SUPPORT HANDBOOK

FortiCompanion to RMA Services

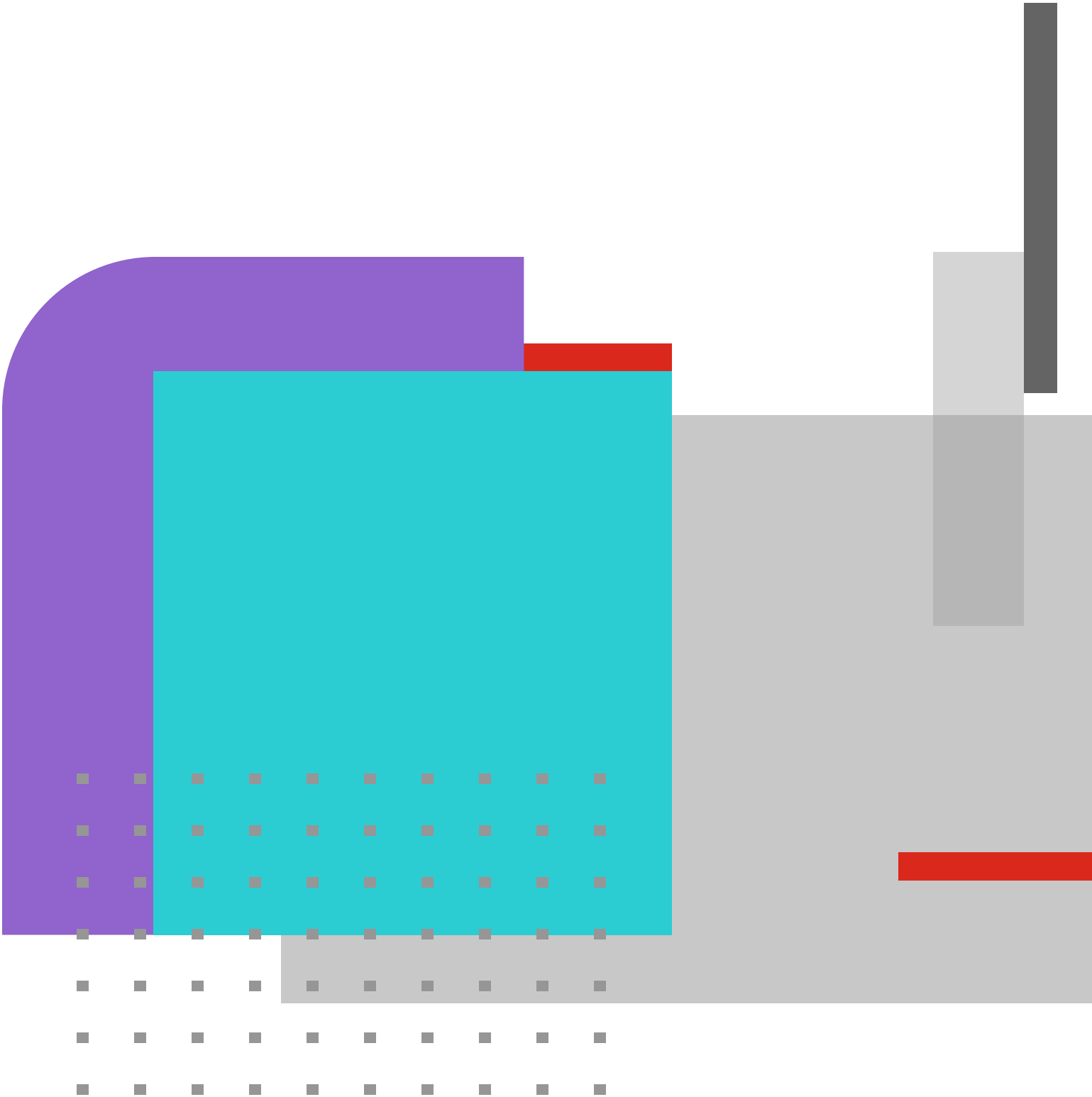

Table of Contents

FortiCare Hardware Support Definitions. 3

Service Scope 4

Requesting Replacement Hardware 5

On-Site Spares 5

Handling Procedure for Customer-Returned Product 6

Priority RMA. 7

Secure RMA. 8

Service Availability 8

Consistent service and the reliability of your security infrastructure are critical to the success of your organization. To address these requirements, the FortiCare service portfolio provides comprehensive programs with global coverage for technical services and security threat management.

Our technical support services aim to prevent problems and recover quickly, with upgrade options available across the portfolio, particularly for replacing defective hardware.

This FortiCompanion handbook will provide you with the information to understand and best use the Return Merchandise Authorization (RMA) hardware replacement services available to you as a valued customer.

Hardware Support Definitions

There are four levels of hardware replacement available for purchase. Refer to the appropriate service description for more information on these service levels.

Return and Replace

After Fortinet confirms a defect, the customer ships the defective hardware (at their expense) to the depot indicated in the RMA ticket. The defective hardware should be packed in its original box with a copy of the RMA form. A replacement will be shipped within three business days of Fortinet receiving the defective hardware.

Advanced Replacement: (Next-Business-Day Delivery)

Fortinet ships a replacement that aims to be delivered the next business day if the defect is confirmed before 14.00 (time of the regional parts depot). The customer ships back the defective hardware, at their expense, to the depot indicated in the RMA ticket. The defective hardware should be packed in its original box with a copy of the RMA form. It should be returned within 30 days following receipt of the replacement. Fortinet reserves the right to invoice for the product if the hardware is not returned within that time.

Priority RMA

Reducing the risk of downtime is vital for customers with critical environments—ranging from small retailers to large enterprises. Priority RMA (PRMA) service can be purchased in one-, three-, or five-year terms to ensure service continuity. Other levels of service are available within the PRMA portfolio to meet your availability needs, which include:

- Next calendar day delivery
- Four-hour hardware delivery
- Four-hour hardware and on-site engineer

The cost of return shipping is included in the Priority RMA service.

Secure RMA

For customers who want to receive a replacement device without returning their defective hardware, the Secure RMA (SRMA) service can be purchased in one-, three-, or five-year terms to ensure service continuity.

Dead on Arrival

Dead on Arrival Manufacturing (DOA-M): If the defect is reported in the first 30 days after receiving the product but no later than 120 days after the date the part was shipped by Fortinet, a new replacement part will be sent to arrive the next business day. The replacement hardware will be a new device. Fortinet will handle the shipping expenses for the return of the defective unit and the shipment of the replacement part.

Dead on Arrival Logistic (DOA-L): If the defect is reported within the first 30 days after receiving a replacement device, a refurbished replacement part will be shipped to arrive at the customer site the next business day. Fortinet will bear the shipping expenses for the return of the defective unit and the shipment of the replacement unit.

DOA Type	Device Type	Shipped Unit
DOA-M	Defective New Product - <120 Days Old	New Product
DOA-L	Defective RMA Replacement	Refurbished Unit

Hardware Warranty

Fortinet recommends purchasing FortiCare services for all products, which will extend hardware coverage on the device. If you do not buy a service contract, you will be covered by a limited hardware warranty service as defined in the End User License Agreement (EULA).

Limitations of the Anti-Tamper Seal

All Fortinet products include a tamper sticker to ensure the device is not compromised. Breaking the seal under any circumstances will void your hardware service coverage, and Fortinet will not accept liability for any damage that may occur.

Chassis and Modules Hardware Coverage

- Fortinet solutions include chassis products (such as the FG-5144C) that can be populated with blades (such as the FG-5001D). The FortiCare service contract on a relevant blade enables hardware replacement services for the chassis. To create a ticket for replacement of any hardware component on the chassis—for example, the shelf manager, power supply, or fan tray—create a ticket against a blade with the appropriate entitlement.
- Fortinet modules provide flexibility for physical network configurations and enhanced firewall performance. Hardware replacement services for a module are enabled through the FortiCare service contract, which is active on the relevant FortiGate product. To create a ticket for the replacement of a module, a ticket should be created against the FortiGate product into which the module is inserted.
- The asset management interface within the support portal allows associating blades or modules with their corresponding chassis to facilitate tracking of the address and physical location.

Product Location

Fortinet will provide hardware services for a product purchased by the customer in one country and installed in another (except in embargoed countries). The regional RMA parts depot closest to the product location will handle the replacement request. As a result, we recommend that you associate an address with each product in the support portal to track assets and facilitate the creation of hardware replacement tickets with the support teams. It is best to keep your product location updated to avoid delays and ensure adequate stock within depots.

Shipment Policy

All shipments are made Delivered at Place (DAP), whereby Fortinet pays the shipping cost, and the customer is responsible for paying all import clearance charges and duties. The replacement will be, in most cases, a refurbished appliance, as noted within the Fortinet EULA. It could be an equivalent or better specification for products that have passed the end-of-order lifecycle phases.

Shipping appliances over 40 kilograms (such as the FortiGate 3980E) may require transportation and handling arrangements, which could extend delivery times.

Hardware Lifecycle Policy

To ensure we provide innovative solutions to customers, products are periodically discontinued. When this occurs, an announcement, including a transition plan, is created. The product then enters the end-of-life phase, during which it is possible to purchase up to 60 months of support services. All information regarding end-of-life announcements is stored on the support portal with the “Hardware and Software Lifecycle Policy.” We recommend that all customers ensure they are familiar with this document.

Requesting Replacement Hardware

Hardware Quick Inspection Package

To verify a hardware failure, you will be requested by the TAC to use a Hardware Quick Inspection Package (HQIP). This dedicated firmware image verifies the CPU, memory, compact flash, hard disk, and PCI devices (NIC/ASIC). For more details on the HQIP process, consult the Knowledge Base.

RMA ticket

Once you have confirmed the failure, TAC will transfer the ticket to RMA. Please ensure you have the following information available:

- Serial number
- Description of the defect
- Steps that were already taken to confirm that the hardware is faulty, including the output of any HQIP testing
- Shipping information

(Note: This is available on ticket creation if you have associated an address with the product in the support portal. To add an address, select the serial number and choose a location.)

On confirmation of the hardware defect, Fortinet will ship a replacement product within the timeframe appropriate for the level of service entitlement.

It is not possible to request the FortiOS version, which will be installed on the replacement unit.

RMA ticket status and definitions

RMA Activity	Support Portal Ticket Status	Definition
Pending Approval	Registered	New RMA request
Approved, Waiting Unit	AwDefUnit	Awaiting defective unit to be returned to initiate a replacement product shipment
Approved, Pending Shipment	In Progress	The RMA team is in the process of preparing and arranging the shipment of a replacement product
Awaiting Defective	RMAReturnPend	Awaiting defective product to be returned by the customer

You may always view your RMA ticket's status by logging in to the support portal.

Service entitlement transfer

Once you have received and installed the replacement hardware, you must transfer service entitlements (FortiCare Technical Support or FortiGuard Security Services) via the support portal. Two options are available for transferring service: Auto Transfer and Manual Transfer.

Note that the automated activation of FortiGuard Services after a license transfer may take up to four hours. You can manually initiate a security service update via the product GUI (Option: Update AV & IPS Definitions).

On-Site Spares

If you use on-site cold spares, you need to follow the procedure outlined below:

(Note: Spares stock must not be registered in the support portal to be able to perform the RMA Transfer.)

1. Log an RMA ticket against the defective hardware with active services upon an incident. This process is required to a) obtain a replacement product and b) ensure transfer of licenses from the defective to replacement hardware.
2. Do not choose the RMA Contract and Service Transfer option within the RMA ticket, as this will transfer the service contract to the replacement unit to be shipped by Fortinet.

3. On approval of the RMA ticket, the licenses may be transferred to the serial number of the on-site spare via the support portal (Product Information/Registration/RMA Transfer). For more information, see this article: Using the RMA Service Transfer Processes.
4. The replacement product, once received, should be stocked until a failure occurs to replace the on-site spare.

Handling Procedure for Customer-Returned Product

Customers should take steps to remove any data stored in the products and reset the equipment's factory default before returning it to Fortinet. Data on the FortiGate boot device and any hard disks can be securely and permanently erased using the **execute erase-disk** command (follows NIST-800-88 - Media Sanitization). This performs a low-level format and overwrites each block with random data. Fortinet retains the right to remove any residual data from the returned equipment. All products that are returned to Fortinet are processed as follows:

- All media is formatted.
- The failure is verified. If it is confirmed that the product is defective, it is sent for repair if viable or scrapped. A certified vendor performs the scrapping of products and includes the physical destruction of the data media.
- If no fault is found, the product is physically refurbished, and any previous customer markings are removed.
- The configuration is erased, and the product is reset to factory defaults.

Customers concerned about the physical retention of secure data on defective products may opt to purchase the Secure RMA service, permitting the local scrapping and nonreturn of the faulty unit.

Statement of policy regarding the removal of data

Upon receipt of defective units, Fortinet uses industry-standard procedures aligned with the National Institute of Standards and Technology (NIST), U.S. Department of Commerce NIST 800-88 "Guidelines for Media Sanitization" to remove data held on specific components within returned systems appropriately.

For products considered repairable for reuse, data will be purged from all storage components, including flash, SSDs, and HDDs, as appropriate for the specific model. The required techniques may differ by technology but shall be based on the above standard definition.

For products deemed damaged beyond repair, Fortinet will use industry-standard procedures aligned to NIST 800-88 to destroy the media, making data retrieval infeasible through physical destruction techniques. The required media to destroy will be dependent on the model and shall include removable flash memory, SSDs, and HDDs. Fortinet will not provide the certificate of destruction.

Storage of defective return products, pending processing

Before products are processed as set forth above, Fortinet will hold such products in a secured warehouse or other storage facility per Fortinet and industry standards.

Prohibited territories

FortiCare Services is not provided in embargoed territories, including Cuba, Iran, North Korea, Syria, and the Region of Ukraine (Crimea, Donetsk, and Luhansk regions). If in doubt, refer to the Global Trade Compliance section of the Fortinet website.

Customs clearance, importation duties, and licenses

Hardware replacements are shipped to the customer with International Commercial Terms DAP using a Fortinet carrier, with the freight prepaid, excluding any import duties, taxes, or other fees.

Fortinet is not responsible for customs clearance, import duties, or licenses for international shipments. For those locations where Fortinet has no local parts depot (as outlined in the Global Service Availability table), an international shipment of the hardware will be required. All international shipments generate customs and duty payment obligations both for the receipt and return shipment of a defective product.

When making a return international shipment of the defective product to Fortinet, it is essential to declare to the relevant authorities certain information, such as a short product description, the Export Control Classification Number (ECCN), and

Harmonized Tariff Schedule (HTS) codes, as well as the value of the defective material. The required information is outlined in the document "Return Proforma Invoice," which can be downloaded from the RMA form contained in each RMA ticket.

This information is vital, as an incorrect declaration may prevent importation. Failure to import will result in the product being returned to the customer with associated costs by their shipping agent. For additional information on customs clearance, contact our customer service team.

The "encryption" aspect of many Fortinet products may require special importation licenses in certain locations. The customer is responsible for ensuring such licenses are available before shipment to avoid delays or confiscating of the products by customs.

Priority RMA

The Priority RMA service is designed for customers who require replacement hardware on-site within a given time frame. The service is initiated by telephone, using dedicated parts strategically located to ensure Fortinet meets the service-level agreement.

Service options

There are three service levels available as an add-on option per product:

- Four-Hour Hardware and On-Site Engineer (4HR-E): A replacement part and engineer will arrive on-site within the four-hour SLA. Note that they may not come together. If requested, an engineer will rack and cable the appliance, restore firmware, IP address, and customer-provided Config, and leave with the defective part.
- Four-Hour Hardware Delivery (4HR): A courier service will deliver a replacement part on-site.
- Next Calendar Day (NCD): A replacement part will be delivered by courier service and arrive on the next calendar day if the exchange is confirmed, per the applicable country cutoff time.

Please note that:

- A Priority RMA service contract may only be activated in combination with FortiCare Premium or FortiCare Elite.
- It is impossible to upgrade to a PRMA service level when a product is in the end-of-life phase.
- Only configurations based on standard base hardware SKUs are maintained with PRMA inventory and covered by the service. For clarity, this excludes SFP, external cables, power supplies, and accessories.

Priority RMA Service Licensing Details

A PRMA contract is required for each Fortinet product for which the service is required. For example:

- If you have a FortiGate with modules installed, you must purchase a PRMA contract for the FortiGate and each module for which the service level is required.
- If you have a chassis, you must purchase a PRMA contract to cover the chassis.

The initial service duration must be a minimum period of 12 months. However, depending on the need, customers can purchase three- or five-year PRMA contracts to ensure service continuity.

Service setup phase

The service includes a 30-day setup phase during which the customer must provide address details, and these are verified to assure the capability to provide the replacement within the service level purchased. This may involve the provisioning of a local parts depot. The progression of the service activation is visible via the support portal, and within 30 days or less, the service will be operational.

PRMA location changes

It is possible to change the location of an appliance by contacting customer service. However, this is subject to service availability at the new address. Ensuring your device location is kept updated is essential. A 30-day setup period may apply to a change of location. Suppose the delivery location is different from the registered location at the time of the request. In that case, Fortinet will work to make best efforts to ensure SLA is achieved but may revert to Advanced Hardware Replacement due to the sudden change and or limitations.

Service Scope

The service delivery process is as follows:

- Upon first contact via telephone, the customer will be asked to confirm the on-site address and a contact name for an individual overseeing the replacement's acceptance.
- For 4HR-E, 4HR, and NCD, the replacement will be delivered to the contact.
- The customer must ensure that the designated individual will be on site to receive the part delivery within the SLA delivery window, and the customer must specify any site-restricted hours.
- The customer is responsible for the product exchange, assuring the configuration and appropriate firmware, and shipment back to the return depot.
- For 4HR-E, the customer must arrange both access to perform the replacement and adequate workspace before the activity. The engineer will exchange the defective part, restore firmware and IP address information, and remain on site until IP connectivity to the unit is confirmed to allow for the restoration of the configuration. The engineer can load the device configuration. However, the customer must provide the device configuration when the ticket is created to be shared with the engineer in advance. The engineer will leave with the defective part if requested. The customer always remains responsible for configuring and managing their Fortinet appliances.

Secure RMA

The Secure RMA service is designed for customers with strict requirements for protecting data within their physical environment. Fortinet products generally store configuration information on solid-state media, which are not field replaceable. As a result, removing these items without invalidating the warranty is impossible.

For maximum security, the Secure RMA service allows for the nonreturn of defective hardware and data protection within the customer's premises. The service is available as an uplift option per product for all RMA replacement levels: FortiCare or Priority RMA.

Service Availability

Please see the service availability page for the latest country-level availability. For your location-specific RMA availability, you may contact your channel partner or your Fortinet account manager.

January 9, 2024 12:20 PM

2331324-B-0-EN