New Features in Cloud-delivered Firewall Management Center 2024

- Welcome to Security Cloud Control, on page 1
- November 8, 2024, on page 2
- August 23, 2024, on page 8
- June 6, 2024 , on page 15
- May 30, 2024, on page 15
- April 2, 2024, on page 16
- February 13, 2024, on page 16

Welcome to Security Cloud Control

Cisco Defense Orchestrator is now "Cisco Security Cloud Control."

Security Cloud Control is a new, AI-embedded management solution designed to unify the Cisco Security Cloud, starting with network security. It is a modern micro-app architecture with an updated user interface, common services, and a service-mesh that connects configuration, logs, and alerts across the security cloud.

It manages Secure Firewall Threat Defense and ASA firewalls, Multicloud Defense, and Hypershield with the intent to expand these management capabilities to additional security products. In addition, AI assistants proactively optimize policy and configuration, and find and troubleshoot issues.

Explore these new Security Cloud Control features:

- Centralized management experience of network security solutions
- A guided “Day 0” experience helping you to quickly onboard threat defense devices and discover new features
- Unified dashboard for end-to-end visibility of all of your managed devices
- Upgraded menu navigation and easy network and security application access for streamlined solution usability
- AI Assistant for ease of firewall rule creation and management
- Simplified operations and enhanced security with AIOps insights
- Policy analysis to improve security posture, eliminate misconfiguration, and optimize rules.

- Strengthened protection in hybrid environments with consistent policy enforcement and object sharing
- Improved monitoring of remote access and site-to-site VPN connections
- Increased scalability to support up to 1000 firewalls with a single tenant

For more information, see the Security Cloud Control product page, the Security Cloud Control documentation, and the FAQ.

November 8, 2024

Table 1: Features in Version 20241030

Feature	Minimum Threat Defense	Details
Platform		
Secure Firewall 1200.	7.6.0	We introduced the Secure Firewall 1200, which includes these models: • Secure Firewall 1210CX, with 8x1000BASE-T ports • Secure Firewall 1210CP, with 8x1000BASE-T ports. Ports 1/5-1/8 support power over Ethernet (PoE). • Secure Firewall 1220CX, with 8x1000BASE-T ports and two SFP+ ports. See: Cisco Secure Firewall CSF-1210CE, CSF-1210CP, and CSF-1220CX Hardware Installation Guide
Disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200.	7.6.0	You can now disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200. By default, the port is enabled. New/modified threat defense CLI commands: **system support usb show**, **system support usb port disable**, **system support usb port enable** New/modified FXOS CLI commands for the Secure Firewall 3100 in multi-instance mode: **show usb-port**, **disable USB port**, **enable usb-port** See: Cisco Secure Firewall Threat Defense Command Reference and Cisco Firepower 4100/9300 FXOS Command Reference
Device Management		

Feature	Minimum Threat Defense	Details
Device templates.	7.4.1	Device templates allow you to deploy multiple branch devices with pre-provisioned initial device configurations (zero-touch provisioning). You can also apply configuration changes to multiple devices with different interface configurations, and clone configuration parameters from existing devices. Restrictions: You can use device templates to configure a device as a spoke in a site-to-site VPN topology, but not as a hub. A device can be part of multiple hub-and-spoke site-to-site VPN topologies. New/modified screens: **Devices** > **Template Management** Supported platforms: Firepower 1000/2100, Secure Firewall 1200/3100. Note that Firepower 2100 support is for threat defense 7.4.1–7.4.x only; those devices cannot run Version 7.6.0. Learn more: • See "Device Management Using Device Templates" • See "Onboard Threat Defense Devices using Device Templates to Cloud-delivered Firewall Management Center using Zero-Touch Provisioning.
AAA for user-defined VRF interfaces.	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. In device platform settings, you can now associate a security zone or interface group having the VRF interface, with a configured external authentication server. New/modified screens: **Devices** > **Platform Settings** > **External Authentication** See: Enable Virtual-Router-Aware Interface for External Authentication of Platform
Policy Analyzer & Optimizer cross-launch for access control.	Any	The Policy Analyzer & Optimizer evaluates access control policies for anomalies such as redundant or shadowed rules, and can take action to fix discovered anomalies. You can now launch the Policy Analyzer & Optimizer directly from the access control policy page. Choose **Policies** > **Access Control**, select policies, and click **Analyze Policies**.
High Availability/Scalability		
Multi-instance mode for the Secure Firewall 4200.	7.6.0	Multi-instance mode is now supported on the Secure Firewall 4200. See: Multi-Instance Mode for the Secure Firewall 3100/4200

Feature	Minimum Threat Defense	Details
Multi-instance mode conversion in the management center for the Secure Firewall 3100/4200.	7.6.0	You can now register an application-mode device to the management center and then convert it to multi-instance mode without having to use the CLI. New/modified screens: • **Devices** > **Device Management** > > **Convert to Multi-Instance** • **Devices** > **Device Management** > **Select Bulk Action** > **Convert to Multi-Instance**
16-node clusters for the Secure Firewall 3100/4200.	7.6.0	For the Secure Firewall 3100 and 4200, the maximum nodes were increased from 8 to 16. See: Clustering for the Secure Firewall 3100/4200
Individual interface mode for Secure Firewall 3100/4200 clusters.	7.6.0	Individual interfaces are normal routed interfaces, each with their own local IP address used for routing. The main cluster IP address for each interface is a fixed address that always belongs to the control node. When the control node changes, the main cluster IP address moves to the new control node, so management of the cluster continues seamlessly. Load balancing must be configured separately on the upstream switch. Restrictions: Not supported for container instances. New/modified screens: • **Devices** > **Device Management** > **Add Cluster** • **Devices** > **Device Management** > **Cluster** > **Interfaces / EIGRP / OSPF / OSPFv3 / BGP** • **Objects** > **Object Management** > **Address Pools** > **MAC Address Pool** See: Clustering for the Secure Firewall 3100/4200 and Address Pools
Deploy threat defense virtual clusters across multiple AWS availability zones.	7.6.0	You can now deploy threat defense virtual clusters across multiple availability zones in an AWS region. This enables continuous traffic inspection and dynamic scaling (AWS Auto Scaling) during disaster recovery. See: Deploy a Threat Defense Virtual Cluster on AWS
Deploy threat defense virtual for AWS in two-arm-mode with GWLB.	7.6.0	You can now deploy threat defense virtual for AWS in two-arm-mode with GWLB. This allows you to directly forward internet-bound traffic after traffic inspection, while also performing network address translation (NAT). Two-arm mode is supported in single and multi-VPC environments. Restrictions: Not supported with clustering. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide

Feature	Minimum Threat Defense	Details
Interfaces		
Deploy without the diagnostic interface on threat defense virtual for Azure and GCP.	7.4.1	You can now deploy without the diagnostic interface on threat defense virtual for Azure and GCP. Previously, we required one management, one diagnostic, and at least two data interfaces. New interface requirements are: • Azure: one management, two data (max eight) • GCP: one management, three data (max eight) Restrictions: This feature is supported for new deployments only. It is not supported for upgraded devices. See: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
SD-WAN		
SD-WAN wizard.	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** See: Configure an SD-WAN Topology Using the SD-WAN Wizard
Access Control: Threat Detection and Application Identification		
QUIC decryption.	7.6.0 with Snort 3	You can configure the decryption policy to apply to sessions running on the QUIC protocol. QUIC decryption is disabled by default. You can selectively enable QUIC decryption per decryption policy and write decryption rules to apply to QUIC traffic. By decrypting QUIC connections, the system can then inspect the connections for intrusion, malware, or other issues. You can also apply granular control and filtering of decrypted QUIC connections based on specific criteria in the access control policy. We modified the decryption policy Advanced Settings to include the option to enable QUIC decryption. See: Decryption Policy Advanced Options

Feature	Minimum Threat Defense	Details
Snort ML: neural network-based exploit detector.	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
Allow Cisco Talos to conduct advanced threat hunting and intelligence gathering using your traffic.	7.6.0 with Snort 3	**Upgrade impact. Upgrade enables telemetry.** You can help Talos (Cisco's threat intelligence team) develop a more comprehensive understanding of the threat landscape by enabling threat hunting telemetry. With this feature, events from special intrusion rules are sent to Talos to help with threat analysis, intelligence gathering, and development of better protection strategies. This setting is enabled by default in new and upgraded deployments. New/modified screens: **System** (⚙) > **Configuration** > **Intrusion Policy Preferences** > **Talos Threat Hunting Telemetry** See: Intrusion Policy Preferences
Access Control: Identity		
Passive identity agent for Microsoft AD.	Any	This feature is introduced. 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) See: User Control With the Passive Identity Agent.

Feature	Minimum Threat Defense	Details
pxGrid Cloud Identity Source.		The Cisco Identity Services Engine (Cisco ISE) pxGrid Cloud Identity Source enables you to use subscription and user data from Cisco ISE in cloud-delivered Firewall Management Center access control rules. The pxGrid cloud identity source enables the use of constantly changing dynamic objects from ISE to be used for user control in access control policies in the cloud-delivered Firewall Management Center. New/updated screens: **Integration** > **Other Integrations** > **Identity Sources** > **Identity Services Engine (pxGrid Cloud)** See: User Control with the pxGrid Cloud Identity Source
New connectors for Cisco Secure Dynamic Attributes Connector	Any	Cisco Secure Dynamic Attributes Connector now supports AWS security groups, AWS service tags, and Cisco Cyber Vision. Version restrictions: For on-prem Cisco Secure Dynamic Attributes Connector integrations, requires Version 3.0. See Amazon Web Services Connector—About User Permissions and Imported Data,
Microsoft Azure AD realms for active or passive authentication.	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 7.4.0): 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. **Upgrade impact**. If you had a Microsoft Azure AD realm configured before the upgrade, it is displayed as a SAML - Azure AD realm configured for passive authentication. All previous user session data is preserved. New/modified screens: **Integration** > **Other Integrations** > **Realms** > **Add Realm** > **SAML - Azure AD** New/modified CLI commands: none See: Create a Microsoft Azure AD (SAML) Realm.
Event Logging and Analysis		

Feature	Minimum Threat Defense	Details
MITRE and other enrichment information in connection events.	7.6.0 with Snort 3	MITRE and other enrichment information in connection events makes it easy to access contextual information for detected threats. This includes information from Talos and from the encrypted visibility engine (EVE). For EVE enrichment, you must enable EVE. Connection events have two new fields, available in both the unified and classic event viewers: • **MITRE ATT&CK**: Click the progression graph to see an expanded view of threat details, including tactics and techniques. • **Other Enrichment**: Click to see any other available enrichment information, including from EVE. The new Talos Connectivity Status health module monitors management center connectivity with Talos, which is required for this feature. For the specific internet resources required, see Internet Access Requirements. See Configure EVE.
Administration		
New theme for the management center..	Any	We introduced new left-hand navigation for the cloud-deilvered Firewall Management Center for streamlined usability; and updated the look and feel of the interface.

August 23, 2024

Table 2: 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	You can now manage threat defense devices running Version 7.6.0. **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 *on-prem* management center guide that matches your threat defense version. **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.
High Availability/Scalability		

Feature	Minimum Threat Defense	Details
Multi-instance mode for the Secure Firewall 3100.	7.4.1	You can deploy the Secure Firewall 3100 as a single device (*appliance mode*) or as multiple container instances (*multi-instance mode*). 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 (*chassis upgrade*) separately from the container instances (*threat defense upgrade*). New/modified screens: • **Inventory** > **FTD Chassis** • **Devices** > **Device Management** > **Device** > **Chassis Manager** • **Devices** > **Platform Settings** > **New Policy** > **Chassis Platform Settings** • **Devices** > **Chassis Upgrade** New/modified threat defense CLI commands: **configure multi-instance network ipv4**, **configure multi-instance network ipv6** New/modified FXOS CLI commands: **create device-manager**, **set deploymode** Platform restrictions: Not supported on the Secure Firewall 3105. See: Use Multi-Instance Mode for the Secure Firewall and Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center
Access Control: Threat Detection and Application Identification		
Easily bypass decryption for sensitive and undecryptable traffic.	Any	It is now easier to bypass decryption for sensitive and undecryptable traffic, which protects users and improves performance. 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. 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. New/modified screens: **Policies** > **Access Control** > **Decryption** > **Create Decryption Policy** See: Create a Decryption Policy See: Create a Decryption Policy

Feature	Minimum Threat Defense	Details
Access Control: Identity		
Microsoft Azure AD as a user identity source.	7.4.2	You can use a Microsoft Azure Active Directory (Azure AD) realm with ISE to authenticate users and get user sessions for user control. New/modified screens: • **Integration** > **Other Integrations** > **Realms** > **Add Realm** > **Azure AD** • **Integration** > **Other Integrations** > **Realms** > Actions, such as downloading users, copying, editing, and deleting Supported ISE versions: 3.0 patch 5+, 3.1 (any patch level), 3.2 (any patch level) See: Create a Microsoft Azure Active Directory Realm
Health Monitoring		
Collect health data without alerting.	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. See: Health Policies
Apply a default health policy upon device registration.	Any	You can now choose a default health policy to apply upon device registration. On the health policy page, the policy name indicates which is the default. If you want to use a different policy for a specific device post-registration, change it there. You cannot delete the default device health policy. New/modified screens: **System** (⚙) > **Health** > **Policy** > **More** (⋮) > **Set as Default** See: Set a Default Health Policy

Feature	Minimum Threat Defense	Details
Chassis-level health alerts for the Firepower 4100/9300.	7.4.1	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. 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. New/modified screens: **Inventory** > **FTD Chassis** See: Onboard a Chassis
Administration		
Threat defense high availability automatically resumes after restoring from backup.	7.6.0	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. Version restrictions: Not supported with threat defense Version 7.0–7.0.6, 7.1.x, 7.2.0–7.2.9, 7.3.x, or 7.4.0–7.4.2. See: Restore Security Cloud Control-Managed Devices
Change management ticket takeover; more features in the approval workflow.	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. See: Change Management
Troubleshooting		

Feature	Minimum Threat Defense	Details
Troubleshoot Snort 3 performance issues with a CPU and rule profiler.	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 Profiling** Platform restrictions: Not supported for container instances. See: Advanced Troubleshooting for the Secure Firewall Threat Defense Device See: Advanced Troubleshooting for the Secure Firewall Threat Defense Device
Deprecated Features		

Feature	Minimum Threat Defense	Details
End of support: analytics-only capabilities with the full range of threat defense devices.	Any	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. 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. You can be prevented from: • 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. 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. In order of preference, you can: • 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. That is, your choices are: • 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 3: Features in Version 20240514

Feature	Minimum Threat Defense	Details
Platform Migration		

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 4: 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: • 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	The Firepower 9300 now supports these optical transceivers: • QSFP-40/100-SRBD • QSFP-100G-SR1.2 • QSFP-100G-SM-SR On these network modules: • FPR9K-NM-4X100G • FPR9K-NM-2X100G • FPR9K-DNM-2X100G See: Cisco Firepower 9300 Hardware Installation Guide
Performance profile support for the Secure Firewall 3100.	7.4.1	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. See: Configure the Performance Profile
NAT		
Create network groups while editing NAT rules.	Any	You can now create network groups in addition to network objects while editing a NAT rule. See: Customizing NAT Rules for Multiple Devices
Device Management		
Device management services supported on user-defined VRF interfaces.	Any	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. Platform restrictions: Not supported with container instances or clustered devices. See Platform Settings
SD-WAN		
SD-WAN Summary dashboard	7.4.1	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. New/modified screens: **Analysis** > **SD-WAN Summary** See: SD-WAN Summary Dashboard

Feature	Minimum Threat Defense	Details
Access Control: Identity		
Captive portal support for multiple Active Directory realms (realm sequences).	7.4.1	**Upgrade impact. Update custom authentication forms.** 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. 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. If you use the HTTP Response Page authentication type, after you upgrade threat defense, you must add **`<select name="realm" id="realm"></select>`** to your custom authentication form. This allows the user to choose between realms. Restrictions: Not supported with Microsoft Azure Active Directory. New/modified screens: • **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** See: How to Configure the Captive Portal for User Control
Share captive portal active authentication sessions across firewalls.	7.4.1	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 *disable* this option. • (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. New/modified screens: **Policies** > **Identity** > **(edit policy)** > **Active Authentication** > **Share active authentication sessions across firewalls** See: How to Configure the Captive Portal for User Control
Deployment and Policy Management		

Feature	Minimum Threat Defense	Details
View and generate reports on configuration changes since your last deployment.	Any	You can generate, view, and download (as a zip file) the following reports on configuration changes since your last deployment: • 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. This is especially useful after you upgrade threat defense devices, so that you can see the changes made by the upgrade before you deploy. New/modified screens: **Deploy** > **Advanced Deploy**. See: Download Policy Changes Report for Multiple Devices
Suggested release notifications.	Any	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. See: Cisco Secure Firewall Management Center New Features by Release
Enable revert from the threat defense upgrade wizard.	Any	You can now enable revert from the threat defense upgrade wizard. Other version restrictions: You must be upgrading threat defense to Version 7.2+. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center
View detailed upgrade status from the threat defense upgrade wizard.	Any	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. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center

Feature	Minimum Threat Defense	Details
Firmware upgrades included in FXOS upgrades.	Any	**Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.** For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1 now include firmware upgrades. 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. Just as with software and operating system upgrades, do not make or deploy configuration changes during firmware upgrade. Even if the system appears inactive, do not manually reboot or shut down during firmware upgrade. See: Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide
Upgrade		
Improved upgrade starting page and package management.	Any	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. 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. New/modified screens: • **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. Deprecated screens/options: • **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. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center
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 *VDB lite*) on lower memory devices running Snort 2. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Lower memory devices: ASA-5508-X 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: Health alerts for `frequent drain of events`.	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: Disk Usage and Drain of Events Health Monitor Alerts

February 13, 2024