



KEY NEW FEATURES IN

Sophos Firewall OS v23

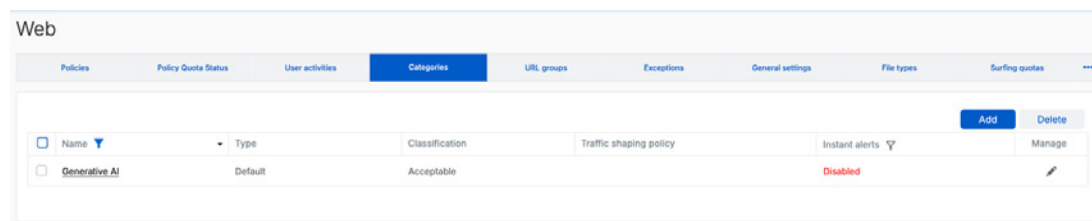
AI and Automation

Sophos Firewall v23 enhances how you manage AI usage within your network, interact with your firewall using AI, and how you protect your network from AI attacks.

Controlling and governing AI at the network level

Sophos Firewall plays a key role in the new Sophos AI Defense solution that enables you to see and control AI usage across your organization quickly and easily. Sophos Firewall provides important network visibility into AI usage and provides an essential enforcement point, especially when combined with DNS Protection included in Xstream Protection licenses for Sophos Firewall. If you haven't already, be sure to check out [Sophos AI Defense](#) and how it can help provide added visibility and control into AI usage on your network.

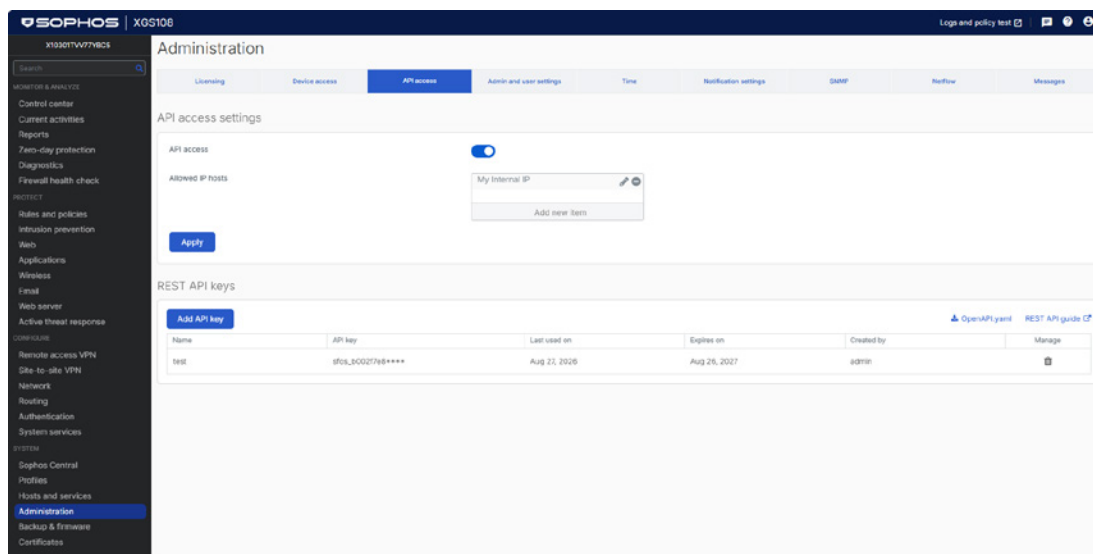
Sophos Firewall v23 also continues to strengthen controls for enabling access to sanctioned AI tools, restricting access to unsanctioned ones, and limiting sensitive data movement into generative AI services. Sophos Firewall's application filters detect and control GenAI traffic at the network level, and a new 'Generative AI' web category makes it easy to build policy around these sites. This complements the new Generative AI category added to Sophos DNS Protection in August and enhancements to Sophos Workspace Protection and Endpoint Web Control for GenAI, enabling consistent policy across all your available enforcement points.



REST API with token-based authentication

Sophos Firewall OS v23 delivers a modern REST API for seamless integration with your existing IT, security, and automation workflows. You can automate routine tasks such as deploying configurations, updating policies, responding to security events, and integrating with orchestration and management platforms. Secure token-based (API key) authentication provides controlled access, while support for the OpenAPI 3.0 specification makes it easy to automate and integrate using industry-standard tools and development frameworks that you use in your business everyday.

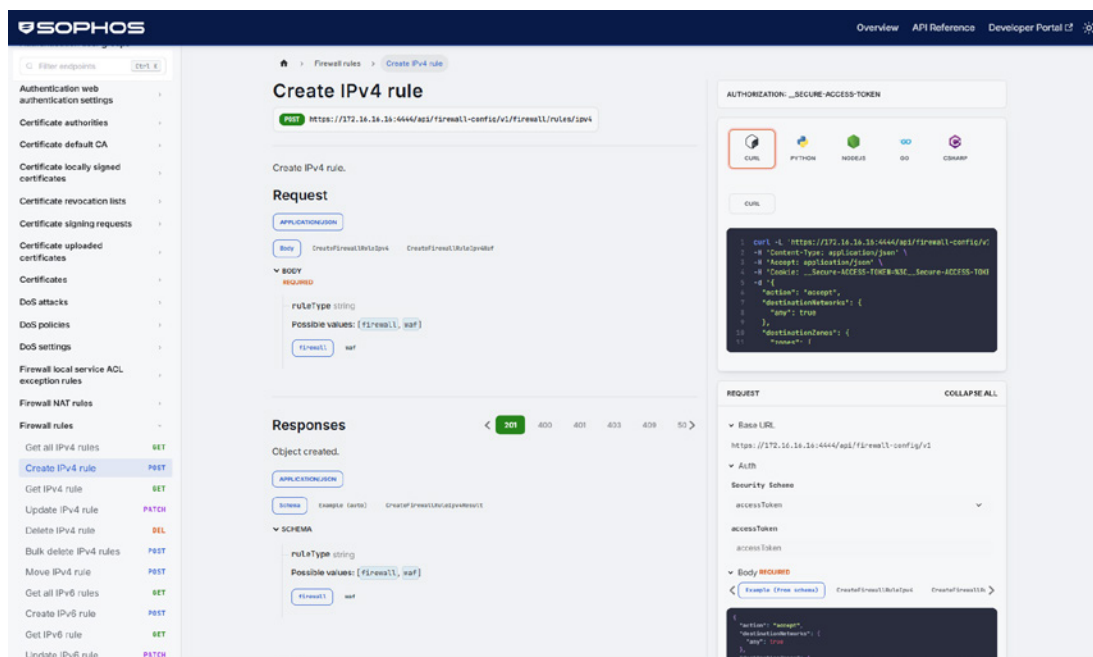
API access is configured under Administration > API access, where you create and manage API keys, set expiry, and restrict access to specific allowed IP hosts.



REST API keys are created and managed under Administration > API access, with per-key expiry and allowed IP host restrictions.

REST API interactive guide

To make the REST API easy to explore and use, v23 includes an [interactive API guide](#) built directly into the firewall. You can browse every available endpoint, and inspect request and response schemas, and example payloads — which dramatically shortens the path from evaluation to working automation.

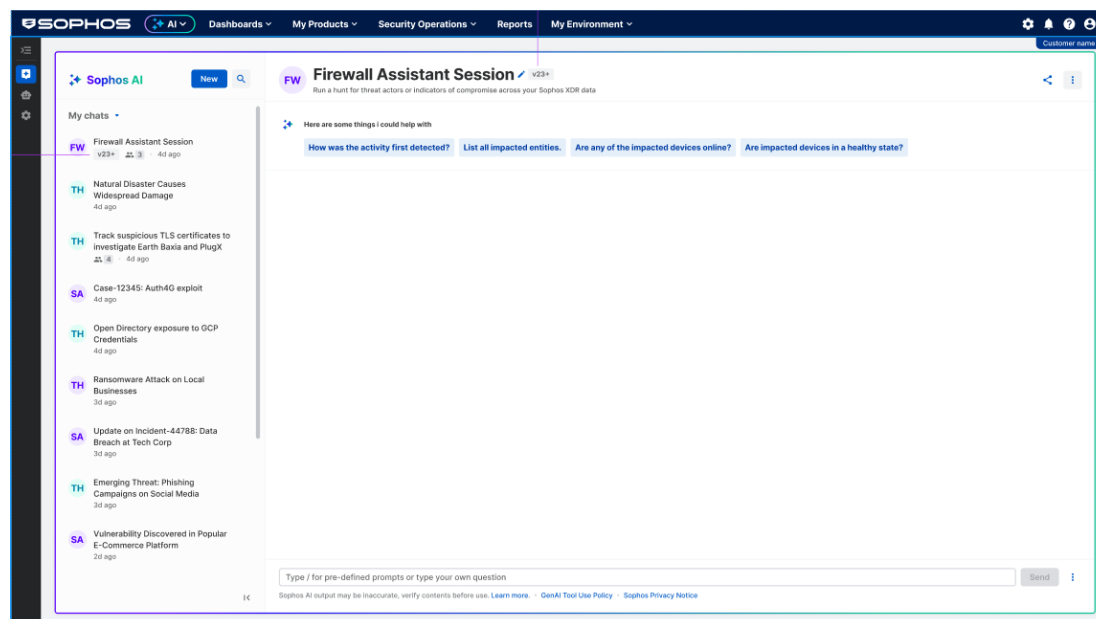


The interactive API guide lets your developers browse endpoints, inspect schemas, and test live requests against their own firewall.

Sophos Firewall AI Assistant

Along with Sophos Firewall OS v23, we are introducing an interactive chat assistant for Sophos Firewall, hosted in Sophos Fusion, that understands natural language queries.

Phase 1, introduced in this release, focuses on firewall rules. The assistant is read-only by design, with one deliberate exception: it can create a firewall rule from a prompt, but that rule is always created in a disabled state and placed last in the rule table. Nothing takes effect until you log into the firewall, review the rule, and enable it. The assistant's access to data is scoped to exactly what an administrator would see when accessing the firewall via Sophos Fusion SSO.



The Sophos Firewall AI Assistant in Sophos Fusion understands natural language queries and offers pre-defined prompts to get administrators started.

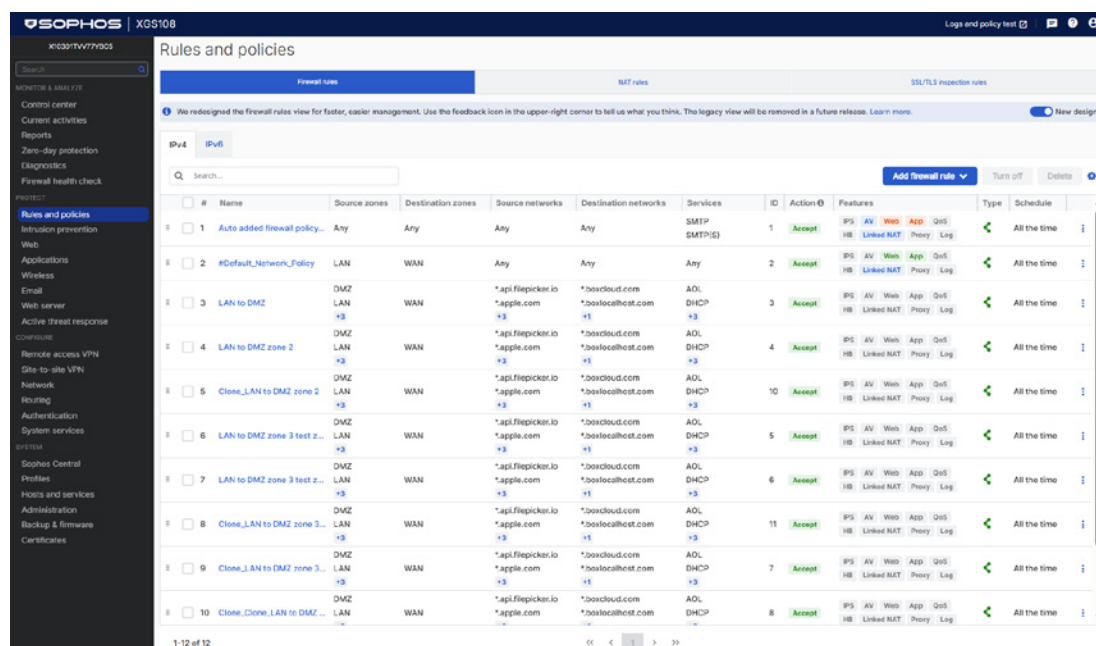
Broader configuration support is planned for future releases.

Streamlined Management and Resiliency Enhancements

Sophos Firewall v23 brings important top requested management and resiliency enhancements. Those of you who manage multiple firewalls will be particularly excited.

Redesigned firewall rule management

The firewall rule management experience has been rebuilt around a cleaner, more flexible table layout. You can select, resize, and freeze columns to suit how you work, use free text to search for firewall rule names, and filter across all of your data.



ID	Name	Source zones	Destination zones	Source networks	Destination networks	Services	ID	Action	Features	Type	Schedule
1	Auto added firewall policy...	Any	Any	Any	Any	SMTP SMTP(S)	1	Accept	IPS AV Web App QoS HB Linked NAT Proxy Log		All the time
2	#Default_Network_Policy	LAN	WAN	*api.fireplex.io *apple.com	*booncloud.com *boonlocalhost.com	AOL DHCP	2	Accept	IPS AV Web App QoS HB Linked NAT Proxy Log		All the time
3	LAN to DMZ	DMZ LAN	WAN	*api.fireplex.io *apple.com	*booncloud.com *boonlocalhost.com	AOL DHCP	3	Accept	IPS AV Web App QoS HB Linked NAT Proxy Log		All the time
4	LAN to DMZ zone 2	DMZ LAN	WAN	*api.fireplex.io *apple.com	*booncloud.com *boonlocalhost.com	AOL DHCP	4	Accept	IPS AV Web App QoS HB Linked NAT Proxy Log		All the time
5	Clone_LAN to DMZ zone 2	DMZ LAN	WAN	*api.fireplex.io *apple.com	*booncloud.com *boonlocalhost.com	AOL DHCP	10	Accept	IPS AV Web App QoS HB Linked NAT Proxy Log		All the time
6	LAN to DMZ zone 3 test z...	DMZ LAN	WAN	*api.fireplex.io *apple.com	*booncloud.com *boonlocalhost.com	AOL DHCP	5	Accept	IPS AV Web App QoS HB Linked NAT Proxy Log		All the time
7	LAN to DMZ zone 3 test z...	DMZ LAN	WAN	*api.fireplex.io *apple.com	*booncloud.com *boonlocalhost.com	AOL DHCP	6	Accept	IPS AV Web App QoS HB Linked NAT Proxy Log		All the time
8	Clone_LAN to DMZ zone 3...	DMZ LAN	WAN	*api.fireplex.io *apple.com	*booncloud.com *boonlocalhost.com	AOL DHCP	11	Accept	IPS AV Web App QoS HB Linked NAT Proxy Log		All the time
9	Clone_LAN to DMZ zone 3...	DMZ LAN	WAN	*api.fireplex.io *apple.com	*booncloud.com *boonlocalhost.com	AOL DHCP	7	Accept	IPS AV Web App QoS HB Linked NAT Proxy Log		All the time
10	Clone_Clone_LAN to DMZ...	DMZ LAN	WAN	*api.fireplex.io *apple.com	*booncloud.com *boonlocalhost.com	AOL DHCP	8	Accept	IPS AV Web App QoS HB Linked NAT Proxy Log		All the time

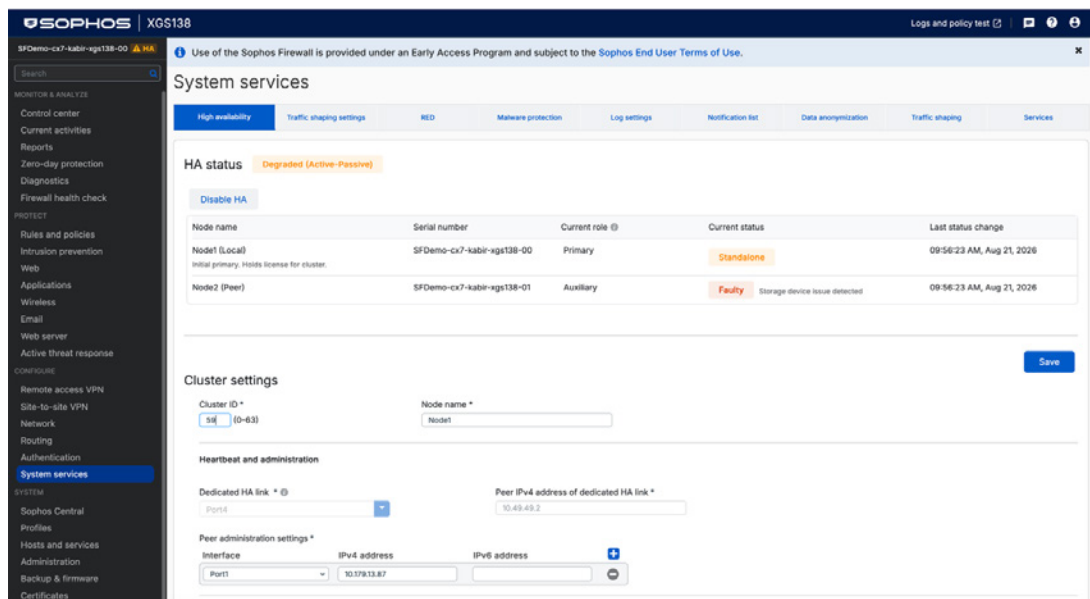
The new firewall rule table shows one rule per row in a unified view, with free-text search, column control, and inline editing.

High-availability (HA) enhancements

Hardware-aware HA - High availability in Sophos Firewall v23 now goes beyond link and service monitoring to include specific hardware resources such as the SSD. The cluster can fail over automatically when SSD health deteriorates to prevent a degraded appliance from disrupting operations.

Faster failover detection - Sophos Firewall now detects genuine peer failures 13x faster. Accelerated keepalive reduces the HA failover detection window from 4 seconds to 300ms.

Improved HA stability under heavy load - HA Heartbeat (keepalive) packets now use an enhanced, prioritized processing path that is isolated from the data traffic pipeline, preventing congestion and CPU pressure from delaying HA heartbeat processing. Adaptive scheduling automatically increases HA heartbeat priority as the system load rises, significantly reducing missed keepalive packets and unexpected HA failovers during high-throughput traffic periods, traffic surges, and DDoS conditions. Automatic fallback ensures improved HA heartbeat stability across platforms and interfaces.



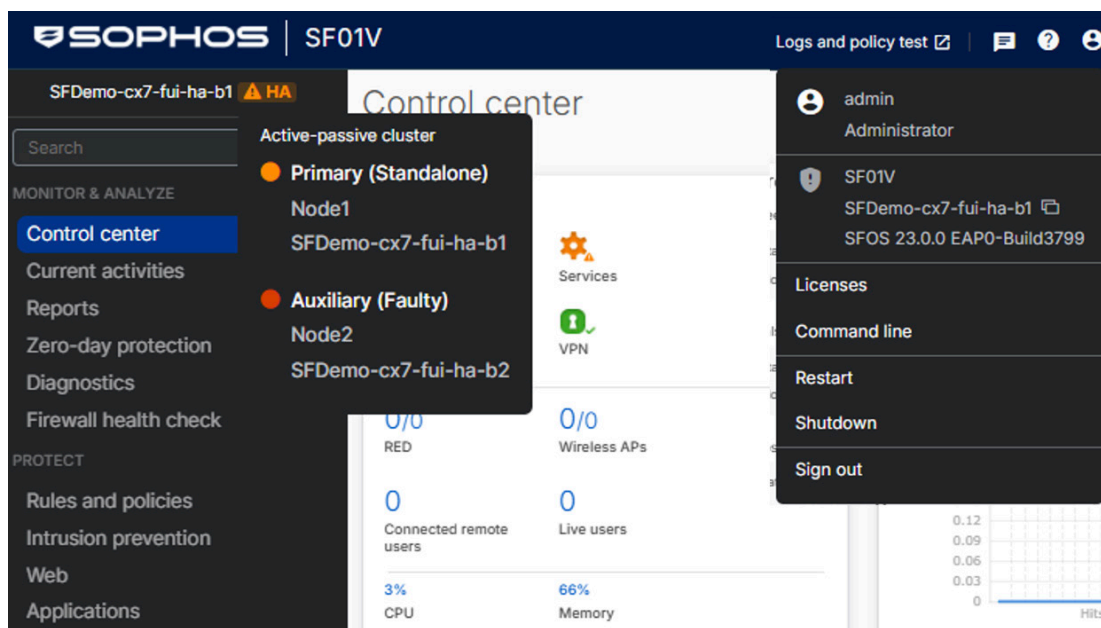
The refreshed High Availability page shows per-node role, status, and status detail (including SSD failures), with hardware component monitoring and tunable keepalive settings.

Other Management Enhancements:

UI performance enhancements - The on-box web admin interface now uses HTTP/2, improving page load performance and responsiveness, particularly on higher-latency connections.

Top navigation enhancements - Sophos Firewall v23 now keeps the serial number visible on the left at all times with a new “Copy” option that makes it easy to copy the serial number. This is a small change that removes a surprising amount of daily friction for administrators and support engineers.

HA cluster state is also surfaced directly at the top of the navigation menu, so node roles and health are visible at a glance from any screen. The right-side top menu now displays the Model, Serial Number, and Hostname for added convenience.



Enhanced top navigation keeps the serial number visible and adds HA status.

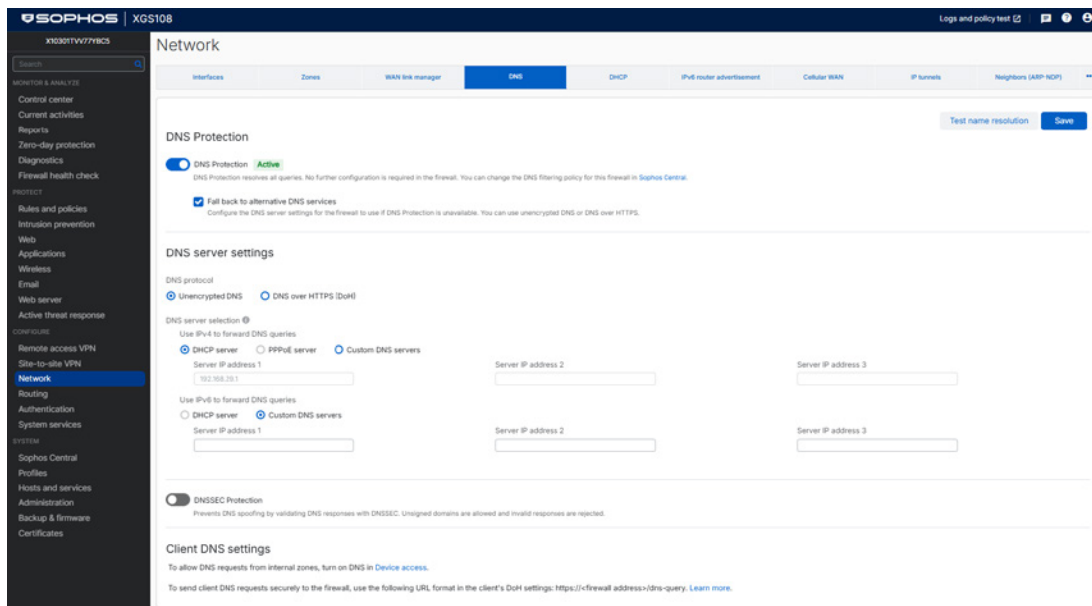
Secure by Design

Sophos Firewall is unique in the industry in being the most Secure by Design, making it a formidable target in the AI era. Our last major release, v22, took Secure by Design to a whole new level, and with this release, we continue to extend the Sophos Firewall Secure by Design advantage further by reducing the attack surface with DNS over HTTPS and providing greater visibility into automated hotfixes while further automating maintenance and feature firmware updates.

DNS over HTTPS

Sophos Firewall v23 simplifies DNS Protection deployment with a single-click and now enhances security using DNS over HTTPS (DoH). By encrypting DNS requests, it helps prevent DNS interception and tampering, strengthening DNS security and adding another layer to Sophos Firewall's Secure by Design architecture.

Sophos Firewall now supports DNS Security Extensions (DNSSEC), which uses cryptographic signatures to authenticate DNS responses and verify the integrity of DNS data received from authoritative DNS servers. By validating the DNSSEC signature chain of trust, including DNSKEY and DS records, the firewall can detect forged or modified DNS responses and help prevent attacks such as DNS cache poisoning and DNS spoofing. This provides an additional layer of protection for DNS.

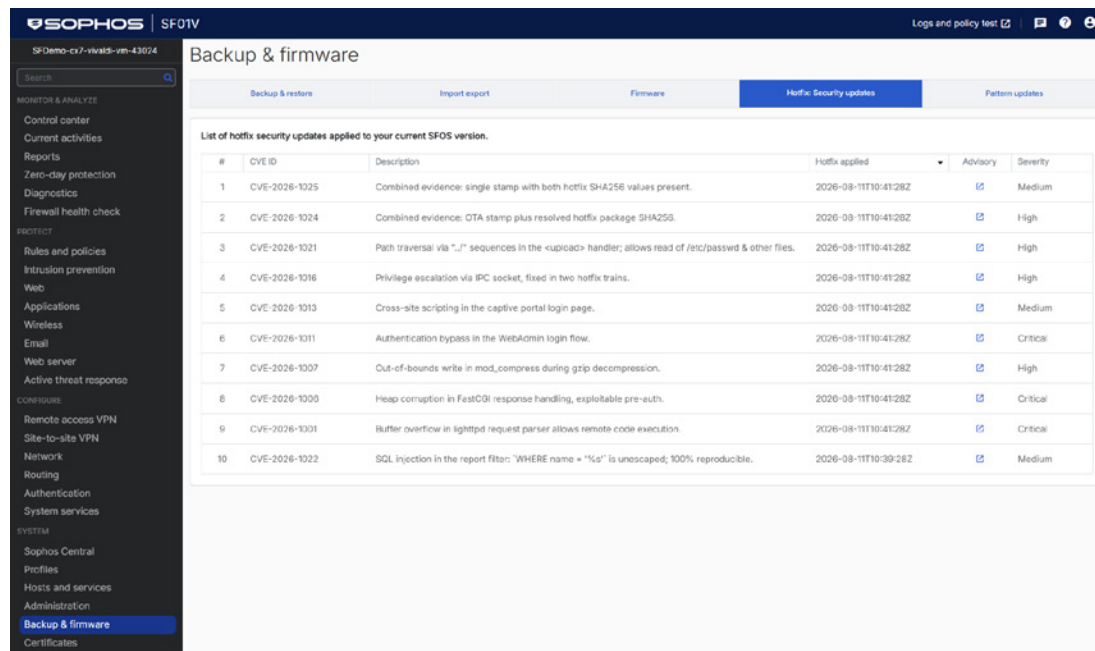


Sophos DNS Protection is now a single toggle, and DNS server settings support DNS over HTTPS with Sophos or a generic DoH provider.

Hotfix and Security Update Visibility

Sophos Firewall is unique in offering over-the-air hotfix security updates that patch new vulnerabilities without scheduling downtime. In Sophos Firewall v23, hotfix details now appear directly in the firewall UI, giving administrators clear insight into which security updates have been applied, including CVE ID, description, the date applied, a link to the associated advisory, and severity. You can find this under “Backup and Firmware” on a new “Hotfix Security Updates” tab.

The same visibility is carried consistently across the Log Viewer, email notifications, and Central Firewall Reporting (CFR), so the information is available wherever you are already working.



The screenshot displays the Sophos Firewall v23 web interface. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The main content area is titled 'Backup & firmware' and includes tabs for 'Backup & restore', 'Import export', 'Firmware', 'Hotfix Security updates' (which is selected), and 'Pattern updates'. Below the tabs, a table lists 'List of hotfix security updates applied to your current SFOS version.' with columns for #, CVE ID, Description, Hotfix applied, Advisory, and Severity.

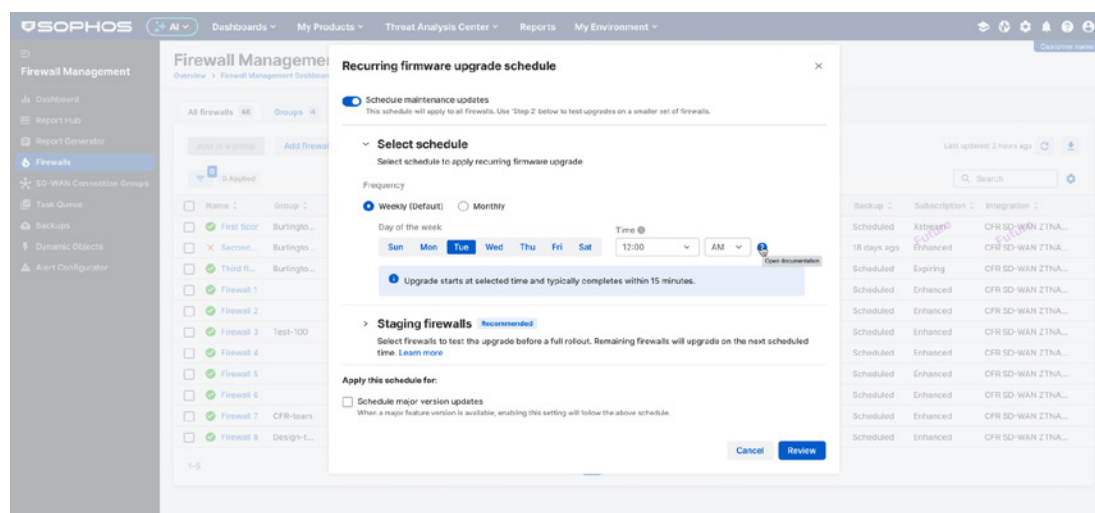
#	CVE ID	Description	Hotfix applied	Advisory	Severity
1	CVE-2026-1025	Combined evidence: single stamp with both hotfix SHA256 values present.	2026-08-11T10:41:28Z	[Link]	Medium
2	CVE-2026-1024	Combined evidence: OTA stamp plus resolved hotfix package SHA256.	2026-08-11T10:41:28Z	[Link]	High
3	CVE-2026-1021	Path traversal via "./" sequences in the <cupicad> handler; allows read of /etc/passwd & other files.	2026-08-11T10:41:28Z	[Link]	High
4	CVE-2026-1016	Privilege escalation via IPC socket, fixed in two hotfix trains.	2026-08-11T10:41:28Z	[Link]	High
5	CVE-2026-1013	Cross-site scripting in the captive portal login page.	2026-08-11T10:41:28Z	[Link]	Medium
6	CVE-2026-1011	Authentication bypass in the WebAdmin login flow.	2026-08-11T10:41:28Z	[Link]	Critical
7	CVE-2026-1007	Out-of-bounds write in mod_compress during gzip decompression.	2026-08-11T10:41:28Z	[Link]	High
8	CVE-2026-1008	Heap corruption in FastCGI response handling, exploitable pre-auth.	2026-08-11T10:41:28Z	[Link]	Critical
9	CVE-2026-1001	Buffer overflow in lighttpd request parser allows remote code execution.	2026-08-11T10:41:28Z	[Link]	Critical
10	CVE-2026-1022	SQL injection in the report filter: 'WHERE name = "%s"' is unescaped; 100% reproducible.	2026-08-11T10:39:28Z	[Link]	Medium

A new Hotfix: Security updates view lists every hotfix applied to the current SFOS version, with CVE, description, advisory link, and severity.

Automated firmware Update schedules

While automated hotfixes are an extremely helpful and important tool for addressing security updates with zero down-time and effort, it's still important to keep firewalls up to date with the latest firmware releases such as Maintenance Releases (MRs) and major feature updates like v23.

Sophos Fusion now further automates firmware updates by letting you define a recurring update schedule for maintenance releases, thereby keeping your firewalls up to date automatically following a release. Staged rollouts and per-firewall overrides provide granular control while reducing the operational effort of managing firmware updates across large firewall estates.



Recurring firmware upgrade schedules in Central Firewall Management, with staging firewalls and optional inclusion of major version updates.

Additional Secure by Design enhancements

Routing Engine Upgrade - Upgraded the SFOS routing engine to a more secure, modern, and feature-rich version of FRR.

Unified routing console - Adds a single interface to access and manage multiple routing protocols. It also brings BFD support as an experimental feature for BGP and static routes, enabling customers to explore faster failure detection and enhanced routing resilience in standalone deployments.

Extended Active Threat Response Events - Alerts are now generated without placing the endpoint into a RED Heartbeat status or isolating it to provide visibility without cutting off access automatically.

Authentication and Identity

Sophos Firewall OS v23 broadens identity support significantly – across cloud identity providers, hybrid directories, and multi-user and non-Windows endpoints

Entra ID Support for Synchronized Security

Sophos Firewall v23 extends Entra ID integration to authenticate clients running Sophos Endpoint and using Synchronized Security. Both on-premises AD and Entra ID can now operate together in a hybrid deployment.

Where you have already configured Entra ID SSO, the firewall will now automatically utilize Synchronized User ID functionality with no additional setup. Users can now authenticate seamlessly across hybrid environments – Entra ID alongside on-premises AD – with no captive portal login required, and Sophos Firewall maps identity consistently using UPN for Entra ID and sAMAccountName for on-premises AD. Windows endpoint support arrives with the 2025.1 release.

Google Identity Provider (IdP) support

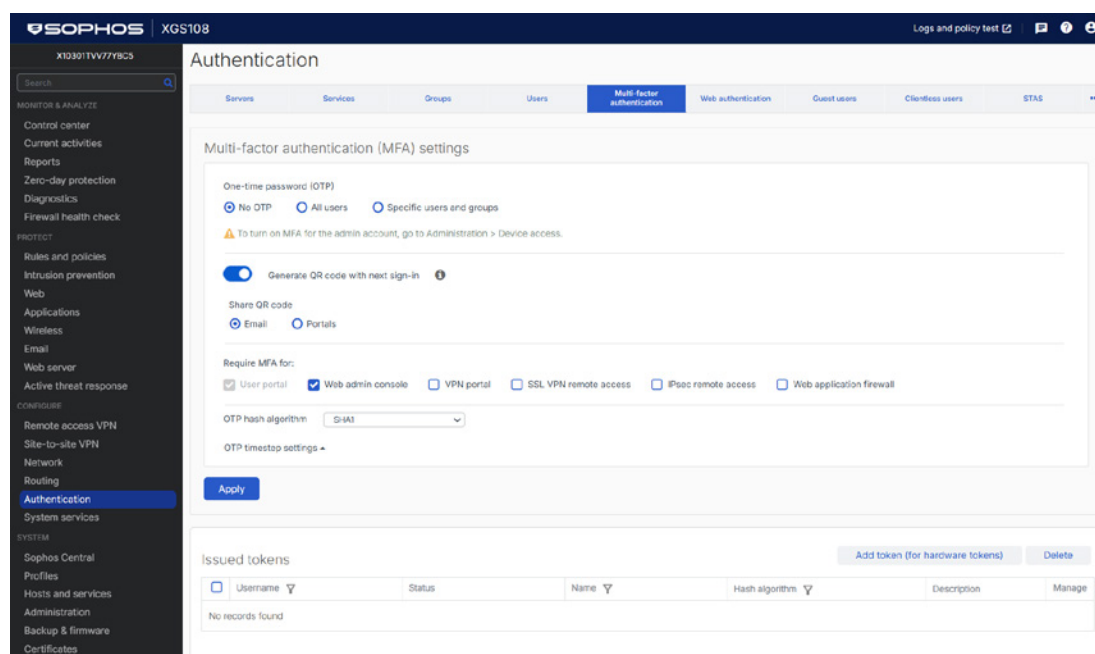
Sophos Firewall v23 now enables authentication of users through Google Identity Provider, adding SSO integration with the Google Workspace IdP. This unifies authentication across the Captive Portal, VPN Portal, Sophos Connect client, and WebAdmin console, and it supports IdP-enforced MFA. The capability suits cloud-first and hybrid organizations moving away from traditional LDAP integration. Note that a single IdP server is used for authentication for a given set of services.

The screenshot displays the Sophos Firewall OS v23 web interface. The left sidebar shows the navigation menu with 'Authentication' selected. The main content area is titled 'Add external server' and contains a form for configuring an external identity provider. The form is divided into several sections: 'General settings', 'Redirect URIs', and 'OpenID Connect URLs'. In the 'General settings' section, 'Server name' is set to 'Server name', 'Server type' is 'OpenID Connect', 'IdP vendor' is 'Google Workspace', 'Client ID' is 'Client ID', and 'Client secret' is 'Client secret'. In the 'Redirect URIs' section, 'Use firewall URL' is selected. In the 'OpenID Connect URLs' section, 'Issuer URL' is 'https://accounts.google.com', 'Discover/Reset endpoint URLs' is 'https://', 'Authorization URL' is 'https://', 'Token URL' is 'https://', 'JWKS URL' is 'https://', 'User info URL' is 'https://', and 'Logout URL' is 'https://'. The 'Send token in logout URL' checkbox is unchecked. At the bottom of the form are buttons for 'Test connection', 'Save', and 'Cancel'.

Google Workspace is added as an OpenID Connect server under Authentication > Servers, with user attribute mapping for display name, username, and email.

Secure MFA Onboarding via E-mail-Based QR Code

The firewall now delivers MFA onboarding QR codes securely via email, reducing the risk of QR code exposure on portals during brute-force or credential-stuffing attacks. Email-based onboarding becomes the default for new deployments so administrators should confirm that user email details are correct; existing and migrated deployments continue to use portal-based onboarding. Unused QR codes expire automatically after 24 hours, and users must complete their first login within that window or re-enroll.



A new QR code via email option is available under Authentication > Multi-factor authentication

Sophos Chromebook user ID SSO

A new Chromebook plug-in built on Manifest V3 is available via the [Chrome Web Store](#), enabling seamless Chromebook SSO with a quick installation and setup. The plug-in is designed to be SFOS version-independent, so it works across all supported Sophos Firewall versions – a meaningful simplification for those of you with large fleets of Chromebooks.

Sophos Authentication for Thin Client (SATC) with the XDR Sensor

A new lightweight XDR Sensor mode deploys alongside existing third-party endpoint and AV solutions without requiring replacement. By integrating Synchronized App Control into the XDR Sensor, the firewall brings user-level identity awareness to shared and terminal servers, enabling per-user web, application, and firewall policy enforcement in multi-user environments such as RDP and Terminal Server. This ensures accurate user mapping even in session-based environments where several users share a single server.

Scalability enhancements

WAF Request Redirection – Granular Traffic Actions per Site Path

SFOS now supports configurable per-path actions within WAF rules, closing a long-standing feature **gap with SG/UTM9**. Administrators can assign one of four actions to each site path entry:

- **Protect** - Standard WAF inspection (existing behaviour, now explicitly selectable)
- **Block** - Return a static 403 response for specified paths
- **Redirect** - Redirect traffic to a specified URL with configurable protocol, host, port, and path
- **Passthrough** - WebSocket passthrough without WAF inspection

Additionally, multiple paths (up to 128) can now be grouped within a single site path route entry, enabling more compact WAF rule configurations. All changes are fully supported via the updated UI traffic routing table and XML API. Existing WAF rules are seamlessly migrated to the new model with the “Protect” action as default.

The screenshot shows the 'Add path' configuration window. The 'Paths *' field has a search bar with a plus icon. The 'Action *' dropdown is set to 'Redirect'. The 'Response code *' dropdown is open, showing options: Multiple Choices (300), Resource Moved Permanently (...), Resource Moved Temporarily (3..., See Another Resource (303), Resource Not Modified (304), Use Proxy (305), Temporary Redirection (307), and Permanent Redirect (308). Other fields like 'Protocol *', 'Host *', 'Path *', and 'Port' are empty. 'Save' and 'Cancel' buttons are at the bottom.

WAF Rule Limit Expanded

SFOS now supports up to 100 WAF rules by default, with the option to increase the limit to 200 for configurations that require it. Organisations with larger or more complex web application environments can now protect more workloads within a single firewall — without hitting rule count limits or needing workarounds.

WAF Performance and Scalability Improvements

Sophos Firewall's Web Application Firewall (WAF) has been re-architected to use **Apache Event MPM**, delivering significant improvements in throughput, scalability, and resilience under load.

Previously, WAF request processing relied on a fixed thread-per-request model that left worker threads idling while waiting on backend tasks such as AV scanning — capping effective concurrency and making the system easier to saturate.

With Event MPM, request processing is broken into parallel tasks handled by free worker threads, so no thread sits idle waiting for a single request to complete. The result:

- **Higher throughput** - workers are kept busy across multiple concurrent requests rather than blocked on a single one
- **Better scalability under load** - the system continues accepting new requests even when all workers are actively processing tasks, absorbing traffic spikes through increased latency rather than rejecting connections outright
- **Improved DoS resilience** - the previous architecture could be overwhelmed with as few as 800 parallel requests; the new model is significantly harder to saturate using the same approach

New DHCP service implemented in the new control plane architecture:

We've modernized the DHCP service with a new-generation architecture designed to deliver better scalability, stronger resilience, and seamless integration with the modern control plane.

What's new

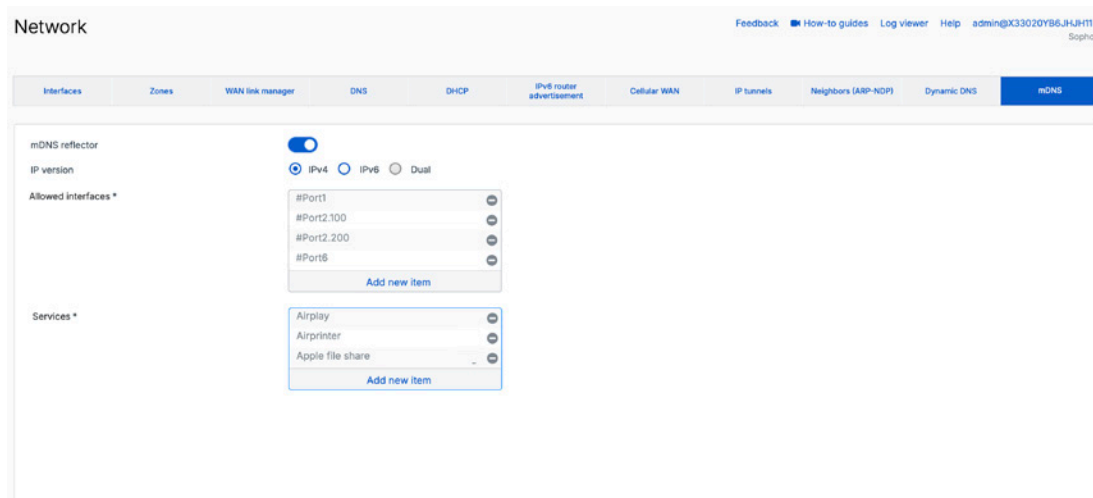
- **Built for scale** — DHCP service is now ported to the new Control Plane, now delivers faster lease processing for larger DHCP scope. DHCP scope update and logging bottlenecks have also been resolved in the new control plane.
- **Protected against DHCP floods** — DHCP traffic is now protected by the firewalling layer before reaching the DHCP service, helping mitigate the impact of DHCP floods or DoS conditions and maintain service availability.
- **Simplified management** — Advanced DHCP configurations, such as lease scopes, static bindings, negative acknowledgements, and allowing only one lease per client, which were previously CLI-driven, are now integrated into the UI.
- **Streamlined DHCP options** — DHCP options are streamlined to ensure RFC compliance.
- **Expanded static binding scalability** - Larger numbers of static IP-MAC bindings for DHCP reservations are now supported, overcoming the previous file-size limitation.
- **Faster configuration and lease management** — Improved reconfiguration and lease handling make it easier to apply changes across DHCP scopes, while faster REST API-based lease retrieval delivers quicker lookups and smoother page loading.

Networking and connectivity

mDNS (Bonjour) reflector

A frequently requested enhancement by those of you in education or campus environments, the firewall now enables seamless service discovery between isolated VLANs and subnets without collapsing network segmentation, with dual-stack support for both IPv4 and IPv6. This is particularly helpful in situations where printers, displays, and shared devices commonly sit on a different VLAN from the users who need to find them.

The mDNS Reflector handles service discovery only; devices still require explicit firewall rules to permit data communication after discovery. Administrators select the interfaces to reflect across and the services to allow. Supported services include All, Printers, Apple AirPlay, Google Chromecast, Scanners, Apple AirDrop, Sonos, Remote Desktop, HomeKit, Apple File Share, Spotify Connect, and IoT device discovery.



The mDNS reflector is configured under Network > mDNS, with IP version selection, allowed interfaces, and per-service control.

IPv6 IPoE support

The firewall now supports IPv6 IPoE and 4in6 tunneling (IPIP/DS-Lite), including Japan IPoE services such as Xpass (CrossPass) delivered over IPIP (4in6) tunneling. Built-in VNE-aware DDNS integration automatically updates the dynamic public IPv6 addresses that IPoE providers assign.

This release also improves IPIP tunnel configuration. Administrators select a source interface rather than depending on a static IP, configure FQDN-based remote endpoints for more resilient tunnels, enable a ToS inherit option to preserve QoS markings across the tunnel, and tune MTU and MSS to optimize throughput and reduce fragmentation. The 4in6 tunnel interface now extends to advanced NAT (sys-nat CLI) use cases, and we will publish a documentation guide covering IPoE setup with the Xpass (CrossPass) VNE provider in this release.

Network

Interfaces Zones WAN link manager DNS DHCP IPv6 router advertisement Cellular WAN IP tunnels Neighbors (ARP-NDP) **Dynamic DNS**

Host configuration

Hostname * (Example: xyz.dyndns.com)

IP version * ☐ IPv4 ☒ IPv6

Interface * Port1 - 240B:40c1:2030:eeef:c84d::9ea:ad25

IPv4 address * ☐ Use port IP ☐ NATed public IP

The firewall checks for a change in the server IP address every 5 minutes.

Service provider settings

Service provider * VNE

Server URL * Server URL

DDNS ID DDNS ID

DDNS Password DDNS Password

Login name * Enter Login name

Password * Enter Password

Dynamic DNS now supports IPv6 with interface selection and VNE as a service provider, keeping IPoE-assigned public IPv6 addresses up to date

Cloud platform expansion – IONOS

The SFOS virtual image is now qualified for deployment on IONOS Cloud, extending the platforms on which customers can standardize their network security. These platforms follow a bring-your-own-image (BYOI) model: customers deploy using the official SFOS images with guided documentation, and step-by-step deployment guides are provided for consistent and validated setup. There is no Marketplace listing for these platforms, so deployment and lifecycle management are performed manually.

Other enhancements

Email content control lists by ID — email policies now refer to CCLs by ID rather than by name, making configuration more robust across upgrades and backups.

Changeable web definitions — Web category versioning introduces a backend configuration option that sets the web category version used when communicating with Sophos, allowing category definitions to change without breaking existing deployments.



United Kingdom and Worldwide Sales

Tel: +44 (0)8447 671131

Email: sales@sophos.com

North America Sales

Toll Free: 1-866-866-2802

Email: nasales@sophos.com

Australia and New Zealand Sales

Tel: +61 2 9409 9100

Email: sales@sophos.com.au

Asia Sales

Tel: +65 62244168

Email: salesasia@sophos.com

© Copyright 2026. Sophos Ltd. All rights reserved.

Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2026-09-29 EN (DD)