



# FORTINET SECURITY FABRIC LICENSING GUIDE

R11 / 04-OCT-2018 / FINAL

ALSO SCHWEIZ AG

Ivo Tibolla

BU Security / Division Solutions

## Table of Content

Document Information .....	2
About ALSO Cyber Security and this Guide .....	2
About Fortinet .....	2
Security Fabric .....	3
FortiGate Security Appliances .....	4
FortiGate Licensing .....	4
FortiGuard Security Services for FortiGate .....	5
FortiMail Secure Email Gateway .....	8
Form Factors .....	8
Deployment Modes .....	8
FortiGuard Security Services for FortiMail .....	9
FortiMail Appliance Licensing .....	10
Resources .....	10
FortiMail Cloud .....	11
FortiMail Cloud — Gateway .....	11
FortiGuard Security Services for FortiMail .....	11
FortiMail Cloud Licensing .....	11
Resources .....	11
FortiClient End-Point Protection .....	12
FortiClient Key Modules .....	12
FortiClient Licensing .....	12
FortiCare Maintenance & Support Services (Ticket) .....	13
FortiCare Hardware Support Definitions (RMA) .....	15
Resources .....	15

## Document Information

This guide contains information on how to license typical Fortinet solutions like **FortiGate**, **FortiMail**, **FortiSandbox**, **FortiClient**, **FortiManager** and **FortiAnalyzer** – all components of the Fortinet Security Fabric.

### Publisher

ALSO Schweiz AG, BU Security  
Meierhofstrasse 5, CH-6032 Emmen

This document, its annexes and all content are the property of ALSO Schweiz AG and may not be copied, reproduced, transmitted or used for any purpose without the written consent of ALSO Schweiz AG. Contents which do not originate from ALSO are protected by copyrights by the respective publisher.

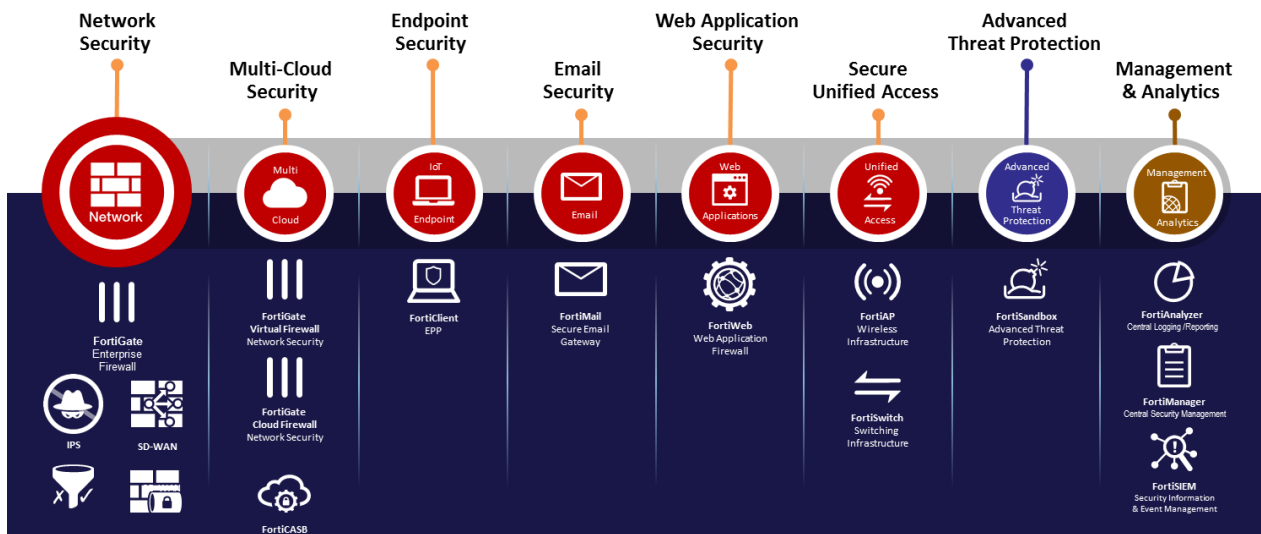
Version / Author	Release Date	Changes
R11 / Tii	October 4, 2019	Modification based on Q4'18 PL valid as of November 1 <sup>st</sup> , 2018
R10 / Tii	October 1 <sup>st</sup> , 2019	Title changed from FortiGate Licensing Guide to "Security Fabric Licensing Guide" to include Security Fabric modules like FortiMail, FortiClient
R09 / Tii	July 26, 2018	FOS 6.01. and Licensing changes with Q3'18 price list.
R01 – R08 / Tii	2017 – 2018	Initial releases

## About ALSO Cyber Security and this Guide

ALSO's European B2B marketplace is the trading center for goods and services of the ICT industry. Exactly tailored to the needs and requirements of the most diverse customers. That makes ALSO a competent, reliable, and sustainable partner. With comprehensive solutions in the field of cyber security, ALSO offers a comprehensive and pioneering portfolio for its channel partners. The experts at ALSO Cyber Security will be happy to assist you.

## About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. This is Fortinet's comprehensive network security portfolio:



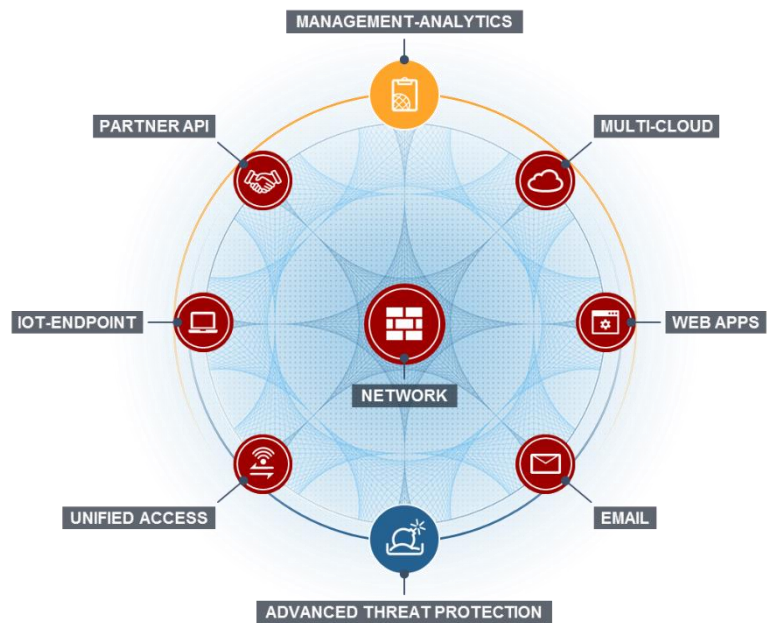
Source and ©: Fortinet Product Guide

## Security Fabric

The Fortinet Security Fabric delivers broad protection and visibility to every network segment, device, and appliance, whether virtual, in the cloud, or on-premises.

The Fortinet Security Fabric segments the entire network—from the Internet of Things (IoT) to the cloud—to provide superior protection against sophisticated threats:

- ▶ **Broad** visibility and protection across the digital attack surface. More than 25% of enterprise attacks are predicted to target IoT devices by 2020. And siloed apps in multi-cloud environments make it even harder to respond to threats. The Fortinet Security Fabric delivers real-time visibility across all devices and applications.
- ▶ **Integrated** detection and response to advanced threats. Enterprises average more than 30 point security products within their environments, resulting in multiple time-consuming security consoles and lack of transparency. The Fortinet Security Fabric streamlines communications among the different security solutions, shrinking detection and remediation windows.
- ▶ **Automated** operations and analytics via a single console. Sophisticated cyberattack technologies such as artificial intelligence (AI) and machine learning (ML) are reducing the time from intrusion to attack. This means enterprises need to detect threats faster. With Fortinet Security Fabric, you can coordinate automated responses and remediation to threats detected anywhere across your extended network.

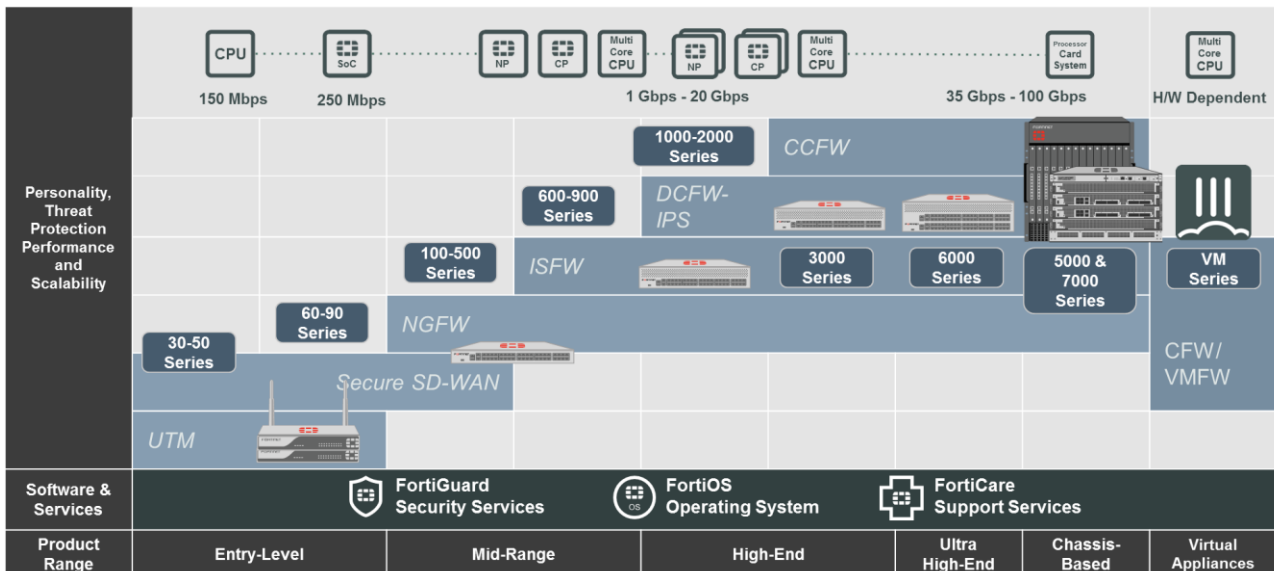


### The Fortinet Security Fabric Solution includes:

- ▶ **Network:** Fortinet high-performance **FortiGate** firewall provide consolidated advanced security and deep visibility that protects the network from known and unknown threats.
- ▶ **Multi-Cloud:** Fortinet's integrated virtual and physical cloud solutions protect all your dynamic cloud environments and SaaS applications.
- ▶ **Web Application:** The **FortiWeb** web application firewall uses the latest intelligence to protect web applications from sophisticated attacks.
- ▶ **Email:** The **FortiMail** secure email gateway inspects incoming and outgoing email, blocks malicious messages, and prevents sensitive information from being leaked.
- ▶ **Advanced Threat Protection:** Fortinet **FortiSandbox** solutions isolate and inspect any suspicious files detected by security tools.
- ▶ **Secure Unified Access:** Fortinet's Secure Unified Access solution extends network protection from the FortiGate to every corner of your network with integrated management and visibility for **switches** and **access points**.
- ▶ **Endpoint:** **FortiClient** adds another layer of automated security for better overall network protection.
- ▶ **Management and Analytics:** Fortinet solutions for logging (**FortiAnalyzer**) and reporting (**FortiManager**), SIEM (**FortiSIEM**), and centralized security management pull data from your Fortinet and Fabric-Ready security products, giving you the visibility to efficiently manage security processes and automate responses.

## FortiGate Security Appliances

Fortinet sells a wide range of FortiGate products, which include Unified Threat Management (UTM) and Next Generation Firewall (NGFW) appliances as well as cloud and services provider based virtual appliances.



Source and ©: Fortinet Product Guide

- ▶ **Entry-level** FortiGate UTM appliances are designed for small and remote offices (30-90 desktop model Series and 100 (rack mountable) Series).
- ▶ **Mid-range** products include the 100-500 Series for branch offices and midsize organizations, and the 600-900 Series for enterprise campuses.
- ▶ **High-end** FortiGate 1000-3000 Series are designed for data centers and multi-tenant cloud environments.
- ▶ **Ultra-High-End** FortiGate 6000 Series and chassis based 5000 and 7000 Series are designed to data centers and Telco environment.

## FortiGate Licensing

Fortinet licenses security features, called **FortiGuard Services**, on a per-device basis and not per IP address or users. The services can be licensed as single subscription (called “a la carte”) or as Security Bundle.

The FortiGate FortiGuard Services are available as “a la Carte” or software bundle with or without hardware<sup>1</sup>:

<b>Hardware (FortiGate)</b>	Hardware only - FortiGate-60E, FortiGate 500E, FortiGate-1200D, etc.
<b>Service(s) (FortiGuard)</b>	FortiGuard AV service, - Intrusion Prevention, AntiVirus, Web Filtering, etc
<b>Support (FortiCare)</b>	24x7 FortiCare (NBD RMA) 8x5 FortiCare (return & replace RMA) 360° FortiCare Contract (same as 24x7 with health care services) PRMA addon contract (NDD, 4 h courier or onsite engineer)
<b>Services Protection Package</b>	FortiCare + FortiGuard Packages FortiGuard only Packages
<b>Hardware + Services Bundle</b>	Hardware + FortiCare + FortiGuard Package Bundles - Typical initial order with 1, 3 or 5 years term

<sup>1</sup> FortiGate FortiGuard Services as of August 6, 2018 with FortiOS 6.0.1 and higher

## FortiCare Support Services

**Support  
(FortiCare)**

Product	SKU	Description
FortiGate-100E	FC-10-FG1HE-311-02-DD	8x5 FortiCare Contract
	FC-10-FG1HE-247-02-DD	24x7 FortiCare Contract
	FC-10-FG1HE-280-02-DD	FortiCare 360 Contract (24x7 FortiCare plus Advanced Support ticket handling & Health Check Monthly Reports; Collector included with Setup & Administration)
	FC-10-FG1HE-210-02-DD	Next Day Delivery Premium RMA Service (Add-On to 24x7 FC)
	FC-10-FG1HE-211-02-DD	4-Hour Hardware Delivery Premium RMA Service (Add-On to 24x7 FC)
	FC-10-FG1HE-212-02-DD	4-Hour Hardware and Onsite Engineer Premium RMA Service (Add-On)
	FC-10-FG1HE-301-02-DD	Secure RMA Service (Add-On to 24x7 FC)

[DD = 12 | 36 | 60 month]

Note: Premium RMA and Secure RMA are add-on services to existing 24x7 FortiCare service. See chapter "FortiCare Maintenance & Support Services" for more information about FortiCare Services

## FortiGuard Security Services for FortiGate

	FortiGuard Security Rating Service				✓
	FortiCASB Connector				✓
	FortiGuard Industrial Security Services				✓
	FortiGuard Web Filtering Service			✓	✓
	FortiGuard AntiSPAM Service			✓	✓
	FortiGuard IPS Service		✓	✓	✓
	FortiGuard Antivirus Service incl. BOTnet/IP Domain and Mobile Security	✓	✓	✓	✓
	Virus Outbreak Service (VOS) + Content Disarm and Reconstruction (CDR)	✓	✓	✓	✓
	FortiSandbox Cloud Service	✓	✓	✓	✓
	FortiGuard Application Control Service	✓	✓	✓	✓
	FortiCare Support & HW + SW Maintenance		✓ 24x7 only	✓ 24x7 / 8x5	✓ 360 / 24x7 / 8x5
	Protection Service Package	Advanced Malware Protection (AMP)	Advanced Threat Protection (ATP)	Unified Protection (UTM)	Enterprise Protection (ENT)
All services as of Q4'18. FortiOS 6.0.1+ is required. AMP is a FortiGuard Service bundle only without FortiCare				Available as bundle with Hardware	

- ▶ **AMP** FortiGuard Malware service bundle: Antivirus, VOS, CDR and Sandbox Cloud without FortiCare
- ▶ **ATP** FortiGuard + FortiCare bundle: AMP + IPS & 24x7 FortiCare
- ▶ **UTM** most sold FortiGuard + FortiCare bundle: ATP + AntiSpam + WebFilter & 24x7 or 8x5 FortiCare
- ▶ **ENT** FortiGuard + FortiCare bundle for Enterprises: UTM + CASB + Security Rating & 24x7 or 8x5 FC

Note: FortiGuard Application Control is part of the FOS and requires FortiCare to receive signature updates.

## A la Carte FortiGuard Services

### A la Carte Service (FortiGuard)

Product	SKU	Description
FortiGate-100E	FC-10-FG1HE-131-02-DD	FortiCloud Management, Analysis and 1 Year Log Retention
	FC-10-FG1HE-185-02-DD	FortiCASB SaaS-only Service, Includes 35 users
	FC-10-FG1HE-100-02-DD	FortiGuard Advanced Malware Protection (AMP) including Antivirus, Mobile Malware and FortiSandbox Cloud Service
	FC-10-FG1HE-108-02-DD	FortiGuard IPS Service
	FC-10-FG1HE-112-02-DD	FortiGuard Web Filtering Service
	FC-10-FG1HE-159-02-DD	FortiGuard Industrial Security Service
	FC-10-FG1HE-175-02-DD	FortiGuard Security Rating Service
	FC-10-FG1HE-189-02-DD	FortiConverter Service for one time configuration conversion service

[DD = 12 month]

## Protection Service Packages a.k.a Bundles

**Support  
(FortiCare)**

**A la Carte Service(s)  
(FortiGuard)**

**Services Protection Package**

Product	SKU	Description
FortiGate-100E	FC-10-FG1HE-928-02-DD	Advanced Threat Protection (24x7 FortiCare plus Application Control, IPS, AV and FortiSandbox Cloud)
	FC-10-FG1HE-900-02-DD	Unified (UTM) Protection (8x5 FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud)
	FC-10-FG1HE-950-02-DD	Unified (UTM) Protection (24x7 FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud)
	FC-10-FG1HE-874-02-DD	Enterprise Protection (8x5 FortiCare plus Application Control, IPS, AV, Web Filtering, Antispam, FortiSandbox Cloud, FortiCASB, Industrial Security and Security Rating)
	FC-10-FG1HE-980-02-DD	Enterprise Protection (24x7 FortiCare plus Application Control, IPS, AV, Web Filtering, Antispam, FortiSandbox Cloud, FortiCASB, Industrial Security and Security Rating)
	FC-10-FG1HE-100-02-DD	FortiGuard Advanced Malware Protection (AMP) including Antivirus, Mobile Malware and FortiSandbox Cloud Service

## Hardware and Software Bundles

Hardware  
(FortiGate)

Support  
(FortiCare)

A la carte Service(s)  
(FortiGuard)

**Services Protection Package**

Hardware + Services Bundle

- Hardware
- HW + Services Bundle
- FortiGuard Service(s)
- Services Package
- Support

Product	SKU	Description
FortiGate-100E	FG-100E-BDL	Hardware plus 1 year 8x5 FortiCare and FortiGuard Unified Protection (UTM) (original standard hardware + services bundle)
Multi-year	FG-100E-BDL-900-DD	Hardware plus 8x5 FortiCare and FortiGuard Unified Protection (UTM) [DD = 36   60 month]
24x7 variant	FG-100E-BDL-950-DD	Hardware plus 24x7 FortiCare and FortiGuard Unified Protection (UTM) [DD = 12   36   60 month]
Multi-year	FG-100E-BDL-871-DD	Hardware plus 8x5 FortiCare and FortiGuard Enterprise Protection (ENT) [DD = 12   36   60 month]
24x7 variant	FG-100E-BDL-974-DD	Hardware plus 24x7 FortiCare and FortiGuard Enterprise Protection (ENT) [DD = 12   36   60 month]

## Licensing Matrix

	FortiCare Services							FortiGuard Services														
<b>FortiGuard Protection Package with/without FortiCare</b>																						
Enterprise Protection (ENT) + FortiCare (8x5) or [24x7 or 360]	[o]	[o]	[o]	o	o	[o]	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
Unified Protection (UTM) + FortiCare (8x5) or [24x7]	[o]	[o]	[o]	o	o	[o]	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
Adv. Threat Protection (ATP) + FortiCare [24x7]		[o]		[o]	[o]	[o]	o	o	o													
Advanced Malware Protection (AMP)							o															
<b>FortiCare Services</b>																						
FortiCare (8x5) / [24x7 or 360]	[o]	[o]		o	o	[o]	o															
Premium-RMA 4h courier / 4h onsite engineer / Next Day Delivery			o				add-on to existing 24x7 FortiCare															
FortiCare 360 Contract (Advanced Services Technical Support)		[o]		o	o	[o]	o															
<b>Individual Service (A la Carte)</b>																						
Advanced Malware Protection (AV, FortiSandbox Cloud + VOS + CDR)							o															
FortiGuard IPS Service									o													
FortiGuard Web Filtering Service										o												
FortiGuard Industrial Security																	o					
FortiGuard Security Rating Service																				o		
FortiGuard CASB Service																					o	
FortiConverter Service for one time configuration conversion service																						
FortiCloud Management, Analysis and 1 Year Log Retention																						



## FortiMail - Secure Email Gateway

FortiMail is a top-rated secure email gateway that stops volume-based and targeted cyber threats to help secure the dynamic enterprise attack surface, prevents the loss of sensitive data and helps maintain compliance with regulations. High performance physical and virtual appliances deploy on-site or in the public cloud to serve any size organization — from small businesses to carriers, service providers, and large enterprises.

### Form Factors

FortiMail is available in many different high performance, low administration form factors with many different options to choose. This ensures that, large or small, FortiMail can fit seamlessly in to your exact on-premise or cloud environment.

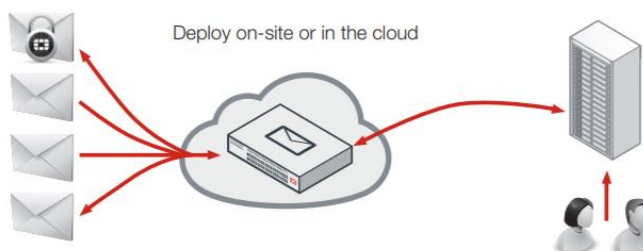
- ▶ **Hardware:** Scales from SMB to provider type installation.
- ▶ **Virtual Appliance:** Virtualized appliance running on VMWare, Hyper-V, KVM Citrix XenServer or as private cloud on Microsoft Azure an Amazon Web Services.
- ▶ **SaaS:** Cloud based offering from Fortinet to run FortiMail in Gateway or Server mode with standard or Premium services. SaaS is licensed per user (mailbox) / year.

### Deployment Modes

Choose from three modes of deployment — Transparent, Gateway, or Server mode – to meet your specific email security requirements, while minimizing infrastructure changes and service disruptions.

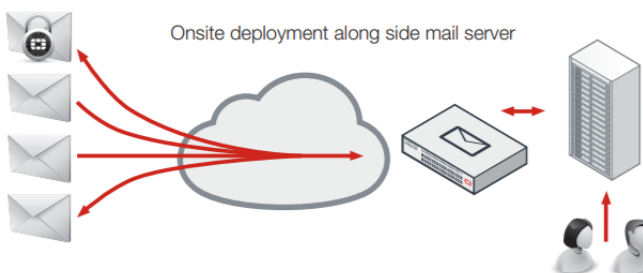
#### ▶ Gateway Mode:

Provides inbound and outbound proxy mail transfer agent (MTA) services for existing email gateways. A simple DNS MX record change redirects email to FortiMail for antispam and antivirus scanning. The FortiMail device receives messages, scans for viruses and spam, then relays email to its destination email server for delivery



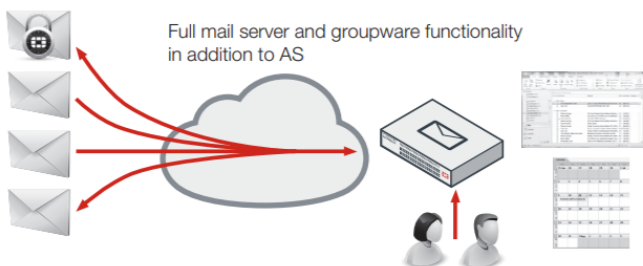
#### ▶ Transparent Mode:

Each network interface includes a proxy that receives and relays email. Each proxy can intercept SMTP sessions even though the destination IP address is not the FortiMail appliance. FortiMail scans for viruses and spam, then transmits email to the destination email server for delivery. This eliminates the need to change the DNS MX record, or to change the existing email server network configuration.



#### ▶ Server Mode:




The FortiMail device acts as a standalone messaging server with full SMTP email server functionality, including flexible support for secure POP3, IMAP and WebMail access. FortiMail scans email for viruses and spam before delivery. As in Server mode, external MTAs connect to FortiMail, allowing it to function as a protected server.



## FortiGuard Security Services for FortiMail

All form factors leverage the same world-class security services from FortiGuard Labs. These include traditional components like the antispam and antivirus service as well as newer protections.





### ► Base Bundle

 <p><b>Antispam Service</b></p> <ul style="list-style-type: none"> <li>• Sender IP ratings</li> <li>• Embedded URL ratings</li> <li>• Content-based hashes for spam and phishing campaigns</li> <li>• Separate "newsletter" identifiers</li> </ul>	 <p><b>Antivirus Service</b></p> <ul style="list-style-type: none"> <li>• One-to-many signatures</li> <li>• Heuristic rules</li> <li>• Emulation</li> <li>• Decrypting/Unpacking</li> <li>• Patented content pattern recognition language (CPRL)</li> </ul>	 <p><b>Outbreak Prevention</b></p> <ul style="list-style-type: none"> <li>• Pre-signature intelligence</li> <li>• Covers emerging spam and malware campaigns</li> <li>• Leverages new sandbox and other intelligence</li> </ul>
---	--	--

- **Outbreak Prevention**, which enables a real-time query back to the labs to check for the very latest intelligence ahead of schedule engine updates

While the outbreak prevention is part of our base FortiMail Bundle, the latest protections are available in our Enterprise ATP offering.

### ► Enterprise ATP Bundle

 <p><b>FortiSandbox Cloud</b></p> <ul style="list-style-type: none"> <li>• FortiSandbox hosted by Fortinet</li> <li>• Includes prefiltering, emulation and full instrumented analysis</li> <li>• Subscription-based</li> <li>• No separate sandbox required</li> </ul>	 <p><b>Content Disarm and Reconstruction</b></p> <ul style="list-style-type: none"> <li>• Removes high risk active content</li> <li>• Supports Microsoft Office and Adobe</li> <li>• Can be applied by user, group or policy</li> <li>• Original documents can be retained and restored</li> </ul>	 <p><b>Click Protect</b></p> <ul style="list-style-type: none"> <li>• Dynamic reputation query</li> <li>• Determines rating at the time of user click</li> <li>• Identifies recently compromised sites changed shortly after campaigns are launched</li> </ul>	 <p><b>Impersonation Analysis</b></p> <ul style="list-style-type: none"> <li>• Identifies spoofed email</li> <li>• Dynamically builds protections for common email addresses</li> <li>• Complements sender authentication</li> </ul>
---	---	---	--

- **Click Protect**: which dynamically checks the very latest ratings of sites at time of end user click
- **Content Disarm and Reconstruction**, allowing the removal of embedded malicious content that can pose a risk to unwary users
- **Sandbox Analysis**, that automatically and security runs attachments and connects to URLs, to assess the runtime behavior of files and links; and
- **Impersonation Analysis**, which dynamically tracks the source characteristics of trusted senders and looks for anomalies in terms of sources with different characteristics purporting to be those same senders

## FortiMail Order Information

Product	SKU	Description
FortiMail 60D	FML-60D	Email Security Appliance — 4x GE RJ45 ports, 500 GB storage.
FortiMail 200E	FML-200E	Email Security Appliance — 4x GE RJ45 ports, 1 TB storage.
FortiMail 400E	FML-400E	Email Security Appliance — 4x GE RJ45 ports, 2 TB storage.
FortiMail 1000D	FML-1000D	Email Security Appliance — 6x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage.
FortiMail 2000E	FML-2000E	Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage.
FortiMail 3000E	FML-3000E	Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage.
FortiMail 3200E	FML-3200E	Email Security Appliance — 4x GE RJ45 ports, 2x 10 GE SFP+ slots, 2x GE SFP slots, dual AC power supplies, 4 TB default storage.
FortiMail VM00	FML-VM00	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 1x vCPU core.
FortiMail VM01	FML-VM01	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 1x vCPU core.
FortiMail VM02	FML-VM02	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 2x vCPU cores.
FortiMail VM04	FML-VM04	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 4x vCPU cores.
FortiMail VM08	FML-VM08	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 8x vCPU cores.
FortiMail VM16	FML-VM16	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 16x vCPU cores.
FortiMail VM32	FML-VM32	FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 32x vCPU cores.

The following licensing is based on a sample FortiMail hardware and virtual appliance.

Product	SKU	Description
FortiMail-60D	FML-60D	Email Security Appliance - 4 x GE RJ45 ports, 500GB Storage
	FML-60D-BDL-640-DD	Hardware plus 24x7 FortiCare and <b>FortiGuard Base Bundle</b>
	FML-60D-BDL-641-DD	Hardware plus 24x7 FortiCare and <b>FortiGuard Enterprise ATP Bundle</b>
	FC-10-FE060-640-02-DD	24x7 FortiCare and FortiGuard Base Bundle Contract
	FC-10-FE060-641-02-DD	24x7 FortiCare and FortiGuard Enterprise ATP Bundle Contract
	FC-10-FE060-123-02-DD	FortiSandbox Cloud Service
	FC-10-FE060-150-02-DD	FortiGuard Virus Outbreak Protection Service
	FC-10-FE060-160-02-DD	Dynamic Adult Image Analysis Service
	FC-10-FE060-311-02-DD	8x5 FortiCare Contract
	FC-10-FE060-247-02-DD	24x7 FortiCare Contract
FortiMail-VM01	FML-VM01	FortiMail-VM virtual appliance for all supported platforms. 1 x vCPU cores
	FC-10-0VM01-642-02-DD	24x7 FortiCare and FortiGuard <b>Base Bundle Contract</b>
	FC-10-0VM01-643-02-DD	24x7 FortiCare and FortiGuard <b>Enterprise ATP Bundle Contract</b>
	FC-10-0VM01-100-02-DD	FortiGuard AV Services
	FC-10-0VM01-114-02-DD	FortiGuard AS Service
	FC-10-0VM01-123-02-DD	FortiSandbox Cloud Service
	FC-10-0VM01-150-02-DD	FortiGuard Virus Outbreak Protection Service
	FC-10-0VM01-160-02-DD	Dynamic Adult Image Analysis Service
	FC-10-0VM01-851-02-DD	8x5 FortiCare Contract
	FC-10-0VM01-248-02-DD	24x7 FortiCare Contract

[DD = 12 | 36 | 60 month]

## Resources

► [FortiMail Datasheet](#)

## FortiMail Cloud - Secure Email as a Service (SaaS)

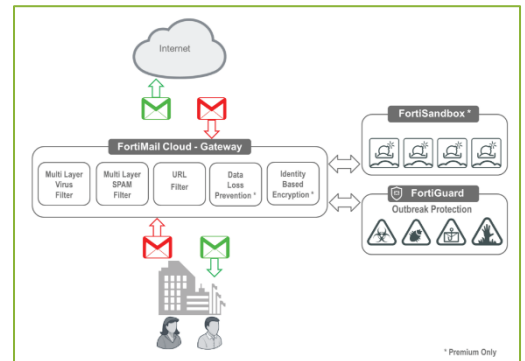
FortiMail Cloud Email Security is an independently validated and top-rated Secure Email Gateway solution delivering >99.5% spam detection rate, multiple layers of malware detection and an extremely low false positive rate. It includes analyst recommended Advanced Threat Defense Capabilities as well as a full complement of data protection features. Fully managed by Fortinet, FortiMail Cloud Email Security allows you to focus on your business by relying on a trusted security expert to manage this key infrastructure security component.

### FortiMail Cloud — Gateway

The FortiMail Cloud — Gateway service provides cloud-based email security for customers with either on-premise or third-party hosted email deployments. The service acts as an inbound and outbound gateway for customer email and cleans it of spam and malware before forwarding to its destination.

### FortiGuard Security Services for FortiMail

The Premium Service includes the same features as with Enterprise Bundle on the FortiMail appliance (Virus Outbreak Service, Content Disarm and Reconstruction, URL Click Protection, Impersonation Analysis, Cloud Sandboxing, Identity-Based Encryption (IBE), Data Leak Prevention).



### FortiMail Ordering Information

FortiMail Cloud is licensed per mailbox / year. The recommended licensing is Gateway.

FortiMail Cloud		
FortiMail Cloud — Server	FC-10-OVMO1-416-02-DD	FortiMail Cloud — Server (25–100 Mailboxes)
	FC-10-OVMO4-416-02-DD	FortiMail Cloud — Server (101–1,000 Mailboxes)
	FC-10-OVMO1-417-02-DD	FortiMail Cloud — Server Premium (25–100 Mailboxes)
FortiMail Cloud — Gateway	FC-10-OVMO4-417-02-DD	FortiMail Cloud — Server Premium (101–1,000 Mailboxes)
	FC-10-OVMO1-414-02-DD	FortiMail Cloud — Gateway (25–100 Mailboxes)
	FC-10-OVMO2-414-02-DD	FortiMail Cloud — Gateway (101–1,000 Mailboxes)
FortiMail Cloud — Gateway MSSP	FC-10-OVMO4-414-02-DD	FortiMail Cloud — Gateway (1,001–5,000 Mailboxes)
	FC-10-OVMO8-414-02-DD	FortiMail Cloud — Gateway (5,001–10,000 Mailboxes)
	FC-10-OVM16-414-02-DD	FortiMail Cloud — Gateway (10,000+ Mailboxes)
	FC-10-OVMO1-415-02-DD	FortiMail Cloud — Gateway Premium (25–100 Mailboxes)
	FC-10-OVMO2-415-02-DD	FortiMail Cloud — Gateway Premium (101–1,000 Mailboxes)
	FC-10-OVMO4-415-02-DD	FortiMail Cloud — Gateway Premium (1,001–5,000 Mailboxes)
	FC-10-OVMO8-415-02-DD	FortiMail Cloud — Gateway Premium (5,001–10,000 Mailboxes)
	FC-10-OVM16-415-02-DD	FortiMail Cloud — Gateway Premium (10,000+ Mailboxes)
	FC1-10-EVMSP-415-02-DD	FortiMail Cloud — Gateway Premium for MSSP (500–1,000 Mailboxes)
	FC3-10-EVMSP-415-02-DD	FortiMail Cloud — Gateway Premium for MSSP (10,000+ Mailboxes)

[DD = 12 | 36 | 60 month]

### Resources

- ▶ [FortiMail Cloud Datasheet](#)

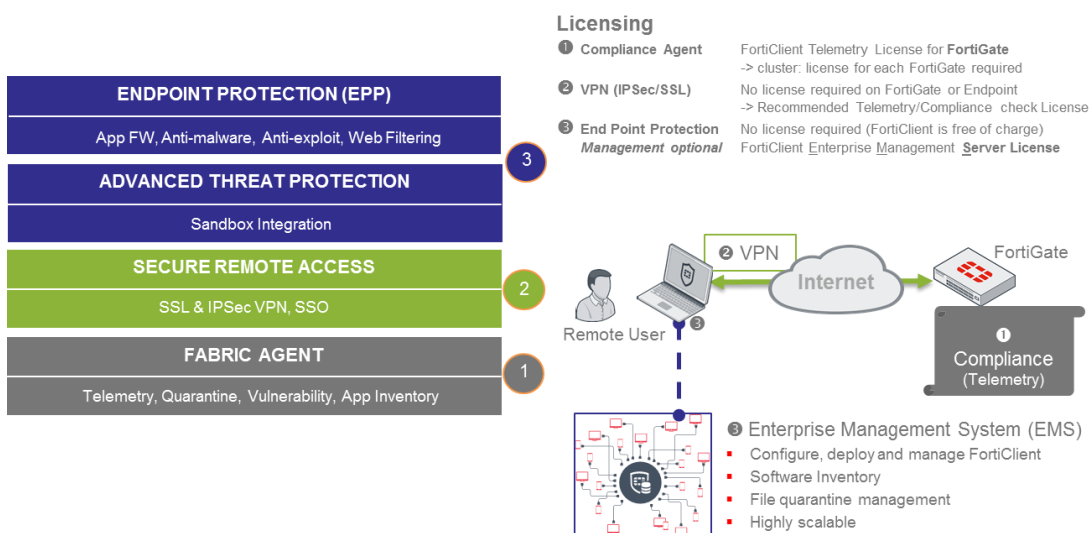
## FortiClient - End-Point Protection

As a key piece of the Fortinet Security Fabric, FortiClient integrates endpoints into the fabric for early detection and prevention of advanced threats. Security events including zero-day malware, botnet detections, and vulnerabilities are reported in real-time. FortiClient integrates with many key components of the Fortinet Security Fabric (FortiGate, FortiSandbox, etc.) and is centrally managed by the **Enterprise Management Server (EMS)**.

### FortiClient Key Modules

- ▶ **Fabric Agent for Security Fabric connectivity**
  - **Endpoint telemetry for visibility:** FortiClient shares endpoint telemetry with the Security Fabric to ensure unified endpoint awareness and deliver integrated endpoint and network security. Endpoint information shared includes device information, OS, security status, vulnerabilities, events, and user ID.
- ▶ **Endpoint security modules**
  - **Anti-malware:** Anti-malware leverages FortiGuard Content Pattern Recognition Language (CPRL), machine learning, and AI to protect endpoint against malware. The pattern-based CPRL is highly effective in detecting and blocking polymorphic malware. It also blocks attack channels and malicious websites.
  - **Anti-exploit:** Protects against advanced threats exploiting zero-day and unpatched vulnerabilities. This signature-less and behavioral-based technology detects and blocks memory violation techniques. It shields web browsers, java/flash plug-ins, office applications, PDF readers, load library, and script interpreters from exploit-based attacks.
  - **Web filtering:** Powered by FortiGuard research, the web filtering function monitors all web browser activities to enforce web security and acceptable usage policy with 75+ categories. It works across all supported operating systems and works with Google SafeSearch. Admins can set black/white lists, on-/off-net policies, and import FortiGate web filtering policies for consistent enforcement.
  - **Application firewall:** Provides the ability to monitor, allow, or block application traffic by categories. It uses the same categories as FortiGate, enabling consistent application traffic control. It leverages FortiGuard anti-botnet, IPS, and application control intelligence and can prevent the use of unwanted applications including proxy apps and HTTPS messaging apps.
- ▶ **Secure remote access modules**
  - **VPN:** FortiClient uses SSL and IPsec VPN to provide secure and reliable access to the corporate network. Two-factor authentication can also be leveraged for additional security. Features such as always-on, auto-connect, dynamic VPN gateway selection and split-tunneling, result in optimized user experience and security.
  - **Single sign-on:** It integrates with FortiAuthenticator identity and access management service to provide single sign-on.

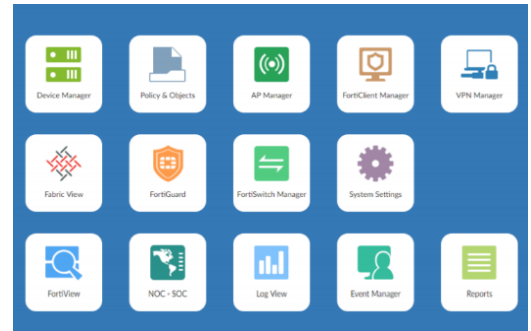
### FortiClient Licensing



## FortiManager - Centralized Security Management

FortiManager provides a single-pane-of-glass to manage Fortinet's security and networking devices. Easily control the deployment of security policies, FortiGuard content security updates, firmware revisions, and individual configurations for thousands of Fortinet devices. In this demo, see how devices are registered, how policies and objects (along with policy packages) can be enacted, and how devices can be configured and updated easily.

Multitenancy support is provided via ADOM (Administrative Domain).



### Form Factors

FortiManager is available in many different form factors:

- ▶ **Hardware Appliance:** Scales from SMB to provider type installation.
- ▶ **Virtual Appliance:** Virtualized appliance running on VMware ESX, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM on Redhat and Ubuntu, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure.
- ▶ **Cloud:** FortiManager for AWS, FortiManager for Azure

### FortiManager VM Licensing

Fortinet offers the FortiManager VM in a stackable license model. This model allows you to expand your VM solution as your environment expands. Utilizing virtualization technology, FortiManager-VM is a software-based version of the FortiManager hardware appliance and is designed to run on many virtualization platforms. It offers all the features of the FortiManager hardware appliance.

The FortiManager virtual appliance family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns that can be used to fine tune the security policy, thwarting future attackers.

### FortiManager Order Information

PRODUCT	SKU	DESCRIPTION
FortiManager	FMG-200F	Centralized management, log and analysis appliance — 2xRJ45 GE, 2xSFP, 8 TB storage, up to 30x Fortinet devices/virtual domains.
	FMG-300F	Centralized management, log and analysis appliance — 4x GE RJ45, 2xSFP, 16 TB storage, up to 100x Fortinet devices/virtual domains.
	FMG-400E	Centralized management, log and analysis appliance — 2x GE RJ45, 24 TB storage, up to 300x Fortinet devices/virtual domains.
	FMG-2000E	Centralized management, log and analysis appliance — 4x GE RJ45, 2x 10 GE SFP+ slots, 36 TB storage, dual power supplies, manages up to 1,200 Fortinet devices/virtual domains.
	FMG-3000F	Centralized management, log and analysis appliance — 4x GE RJ45, 2x 10 GE SFP+ slots, 48 TB storage, dual power supplies, manages up to 4,000 Fortinet devices/virtual domains.
FortiManager Device Upgrade	FMG-DEV-100-UG	FortiManager device upgrade license for adding 100 Fortinet devices/VDOMs (3000 series and above - hardware only)
FortiManager VM	Built-in Evaluation	Built-in 15-day EVAL license, no activation required.
	Full Evaluation (60-days)	EVAL license. License and activation required.
	FMG-VM-Base	Base license for stackable FortiManager-VM. Manages up to 10 Fortinet devices/Virtual Domains, 1 GB/Day of Logs and 100 GB storage capacity. Designed for all supported platforms.
	FMG-VM-10-UG	Upgrade license for adding 10 Fortinet devices/Virtual Domains; allows for total of 2 GB/Day of Logs and 200 GB storage capacity.
	FMG-VM-100-UG	Upgrade license for adding 100 Fortinet devices/Virtual Domains; allows for total of 5 GB/Day of Logs and 1 TB storage capacity.
	FMG-VM-1000-UG	Upgrade license for adding 1,000 Fortinet devices/Virtual Domains; allows for total of 10 GB/Day of Logs and 4 TB storage capacity.
	FMG-VM-5000-UG	Upgrade license for adding 5,000 Fortinet devices/Virtual Domains; allows for total of 25 GB/Day of Logs and 8 TB storage capacity.
	FMG-VM-10K-UG	Upgrade license for adding 10,000 Fortinet devices/Virtual Domains by default, with capacity to increase with add-on license. Allows for total of 50 GB/Day of Logs and 16 TB storage capacity.
Additional FortiManager Items	FC-10-FNDN1-139-02-12	1 Year Subscription Renewal for 1 User to Fortinet Developer Network
	FC-10-FNDN2-139-02-12	1 Year Subscription for Unlimited Users to Fortinet Developer Network
	FMG-SDNS	License to operate FortiManager as a dedicated Secure DNS server appliance (3000 series and above – hardware only)

## FortiAnalyzer - Centralized Security Analysis

FortiAnalyzer is the NOC-SOC security analysis tool built with operations perspective. FortiAnalyzer offers centralized network security logging and reporting for the Fortinet Security Fabric.

FortiAnalyzer provides real-time alerts that expedite the discovery, investigation, and response to events even as they're happening. With consolidated action oriented views and deep drill-down capabilities. It also provides real-time threat intelligence and actionable analytics via global IOC feeds check for emerging and recent threats throughout the organization.

### Form Factors

FortiAnalyzer is available in many different form factors:

- ▶ **Hardware Appliance:** Scales from SMB to provider type installation.
- ▶ **Virtual Appliance:** Virtualized appliance running on VMware ESX, Microsoft Hyper-V, Citrix XenServer and Open Source, Xen, KVM on Redhat and Ubuntu, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI)
- ▶ **Cloud:** FortiAnalyzer for AWS, FortiAnalyzer for Azure

### Incident Response (IOC – Indicator of Compromise)

FortiAnalyzer's Incident Response capability improves Management & Analytics with focus on event management and identification of compromised endpoints. Use improved default and custom event handlers to detect malicious and suspicious activities on the spot. Integration of events with the FOS automation framework for automated endpoint quarantine. Incident detection and tracking, as well as evidence collection and analysis are streamlined through integration with ITSM platforms, helping to bridge gaps in your Security Operations Center and reinforce your Security Posture

### FortiAnalyzer VM Licensing

Fortinet offers the FortiAnalyzer VM in a stackable license model. The log capacity can be upgraded allowing you to expand your VM solution as your environment expands.

### FortiAnalyzer Order Information

PRODUCT	SKU	DESCRIPTION
FortiAnalyzer 200F	FAZ-200F	Centralized log and analysis appliance — 2xRJ45 GE, 4 TB storage, up to 100 GB/day of logs.
FortiAnalyzer 300F	FAZ-300F	Centralized log and analysis appliance — 2xRJ45 GE, 8 TB storage, up to 150 GB/day of logs.
FortiAnalyzer 400E	FAZ-400E	Centralized log and analysis appliance — 4x GE RJ45, 12 TB storage, up to 200 GB/day of logs.
FortiAnalyzer 800F	FAZ-800F	Centralized log and analysis appliance — 4 x GE, 2x SFP, 16 TB storage, up to 300 GB/day of logs.
FortiAnalyzer 1000E	FAZ-1000E	Centralized log and analysis appliance — 2x GE RJ45, 24 TB storage, dual power supplies, up to 650 GB/day of logs.
FortiAnalyzer 2000E	FAZ-2000E	Centralized log and analysis appliance — 4x GE RJ45, 2 x SFP+, 36 TB storage, dual power supplies, up to 1,000 GB/day of logs.
FortiAnalyzer 3000F	FAZ-3000F	Centralized log and analysis appliance — 4x GE RJ45, 2 x SFP+, 48 TB storage, dual power supplies, up to 3,000 GB/day of logs.
FortiAnalyzer 3700F	FAZ-3700F	Centralized log and analysis appliance — 2x SFP+, 2x1GE slots, 240 TB storage, up to 8,300 GB/day of logs.
FortiAnalyzer VM	FAZ-VM-BASE	Base license for stackable FortiAnalyzer-VM; 1 GB/Day of Logs and 500 GB storage capacity. Unlimited GB/Day when used in collector mode only. Designed for all supported platforms.
	FAZ-VM-GB1	Upgrade license for adding 1 GB/Day of Logs and 500 GB storage capacity.
	FAZ-VM-GB5	Upgrade license for adding 5 GB/day of logs and 3 TB storage capacity.
	FAZ-VM-GB25	Upgrade license for adding 25 GB/day of logs and 10 TB storage capacity.
	FAZ-VM-GB100	Upgrade license for adding 100 GB/day of logs and 24 TB storage capacity.
	FAZ-VM-GB500	Upgrade license for adding 500 GB/day of logs and 48 TB storage capacity.
	FAZ-VM-GB2000	Upgrade license for adding 2 TB/Day of Logs and 100 TB storage capacity.
	FortiAnalyzer AWS On-Demand	<a href="https://aws.amazon.com/marketplace/pp/B01N5K7210/ref=portal_asin_url">https://aws.amazon.com/marketplace/pp/B01N5K7210/ref=portal_asin_url</a>
	FortiAnalyzer Azure On-Demand	<a href="https://azuremarketplace.microsoft.com/en-us/marketplace/apps/fortinet.fortianalyzer">https://azuremarketplace.microsoft.com/en-us/marketplace/apps/fortinet.fortianalyzer</a>
FortiAnalyzer Add-on Management Capabilities	FAZ-MGMT20	License to add FortiManager capabilities for up to 20 devices (1000 series and above — hardware only).
FortiGuard Indicator of Compromise (IOC) Subscription	FC-10-[Model code] -149-02-DD	1 Year Subscription license for the FortiGuard Indicator of Compromise (IOC).

## FortiCare Maintenance & Support Services (Ticket)

Fortinet offers several hardware replacement (RMA) options that are bundled with a FortiCare maintenance contract. The following information provides a quick overview.

FortiCare Support Services subscriptions provide global support on a per product basis for 1, 3 or 5 years – PRMA only on a 1-year base.

FortiCare Service Level	Service Description and SLA	Hardware RMA SLA
FortiCare 8x5	Hardware Coverage + Firmware Update + 8x5 Email & Web Support	Return & Replace
FortiCare 24x7	Hardware Coverage + Firmware Update + 24x7 Email, Web & Telephone Support	Next Business Day advanced replacement from local Swiss RMA depot (@ ALSO Switzerland)
FortiCare 360	Same as 24x7 FortiCare + Advanced Services Technical Support. Combines elements of FortiSIEM analytics with premium support to enable organizations to take a more proactive approach to the rapid detection and remediation of current and potential performance issues associated with their FortiGate and FortiWifi devices to minimize down time	Next Business Day advanced shipment from local Swiss RMA depot (@ ALSO Switzerland)
Premium RMA Next Day Delivery (NDD)	<i>Add-On to existing 24x7 FortiCare</i>	Next Day Delivery (any day)
Premium RMA 24x7 4 hours Courier	<i>Add-On to existing 24x7 FortiCare</i>	4 hours courier (delivery only)
Premium RMA 24x7 4 hours Onsite	<i>Add-On to existing 24x7 FortiCare</i>	4 hours with Systems Engineer

**Note:** Standard RMA: SLA after acceptance of RMA ticket by Fortinet (local TAC time approx. 15:00).  
Premium RMA: Customer must **call** to open a high priority ticket. SLA after acceptance by Fortinet.  
New as of November 1st, 2018 the **Premium RMA service is an add-on to an existing 24x7 FortiCare** and no longer available as PRMA bundle.

## FortiCare Hardware Support Definitions (RMA)

There are basically three levels of hardware replacement available for purchase. For more information on these service levels refer to the appropriate service description.

Service Level	Description
<b>Return &amp; Replace</b>	After Fortinet provides confirmation of a defect, the customer ships the defective hardware at their expense to the depot indicated in the RMA (Return Merchandise Authorization) 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.
<b>Adv. Replacement</b>	Fortinet ships a replacement to arrive 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 thirty days following receipt of the replacement, beyond that time, Fortinet reserves the right to invoice for product
<b>Premium RMA</b>	For customers with critical environments higher levels of service are available within the Premium RMA (PRMA) portfolio. These levels are: <b>Next-day Delivery:</b> Parts delivered the day following RMA approval by Fortinet support <b>4-Hour Courier:</b> Parts delivered on-site 24 hours a day, 7 days a week within 4 hours of RMA approval by Fortinet support. <b>4-Hour On-site Engineer:</b> Parts delivered on-site with an engineer, 24 hours a day, 7 days a week within 4 hours of RMA approval by Fortinet support.
<b>Secure RMA</b>	Allows for <b>NON-Return</b> of an appliance for those customers with strict rules and requirements for physical data protection.

## Resources

- ▶ [FortiCare Services](#)
- ▶ [FortiGuard Security Services](#)
- ▶ [FortiCompanion to Technical Support, FortiCompanion to RMA Ticket, Ticket Creation Guide](#)
- ▶ [Hardware Lifecycle Policy](#)