



# New Features in Cloud-delivered Firewall Management Center 2024

- [April 2, 2024, on page 1](#)
- [February 13, 2024, on page 1](#)

## April 2, 2024

This release introduces stability, hardening, and performance enhancements.

## February 13, 2024

### New Features

*Table 1: New Features: Version 20240203*

Feature	Min. Threat Defense	Details
<b>Platform</b>		
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"><li>• 2-port 100G QSFP+ network module (FPR3K-XNM-2X100G)</li></ul> See: <a href="#">Cisco Secure Firewall 3110, 3120, 3130, and 3140 Hardware Installation Guide</a>

Feature	Min. 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"> <li>• QSFP-40/100-SRBD</li> <li>• QSFP-100G-SR1.2</li> <li>• QSFP-100G-SM-SR</li> </ul> <p>On these network modules:</p> <ul style="list-style-type: none"> <li>• FPR9K-NM-4X100G</li> <li>• FPR9K-NM-2X100G</li> <li>• FPR9K-DNM-2X100G</li> </ul> <p>See: <a href="#">Cisco Firepower 9300 Hardware Installation Guide</a></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: <a href="#">Configure the Performance Profile</a></p>
<b>NAT</b>		
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: <a href="#">Customizing NAT Rules for Multiple Devices</a></p>
<b>Device Management</b>		
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 <a href="#">Platform Settings</a></p>
<b>SD-WAN</b>		
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 <b>Application Monitoring</b> tab.</p> <p>New/modified screens: <b>Analysis &gt; SD-WAN Summary</b></p> <p>See: <a href="#">SD-WAN Summary Dashboard</a></p>
<b>Access Control: Identity</b>		

Feature	Min. Threat Defense	Details
Captive portal support for multiple Active Directory realms (realm sequences).	7.4.1	<p><b>Upgrade impact. Update custom authentication forms.</b></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>&lt;select name="realm" id="realm"&gt;&lt;/select&gt;</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"> <li>• <b>Policies &gt; Identity &gt; (edit policy) &gt; Active Authentication &gt; Share active authentication sessions across firewalls</b></li> <li>• <b>Identity policy &gt; (edit) &gt; Add Rule &gt; Passive Authentication &gt; Realms &amp; Settings &gt; Use active authentication if passive or VPN identity cannot be established</b></li> <li>• <b>Identity policy &gt; (edit) &gt; Add Rule &gt; Active Authentication &gt; Realms &amp; Settings &gt; Use active authentication if passive or VPN identity cannot be established</b></li> </ul> <p>See: <a href="#">How to Configure the Captive Portal for User Control</a></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"> <li>• (Default.) Enable to allow users to authenticate with any managed device associated with the active authentication identity rule.</li> <li>• 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.</li> </ul> <p>New/modified screens: <b>Policies &gt; Identity &gt; (edit policy) &gt; Active Authentication &gt; Share active authentication sessions across firewalls</b></p> <p>See: <a href="#">How to Configure the Captive Portal for User Control</a></p>

## Deployment and Policy Management

Feature	Min. 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"> <li>• 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.</li> <li>• A consolidated report that categorizes each device based on the status of policy changes report generation.</li> </ul> <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: <b>Deploy &gt; Advanced Deploy</b>.</p> <p>See: <a href="#">Download Policy Changes Report for Multiple Devices</a></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: <a href="#">Cisco Secure Firewall Management Center New Features by Release</a></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: <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center</a></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, <b>Devices &gt; Threat Defense Upgrade</b> 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: <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center</a></p>
Firmware upgrades included in FXOS upgrades.	Any	<p><b>Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.</b></p> <p>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.</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: <a href="#">Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide</a></p>

## Upgrade

Feature	Min. Threat Defense	Details
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"> <li>• <b>System (⚙️) &gt; Product Upgrades</b> is now where you upgrade devices, as well as manage upgrade packages.</li> <li>• <b>System (⚙️) &gt; Content Updates</b> is now where you update intrusion rules, the VDB, and the GeoDB.</li> <li>• <b>Devices &gt; Threat Defense Upgrade</b> takes you directly to the threat defense upgrade wizard.</li> </ul> <p>Deprecated screens/options:</p> <ul style="list-style-type: none"> <li>• <b>System (⚙️) &gt; Updates</b> is deprecated. All threat defense upgrades now use the wizard.</li> <li>• The <b>Add Upgrade Package</b> button on the threat defense upgrade wizard has been replaced by a <b>Manage Upgrade Packages</b> link to the new upgrade page.</li> </ul> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center</a></p>
<b>Administration</b>		
Updated internet access requirements for direct-downloading software upgrades.	Any	<p>The management center has changed its direct-download location for software upgrade packages from sourcefire.com to amazonaws.com.</p> <p>See: <a href="#">Internet Access Requirements</a></p>
Scheduled tasks download patches and VDB updates only.	Any	<p>The <b>Download Latest Update</b> 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 <b>System (⚙️) &gt; Product Upgrades</b>.</p> <p>See: <a href="#">Software Update Automation</a></p>
Smaller VDB for lower memory Snort 2 devices.	Any with Snort 2	<p>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.</p> <p>Lower memory devices: ASA-5508-X and ASA 5516-X</p> <p>See: <a href="#">Update the Vulnerability Database</a></p>

## Deprecated Features

**Table 2: Deprecated Features: Version 20240203**

Feature	Deprecated in Threat Defense	Details
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: <a href="#">Configure the DHCP Relay Agent</a>
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 frequent drain of events. 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: <a href="#">Disk Usage and Drain of Events Health Monitor Alerts</a>