SUPPORT SERVICES
DECEMBER 2021

ROHDE&SCHWARZ

Make ideas real

Table of Contents

1 Overview

Rohde & Schwarz Cybersecurity offers customers and partners support services for anomalies and technical specific requests.

The Support web portal (https://my.appsec.rohde-schwarz.com) provides access to support tools, online documentation, release and security notes as well as other services.

Customers and partners have also access to the DevSecOps community (https://dev-appsec.rohde-schwarz.com/), a website for DevSecOps teams operated by Rohde & Schwarz Cybersecurity, where they can keep up to date with the latest news in application security, interact with a community to benefit from the expertise of our team as well as their peers, and share their knowledge.

The procedures or services described in this document may be updated at any time by Rohde & Schwarz Cybersecurity to match internal evolutions and to better serve our customers.

You can find the latest version of this document directly on the Support web portal, as an appendix of the Maintenance and Support Contract : https://my.appsec.rohde-schwarz.com

2 Support offerings

To support its products Rohde & Schwarz Cybersecurity offers two support plans that allows you to define the scope of service that best matches your business and technical requirements.

Taking into account the purchased support plan, Rohde & Schwarz Cybersecurity will use commercially reasonable efforts to provide the applicable services, as set forth in this document.

Support plan features	Advanced	Standard
Supported products	All	All
Support access	Phone / Web Portal	Phone / Web Portal
Spoken languages	English / French	English / French
Hours of operation	24/7[1]	8/5
24/7 web portal access for patches, major/minor releases, documentation & notes	×	×
Hardware advanced repair and replacement[2]	Next business day	J+2 business days
Shipping Cost	Rohde & Schwarz Cybersecurity	Customer

2.1 Support Services

2.1.1 Support web portal

Rohde & Schwarz Cybersecurity maintains an online ticket tracking service via a dedicated Support web portal: https://my.appsec.rohde-schwarz.com

The web portal is the primary contact channel for the technical Support team. Both service offerings, Standard and Advanced, come with 24 x 7 access to the support web portal. Each customer receives dedicated credentials to access the portal.

2.1.1.1 Ticketing system

The Support web portal allows customers and partners to :

- Report any technical problem
- Open / manage trouble tickets
- Handle priority levels
- Stay tuned to ticket status
- Share documents and attachments

[1] for Priority 1 issues only

[2] only applicable if the customer purchased the hardware from Rohde & Schwarz Cybersecurity

2.1.1.2 Other services

In addition to the online ticket tracking service, the web portal also allows customers to acquire :

- The latest software fixes
- Feature releases
- Security advisories and release notes
- Signature updates
- FAQs
- Case management
- Technical documentation

2.1.2 Phone assistance

Phone assistance is available during the times specified for the Rohde & Schwarz Cybersecurity support plan purchased by customer.

The customer must always open a ticket before contacting the technical support engineer by phone. **The phone support channel is intended exclusively for problems with Priority 1**.

Standard support hours are Monday through Friday, 8:00 a.m. to 6:00 p.m. CET.

Advanced support hours are around the clock, 365 days a year.

Phone numbers		
France +33 499 646 760	Germany +49 1805 558 825	USA +1 888 364 7382

2.1.3 Software versions and releases

The support team will maintain and support the list of releases defined as the current support releases on the Rohde & Schwarz Cybersecurity support web portal and make available all supported maintenance releases, minor releases and major releases. It will also verify and correct identified defects in the software for the currently supported maintenance releases.

2.1.4 Appliance support

Appliance support is managed remotely, except for very specific cases.

If a hardware defect is detected by Rohde & Schwarz Cybersecurity Support team or by the hardware manufacturer, an appliance replacement process is initiated within the limits of the manufacturer warranties.

Please refer to the *Rohde & Schwarz Cybersecurity SAS END USER LICENSE AGREEMENT (EULA)* available on the support web portal for more information regarding appliance warranties.

2.2 Support Service Level Agreements

2.2.1 Incident response time objectives

A response time objective for incident and technical problem represents the maximum time for a Rohde & Schwarz Cybersecurity support engineer before contacting a customer or partner after a ticket is logged. This time objective does not predict all the actions that could have been performed before this contact, among which we can have, non-exhaustively, analyzing context, collecting information, gathering datas, identifying known errors.

Response time objectives	Advanced	Standard
Priority 1	within 1 hour	1 business hour
Priority 2	2 business hours	4 business hours
Priority 3	4 business hours	8 business hours
Priority 4	8 business hours	8 business hours

2.2.2 SaaS Service Level Agreement

In Rohde & Schwarz Cybersecurity product portfolio, the Software as a Service (SaaS) cloud WAF provides strong commitments to meet your business needs.

The WAF-as-a-Service (WaaS) R&S®Cloud Protector solution guarantee the following Service Level Agreements:

► Platform availability: 99.95%

► Availability of the administration platform: 99%

3 Customer/Partner roles and responsibilities

3.1 Submitting request

Submitting a request on the support web portal is subject for customers or partners to holding a valid license and being up-to-date with its maintenance.

1. To open a ticket via the support web portal you need the following information:
   - Serial number for appliance or VM number for virtual machine (*for WAF*)
2. If your request is eligible for phone support, you may call the support team once you have created a ticket.
   - You will be requested to:
   - Select your language (English/French)
   - Select your product (Web Application Firewall)
   - Select access to support:
     - For the Advanced Support plan: enter the PIN code if calling outside office hours and your call will redirected to the 24/7 support team
     - For the Standard Support plan you will redirected to the support team during business hours
3. In case of **Priority 1 issue** you have to contact also our hotline by phone and provide the ticket number of your incident
4. You will receive an email notification of the handling of your incident

Please ensure to send all documents requested by the support team at your earliest possible convenience.

3.2 Incident classification

Incidents are defined according to 4 levels of priority:

Priority	Definition
1 (P1)	**Critical | Product is down.** The impact is critical for customer production environment. There is no known workaround.
2 (P2)	**High | Product is impaired** Customer production up, but affected. There is no known workaround
3 (P3)	**Medium | Product function failed, customer production not impacted** Support is aware of the issue and a workaround is available.
4 (P4)	**Low | Non-critical issue** Does not affect customer business. Feature, information, documentation, how-to and enhancement requests from the customer.

When logging a ticket on the Support web portal, you are in charge of identifying the appropriate level of priority regarding the impact and the urgency of the issue from a technical and a business point of view.

The Rohde & Schwarz Cybersecurity Support team will then help you with adapting the level of priority of the issue if necessary to determine the required level of support.

3.3 Best practices for WAF

In order to guarantee the best management of your request by the Rohde & Schwarz Support team and allow for quick action on issues, we strongly encourage you to follow these best practices when opening an incident ticket related to R&S® WAF product (Web Application Firewall, Web Access Manager, Web Service Firewall):

- Provide the more information and technical possible details relative to the incident
- If possible, upload a *debug.dat file* and a *backup* of the impaired equipment by reproducing the issue in debug mode (procedure can be found on https://documentation.appsec.rohde-schwarz.com/display/FAQEN/Generating+a+debug+file)
- If possible provide additional logs (*tunnel's error logs* or *access logs*) that can speed up the understanding and the resolution of your issue
- For security or false positives issues, the *json export* of the security alert is mandatory, the *raw http request* is a plus
- Specify your appliance serial number as it can speed up the process for hardware replacement or root mode troubleshooting if needed
- Give access the Rohde & Schwarz Support team to privileged technical contacts that are certified or trained on our products and your infrastructure

3.4 Best practices for SaaS

In order to guarantee the best management of your request by the Rohde & Schwarz Support team and allow for quick action on issues, we strongly encourage you to follow these best practices when opening an incident ticket related to the SaaS platform for WAF-as-a-Service R&S®Cloud Protector:

- Provide the more information and technical possible details relative to the incident
- Provide the servername and the aliases of the applications impaired
- Provide the tenant of the applications
- Provide the name of the user's tenant
- Give access the Rohde & Schwarz Support team to privileged technical contacts that are certified or trained on our products and your infrastructure

4 Support process, roles and objectives

4.1 Ticket management process overview

When an incident ticket is taken in charge by the Rohde & Schwarz Cybersecurity Support team:

a) An email notification is sent to the user who has logged the ticket

b) a (bis). Additional users may be notified if they have been declared at the ticket creation by the initial user

c) On each response provided by Support team a notification by email is sent

d) In case of **Priority 1**, your Rohde & Schwarz Cybersecurity Sales representative or account manager is also notified

e) In case of improper use of the product, installation of third-party product, incidents generated by third-party product, Rohde & Schwarz Cybersecurity Support team will apply warranty limitation

f) If no response of your part is provided in the ticket within two weeks you will receive a notification during two more weeks and then the ticket will be closed automatically

g) If the incident ticket lead to a product bug, a development ticket will be created and your incident ticket will be closed after notification

4.2 Priority 1 specific management

The Rohde & Schwarz Cybersecurity Support team is composed of highly-qualified engineers that can each handle complex issues. They can also rely on specific tooling developed over the years to help them analyzing and investigating problems. Engineers can also consult the Development teams to resolve issues.

Furthermore, a specific visibility for Priority 1 issues have been put in place:

- Automatic email notification to your Sales representative at ticket creation
- Automatic email notification to the Rohde & Schwarz Cybersecurity Support team Manager at ticket creation
- Automatic email notification to the CODIR members once per day

4.3 Appliance replacement process

1. Rohde & Schwarz Cybersecurity Support receives a product fault complaint via https://my.appsec.rohde-schwarz.com
2. A technical support engineer from Rohde & Schwarz Cybersecurity or the hardware manufacturer will work to troubleshoot the issue and verify if a hardware repair or replacement is required.
3. Support team will validate the warranty, with the appliance serial number. If hardware is not under warranty, Sales team will then provide a quote for the replacement of the hardware.
4. Customer will post the assigned serial number on outside of each box and ship the unit, freight prepaid, to the following address:

Rohde & Schwarz Cybersecurity SAS
501 Rue Denis Papin
34000 Montpellier | France

Customer with Advanced Support plan will not incur any shipping costs for return of equipment.

Germany

Rohde & Schwarz Cybersecurity GmbH
Muehldorfstrasse 15
81671 Munich

Tel: +49(0)89 41 29 - 200 600
Fax: +49(0)30 65 884 – 223

France

Rohde & Schwarz Cybersecurity SAS
Parc Tertiaire de Meudon
9-11 Rue Jeanne Braconnier
92366 Meudon

Tel: +33 1 46 20 96 00
Fax: +33 1 46 20 96 02