

## Manuals+

[Q & A](#) | [Deep Search](#) | [Upload](#)

manuals.plus /

- › [Sophos](#) /
- › [Sophos XGS 87 Next-Gen Firewall Instruction Manual](#)

## Sophos XGS 87

# Sophos XGS 87 Next-Gen Firewall Instruction Manual

Model: XGS 87 (JA8B1CSUS)

## 1. PRODUCT OVERVIEW

The Sophos XGS 87 is a next-generation firewall designed to provide robust network security for small to medium-sized businesses. It integrates advanced threat protection capabilities, including Xstream Architecture, TLS 1.3 Decryption, Deep Packet Inspection, Next-Gen IPS, Web Protection, and Application Control. This device ensures comprehensive defense against various network threats, offering a secure and reliable network environment.



Image: Sophos XGS Next-Gen Firewall with Xstream Protection. This image displays the Sophos XGS series appliances, highlighting their advanced Xstream Flow Processors for high-performance threat protection.

## 2. SETUP INSTRUCTIONS

## 2.1 Unpacking and Inspection

- Carefully remove the Sophos XGS 87 firewall from its packaging.
- Inspect the device for any signs of physical damage. If damage is found, contact your vendor immediately.
- Verify that all components listed in the packing slip are present.

## 2.2 Connecting the Device

The Sophos XGS 87 features multiple ports for network connectivity and management. Refer to the diagrams below for port identification.



Image: Rear panel of the Sophos XGS 87 firewall. This view shows the DC IN 12V power input, COM port, USB port, and the LAN/WAN Ethernet ports (L/LAN, S/PoE, 2/WAN, 4).

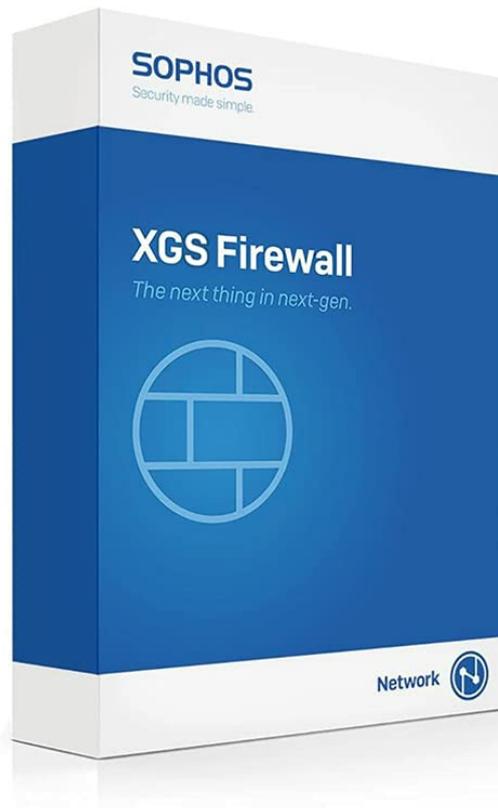


Image: Front panel of the Sophos XGS 87 firewall. This view displays the XGS 87 model label, a COM port, a USB port, status LEDs for LAN/WAN activity and speed, and system status indicators.

1. **Power Connection:** Connect the provided power adapter to the DC IN 12V port on the rear panel and plug it into a power outlet.
2. **Network Connections:**
  - Connect your internet service provider's modem or router to the **2/WAN** port.
  - Connect your internal network devices (switches, computers) to the **L/LAN** or other available LAN ports.
3. **Console Connection (Optional):** For initial configuration or troubleshooting, connect a console cable from your computer to the **COM** port.
4. **USB Devices (Optional):** USB ports can be used for external storage or other compatible peripherals.

## 2.3 Initial Configuration

Upon first power-on, the device will boot up running Sophos Firewall OS. Initial configuration is typically performed via a web-based interface accessible from a connected computer on the LAN side. Refer to the Sophos documentation for detailed steps on accessing the web interface and completing the initial setup wizard.

## 3. OPERATING THE FIREWALL

---

The Sophos XGS 87 operates by inspecting and controlling network traffic based on configured security policies. Its core functionality revolves around the Sophos Firewall OS, which provides a comprehensive suite of security features.

### 3.1 Key Protection Features

The XGS 87 includes a 1-year Standard Protection license, offering:

- **Xstream Architecture:** High-performance deep packet inspection and TLS 1.3 decryption.
- **Network Protection:** Intrusion Prevention System (IPS), Advanced Threat Protection (ATP), and SD-RED support.
- **Web Protection:** Web filtering, application control, and secure web gateway features.
- **Application Control:** Granular control over thousands of applications.
- **Reporting:** Extensive logging and reporting capabilities for network visibility.

# Sophos XGS Series Desktop: SMB and Branch Office

## XGS 87 and XGS 87w

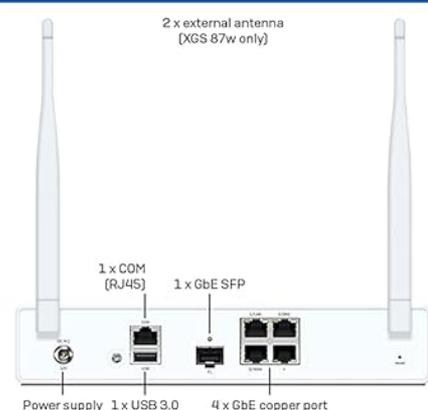
### Technical Specifications

**Note:** The XGS 87 and 87w do not support some advanced features like on-box reporting, dual AV scanning, WAF AV scanning and the email message transfer agent (MTA) functionality. If you need these capabilities, the XGS 107(w) is recommended.

#### Front View



#### Back View



#### Physical specifications

Mounting	Rackmount kit available (to be ordered separately)
Dimensions Width x Height x Depth	230 x 44 x 205.5 mm
Weight	1.36 kg/3 lbs (unpacked) 2.75 kg/6.06 lbs (packed) (w-model minimally more)

#### Environment

Power supply	External auto-ranging AC-DC 100-240VAC, 1.7A@50-60 Hz 12VDC, 5A, 60W
Power consumption	23.2 W / 79.16 BTU/hr (87) [idle] 27.1 W / 92.13 BTU/hr (87w) [idle] 43.4 W / 148.09 BTU/hr (87) [max.] 46.8 W / 159.69 BTU/hr (87w) [max.]
Operating temperature	0°C to 40°C (operating) -20°C to +70°C (storage)
Humidity	10% to 90%, non-condensing

#### Product Certifications

Certifications	CB, CE, UL, FCC, ISED, VCCI, CCC, KC, BSMI, NOM, Anatel (87 only)
----------------	---

#### Performance

	XGS 87(w)
Firewall throughput	3,700 Mbps
Firewall IMIX	2,500 Mbps
Firewall Latency (64 byte UDP)	6 μs
IPS throughput	1,015 Mbps
Threat Protection throughput	240 Mbps
Concurrent connections	1,600,000
New connections/sec	35,700
IPsec VPN throughput	-
Xstream SSL/TLS Inspection	375 Mbps
Xstream SSL/TLS Concurrent connections	8,192

Note: For performance testing methodology see page 12

#### Wireless Specification (XGS 87w only)

No. of antennas	2 external
MIMO capabilities	2 x 2:2
Wireless interface	802.11a/b/g/n/ac (2.4 GHz / 5 GHz)

#### Physical interfaces

Storage	16 GB eMMC
Ethernet interfaces (fixed)	4 x GbE copper 1 x SFP fiber*
Management ports	1 x COM RJ45 1 x Micro-USB (cable incl.)
Other I/O ports	1 x USB 2.0 (front) 1 x USB 3.0 (rear)
Number of expansion slots	0
Optional add-on connectivity	SFP DSL module (VDSL2) SFP transceivers

\* SFP transceivers sold separately

Image: Sophos XGS Protection Modules. This diagram details the various protection modules available, including Base Firewall, Network Protection, Web Protection, Zero-Day Protection, and Central Orchestration, allowing for customized security deployments.

## 3.2 Management and Monitoring

The firewall can be managed through its web interface or via the Sophos Central platform. The web interface provides detailed control over all settings, policies, and monitoring tools. Sophos Central offers cloud-based management, allowing for centralized control of multiple Sophos devices and enhanced reporting.

- **Dashboard:** Provides an overview of network status, threats, and system performance.
- **Policy Configuration:** Define firewall rules, NAT policies, VPN settings, and application control policies.
- **Logging and Reporting:** Access detailed logs and generate reports on network activity, security events, and user behavior.

## 4. MAINTENANCE

---

Regular maintenance ensures the optimal performance and security of your Sophos XGS 87 firewall.

- **Firmware Updates:** Regularly check for and apply the latest firmware updates to ensure your device has the most current security patches and features. The device has security updates available.
- **Configuration Backups:** Periodically back up your firewall configuration. This allows for quick restoration in case of an issue or misconfiguration.
- **Log Review:** Regularly review system logs and security reports to identify potential threats or anomalies.
- **Physical Inspection:** Ensure the device is in a well-ventilated area and free from dust accumulation. Check all cable connections for security.

## 5. TROUBLESHOOTING

---

This section provides basic troubleshooting steps for common issues.

### 5.1 No Power

- Verify the power adapter is securely connected to the device and a working power outlet.
- Check the power LED on the front panel. If it is off, try a different power outlet or adapter.

### 5.2 No Network Connectivity

- Ensure all Ethernet cables are properly connected to the correct ports (WAN, LAN).
- Check the link/activity LEDs on the Ethernet ports. They should be lit or blinking.
- Verify your computer's network settings (IP address, gateway) are correctly configured or set to obtain automatically.
- Restart the firewall and connected network devices.

### 5.3 Device Unresponsive / Factory Reset

- If the device becomes unresponsive, you may need to perform a factory reset. Locate the **Reset** button on the rear panel (refer to the rear panel image).
- Use a paperclip or similar pointed object to press and hold the reset button for approximately 10 seconds while the device is powered on. This will restore the device to its factory default settings.

## 6. SPECIFICATIONS

---

The following table outlines the key technical specifications for the Sophos XGS 87 Next-Gen Firewall.

## All Licensing Options

We recommend the Xstream Protection bundle for the ultimate in security, but if you prefer to customize your protection, all subscriptions are also available for individual purchase.

<b>Xstream Protection Bundle:</b>	
Base License	Networking, Wireless, Xstream Architecture, Unlimited Remote Access VPN, Site-to-Site VPN, reporting
Network Protection	Xstream TLS and DPI engine, IPS, ATP, Security Heartbeat, SD-RED VPN, reporting
Web Protection	Xstream TLS and DPI engine, Web Security and Control, Application Control, reporting
Zero-Day Protection	Machine Learning and Sandboxing File Analysis, reporting
Central Orchestration*	SD-WAN VPN Orchestration, Central Firewall Advanced Reporting (30-days), MTR/XDR ready
Enhanced Support	24/7 support, feature updates, advanced replacement hardware warranty for term

\* Expected soon

**Custom Protection:** If you only require basic protection or want to customize your protection, you can choose the Standard Protection Bundle or purchase any of the protection modules separately.

<b>Standard Protection Bundle:</b>	
Base License	Networking, wireless, Xstream Architecture, unlimited Remote Access VPN, Site-to-Site VPN, reporting
Network Protection	Xstream TLS and DPI engine, IPS, ATP, Security Heartbeat, SD-RED VPN, reporting
Web Protection	Xstream TLS and DPI engine, Web Security and Control, Application Control, reporting
Enhanced Support	24/7 support, feature updates, advanced replacement hardware warranty for term

<b>Additional Protection Modules:</b>	
Email Protection	On-box antispam, AV, DLP, encryption
Web Server Protection	Web Application Firewall

**Sophos Central Management and Reporting:** All Sophos Firewalls include cloud management and reporting at no extra charge.

<b>Sophos Central Management and Reporting (Included at no charge):</b>	
Sophos Central Management	Group firewall management, backup management, firmware update scheduling
Sophos Central Firewall Reporting	Prepackaged and custom report tools with seven days cloud storage for no extra charge (see other options)

**Additional Protection:** Extend your protection further with these additional products and services.

<b>Additional Protection Services, Products and Modules:</b>	
Managed Threat Response	24/7 threat hunting, detection and response delivered by an expert team ( <a href="#">more info</a> )
Sophos Intercept X Endpoint with XDR	Sophos Central managed next-gen endpoint protection with EDR ( <a href="#">more info</a> )
ZTNA	Sophos Central managed Zero Trust Network Access ( <a href="#">more info</a> )
Central Email Advanced	Sophos Central managed antispam, AV, DLP, encryption ( <a href="#">more info</a> )

**Support:** Enhanced support is included in all protection bundles, but you can enhance your support experience further by upgrading.

<b>Additional Support Options:</b>	
Enhanced Plus Support Upgrade	Upgrade your support with VIP support, HW warranty for add-ons, TAM option (extra cost)

### Cloud, Virtual and Software Appliance Licensing Options:

If you're deploying Sophos Firewall in the cloud, in a virtual environment, or as software on your own hardware, the licensing guide below can help you find the right option.

Model	Equivalent AWS instance	Equivalent Azure VM	Software/Virtual License*
XGS 87	t3.medium	Standard_F2s_v2	2C4
XGS 107			
XGS 116			
XGS 126	c5.large		
XGS 136	m5.large	Standard_F4s_v2	4C6
XGS 2100			6C8
XGS 2300	c5.xlarge		
XGS 3100	m5.xlarge	Standard_F8s_v2	8C16
XGS 3300			
XGS 4300			
XGS 4500	c5.2xlarge		
XGS 5500	c5.4xlarge	Standard_F16s_v2	16C24
XGS 6500			Unlimited

\*\* Based upon CPU cores and RAM

For a complete list of features included in each protection subscription see the Sophos Firewall Feature List.

Feature	Specification
Brand	Sophos
Model Name	XGS 87
Model Number	JA8B1CSUS
Operating System	Sophos Firewall OS
Number of Ports	9 (including LAN/WAN)
Data Transfer Rate	3700 Megabits Per Second
Connectivity Technology	Wi-Fi (802.11ac), Ethernet
Security Protocol	WPS (Wireless Protected Setup)
Item Weight	8 Pounds
Control Method	App
Coverage	Protection against various network threats through Xstream Architecture, TLS 1.3 Decryption, Deep Packet Inspection, Next-Gen IPS, Web Protection, and App Control

## 7. WARRANTY AND SUPPORT

The Sophos XGS 87 Next-Gen Firewall includes a 1-Year Standard Protection plan, which typically covers essential security features and basic support during the subscription period. For detailed information regarding your specific warranty coverage and support options, please refer to the documentation provided with your purchase or visit the official Sophos website.

### Protection Modules

You can choose from a number of modules to customize the protection offered by your firewall to your individual needs and deployment scenario.

#### Base Firewall

The Sophos Firewall Base license includes the Xstream Architecture, networking, wireless, SD-WAN, VPN, and reporting.

#### Xstream Architecture

Enables high performance TLS 1.3 inspection, deep-packet inspection, and network flow FastPath to accelerate trusted SaaS, SD-WAN, and cloud application traffic. Note that Network and Web Protection are required to get the full benefits of the Xstream Architecture.

#### Networking and SD-WAN

Includes networking, routing, and SD-WAN capabilities with zone-based stateful firewall, NAT, VLAN support, multiple WAN link options with SD-WAN routing, fail-over, and fail-back.

#### Secure Wireless

Built-in wireless controller for Sophos APX wireless access points. Plug-and-play access point discovery makes setup easy. Support for multiple SSIDs, hotspots, guest networks, and the diverse encryption and security standards.

#### VPN

Provides standards-based site-to-site and remote access VPN (free up to the capacity of the firewall) with support

#### Network Protection

All the protection you need to stop sophisticated attacks and advanced threats while providing secure network access to those you trust.

#### Next-Gen Intrusion Prevention System

Provides advanced protection from all types of modern attacks. It goes beyond traditional server and network resources to protect users and apps on the network as well.

#### Security Heartbeat

Creates a link between your Sophos Central protected endpoints and your firewall to identify threats faster, simplify investigation, and minimize impact from attacks. Easily incorporate Heartbeat status into firewall policies to automatically isolate compromised systems.

#### Advanced Threat Protection

Instant identification and immediate response to today's most sophisticated attacks. Multi-layered protection identifies threats instantly and Security Heartbeat provides an emergency response.

#### Advanced VPN technologies

Adds unique and simple VPN technologies, including our clientless HTML5 self-service portal that makes remote access incredibly simple or utilize our exclusive lightweight

VPN gives up to the capacity to the network and support for IPsec and SSL. Sophos Connect remote access VPN client for Windows and Macs offers seamless and easy deployment and configuration options. Sophos unique SD-RED layer 2 site-to-site tunnels offers a light-weight robust VPN alternative.

#### Reporting

Extensive on-box reporting provides valuable insights into threats, users, applications, web activity, and much more. Note that specific reporting functionality may be dependent on other protection modules to get the full benefits (for example, Web Protection or web and app reports).

The Base Firewall is included with every appliance.

#### Web Protection

Unmatched visibility and control over all your user's web and application activity.

#### Powerful user and group web policy

Provides enterprise-level Secure Web Gateway policy controls to easily manage sophisticated user and group web controls. Apply policies based upon uploaded web keywords indicating inappropriate use or behavior.

#### Application Control and QoS

Enables user-aware visibility and control over thousands of applications with granular policy and traffic-shaping (QoS) options based on application category, risk, and other characteristics. Synchronized Application Control automatically identifies all the unknown, evasive, and custom applications on your network.

#### Advanced Web Threat Protection

Backed by SophosLabs, our advanced engine provides the ultimate protection from today's polymorphic and obfuscated web threats. Innovative techniques like JavaScript emulation, behavioral analysis, and origin reputation help keep your network safe.

#### High-performance traffic scanning

Optimized for top performance, our Xstream SSL inspection provides ultra-low latency inspection and HTTPS scanning while maintaining performance.

Web Protection is included in the Xstream and Standard Protection bundles and is also available for separate purchase.

#### Central Orchestration\*

Sophos Central cloud-managed VPN orchestration, firewall reporting, and MTR/XDR integration.

#### Sophos Central VPN Orchestration

Makes VPN orchestration easy. Wizard-based tunnel configuration helps create full mesh networks, hub-and-spoke models, or complex tunnel setups between multiple firewalls a quick point-and-click exercise. Seamlessly integrates multiple WAN link and SD-WAN functionality and routing optimizations to improve resilience and performance and also integrates with user authentication and Synchronized Security Heartbeat to control access.

#### Central Firewall Reporting Advanced (30-day)

Cloud-based reporting with several pre-packaged common reports for threats, compliance, and user activity. Includes advanced options for creating custom reports and views with the option to save, schedule or export your custom reports. Includes 30 days of log data retention with the option to add additional storage for additional historical reporting needs.

#### MTR/XDR Ready

Sophos MTR provides optional 24/7 threat hunting, detection and response delivered by an expert team as a fully-managed service. Sophos XDR offers extended detection and response managed by your own team. Regardless of whether you manage it yourself, or Sophos manages it for you, your Sophos Firewall is ready to share the necessary threat intelligence and data to the cloud.

Central Orchestration is included in the Xstream Protection bundle and is available for separate purchase.

\* Expected soon.

Secure Mobility and Remote Access use exclusive high-throughput secure SD-RED (Remote Ethernet Device) VPN technology. Network Protection is included in the Xstream and Standard Protection bundles and is also available for separate purchase.

#### Zero-Day Protection

AI-driven static and dynamic file analysis techniques combine to bring unprecedented threat intelligence to your firewall and so effectively identify and block ransomware and other known and unknown threats.

#### Powered by SophosLabs

Powered by the industry-leading SophosLabs, the Zero-Day Protection subscription includes a fully cloud-based threat intelligence and threat analysis platform. This provides deep learning-based file analysis, detailed analysis reporting, and a threat meter to show the risk summary for a file.

We use layers of analytics to identify known and potential threats, reduce unknowns, and derive verdicts and intelligence reports for the most commonly used file types.

#### Static File Analysis

By harnessing the power of multiple machine learning models, global reputation, deep file scanning, and more, you can quickly identify threats without the need to execute the files in real time.

#### Dynamic File Analysis

Execute a file in a secure cloud-based sandbox to observe its behavior and intent. Screenshots provide added insight into any key events during the analysis.

#### Threat Intelligence Analysis Reporting

Rich intelligence reports provide you with much more than just a 'good,' 'bad,' or 'unknown' verdict. Full insight into the nature and capabilities of a threat are delivered through the use of data science and SophosLabs research.

Zero-Day Protection is included in the Xstream Protection bundle and is also available for separate purchase.

#### Email Protection

Consolidate your email protection with anti-spam, DLP, and encryption. We recommend Sophos Central Email Advanced for the best cloud-based email protection solution. If you require on-box email protection, this module offers essential anti-spam, DLP and encryption.

#### Integrated Message Transfer Agent

Ensures always-on business continuity for your email, allowing the firewall to automatically queue mail in the event servers become unavailable.

#### Live Anti-Spam

Provides protection from the latest spam campaigns, phishing attacks, and malicious attachments.

#### Self-serve Quarantine

Gives employees direct control over their spam quarantine, saving you time and effort.

#### SPX Email Encryption

Unique to Sophos, SPX makes it easy to send encrypted email to anyone, even those without any kind of trust infrastructure, using our patent-pending password-based encryption technology.

#### Data Loss Prevention

Policy-based DLP can automatically trigger encryption or block/notify based on the presence of sensitive data in emails leaving the organization.

Email Protection is available for individual purchase only.

#### Web Server Protection

Harden your web servers and business applications against hacking attempts while providing secure access.

#### Business Application Policy Templates

Pre-defined policy templates let you protect common applications like Microsoft Exchange Outlook Anywhere or SharePoint quickly and easily.

#### Protection from the latest hacks and attacks

With a variety of advanced protection technologies including URL and form hardening, deep-linking and directory traversal prevention, SQL injection and cross-site scripting protection, cookie signing and more.

#### Reverse proxy

With authentication options, SSL offloading, and server load balancing ensure maximum protection and performance for your servers being accessed from the internet.

Web Server Protection is available for individual purchase only.

Image: Sophos XGS All Licensing Options. This document outlines various licensing bundles, including Base License, Network Protection, Web Protection, Zero-Day Protection, Central Orchestration, and Enhanced Support options, allowing users to customize their protection.

Sophos offers various support options, including online resources, knowledge bases, and direct technical support. For advanced issues or to inquire about extended support plans, please contact Sophos customer service or your authorized

Sophos partner.

- **Online Resources:** Visit the Sophos support portal for documentation, FAQs, and community forums.
- **Technical Support:** Contact Sophos technical support for assistance with product issues.
- **Enhanced Support:** Upgrade options are available for extended hardware warranty and advanced support services.