Sophos release notes

Product type: Network Security Product: Sophos Firewall Version: 21.5

Sophos Firewall

These release notes are for Sophos Firewall (formerly known as Sophos XG Firewall).

Latest version | Previous versions | Resolved issues | Known issues | Upgrade information | Supported platforms | Support

Version 21.5 GA Build 171

Released on June 02, 2025

New features

This page describes the new features introduced in this release. For more information, see the Sophos Firewall help.

SFOS 21.0 GA and later versions, including SFOS 21.5 GA, do not support XG and SG Series hardware appliances.

NDR Essentials

Sophos NDR Essentials is now integrated with Sophos Firewall, offering a new layer of threat protection under Active threat response. It analyzes traffic flows using cloud-hosted NDR Machine Learning, offloading heavy processing to the cloud.

NDR Essentials inspects traffic using the following engines:

- **Encrypted Payload Analysis**: Analyzes encrypted payloads without requiring TLS decryption.
- **Domain Generation Algorithm**: The ML-powered engine detects newly discovered active adversaries.

The detection triggers logs, alerts, and notifications based on thresholds that you specify.

The feature is currently available as part of the Xstream Protection bundle for XGS Series firewalls only.

See the following resources:

- Read NDR Essentials.
- Watch NDR Essentials for Sophos Firewall.

Microsoft Entra ID SSO for the Sophos Connect client and VPN portal

Users can establish remote access IPsec and SSL VPN tunnels using their network credentials.

- Integration with Microsoft Entra ID (Azure AD) Single Sign-On (SSO) now extends to the Sophos Connect client and VPN portal.
- It provides cloud-native Active Directory integration over the industry standard OAuth 2.0 and OpenID Connect protocols for a seamless SSO experience.
- This feature is available with Sophos Connect client 2.4 and later versions on Microsoft Windows.

See the following resources:

- Read Microsoft Entra ID (Azure AD) server.
- Watch Entra ID SSO Integration for Sophos Connect Client.

DNS Protection

Sophos DNS Protection was previously integrated with Sophos Firewall. The service protects against malicious domains and risky DNS activities across your network.

This release provides the following enhancements:

- A new Control center widget to show the DNS Protection status.
- Enhanced troubleshooting insights through logs, notification emails, and the current status to more easily identify issues.
- Sophos Assistant now provides guided steps to configure Sophos DNS Protection.

This feature is included in the Xstream Protection bundle.

See the following resources:

- Read DNS Protection.
- Watch DNS Protection.

 Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_215_rn.html

Sophos release notes

Product type: Network Security Product: Sophos Firewall Version: 21.5

dress conflicts across these types of VPN.

- **IPsec profile selection**: The "Use strict profile" field in IPsec profiles excludes default values, ensures a successful handshake, eliminates packet fragmentation, and minimizes tunnel establishment issues.
- **Route-based IPsec VPN scalability**: The firewall's route-based VPN capacity has been doubled with support for up to 3,000 tunnels.
- **SD-RED scalability**: Sophos Firewall devices now support up to 1,000 site-to-site RED tunnels and 650 SD-RED devices.

Streamlined management and quality-of-life enhancements

This version offers multiple quality-of-life enhancements to simplify and improve firewall management.

- **Resizable table columns**: Many features, including SD-WAN routes and profiles, NAT rules, SSL/TLS inspection rules, Hosts and services, and Site-to-site IPsec VPN, support resizable table columns. Column sizes are retained in the browser memory for the administrator's subsequent visits to the web admin console.
- **Extended free text search**: SD-WAN routes now offer a search capability using the route name, ID, objects, and object values, such as IP addresses, domains, and other criteria. Local ACL exception rules support search using the object name and value. This also includes content-based search.
- **New Inter Font**: The firewall has introduced a sharper, clearer text experience with a modern and consistent user interface across platforms. The font is lightweight, reducing the asset size and API calls by up to 50 percent.
- **Default firewall rules**: The default firewall rules and rule group created when setting up a new firewall have been removed. Only the default network rule and MTA rule remain in new deployments. The default firewall rule group is now set to None.
- **Default gateway configuration**: Default gateway probing for custom gateways is now set to None.

Watch Quality-of-life enhancements.

Other enhancements

This version offers other important enhancements.

- **Virtual, software, cloud licensing and Home edition**: Removed the RAM restrictions on Sophos Firewall virtual, software, Cloud BYOL and Firewall Home edition licenses. All new and existing instances of Sophos Firewall no longer have RAM restrictions as part of their license and are now restricted only by the CPU core count.
- **Larger file size limit in WAF**: Web Application Firewall supports a configurable request (upload) file size limit and can scan file sizes up to 1 GB.
- **Secure by Design**: In our efforts to continually improve the security of Sophos Firewall, this release adds real-time telemetry gathering, using secure hash validation to flag unexpected changes to core OS files. This will enable our monitoring teams to proactively identify potential security incidents before they become a problem.
- **DHCP prefix delegation relaxation**: DHCP PD now supports /48 to /64 prefixes, improving interoperability with ISPs. In addition, Router Advertisements (RA) and the DHCPv6 server are turned on by default.
- **Path MTU discovery in DPI mode**: This feature resolves connection errors caused by the latest ML-KEM (Kyber) key exchange supported in browsers, specifically for connections handled by the DPI engine. The firewall's deep packet inspection engine now automatically detects and adjusts the MTU for each flow, ensuring optimal performance based on specific network conditions.
- **NAT64 support**: The firewall supports NAT64 for IPv6 to IPv4 traffic in explicit proxy mode. In this mode, IPv6-only clients can access IPv4 websites. The firewall also supports IPv4 upstream proxy for IPv6-only clients.

 Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_215_rn.html