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 MR1 Build 261

Released on October 08, 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 do not support XG and SG Series hardware appliances.

OAuth 2.0 for email notifications

The firewall supports OAuth 2.0 as an additional authentication method for the email notifications it sends. We recommend that you move to OAuth 2.0 for Gmail. Gmail may stop supporting password-based authentication very soon.

Read Notification settings.

NDR Essentials

NDR Essentials delivers the following enhancements:

- **Data center**: To meet regional and data residency requirements, you can select the data center location to which your traffic is sent for analysis. By default, the firewall selects the location with the least latency.
- **Threat score in logs**: The assigned threat score appears in the Active threat response logs, offering enhanced visibility, reporting, and analytics.

Active Directory integration

The firewall supports Windows Server 2025 for Active Directory SSO (NTLM and Kerberos) authentication.

RED

System hosts

RED system host objects now have the correct subnet mask of `/32`. You can see system host details in **Hosts and services** > **IP host**. Previously, when you created a RED interface, the system host was assigned the subnet mask you configured.

If you're using the RED system host for traffic other than a `/32` subnet in configurations, such as firewall rules, the traffic won't match any longer. To resolve this, you must replace the RED system host with the correct IP host or network host in these dependent configurations.

Legacy site-to-site RED Early End-of-Life notification

The legacy RED site-to-site tunnels (Legacy firewall RED server and client configurations) won't be supported in SFOS 22.0 and later. We recommend that you migrate to the supported RED site-to-site or VPN tunnels.

Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_215_rn.html eduled PDF reports in multiple languages. They are automatically generated in the language the administrator uses when signing in to the firewall to schedule them.

Syslog enhancements

The `device_name` field captures the hostname of the firewall that produced the logs, enabling clear identification across multiple firewalls. This facilitates effective syslog-based integrations and helps XDR and Taegis administrators in differentiating the data sources.

High availability

The security enhancements in high availability configurations are as follows:

- Passphrase: The firewall doesn't generate the passphrase automatically any longer. You can use strong passphrases that meet the complexity requirements.
- SSH key: A unique SSH host key verification has been introduced to strengthen HA authentication and prevent man-in-the-middle attacks.
- Improved troubleshooting: The high availability log, `ha.log`, has been enhanced to include the node name and the current role information.
- LINCE: You must turn on LINCE mode for both devices, then configure HA. To restore an HA backup, the receiving devices must match the backup's LINCE status.

VPN improvements

- L2TP and PPTP: When you import groups from the Active Directory and Microsoft Entra ID authentication servers, L2TP and PPTP won't be turned on by default. You can turn them on in the groups or the corresponding VPN configurations.
- MTU of XFRM interfaces: To prevent packet fragmentation and ensure reliable TCP connectivity in route-based VPN tunnels, the firewall automatically assigns an XFRM MTU value after subtracting the maximum IPsec overhead from the physical interface MTU. You can change this value to meet your network requirements.

Quality-of-life enhancements

FastPath

Optimized memory in the Data Plane Development Kit (DPDK) of the Data Acquisition (DAQ) layer, eliminating many out-of-memory instances in the following desktop firewalls: XGS 87, 87w, 107, 107w, 116, and 116w.

Identifying firewalls from backup emails

The subject line of backup emails now includes the firewall's hostname, firmware version, serial number, and model. This enhancement makes it easier to identify which firewall a backup belongs to when you manage multiple firewalls.

Hotspot vouchers

The hotspots page in the user portal has a "Created date" column. You can sort vouchers based on the date you've created them, which lets you see the latest vouchers at the top.

SNMP

Improved RFC compliance in SNMP MIB files to enhance compatibility with third-party SNMP tools. The firewall supports the following RFCs for the MIB file:

- SNMPv1: RFC 1157
- SNMPv2: RFCs 1901, 1905, and 1906
- SNMPv3: RFCs 3411 to 3418

Resizable columns

More features, including most of the network menu, SD-WAN routes and profiles, gateways, and local service ACL exception rules support resizable columns. When you resize a column, the change is stored in the browser memory, and the resized column appears when you visit the page again.

Live users

Data usage for live users is now shown using the standard unit formats (KB, MB, and GB) for enhanced usability.

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