

# FortiCare Reference Guide



## Support FortiCare Reference Guide



# Table of Contents

<b>INTRODUCTION</b> .....	<b>5</b>
<b>SUPPORT OVERVIEW</b> .....	<b>6</b>
<b>FORTICARE SERVICE DELIVERY</b> .....	<b>7</b>
FortiCare Partner Support .....	7
Direct FortiCare Support .....	7
Premium FortiCare Support .....	7
<b>SUPPORT DEFINED</b> .....	<b>8</b>
Product Registration .....	8
Scope .....	8
Product Training .....	8
Third-Party Equipment .....	8
Other Exclusions .....	9
<b>FORTICARE SERVICE LEVEL AGREEMENTS</b> .....	<b>10</b>
FortiCare Case Priority .....	10
Technical Controls .....	11
PriorityFirst Service Level Agreement .....	11
<b>FORTICARE CASE MANAGEMENT</b> .....	<b>13</b>
Case Creation .....	13
Case Owner Communications .....	13
Technical Account Management .....	13
Case Priority Management and Escalation .....	15
Case Closure .....	15
<b>REGIONAL TAC STRUCTURE AND ACCESS</b> .....	<b>16</b>
Structure .....	16
Technical Support .....	16
Customer Service .....	16
Return Materials Authorization .....	16
Technical Account Management .....	16
<b>HOW TO ENGAGE FORTINET SUPPORT</b> .....	<b>17</b>
Product Registration .....	17
Service and Support Entitlement .....	17
FortiCare Knowledge Center .....	19
Downloading Firmware .....	19
Feature Enhancement Requests .....	19
<b>CONTACTING THE TAC</b> .....	<b>20</b>
Opening Cases via the Web .....	20
Logging Problem Reports by Phone .....	20
<b>REGIONAL TAC CONTACT INFORMATION AND COVERAGE HOURS</b> .....	<b>22</b>
Customer Obligations .....	23
<b>RETURN MATERIAL AUTHORIZATION SUPPORT AND POLICY</b> .....	<b>24</b>
Dead on Arrival .....	24
Advance Replacement .....	24
Return & Replace .....	24
Premium RMA .....	25
Premium RMA Service Delivery Terms and Conditions .....	25
Shipping Instructions .....	26

<b>Regional Variations.....</b>	<b>27</b>
Americas .....	27
EMEA .....	27
APAC.....	28
<b>APPENDIX I – DEFINITIONS USED IN THIS DOCUMENT.....</b>	<b>30</b>

## **Introduction**

The Fortinet-branded FortiCare family of support services provides software, firmware and hardware support for all Fortinet products and services to our customers. FortiCare services also include enhanced support such as professional services and technical account management to customers that require the highest service levels and expert implementation consulting.

FortiGuard AV, IPS, URL rating and anti-spam service subscriptions are distinct from FortiCare services and must be purchased separately. Fortinet will provide technical support to all valid subscription holders for any problems that affect the delivery and use of these services.

This reference guide defines the scope and delivery of Fortinet's support service suite as it is delivered by the Fortinet support organization to its Partners and End-Users.

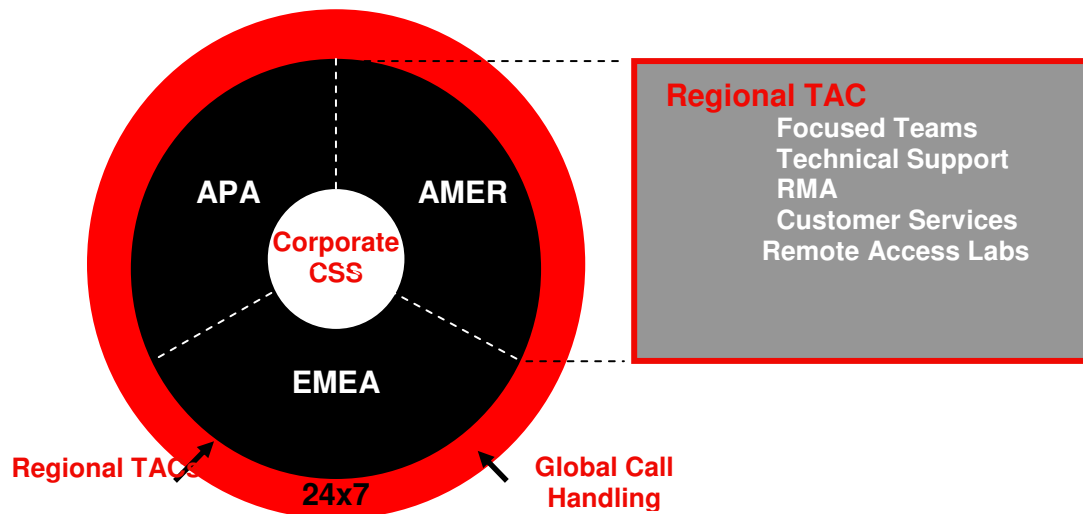
The descriptions of service level agreements (SLA), organizational structures and processes in this guide complement the FortiCare service contract by defining the obligations, expectations and relationship between Fortinet and its FortiCare customers. This document is subject to changes from time to time, so please consult the most current version posted on our support website at <http://support.fortinet.com>.

## Support Overview

The Fortinet support organization is composed of three regional Technical Assistance Centers: the Americas (AMER), Europe Middle East and Africa (EMEA), and Asia Pacific (APAC). These three TACs coordinate with other Fortinet departments such as engineering and logistics that are integral to problem resolution. The regional TACs are contacted through a global call center that provides intelligent routing of incoming service requests to the responsible TAC.

Each regional TAC delivers technical support to the customers in its region during its hours of operation. These TACs also combine to provide seamless support for all customers around the clock.

**Figure 1 – Fortinet Global CSS Organization**



FortiCare *technical support* functions cover the *operate* phase in the lifecycle of a deployed Fortinet product or service. These functions include software, firmware, hardware and FortiGuard service support.

Other FortiCare service components may be engaged in other phases of the complete product deployment lifecycle.

**FortiCare Technical Account Management Services** – dedicated senior technical engineer that provides a single point of contact within Fortinet to coordinate support activities and drive case resolution.

**FortiCare Professional Services** – design, deployment and optimization of Fortinet product deployments through on-demand consulting resources for specific customer projects.

## FortiCare Service Delivery

Fortinet provides differentiated service levels with service level agreements (SLA) that define the commitments and expectations for each level. Fortinet offers both standard and enhanced **PRIORITYFIRST** SLAs to the End-User. **PRIORITYFIRST** decreases the initial time to respond and shortens the reporting interval for increased visibility of the resolution process.

Depending on the subscription purchased, FortiCare Technical Support is delivered via **partner** or **direct** support:

### FortiCare Partner Support

Certified FortiPartners deliver support services on behalf of Fortinet to the End-Users of Fortinet Products and services. End-users who purchase FortiCare contracts from FortiPartners must initially contact the reseller for support. The FortiPartners will provide first and second tier configuration assistance and problem determination to their customers.

Fortinet provides backup and escalation support to the Partner and/or the End-User.

### Direct FortiCare Support

Customers who purchase support directly from Fortinet should contact the Fortinet TAC directly through our main support number or online at <http://support.fortinet.com>. In the United States, all support is provided directly.

The primary language of support is English, though local language support may be provided within each region.

### Premium FortiCare Support

FortiCare Technical Account Management and **PRIORITYFIRST** services provide enhanced enterprise support in all regions. In EMEA and APAC, this is the only direct FortiCare support offering that is provided.

## Support Defined

### Product Registration

***Products must be registered to qualify for technical support.***

Fortinet Products and services may only be registered by the a FortiPartner on behalf of the End-User with the consent and at the behest of the End-User. Alternatively the End-User may register the product directly. Product registration must be performed online through the FortiCare Support Web Site <https://support.fortinet.com/registration>. You must register the Product within twelve months from the date Fortinet originally shipped the Product or all warranty and service entitlements will be forfeited.

### Scope

Subject to entitlement and the guidelines in this document, Fortinet support will diagnose and resolve defects of Fortinet products or services that do not conform to our published documentation. You must install and operate these products and services according to Fortinet specifications.

Fortinet agrees to provide technical support where appropriate to the customer, including:

- Defects exposed during the configuration or operation of Fortinet Products and services
- Hardware failures of devices or components of Fortinet Products
- Availability and operation of Fortinet FortiGuard services

Customer Support does not include the following:

- Step-by-step installation of hardware
- Step-by-step configuration or installation of Products or services
- Professional Services or Technical Account Management
- Modification of firmware, hardware, Products or services

### Product Training

Product training is outside of the scope of Fortinet technical support but is available through Fortinet's training department– for more information see:

<http://www.fortinet.com/support/training.html>.

### Third-Party Equipment

Fortinet Support is provided to assist customers in troubleshooting of Fortinet Products only. Although this support often involves assistance with network configuration and other networking devices such as routers, the customer is responsible for resolving problems that are not directly related to Fortinet Products.

### **Other Exclusions**

Fortinet shall have no obligation to provide Technical Support:

- In the event the customer alters, damages or modifies the Product or any portion thereof;
- For any Product that is not the current Major Release or immediately previous Major Release except as set forth in Fortinet's Product Life Cycle Policy;
- For any Product that has not been publicly released;
- For any problem caused by: accident; transportation; neglect or misuse; alteration, modification, or enhancement of the Product; failure to provide a suitable installation environment; use of supplies or materials not meeting specifications; use of the Product for other than the specific purposes for which the Product is designed; for any problems caused by the End User's negligence, abuse or misapplication;
- For use of the Product on any systems other than the specified hardware platform for such Product. Fortinet shall have no liability for any changes in the End User's hardware, which may be necessary to use the Product due to a Workaround or maintenance release.

## FortiCare Service Level Agreements

All service requests are recorded in the FortiCare Case tracking system. Case Priority determined by business impact drives FortiCare Cases. The Fortinet customer service representative (CSR) will help the Customer Contact to assess the business impact of the support request within the guidelines of the SLA. Case Priority determines all the initial response, reporting interval and notification schedule. This priority can be changed to reflect changed business impact during the life of a case.

### FortiCare Case Priority

By prioritizing Fortinet resources based upon business impact, Fortinet ensures that cases are quickly resolved within expectations defined by the FortiCare SLA.

- Priority is a determination made by Fortinet based on by the priority definitions in this document and the customer's unique problem set;
- Priority is aligned with business impact rather than with any specific technical feature or capability;
- Business impact and therefore Case Priority is a function of the number of users impacted and/or the financial impact to the customer;
- The current Case Priority determines initial response, reporting interval and notification schedule.

**Figure 2 - Case Priority Definitions**

<b>P1</b>	<p>Catastrophic impact to mission critical functionality:            Total loss or continuous instabilities of mission critical functionality.            Critical traffic impact, major loss of connectivity or vital security flaw            Creation of a hazard or an emergency</p> <p><b>Fortinet engagement</b> - resources dedicated 24x7 until resolution or Workaround in place  <b>Customer engagement</b> - designated resources available 24x7 with ability to provide required information</p>
<b>P2</b>	<p>Significant impact to mission critical functionality:            Serious loss or frequent instabilities of mission critical functionality</p> <p><b>Fortinet engagement</b> - resources dedicated 8x5 until resolution or Workaround in place  <b>Customer engagement</b> – designated resources available <b>8x5</b> with ability to provide required information</p>
<b>P3</b>	<p>Minimal impact to major business operations            Occasional or intermittent instabilities of core functions            Limited traffic impact, loss of connectivity or security exposure</p> <p><b>Fortinet engagement</b> – resources committed <b>during normal business hours</b> to provide a resolution or Workaround to restore business operations to acceptable levels  <b>Customer engagement</b> – resources made available <b>during normal business hours</b> with ability to provide required information</p>
<b>P4</b>	<p>Cases involving minor defects to Product, documentation or service, or information requests, or configuration assistance</p> <p><b>Fortinet engagement</b> – to investigate the issue and to provide feedback on the expected resolution.  <b>Customer engagement</b> – to provide additional qualification information as requested by Fortinet</p>

### Technical Controls

The FortiCare SLA provides three important commitments to ensure an timely initial response, transparency of the case resolution progress, and visibility within Fortinet management. The FortiCare case tracking system enforces the following three commitments:

- Initial Response Time – The length of time before a qualified TAC representative will contact the Customer Contact.
- Reporting Interval – The length of time between updates by the TAC Case Owner when a Fortinet action is pending.
- Notification Schedule – Automatic notification of Fortinet management if cases are not resolved in a timely manner. These notifications escalate through the Fortinet management chain as time progresses.

### PriorityFirst Service Level Agreement

Subscription to PriorityFirst service significantly shortens initial response time and increases the reporting intervals, with priority access to TAC and engineering resources to accelerate the Problem Resolution process. The two tables below illustrate the differences between standard and **PRIORITYFIRST** SLAs.

**Figure 3 - Standard FortiCare SLA**

Case Priority	Initial Response	Reporting Interval	Fortinet Notifications
P1	< 1 hour	Every 6 hours	TAC Manager- immediately Regional Sales Director- 6 hours VP Sales- 12 hours Fortinet CEO- 24 hours
P2	< 1 hour	Daily	TAC Manager- immediately Regional Sales Director- 1 business day VP Sales- 2 business days Fortinet CEO- 1 week
P3	Next business day	Every 3 business days	TAC Manager- 1 week Regional Sales Director- 1 month
P4	Next 2 business days	Weekly	TAC Manager- 2 weeks Regional Sales Director- 3 months

**Figure 4 - PriorityFirst FortiCare SLA**

Case Priority	Initial Response	Reporting Interval	Fortinet Notifications
P1	< 15 minutes	Every 3 hours	TAC Manager- immediately Regional Sales Director- 3 hours VP Sales- 6 hours Fortinet CEO- 12 hours
P2	< 15 minutes	Twice daily	TAC Manager- immediately Regional Sales Director- 4 hours VP Sales- 1 business day Fortinet CEO- 2 business days
P3	Same Day (16:00 cut off)	Every business day	TAC Manager- 3 business days Regional Sales Director- 2 weeks
P4	Next business day	Every 3 business days	TAC Manager- 1 week Regional Sales Director- 6 weeks

## **FortiCare Case Management**

### **Case Creation**

Cases can be opened either by phone or the web according to the restrictions of the FortiCare subscription purchased by the customer.

All FortiCare Cases are entered into the tracking system in the form of trouble tickets. All queries and actions taken to resolve the reported issue are documented in this ticket which is continually updated to reflect the ongoing priority, ownership and status of the problem.

The FortiCare ticketing system continuously tracks and reports the associated SLA. The TAC Case Owner is automatically alerted to required actions. Scheduled notifications are sent to management to ensure the visibility of each customer situation. The FortiCare system also delivers automatic alerts of any SLA violations in active cases.

### **Case Owner Communications**

Both the Customer Contact and TAC Case Owner contact information is recorded in each FortiCare Case. Communications between the case owners may use a combination of telephone and web updates driven by the SLA in force. Regardless of the communication method, all information exchanged is recorded in the case tracking system.

The Customer Contact is notified automatically by e-mail when there has been a change to the ticket status or when a comment has been added. Customers may login to the support web portal at any time to review their FortiCare Cases.

### **Technical Account Management**

If you subscribe to Technical Account Management (TAM) services, your TAM engineer is automatically notified when a new case is opened. The TAM contributes a detailed, current understanding of the entire customer environment directly to case resolution. TAMs are senior, experienced security engineers with extensive support and deployment experience with Fortinet products. The TAM advocates for the customer within the support and engineering departments to make sure that issues are addressed and resolved as quickly as possible.

## Case Status

The TAC Case Owner moves the FortiCare Case towards resolution according to the operating SLA using the following case status fields:

**Figure 5 - FortiCare Case Status**

Status	Description
Registered	A new case has been opened. (SLA timer running)
Researching	The TAC engineer is researching the Problem Report. (SLA timer running)
Pending Customer Feedback	An action is required by the customer. (SLA timer stopped) (see section on Case Closure)
Received Customer Feedback	Action completed by the customer (SLA timer running)
On Hold	The customer and TAC engineer have agreed to temporarily suspend the case resolution process. (SLA timer stopped)
Pending Bug Fix	A bug fix request has been submitted. Awaiting a fix from engineering. (SLA timer stopped) (see section on Case Closure)
Solution Provided	A solution has been developed which the customer is evaluating. (SLA timer stopped)
Pending Close Confirmation	Final state before closing the ticket. (SLA timer stopped)
Approval Pending	Specific to Customer Services cases and relating to contract issues etc that fall outside the scope of established policy and for which sales/finance approval is being sought. (timer stopped)
RMA-Conf	The RMA process has been initiated to send a replacement Product to the customer site
RMA-Ship	The RMA unit has been shipped.
RMA-ReturnPend	RMA Advanced Replacement service – awaiting the failed unit to be returned. RMA Return and Replace service – awaiting the return of the defective Product before initiating RMA shipment.
Closed	The problem is resolved and the case is now closed. No further actions are required for this issue. Cases can not be reopened once closed. A new case must be opened.

The SLA timers are operational if an action is assigned to Fortinet. The timers do not run if an action is required from the customer. These status fields are indicated in blue on the above chart. The reporting timers start again once the customer completes the requested action.

## **Case Priority Management and Escalation**

The customer can request the TAC Case Owner to adjust the Case Priority. These changes may occur at any time during the case resolution process. The operating SLA intervals are correspondingly altered.

The customer may request escalation to the TAC manager if an agreement on priority cannot be reached or when the customer feels that insufficient progress is being made. The notification timers ensure that TAC management has a proactive view of customer issues to ensure that adequate resources are dedicated to high priority issues.

## **Case Closure**

As indicated by the SLA definitions, case resolution is an engagement between the TAC and customer which requires constant communication and collaboration.

When a case is moved to "Solution Provided" or "Pending Customer Feedback" states, feedback from the Customer Contact is required. In the case of "Solution Provided", the TAC is awaiting confirmation that the problem has been resolved.

The FortiCare system will automatically send weekly reminders to the Customer Contact to notify them that an action is required. This continues for four weeks. After that period, the case will move to "Pending Close Confirmation" and wait for three more working days sending daily reminders to the Customer Contact. If after that time there has been no response from the customer, the case is automatically closed.

If customer feedback is not possible within the 4 week notification period, the customer should ask the TAC Case Owner to place the ticket on hold to avoid closing.

## **Regional TAC Structure and Access**

### **Structure**

The regional TACs in EMEA (Europe, Middle East and Africa), AMER (Americas) and APAC (Asia Pacific) deliver 8x5 customer support for their regions according to the time-zone where the TAC is located. The regional TACs also combine to deliver out-of-hours support to customers who have 24x7 FortiCare service subscriptions.

In each Fortinet TAC are four main teams: Technical Support, Return Material Authorization, Customer Service and Technical Account Management.

### **Technical Support**

The *Technical Support team* is subdivided into specialized groups of support engineers that work together to quickly answer Product questions and resolve network integration issues. The Technical Support team interfaces with the Fortinet engineering organization to ensure that bug fixes are addressed promptly.

### **Customer Service**

The *Customer Service Team* is composed of customer service specialists who are responsible for entitlement, contracts and the resolution of product registration issues. They are also responsible for related service programs such as FortiCare, FortiGuard, Evaluation & Co-terminus agreements.

### **Return Materials Authorization**

The Return Material Authorization Team handles all RMA requests. They manage the shipping process and the return of defective hardware Products.

### **Technical Account Management**

The technical account managers (TAMs) are co-located with the Technical Support teams to ensure maximum management oversight for problem resolution, to facilitate communications and to ensure expedient escalations as necessary.

## How to Engage Fortinet Support

To engage Support you should complete the following:

- Register your product online to confirm entitlement to FortiCare services
- Log onto FortiCare support portal at <http://support.fortinet.com> – verify FortiCare status, determine contact information to access Fortinet Support
- Use the FortiCare Support Portal for instant access to the Knowledge Center, documentation, release notes, etc.
- **For direct support customers:** contact the Fortinet TAC
- Contact your Certified FortiPartner.

### Product Registration

The customer must register all Fortinet Products (hardware and service contracts) at <https://support.fortinet.com/Login/UserRegistration.aspx> prior to requesting support. This is the responsibility of the customer although in some cases your FortiPartner may register the Product on your behalf.

For further instructions on logging into the Customer Support Web Portal and registering Product and service contracts, please refer to the [Fortinet Product Registration Guide](#) at:

<http://kc.forticare.com/redirfile.asp?id=1681&SID=>

### Service and Support Entitlement

To determine support entitlement, log onto the FortiCare support portal at <https://support.fortinet.com>. The level of support entitlement is illustrated in the table below. The default coverage applies unless a FortiCare bundle is purchased along with the unit.

All FortiCare & FortiGuard Service contracts must be registered in order to activate services. If you do not register with the registration code located on your support contract, you will be ineligible for technical support. Your network may also be susceptible to unknown threats and possible vulnerabilities through not receiving updates from the FortiGuard Distribution Network.

All unregistered FortiCare and FortiGuard service contracts expire twelve months from the date of shipment from Fortinet.

**Figure 6 - Service Entitlement**

FORTICARE	BUNDLES*	DEFAULT	FORTICARE 24x7	FORTICARE 8x5*
<b>PRIVILEGED WEB ACCESS</b>				
Online Documentation	First year 24x7	First 90 days 24x7	24x7	24x7
Product Registration & Contract Management	First year 24x7	First 90 days 24x7	24x7	24x7
<b>TECHNICAL SUPPORT</b>				
Phone	First year 8x5	No	24x7	8x5
Web	First year 8x5	First 90 days 8x5	8x5	8x5
<b>SOFTWARE SUPPORT</b>				
Maintenance and Feature Releases	First year 24x7	First 90 days 24x7	24x7	24x7
<b>HARDWARE WARRANTY</b>				
Warranty	First year Return & Replace 3 days	First year Return & Replace 3 days	Advanced Replacement Next Business Day	Return and Replace 3 days

\* does not include phone support in EMEA or APAC.

**Figure 7 - FortiGuard Services**

FORTIGUARD	BUNDLES	ALL OTHER PRODUCTS	SUBSCRIPTION
Anti-Virus Updates	First Year, 24x7	30 Day Trial, 24x7	24x7
IPS Updates	First Year, 24x7	30 Day Trial, 24x7	24x7
Web Content Filtering	First Year, 24x7	30 Day Trial, 24x7	24x7
Anti-Spam	First Year, 24x7	30 Day Trial, 24x7	24x7

**Note:** The Services provided here do not include installation services which may be purchased separately. 30 Day Trials for non bundle Products are self-administered online.

All service contracts start immediately upon registration. If the Product has not been registered within one year of being shipped by Fortinet, all service contracts are automatically voided. Standard or renewal contracts apply an extended period of coverage to Fortinet Products.

## FortiCare Knowledge Center

The [Fortinet Knowledge Center \(http://kc.fortinet.com\)](http://kc.fortinet.com) contains how-to and troubleshooting articles, FAQs and detailed technical information to familiarize you with the operation of your Fortinet Product. The site also contains links to both the Fortinet support site and documentation site for all official guides.

The Fortinet Knowledge Center interfaces to all Fortinet Product technical information, and should be consulted prior to contacting the Fortinet technical support team.

## Downloading Firmware

Fortinet uses the following naming convention for firmware releases:

<Major Release><Maintenance Release><Patch Build>

For example: *FortiOS 3.0 MR4 Patch 7*

**Major Release** – a new major release signifies a significant change in feature set.

**Maintenance Release** – contains minor additions to the feature set that have passed both internal QA and field testing and is recommended by Fortinet for use in Production environments. Customers are still encouraged to review the release notes provided along to check for any outstanding issues that are known at the time of release.

**Patch Build** – built to address specific issues affecting the maintenance release. No feature changes from the associated Maintenance Release are made in this build.

Firmware images and associated release notes for all Fortinet Products are available for download from the Fortinet Support web portal:

<https://support.fortinet.com/EndUser/FirmwareImages.aspx>

An RSS feed is available to notify registered customers of newly available firmware at:

<http://docs.fortinet.com/firmware.xml>

## Feature Enhancement Requests

Feature Enhancement Requests should be directed to a Fortinet Sales Engineer or FortiPartner. The sales channel will be in the best position to assess the business value of your proposed request and promote its implementation.

Fortinet Maintenance Release notes include a list of Feature Enhancements introduced in the release.

## Contacting the TAC

End-users who purchase FortiCare contracts from FortiPartners should contact them for all support issues. The FortiPartner is committed to provide first and second level support to the End-User, such as configuration assistance and fault isolation.

Fortinet provides escalation support to the FortiPartner in the event that the Level 1 and Level 2 support provided by the Partner does not resolve the reported issue.

In the case of *direct support*, the End-User may directly engage the Fortinet TAC for all support calls.

For escalation issues and direct support contracts, the FortiCare customer may open cases with Fortinet Support by the phone or web subject to entitlement.

- P1 and P2 problems should be created by contacting Fortinet TACs by phone.
- P3 and P4 problems should be created directly on the web and may be done at any time regardless of the level of FortiCare entitlement.

### *Opening Cases via the Web*

End-users may open cases by logging onto Fortinet's support website <https://support.fortinet.com>. This is only available to customers with a valid service contract. Accounts for this site are provided upon initial Product registration. (See the "Fortinet Product Registration" guide).

FortiPartners may create FortiCare cases on their customers' behalf via the Fortinet Partner website <https://partners.fortinet.com> by selecting "Online Support Ticket".

### *Logging Problem Reports by Phone*

Calls made to Fortinet Support are handled consistently regardless of time or location. Incoming calls enter a call center where they are answered by a Customer Services Representative (CSR) and routed to the appropriate specialist Customer Services Engineer (CSE) in the TAC if phone support has been purchased.

The following information must be made available to the CSR:

- Customer or Partner Name
- Serial Number
- Fortinet Product Type and Description
- Software/Firmware Version
- Customer Contact Name
- Customer Contact Contact Information
- Problem Description.
- Configuration file(s)

The role of the CSR is:

- Verify FortiCare entitlement
- Describe the problem in the ticket
- Establish Case Priority with the customer
- Assign the case to the appropriate TAC team

The CSR will not start troubleshooting the case on this initial contact. The objective is to align the problem with the appropriate TAC team from the outset. P1 and P2 cases are transferred immediately while on the phone with the CSR. P3 and P4 cases are logged and the ticket is responded to within the defined response and report intervals.

The following information should be available to the CSE.

- Troubleshooting conducted to date
- Network topology diagrams
- Network map
- FGT debug log file

The role of the CSE is to diagnose and resolve the reported technical issue.

## Regional TAC Contact Information and Coverage Hours

### **Americas**

Located in Vancouver, BC, Canada  
Phone: 1-866-648-4638 (toll-free)<sup>1</sup>  
1-408-486-7899  
Web site: <https://support.fortinet.com>  
Normal office hours: Monday-Friday 6:00 AM - 6:00 PM Pacific Time

### **EMEA**

Located in Sophia Antipolis, France  
Phone: +33-4-8987-0555  
Web site: <https://support.fortinet.com>  
Normal office hours: Monday-Friday, 9:00 AM – 6:00 PM Central European Time

### **APAC – Kuala Lumpur**

(Support offered in English and Chinese)  
Located in Kuala Lumpur, Malaysia  
Phone: Please contact your local Partner  
Web site: <https://support.fortinet.com>  
E-mail: Please contact your local Partner  
Normal office hours: Monday-Friday, 9:00 AM-5:00 PM Malaysia Time (GMT+08:00)

### **APAC - Tokyo**

(Support offered in Japanese)  
Located in Tokyo, Japan  
Phone: Please contact your local Partner  
Web site: <https://support.fortinet.com>  
E-mail: Please contact your local Partner  
Normal office hours: Monday-Friday, 9:00 AM-5:00 PM Japan Standard Time (GMT+09:00)

### **APAC - Beijing**

(Support offered in Mandarin)  
Located in Beijing, China  
Phone: Please contact your local Partner  
Web site: <https://support.fortinet.com>  
E-mail: Please contact your local Partner  
Normal office hours: Monday-Friday, 9:00 AM-5:00 PM China Coastal Time (GMT+08:00)

---

<sup>1</sup> Toll-free calls are permitted from US & Canada only

### **Customer Obligations**

- The customer is responsible for ensuring that the Fortinet system is used and maintained in accordance with applicable Product documentation.
- Fortinet is not responsible for supporting third party products that Fortinet has not supplied. The customer is responsible for maintaining a support agreement with the third party for such products.
- The customer shall make all reasonable efforts to maintain Fortinet software at the **most current software release** level.
- The customer will **provide connectivity** to the Product in order for Fortinet to establish a data link for Fortinet Support to conduct remote access and maintenance. The customer and Fortinet will agree on the appropriate security measures to prevent unauthorized access but ultimate responsibility for the security of the network lies with the customer. Fortinet will not connect to the customer's network without prior authorization and such connection will be solely to provide technical support.
- The **customer's staff must be available** as required by Fortinet to aid in problem diagnosis and provide electronic access to the affected Product. Should the customer fail or cause delay in providing connectivity Fortinet will be excused from its fault resolution performance for a period equal to such failure or delay.
- Many features on Fortinet Product require **a familiarity with data networking** in order to implement. In general, Fortinet recommends that Fortinet Product be maintained by staff that is familiar with the basics of data networking. In cases where a customer does not have IT staff with the requisite background, the customer may need to involve a 3<sup>rd</sup>-party consultant to work with Fortinet Support to resolve the issue.

## **Return Material Authorization Support and Policy**

The return and replacement of defective hardware follows the Return Material Authorization (RMA) process. Three types of support for RMA are offered: Dead On Arrival, Advanced Replacement and Return & Replace.

Once we have processed and accepted your request, the regional Fortinet RMA coordinator will provide you with an RMA number and a form for you to complete to confirm shipping address information.

To help expedite the RMA acceptance process, we strongly recommend you to visit our online troubleshooting site (<http://kc.forticare.com/default.asp?id=1067&SID=&Lang=1> ) and provide us with diagnostic results.

Please note that an RMA will be refused if:

- The defective unit is received with a broken warranty seal
- The defective unit was not packed properly (see Shipping instructions)
- The defective unit is received while the RMA is not yet approved
- The defective unit has an abnormal physical damage

### **Dead on Arrival**

A unit is classified as DOA (Dead on Arrival) if a defect is reported within the first 30 days of Product Warranty which commences on the product registration date but not later than 120 days from shipment. Fortinet handles all DOA requests as advanced replacement within the next business day.

Fortinet will bear the cost of shipment for both the return of the defective unit and the supply of the replacement unit.

### **Advance Replacement**

*"We ship you a replacement unit, then you return the defective unit"*

Advance Replacement is available for registered hardware covered by a support contract that allows the customer to request that a replacement unit ship prior to the return of the failed unit.

This service requires an evaluation of the failed system by a Fortinet Technical Support Engineer who issues an RMA number. Fortinet ships Advance Replacements at our expense via ground carrier by the next business day following the issue of the RMA authorization.

You must send the failed unit to Fortinet at your expense, within 30 days after issuance of the RMA to avoid replacement charges, billed at the current list price of the unit including installed options. A replacement unit may be a new or reconditioned unit of equivalent or better value.

### **Return & Replace**

*"You ship us the defective unit, we replace it for you"*

Return and Replace Replacement is available for registered hardware covered by a support contract or still under warranty.

Replacement of hardware under Fortinet's standard warranty requires an evaluation of the failed system by a Fortinet Technical Support Engineer who issues an RMA number.

Customers must ship the subject unit pre-paid to Fortinet. You must indicate the RMA number clearly on the box and shipping papers – failure to do so will result in delays. We will ship you a replacement unit via ground carrier at our expense within 3-5 (**See Regional Variations**) business days after receipt of the failed unit. A replacement unit may be a new or reconditioned unit of equivalent or better value.

### **Premium RMA**

Fortinet offers a Premium RMA service. This service allows customers to choose from several different types of service, including 4 hour Parts on Site, 4 hour with On-site Engineer or next day replacement.

Premium Service provides the customer with a choice of service delivery options:

- **4HR Onsite Engineer (4HR-OSE)** – RMA parts delivered by an installation engineer, 24 hours a day, 7 days a week; hardware and engineer arrive within 4 hours of RMA verification and approval by the TAC
- **4HR Courier (4HR-C)** – RMA parts only delivery 24 hours a day, 7 days a week, hardware is delivered within 4 hours of RMA verification and approval by the TAC
- **Next Day Delivery (NDD)** – RMA parts only orderable up until midnight for next day delivery following verification and approval by the TAC

The Premium SLA is measured from the time the TAC determines a part is defective and issues the RMA order, to the time when the replacement part arrives on site. Installation of the replacement part is outside the scope of the SLA.

#### *Premium RMA Service Delivery Terms and Conditions*

Due to the elevated service level agreements associated with the Premium RMA services, these service capabilities are not available in all geographies and in all cases, subscription is subject to the following terms and conditions:

- Availability and ordering is conditional on the receipt of pre-approval from the Fortinet service capability process.
- Only annual contracts are available
- A 24x7 basic FortiCare service contract is required for any upgrades to Premium RMA service
- Products in the End Of Life phase are not eligible for Premium RMA services
- The first year of Premium RMA service includes a 30 day set up time plus 11 months service capability. The first 30 days are covered by 24x7 next business day delivery.
- Renewals of Premium RMA services are valid for a full 12 months

## Shipping Instructions

Unit should be packed and sealed/closed in a manner that allows them to be opened and resealed/reused without altering the basic integrity of the package. This applies particularly to export packaging going through customs.

Logistic documents should include packing list and shipping invoice with the following information supplied:

No serial number should appear on the shipping invoice. When returning defective material, a Pro-forma invoice must be provided from non-EU countries indicating the Pro-forma invoice is for custom only with no commercial value. To minimize lead-times, please ensure there is no mismatch between the logistic documents and the physical goods (in terms of part reference, serial number and quantity) as this will result in customs non-conformity. In this case, all original shipping documents have to be re-issued and expedited to the Customs Office to get the goods cleared. Customers should return any defective unit within 30 days of receiving the replacement. After 30 days, Fortinet may invoice the customer for units not returned. Shipment of a defective unit should use the same box the replacement product was shipped in.

Upon your receipt of the RMA replacement (and/or related parts), carefully pack and return the original system and/or related parts to Fortinet in the same box in which the replacement was shipped. Include the form with your shipment and indicate the RMA # on your shipping documentation as well as on the box. Fortinet has no obligation to:

- a) Accept any systems (and/or related parts) which have been damaged in shipment, or
- b) Issue the applicable RMA credit(s) to Company in the event of such damaged shipments.

### Packing list

- Product Descriptions
- Quantity per item
- Serial number
- Net and gross weight
- Quantity of crates or parcels
- RMA form

### Shipping invoice

- Ship to address
- Product Descriptions
- Quantity per item
- Defective Unit value
- Total value for customs only
- Currency

## ***Regional Variations***

Due to country-specific import and export regulations, customs and shipping authorization may take longer to obtain for some countries than for others. Warranty Returns for customers outside of North America will be shipped within 3 business days after receipt of the failed unit.

### **Americas**

#### *Contact*

Americas Technical Assistance Center is the primary contact point to reach logistics for all service enquires:

Phone: 1-866-648-4638 (toll-free)  
1-408-486-7899

Web site: <https://support.fortinet.com>

#### *Shipping Address*

Fortinet, Inc.  
1090 Kifer Road  
Sunnyvale, CA 94086  
USA

### **EMEA**

#### *Contact Point*

EMEA Technical Assistance Center is the primary contact point to reach logistics for all service enquires:

Phone: +33 4 8987 0500

Fax: +33 4 8987 0501

Web site: <https://support.fortinet.com>

#### *Shipping Address*

FORTINET RMA Department  
120 rue Albert Caquot  
06560, Sophia Antipolis  
France

## APAC

RMA Coordinators are located in each of the 3 Technical Assistance Centers in the APAC region. RMA issues however should be reported to your local partner who will coordinate with the regional TAC to handle the logistics aspects.

### *Kuala Lumpur*

(Support offered in English and Chinese)  
Located in Kuala Lumpur, Malaysia  
Phone: Please contact your local Partner  
Web site: <https://support.fortinet.com>  
E-mail: Please contact your local Partner  
Normal office hours: Monday-Friday, 9:00 AM-5:00 PM Malaysia Time (GMT+08:00)

### *Tokyo*

(Support offered in Japanese)  
Located in Tokyo, Japan  
Phone: Please contact your local Partner  
Web site: <https://support.fortinet.com>  
E-mail: Please contact your local Partner  
Normal office hours: Monday-Friday, 9:00 AM-5:00 PM Japan Standard Time (GMT+09:00)

### *Beijing*

(Support offered in Mandarin)  
Located in Beijing, China  
Phone: Please contact your local Partner  
Web site: <https://support.fortinet.com>  
E-mail: Please contact your local Partner  
Normal office hours: Monday-Friday, 9:00 AM-5:00 PM China Coastal Time (GMT+08:00)

### *APAC Region Logistics Consolidation Center*

Fortinet International Inc C/O JvanAn International Logistic Company Inc  
No. 2 Lane 43, Shingbang Road.  
Taoyuan City, Taoyuan, Taiwan 330, ROC.

## Disclaimers, Exclusions, Warranties and Other Terms

### Terms and Conditions:

Support services. All support services (FortiCare or FortiGaurd) provided by Fortinet are subject to and governed by Fortinet's support services contract. For more information regarding the applicable terms and conditions, please see the following link. <provide link to service contract>

Warranty Services. All warranty rights, services, and claims are subject to and governed by Fortinet's End User License Agreement. For more information regarding the applicable terms and conditions please see the following link:

[http://www.fortinet.com/doc/legal/EULA\\_June\\_2007.pdf](http://www.fortinet.com/doc/legal/EULA_June_2007.pdf)

Limitation of Liability. NOTWITHSTANDING ANYTHING TO THE CONTRARY, IN NO EVENT WILL FORTINET BE LIABLE TO THE CUSTOMER FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES OF ANY KIND, INCLUDING BUT NOT LIMITED TO ANY LOST PROFITS OR LOSS OF DATA HOWEVER CAUSED, WHETHER FOR BREACH OR REPUDIATION OF CONTRACT, TORT, BREACH OF WARRANTY, NEGLIGENCE, OR OTHERWISE, WHETHER OR NOT FORTINET WAS ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES. NOTWITHSTANDING ANY OTHER PROVISIONS OF THIS AGREEMENT, FORTINET'S TOTAL LIABILITY TO THE CUSTOMER ARISING FROM OR IN RELATION TO THIS AGREEMENT AND THE SERVICES, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR STRICT LIABILITY, SHALL BE LIMITED TO THE TOTAL PAYMENTS MADE BY CUSTOMER TO FORTINET UNDER THIS AGREEMENT. THIS LIMITATION WILL APPLY TO ALL CAUSES OF ACTION IN THE AGGREGATE. IN NO EVENT WILL FORTINET BE LIABLE FOR THE COST OF PROCUREMENT OF SUBSTITUTE GOODS. THE FOREGOING LIMITATIONS OF LIABILITY SHALL NOT APPLY TO DAMAGES ARISING FROM DEATH OR PERSONAL INJURY IN ANY JURISDICTION WHERE SUCH LIMITATION IS PROHIBITED BY APPLICABLE LAW. TO THE EXTENT PERMITTED BY LAW, IN NO EVENT SHALL FORTINET'S TOTAL LIABILITY UNDER THIS AGREEMENT EXCEED THE AMOUNT ACTUALLY RECEIVED BY FORTINET FROM FORTIPARTNER DURING THE THREE (3) MONTHS PRECEDING THE EVENT WHICH GAVE RISE TO SUCH FORTINET LIABILITY.

Warranty Disclaimer. EXCEPT FOR WARRANTIES CLEARLY AND EXPRESSLY STATED IN THE FORTINET SERVICE REGISTRATION AGREEMENT, NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET MAKES, AND YOU RECEIVE, NO OTHER WARRANTIES OF ANY KIND, EXPRESS, IMPLIED OR STATUTORY, ARISING IN ANY WAY OUT OF, RELATED TO, OR UNDER THIS AGREEMENT OR THE PROVISION OF MATERIALS OR SERVICES HEREUNDER, AND, TO THE EXTENT PERMISSIBLE BY LAW, FORTINET SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY OF SATISFACTORY QUALITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY RIGHTS

Information Disclaimer. FORTINET MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN MATERIAL PROVIDED IN FORTINET'S KNOWLEDGE CENTER. FORTINET INTENDS THE INFORMATION CONTAINED IN THERE TO BE ACCURATE AND RELIABLE. HOWEVER, ERRORS MAY OCCASIONALLY OCCUR. THEREFORE, ALL INFORMATION AND MATERIALS ARE PROVIDED "AS IS" WITHOUT ANY WARRANTY OF ANY KIND. FORTINET DISCLAIMS ANY WARRANTIES, EXPRESS OR IMPLIED, REGARDING ANY MATTER WHATSOEVER RELATING TO OR REFERENCED BY THIS WEB SITE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

## Appendix I – Definitions used in this Document

End-user	The purchasing organization of a FortiCare service contract.
Partner	A Fortinet certified partner who is engaged in and meets the requirements of the FortiPartner Program.
Product	A Fortinet product or service.
Support	Assistance provided by the TAC to the End-User or Partner to resolve a reported problem.
Level 1 Support	Product information, hardware and software configuration, installation and upgrade questions. Basic problem isolation such as searching the Knowledgebase for known problems and providing existing solutions to customers. Hardware replacement as needed.
Level 2 Support	In-depth problem determination and resolution by analysis of logs and traces, remote diagnosis where possible or local problem recreation. Documentation of all troubleshooting, actions taken and their results. Define action plans including validation of Workarounds or resolutions in the simulation environment prior to deployment. Complex Problem Resolution should be achieved in most cases by Level 2 Support.
Level 3 Support	Advanced fault isolation by closely simulating the customer environment in the FortiLab. Document and correlate all symptoms, problem scenarios, analyses and observations. Deliver Workarounds when possible to resolve critical situations.
SLA	The service level agreement set out in this guide which defines the services and accountabilities Fortinet contracts to provide.
FortiCare Case	A trouble ticket detailing the activity on a particular service request to the Fortinet TAC from an End-User or Partner.
Customer Contact	The primary contact person in the End-User or Partner recorded in a FortiCare Case that is engaged by the TAC according to the SLA and Case Priority definitions.
TAC Case Owner	The primary engineer in the TAC recorded in a FortiCare Case, that the Customer Contact engages according to the SLA and Case Priority definitions.
Problem Report	A description of unexpected behavior of a Product or caused by a Product described in a FortiCare Case.

Case Priority	A measure of the business impact of the FortiCare Case as specified by the End-User and agreed by Fortinet within the context of the Case Priority definitions within the SLA.
TAC	A regional Fortinet Technical Assistance Center staffed by Fortinet Personnel providing assistance with Problem Resolution. Consists of Level 1, 2 and 3 Support.
Problem Resolution	<p>The engagement by the TAC and the Customer Contacts according to the SLA and using all reasonable commercial efforts to resolve a Problem Report, that results in any one or more of the mutually agreed conclusions:</p> <ol style="list-style-type: none"> <li>1) The reported problem does not reoccur and cannot be reproduced by the Customer Contact or the TAC;</li> <li>2) The reported problem is not caused by the failure of the Product to meet its published specifications, i.e. the problem is caused by the operation of a Third Party product;</li> <li>3) A Workaround is delivered to and accepted by the Customer Contact as a final solution to the Problem Report;</li> <li>4) The Product conforms to design specifications, and a Feature Request will be opened to address the behavior requested by the customer;</li> <li>5) A new and officially released version of the Product has been installed that corrects the problem;</li> <li>6) Engineering has fixed the reported problem. The fix will be released in the next MR release.</li> </ol>
Case closed	The closing of a FortiCare case, either when a Problem Resolution is achieved or when the Customer Contact fails to respond within the time described by the automatic case closure process described by the SLA.
Workaround	A configuration or procedural change to avoid the reported problem without substantially impairing the use of the Product.
Bug Fix Request	A request to modify a Product or service to align its functionality or performance with the published specification.
Feature Request	A request to modify the published specification or capabilities of a Fortinet Product or service. Tracking and reporting is provided by Fortinet sales personnel or through TAM services where applicable.