



Features and Functionality

This document describes new and deprecated features for Version 7.1, including upgrade impact.

For Cisco Defense Orchestrator (CDO) deployments, see [What's New for Cisco Defense Orchestrator](#).



Important New and deprecated features can require pre- or post-upgrade configuration changes, or even prevent upgrade. If your upgrade skips versions, see those release notes for historical feature information and upgrade impact, or see the appropriate [New Features by Release](#) guide.

- [New Features in FMC Version 7.1, on page 1](#)
- [New Features in FDM Version 7.1, on page 19](#)
- [Intrusion Rules and Keywords, on page 25](#)
- [Deprecated FlexConfig Commands, on page 26](#)

New Features in FMC Version 7.1

Although you can manage older devices with a newer customer-deployed FMC, we recommend you always update your entire deployment. You should assume that new traffic-handling features require the latest release on both the FMC *and* device. Features where devices are not obviously involved (cosmetic changes to the web interface, cloud integrations) may only require the latest version on the FMC, but that is not guaranteed. In the new feature descriptions, we are explicit when version requirements deviate from the standard expectation.

New Features

Table 1: New Features in FMC Version 7.1 Patches

New Feature	Description
<p>Version 7.1.0.3</p> <p>Automatically update CA bundles</p>	<p>Upgrade impact.</p> <p>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.</p> <p>Note This feature is not supported in Version 7.0.0–7.0.4, 7.1.0–7.1.0.2, or 7.2.0–7.2.3. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco.</p> <p>New/modified CLI commands: configure cert-update auto-update, configure cert-update run-now, configure cert-update test, show cert-update</p> <p>For more information, see the Firepower Management Center Command Line Reference in the management center administration guide, and the Cisco Secure Firewall Threat Defense Command Reference.</p>

Table 2: New Features in FMC Version 7.1.0

New Feature	Description
<p>Platform</p>	

New Feature	Description
Secure Firewall 3100	<p>We introduced the Secure Firewall 3110, 3120, 3130, and 3140.</p> <p>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. These devices support up to 8 units for Spanned EtherChannel clustering.</p> <p>Note that the Version 7.1.0 release does not include online help for these devices; new online help is included in Version 7.1.0.2.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Devices > Device Management > Add Cluster • Devices > Device Management > More • Devices > Device Management > Cluster • Devices > Device Management > Chassis Operations • Devices > Device Management > Interfaces > edit physical interface > Hardware Configuration • Devices > Device Management <p>New/modified FTD CLI commands: configure network speed, configure raid, show raid, show ssd</p>
FMCv300 for AWS FMCv300 for OCI	<p>We introduced the FMCv300 for both AWS and OCI. The FMCv300 can manage up to 300 devices.</p>

New Feature	Description
FTDv for AWS instances.	FTDv for AWS adds support for these instances: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2

New Feature	Description
Use FDM to configure the FTD for management by the FMC.	<p>When you perform initial setup using FDM, all interface configuration completed in FDM is retained when you switch to FMC for management, in addition to the Management and FMC access settings. Note that other default configuration settings, such as the access control policy or security zones, are not retained. When you use the FTD CLI, only the Management and FMC access settings are retained (for example, the default inside interface configuration is not retained).</p> <p>After you switch to FMC, you can no longer use FDM to manage the FTD.</p> <p>New/modified FDM screens: System Settings > Management Center</p>
Device Upgrade	
Revert a successful device upgrade.	<p>You can now revert major and maintenance upgrades to FTD. Reverting returns the software to its state just before the last upgrade, also called a <i>snapshot</i>. If you revert an upgrade after installing a patch, you revert the patch as well as the major and/or maintenance upgrade.</p> <p>Important If you think you might need to revert, you must use System (⚙️) > Updates to upgrade FTD. The System Updates page is the only place you can enable the Enable revert after successful upgrade option, which configures the system to save a revert snapshot when you initiate the upgrade. This is in contrast to our usual recommendation to use the wizard on the Devices > Device Upgrade page.</p> <p>This feature is not supported for container instances.</p> <p>Minimum FTD: 7.1</p>
Improvements to the upgrade workflow for clustered and high availability devices.	<p>We made the following improvements to the upgrade workflow for clustered and high availability devices:</p> <ul style="list-style-type: none"> • The upgrade wizard now correctly displays clustered and high availability units as groups, rather than as individual devices. The system can identify, report, and preemptively require fixes for group-related issues you might have. For example, you cannot upgrade a cluster on the Firepower 4100/9300 if you have made unsynced changes on Firepower Chassis Manager. • We improved the speed and efficiency of copying upgrade packages to clusters and high availability pairs. Previously, the FMC copied the package to each group member sequentially. Now, group members can get the package from each other as part of their normal sync process. • You can now specify the upgrade order of data units in a cluster. The control unit always upgrades last.

New Feature	Description
Snort 3 backwards compatibility.	<p>For Snort 3, new features and resolved bugs require that you fully upgrade the FMC <i>and</i> its managed devices. Unlike Snort 2, you cannot update the inspection engine on an older device (for example, Version 7.0) by deploying from a newer FMC (for example, Version 7.1).</p> <p>When you deploy to an older device, the system lists any unsupported configurations and warns you that they will be skipped. We recommend you always update your entire deployment.</p>
Device Management	
Geneve interface support for an FTDv on AWS instances.	<p>Geneve encapsulation support was added to support single-arm proxy for the AWS Gateway Load Balancer (GWLB). The AWS GWLB combines a transparent network gateway (with a single entry and exit point for all traffic) and a load balancer that distributes traffic and scales FTDv to match the traffic demand.</p> <p>This support requires FMC with Snort 3 enabled and is available on the following performance tiers:</p> <ul style="list-style-type: none"> • FTDv20 • FTDv30 • FTDv50 • FTDv100
Single Root I/O Virtualization (SR-IOV) support for FTDv on OCI.	<p>You can now implement Single Root Input/Output Virtualization (SR-IOV) for FTDv on OCI. SR-IOV can provide performance improvements for an FTDv. Mellanox 5 as vNICs are not supported in SR-IOV mode.</p>
LLDP support for the Firepower 1100.	<p>You can now enable Link Layer Discovery Protocol (LLDP) for Firepower 1100 interfaces.</p> <p>New/modified screens: Devices > Device Management > Interfaces > Hardware Configuration > LLDP</p> <p>New/modified commands: show lldp status, show lldp neighbors, show lldp statistics</p> <p>Supported platforms: Firepower 1100 (1120, 1140, and 1150)</p>
Interface auto-negotiation is now set independently from speed and duplex, interface sync improved.	<p>Interface auto-negotiation is now set independently from speed and duplex. Also, when you sync the interfaces in FMC, hardware changes are detected more effectively.</p> <p>New/modified screens: Devices > Device Management > Interfaces > Hardware Configuration > Speed</p> <p>Supported platforms: Firepower 1000/2100, Secure Firewall 3100</p>
Support to specify trusted DNS servers.	<p>You can use FTD platform settings to specify trusted DNS servers for DNS snooping. This helps detect applications on the first packet by mapping domains to IP addresses. By default, trusted DNS servers include those in DNS server objects, and those discovered by dhcp-pool, dhcp-relay, and dhcp-client.</p>

New Feature	Description
Import and export device configurations.	<p>You can export the device-specific configuration, and you can then import the saved configuration for the same device in the following use cases:</p> <ul style="list-style-type: none"> • Moving the device to a different FMC. • Restore an old configuration. • Reregistering a device. <p>New/modified screens: Devices > Device Management > Device > General</p>
High Availability/Scalability	
High availability for: <ul style="list-style-type: none"> • FMCv for AWS • FMCv for OCI 	<p>We now support high availability on FMCv for AWS and FMCv for OCI.</p> <p>In an FTD deployment, you need two identically licensed FMCs, as well as one FTD entitlement for each managed device. For example, to manage 10 FTD devices with an FMCv10 high availability pair, you need two FMCv10 entitlements and 10 FTD entitlements. If you are managing Version 6.5.0–7.0.x Classic devices only (NGIPSv or ASA FirePOWER), you do not need FMCv entitlements.</p> <p>Supported platforms: FMCv10, FMCv25, FMCv300 (not supported for FMCv2)</p>
Autoscale on FTDv for OCI.	<p>We now support autoscaling on FTDv for OCI.</p> <p>The serverless infrastructure in cloud-based deployments allow you to automatically adjust the number of FTDv instances in an autoscale group based on capacity needs. This includes automatic registering/unregistering to and from the managing FMC.</p>
Cluster deployment for firewall changes completes faster.	<p>Cluster deployment for firewall changes now completes faster.</p> <p>Supported platforms: Firepower 4100/9300, Secure Firewall 3100</p>
Clearing routes in a high availability group or cluster.	<p>In previous releases, the clear route command cleared the routing table on the unit only. Now, when operating in a high availability group or cluster, the command is available on the active or control unit only, and clears the routing table on all units in the group or cluster.</p>
NAT	
Manual NAT support for fully-qualified domain name (FQDN) objects as the translated destination.	<p>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.</p>
Routing	

New Feature	Description
BGP configuration to interconnect virtual routers.	<p>You can configure BGP settings to dynamically leak routes among user-defined virtual routers, and between global virtual router and user-defined virtual routers. The import and export routes feature was introduced to exchange routes among the virtual routers by tagging them with route targets and optionally, filtering the matched routes with route maps. This BGP feature is accessible only when you select a user-defined virtual router.</p> <p>New/modified screens: For a selected user-defined virtual router, Devices > Device Management > Routing > BGPv4/v6 > Route Import/Export</p>
BGPv6 support for user-defined virtual routers.	<p>FTD now supports configuring BGPv6 on user-defined virtual routers.</p> <p>New/modified screens: For a selected user-defined virtual router, Devices > Device Management > Routing > BGPv6</p>
Equal-Cost-Multi-Path (ECMP) zone support.	<p>You can now group interfaces in traffic zones and configure Equal-Cost-Multi-Path (ECMP) routing in FMC.</p> <p>ECMP routing was previously supported through FlexConfig policies.</p> <p>New/modified screens: Devices > Device Management > Routing > ECMP</p>
Direct Internet Access/Policy Based Routing	
Direct internet access with policy based routing.	<p>You can now configure policy based routing through the FMC to classify network traffic based on applications and to implement Direct Internet Access (DIA) to send traffic to the internet from a branch deployment. You can define a PBR policy and configure it on ingress interfaces, specifying match criteria and egress interfaces. Network traffic that matches the access control policy is forwarded through the egress interface based on priority or the order as configured in the policy.</p> <p>New/modified screens: New policy page for configuring the policy based routing policy: Devices > Device Management > Routing > Policy Based Routing</p> <p>Supported platforms: FTD</p>
FMC REST API enhancements for direct internet access and policy based routing.	<p>You can use the FMC REST API to configure Direct Internet Access through Policy Based Routing. The following enhancements have been made to the FMC REST API to support this:</p> <ul style="list-style-type: none"> • New APIs were added to enable you to create, view, edit, and delete your Policy Based Routing configuration • New parameters added to existing APIs for Extended Access Control Lists to define applications • New parameters added to existing APIs for device interfaces to define interface priority
Remote Access VPN	
Copy RA VPN policies.	<p>You can now create a new RA VPN policy by copying an existing policy. We added a copy button next to each policy on Devices > VPN > Remote Access.</p>

New Feature	Description
AnyConnect VPN SAML external browser.	<p>You can now configure AnyConnect VPN SAML External Browser to enable additional authentication choices, such as passwordless authentication, WebAuthN, FIDO, SSO, U2F, and an improved SAML experience due to the persistence of cookies. 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 and Yubikeys, that cannot be performed in the embedded browser.</p> <p>We updated the remote access VPN connection profile wizard to allow you to configure the SAML Login Experience.</p>
Multiple trustpoints for SAML identity providers on Microsoft Azure.	<p>You can now add multiple RA VPN trustpoints for SAML identity providers, as required by Microsoft Azure.</p> <p>In a Microsoft Azure network, Azure can support multiple applications for the same Entity ID. Each application (typically mapped to a different tunnel group) requires a unique certificate. This feature enables you to add multiple trustpoints for RA VPN in FTDv for Microsoft Azure.</p>
Site to Site VPN	
VPN filters.	<p>You can now configure site to site VPN filters with rules that determine whether to allow or reject tunneled data packets based on criteria such as source address, destination address, and protocol.</p> <p>The VPN filter is applied to post-decrypted traffic after it exits a tunnel and to pre-encrypted traffic before it enters a tunnel.</p>
Unique local tunnel ID for IKEv2.	<p>You can now configure a Local Tunnel ID per IKEv2 tunnel for both policy-based and route-based Site to Site VPNs. You can configure the local tunnel ID with the FMC web interface or from the REST API.</p> <p>This local tunnel ID configuration enables Umbrella SIG integration with FTD.</p>
Multiple IKE policies.	<p>You can now configure multiple IKE policies for both policy-based and route-based Site to Site VPNs.</p> <p>Multiple IKE policies can be configured through the FMC GUI and the REST API.</p>

New Feature	Description
VPN monitoring dashboard.	<p>Beta.</p> <p>The Site to Site VPN Monitoring Dashboard provides:</p> <ul style="list-style-type: none"> • Visualization of tunnel status distribution across all devices • Visualization of network topology consisting of VPN tunnels • Ability to visually isolate and examine tunnels based on criteria like Topology, Device and Status <p>Note The Site to Site Monitoring Dashboard is a Beta feature and may not work as expected. Do not use it in production environments.</p>
Security Intelligence	
Snort 3 support for Security Intelligence on proxied traffic.	With Snort 3, you can now apply Security Intelligence to HTTP proxy traffic where the IP address is embedded into the HTTP request. For example, when a user uploads a Block list or an Allow list containing IP addresses or networks, the system matches on the destination server IP instead of proxy IP. As a result, traffic to the destination server can be blocked, monitored, or allowed (according to your Security Intelligence configuration).
Intrusion Detection and Prevention	
Snort 3 support for drop, reject, rewrite, and pass rule actions.	<p>Version 7.1 FMCs now support the following intrusion rule actions for FTD devices with Snort 3, including Version 7.0 devices:</p> <ul style="list-style-type: none"> • Drop: Drops the matching packet, but does not block further traffic in this connection. Generates an intrusion event. • Reject: Drops the matching packet and blocks further traffic in this connection. For TCP traffic, sends a TCP reset. For UDP traffic, sends ICMP port unreachable to the source and destination hosts. Generates an intrusion event. • Rewrite: Overwrites the matching packet based on the replace option in the rule. Generates an intrusion event. • Pass: Allows matching packet to pass without further evaluation by any other intrusion rules. Does not generate an intrusion event. <p>To configure these new rule actions, edit the Snort 3 version of an intrusion policy and use the Rule Action drop-down for each rule.</p>
Snort 3 support for TLS-based intrusion rules.	You can now create TLS-based intrusion rules to inspect decrypted TLS traffic with Snort 3. This feature allows Snort 3 intrusion rules to use TLS information.

New Feature	Description
Snort 3 support for inspection of DCE/RPC over SMB2.	<p>Upgrade impact.</p> <p>Version 7.1 with Snort 3 supports DCE/RPC inspection over SMB2.</p> <p>After the first post-upgrade deploy to Snort 3 devices, existing DCE/RPC rules begin inspecting DCE/RPC over SMB2; previously these rules only inspected DCE/RPC over SMB1.</p>
Snort 3 support for intrusion rule recommendations.	<p>Version 7.1 FMCs now support intrusion rule recommendations for FTD devices with Snort 3, including Version 7.0 devices.</p> <p>To configure this feature, edit the Snort 3 version of an intrusion policy and click the Recommendations button (in the left pane, next to All Rules).</p>
Snort 3 support for ssl_version and ssl_state keywords.	<p>Upgrade impact.</p> <p>Version 7.1 with Snort 3 supports the ssl_version and ssl_state intrusion rule keywords.</p> <p>Cisco-provided intrusion policies include active rules using those keywords. You can also create, upload, and deploy custom/third party rules using them. In Version 7.0.x, we supported those keywords with Snort 2 only. With Snort 3, rules with those keywords did not match traffic, and thus could not generate alerts or affect traffic. There was no indication that the rules were not working as expected. After the first post-upgrade deploy to Version 7.1+ Snort 3 devices, existing rules with those keywords can match traffic.</p>
Identity Services and User Control	
Snort 3 captive portal support for interception of HTTP/2 traffic.	<p>You can now intercept and redirect HTTP/2 traffic for user authentication with captive portal.</p> <p>When a redirect is received by the browser, the browser follows the redirect and authenticates with idhttpsd (Apache web server) using the same process as the HTTP/1 captive portal. After authentication, idhttpsd redirects the user back to the original URL.</p>
Snort 3 captive portal support for hostname-based redirect.	<p>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.</p> <p>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.</p> <p>New/modified screens: We added the Redirect to Host Name option in the identity policy settings.</p>
Encrypted Traffic Handling (TLS/SSL)	

New Feature	Description
Advanced TLS/SSL policy options.	<p>You can now configure the following advanced TLS/SSL policy options in the Advanced Settings tab on the SSL Policy page:</p> <ul style="list-style-type: none"> • Block flows requesting ESNI (Encrypted Server Name Identification) • Disable HTTP/3 advertisement • Propagate untrusted server certificates to clients
Encrypted Visibility Engine for visibility into encrypted sessions.	<p>Beta.</p> <p>You can enable the Encrypted Visibility Engine to gain visibility into an encrypted session without needing to decrypt it. The engine fingerprints and analyzes encrypted traffic. In FMC 7.1, the Encrypted Visibility Engine provides more visibility into encrypted traffic, including protocols such as TLS and QUIC. It does not enforce any actions on that traffic.</p> <p>The Encrypted Visibility Engine is disabled by default. You can enable it on the Advanced tab of an access control policy in the Experimental Features section.</p> <p>New/modified screens: Policies > Access Control > Access Control Policy name > Advanced</p> <p>Note The Encrypted Visibility Engine is an experimental Beta feature provided for visibility. It may cause false positives.</p>
Service Policy	
Configure the maximum segment size (MSS) for embryonic connections.	<p>You can configure a service policy to set the server maximum segment size (MSS) for SYN-cookie generation for embryonic connections upon reaching the embryonic connections limit. This is meaningful for service policies where you are also setting embryonic connection maximums.</p> <p>New/modified screens: Connection Settings in the Add/Edit Service Policy wizard.</p>
Network Discovery	

New Feature	Description
Improved Snort 3 support for network discovery (remote network access support).	<p>With improvements to network discovery and remote network access support, Snort 3 is now at parity with Snort 2 for those features. The improvements include:</p> <ul style="list-style-type: none"> • Discovery of hosts and applications for SMB traffic: For SMB traffic on your network, the host is discovered in the network map, and the SMB application protocol and associated operating system information are discovered. • Discovery of NetBIOS traffic: For NetBIOS traffic, the NetBIOS name is discovered as well as associated information related to applications, such as the client application and operating system. • Discovery of applications only for hosts/networks monitored by the network discovery policy: This enhancement to the filtering logic enables you to discover applications for networks that are being monitored based on a network discovery rule. <p>In Snort 3, application detection is always enabled for all networks by default.</p>
Event Logging and Analysis	
Snort 3 support for elephant flow identification and monitoring.	<p>With FTD running Snort 3, you can now identify <i>elephant flows</i>—single-session network connections that are large enough to affect overall system performance. By default, elephant flow detection is automatically enabled, and tracks and logs connections larger than 1GB/10 seconds.</p> <p>A new predefined search for connection events (Reason = Elephant Flow) allows you to quickly identify elephant flows. You can also use the health monitor to view active elephant flows on your devices, and to create a custom health dashboard to correlate elephant flow incidence with other device metrics such as CPU usage.</p> <p>To disable this feature or to configure the size and time thresholds, use the FTD CLI.</p> <p>New/modified FTD CLI commands:</p> <ul style="list-style-type: none"> • show elephant-flow status • show elephant-flow detection-config • system support elephant-flow-detection enable • system support elephant-flow-detection disable • system support elephant-flow-detection bytes-threshold <i>bytes-in-MB</i> • system support elephant-flow-detection time-threshold <i>time-in-seconds</i>

New Feature	Description
Send intrusion events and retrospective malware events to the Secure Network Analytics cloud from the FMC.	<p>Upgrade impact.</p> <p>When you configure the system to send security events to the Stealthwatch cloud using Cisco Security Analytics and Logging (SaaS), the FMC now sends:</p> <ul style="list-style-type: none"> • Intrusion events. This allows remotely stored intrusion events to include impact flag data. Previously, these events were sent to the cloud by FTD and did not include the impact flag. • Retrospective malware events. These supplement the "original disposition" file and malware events that are still sent to the cloud by devices. <p>If you already enabled this feature, the FMC starts sending this information after a successful upgrade.</p>
New datastore for intrusion events improves performance.	<p>To improve performance, Version 7.1 uses a new datastore for intrusion events. After the upgrade finishes and the FMC reboots, historical events are migrated in the background, newest events first.</p> <p>As part of this migration, we deprecated intrusion incidents, the intrusion event clipboard, and custom tables for intrusion events. We also introduced two new fields in the intrusion event table: Source Host Criticality and Destination Host Criticality.</p>
NAT IP address and port information in connection and Security Intelligence events.	<p>For additional visibility into NAT translations, we added the following fields to connection and Security Intelligence events:</p> <ul style="list-style-type: none"> • NAT Source IP • NAT Destination IP • NAT Source Port • NAT Destination Port <p>In the table view of events, these fields are hidden by default. To change the fields that appear, click the x in any column name to display a field chooser.</p>

New Feature	Description
Packet tracer enhancements.	<p>Version 7.1 updates the packet tracer interface for better usability. In addition, you can now:</p> <ul style="list-style-type: none"> • Access the packet tracer directly from the main menu: Devices > Troubleshoot > Packet Tracer. • Save packet traces. • Run parallel packet traces across multiple devices. • Replay PCAPs through a device. • For Snort 3 devices, view enhanced output that provides new details on the phases of traffic evaluation from L2 to L7 (application identification, file/malware detection, intrusion detection, Security Intelligence, and so on), as well as how long each phase takes. <p>New/modified FTD CLI commands:</p> <ul style="list-style-type: none"> • packet-tracer input<i>source_interface</i>pcap<i>pcap_filename</i>
Object Management	
Network object support for HTTP, ICMP, and SSH platform settings.	You can now use network object groups that contain network objects for hosts or networks when configuring the IP addresses in the Threat Defense Platform Settings policy.
Snort 3 support for network wildcard mask objects.	You can now create and manage network wildcard mask objects on the Object Management page. You can use network wildcard mask objects in access control, prefilter, and NAT policies.
Deployment preview enhancements for objects.	<p>You can now preview deployment changes to Geolocation, File List, and Security Intelligence objects.</p> <p>Updated screen: Deploy > Deployment. In the Preview column, click the Preview icon for a device to see the changes to the file list objects.</p>
Integrations	
Support for Cisco ACI Endpoint Update App, Version 2.0 and remediation module.	<p>Version 2.0 of the Cisco ACI Endpoint Update App has the following improvements over previous versions:</p> <ul style="list-style-type: none"> • The minimum update interval (how often the app updates the FMC) is now 10 seconds. Previously, it was 30 seconds. • The site prefix (a string that creates a network group object on the FMC associated with each APIC tenant) is now limited to 10 characters. Previously, it was 5 characters. <p>A new Cisco ACI Endpoint remediation module is also available with this update.</p>
Usability, Performance, and Troubleshooting	

New Feature	Description
Health monitoring enhancements.	<p>We updated the health monitor as follows:</p> <ul style="list-style-type: none"> • The health policy editor now groups similar health modules. You can enable and disable entire module groups. • The health policy exclusion editor is updated for better usability. Also, when you exclude a device or health module from alerting, you can now specify a time period for the exclusion, from 15 minutes to permanently. • The health monitor alert editor is updated for better usability. • The health policy deployment interface is updated for better usability. <p>Note To use the updated health monitor, you must enable REST API access on System (⚙️) > Configuration > REST API Preferences.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • System (⚙️) > Health > Policy > Edit Policy • System (⚙️) > Health > Exclude • System (⚙️) > Health > Monitor Alerts • System (⚙️) > Health > Policy > Deploy Policy
Deployment history enhancements.	<p>You can now bookmark a deployment job, edit the deployment notes for a job, and generate a report.</p>
Global search enhancements.	<p>Global search now has the following capabilities:</p> <ul style="list-style-type: none"> • You can search the full text of FMC walkthroughs (<i>how-tos</i>). • You can search extended community list names or configured values. • You can restrict searches by domain.
New walkthroughs.	<p>We added the following walkthroughs:</p> <ul style="list-style-type: none"> • Create a Snort 3 intrusion policy. • Enable or disable Snort 3 on an individual device. • Create a Snort 3 network analysis policy. • View the network analysis policy mapping. • Upgrade FTD. • Create and manage a cluster. • Change the FMC access interface from Management to Data. • Change the FMC access interface from Data to Management.

New Feature	Description
<p>Snort memory usage telemetry sent to Cisco Success Network.</p>	<p>For improved serviceability, we now send telemetry on Snort memory and swap usage, including out-of-memory events, to Cisco Success Network.</p> <p>We send this information for both Snort 2 and Snort 3. You can change your Cisco Success Network enrollment at any time.</p>
<p>Snort 3 support for statistics on start-of-flow and end-of-flow events.</p>	<p>For FTD with Snort 3, the output of the show snort statistics command now reports statistics on start-of-flow and end-of-flow events.</p>
<p>Web interface changes: SecureX, threat intelligence, and other integrations.</p>	<p>Version 7.1 changes these FMC menu options if you are upgrading from Version 7.0.2 or any later Version 7.0.x maintenance release.</p> <p>Note These changes will switch back in Version 7.2.</p> <p>Integration > AMP > AMP Management is now AMP > AMP Management</p> <p>Integration > AMP > Dynamic Analysis Connections is now AMP > Dynamic Analysis Connections</p> <p>Integration > Intelligence > Sources is now Intelligence > Sources</p> <p>Integration > Intelligence > Elements is now Intelligence > Elements</p> <p>Integration > Intelligence > Settings is now Intelligence > Settings</p> <p>Integration > Intelligence > Incidents is now Intelligence > Incidents</p> <p>Integration > Other Integrations is now System (⚙️) > Integration</p> <p>Integration > Security Analytics & Logging is now System (⚙️) > Logging > Security Analytics & Logging</p> <p>Integration > SecureX is now System (⚙️) > SecureX</p>
<p>FMC REST API</p>	
<p>FMC REST API services/operations.</p>	<p>For information on changes to the FMC REST API, see What's New in 7.1 in the REST API quick start guide.</p>

Deprecated Features

Table 3: Deprecated Features in FMC Version 7.1.0

Deprecated Feature	Description
End of support: FMC 1000, 2500, 4500	You cannot run Version 7.1+ on the FMC models FMC 1000, 2500, and 4500. You cannot manage Version 7.1+ devices with these FMCs.
End of support: ASA 5508-X and 5516-X	You cannot run Version 7.1+ on the ASA 5508-X or 5516-X.
End of support: NGIPS software (ASA FirePOWER/NGIPSv).	Version 7.1 is supported on the FMC and on FTD devices only. It is not supported on ASA FirePOWER or NGIPSv devices. You can still use a Version 7.1 FMC to manage older devices — FTD as well as ASA FirePOWER and NGIPSv — that are running Version 6.5 through 7.0.
Deprecated: Intrusion incidents and the intrusion event clipboard.	<p>Data and configurations can be deleted.</p> <p>We removed the intrusion incidents feature and the related intrusion event clipboard. The upgrade removes all data related to incidents, and deletes report templates sections that use the clipboard as a data source.</p> <p>Deprecated screens/options:</p> <ul style="list-style-type: none"> • Analysis > Intrusions > Incidents • Analysis > Intrusions > Clipboard • Copy and Copy All on intrusion event workflow pages and packet views • When adding sections to a report template (Overview > Reporting > Report Templates), you can no longer choose the Clipboard table as a data source.
Deprecated: Custom tables for intrusion events.	<p>Custom tables can be deleted.</p> <p>Version 7.1 ends support for custom tables for intrusion events. The upgrade deletes custom tables that contain fields from the intrusion event table.</p> <p>When adding fields to a custom table (Analysis > Advanced > Custom Tables), you can no longer choose the Intrusion Events table as a data source.</p>
Deprecated: ECMP zones with FlexConfig.	<p>FlexConfig settings ignored. Can prevent deploy.</p> <p>You can now group interfaces in traffic zones and configure Equal-Cost-Multi-Path (ECMP) routing in the management center web interface. After upgrade, the system ignores ECMP zones configured with FlexConfig. You cannot deploy with equal-cost static routes exist and must assign their interfaces to an ECMP zone.</p>

Deprecated Feature	Description
Temporarily deprecated: Improved SecureX integration, SecureX orchestration.	<p>Can prevent upgrade.</p> <p>Version 7.1 temporarily deprecates the SecureX integration and orchestration improvements introduced in Version 7.0.2. The improved experience returns in Version 7.2.</p> <p>If you newly enabled SecureX integration in Version 7.0.2 or later maintenance release, you must disable the feature before you upgrade to Version 7.1. You can re-enable the feature after successful upgrade, using the older method. There are no upgrade issues if you enabled SecureX integration in Version 7.0.0 or 7.0.1, or if you upgrade to Version 7.2.</p>
Deprecated: Geolocation details.	<p>In May 2022 we split the GeoDB into two packages: a country code package that maps IP addresses to countries/continents, and an IP package that contains additional contextual data associated with routable IP addresses. The contextual data in the IP package can include additional location details, as well as connection information such as ISP, connection type, proxy type, domain name, and so on.</p> <p>The new country code package has the same file name as the old all-in-one package: <code>Cisco_GEODB_Update-<i>date-build</i></code>. This allows deployments running Version 7.1 and earlier to continue to obtain GeoDB updates. If you manually download GeoDB updates—for example, in an air-gapped deployment—make sure you get the country code package and not the IP package.</p> <p>Important This split does not affect geolocation rules or traffic handling in any way—those rules rely only on the data in the country code package. However, because the country code package essentially replaces the all-in-one package, the contextual data is no longer updated and will grow stale. To obtain fresh data, upgrade or reimagine the FMC to Version 7.2+ and update the GeoDB.</p>

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	<p>We introduced the Secure Firewall 3110, 3120, 3130, and 3140.</p> <p>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.</p> <p>Note that the Version 7.1 device manager does not include online help for these devices. See the documentation posted on Cisco.com.</p> <p>New/Modified screens: Device > Interfaces</p> <p>New/Modified Firepower Threat Defense commands: configure network speed, configure raid, show raid, show ssd</p>

Feature	Description
FTDv for AWS instances.	FTDv for AWS adds support for these instances: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 Firepower Threat Defense 7.0.	You cannot install Firepower Threat Defense 7.1 on an ASA 5508-X or 5516-X. The last supported release for these models is Firepower Threat Defense 7.0.

Feature	Description
Firewall and IPS Features	
Network Analysis Policy (NAP) configuration for Snort 3.	<p>You can use FDM 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.</p> <p>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.</p>
Manual NAT support for fully-qualified domain name (FQDN) objects as the translated destination.	<p>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.</p>
Improved active authentication for identity rules.	<p>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.</p> <p>We added the Redirect to Host Name option in the identity policy settings.</p>
VPN Features	
Backup remote peers for site-to-site VPN.	<p>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.</p> <p>We updated the site-to-site VPN wizard to include backup peer configuration.</p>

Feature	Description
Password management for remote access VPN (MSCHAPv2).	<p>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.</p> <p>We added the Enable Password Management option to the authentication settings for remote access VPN connection profiles.</p>
AnyConnect VPN SAML External Browser	<p>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.</p> <p>We updated the remote access VPN connection profile wizard to allow you to configure the SAML Login Experience.</p>
Administrative and Troubleshooting Features	
Dynamic Domain Name System (DDNS) support for updating fully-qualified domain name (FQDN) to IP address mappings for system interfaces.	<p>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.</p> <p>After upgrade, if you had used FlexConfig to configure DDNS, you must redo your configuration using FDM or the Firepower Threat Defense API, and remove the DDNS FlexConfig object from the FlexConfig policy, before you can deploy changes again.</p> <p>If you configure DDNS using FDM, then switch to FMC management, the DDNS configuration is retained so that FMC can find the system using the DNS name.</p> <p>In FDM, we added the System Settings > DDNS Service page. In the Firepower Threat Defense API, we added the DDNSService and DDNSInterfaceSettings resources.</p>
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 FDM.	<p>You can use FDM 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.</p> <p>We added the System Settings > DHCP > DHCP Relay page, and moved DHCP Server under the new DHCP heading.</p>
Key type and size for self-signed certificates in FDM.	<p>You can specify the key type and size when generating new self-signed internal and internal CA certificates in FDM. 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.</p>
Usage validation restrictions for trusted CA certificates.	<p>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.</p> <p>We added Validation Usage as a property for trusted CA certificates.</p>
Generating the admin password in FDM.	<p>During initial system configuration in FDM, or when you change the admin password through FDM, you can now click a button to generate a random 16 character password.</p>
Startup time and tmatch compilation status.	<p>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.</p> <p>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.</p>
Enhancements to show access-list element-count output.	<p>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.</p> <p>In addition, the show tech-support output now includes the output from show access-list element-count and show asp rule-engine.</p>

Feature	Description
Use FDM to configure the Firepower Threat Defense for management by a FMC.	<p>When you perform initial setup using FDM, all interface configuration completed in FDM is retained when you switch to FMC for management, in addition to the Management and FMC access settings. Note that other default configuration settings, such as the access control policy or security zones, are not retained. When you use the Firepower Threat Defense CLI, only the Management and FMC access settings are retained (for example, the default inside interface configuration is not retained).</p> <p>After you switch to FMC, you can no longer use FDM to manage the Firepower Threat Defense.</p> <p>New/Modified screens: System Settings > Management Center</p>
Automatically update CA bundles	<p>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.</p> <p>Note This feature is not supported in Version 7.0.0–7.0.4, 7.1.0–7.1.0.2, or 7.2.0–7.2.3. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco.</p> <p>New/modified CLI commands: configure cert-update auto-update, configure cert-update run-now, configure cert-update test, show cert-update</p> <p>For more information, see the Cisco Secure Firewall Threat Defense Command Reference.</p>
FTD REST API version 6.2 (v6).	<p>The Firepower 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.</p> <p>Please re-evaluate all existing calls, as changes might have been made 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.</p>

Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

Intrusion rule updates (SRUs/LSPs) provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. If a newer intrusion rule uses keywords that are not supported in your current version, that rule is not imported when you update the SRU/LSP.

After you upgrade and those keywords become supported, the new intrusion rules are imported and, depending on your IPS configuration, can become auto-enabled and thus start generating events and affecting traffic flow.

You can find your Snort version in the *Bundled Components* section of the compatibility guide, or use one of these commands:

- FMC: Choose **Help > About**.
- FDM: Use the **show summary** CLI command.

The Snort release notes contain details on new keywords. You can read the release notes on the Snort download page: <https://www.snort.org/downloads>.

Deprecated FlexConfig Commands

This document lists deprecated FlexConfig objects and commands along with the other deprecated features for this release. For a full list of prohibited commands, including those prohibited when FlexConfig was introduced and those deprecated in previous releases, see your configuration guide.



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

About FlexConfig

Some FTD features are configured using ASA configuration commands. You can use Smart CLI or FlexConfig to manually configure various ASA features that are not otherwise supported in the web interface.

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

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