



New Features in Cloud-delivered Firewall Management Center 2024

- [August 23, 2024, on page 1](#)
- [June 6, 2024, on page 7](#)
- [May 30, 2024, on page 7](#)
- [April 2, 2024, on page 8](#)
- [February 13, 2024, on page 8](#)

August 23, 2024

Table 1: Features in Version 20240808

Feature	Minimum Threat Defense	Details
Platform		


Feature	Minimum Threat Defense	Details
Threat defense Version 7.6.0 support.	7.6.0	<p>You can now manage threat defense devices running Version 7.6.0.</p> <p>Note The Firepower 2100 is deprecated in Version 7.6.0. Although you can continue managing these devices running Version 7.0.3–7.4.x, you cannot upgrade them further. Because there is a single configuration guide that covers the latest version, for features that are only supported with older devices, refer to the <i>on-prem</i> management center guide that matches your threat defense version.</p> <p>Note The cloud-delivered Firewall Management Center supports a wider range of managed device versions than on-prem management centers. If you are using an on-prem management center for analytics with Version 7.0.x devices, we recommend you upgrade those devices to at least Version 7.2.x, if possible. This will allow you to get events from those older devices while also adding devices running the latest release. For more information, see End of support: analytics-only capabilities with the full range of threat defense devices.</p>

High Availability/Scalability

Feature	Minimum Threat Defense	Details
Multi-instance mode for the Secure Firewall 3100.	7.4.1	<p>You can deploy the Secure Firewall 3100 as a single device (<i>appliance mode</i>) or as multiple container instances (<i>multi-instance mode</i>). In multi-instance mode, you can deploy multiple container instances on a single chassis that act as completely independent devices. Note that in multi-instance mode, you upgrade the operating system and the firmware (<i>chassis upgrade</i>) separately from the container instances (<i>threat defense upgrade</i>).</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Inventory > FTD Chassis • Devices > Device Management > Device > Chassis Manager • Devices > Platform Settings > New Policy > Chassis Platform Settings • Devices > Chassis Upgrade <p>New/modified threat defense CLI commands: configure multi-instance network ipv4, configure multi-instance network ipv6</p> <p>New/modified FXOS CLI commands: create device-manager, set deploymode</p> <p>Platform restrictions: Not supported on the Secure Firewall 3105.</p> <p>See: Use Multi-Instance Mode for the Secure Firewall and Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center</p>

Access Control: Threat Detection and Application Identification

Easily bypass decryption for sensitive and undecryptable traffic.	Any	<p>It is now easier to bypass decryption for sensitive and undecryptable traffic, which protects users and improves performance.</p> <p>New decryption policies now include predefined rules that, if enabled, can automatically bypass decryption for sensitive URL categories (such as finance or medical), undecryptable distinguished names, and undecryptable applications. Distinguished names and applications are undecryptable typically because they use TLS/SSL certificate pinning, which is itself not decryptable.</p> <p>For outbound decryption, you enable/disable these rules as part of creating the policy. For inbound decryption, the rules are disabled by default. After the policy is created, you can edit, reorder, or delete the rules entirely.</p> <p>New/modified screens: Policies > Access Control > Decryption > Create Decryption Policy</p> <p>See: Create a Decryption Policy</p> <p>See: Create a Decryption Policy</p>
---	-----	---

Feature	Minimum Threat Defense	Details
Access Control: Identity		
Microsoft Azure AD as a user identity source.	7.4.2	<p>You can use a Microsoft Azure Active Directory (Azure AD) realm with ISE to authenticate users and get user sessions for user control.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Integration > Other Integrations > Realms > Add Realm > Azure AD • Integration > Other Integrations > Realms > Actions, such as downloading users, copying, editing, and deleting <p>Supported ISE versions: 3.0 patch 5+, 3.1 (any patch level), 3.2 (any patch level)</p> <p>See: Create a Microsoft Azure Active Directory Realm</p>
Health Monitoring		
Collect health data without alerting.	Any	<p>You can now disable health alerts/health alert sub-types for ASP Drop, CPU, and Memory health modules, while continuing to collect health data. This allows you to minimize health alert noise and focus on the most critical issues.</p> <p>New/modified screens: In any health policy (System  > Health > Policy), there are now checkboxes that enable and disable ASP Drop (threat defense only), CPU, and Memory health alert sub-types.</p> <p>See: Health Policies</p>
Chassis-level health alerts for the Firepower 4100/9300.	7.4.1	<p>You can now view chassis-level health alerts for Firepower 4100/9300 by registering the chassis to the management center as a read-only device. You must also enable the Firewall Threat Defense Platform Faults health module and apply the health policy. The alerts appear in the Message Center, the health monitor (in the left pane, under Devices, select the chassis), and in the health events view.</p> <p>You can also add a chassis (and view health alerts for) the Secure Firewall 3100 in multi-instance mode. For those devices, you use the management center to manage the chassis. But for the Firepower 4100/9300 chassis, you still must use the chassis manager or the FXOS CLI.</p> <p>New/modified screens: Inventory > FTD Chassis</p> <p>See: Onboard a Chassis</p>
Threat Defense Upgrade		
Administration		

Feature	Minimum Threat Defense	Details
Threat defense high availability automatically resumes after restoring from backup.	Any	When replacing a failed unit in a high availability pair, you no longer have to manually resume high availability after the restore completes and the device reboots. You should still confirm that high availability has resumed before you deploy.
Change management ticket takeover; more features in the approval workflow.	Any	<p>You can now take over another user's ticket. This is useful if a ticket is blocking other updates to a policy and the user is unavailable.</p> <p>These features are now included in the approval workflow: decryption policies, DNS policies, file and malware policies, network discovery, certificates and certificate groups, cipher suite lists, Distinguished Name objects, Sinkhole objects.</p> <p>See: Change Management</p>
Troubleshooting		
Troubleshoot Snort 3 performance issues with a CPU and rule profiler.	7.6.0 with Snort 3	<p>New CPU and rule profilers help you troubleshoot Snort 3 performance issues. You can now monitor:</p> <ul style="list-style-type: none"> • CPU time taken by Snort 3 modules/inspectors to process packets. • CPU resources each module is consuming, relative to the total CPU consumed by the Snort 3 process. • Modules with unsatisfactory performance when Snort 3 is consuming high CPU. • Intrusion rules with unsatisfactory performance. <p>New/modified screens: Devices > Troubleshoot > Snort 3 Profiling</p> <p>Platform restrictions: Not supported for container instances.</p> <p>See: Advanced Troubleshooting for the Secure Firewall Threat Defense Device</p> <p>See: Advanced Troubleshooting for the Secure Firewall Threat Defense Device</p>
Deprecated Features		

Feature	Minimum Threat Defense	Details
End of support: analytics-only capabilities with the full range of threat defense devices.	Any	<p>If you are using an on-prem management center for analytics with Version 7.0.x devices, we recommend you upgrade those devices to at least Version 7.2.x, if possible. This will allow you to get events from those older devices while also adding devices running the latest release.</p> <p>The cloud-delivered Firewall Management Center supports a wider range of managed device versions than on-prem management centers. This can cause issues if you use an on-prem management center for analytics because devices can be "too old" or "too new" to co-manage.</p> <p>You can be prevented from:</p> <ul style="list-style-type: none"> • Registering newer devices to the analytics management center because older devices are blocking the required management center upgrade. • Upgrading co-managed devices to the latest release, because the analytics management center is "stuck" at an older release. • Reverting device upgrade, if revert would take the device out of compatibility with the analytics management center. <p>For example, consider a scenario where you want to add co-managed Version 7.6.0 devices to a deployment that currently includes co-managed Version 7.0.x devices. The cloud-delivered Firewall Management Center can manage this full range of devices, but the on-prem analytics management center cannot.</p> <p>In order of preference, you can:</p> <ul style="list-style-type: none"> • Upgrade the Version 7.0.x devices to at least Version 7.2.0, upgrade the analytics management center to Version 7.6.0, then add the Version 7.6.0 devices to both management centers. • Remove the Version 7.0.x devices from the analytics management center, upgrade the analytics management center to Version 7.6.0, then add the Version 7.6.0 devices to both management centers. • Leave the analytics management center as it is and do not add your Version 7.6.0 devices. <p>That is, your choices are:</p> <ul style="list-style-type: none"> • To get events from all devices, upgrade (or replace) the analytics management center and your older devices. • To forgo events from older devices, upgrade (or replace) the analytics management center only. • To forgo events from newer devices, leave the analytics management center at an older release.

June 6, 2024

Firewall Management with Cisco AI Assistant

CDO administrators now have a more efficient way to manage Secure Firewall Threat Defense policies and access documentation with the integration of the Cisco AI Assistant in Cisco Defense Orchestrator (CDO) and cloud-delivered Firewall Management Center. The Cisco AI Assistant has several key features:

- **Pre-Enabled Assistant:** The AI Assistant is enabled by default on every CDO tenant. If needed, you can disable it on the General Settings page of your tenant.
- **Easy Access:** CDO Super Admins and Admin can access the AI Assistant directly from the top menu bar of their tenant's dashboard after logging in.



- **User Orientation:** Upon opening the AI Assistant widget for the first time, users are greeted with a carousel window that introduces the AI Assistant, explains data privacy protections, and provides tips on effective usage.
- **Policy Rule Assistance:** The AI Assistant simplifies the process of creating policy rules on Secure Firewall Threat Defense devices. Administrators can quickly create access control rules using simple prompts.
- **Product Knowledge Resource:** The AI Assistant has ingested CDO's and the cloud-delivered Firewall Management's documentation. If you need help, you can ask it a question.
- **User-Friendly Interface:**
 - **Simple Text Input Box:** Located at the bottom of the window for easy engagement with the Assistant.
 - **Thread History:** The questions, or series of questions, you ask the AI Assistant are called threads. The AI Assistant retains your thread history so you can refer to the questions you've asked.
 - **Feedback:** Provide feedback on the Assistant's responses with thumbs up or thumbs down.

See the [Cisco AI Assistant User Guide](#) for more information.

May 30, 2024

Table 2: Features in Version 20240514

Feature	Minimum Threat Defense	Details
Platform Migration		

April 2, 2024

Feature	Minimum Threat Defense	Details
Migrate clustered threat defense devices from an on-prem management center to the cloud-delivered Firewall Management Center.	7.0.6 7.2.1	Clustered Secure Firewall Threat Defense devices are now migrated along with the rest of the configuration when they are migrated from the on-prem management center to the cloud-delivered Firewall Management Center. See: Migrate On-Prem Management Center managed Secure Firewall Threat Defense to Cloud-delivered Firewall Management Center
Deployment and Policy Management		
Change management.	Any	You can enable change management if your organization needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed. We added the System (⚙️) > Configuration > Change Management page to enable the feature. When enabled, there is a System (⚙️) > Change Management Workflow page, and a new Ticket (📄) quick access icon in the menu. See: Change Management

April 2, 2024

This release introduces stability, hardening, and performance enhancements.

February 13, 2024

Table 3: Features in Version 20240203

Feature	Minimum Threat Defense	Details
Platform		
Threat defense Version 7.4.1 support.	7.4.1	You can now manage threat defense devices running Version 7.4.1.
Network modules for the Secure Firewall 3130 and 3140.	7.4.1	The Secure Firewall 3130 and 3140 now support these network modules: <ul style="list-style-type: none"> • 2-port 100G QSFP+ network module (FPR3K-XNM-2X100G) See: Cisco Secure Firewall 3110, 3120, 3130, and 3140 Hardware Installation Guide

Feature	Minimum Threat Defense	Details
Optical transceivers for Firepower 9300 network modules.	7.4.1	<p>The Firepower 9300 now supports these optical transceivers:</p> <ul style="list-style-type: none"> • QSFP-40/100-SRBD • QSFP-100G-SR1.2 • QSFP-100G-SM-SR <p>On these network modules:</p> <ul style="list-style-type: none"> • FPR9K-NM-4X100G • FPR9K-NM-2X100G • FPR9K-DNM-2X100G <p>See: Cisco Firepower 9300 Hardware Installation Guide</p>
Performance profile support for the Secure Firewall 3100.	7.4.1	<p>The performance profile settings available in the platform settings policy now apply to the Secure Firewall 3100. Previously, this feature was supported on the Firepower 4100/9300, the Secure Firewall 4200, and on threat defense virtual.</p> <p>See: Configure the Performance Profile</p>
NAT		
Create network groups while editing NAT rules.	Any	<p>You can now create network groups in addition to network objects while editing a NAT rule.</p> <p>See: Customizing NAT Rules for Multiple Devices</p>
Device Management		
Device management services supported on user-defined VRF interfaces.	Any	<p>Device management services configured in the threat defense platform settings (NetFlow, SSH access, SNMP hosts, syslog servers) are now supported on user-defined Virtual Routing and Forwarding (VRF) interfaces.</p> <p>Platform restrictions: Not supported with container instances or clustered devices.</p> <p>See Platform Settings</p>
SD-WAN		
SD-WAN Summary dashboard	7.4.1	<p>The WAN Summary dashboard provides a snapshot of your WAN devices and their interfaces. It provides insight into your WAN network and information about device health, interface connectivity, application throughput, and VPN connectivity. You can monitor the WAN links and take proactive and prompt recovery measures. In addition, you can also monitor the WAN interface application performance using the Application Monitoring tab.</p> <p>New/modified screens: Analysis > SD-WAN Summary</p> <p>See: SD-WAN Summary Dashboard</p>

Feature	Minimum Threat Defense	Details
Access Control: Identity		
Captive portal support for multiple Active Directory realms (realm sequences).	7.4.1	<p>Upgrade impact. Update custom authentication forms.</p> <p>You can configure active authentication for either an LDAP realm; or a Microsoft Active Directory realm or a realm sequence. In addition, you can configure a passive authentication rule to fall back to active authentication using either a realm or a realm sequence. You can optionally share sessions between managed devices that share the same identity policy in access control rules.</p> <p>In addition, you have the option to require users to authenticate again when they access the system using a different managed device than they accessed previously.</p> <p>If you use the HTTP Response Page authentication type, after you upgrade threat defense, you must add <code><select name="realm" id="realm"></select></code> to your custom authentication form. This allows the user to choose between realms.</p> <p>Restrictions: Not supported with Microsoft Azure Active Directory.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Policies > Identity > (edit policy) > Active Authentication > Share active authentication sessions across firewalls • Identity policy > (edit) > Add Rule > Passive Authentication > Realms & Settings > Use active authentication if passive or VPN identity cannot be established • Identity policy > (edit) > Add Rule > Active Authentication > Realms & Settings > Use active authentication if passive or VPN identity cannot be established <p>See: How to Configure the Captive Portal for User Control</p>
Share captive portal active authentication sessions across firewalls.	7.4.1	<p>Determines whether or not users are required to authenticate when their authentication session is sent to a different managed device than one they previously connected to. If your organization requires users to authenticate every time they change locations or sites, you should <i>disable</i> this option.</p> <ul style="list-style-type: none"> • (Default.) Enable to allow users to authenticate with any managed device associated with the active authentication identity rule. • Disable to require the user to authenticate with a different managed device, even if they have already authenticated with another managed device to which the active authentication rule is deployed. <p>New/modified screens: Policies > Identity > (edit policy) > Active Authentication > Share active authentication sessions across firewalls</p> <p>See: How to Configure the Captive Portal for User Control</p>

Deployment and Policy Management

Feature	Minimum Threat Defense	Details
View and generate reports on configuration changes since your last deployment.	Any	<p>You can generate, view, and download (as a zip file) the following reports on configuration changes since your last deployment:</p> <ul style="list-style-type: none"> • A policy changes report for each device that previews the additions, changes, or deletions in the policy, or the objects that are to be deployed on the device. • A consolidated report that categorizes each device based on the status of policy changes report generation. <p>This is especially useful after you upgrade threat defense devices, so that you can see the changes made by the upgrade before you deploy.</p> <p>New/modified screens: Deploy > Advanced Deploy.</p> <p>See: Download Policy Changes Report for Multiple Devices</p>
Suggested release notifications.	Any	<p>The management center now notifies you when a new suggested release is available. If you don't want to upgrade right now, you can have the system remind you later, or defer reminders until the next suggested release. The new upgrade page also indicates suggested releases.</p> <p>See: Cisco Secure Firewall Management Center New Features by Release</p>
Enable revert from the threat defense upgrade wizard.	Any	<p>You can now enable revert from the threat defense upgrade wizard.</p> <p>Other version restrictions: You must be upgrading threat defense to Version 7.2+.</p> <p>See: Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center</p>
View detailed upgrade status from the threat defense upgrade wizard.	Any	<p>The final page of the threat defense upgrade wizard now allows you to monitor upgrade progress. This is in addition to the existing monitoring capability on the Upgrade tab on the Device Management page, and on the Message Center. Note that as long as you have not started a new upgrade flow, Devices > Threat Defense Upgrade brings you back to this final wizard page, where you can view the detailed status for the current (or most recently complete) device upgrade.</p> <p>See: Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center</p>

Feature	Minimum Threat Defense	Details
Firmware upgrades included in FXOS upgrades.	Any	<p>Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.</p> <p>For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1 now include firmware upgrades. Secure Firewall 3100 in multi-instance mode (new in Version 7.4.1) also bundles FXOS and 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.</p> <p>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.</p> <p>See: Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide</p>

Upgrade

Improved upgrade starting page and package management.	Any	<p>A new upgrade page makes it easier to choose, download, manage, and apply upgrades to your entire deployment. The page lists all upgrade packages that apply to your current deployment, with suggested releases specially marked. You can easily choose and direct-download packages from Cisco, as well as manually upload and delete packages.</p> <p>Patches are not listed unless you have at least one appliance at the appropriate maintenance release (or you manually uploaded the patch). You must manually upload hotfixes.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • System (⚙️) > Product Upgrades is now where you upgrade devices, as well as manage upgrade packages. • System (⚙️) > Content Updates is now where you update intrusion rules, the VDB, and the GeoDB. • Devices > Threat Defense Upgrade takes you directly to the threat defense upgrade wizard. <p>Deprecated screens/options:</p> <ul style="list-style-type: none"> • System (⚙️) > Updates is deprecated. All threat defense upgrades now use the wizard. • The Add Upgrade Package button on the threat defense upgrade wizard has been replaced by a Manage Upgrade Packages link to the new upgrade page. <p>See: Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center</p>
--	-----	--

Administration

Feature	Minimum Threat Defense	Details
Updated internet access requirements for direct-downloading software upgrades.	Any	The management center has changed its direct-download location for software upgrade packages from sourcefire.com to amazonaws.com. See: Internet Access Requirements
Scheduled tasks download patches and VDB updates only.	Any	The Download Latest Update scheduled task no longer downloads maintenance releases; now it only downloads the latest applicable patches and VDB updates. To direct-download maintenance (and major) releases to the management center, use System (⚙️) > Product Upgrades . See: Software Update Automation
Smaller VDB for lower memory Snort 2 devices.	Any with Snort 2	For VDB 363+, the system now installs a smaller VDB (also called <i>VDB lite</i>) 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 and ASA 5516-X See: Update the Vulnerability Database

Deprecated Features

Deprecated: DHCP relay trusted interfaces with FlexConfig.	Any	You can now use the management center web interface to configure interfaces as trusted interfaces to preserve DHCP Option 82. If you do this, these settings override any existing FlexConfigs, although you should remove them. See: Configure the DHCP Relay Agent
Deprecated: Merging downloadable access control list with a Cisco attribute-value pair ACL for RADIUS identity sources with FlexConfig.	Any	This feature is now supported in the management center web interface.
Deprecated: frequent drain of events health alerts.	7.4.1	The Disk Usage health module no longer alerts with <code>frequent drain of events</code> . You may continue to see these alerts until you either deploy health policies to managed devices (stops the display of alerts) or upgrade devices to Version 7.4.1+ (stops the sending of alerts). See: Disk Usage and Drain of Events Health Monitor Alerts

