until the next major release.

Suggested Release: Version 7.2.5.x

To take advantage of new features and resolved issues, we recommend you upgrade all eligible appliances to at least the suggested release, including the latest patch. On the Cisco Support & Download site, the suggested release is marked with a gold star. In Version 7.2.6+/7.4.1+, the management center notifies you when a new suggested release is available, and indicates suggested releases on its product upgrades page.

Suggested Releases for Older Appliances

If an appliance is too old to run the suggested release and you do not plan to refresh the hardware right now, choose a major version then patch as far as possible. Some major versions are designated *long-term* or *extra long-term*, so consider one of those. For an explanation of these terms, see Cisco NGFW Product Line Software Release and Sustaining Bulletin.

If you are interested in a hardware refresh, contact your Cisco representative or partner contact.

New Features in Device Manager Version 7.4

Note Device manager support for Version 7.4 features begins with Version 7.4.1. This is because Version 7.4.0 is not available on any platforms that support device manager.

Table 1: Device Manager Features in Version 7.4.1

Feature	Description
Platform Features	
Firepower 1010E support returns..	Support returns for the Firepower 1010E, which was introduced in Version 7.2.3 and temporarily deprecated in Version 7.3. See: Cabling for the Firepower 1010
Network modules for the Secure Firewall 3130 and 3140.	We introduced these network modules for the Secure Firewall 3130 and 3140: • 2-port 100G QSFP+ network module (FPR3K-XNM-2X100G) See: Cisco Secure Firewall 3110, 3120, 3130, and 3140 Hardware Installation Guide
VPN Features	
IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100.	**Upgrade impact. Qualifying connections start being offloaded.** On the Secure Firewall 3100, qualifying IPsec connections through the VTI loopback interface are now offloaded by default. Previously, this feature was only supported on physical interfaces. This feature is automatically enabled by the upgrade. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command.
Interface Features	

Feature	Description
Merged management and diagnostic interfaces.	**Upgrade impact. Merge interfaces after upgrade.** For new devices using 7.4 and later, you cannot use the legacy diagnostic interface. Only the merged management interface is available. If you upgraded to 7.4 or later, and you did not have any configuration for the diagnostic interface, then the interfaces will merge automatically. If you upgraded to 7.4 or later, and you have configuration for the diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate diagnostic interface. Note that support for the diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including management) in the configuration. New/modified screens: • **Devices** > **Interfaces** > **Management** interface • (Moved to Interfaces) **System Settings** > **Management Interface** • **Devices** > **Interfaces** > **Merge Interface action needed** > **Management Interface Merge** New/modified commands: **show management-interface convergence**
Deploy without the diagnostic interface on threat defense virtual for Azure and GCP.	You can now deploy without the diagnostic interface on threat defense virtual for Azure and GCP. Azure deployments still require at least two data interfaces, but GCP requires that you replace the diagnostic interface with a data interface, for a new minimum of three. (Previously, threat defense virtual deployments required one management, one diagnostic, and at least two data interfaces.) Restrictions: This feature is supported for new deployments only. It is not supported for upgraded devices. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
Inline sets for Firepower 1000 series, Firepower 2100, and Secure Firewall 3100.	You can configure inline sets on Firepower 1000 series, Firepower 2100, and Secure Firewall 3100 devices. We added the inline sets tab to the Interface page.
Licensing Features	

Feature	Description
Changes to license names and support for the Carrier license.	Licenses have been renamed: • Threat is now IPS • Malware is now Malware Defense • Base is now Essentials • AnyConnect Apex is now Secure Client Premier • AnyConnect Plus is now Secure Client Advantage • AnyConnect VPN Only is now Secure Client VPN Only In addition, you can now apply the Carrier license, which allows you to configure GTP/GPRS, Diameter, SCTP, and M3UA inspections. Use FlexConfig to configure these features. See: Licensing the System
Administrative and Troubleshooting Features	
Default NTP server updated.	**Upgrade impact. The system connects to new resources.** The default NTP servers have changed from sourcefire.pool.ntp.org to time.cisco.com. To use a different NTP server, select **Device**, then click **Time Services** in the **System Settings** panel.
SAML servers for HTTPS management user access.	You can configure a SAML server to provide external authentication for HTTPS management access. You can configure external users with the following types of authorization access: Administrator, Audit Admin, Cryptographic Admin, Read-Write User, Read-Only User. You can use Common Access Card (CAC) for login when using a SAML server. We updated the SAML identity source object configuration, and the **System Settings** > **Management Access** page to accept them.
Detect configuration mismatches in threat defense high availability pairs.	You can now use the CLI to detect configuration mismatches in threat defense high availability pairs. New/modified CLI commands: **show failover config-sync error**, **show failover config-sync stats** See: Cisco Secure Firewall Threat Defense Command Reference
Capture dropped packets with the Secure Firewall 3100.	Packet losses resulting from MAC address table inconsistencies can impact your debugging capabilities. The Secure Firewall 3100 can now capture these dropped packets. New/modified CLI commands: [**drop** { **disable** | **mac-filter** }] in the **capture** command. See: Cisco Secure Firewall Threat Defense Command Reference

Feature	Description
Firmware upgrades included in FXOS upgrades.	**Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.** For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1+ now include firmware upgrades. If any firmware component on the device is older than the one included in the FXOS bundle, the FXOS upgrade also updates the firmware. If the firmware is upgraded, the device reboots twice—once for FXOS and once for the firmware. Just as with software and operating system upgrades, do not make or deploy configuration changes during firmware upgrade. Even if the system appears inactive, do not manually reboot or shut down during firmware upgrade. See: Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide
Quick recovery after data plane failure for the Firepower 1000/2100 and Firepower 4100/9300.	When the data plane process on the Firepower 1000/2100 or the Firepower 4100/9300 crashes, the system reloads the process instead of rebooting the device. Reloading the data plane also restarts other processes, including Snort. If the data plane crashes during bootup, the device follows the normal reload/reboot sequence; this avoids a reload loop. This feature is enabled by default for both new and upgraded devices. To disable it, use FlexConfig. New/modified ASA CLI commands: **data-plane quick-reload**, **show data-plane quick-reload status** New/modified threat defense CLI commands: **show data-plane quick-reload status** Supported platforms: Firepower 1000/2100, Firepower 4100/9300 See: Cisco Secure Firewall Threat Defense Command Reference and Cisco Secure Firewall ASA Series Command Reference.

New Features in Device Manager Version 7.3

Table 2: Device Manager Features in Version 7.3.x

Feature	Description
Platform Features	
Secure Firewall 3105.	We introduced the Secure Firewall 3105. Minimum threat defense: Version 7.3.1

Feature	Description
Network modules for the Secure Firewall 4100.	We introduced these network modules for the Firepower 4100: • 2-port 100G network module (FPR4K-NM-2X100G) Supported platforms: Firepower 4112, 4115, 4125, 4145
ISA 3000 System LED support for shutting down.	Support returns for this feature. When you shut down the ISA 3000, the System LED turns off. Wait at least 10 seconds after that before you remove power from the device. This feature was introduced in Version 7.0.5 but was temporarily deprecated in Versions 7.1–7.2.
New compute shapes for threat defense virtual for OCI.	Threat defense virtual for OCI adds support for the following compute shapes: • Intel VM.DenseIO2.8 • Intel VM.StandardB1.4 • Intel VM.StandardB1.8 • Intel VM.Standard1.4 • Intel VM.Standard1.8 • Intel VM.Standard3.Flex • Intel VM.Optimized3.Flex • AMD VM.Standard.E4.Flex Note that the VM.Standard2.4 and VM.Standard2.8 compute shapes reached end of orderability in February 2022. If you are deploying Version 7.3+, we recommend a different compute shape. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
Support ends: Firepower 4110, 4120, 4140, 4150.	You cannot run Version 7.3+ on the Firepower 4110, 4120, 4140, or 4150.
Support ends: Firepower 9300: SM-24, SM-36, SM-44 modules.	You cannot run Version 7.3+ on the Firepower 9300 with SM-24, SM-36, or SM-44 modules.
No support for Firepower 1010E (temporary).	The Firepower 1010E, which was introduced in Version 7.2.3, does not support Version 7.3. Support returns in Version 7.4. You cannot upgrade a Version 7.2.x Firepower 1010E to Version 7.3, and you should not reimage there either. If you have a Firepower 1010E device running Version 7.3, reimage to a supported release.
Firewall and IPS Features	

Feature	Description
TLS 1.3 support in SSL decryption policies, and configurable behavior for undecryptable connections.	**Upgrade impact.** You can configure SSL decryption rules for TLS 1.3 traffic. TLS 1.3 support is available when using Snort 3 only. You can also configure non-default behavior for undecryptable connections. If you are using Snort 3, upon upgrade, TLS 1.3 is automatically selected for any rules that have all SSL/TLS versions selected; otherwise, TLS 1.3 is not selected. The same behavior happens if you switch from Snort 2 to Snort 3. We added TLS 1.3 as an option on the advanced tab of the add/edit rule dialog box. We also redesigned the SSL decryption policy settings to include the ability to enable TLS 1.3 decryption, and to configure undecryptable connection actions. See: Advanced Criteria for SSL Decryption Rules and Configure Advanced and Undecryptable Traffic Settings
Refined URL filtering lookup.	You can now explicitly set how URL filtering lookups occur. You can select to use the local URL database only, both the local database and cloud lookup, or cloud lookup only. We augmented the URL Filtering system setting options. See: Configuring URL Filtering Preferences
Interface Features	
IPv6 support for virtual appliances.	Threat defense virtual now supports IPv6 in the following environments: • AWS • Azure • KVM • VMware See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
DHCPv6 Client.	You can now obtain an IPv6 address from DHCPv6. New/modified screens: **Device** > **Interfaces** > **Edit Interface** > **Advanced** See: Configure Advanced Interface Options
Administrative and Troubleshooting Features	

Feature	Description
Automatically update CA bundles.	**Upgrade impact. The system connects to Cisco for something new.** The local CA bundle contains certificates to access several Cisco services. The system now automatically queries Cisco for new CA certificates at a daily system-defined time. Previously, you had to upgrade the software to update CA certificates. You can use the CLI to disable this feature. New/modified CLI commands: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** Version restrictions: This feature is included in Versions 7.0.5+, 7.1.0.3+, and 7.2.4+. It is not supported in earlier 7.0, 7.1, or 7.2 releases. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco. See: Cisco Secure Firewall Threat Defense Command Reference
Skip Certificate Authority checking for trusted certificates.	You can skip the check if you need to install a local CA certificate as the trusted CA certificate. We added the **Skip CA Certificate Check** option when uploading trusted CA certificates.

Feature	Description
Combined upgrade and install package for Secure Firewall 3100.	**Reimage Impact.** In Version 7.3, we combined the threat defense install and upgrade package for the Secure Firewall 3100, as follows: • Version 7.1–7.2 install package: cisco-ftd-fp3k.*version*.SPA • Version 7.1–7.2 upgrade package: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • Version 7.3+ combined package: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar Although you can upgrade threat defense without issue, you cannot reimage from older threat defense and ASA versions directly to threat defense Version 7.3+. This is due to a ROMMON update required by the new image type. To reimage from those older versions, you must "go through" ASA 9.19+, which is supported with the old ROMMON but also updates to the new ROMMON. There is no separate ROMMON updater. To get to threat defense Version 7.3+, your options are: • Upgrade from threat defense Version 7.1 or 7.2 — use the normal upgrade process. See the appropriate Upgrade Guide. • Reimage from threat defense Version 7.1 or 7.2 — reimage to ASA 9.19+ first, then reimage to threat defense Version 7.3+. See *Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100* and then *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100* in the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide. • Reimage from ASA 9.17 or 9.18 — upgrade to ASA 9.19+ first, then reimage to threat defense Version 7.3+. See the Cisco Secure Firewall ASA Upgrade Guide and then *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100* in the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide. • Reimage from threat defense Version 7.3+ — use the normal reimage process. See *Reimage the System with a New Software Version* in the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense.

Feature	Description
Threat Defense REST API version 6.4 (v6).	The threat defense REST API for software version 7.3 is version 6.4. You can use v6 in the API URLs, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. Note that the URL version path element for 6.4 is the same as all other 6.x versions: v6. 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, log into device manager, then click the more options button (⋮) and choose **API Explorer**. See: Cisco Secure Firewall Threat Defense REST API Guide

New Features in Device Manager Version 7.2

Table 3: Device Manager Features in Version 7.2.x

Feature	Description
Platform Features	
Firepower 1010E.	We introduced the Firepower 1010E, which does not support power over Ethernet (PoE). Minimum threat defense: 7.2.3 See: Cabling for the Firepower 1010
Threat defense virtual for GCP.	You can now use device manager to configure threat defense virtual for GCP. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide

Feature	Description
Network modules for the Secure Firewall 3100.	We introduced these network modules for the Secure Firewall 3100: • 6-port 1G SFP Network Module, SX (multimode) (FPR-X-NM-6X1SX-F) • 6-port 10G SFP Network Module, SR (multimode) (FPR-X-NM-6X10SR-F) • 6-port 10G SFP Network Module, LR (single mode) (FPR-X-NM-6X10LR-F) • 6-port 25G SFP Network Module, SR (multimode) (FPR-X-NM-X25SR-F) • 6-port 25G Network Module, LR (single mode) (FPR-X-NM-6X25LR-F) • 8-port 1G Copper Network Module, RJ45 (copper) (FPR-X-NM-8X1G-F) Minimum threat defense: 7.2.1
Intel Ethernet Network Adapter E810-CQDA2 driver with threat defense virtual for KVM.	We now support the Intel Ethernet Network Adapter E810-CQDA2 driver with threat defense virtual for KVM. Minimum threat defense: 7.2.1 See: Deploy the Threat Defense Virtual on KVM
ISA 3000 support for shutting down.	Support returns for shutting down the ISA 3000. This feature was introducted in Version 7.0.2 but was temporarily deprecated in Version 7.1.
Firewall and IPS Features	
Object-group search is enabled by default for access control.	The CLI configuration command **object-group-search access-control** is now enabled by default for new deployments. If you are configuring the command using FlexConfig, you should evaluate whether that is still needed. If you need to disable the feature, use FlexConfig to implement the **no object-group-search access-control** command. See: Cisco Secure Firewall ASA Series Command Reference
Rule hit counts persist over reboot.	Rebooting a device no longer resets access control rule hit counts to zero. Hit counts are reset only if you actively clear the counters. In addition, counts are maintained by each unit in an HA pair or cluster separately. You can use the **show rule hits** command to see cumulative counters across the HA pair or cluster, or see the counts per node. We modified the following threat defense CLI command: **show rule hits**. See: Examining Rule Hit Counts
VPN Features	

Feature	Description
IPsec flow offload.	On the Secure Firewall 3100, IPsec flows are offloaded by default. After the initial setup of an IPsec site-to-site VPN or remote access VPN security association (SA), IPsec connections are offloaded to the field-programmable gate array (FPGA) in the device, which should improve device performance. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command. See: IPSec Flow Offload
Interface Features	
Breakout port support for the Secure Firewall 3130 and 3140.	You can now configure four 10GB breakout ports for each 40GB interface on the Secure Firewall 3130 and 3140. New/modified screens: **Devices** > **Interfaces** See: Manage the Network Module for the Secure Firewall 3100
Enabling or disabling Cisco Trustsec on an interface.	You can enable or disable Cisco Trustsec on physical, subinterface, EtherChannel, VLAN, Management, or BVI interfaces, whether named or unnamed. By default, Cisco Trustsec is enabled automatically when you name an interface. We added the **Propagate Security Group Tag** attribute to the interface configuration dialog boxes, and the **ctsEnabled** attribute to the various interface APIs. See: Configure Advanced Options
Licensing Features	
Permanent License Reservation Support for ISA 3000.	ISA 3000 now supports Universal Permanent License Reservation for approved customers. See: Applying Permanent Licenses in Air-Gapped Networks
Administrative and Troubleshooting Features	
Ability to force full deployment.	When you deploy changes, the system normally deploys just the changes made since the last successful deployment. However, if you are experiencing problems, you can elect to force a full deployment, which completely refreshes the configuration on the device. We added the **Apply Full Deployment** option to the deployment dialog box. See: Deploying Your Changes

Feature	Description
Automatically update CA bundles.	**Upgrade impact. The system connects to Cisco for something new.** The local CA bundle contains certificates to access several Cisco services. The system now automatically queries Cisco for new CA certificates at a daily system-defined time. Previously, you had to upgrade the software to update CA certificates. You can use the CLI to disable this feature. New/modified CLI commands: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** Version restrictions: This feature is included in Versions 7.0.5+, 7.1.0.3+, and 7.2.4+. It is not supported in earlier 7.0, 7.1, or 7.2 releases. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco. See: Cisco Secure Firewall Threat Defense Command Reference
Threat defense REST API version 6.3 (v6).	The threat defense REST API for software version 7.2 is version 6.3. You can use v6 in the API URLs, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. Note that the URL version path element for 6.3 is the same as 6.0, 6.1, and 6.2: v6. 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, log into device manager, then click the more options button (⋮) and choose **API Explorer**. See: Cisco Secure Firewall Threat Defense REST API Guide

New Features in FDM Version 7.1

Table 4: New and Deprecated Features in FDM Version 7.1

Feature	Description
Platform Features	

Feature	Description
Secure Firewall 3100.	We introduced the Secure Firewall 3110, 3120, 3130, and 3140. You can hot swap a network module of the same type while the firewall is powered up without having to reboot; making other module changes requires a reboot. Secure Firewall 3100 25 Gbps interfaces support Forward Error Correction as well as speed detection based on the SFP installed. The SSDs are self-encrypting drives (SEDs), and if you have 2 SSDs, they form a software RAID. Note that the Version 7.1 device manager does not include online help for these devices. See the documentation posted on Cisco.com. New/Modified screens: **Device** > **Interfaces** New/Modified threat defense commands: **configure network speed, configure raid, show raid, show ssd**

Feature	Description
FTDv for AWS instances.	FTDv for AWS adds support for these instances: • c5a.xlarge, c5a.2xlarge, c5a.4xlarge • c5ad.xlarge, c5ad.2xlarge, c5ad.4xlarge • c5d.xlarge, c5d.2xlarge, c5d.4xlarge • c5n.xlarge, c5n.2xlarge, c5n.4xlarge • i3en.xlarge, i3en.2xlarge, i3en.3xlarge • inf1.xlarge, inf1.2xlarge • m5.xlarge, m5.2xlarge, m5.4xlarge • m5a.xlarge, m5a.2xlarge, m5a.4xlarge • m5ad.xlarge, m5ad.2xlarge, m5ad.4xlarge • m5d.xlarge, m5d.2xlarge, m5d.4xlarge • m5dn.xlarge, m5dn.2xlarge, m5dn.4xlarge • m5n.xlarge, m5n.2xlarge, m5n.4xlarge • m5zn.xlarge, m5zn.2xlarge, m5zn.3xlarge • r5.xlarge, r5.2xlarge, r5.4xlarge • r5a.xlarge, r5a.2xlarge, r5a.4xlarge • r5ad.xlarge, r5ad.2xlarge, r5ad.4xlarge • r5b.xlarge, r5b.2xlarge, r5b.4xlarge • r5d.xlarge, r5d.2xlarge, r5d.4xlarge • r5dn.xlarge, r5dn.2xlarge, r5dn.4xlarge • r5n.xlarge, r5n.2xlarge, r5n.4xlarge • z1d.xlarge, z1d.2xlarge, z1d.3xlarge
FTDv for Azure instances.	FTDv for Azure adds support for these instances: • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2
Support ends for the ASA 5508-X and 5516-X. The last supported release is threat defense 7.0.	You cannot install threat defensethreat defense 7.1 on an ASA 5508-X or 5516-X. The last supported release for these models is threat defense 7.0.

Feature	Description
Firewall and IPS Features	
Network Analysis Policy (NAP) configuration for Snort 3.	You can use device manager to configure the Network Analysis Policy (NAP) when running Snort 3. Network analysis policies control traffic preprocessing inspection. Inspectors prepare traffic to be further inspected by normalizing traffic and identifying protocol anomalies. You can select which NAP is used for all traffic, and customize the settings to work best with the traffic in your network. You cannot configure the NAP when running Snort 2. We added the Network Analysis Policy to the **Policies** > **Intrusion** settings dialog box, with an embedded JSON editor to allow direct changes, and other features to let you upload overrides, or download the ones you create.
Manual NAT support for fully-qualified domain name (FQDN) objects as the translated destination.	You can use an FQDN network object, such as one specifying www.example.com, as the translated destination address in manual NAT rules. The system configures the rule based on the IP address returned from the DNS server.
Improved active authentication for identity rules.	You can configure active authentication for identity policy rules to redirect the user's authentication to a fully-qualified domain name (FQDN) rather than the IP address of the interface through which the user's connection enters the device. The FQDN must resolve to the IP address of one of the interfaces on the device. By using an FQDN, you can assign a certificate for active authentication that the client will recognize, thus avoiding the untrusted certificate warning users get when being redirected to an IP address. The certificate can specify the FQDN, a wildcard FQDN, or multiple FQDNs in the Subject Alternate Names (SAN) in the certificate. We added the **Redirect to Host Name** option in the identity policy settings.
VPN Features	
Backup remote peers for site-to-site VPN.	You can configure a site-to-site VPN connection to include remote backup peers. If the primary remote peer is unavailable, the system will try to re-establish the VPN connection using one of the backup peers. You can configure separate pre-shared keys or certificates for each backup peer. Backup peers are supported for policy-based connections only, and are not available for route-based (virtual tunnel interface) connections. We updated the site-to-site VPN wizard to include backup peer configuration.

Feature	Description
Password management for remote access VPN (MSCHAPv2).	You can enable password management for remote access VPN. This allows AnyConnect to prompt the user to change an expired password. Without password management, users must change expired passwords directly with the AAA server, and AnyConnect does not prompt the user to change passwords. For LDAP servers, you can also set a warning period to notify users of upcoming password expiration. We added the Enable Password Management option to the authentication settings for remote access VPN connection profiles.
AnyConnect VPN SAML external browser.	When you use SAML as the primary authentication method for a remote access VPN connection profile, you can elect to have the AnyConnect client use the client's local browser instead of the AnyConnect embedded browser to perform the web authentication. This option enables single sign-on (SSO) between your VPN authentication and other corporate logins. Also choose this option if you want to support web authentication methods, such as biometric authentication, that cannot be performed in the embedded browser. We updated the remote access VPN connection profile wizard to allow you to configure the **SAML Login Experience**.
Administrative and Troubleshooting Features	
Dynamic Domain Name System (DDNS) support for updating fully-qualified domain name (FQDN) to IP address mappings for system interfaces.	**Upgrade impact. Redo FlexConfigs after upgrade.** You can configure DDNS for the interfaces on the system to send dynamic updates to DNS servers. This helps ensure that FQDNs defined for the interfaces resolve to the correct address, making it easier for users to access the system using a hostname rather than an IP address. This is especially useful for interfaces that get their addresses using DHCP, but it is also useful for statically-addressed interfaces. After upgrade, if you had used FlexConfig to configure DDNS, you must redo your configuration using device manager or the threat defense API, and remove the DDNS FlexConfig object from the FlexConfig policy, before you can deploy changes again. If you configure DDNS using device manager, then switch to management center management, the DDNS configuration is retained so that management center can find the system using the DNS name. In device manager, we added the **System Settings** > **DDNS Service** page. In the threat defense API, we added the DDNSService and DDNSInterfaceSettings resources.
The **dig** command replaces the **nslookup** command in the device CLI.	To look up the IP address of a fully-qualified domain name (FQDN) in the device CLI, use the **dig** command. The **nslookup** command has been removed.

Feature	Description
DHCP relay configuration using device manager.	You can use device manager to configure DHCP relay. Using DHCP relay on an interface, you can direct DHCP requests to a DHCP server that is accessible through the other interface. You can configure DHCP relay on physical interfaces, subinterfaces, EtherChannels, and VLAN interfaces. You cannot configure DHCP relay if you configure a DHCP server on any interface. We added the **System Settings** > **DHCP** > **DHCP Relay** page, and moved DHCP Server under the new DHCP heading.
Key type and size for self-signed certificates in device manager.	You can specify the key type and size when generating new self-signed internal and internal CA certificates in device manager. Key types include RSA, ECDSA, and EDDSA. The allowed sizes differ by key type. We now warn you if you upload a certificate whose key size is smaller than the minimum recommended length. There is also a weak key pre-defined search filter to help you find weak certificates, which you should replace if possible.
Usage validation restrictions for trusted CA certificates.	You can specify whether a trusted CA certificate can be used to validate certain types of connections. You can allow, or prevent, validation for SSL server (used by dynamic DNS), SSL client (used by remote access VPN), IPsec client (used by site-to-site VPN), or other features that are not managed by the Snort inspection engine, such as LDAPS. The primary purpose of these options is to let you prevent VPN connections from getting established because they can be validated against a particular certificate. We added **Validation Usage** as a property for trusted CA certificates.
Generating the **admin** password in device manager.	During initial system configuration in device manager, or when you change the **admin** password through device manager, you can now click a button to generate a random 16 character password.
Startup time and tmatch compilation status.	The **show version** command now includes information on how long it took to start (boot) up the system. Note that the larger the configuration, the longer it takes to boot up the system. The new **show asp rule-engine** command shows status on tmatch compilation. Tmatch compilation is used for an access list that is used as an access group, the NAT table, and some other items. It is an internal process that can consume CPU resources and impact performance while in progress, if you have very large ACLs and NAT tables. Compilation time depends on the size of the access list, NAT table, and so forth.
Enhancements to **show access-list element-count** output.	The output of the **show access-list element-count** command has been enhanced. When used with object-group search enabled, the output includes details about the number of object groups in the element count. In addition, the **show tech-support** output now includes the output from **show access-list element-count** and **show asp rule-engine**.

Feature	Description
Use device manager to configure the threat defense for management by a management center.	When you perform initial setup using device manager, all interface configuration completed in device manager is retained when you switch to management center for management, in addition to the Management and management center access settings. Note that other default configuration settings, such as the access control policy or security zones, are not retained. When you use the threat defense CLI, only the Management and management center access settings are retained (for example, the default inside interface configuration is not retained). After you switch to management center, you can no longer use device manager to manage the threat defense. New/Modified screens: **System Settings** > **Management Center**
Automatically update CA bundles.	**Upgrade impact. The system connects to Cisco for something new.** The local CA bundle contains certificates to access several Cisco services. The system now automatically queries Cisco for new CA certificates at a daily system-defined time. Previously, you had to upgrade the software to update CA certificates. You can use the CLI to disable this feature. New/modified CLI commands: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** Version restrictions: This feature is included in Versions 7.0.5+, 7.1.0.3+, and 7.2.4+. It is not supported in earlier 7.0, 7.1, or 7.2 releases. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco. See: Cisco Secure Firewall Threat Defense Command Reference
FTD REST API version 6.2 (v6).	The threat defense REST API for software version 7.1 is version 6.2. You can use v6 in the API URLs, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. Note that the URL version path element for 6.2 is the same as 6.0/1: v6. 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, log into device manager, then click the more options button (⋮) and choose **API Explorer**.

New Features in FDM Version 7.0

Table 5: New and Deprecated Features in FDM Version 7.0

Feature	Description
Platform Features	

Feature	Description
FTDv for HyperFlex and Nutanix.	We introduced FTDv for Cisco HyperFlex and Nutanix Enterprise Cloud.
FTDv for VMware vSphere/VMware ESXi 7.0.	You can now deploy FTDv on VMware vSphere/VMware ESXi 7.0. Note that Version 7.0 also discontinues support for VMware 6.0. Upgrade the hosting environment to a supported version before you upgrade the FTD.
New default password for the threat defense virtual on AWS.	On AWS, the default admin password for the threat defense virtual is the AWS Instance ID, unless you define a default password with user data (**Advanced Details** > **User Data**) during the initial deployment.
ISA 3000 support for shutting down.	In Version 7.0.2+, you can shut down the ISA 3000; previously, you could only reboot the device. In Version 7.0.5+, when you shut down the ISA 3000, the System LED turns off. Wait at least 10 seconds after that before you remove power from the device. Version restrictions: Version 7.1 temporarily deprecates support for this feature. Support returns in Version 7.2.
Firewall and IPS Features	
New Section 0 for system-defined NAT rules.	A new Section 0 has been added to the NAT rule table. This section is exclusively for the use of the system. Any NAT rules that the system needs for normal functioning are added to this section, and these rules take priority over any rules you create. Previously, system-defined rules were added to Section 1, and user-defined rules could interfere with proper system functioning. You cannot add, edit, or delete Section 0 rules, but you will see them in **show nat detail** command output.
Custom intrusion rules for Snort 3.	You can use offline tools to create custom intrusion rules for use with Snort 3, and upload them into an intrusion policy. You can organize custom rules in your own custom rule groups, to make it easy to update them as needed. You can also create the rules directly in device manager, but the rules have the same format as uploaded rules. Device Manager does not guide you in creating the rules. You can duplicate existing rules, including system-defined rules, as a basis for a new intrusion rule. We added support for custom groups and rules to the **Policies** > **Intrusion** page, when you edit an intrusion policy.
Snort 3 new features for device manager-managed systems.	You can now configure the following additional features when using Snort 3 as the inspection engine on an device manager-managed system: • Time-based access control rules. (Threat Defense API only.) • Multiple virtual routers. • The decryption of TLS 1.1 or lower connections using the SSL Decryption policy. • The decryption of the following protocols using the SSL Decryption policy: FTPS, SMTPS, IMAPS, POP3S.

Feature	Description
DNS request filtering based on URL category and reputation.	You can apply your URL filtering category and reputation rules to DNS lookup requests. If the fully-qualified domain name (FQDN) in the lookup request has a category and reputation that you are blocking, the system blocks the DNS reply. Because the user does not receive a DNS resolution, the user cannot complete the connection. Use this option to apply URL category and reputation filtering to non-web traffic. You must have the URL filtering license to use this feature. We added the **Reputation Enforcement on DNS Traffic** option to the access control policy settings.
Smaller VDB for lower memory devices with Snort 2.	**Upgrade impact. Application identification on lower memory devices is affected.** For Version 7.0.6+ devices with Snort 2, for VDB 363+, the system now installs a smaller VDB (also called *VDB lite*) on lower memory devices running Snort 2. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Lower memory devices: ASA-5508-X, ASA-5516-X Version restrictions: The smaller VDB is not supported in all versions. If you upgrade from a supported version to an unsupported version, you cannot install VDB 363+ on lower memory devices running Snort 2. For a list of affected releases, see CSCwd88641.
VPN Features	
Device Manager SSL cipher settings for remote access VPN.	You can define the TLS versions and encryption ciphers to use for remote access VPN connections in device manager. Previously, you needed to use the threat defense API to configure SSL settings. We added the following pages: **Objects** > **SSL Ciphers**; **Device** > **System Settings** > **SSL Settings**.
Support for Diffie-Hellman group 31.	You can now use Diffie-Hellman (DH) group 31 in IKEv2 proposals and policies.
The maximum number of Virtual Tunnel Interfaces on the device is 1024.	The maximum number of Virtual Tunnel Interfaces (VTI) that you can create is 1024. In previous versions, the maximum was 100 per source interface.
IPsec lifetime settings for site-to-site VPN security associations.	You can change the default settings for how long a security association is maintained before it must be re-negotiated. We added the **Lifetime Duration** and **Lifetime Size** options to the site-to-site VPN wizard.
Routing Features	
Virtual router support for the ISA 3000.	You can configure up to 10 virtual routers on an ISA 3000 device.

Feature	Description
Equal-Cost Multi-Path (ECMP) routing.	You can configure ECMP traffic zones to contain multiple interfaces, which lets traffic from an existing connection exit or enter the threat defense device on any interface within the zone. This capability allows Equal-Cost Multi-Path (ECMP) routing on the threat defense device as well as external load balancing of traffic to the threat defense device across multiple interfaces. ECMP traffic zones are used for routing only. They are not the same as security zones. We added the **ECMP Traffic Zones** tab to the Routing pages. In the threat defense API, we added the ECMPZones resources.
Interface Features	
New default inside IP address.	The default IP address for the inside interface is being changed to **192.168.95.1** from 192.168.1.1 to avoid an IP address conflict when an address on 192.168.1.0/24 is assigned to the outside interface using DHCP.
Default outside IP address now has IPv6 autoconfiguration enabled; new default IPv6 DNS server for Management.	The default configuration on the outside interface now includes IPv6 autoconfiguration, in addition to the IPv4 DHCP client. The default Management DNS servers now also include an IPv6 server: 2620:119:35::35.
EtherChannel support for the ISA 3000.	You can now use device manager to configure EtherChannels on the ISA 3000. New/modified screens: **Devices** > **Interfaces** > **EtherChannels**
Licensing Features	
Performance-Tiered Licensing for threat defense virtual.	The threat defense virtual now supports performance-tiered Smart Licensing based on throughput requirements and RA VPN session limits. When the threat defense virtual is licensed with one of the available performance licenses, two things occur. First, a rate limiter is installed that limits the device throughput to a specified level. Second, the number of VPN sessions is capped to the level specified by the license.
Administrative and Troubleshooting Features	

Feature	Description
DHCP relay configuration using the threat defense API.	**Upgrade impact. Can prevent post-upgrade deploy.** You can use the threat defense API to configure DHCP relay. Using DHCP relay on an interface, you can direct DHCP requests to a DHCP server that is accessible through the other interface. You can configure DHCP relay on physical interfaces, subinterfaces, EtherChannels, and VLAN interfaces. You cannot configure DHCP relay if you configure a DHCP server on any interface. Note that if you used FlexConfig in prior releases to configure DHCP relay (the **dhcprelay** command), you must re-do the configuration using the API, and delete the FlexConfig object, after you upgrade. We added the following model to the threat defense API: dhcprelayservices
Faster bootstrap processing and early login to device manager.	The process to initially bootstrap an device manager-managed system has been improved to make it faster. Thus, you do not need to wait as long after starting the device to log into device manager. In addition, you can now log in while the bootstrap is in progress. If the bootstrap is not complete, you will see status information on the process so you know what is happening on the device.
Improved CPU usage and performance for many-to-one and one-to-many connections.	The system no longer creates local host objects and locks them when creating connections, except for connections that involve dynamic NAT/PAT and scanning threat detection and host statistics. This improves performance and CPU usage in situations where many connections are going to the same server (such as a load balancer or web server), or one endpoint is making connections to many remote hosts. We changed the following commands: **clear local-host** (deprecated), **show local-host**
Upgrade readiness check for device manager-managed devices.	You can run an upgrade readiness check on an uploaded threat defense upgrade package before attempting to install it. The readiness check verifies that the upgrade is valid for the system, and that the system meets other requirements needed to install the package. Running an upgrade readiness check helps you avoid failed installations. A link to run the upgrade readiness check was added to the **System Upgrade** section of the **Device** > **Updates** page.

Feature	Description
Automatically update CA bundles.	**Upgrade impact. The system connects to Cisco for something new.** The local CA bundle contains certificates to access several Cisco services. The system now automatically queries Cisco for new CA certificates at a daily system-defined time. Previously, you had to upgrade the software to update CA certificates. You can use the CLI to disable this feature. New/modified CLI commands: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** Version restrictions: This feature is included in Versions 7.0.5+, 7.1.0.3+, and 7.2.4+. It is not supported in earlier 7.0, 7.1, or 7.2 releases. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco. See: Cisco Secure Firewall Threat Defense Command Reference
FTD REST API version 6.1 (v6).	The threat defense REST API for software version 7.0 is version 6.1 You can use v6 in the API URLs, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. Note that the URL version path element for 6.1 is the same as 6.0: v6. 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, log into device manager, then click the more options button (⋮) and choose **API Explorer**.

New Features in FDM Version 6.7

Table 6: New and Deprecated Features in FDM Version 6.7

Feature	Description
Platform Features	
Support ends for the ASA 5525-X, 5545-X, and 5555-X. The last supported release is threat defense 6.6.	You cannot install threat defense 6.7 on an ASA 5525-X, 5545-X, or 5555-X. The last supported release for these models is threat defense 6.6.
Firewall and IPS Features	

Feature	Description
TLS server identity discovery for access control rule matching.	TLS 1.3 certificates are encrypted. For traffic encrypted with TLS 1.3 to match access rules that use application or URL filtering, the system must decrypt the TLS 1.3 certificate. We recommend that you enable **TLS Server Identity Discovery** to ensure encrypted connections are matched to the right access control rule. The setting decrypts the certificate only; the connection remains encrypted. We added the **Access Control Settings** (⚙) button and dialog box to the **Policy** > **Access Control** page.
External trusted CA certificate groups.	You can now customize the list of trusted CA certificates used by the SSL decryption policy. By default, the policy uses all system-defined trusted CA certificates, but you can create a custom group to add more certificates, or replace the default group with your own, more limited, group. We added certificate groups to the **Objects** > **Certificates** page, and modified the SSL decryption policy settings to allow the selection of certificate groups.
Active Directory realm sequences for passive identity rules.	You can create a realm sequence, which is an ordered list of Active Directory (AD) servers and their domains, and use them in a passive authentication identity rule. Realm sequences are useful if you support more than one AD domain and you want to do user-based access control. Instead of writing separate rules for each AD domain, you can write a single rule that covers all of your domains. The ordering of the AD realms within the sequence is used to resolve identity conflicts if any arise. We added the AD realm sequence object on the **Objects** > **Identity Sources** page, and the ability to select the object as a realm in a passive authentication identity rule. In the threat defense API, we added the **RealmSequence** resource, and in the **IdentityRule** resource, we added the ability to select a realm sequence object as the realm for a rule that uses passive authentication as the action.
FDM support for Trustsec security group tag (SGT) group objects and their use in access control rules.	In threat defense 6.5, support was added to the threat defense API to configure SGT group objects and use them as matching criteria in access control rules. In addition, you could modify the ISE identity object to listen to the SXP topic published by ISE. Now, you can configure these features directly in FDM. We added a new object, SGT groups, and updated the access control policy to allow their selection and display. We also modified the ISE object to include the explicit selection of topics to subscribe to.

Feature	Description
Snort 3.0 support.	For new systems, Snort 3.0 is the default inspection engine. If you upgrade to 6.7 from an older release, Snort 2.0 remains the active inspection engine, but you can switch to Snort 3.0. For this release, Snort 3.0 does not support virtual routers, time-based access control rules, or the decryption of TLS 1.1 or lower connections. Enable Snort 3.0 only if you do not need these features. You can freely switch back and forth between Snort 2.0 and 3.0, so you can revert your change if needed. Traffic will be interrupted whenever you switch versions. We added the ability to switch Snort versions to the **Device** > **Updates** page, in the **Intrusion Rules** group. In the threat defense API, we added the IntrusionPolicy resource action/toggleinspectionengine. In addition, there is a new audit event, Rules Update Event, that shows which intrusion rules were added, deleted, or changed in a Snort 3 rule package update.
Custom intrusion policies for Snort 3.	You can create custom intrusion policies when you are using Snort 3 as the inspection engine. In comparison, you could use the pre-defined policies only if you use Snort 2. With custom intrusion policies, you can add or remove groups of rules, and change the security level at the group level to efficiently change the default action (disabled, alert or drop) of the rules in the group. Snort 3 intrusion policies give you more control over the behavior of your IPS/IDS system without the need to edit the base Cisco Talos-provided policies. We changed the **Policies** > **Intrusion** page to list intrusion policies. You can create new ones, and view or edit existing policies, including adding/removing groups, assigning security levels, and changing the action for rules. You can also select multiple rules and change their actions. In addition, you can select custom intrusion policies in access control rules.
Multiple syslog servers for intrusion events.	You can configure multiple syslog servers for intrusion policies. Intrusion events are sent to each syslog server. We added the ability to select multiple syslog server objects to the intrusion policy settings dialog box.
URL reputation matching can include sites with unknown reputations.	When you configure URL category traffic-matching criteria, and select a reputation range, you can include URLs with unknown reputation in the reputation match. We added the **Include Sites with Unknown Reputation** check box to the URL reputation criteria in access control and SSL decyption rules.
VPN Features	

Feature	Description
Virtual Tunnel Interface (VTI) and route-based site-to-site VPN.	You can now create route-based site-to-site VPNs by using a Virtual Tunnel Interface as the local interface for the VPN connection profile. With route-based site-to-site VPN, you manage the protected networks in a given VPN connection by simply changing the routing table, without altering the VPN connection profile at all. You do not need to keep track of remote networks and update the VPN connection profile to account for these changes. This simplifies VPN management for cloud service providers and large enterprises. We added the **Virtual Tunnel Interfaces** tab to the Interface listing page, and updated the site-to-site VPN wizard so that you can use a VTI as the local interface.
Threat Defense API support for Hostscan and Dynamic Access Policy (DAP) for remote access VPN connections.	You can upload Hostscan packages and the Dynamic Access Policy (DAP) rule XML file, and configure DAP rules to create the XML file, to control how group policies are assigned to remote users based on attributes related to the status of the connecting endpoint. You can use these features to perform Change of Authorization if you do not have Cisco Identity Services Engine (ISE). You can upload Hostscan and configure DAP using the threat defense API only; you cannot configure them using FDM. See the AnyConnect documentation for information about Hostscan and DAP usage. We added or modified the following threat defense API object models: dapxml, hostscanpackagefiles, hostscanxmlconfigs, ravpns.
Enabling certificate revocation checking for external CA certificates.	You can use the threat defense API to enable certificate revocation checking on a particular external CA certificate. Revocation checking is particularly useful for certificates used in remote access VPN. You cannot configure revocation checking on a certificate using FDM, you must use the threat defense API. We added the following attributes to the ExternalCACertificate resource: revocationCheck, crlCacheTime, oscpDisableNonce.
Support removed for less secure Diffie-Hellman groups, and encryption and hash algorithms.	**Upgrade impact. Can prevent post-upgrade deploy.** The following features were deprecated in 6.6 and they are now removed. If you are still using them in IKE proposals or IPsec policies, you must replace them after upgrade before you can deploy any configuration changes. We recommend that you change your VPN configuration prior to upgrade to supported DH and encryption algorithms to ensure the VPN works correctly. • Diffie-Hellman groups: 2, 5, and 24. • Encryption algorithms for users who satisfy export controls for strong encryption: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continues to be supported (and is the only option) for users who do not satisfy export controls. • Hash algorithms: MD5.

Feature	Description
Custom port for remote access VPN.	You can configure the port used for remote access VPN (RA VPN) connections. If you need to connect to FDM on the same interface used for RA VPN, you can change the port number for RA VPN connections. FDM uses port 443, which is also the default RA VPN port. We updated the global settings step of the RA VPN wizard to include port configuration.
SAML Server support for authenticating remote access VPN.	You can configure a SAML 2.0 server as the authentication source for a remote access VPN. Following are the supported SAML servers: Duo. We added SAML server as an identity source on the **Objects** > **Identity Sources** page, and updated remote access VPN connection profiles to allow its use.
Threat Defense API Support for AnyConnect module profiles.	You can use the threat defense API to upload module profiles used with AnyConnect, such as AMP Enabler, ISE Posture, or Umbrella. You must create these profiles using the offline profile editors that you can install from the AnyConnect profile editor package. We added the anyConnectModuleType attribute to the AnyConnectClientProfile model. Although you can initially create AnyConnect Client Profile objects that use module profiles, you will still need to use the API to modify the objects created in FDM to specify the correct module type.
Routing Features	
EIGRP support using Smart CLI.	**Upgrade impact. Can prevent post-upgrade deploy.** In previous releases, you configured EIGRP in the Advanced Configuration pages using FlexConfig. Now, you configure EIGRP using Smart CLI directly on the Routing page. If you configured EIGRP using FlexConfig, when you upgrade to release 6.7, you must remove the FlexConfig object from the FlexConfig policy, and then recreate your configuration in the Smart CLI object. You can retain your EIGRP FlexConfig object for reference until you have completed the Smart CLI updates. Your configuration is not automatically converted. We added the EIGRP Smart CLI object to the Routing pages.
Interface Features	

Feature	Description
ISA 3000 hardware bypass persistence.	You can now enable hardware bypass for ISA 3000 interface pairs with the persistence option: after power is restored, hardware bypass remains enabled until you manually disable it. If you enable hardware bypass without persistence, hardware bypass is automatically disabled after power is restored. There may be a brief traffic interruption when hardware bypass is disabled. The persistence option lets you control when the brief interruption in traffic occurs. New/Modified screen: **Device** > **Interfaces** > **Hardware Bypass** > **Hardware Bypass Configuration**
Synchronization between the threat defense operational link state and the physical link state for the Firepower 4100/9300.	The Firepower 4100/9300 chassis can now synchronize the threat defense operational link state with the physical link state for data interfaces. Currently, interfaces will be in an Up state as long as the FXOS admin state is up and the physical link state is up. The threat defense application interface admin state is not considered. Without synchronization from threat defense, data interfaces can be in an Up state physically before the threat defense application has completely come online, for example, or can stay Up for a period of time after you initiate an threat defense shutdown. This feature is disabled by default, and can be enabled per logical device in FXOS. **Note** This feature is not supported for an threat defense with a Radware vDP decorator. New/Modified chassis manager screens: **Logical Devices > Enable Link State** New/Modified FXOS commands: **set link-state-sync enabled**, **show interface expand detail** Supported platforms: Firepower 4100/9300
Firepower 1100 and 2100 SFP interfaces now support disabling auto-negotiation.	You can now configure a Firepower 1100 and 2100 SFP interface to disable auto-negotiation. For 10GB interfaces, you can configure the speed down to 1GB without auto-negotiation; you cannot disable auto-negotiation for an interface with the speed set to 10GB. New/Modified screen: **Device > Interfaces > Edit Interface > Advanced Options > Speed** Supported platforms: Firepower 1100 and 2100
Administrative and Troubleshooting Features	

Feature	Description
Ability to cancel a failed threat defense software upgrade and to revert to the previous release.	If an threat defense major software upgrade fails or is otherwise not functioning correctly, you can revert to the state of the device as it was when you installed the upgrade. We added the ability to revert the upgrade to the System Upgrade panel in FDM. During an upgrade, the FDM login screen shows the upgrade status and gives you the option to cancel or revert in case of upgrade failure. In the threat defense API, we added the CancelUpgrade, RevertUpgrade, RetryUpgrade, and UpgradeRevertInfo resources. In the threat defense CLI, we added the following commands: **show last-upgrade status**, **show upgrade status**, **show upgrade revert-info**, **upgrade cancel**, **upgrade revert**, **upgrade cleanup-revert**, **upgrade retry**.
Custom HTTPS port for FDM/threat defense API access on data interfaces.	You can change the HTTPS port used for FDM or threat defense API access on data interfaces. By changing the port from the default 443, you can avoid conflict between management access and other features, such as remote access VPN, configured on the same data interface. Note that you cannot change the management access HTTPS port on the management interface. We added the ability to change the port to the **Device** > **System Settings** > **Management Access** > **Data Interfaces** page.
Low-touch provisioning for Cisco Defense Orchestrator on Firepower 1000 and 2100 series devices.	If you plan on managing a new threat defense device using Cisco Defense Orchestrator (CDO), you can now add the device without completing the device setup wizard or even logging into FDM. New Firepower 1000 and 2100 series devices are initially registered in the Cisco cloud, where you can easily claim them in CDO. Once in CDO, you can immediately manage the devices from CDO. This low-touch provisioning minimizes the need to interact directly with the physical device, and is ideal for remote offices or other locations where your employees are less experienced working with networking devices. We changed how Firepower 1000 and 2100 series devices are initially provisioned. We also added auto-enrollment to the **System Settings** > **Cloud Services** page, so that you can manually start the process for upgraded devices or other devices that you have previously managed using FDM.

Feature	Description
Threat Defense API support for SNMP configuration.	**Upgrade impact. Can prevent post-upgrade deploy.** You can use the threat defense API to configure SNMP version 2c or 3 on an FDM or CDO managed threat defense device. We added the following API resources: SNMPAuthentication, SNMPHost, SNMPSecurityConfiguration, SNMPServer, SNMPUser, SNMPUserGroup, SNMPv2cSecurityConfiguration, SNMPv3SecurityConfiguration. **Note** If you used FlexConfig to configure SNMP, you must redo your configuration using the threat defense API SNMP resources. The commands for configuring SNMP are no longer allowed in FlexConfig. Simply removing the SNMP FlexConfig object from the FlexConfig policy will allow you to deploy changes; you can then use the object as reference while you use the API to reconfigure the feature.
Maximum backup files retained on the system is reduced from 10 to 3.	The system will retain a maximum of 3 backup files on the system rather than 10. As new backups are created, the oldest backup file is deleted. Please ensure that you download backup files to a different system so that you have the versions required to recover the system in case you need to.
Support ended for Microsoft Internet Explorer.	We no longer test Firepower web interfaces using Microsoft Internet Explorer. We recommend you switch to Google Chrome, Mozilla Firefox, or Microsoft Edge.
Threat Defense API Version backward compatibility.	Starting with threat defense Version 6.7, if an API resource model for a feature does not change between releases, then the threat defense API can accept calls that are based on the older API version. Even if the feature model did change, if there is a logical way to convert the old model to the new model, the older call can work. For example, a v4 call can be accepted on a v5 system. If you use “latest” as the version number in your calls, these “older” calls are interpreted as a v5 call in this scenario, so whether you are taking advantage of backward compatibility depends on how you are structuring your API calls.
Threat Defense REST API version 6 (v6).	The threat defense REST API for software version 6.7 is version 6. You can use v6 in the API URLs, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. 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, log into FDM, then click the more options button (⋮) and choose **API Explorer**.

New Features in FDM Version 6.6

Table 7: New and Deprecated Features in FDM Version 6.6

Feature	Description
Platform Features	
Device Manager support for threat defense virtual for the Amazon Web Services (AWS) Cloud.	You can configure threat defense on threat defense virtual for the AWS Cloud using device manager.
Device Manager for the Firepower 4112.	We introduced threat defense for the Firepower 4112. **Note** Requires FXOS 2.8.1.
e1000 Interfaces on FTDv for VMware.	**Prevents upgrade.** Version 6.6 ends support for e1000 interfaces on FTDv for VMware. You cannot upgrade until you switch to vmxnet3 or ixgbe interfaces. Or, you can deploy a new device. For more information, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.
Firewall and IPS Features	
Ability to enable intrusion rules that are disabled by default.	Each system-defined intrusion policy has a number of rules that are disabled by default. Previously, you could not change the action for these rules to alert or drop. You can now change the action for rules that are disabled by default. We changed the Intrusion Policy page to display all rules, even those that are disabled by default, and allow you to edit the action for these rules.
Intrusion Detection System (IDS) mode for the intrusion policy.	You can now configure the intrusion policy to operate in Intrusion Detection System (IDS) mode. In IDS mode, active intrusion rules issue alerts only, even if the rule action is Drop. Thus, you can monitor or test how an intrusion policy works before you make it an active prevention policy in the network. In device manager, we added an indication of the inspection mode to each intrusion policy on the **Policies** > **Intrusion** page, and an **Edit** link so that you can change the mode. In the threat defense API, we added the inspectionMode attribute to the IntrusionPolicy resource.

Feature	Description
Support for manually uploading Vulnerability Database (VDB), Geolocation Database, and Intrusion Rule update packages.	You can now manually retrieve update packages for VDB, Geolocation Database, and Intrusion Rules, and then upload them from your workstation to the threat defense device using device manager. For example, if you have an air-gapped network, where device manager cannot retrieve updates from the Cisco Cloud, you can now get the update packages you need. We updated the **Device** > **Updates** page to allow you to select and upload a file from your workstation.
threat defense API support for access control rules that are limited based on time.	Using the threat defense API, you can create time range objects, which specify one-time or recurring time ranges, and apply these objects to access control rules. Using time ranges, you can apply an access control rule to traffic during certain times of day, or for certain periods of time, to provide flexibility to network usage. You cannot use device manager to create or apply time ranges, nor does device manager show you if an access control rule has a time range applied to it. The TimeRangeObject, Recurrence, TimeZoneObject, DayLightSavingDateRange, and DayLightSavingDayRecurrence resources were added to the threat defense API. The timeRangeObjects attribute was added to the accessrules resource to apply a time range to the access control rule. In addition, there were changes to the GlobalTimeZone and TimeZone resources.
Object group search for access control policies.	While operating, the threat defense device expands access control rules into multiple access control list entries based on the contents of any network objects used in the access rule. You can reduce the memory required to search access control rules by enabling object group search. With object group search enabled, the system does not expand network objects, but instead searches access rules for matches based on those group definitions. Object group search does not impact how your access rules are defined or how they appear in device manager. It impacts only how the device interprets and processes them while matching connections to access control rules. Object group search is disabled by default. In device manager, you must use FlexConfig to enable the **object-group-search access-control** command.
VPN Features	

Feature	Description
Backup peer for site-to-site VPN. (threat defense API only.)	You can use the threat defense API to add a backup peer to a site-to-site VPN connection. For example, if you have two ISPs, you can configure the VPN connection to fail over to the backup ISP if the connection to the first ISP becomes unavailable. Another main use of a backup peer is when you have two different devices on the other end of the tunnel, such as a primary-hub and a backup-hub. The system would normally establish the tunnel to the primary hub. If the VPN connection fails, the system automatically can re-establish the connection with the backup hub. We updated the threat defense API so that you can specify more than one interface for outsideInterface in the SToSConnectionProfile resource. We also added the BackupPeer resource, and the remoteBackupPeers attribute to the SToSConnectionProfile resource. You cannot configure a backup peer using device manager, nor will the existence of a backup peer be visible in device manager.
Support for Datagram Transport Layer Security (DTLS) 1.2 in remote access VPN.	You can now use DTLS 1.2 in remote access VPN. This can be configured using the threat defense API only, you cannot configure it using device manager. However, DTLS 1.2 is now part of the default SSL cipher group, and you can enable the general use of DTLS using device manager in the AnyConnect attributes of the group policy. Note that DTLS 1.2 is not supported on the ASA 5508-X or 5516-X models. We updated the protocolVersion attribute of the sslcipher resource to accept DTLSV1_2 as an enum value.
Deprecated support for less secure Diffie-Hellman groups, and encryption and hash algorithms.	The following features are deprecated and will be removed in a future release. You should avoid configuring these features in IKE proposals or IPSec policies for use in VPNs. Please transition away from these features and use stronger options as soon as is practical. • Diffie-Hellman groups: 2, 5, and 24. • Encryption algorithms for users who satisfy export controls for strong encryption: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continues to be supported (and is the only option) for users who do not satisfy export controls. • Hash algorithms: MD5.
Routing Features	

Feature	Description
Virtual routers and Virtual Routing and Forwarding (VRF)-Lite.	You can create multiple virtual routers to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device. Virtual routers implement the "light" version of Virtual Routing and Forwarding, or VRF-Lite, which does not support Multiprotocol Extensions for BGP (MBGP). We changed the **Routing** page so you can enable virtual routers. When enabled, the **Routing** page shows a list of virtual routers. You can configure separate static routes and routing processes for each virtual router. We also added the [**vrf** *name* | **all**] keyword set to the following CLI commands, and changed the output to indicate virtual router information where applicable: **clear ospf**, **clear route**, **ping**, **show asp table routing**, **show bgp**, **show ipv6 route**, **show ospf**, **show route**, **show snort counters**. We added the following command: **show vrf**.
OSPF and BGP configuration moved to the Routing pages.	In previous releases, you configured OSPF and BGP in the Advanced Configuration pages using Smart CLI. Although you still configure these routing processes using Smart CLI, the objects are now available directly on the Routing pages. This makes it easier for you to configure processes per virtual router. The OSPF and BGP Smart CLI objects are no longer available on the Advanced Configuration page. If you configured these objects before upgrading to 6.6, you can find them on the Routing page after upgrade.
High Availability Features	
The restriction for externally authenticated users logging into the standby unit of a high availability (HA) pair has been removed.	Previously, an externally-authenticated user could not directly log into the standby unit of an HA pair. The user first needed to log into the active unit, then deploy the configuration, before login to the standby unit was possible. This restriction has been removed. Externally-authenticated users can log into the standby unit even if they never logged into the active unit, so long as they provide a valid username/password.

Feature	Description
Change to how interfaces are handled by the BreakHAStatus resource in the threat defense API.	Previously, you could include the **clearIntfs** query parameter to control the operational status of the interfaces on the device where you break the high availability (HA) configuration. Starting with version 6.6, there is a new attribute, **interfaceOption**, which you should use instead of the clearIntfs query parameter. This attribute is optional when used on the active node, but required when used on a non-active node. You can choose from one of two options: • DISABLE_INTERFACES (the default)—All data interfaces on the standby device (or this device) are disabled. • ENABLE_WITH_STANDBY_IP—If you configured a standby IP address for an interface, the interface on the standby device (or this device) is reconfigured to use the standby address. Any interface that lacks a standby address is disabled. If you use break HA on the active node when the devices are in a healthy active/standby state, this attribute applies to the interfaces on the standby node. In any other state, such as active/active or suspended, the attribute applies to the node on which you initiate the break. If you do use the clearIntfs query parameter, clearIntfs=true will act like interfaceOption = DISABLE_INTERFACES. This means that breaking an active/standby pair with clearIntfs=true will no longer disable both devices; only the standby device will be disabled. When you break HA using device manager, the interface option is always set to DISABLE_INTERFACES. You cannot enable the interfaces with the standby IP address. Use the API call from the API Explorer if you want a different result.
The last failure reason for High Availability problems is now displayed on the High Availability page.	If High Availability (HA) fails for some reason, such as the active device becoming unavailable and failing over to the standby device, the last reason for failure is now shown below the status information for the primary and secondary device. The information includes the UTC time of the event.
Interface Features	
PPPoE support.	You can now configure PPPoE for routed interfaces. PPPoE is not supported on High Availability units. New/Modified screens: **Device** > **Interfaces** > **Edit** > **IPv4 Address** > **Type** > **PPPoE** New/Modified commands: **show vpdn group, show vpdn username, show vpdn session pppoe state**

Feature	Description
Management interface acts as a DHCP client by default.	The Management interface now defaults to obtaining an IP address from DHCP instead of using the 192.168.45.45 IP address. This change makes it easier for you to deploy an threat defense in your existing network. This feature applies to all platforms except for the Firepower 4100/9300 (where you set the IP address when you deploy the logical device), and the threat defense virtual and ISA 3000 (which still use the 192.168.45.45 IP address). The DHCP server on the Management interface is also no longer enabled. You can still connect to the default inside IP address by default (192.168.1.1).
HTTP proxy support for device manager management connections.	You can now configure an HTTP proxy for the management interface for use with device manager connections. All management connections, including manual and scheduled database updates, go through the proxy. We added the **System Settings** > **HTTP Proxy** page to configure the setting. In addition, we added the HTTPProxy resource to the threat defense API.
Set the MTU for the Management interface.	You can now set the MTU for the Management interface up to 1500 bytes. The default is 1500 bytes. New/Modified commands: **configure network mtu, configure network management-interface mtu-management-channel** No modified screens.
Licensing Features	
Smart Licensing and Cloud Services enrollment are now separate, and you can manage your enrollments separately.	You can now enroll for cloud services using your security account rather than your Smart Licensing account. Enrolling using the security account is the recommended approach if you intend to manage the device using Cisco Defense Orchestrator. You can also unregister from cloud services without unregistering from Smart Licensing. We changed how the **System Settings** > **Cloud Services** page behaves, and added the ability to unregister from cloud services. In addition, the Web Analytics feature was removed from the page and you can now find it at **System Settings** > **Web Analytics**. In the threat defense API, the CloudServices resources were modified to reflect the new behavior.

Feature	Description
Support for Permanent License Reservation.	If you have an air-gapped network, where there is no path to the internet, you cannot register directly with the Cisco Smart Software Manager (CSSM) for Smart Licensing. In this situation, you can now get authorization to use Universal Permanent License Reservation (PLR) mode, where you can apply a license that does not need direct communication with CSSM. If you have an air-gapped network, please contact your account representative and ask for authorization to use Universal PLR mode in your CSSM account, and to obtain the necessary licenses. ISA 3000 does not support Universal PLR. We added the ability to switch to PLR mode, and to cancel and unregister a Universal PLR license, to the **Device** > **Smart License** page. In the threat defense API, there are new resources for PLRAuthorizationCode, PLRCode, PLRReleaseCode, PLRRequestCode, and actions for PLRRequestCode, InstallPLRCode, and CancelReservation.
Administrative and Troubleshooting Features	
Device Manager direct support for Precision Time Protocol (PTP) configuration for ISA 3000 devices.	You can use device manager to configure the Precision Time Protocol (PTP) on ISA 3000 devices. PTP is a time-synchronization protocol developed to synchronize the clocks of various devices in a packet-based network. The protocol is designed specifically for industrial, networked measurement and control systems. In previous releases, you had to use FlexConfig to configure PTP. We grouped PTP with NTP on the same System Settings page, and renamed the **System Settings** > **NTP** page to **Time Services**. We also added the PTP resource to the threat defense API.
Trust chain validation for the device manager management web server certificate.	When you configure a non-self-signed certificate for the device manager web server, you now need to include all intermediate certificates, and the root certificate, in the trust chain. The system validates the entire chain. We added the ability to select the certificates in the chain on the **Management Web Server** tab on the **Device** > **System Settings** > **Management Access** page.
Support for encrypting backup files.	You can now encrypt backup files using a password. To restore an encrypted backup, you must supply the correct password. We added the ability to choose whether to encrypt backup files for recurring, scheduled, and manual jobs, and to supply the password on restore, to the **Device** > **Backup and Restore** page. We also added the encryptArchive and encryptionKey attributes to the BackupImmediate and BackupSchedule resources, and encryptionKey to the RestoreImmediate resource in the threat defense API.

Feature	Description
Support for selecting which events to send to the Cisco cloud for use by cloud services.	When you configure the device to send events to the Cisco cloud, you can now select which types of events to send: intrusion, file/malware, and connection. For connection events, you can send all events or just the high-priority events, which are those related to connections that trigger intrusion, file, or malware events, or that match Security Intelligence blocking policies. We changed how the Send Events to the Cisco Cloud Enable button works. The feature is on the **System Settings** > **Cloud Services** page.
threat defense REST API version 5 (v5).	The threat defense REST API for software version 6.6 has been incremented to version 5. You must replace v1/v2/v3/v4 in the API URLs with v5, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. The v5 API includes many new resources that cover all features added in software version 6.6. 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, log into device manager, then click the more options button (⋮) and choose **API Explorer**.

New Features in FDM Version 6.4

Table 8: New and Deprecated Features in FDM Version 6.4

Feature	Description
Firepower 1000 series device configuration.	You can configure threat defense on Firepower 1000 series devices using device manager. Note that you can configure and use the Power over Ethernet (PoE) ports as regular Ethernet ports, but you cannot enable or configure any PoE-related properties.
Hardware bypass for the ISA 3000.	You can now configure hardware bypass for the ISA 3000 on the **Device** > **Interfaces** page. In release 6.3, you needed to configure hardware bypass using FlexConfig. If you are using FlexConfig, please redo the configuring on the Interfaces page and remove the hardware bypass commands from FlexConfig. However, the portion of the FlexConfig devoted to disabling TCP sequence number randomization is still recommended.
Ability to reboot and shut down the system from the device manager CLI Console.	You can now issue the **reboot** and **shutdown** commands through the CLI Console in device manager. Previously, you needed to open a separate SSH session to the device to reboot or shut down the system. You must have Administrator privileges to use these commands.

Feature	Description
External Authentication and Authorization using RADIUS for threat defense CLI Users.	You can use an external RADIUS server to authenticate and authorize users logging into the threat defense CLI. You can give external users config (administrator) or basic (read-only) access. We added the SSH configuration to the **AAA Configuration** tab on the **Device** > **System Settings** > **Management Access** page.
Support for network range objects and nested network group objects.	You can now create network objects that specify a range of IPv4 or IPv6 addresses, and network group objects that include other network groups (that is, nested groups). We modified the network object and network group object Add/Edit dialog boxes to include these features, and modified the various security policies to allow the use of these objects, contingent on whether address specifications of that type make sense within the context of the policy.
Full-text search options for objects and rules.	You can do a full-text search on objects and rules. By searching a policy or object list that has a large number of items, you can find all items that include your search string anywhere within the rule or object. We added a search box to all policies that have rules, and to all pages on the **Objects** list. In addition, you can use the **filter=fts~***search-string* option on GET calls for supported objects in the API to retrieve items based on a full-text search.
Obtaining a list of supported API versions for an device manager-managed threat defense device.	You can use the GET /api/versions (ApiVersions) method to get a list of the API versions that are supported on a device. You can use your API client to communicate and configure the device using commands and syntax valid for any of the supported versions.
Hit counts for access control rules.	You can now view hit counts for access control rules. The hit counts indicate how often connections matched the rule. We updated the access control policy to include hit count information. In the threat defense API, we added the HitCounts resource and the **includeHitCounts** and **filter=fetchZeroHitCounts** options to the GET Access Policy Rules resource.
Site-to-Site VPN enhancements for dynamic addressing and certificate authentication.	You can now configure site-to-site VPN connections to use certificates instead of preshared keys to authenticate the peers. You can also configure connections where the remote peer has an unknown (dynamic) IP address. We added options to the Site-to-Site VPN wizard and the IKEv1 policy object.
Support for RADIUS servers and Change of Authorization in remote access VPN.	You can now use RADIUS servers for authenticating, authorizing, and accounting remote access VPN (RA VPN) users. You can also configure Change of Authentication (CoA), also known as dynamic authorization, to alter a user's authorization after authentication when you use a Cisco ISE RADIUS server. We added attributes to the RADIUS server and server group objects, and made it possible to select a RADIUS server group within an RA VPN connection profile.

Feature	Description
Multiple connection profiles and group policies for remote access VPN.	You can configure more than one connection profile, and create group policies to use with the profiles. We changed the **Device** > **Remote Access VPN** page to have separate pages for connection profiles and group policies, and updated the RA VPN Connection wizard to allow the selection of group policies. Some items that were previously configured in the wizard are now configured in the group policy.
Support for certificate-based, second authentication source, and two-factor authentication in remote access VPN.	You can use certificates for user authentication, and configure secondary authentication sources so that users must authenticate twice before establishing a connection. You can also configure two-factor authentication using RSA tokens or Duo passcodes as the second factor. We updated the RA VPN Connection wizard to support the configuration of these additional options.
Support for IP address pools with multiple address ranges, and DHCP address pools, for remote access VPN.	You can now configure address pools that have more than one address range by selecting multiple network objects that specify subnets. In addition, you can configure address pools in a DHCP server and use the server to provide addresses to RA VPN clients. If you use RADIUS for authorization, you can alternatively configure the address pools in the RADIUS server. We updated the RA VPN Connection wizard to support the configuration of these additional options. You can optionally configure the address pool in the group policy instead of the connection profile.
Active Directory realm enhancements.	You can now include up to 10 redundant Active Directory (AD) servers in a single realm. You can also create multiple realms and delete realms that you no longer need. In addition, the limit for downloading users in a realm is increased to 50,000 from the 2,000 limit in previous releases. We updated the **Objects** > **Identity Sources** page to support multiple realms and servers. You can select the realm in the user criteria of access control and SSL decryption rules, to apply the rule to all users within the realm. You can also select the realm in identity rules and RA VPN connection profiles.
Redundancy support for ISE servers.	When you configure Cisco Identity Services Engine (ISE) as an identity source for passive authentication, you can now configure a secondary ISE server if you have an ISE high availability setup. We added an attribute for the secondary server to the ISE identity object.
File/malware events sent to external syslog servers.	You can now configure an external syslog server to receive file/malware events, which are generated by file policies configured on access control rules. File events use message ID 430004, malware events are 430005. We added the File/Malware syslog server options to the **Device** > **System Settings** > **Logging Settings** page.

Feature	Description
Logging to the internal buffer and support for custom event log filters.	You can now configure the internal buffer as a destination for system logging. In addition, you can create event log filters to customize which messages are generated for the syslog server and internal buffer logging destinations. We added the Event Log Filter object to the **Objects** page, and the ability to use the object on the **Device** > **System Settings** > **Logging Settings** page. The internal buffer options were also added to the **Logging Settings** page.
Certificate for the device manager Web Server.	You can now configure the certificate that is used for HTTPS connections to the device manager configuration interface. By uploading a certificate your web browsers already trust, you can avoid the Untrusted Authority message you get when using the default internal certificate. We added the **Device** > **System Settings** > **Management Access** > **Management Web Server** page.
Cisco Threat Response support.	You can configure the system to send intrusion events to the Cisco Threat Response cloud-based application. You can use Cisco Threat Response to analyze intrusions. We added Cisco Threat Response to the **Device** > **System Settings** > **Cloud Services** page.
Manually upload VDB, GeoDB, and SRU updates.	You can now manually retrieve update packages for VDB, Geolocation Database, and Intrusion Rules, and then upload them from your workstation to the FTD device using FDM. For example, if you have an air-gapped network, where FDM cannot retrieve updates from the Cisco Cloud, you can now get the update packages you need. We updated the **Device > Updates** page to allow you to select and upload a file from your workstation. Minimum FTD: 6.4.0.10. Version restrictions: This feature is not available in Version 6.5. Support returns in Version 6.6.
Smaller VDB for lower memory devices devices.	For VDB 363+, the system now installs a smaller VDB (also called *VDB lite*) on lower memory devices. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Minimum FTD: 6.4.0.17 Lower memory devices: ASA-5508-X, ASA-5515-X, ASA-5516-X, ASA-5525-X, ASA-5545-X Version restrictions: The smaller VDB is not supported in all versions. If you upgrade from a supported version to an unsupported version, you cannot install VDB 363+ on lower memory devices. For a list of affected releases, see CSCwd88641.

Feature	Description
Universal Permanent License Reservation (PLR) mode.	If you have an air-gapped network, where there is no path to the internet, you cannot register directly with the Cisco Smart Software Manager (CSSM) for Smart Licensing. In this situation, you can now get authorization to use Universal Permanent License Reservation (PLR) mode, where you can apply a license that does not need direct communication with CSSM. If you have an air-gapped network, please contact your account representative and ask for authorization to use Universal PLR mode in your CSSM account, and to obtain the necessary licenses. We added the ability to switch to PLR mode, and to cancel and unregister a Universal PLR license, to the **Device > Smart License** page. In the FTD API, there are new resources for PLRAuthorizationCode, PLRCode, PLRReleaseCode, PLRRequestCode, and actions for PLRRequestCode, InstallPLRCode, and CancelReservation. Minimum FTD: 6.4.0.10. This feature is temporarily deprecated in Version 6.5 and returns in Version 6.6. If you are running Version 6.4.0.10 or later patch, we recommend you upgrade directly to Version 6.6+.
Default HTTPS server certificates.	**Upgrade impact.** Patching may renew the device's current *default* HTTPS server certificate. Your certificate is set to expire depending on when it is generated, as follows: • 6.5.0.5+: 800 days • 6.5.0 to 6.5.0.4: 3 years • 6.4.0.9 and later patches: 800 days • 6.4.0 to 6.4.0.8: 3 years • 6.3.0 and all patches: 3 years • 6.2.3: 20 years
New syslog fields.	These new syslog fields collectively identify a unique connection event: • Sensor UUID • First Packet Time • Connection Instance ID • Connection Counter These fields also appear in syslogs for intrusion, file, and malware events, allowing connection events to be associated with those events. Minimum FTD: 6.4.0.4

Feature	Description
Threat Defense REST API version 3 (v3).	The threat defense REST API for software version 6.4 has been incremented to version 3. You must replace v1/v2 in the API URLs with v3. The v3 API includes many new resources that cover all features added in software version 6.4. 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 device manager URL to **/#/api-explorer** after logging in.

New Features in FDM Version 6.3

Table 9: New and Deprecated Features in FDM Version 6.3

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.
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 device manager. 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.

Feature	Description
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.
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 device manager Users.	You can use an external RADIUS server to authenticate and authorize users logging into device manager. You can give external users administrative, read-write, or read-only access. Device Manager can support 5 simultaneous logins; the sixth session automatically logs off the oldest session. You can forcefully end a device manager 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.

Feature	Description
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.
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 threat defense virtual). You can use passive mode to evaluate how the threat defense virtual 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.

Feature	Description
Deprecated FlexConfig commands.	We deprecated the following FlexConfig commands: • **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.
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 device manager.
Support for ASA 5506-X, 5506W-X, 5506H-X, and 5512-X removed starting with threat defense 6.3.	You cannot install threat defense 6.3 or subsequent releases on the ASA 5506-X, 5506W-X, 5506H-X, and 5512-X. The final supported threat defense release for these platforms is 6.2.3.
Support for VMware vSphere/VMware ESXi 5.5 removed.	Version 6.3 discontinues support for FTDv on VMware vSphere/VMware ESXi 6.0. Upgrade the hosting environment to a supported version before you upgrade FTD.

Feature	Description
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.
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.
EMS extension support.	**Upgrade impact.** Version 6.3.0 temporarily 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 temporarily do not support the EMS extension during ClientHello negotiation, which enables more secure communications. The EMS extension is defined by RFC 7627. Support returns in Version 6.3.0.1.
threat defense REST API version 2 (v2).	The threat defense 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 device manager URL to **/#/api-explorer** after logging in.

New Features in FDM Version 6.2.3

Table 10: New and Deprecated Features in FDM Version 6.2.3

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 blocking.	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.

Feature	Description
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.
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.
Threat Defense Virtual for Kernel-based Virtual Machine (KVM) hypervisor device configuration.	You can configure threat defense on threat defense virtual for KVM devices using device manager. Previously, only VMware was supported. **Note** You must install a new 6.2.3 image to get device manager support. You cannot upgrade an existing virtual machine from an older version and then switch to device manager.

Feature	Description
Support for VMware ESXi 6.5.	You can now deploy FTDv on VMware vSphere/VMware ESXi 6.5.
ISA 3000 (Cisco 3000 Series Industrial Security Appliances) device configuration.	You can configure threat defense on ISA 3000 devices using 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.	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, 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 device manager.	You can now open a CLI Console from 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.

Feature	Description
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, 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.
EMS extension support.	Both the **Decrypt-Resign** and **Decrypt-Known Key** SSL policy actions now support the EMS extension during ClientHello negotiation, enabling more secure communications. The EMS extension is defined by RFC 7627. **Note** Version 6.2.3.8 was removed from the Cisco Support & Download site on 2019-01-07. Upgrading to Version 6.2.3.9 also enables EMS extension support. Version 6.3.0 discontinues EMS extension support. Support is reintroduced in Version 6.3.0.1. Minimum FTD: Version 6.2.3.8
TLS v1.3 downgrade CLI command for FTD.	A new CLI command allows you to specify when to downgrade TLS v1.3 connections to TLS v1.2. Many browsers use TLS v1.3 by default. If you are using an SSL policy to handle encrypted traffic, and people in your monitored network use browsers with TLS v1.3 enabled, websites that support TLS v1.3 fail to load. For more information, see the **system support** commands in the Cisco Secure Firewall Threat Defense Command Reference. We recommend you use these commands only after consulting with Cisco TAC. Minimum FTD: Version 6.2.3.7

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 device manager policies and settings. 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.
Threat Defense REST API, and an API Explorer.	You can use a REST API to programmatically interact with a threat defense device that you are managing locally through 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 device manager, and then change the path on the URL to /#/api-explorer, for example, https://ftd.example.com/#/api-explorer.

New Features in FDM Version 6.2.2

Table 11: New Features in FDM Version 6.2.2

Feature	Description
Remote access VPN configuration for ASA 5500-X series devices.	You can configure remote access SSL VPN for the AnyConnect client on ASA 5500-X series devices. Configure RA VPN from the **Device** > **Remote Access VPN** group. Configure RA VPN licenses from the **Device** > **Smart License** group.

Feature	Description
Threat Defense Virtual for VMware device configuration.	You can configure threat defense on threat defense virtual for VMware devices using device manager. Other virtual platforms are not supported by device manager. **Note** You must install a new 6.2.2 image to get device manager support. You cannot upgrade an existing virtual machine from an older version and then switch to device manager.

New Features in FDM Version 6.2.1

This release applies to the Firepower 2100 series only.

Table 12: New Features in FDM Version 6.2.1

Feature	Description
Remote access VPN configuration.	You can configure remote access SSL VPN for the AnyConnect client. Configure RA VPN from the **Device** > **Remote Access VPN** group. Configure RA VPN licenses from the **Device** > **Smart License** group.
Firepower 2100 series device configuration.	You can configure threat defense on Firepower 2100 series devices using device manager.

New Features in FDM Version 6.2

Table 13: New Features in FDM Version 6.2

Feature	Description
Cisco Defense Orchestrator (CDO) cloud management.	You can manage the device using the Cisco Defense Orchestrator cloud-based portal. Select **Device** > **System Settings** > **Cloud Management**. For more information on Cisco Defense Orchestrator, see http://www.cisco.com/go/cdo.
Drag and drop for access rules.	You can drag and drop access rules to move them in the rules table.
Upgrade threat defense software through device manager.	You can install software upgrades through device manager. Select **Device** > **Updates**.

Feature	Description
Default configuration changes.	For new or reimaged devices, the default configuration includes significant changes, including: • (ASA 5506-X, 5506W-X, 5506H-X.) Except for the first data interface, and the Wi-Fi interface on an ASA 5506W-X, all other data interfaces on these device models are structured into the "inside" bridge group and enabled. There is a DHCP server on the inside bridge group. You can plug endpoints or switches into any bridged interface and endpoints get addresses on the 192.168.1.0/24 network. • The inside interface IP address is now 192.168.1.1, and a DHCP server is defined on the interface with the address pool 192.168.1.5-192.168.1.254. • HTTPS access is enabled on the inside interface, so you can open device manager through the inside interface at the default address, 192.168.1.1. For the ASA 5506-X models, you can do this through any inside bridge group member interface. • The management port hosts a DHCP server for the 192.168.45.0/24 network. You can plug a workstation directly into the management port, get an IP address, and open device manager to configure the device. • The OpenDNS public DNS servers are now the default DNS servers for the management interface. Previously, there were no default DNS servers. You can configure different DNS servers during device setup. • The default gateway for the management IP address is to use the data interfaces to route to the Internet. Thus, you do not need to wire the Management physical interface to a network.

Feature	Description
Management interface and access changes.	Several changes to how the management address, and access to device manager, works: • You can now open data interfaces to HTTPS (for device manager) and SSH (for CLI) connections. You do not need a separate management network, or to connect the Management/Diagnostic physical port to the inside network, to manage the device. Select **Device** > **System Settings** > **Management Access List**. • The system can obtain system database updates through the gateway for the outside interface. You do not need to have an explicit route from the management interface or network to the Internet. The default is to use internal routes through the data interfaces. However, you can set a specific gateway if you prefer to use a separate management network. Select **Device** > **System Settings** > **Management Interface**. • You can use device manager to configure the management interface to obtain its IP address through DHCP. Select **Device** > **System Settings** > **Management Interface**. • You can configure a DHCP server on the management address if you configure a static address. Select **Device** > **System Settings** > **Management Interface**.
Miscellaneous user interface changes.	The following are notable changes to the device manager user interface. • **Device** main menu item. In previous releases, this menu item was the host name of your device. Also, the page opened is called Device Summary instead of Device Dashboard. • You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface. • **Device** > **System Settings** > **Cloud Preferences** is now called **Device** > **System Settings** > **URL Filtering Preferences**. • The **System Settings** > **DHCP Server** page is now organized on two tabs, with the table of DHCP servers separated from the global parameters.
Site-to-site VPN connections.	You can configure site-to-site virtual private network (VPN) connections using preshared keys. You can configure IKEv1 and IKEv2 connections.

Feature	Description
Integrated Routing and Bridging support.	Integrated Routing and Bridging provides the ability to route between a bridge group and a routed interface. A bridge group is a group of interfaces that the threat defense device bridges instead of routes. The threat defense device is not a true bridge in that the threat defense device continues to act as a firewall: access control between interfaces is controlled, and all of the usual firewall checks are in place. This feature lets you configure bridge groups and to route between bridge groups and between a bridge group and a routed interface. The bridge group participates in routing by using a Bridge Virtual Interface (BVI) to act as a gateway for the bridge group. Integrated Routing and Bridging provides an alternative to using an external Layer 2 switch if you have extra interfaces on the threat defense device to assign to the bridge group. The BVI can be a named interface and can participate separately from member interfaces in some features, such as DHCP server, where you configure other features on bridge group member interfaces, such as NAT and access control rules. Select **Device** > **Interfaces** to configure a bridge group.

New Features in FDM Version 6.1

Table 14: New Features in FDM Version 6.1.0

Feature	Description
Supported devices.	You can manage the following device types using Firepower Device Manager: • ASA 5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X • ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X
Supported firewall mode.	You can configure devices running in routed mode only. Transparent mode is not supported.
Supported interface types and modes.	You can configure routed interfaces only; you cannot configure inline, inline tap, or passive interfaces. In addition, you can configure physical and sub-interfaces only. You cannot configure Etherchannel or redundant interfaces. You also cannot configure PPPoE.

Feature	Description

Security Policies.	You can configure the following types of security policy:
	• Access control—Determine which connections are allowed to pass through the device. You can perform the following types of access control:
	  • Filtering on security zone, IP address, geolocation, protocol and port.
	  • Filtering on user name and user group.
	  • Application filtering.
	  • URL category, reputation, and individual URL filtering.
	  • Intrusion policies, preventing threats.
	  • File policies, preventing malware.
	• Identity policies—Determine which user is associated with an IP address. The system supports active authentication only, not passive authentication.
	• Network address translation—Convert between internal and external addresses. Most NAT features are supported, except for PAT pools.

Routing.	You can configure static routes. Dynamic routing protocols are not support.
System monitoring and syslog.	Firepower Device Manager includes an event viewer so that you can view recent connection events. You can also configure an external syslog server to collect events for longer term analysis. There are also many dashboards that provide statistical information about the system and the traffic that is passing through the system.
Management interface configuration.	You can configure the management address and interface from Firepower Device Manager; you do not need to use the CLI. You can configure the system hostname, management IP address and gateway, DNS servers, NTP servers, and access rules to limit the IP addresses that can access the CLI or Firepower Device Manager.

Feature	Description
Scheduling updates.	You can control how often system databases are updated. • **Device** main menu item. In previous releases, this menu item was the host name of your device. Also, the page opened is called Device Summary instead of Device Dashboard. • You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface. • **Device** > **System Settings** > **Cloud Preferences** is now called **Device** > **System Settings** > **URL Filtering Preferences**. • The **System Settings** > **DHCP Server** page is now organized on two tabs, with the table of DHCP servers separated from the global parameters.
Backup and restore.	You can back up the system and restore it from Firepower Device Manager.
Troubleshooting file.	You can generate a troubleshooting file from Firepower Device Manager when working with Cisco Technical Support.

Release Dates

Table 15: Version 7.4 Dates

Version	Build	Date	Platforms
7.4.1	172	2023-12-13	All
7.4.0	81	2023-09-07	Management center Secure Firewall 4200 series

Table 16: Version 7.3 Dates

Version	Build	Date	Platforms
7.3.1.1	83	2023-08-24	All
7.3.1	19	2023-03-14	All
7.3.0	69	2022-11-29	All

Table 17: Version 7.2 Dates

Version	Build	Date	Platforms
7.2.6	167	2024-03-19	All

Version	Build	Date	Platforms
7.2.5.1	29	2023-11-14	All
7.2.5	208	2023-07-27	All
7.2.4.1	43	2023-07-27	All
7.2.4	169	2023-05-10	Management center
	165	2023-05-03	Devices
7.2.3.1	13	2023-04-18	Management center
7.2.3	77	2023-02-27	All
7.2.2	54	2022-11-29	All
7.2.1	40	2022-10-03	All
7.2.0.1	12	2022-08-10	All
7.2.0	82	2022-06-06	All

Table 18: Version 7.1 Dates

Version	Build	Date	Platforms
7.1.0.3	108	2022-03-15	All
7.1.0.2	28	2022-08-03	FMC/FMCv Secure Firewall 3100 series
7.1.0.1	28	2022-02-24	FMC/FMCv All devices except Secure Firewall 3100 series
7.1.0	90	2021-12-01	All

Table 19: Version 7.0 Dates

Version	Build	Date	Platforms
7.0.6.1	36	2023-11-13	All
7.0.6	236	2023-07-18	All
7.0.5.1	5	2023-04-26	NGIPSv For devices with security certifications compliance enabled (CC/UCAPL mode). Use with a Version 7.0.5 FMC.
7.0.5	72	2022-11-17	All
7.0.4	55	2022-08-10	All

Version	Build	Date	Platforms
7.0.3	37	2022-06-30	All
7.0.2.1	10	2022-06-27	All
7.0.2	88	2022-05-05	All
7.0.1.1	11	2022-02-17	All
7.0.1	84	2021-10-07	All
7.0.0.1	15	2021-07-15	All
7.0.0	94	2021-05-26	All

Table 20: Version 6.7 Dates

Version	Build	Date	Platforms
6.7.0.3	105	2022-02-17	All
6.7.0.2	24	2021-05-11	All
6.7.0.1	13	2021-03-24	All
6.7.0	65	2020-11-02	All

Table 21: Version 6.6 Dates

Version	Build	Date	Platforms
6.6.7.1	42	2023-01-26	All
6.6.7	223	2022-07-14	All
6.6.5.2	14	2022-03-24	All
6.6.5.1	15	2021-12-06	All
6.6.5	81	2021-08-03	All
6.6.4	64	2021-04-29	Firepower 1000 series
	59	2021-04-26	FMC/FMCv All devices except Firepower 1000 series
6.6.3	80	2020-03-11	All
6.6.1	91	2020-09-20	All
	90	2020-09-08	—
6.6.0.1	7	2020-07-22	All

Version	Build	Date	Platforms
6.6.0	90	2020-05-08	Firepower 4112
		2020-04-06	FMC/FMCv All devices except Firepower 4112

Table 22: Version 6.5 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.5.0.5	95	2021-02-09	All	—
6.5.0.4	57	2020-03-02	All	—
6.5.0.3	30	2020-02-03	No longer available.	—
6.5.0.2	57	2019-12-19	All	—
6.5.0.1	35	2019-11-20	No longer available.	—
6.5.0	123	2020-02-03	FMC/FMCv	FMC/FMCv
	120	2019-10-08	—	—
	115	2019-09-26	All devices	All devices

Table 23: Version 6.4 Dates

Version	Build	Date	Platforms
6.4.0.17	26	2023-09-28	All
6.4.0.16	50	2022-11-21	All
6.4.0.15	26	2022-05-31	All
6.4.0.14	67	2022-02-18	All
6.4.0.13	57	2021-12-02	All
6.4.0.12	112	2021-05-12	All
6.4.0.11	11	2021-01-11	All
6.4.0.10	95	2020-10-21	All
6.4.0.9	62	2020-05-26	All
6.4.0.8	28	2020-01-29	All
6.4.0.7	53	2019-12-19	All
6.4.0.6	28	2019-10-16	No longer available.

Version	Build	Date	Platforms
6.4.0.5	23	2019-09-18	All
6.4.0.4	34	2019-08-21	All
6.4.0.3	29	2019-07-17	All
6.4.0.2	35	2019-07-03	FMC/FMCv FTD/FTDv, except Firepower 1000 series
	34	2019-06-27	—
		2019-06-26	Firepower 7000/8000 series ASA FirePOWER NGIPSv
6.4.0.1	17	2019-06-27	FMC 1600, 2600, 4600
		2019-06-20	Firepower 4115, 4125, 4145 Firepower 9300 with SM-40, SM-48, and SM-56 modules
		2019-05-15	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv Firepower 2110, 2120, 2130, 2140 Firepower 4110, 4120, 4140, 4150 Firepower 9300 with SM-24, SM-36, and SM-44 modules ASA 5508-X, 5515-X, 5516-X, 5525-X, 5545-X, 5555-X ASA 5585-X-SSP-10, -20, -40, -60 ISA 3000 FTDv Firepower 7000/8000 series NGIPSv

Version	Build	Date	Platforms
6.4.0	113	2020-03-03	FMC/FMCv
	102	2019-06-20	Firepower 4115, 4125, 4145 Firepower 9300 with SM-40, SM-48, and SM-56 modules
		2019-06-13	Firepower 1010, 1120, 1140
		2019-04-24	Firepower 2110, 2120, 2130, 2140 Firepower 4110, 4120, 4140, 4150 Firepower 9300 with SM-24, SM-36, and SM-44 modules ASA 5508-X, 5515-X, 5516-X, 5525-X, 5545-X, 5555-X ASA 5585-X-SSP-10, -20, -40, -60 ISA 3000 FTDv Firepower 7000/8000 series NGIPSv

Table 24: Version 6.3 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.3.0.5	35	2019-11-18	Firepower 7000/8000 series NGIPSv	—
	34	2019-11-18	FMC/FMCv All FTD devices ASA FirePOWER	—
6.3.0.4	44	2019-08-14	All	—
6.3.0.3	77	2019-06-27	FMC 1600, 2600, 4600	—
		2019-05-01	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices	—
6.3.0.2	67	2019-06-27	FMC 1600, 2600, 4600	—
		2019-03-20	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices	—

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.3.0.1	85	2019-06-27	FMC 1600, 2600, 4600	—
		2019-02-18	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices	—
6.3.0	85	2019-01-22	Firepower 4100/9300	Firepower 4100/9300
	84	2018-12-18	FMC/FMCv ASA FirePOWER	—
	83	2019-06-27	—	FMC 1600, 2600, 4600
		2018-12-03	All FTD devices except Firepower 4100/9300 Firepower 7000/8000 NGIPSv	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices except Firepower 4100/9300

Table 25: Version 6.2.3 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.2.3.18	50	2022-02-16	All	—
6.2.3.17	30	2021-06-21	All	—
6.2.3.16	59	2020-07-13	All	—
6.2.3.15	39	2020-02-05	FTD/FTDv	—
	38	2019-09-18	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv	—
6.2.3.14	41	2019-07-03	All	—
	36	2019-06-12	All	—
6.2.3.13	53	2019-05-16	All	—
6.2.3.12	80	2019-04-17	All	—
6.2.3.11	55	2019-03-17	All	—
	53	2019-03-13	—	—

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.2.3.10	59	2019-02-07	All	—
6.2.3.9	54	2019-01-10	All	—
6.2.3.8	51	2019-01-02	No longer available.	—
6.2.3.7	51	2018-11-15	All	—
6.2.3.6	37	2018-10-10	All	—
6.2.3.5	53	2018-11-06	FTD/FTDv	—
	52	2018-09-12	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv	—
6.2.3.4	42	2018-08-13	All	—
6.2.3.3	76	2018-07-11	All	—
6.2.3.2	46	2018-06-27	All	—
	42	2018-06-06	—	—
6.2.3.1	47	2018-06-28	All	—
	45	2018-06-21	—	—
	43	2018-05-02	—	—

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.2.3	113	2020-06-01	FMC/FMCv	FMC/FMCv
	111	2019-11-25	—	FTDv: AWS, Azure
	110	2019-06-14	—	—
	99	2018-09-07	—	—
	96	2018-07-26	—	—
	92	2018-07-05	—	—
	88	2018-06-11	—	—
	85	2018-04-09	—	—
	84	2018-04-09	Firepower 7000/8000 series NGIPSv	—
	83	2018-04-02	FTD/FTDv ASA FirePOWER	FTD: Physical platforms FTDv: VMware, KVM Firepower 7000/8000 ASA FirePOWER NGIPSv
	79	2018-03-29	—	—

Table 26: Version 6.2.2 Dates

Version	Build	Date	Platforms
6.2.2.5	57	2018-11-27	All
6.2.2.4	43	2018-09-21	FTD/FTDv
	34	2018-07-09	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
	32	2018-06-15	—
6.2.2.3	69	2018-06-19	All
	66	2018-04-24	—
6.2.2.2	109	2018-02-28	All

Version	Build	Date	Platforms
6.2.2.1	80	2017-12-05	Firepower 2100 series
	78	2017-11-20	—
	73	2017-11-06	FMC/FMCv All devices except Firepower 2100 series
6.2.2	81	2017-09-05	All