SOPHOS
Cybersecurity made simple.

Support Services Guide – Enhanced, Enhanced Plus, TAM

Contents

Overview

Sophos Technical Support offers customers three distinct Enhanced support service options: Enhanced, Enhanced Plus and Technical Account Manager. This Support Services Guide documents what is offered for customers who purchased one of these three support plans with respect to the operation of their Products. This document does not cover UTM9 or Cyberoam products.

Capitalized terms used in this document shall have the meanings assigned to them in the Sophos End User License Agreement, unless stated otherwise.

This document includes the following:

- The scope of technical support provided for the Products
- Definition of the severity levels assigned to customer reported Product issues
- Definition of technical support service level targets
- An outline of technical support escalation procedures
- A description of all other service components associated with the Enhanced and Enhanced Plus Support Plans

1. SUPPORT SCOPE AND COMMUNICATION METHODS

1.1 Scope of Support

Support is available 24 hours per day, 7 days per week, 52 weeks per year, including statutory, public and bank holidays. While 24x7 support is offered in English, we do also offer local language support (Italian, German, Spanish, French, Japanese) during local business hours.

Sophos Technical Support will respond to and work to resolve customer-submitted problems (collectively in this document, "Incidents") related to the Products' installation, administration and operation in accordance with the response times, escalation procedures and status updates set out in this document, in order to:

- Answer general questions not addressed in the Documentation
- Address issues resulting from the Products not functioning as described in the Documentation
- Provide help and guidance with respect to virus disinfection and the use of virus recovery/disinfectant utilities provided by Sophos
- Provide help and guidance with respect to threat detection
- Provide help and guidance with respect to extended policy configuration and customer filter optimization

In addition, Sophos Technical Support will provide the components described in Section 2, 3 and 4 of this document.

1.2 Communication Methods

Sophos Technical Support will receive and respond to Incidents through one or a combination of the following communication methods:

Submission of support incidents via any of the following support channels:

- Phone
- Webform
- Online Support portal - SophServ
- Chat

2. ENHANCED

The following service components are available to all Sophos customers who are entitled to Enhanced support and have valid licenses and, solely with respect to products, paid up maintenance fees.

2.1 Software downloads, updates and maintenance

- Web-based access to the latest scheduled software upgrades, including error correction packages and functionality upgrades
- Web-based access to Sophos malware and spam updates in order to provide rapid protection against the latest security threats

2.2 Web self-help support and Support Forums

- Web-based access to our forums: https://community.sophos.com
- Comprehensive, searchable knowledgebase: https://community.sophos.com/kb
- Customer Resource Centers for each Sophos solution including:
  - "Getting Started and Making the Most of Your Solution" tips and best practices
  - System requirements, start up guides and manuals
  - Videos and demonstrations of the Sophos solutions
- Product Upgrade Center with information on new versions, system requirements and upgrade guides
- Product advisories and security threat information

2.3 Access to news subscriptions

- Registration for news and alerts:
- General information on security threats and protection strategies through support news bulletins
- Product release information on errors corrected, new features and installation instructions
- Keep up to date on the latest products news, customer events and news via Twitter; follow @SophosSupport
- Control which Sophos product notifications get sent to your mobile device through Manage Alerts

2.4 Online Support case management and reporting portal

- Unlimited access to SophServ, an online Support Portal
  - View, open, close and manage Sophos Support cases
  - Access the latest support notifications, advisories and articles
  - Ability to grant administrator or user rights
  - Create groups allowing teams within the organization to view and take action on cases for other members
  - Export case reporting and statistics

2.5 Remote Assistance Support

- In order to expedite the diagnosis and resolution of Incidents, Sophos Technical Support may request remote access to the customer's system. In the event that remote access to the customer's system is not available, the elapsed time to resolve Incidents may be extended. During remote access sessions, the tech support engineer might also request access to items such as diagnostic logs to aid in the investigation.
- Remote access will only be carried out with the express permission of the customer and shall remain under the customer's supervision and instruction.
- Sophos Technical Support will only use industry recognized tools such as SSH (Secure Shell), Microsoft Terminal Services, LogMeIn Rescue or TeamViewer, to enable remote access to the customer's system.

2.6 Warranty (Sophos XG Appliances only)

The Benefits listed below are provided for customers who are on valid and continuous support contracts. As well, these benefits are valid for Sophos XG appliances only. If the appliance is an SG appliance, please see our UTM 9 guide for options on warranty, extended warranty and technical support.

- Extended Warranty on Sophos XG appliances
  - If a customer wishes to extend their warranty beyond the 1 year included warranty, they will be required to purchase a support plan
- Advanced RMA
  - All customers on a support plan are entitled to Advanced RMA. Sophos will use reasonable endeavors to send a replacement unit to the customer within 24 hours of the notification and receipt of an RMA number, at Sophos' expense. The 24-hour, upfront service is valid for the lifetime of the purchased support contact. When the customer sends the device to Sophos, it is at their own risk
- Technical Support and Warranty for Sophos RED and Access point devices
  - Technical support and software downloads and updates for RED and AP Series Access points follow the appliance to which the devices are associated. If the customer has a valid support contract on their XG appliance, any RED or AP Series Access Points will be covered.
  - If the customer wishes to have an extended hardware warranty for RED and AP Series Access Points, the XG appliance must be covered under an Enhanced Plus support plan.
  - APX Series Access Points are supplied with a 5-year warranty. Further warranty extensions are not possible.
  - The APX Warranty is 5 years from Sophos invoice date. After warranty expires no RMA will be accepted. The APX warranty is independent of any other product.
- High Availability
  - Active/Active: A customer needs to buy a support plan (Enhanced or Enhanced Plus) for each of the active appliances in order receive technical support, advanced replacement or extended warranty for each unit
  - Active/Passive: Technical support on the passive unit will be provided if the active unit has Enhanced or Enhanced Plus support on the appliance. An Enhanced Plus support contract is required for the master (active) unit in order to receive advanced replacement and/or extended warranty for the slave (passive) unit
- For the detailed warranty policy see the following
  - Warranty policy
  - Sophos UTM XG Lifecycle Policy

2.7 Continuous Support Contracts

A customer will receive the above mentioned warranty benefits (section 2.6) only if their support contract is valid and kept continuously active. In the event the support contract lapses, and the customer wishes to receive the benefits mentioned above in 2.6, they may renew their contract. Sophos reserves the right to charge Licensee a reinstatement charge in accordance with its then current price list (which shall be no greater than 6 months of Fees).

3. ENHANCED PLUS

The following service components are available to all Sophos customers who are entitled to Enhanced PLUS support and have valid licenses and, solely with respect to products, paid up maintenance fees.

Enhanced Plus customers receive all the benefits outlined in section 2 as well as the additional benefits outlined below.

3.1 VIP access to Senior Technical Resource Team

- All Incidents submitted by the customer will be tracked in the Sophos incident management system with individual reference numbers and prioritized according to their assigned Severity Level.
- All Incidents submitted via the designated Enhanced Plus support plan (telephone, web and portal) are automatically assigned to priority queues within Sophos Technical Support incident handling procedures.
- Incidents in the priority queues are automatically routed to senior level Sophos Technical Support engineers.

3.2 Remote Consulting

Includes up to 8 hours of Remote Consulting per year provided by a senior Sophos engineer while your support contract is active.

The number of remote consulting hours you receive are based on the type of product you have purchased.

Remote consulting hours for XG Firewall

- 85-200 series: 2 hours
- 300-400 series: 4 hours
- 500-700 series: 8 hours

All other Sophos products: 4 hours

Key services provided as part of remote consulting engagement can include the following:

- A proactive health check:
- Troubleshooting on issues you may be experiencing
- Demonstration of best practices for configuring, managing and basic troubleshooting
- Performance and feature optimization

Items that are out of scope for a remote consulting engagement include the following:

- New setup or installations
- Actual deployment of new appliances
- Configuration changes
- Professional services engagements
- Development or modification of custom scripts

The Remote Consulting Service may include use of a remote connection established through secure encrypted tools (e.g., LogMeIn Rescue, Secure Shell (SSH), Microsoft Terminal Services, TeamViewer). Remote access will only be carried out with the express permission of the customer and shall remain under the customer's supervision and instruction.

3.3 Malware Sample Handling

- All suspicious files submitted via the defined sample submission process (see www.sophos.com/support/samples) are designated for priority malware analysis.

4. TECHNICAL ACCOUNT MANAGER (TAM)

The following service components are available to all Sophos customers who are entitled to a TAM and have valid licenses and, solely with respect to products, paid up Maintenance Fees.

Enhanced Plus is a prerequisite for our Technical Account Management offering.

4.1 Named Technical Account Manager (TAM)

A named Sophos technical support engineer who is dedicated to your account and will perform the following:

- Monitor all customer-logged incidents to facilitate timely, high-quality handling and resolution
- Conduct quarterly customer account reviews
- Champion customer feedback with Sophos product and services management
- Partner with you to understand your business and security needs and help you to maximize the benefit from your Sophos solutions

4.2 Proactive communications and alerts

- Advanced notification of product enhancements, updates, upgrades and advisories
- Access to the VIP Customer Newsletter and VIP Customer Notification

4.3 Performance and feature optimization

- Expert technical advice, assisting you in determining the correct number of servers, hardware capacity and product architecture to account for the evolution of enterprise needs and product requirements
- Annual remote system health checks monitoring Sophos product and making recommendations for product parameter tuning to optimize performance
- Direct access to a senior support engineer during product upgrades

4.4 Enhanced SophosLabs Services

- Advanced assistance for malware outbreaks and access to a SophosLabs Incident Response Manager

4.5 Emergency onsite support

- With a situation of Critical Severity, where other forms of support have been unable to resolve the issue, the customer will have the option to request that a product expert be available on-site as soon as reasonably practicable. We will analyze the critical aspects of the incident and take steps to correct the incident or reduce the severity level

4.6 Championed access to Sophos resources

- Advance notice and access to beta versions of Sophos solutions
- Your TAM will connect directly with Product Managers, SophosLabs Managers, Development, Senior Executives or any other Sophos members as needed to act as your champion within Sophos

5. INCIDENT SEVERITY LEVELS

In order for Sophos Technical Support to prioritize Incidents effectively, Sophos customers should request a Severity Level for each submitted Incident according to the levels detailed in Section 5.1 below.

5.1 Definition of Severity Levels

Critical	High	Medium	Low
A problem related to a Licensed Product that causes a complete loss of a mission critical service in a live or production environment; work cannot continue at all or there is a critical impact to the customer's business operations. No acceptable workaround to the problem exists.	A High Severity is assigned to an Incident that is causing a significant loss of service and no workaround is available. The problem adversely impacts customer business, but operation can continue in a restricted fashion or be alternatively routed.	A Medium Severity is assigned to an Incident that is causing no loss, or only very minor loss in service. The impact is an inconvenience, which does not impede operation or customer business. All Incidents initiated by email will be assigned Medium Severity in the first instance, except those of a Low Severity level, as defined in the next column.	A Low Severity is assigned to a question concerning the operation of a Sophos product, or a suggested change to a product or to the product documentation.

NOTE: Sophos requires that all Critical and High Severity Level Incidents (as such Severity Level is defined in Section 5.1) be submitted via telephone rather than via email or the web in order to facilitate the timeliest response. The initial response from Sophos Technical Support to a Critical Severity Level Incident will normally be by telephone. Subsequent correspondence may be by one or a combination of the above communication methods.

5.2 Severity Level Assignment

All Incidents submitted by a customer will be assigned a Severity Level at the discretion of Sophos Technical Support; taking into account the customer's requested level in accordance with Section 5.1 and the information provided by the customer regarding the Incident.

In the event that a requested Severity Level is not indicated by the customer with the submitted Incident, Sophos Technical Support will assign the Incident a Severity Level of "Medium" or "Low", as detailed in Section 5.1 above.

5.3 Multiple Support Incidents

In the event that an Incident addresses several separate problems, Sophos Technical Support will separate each problem into independent Incidents and classify such Incidents according to the Severity Levels detailed in Section 5.1 above.

5.4 Severity Level Reassignment

Customers who encounter a problem with the Products which is identical to an Incident previously submitted and resolved, must submit a new Incident to be registered. The recurrence of the Incident will again be prioritized according to the Severity Levels detailed in Section 5.1 above. In the event that a submitted Incident with the Products worsens, customers may request that such Incident be reclassified with a higher Severity Level.

6. SERVICE LEVEL TARGETS

6.1 Definition

Response

Sophos Technical Support will respond to every Incident submitted by customers with an acknowledgement that the Incident has been registered, assigned a Severity Level and assigned to a Sophos Technical Support engineer.

Status Updates

Sophos Technical Support will provide the customer with Incident status updates at regular intervals (as set out in Section 6.2 below) to ensure the customer is kept informed of progress in resolving each Incident.

Resolution

An Incident shall be considered resolved when one of the following has occurred:

- The initial question asked has been answered
- A solution has been delivered for the problem initially reported
- A workaround has been delivered for the problem initially reported with a solution to be delivered through a future update
- The problem is scheduled for resolution in a future update and the customer has agreed to wait for the release of such update and does not require a workaround

6.2 Target Service Level Response Times

Sophos Technical Support aims to handle all customer submitted Incidents in accordance with the target service times for the relevant Severity Level as outlined in Table 1 below.

	Severity Level	Target Response Time	Target Status Update Frequency
Enhanced	Critical	Within 4 hours	Daily, or as agreed with the customer/partner
	High	Within 8 hours	Every business day, or as agreed with the customer/partner
	Medium	Within 24 hours	As agreed with the customer/partner
	Low	Within 24 hours	As agreed with the customer/partner

	Severity Level	Target Response Time	Target Status Update Frequency
Enhanced Plus	Critical	Within 1 hour	Every 2 hours, or as agreed with the customer/partner
	High	Within 2 hours	Daily, or as agreed with the customer/partner
	Medium	Within 24 hours	As agreed with the customer/partner
	Low	Within 24 hours	As agreed with the customer/partner

NOTE: In practice, a high percentage of Incidents are resolved by Sophos Technical Support during the first telephone call or email interaction. The Severity Levels and service times below are intended for the percentage of Incidents that require more lengthy investigation, analysis and possibly the development of Products bug fixes or workarounds.

7. ESCALATION PROCEDURES

Sophos' goal is to resolve all Incidents professionally, accurately and in a timely manner. As part of the analysis stage of an Incident, or at any point prior to the resolution of an Incident, Sophos Technical Support may decide to escalate the Incident internally. Depending upon the Severity Level of the Incident, internal escalation will normally occur when Sophos Technical Support determines that further technical assistance and problem diagnosis are needed from senior support staff, or support management, in order to resolve the Incident.

In order to ensure Incidents are resolved in a timely manner, submitted Incidents are normally subject to the following escalation procedures:

Target response/escalation times

Severity	Action	Enhanced	Enhanced Plus
Critical	Engineer actively working on the resolution	Hour 0-8*	Hour 0-2**
	Escalation to Support Management	Hour 8	Hour 2
	Product development	Hour 8	Involved as required
High	Engineer actively working on the resolution	Hour 0-72	Hour 0-48
	Escalation to Support Management	Hour 72	Hour 48
	Plan drafted to ensure reasonable efforts are made to correct the problem or provide a workaround	Time frame agreed upon with customer	Time frame agreed upon with customer
Medium	Engineer actively working on the resolution	Day 0-15	Day 0-15
	In the event the incident worsens, Customer may request severity reclassification	Day 30	Day 30
Low	Engineer actively working on the resolution	Day 0-30	Day 0-30

* During the investigation of a "Critical" Severity Level Incident, if the customer contact person for the Incident (or their suitably technically qualified representative) is unavailable for a period of more than 8 hours, then the Incident will be downgraded to a "High" Severity Level.

** During the investigation of a "Critical" Severity Level Incident, if the customer contact person for the Incident (or their suitably technically qualified representative) is unavailable for a period of more than 2 hours, then the Incident will be downgraded to a "High" Severity Level.

NOTE: Escalations are only possible for Licensed Product-related problems. Problems related to customer-specific environments and/or unsupported use or modification of the Products by customers are not eligible for escalation. All hours are defined as business days.

"With Sophos' consistent 24/7 support, we know we can pick up up the phone anytime and speak immediately to a knowledgeable expert."

Mike Rider, First Keystone Community Bank

Ready to purchase your plan?

Contact your Sophos authorized reseller to get further information today.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American 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

18-11-13 DS-NA (MP)

SOPHOS