Cisco Secure Firewall Threat Defense Release Notes, Version 7.6.0

First Published: 2024-06-28

Last Modified: 2024-06-28

Cisco Secure Firewall Threat Defense Release Notes

This document contains release information for:

- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center (on-prem)

For Cisco Defense Orchestrator (CDO) deployments, see the Cisco Cloud-Delivered Firewall Management Center Release Notes or What's New for Cisco Defense Orchestrator.

Release Dates

Table 1: Version 7.6 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
7.6.0	41	2024-06-27	—	Management center virtual for KVM, v25 only Threat defense virtual for KVM

Compatibility

Version 7.6.0 is available only for new installations of the Secure Firewall Management Center Virtual for KVM (v25 only) and Secure Threat Defense Virtual for KVM. Support for device manager, upgrades, and all other platforms begins soon.

For compatibility information for earlier releases, see:

- Cisco Secure Firewall Management Center Compatibility Guide
- Cisco Secure Firewall Threat Defense Compatibility Guide
- Cisco Firepower 4100/9300 FXOS Compatibility

Features

The following features are new in Version 7.6.0. For earlier releases, see Cisco Secure Firewall Management Center New Features by Release.

Table 2: Management Center Features in Version 7.6.0

Feature	Minimum Management Center	Minimum Threat Defense	Details
Device Management			
Device templates.	7.6.0	7.4.1	Device templates enable deployment of multiple branch devices with pre-provisioned initial device configurations, including site-to-site VPN connections. You can also apply configuration changes to multiple devices with different interface configurations, and clone configuration parameters from existing devices.
AAA for user-defined VRF interfaces.	7.6.0	7.6.0	A device's authentication, authorization, and accounting (AAA) is now supported on user-defined Virtual Routing and Forwarding (VRF) interfaces. The default is to use the management interface. To enable this feature, add the security zone having a VRF interface to the platform External Authentication servers. When enabled, the AAA route lookup refers to the VRF routing domain, and the AAA management traffic are forwarded to the data interfaces. New/modified screens: **Devices** > **Platform Settings** > **External Authentication**
SD-WAN			
SD-WAN wizard.	7.6.0	Hub: 7.6.0 Spoke: 7.3.0	A new wizard allows you to easily configure VPN tunnels between your centralized headquarters and remote branch sites. New/modified screens: **Devices** > **VPN** > **Site To Site** > **Add** > **SD-WAN Topology**
Access Control: Threat Detection and Application Identification			
Snort ML: neural network-based exploit detector.	7.6.0	7.6.0 with Snort 3	A new Snort 3 inspector, snort_ml, uses neural network-based machine learning (ML) to detect known and 0-day attacks without needing multiple preset rules. The inspector subscribes to HTTP events and looks for the HTTP URI, which in turn is used by a neural network to detect exploits (currently limited to SQL injections). The new inspector is currently disabled in all default policies except maximum detection. A new intrusion rule, GID:411 SID:1, generates an event when the snort_ml detects an attack. This rule is also currently disabled in all default policies except maximum detection. See: Snort 3 Inspector Reference

Feature	Minimum Management Center	Minimum Threat Defense	Details
Bypass EVE block verdict for trusted traffic.	7.6.0	Any with Snort 3	You can now bypass EVE (encrypted visibility engine) block verdicts for known trusted traffic, based on destination network or EVE process name. Connections that bypass EVE in this way have the new **EVE Exempted** reason. New/modified screens: • To add an exception from the access control policy, in the advanced settings, edit and enable **Encrypted Visibility Engine**, enable **Block Traffic Based on EVE Score**, and **Add Exception Rule**. • To add an exception from the Unified Events viewer, right-click a connection that was blocked by EVE and select **Add EVE Exception**. See: Cisco Secure Firewall Management Center Snort 3 Configuration Guide, Version 7.6
Bypass decryption for sensitive and undecryptable traffic.	7.6.0	Any	When you create a decryption policy for outbound traffic protection, you can choose to exempt certain traffic from being decrypted. We'll automatically add Do Not Decrypt rules to your policy to simplify the process of bypassing decryption for specific outbound connections. Outbound decryption (using a Decrypt - Resign rule action) enables you to choose to exempt from decryption: 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. We add Do Not Decrypt rules to your policy to prevent any of the categories you chose to bypass from being decrypted, which improves overall performance by reducing the amount of outbound traffic that is decrypted and also preventing the decryption of undecryptable traffic. Decryption policies for inbound traffic protection only (using a Decrypt - Known Key rule action) include all of the same Do Not Decrypt rules in your policy but they will be disabled and can be enabled and modified as needed later. The Do Not Decrypt rules added are meant to prevent decrypting outbound connections for sensitive URL categories or undecryptable traffic. We assume traffic going to inbound servers should be decrypted and do not automatically bypass decryption for those inbound connections. For any decryption policy, you can edit, reorder, delete, disable, or enable all rules in the policy to meet your needs.
Access Control: Identity			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Passive identity agent for Microsoft AD.	7.6.0	Any	The passive identity agent identity source sends session data from Microsoft Active Directory (AD) to the management center. Passive identity agent software is supported on: • Microsoft AD server (Windows Server 2008 or later) • Microsoft AD domain controller (Windows Server 2008 or later) • Any client connected to the domain you want to monitor (Windows 8 or later)
Microsoft Azure AD realms for active or passive authentication.	7.6.0	Active: 7.6.0 with Snort 3 Passive: 7.4.1 with Snort 3	You can now use Microsoft Azure Active Directory (AD) realms for active and passive authentication: • Active authentication using Azure AD: Use Azure AD as a captive portal. • Passive authentication using Cisco ISE (introduced in Version 7.4.1): The management center gets groups from Azure AD and logged-in user session data from ISE. We use SAML (Security Assertion Markup Language) to establish a trust relationship between a service provider (the devices that handle authentication requests) and an identity provider (Azure AD). For upgraded management centers, existing Azure AD realms are displayed as SAML - Azure AD realms.
Event Logging and Analysis			
MITRE information in connection events.	7.6.0	7.6.0 with Snort 3	You can now find better insights into threat detections with: • Contextual enrichment of detections using the Talos taxonomy and enrichment service. • Simplified event analysis (link to ATT&CK framework and single pane view connecting different events with MITRE enrichment). • Content tagging for detections by EVE. New/modified screens: Connection events have two new fields: **MITRE ATT&CK** and **Other Enrichment**.
Filter unified events viewer by event type.	7.6.0	Any	The unified events viewer now has buttons under the Search field that allow you to quickly filter by event type.
Health Monitoring			
Collect health data without alerting.	7.6.0	Any	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. 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.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Administration			
Change management ticket takeover; more features in the approval workflow.	7.6.0	Any	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. 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.
Report template improvements.	7.6.0	Any	There is a new user interface for setting the search fields that appear in table-format sections of the report. The improved user interface now includes buttons for adding and deleting report fields, a drag-and-drop function for rearranging the fields, and simplified sorting options. New/modified screens: **Overview** > **Reporting** > **Report Templates** > **Create Report Template**, click the **Add Table View** icon, and then click the edit icon next to **Fields**.
New theme for the management center.	7.6.0	Any	We introduced a new left-hand navigation theme for the management center. To try it, click your user name in the top right corner and select the **New** theme. We also deprecated the Classic theme.
Subscribe to Cisco newsletters and other product-related communications.	7.6.0	Any	Provide an email address to receive sales and product renewal conversations, new release adoption newsletters, and other product-related communications from Cisco. Each management center user has its own email address. Do not associate the admin user with an email address that you cannot recover. New/modified screens: **System** (⚙) > **Users** > **Edit** > **Email Address**
Usability, Performance, and Troubleshooting			
Object group search enhancements.	7.6.0	Any	Object group search is now faster and uses fewer resources. New CLI commands: **clear asp table network-object**, **show asp table network-group** Modified CLI comments (enhanced output): **debug acl logs**, **packet-tracer**, **show access-list**, **show object-group**

Feature	Minimum Management Center	Minimum Threat Defense	Details
Troubleshoot Snort 3 performance issues with a CPU and rule profiler.	7.6.0	7.6.0 with Snort 3	New CPU and rule profilers help you troubleshoot Snort 3 performance issues. You can now monitor: • 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. New/modified screens: **Devices** > **Troubleshoot** > **Snort 3 Profiler** Platform restrictions: Not supported for container instances.
Receive additional threat defense troubleshooting syslogs, and view them as unified events.	7.6.0	Any with Snort 3	You can now configure threat defense devices to send all device troubleshooting syslogs (instead of just VPN troubleshooting syslogs) to the management center. New/modified screens: • To send device troubleshooting syslogs to the management center, use threat defense platform settings: **Devices** > **Platform Settings** > **Syslog** > **Logging to Secure Firewall Management Center** • To view all device troubleshooting syslogs, **Devices** > **Troubleshooting Logs** replaces **Devices** > **VPN** > **Troubleshooting**. • To view device troubleshooting syslogs in context with other events, use **Analysis** > **Unified Events**, where we added a **Troubleshoot Events** type.
Application detection debug logs in connection-based troubleshooting.	7.6.0	7.6.0 with Snort 3	Connection-based debugging (CBD) has already been adopted by different Snort 3 modules, such as File, SMB, and xTLS to emit logs at defined levels. Application detection (AppID) debugs are now included in the logs collected by the CBD framework, which helps you correlate information from the different Snort 3 modules. This feature enables Lua logging by default, making information collection easier and faster. New/modified CLI commands: **debug packet-module appid**

Feature	Minimum Management Center	Minimum Threat Defense	Details
Packet tracer improvements.	7.6.0	Identity trace data: 7.6.0 with Snort 3 Other improvements: Any	Packet tracker improvements allow you to: • Capture and replay identity trace data (requires threat defense 7.6.0 with Snort 3). • Replay packet trace data on NAT-configured devices. • Replay packet trace data that imitates the actual timing of the packets, for a more realistic simulation. • Save packet trace data as PCAP file, which can be viewed using third-party tools like Wireshark. New/modified commands: • To enable the timestamp option, use the **honor-timestamp** keyword in the **packet-tracer** command: **packet-tracer input***ifc_name* **pcap***pcap_filename* [**honor-timestamp**] • To store the device-generated packet trace data as part of the PCAP file, use the **export-pcapng** keyword in the **show packet tracer** command: **show packet-tracer pcap trace** [**export-pcapng**]

Bugs

Important Bug lists are auto-generated once and may not be subsequently updated. If updated, the 'table last updated' date does not mean that the list was fully accurate on that date—only that some change was made. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes. If you have a support contract, you can obtain up-to-date bug lists with the Cisco Bug Search Tool.

Table last updated: 2024-06-27

Table 3: Open Bugs in Version 7.6.0

Bug ID	Headline
CSCwk33577	Devices not listed to add a data node when creating a cluster because of OS version mismatch
CSCwk35876	S2S VPN Dashboard shows incorrect tunnel status for FTD HA device with standby IP configured
CSCwk36860	IPv6 tunnel packets to DVTI Tunnel source on vrf loopback dropped (acl-drop)
CSCwk36879	User authentication failed while login into FMC https

For Assistance

Install Guides

Table 4: Install Guides

Platform	Install Guide	Link
Management center virtual	Getting started guide for the management center virtual.	https://www.cisco.com/go/fmcv-quick
Threat defense virtual	Getting started guide for your threat defense virtual version.	https://www.cisco.com/go/ftdv-quick

More Online Resources

Cisco provides the following online resources to download documentation, software, and tools; to query bugs; and to open service requests. Use these resources to install and configure Cisco software and to troubleshoot and resolve technical issues.

- Documentation: http://www.cisco.com/go/ftd-docs
- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.cisco.com/cisco/support/notifications.html

Access to most tools on the Cisco Support & Download site requires a Cisco.com user ID and password.

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts