ORDERING GUIDE

FortiAnalyzer

Available in

Appliance

Virtual

Cloud

As the Fortinet Security Fabric data lake, FortiAnalyzer consolidates vast datasets and simplifies the management of logs, incidents, and reporting, within a single console view. Integrating FortiAI's AI assistance and FortiGuard Labs' threat intelligence aids in rapid Detection, streamlined and remediation. FortiAnalyzer's security automation subscription delivers SIEM/SOAR lite capabilities enhanced by prebuilt content packs, including advanced correlation rules, playbooks, and more, maximizing threat response efficiency. Delivering a lightweight deployment with minimal configuration that provides AI-driven analytics and automated incident management, enabling organizations of all sizes to detect smarter, respond faster, and scale without disruption.

Key Values of FortiAnalyzer:

- **Unified Visibility and Management**: FortiAnalyzer's seamless NOC-SOC integration with FortiManager provides a unified view for operations, consolidates configurations, events, and alerts across the Security Fabric into a single console, simplifying log, analytics, and reporting management.
- **FortiAI Gen-AI Assistance**: Enhances analyst productivity with Gen-AI assistance embedded in the user interface, accelerating threat investigation and response times.
- **Advanced Threat Detection**: Provides automated detection alerts and downloads event handlers, correlation rules, and reports specific to each outbreak, ensuring proactive threat management.
- **Security Automation**: Delivers SIEM/SOAR lite functionalities with monthly updates of prebuilt content packs, including event handlers, playbooks, and connectors, automating security operations efficiently.
- **Future-Ready Scalability**: FortiAnalyzer's horizontal scalability ensures that as your organization grows, your security infrastructure evolves alongside, providing continuous protection without system overhauls.

The product offering includes:

- **FortiAnalyzer Appliance**: on-premise solution provides the best response times and detection technology with the full range of features and benefits.
- **FortiAnalyzer Perpetual VM**: virtual appliance offering supported across public and private clouds.
- **FortiAnalyzer VM Subscription**: subscription based offering of the VM model, that bundles support and services.
- **FortiAnalyzer Cloud**: subscription to cloud-based central logging & analytics.

This ordering guide provides a consolidated reference to the relevant FortiAnalyzer products and services available to your organization

	150G	300G	810G	1000G	3100G	3510G	3700G	4500G	FAZ-VM	BD-VM	CLOUD
GB/Day	**25**	**100**	**200**	**660**	**3,000**	**5,000**	**8,300**	**20TB**	**Stackable**	**Stackable**	**Stackable**
Sustained LPS	500	2,000	4,000	20,000	42,000	60,000	100,000	300,000		Stackable	
Collector Mode Sustained LPS	750	3,000	6,000	30,000	60,000	90,000	150,000				
No. Days @ Max Sustained LPS	90	50	50	60	30	35	60	30		Stackable	
Max Devices/VDOMs	50	180	800	2,000	4,000	10,000	10,000	10,000+	10,000	10,000	10,000
Max ADOMs	3	25	50	50	500	500	1,200	2,500	1,200	1,200	
Max ADOMs with add-on license					1,200	1,200	10,000				
Security Services											
Security Automation Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
FortiGuard Outbreak Detection Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
FortiGuard IOC Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
OT Security Service	7.4	7.4	7.4	7.4	7.4	7.4	7.4	7.4	7.4	7.4	
FortiAnalyzer Attack Surface Rating and Compliance	7.4	7.4	7.4	7.4	7.4	7.4	7.4	7.4	7.4	7.4	
FortiAI Subscription	7.6	7.6	7.6	7.6	7.6	7.6	7.6	7.6	7.6	7.6	7.6
FortiCASB ShadowIT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SIEM Database Capable	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
UEBA Database Capable	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Additional Services											
FortiCare Premium Contract	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
FortiCare Elite Contract	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Replacement Disks					✓	✓	✓	✓			
How to Buy	Hardware Bundle	Hardware Bundle	Hardware Bundle	Hardware Bundle	Hardware Bundle	Hardware Bundle	Hardware Bundle	Hardware Bundle	VM Bundle/ Subscription	VM Bundle	FortiGate Subscription

ORDER INFORMATION

FORTIANALYZER	HARDWARE DEVICES							
	150G	300G	810G	1000G	3100G	3510G	3700G	4500G (FAZ-BD)
Hardware	FAZ-150G	FAZ-300G	FAZ-810G	FAZ-1000G	FAZ- 3100G	FAZ- 3510G	FAZ- 3700G	FAZ-BD-4500G
Hardware Bundle	FAZ-150G-BDL-466-DD	FAZ-300G-BDL-466-DD	FAZ-810G-BDL-466-DD	FAZ-1000G-BDL-466-DD	FAZ-3100G-BDL-466-DD	FAZ-3510G-BDL-466-DD	FAZ-3700G-BDL-466-DD	FAZ-BD-4500G-BDL-466-DD
Renew Bundle	FC-10-L150G-466-02-DD	FC-10-L03HG-466-02-DD	FC-10-AZ81G-466-02-DD	FC-10-AZ1KG-466-02-DD	FC-10-AZ31G-466-02-DD	FC-10-AZ3AG-466-02-DD	FC-10-L3K7G-466-02-DD	FC-10-FB45G-466-02-DD
Support-only Renewal	FC-10-L150G-247-02-DD	FC-10-L03HG-247-02-DD	FC-10-AZ81G-247-02-DD	FFC-10-AZ1KG-247-02-DD	FC-10-AZ31G-247-02-DD	FC-10-AZ3AG-247-02-DD	FC-10-L3K7G-247-02-DD	FC-10-FB45G-247-02-DD
Add-On Services								
OT Service	FC-10-L150G-159-02-DD	FC-10-L03HG-159-02-DD	FC-10-AZ81G-159-02-DD	FC-10-AZ1KG-159-02-DD	FC-10-AZ31G-159-02-DD	FC-10-AZ3AG-159-02-DD	FC-10-L3K7G-159-02-DD	FC-10-FB45G-159-02-DD
Attack Surface Rating and Compliance	FC-10-L03HG-175-02-DD	FC-10-L03HG-175-02-DD	FC-10-AZ81G-175-02-DD	FC-10-AZ1KG-175-02-DD	FC-10-AZ31G-175-02-DD	FC-10-AZ3AG-175-02-DD	FC-10-L3K7G-175-02-DD	FC-10-FB45G-175-02-DD
FortiAI Subscription	FC-10-L03HG-1118-02-DD	FC-10-L03HG-1118-02-DD	FC-10-AZ81G-1118-02-DD	FC-10-AZ1KG-1118-02-DD	FC-10-AZ31G-1118-02-DD	FC-10-AZ3AG-1118-02-DD	FC-10-L3K7G-1118-02-DD	FC-10-FB45G-1118-02-DD
Replacement Disks								
Replacement Disk SKU							SP-DAM37G4T	BDM-4500G
Replacement PSUs								
Replacement PSU SKU		SP-FAD400F-PS	SP-FAZ800G-PS				SP-FAZ3700F-PS	

FORTIANALYZER VM

	5GB/Day	50GB/Day	500GB/Day	Description
Subscription Bundles	FC1-10-AZVMS-465-01-DD	FC2-10-AZVMS-465-01-DD	FC3-10-AZVMS-465-01-DD	All in one subscription bundle including 24×7 FortiCare Premium Support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service. Fully stackable.
Add-On Services				
OT Service	FC1-10-AZVMS-159-01-DD	FC2-10-AZVMS-159-01-DD	FC3-10-AZVMS-159-01-DD	
Attack Surface Rating and Compliance	FC1-10-AZVMS-175-01-DD	FC2-10-AZVMS-175-01-DD	FC3-10-AZVMS-175-01-DD	
FortiAI Subscription	FC1-10-AZVMS-1118-01-DD	FC2-10-AZVMS-1118-01-DD	FC3-10-AZVMS-1118-01-DD	
FortiCare Elite Upgrade	FC1-10-AZVMS-204-01-DD	FC2-10-AZVMS-204-01-DD	FC3-10-AZVMS-204-01-DD	

	1GB/Day	5GB/Day	25GB/Day	100GB/Day	500GB/Day	2000GB/Day	
Perpetual License	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000	Perpetual license. Purchase 24×7 FortiCare Premium Support, IOC, Security Automation Service, and FortiGuard Outbreak Detection Service separately. Only GB/Day is stackable.
Add-On Services							
OT Service			FCx-10-LV0VM-159-02-DD				
Attack Surface Rating and Compliance			FCx-10-LV0VM-175-02-DD				
IOC and Outbreak Service			FCx-10-LV0VM-661-02-DD				
SOC Automation Service			FCx-10-LV0VM-335-02-DD				
FortiAI Subscription			FCx-10-LV0VM-1118-02-DD				
FortiCare Premium			FCx-10-LV0VM-248-02-DD				
FortiCare Elite			FCx-10-LV0VM-285-02-DD				
FortiCare Elite Upgrade			FCx-10-LV0VM-204-02-DD				

FORTIANALYZER BD-VM

License Type	SKU	Logs/Sec	Storage capacity	Description
Base License	FAZ-BD-VM	150,000	200 TB	FortiAnalyzer-BD virtual appliance with 150,000 logs/sec ingestion rate and 200TB storage capacity to start. Support add-on to scale up performance and storage.
Add-On License	FAZ-BD-VM-UG	50,000	50 TB	FortiAnalyzer-BD virtual appliance ADD-ON to add additional capacity with 50,000 logs/sec ingestion rate and 50TB storage. Multiple ADD-ONs can be stacked together to scale up the ingestion rate and storage.
Add-On Services				
OT Service	FC-10-ZBDVM-159-02-DD			
Attack Surface Rating and Compliance	FC-10-ZBDVM-175-02-DD			
FortiAI Subscription	FC-10-ZBDVM-1118-02-DD			

FORTIANALYZER CLOUD

		Description
Per Device Subscription	FC-10-[FortiGate Model Code]-585-02-DD	FortiAnalyzer Cloud: cloud-Based central logging & analytics. Include All FortiGate log types, IOC Service, Security Automation Service and FortiGuard Outbreak Detection Service.

	5GB/Day	50GB/Day	500GB/Day	
Cloud Storage Add-On	FC1-10-AZCLD-463-01-DD	FC2-10-AZCLD-463-01-DD	FC3-10-AZCLD-463-01-DD	FortiAnalyzer Cloud Storage Add-On for Central Logging & Analytics. Stackable.

FORTIANALYZER VM: PRIVATE CLOUD SUPPORT

	VMware	Citrix Xen	KVM	Microsoft Hyper-V	Nutanix AHV	Oracle Private Cloud	OpenSource Xen
FAZ-VM	✓	✓	✓	✓	✓	✓	✓

FORTIANALYZER VM: PUBLIC CLOUD SUPPORT

	Amazon AWS	Microsoft Azure	Google GCP	Oracle OCI / OPC
FAZ-VM	✓	✓	✓	✓

		Description
FAZ Backup to Cloud Service	FC-10-FAZ00-286-02-DD	One year subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud.

ORDER INFORMATION: FORTIANALYZER VM PERPETUAL

Perpetual licensing model with a-la-carte support and services available for purchase.

Step 1: Select the FortiAnalyzer VM SKU based on the amount of GB/Day of logs to ingest per day. Multiple SKUs can be combined to reach the desired amount.

SKU	DESCRIPTION
FAZ-VM-GB1	License for 1 GB/Day of Logs.
FAZ-VM-GB5	License for 5 GB/Day of Logs.
FAZ-VM-GB25	License for 25 GB/Day of Logs.
FAZ-VM-GB100	License for 100 GB/Day of Logs.
FAZ-VM-GB500	License for 500 GB/Day of Logs.
FAZ-VM-GB2000	License for 2 TB/Day of Logs.

Step 2: Select "a-la-carte" support and services matching your tier of GB/Day of Logs.

TIER	SECURITY AUTOMATION SERVICE	FORTIGUARD IOC AND OUTBREAK DETECTION SERVICE	FORTICARE PREMIUM SUPPORT	FORTICARE ELITE SUPPORT	FORTIANALYZER-FORTICARE UPGRADE FROM PREMIUM TO ELITE
1-6 GB/Day of Logs	FC1-10-LV0VM-335-02-DD	FC1-10-LV0VM-661-02-DD	FC1-10-LV0VM-248-02-DD	FC1-10-LV0VM-285-02-DD	FC1-10-LV0VM-204-02-DD
1-11 GB/Day of Logs	FC2-10-LV0VM-335-02-DD	FC2-10-LV0VM-661-02-DD	FC2-10-LV0VM-248-02-DD	FC2-10-LV0VM-285-02-DD	FC2-10-LV0VM-204-02-DD
1-26 GB/Day of Logs	FC3-10-LV0VM-335-02-DD	FC3-10-LV0VM-661-02-DD	FC3-10-LV0VM-248-02-DD	FC3-10-LV0VM-285-02-DD	FC3-10-LV0VM-204-02-DD
1-101 GB/Day of Logs	FC5-10-LV0VM-335-02-DD	FC5-10-LV0VM-661-02-DD	FC5-10-LV0VM-248-02-DD	FC5-10-LV0VM-285-02-DD	FC5-10-LV0VM-204-02-DD
1-501 GB/Day of Logs	FC6-10-LV0VM-335-02-DD	FC6-10-LV0VM-661-02-DD	FC6-10-LV0VM-248-02-DD	FC6-10-LV0VM-285-02-DD	FC6-10-LV0VM-204-02-DD
1-2001 GB/Day of Logs	FC7-10-LV0VM-335-02-DD	FC7-10-LV0VM-661-02-DD	FC7-10-LV0VM-248-02-DD	FC7-10-LV0VM-285-02-DD	FC7-10-LV0VM-204-02-DD
1-unlimited GB/Day of Logs	FC4-10-LV0VM-335-02-DD	FC4-10-LV0VM-661-02-DD	FC4-10-LV0VM-248-02-DD	FC4-10-LV0VM-285-02-DD	FC4-10-LV0VM-204-02-DD

ORDER LIFECYCLE: FORTIANALYZER VM PERPETUAL

NEW ORDER

Example

- Logs to ingest: 10 GB/Day
- A la carte support and services: Security Automation Service, FortiCare Elite Support

Purchase the following SKUs:

- 2 x FAZ-VM-GB5 "License for 5 GB/Day of Logs"
- 1x FC2-10-LV0VM-335-02-DD "Security Automation tier 1-11 GB/Day"
- 1x FC2-10-LV0VM-285-02-DD "FortiCare Elite Support tier 1-11 GB/Day"

ADD MORE GB/DAY OF LOGS TO INGEST

Example: Add immediately 15 GB/Day of Logs for a total of 25 GB/Day of Logs.

1. Purchase the following SKUs as net new
   3x FAZ-VM-GB5 (License for adding 5 GB/Day Logs)
2. Purchase the following SKUs via a co-term agreement
   1x FC3-10-LV0VM-335-02-DD (Security Automation service for 1-26 GB/Day)
   1x FC3-10-LV0VM-285-02-DD (FortiCare Elite Support for 1-26 GB/Day)

Apply the support and services SKUs via co-term to align all contracts to the same expiration date. Co-term agreement consolidates multiple contracts and services under a single end date to make it easier to track and manage renewals.

NSE TRAINING AND CERTIFICATION

FCP – FortiAnalyzer Administrator Training and Certification

Learn how to deploy, configure, and secure FortiAnalyzer, register and manage devices with FortiAnalyzer. At the same time, explore the fundamentals of the logging and reporting management capabilities included in FortiAnalyzer to become a professional FortiAnalyzer administrator.

FCP – FortiAnalyzer Analyst Training and Certification

Learn the fundamentals of using FortiAnalyzer for centralized logging, identify current and potential threats through log analysis, examine the management of events, incidents, reports, and task automation with playbooks to become a SOC analyst in an environment using Fortinet products.

Ordering Information

SKU	DESCRIPTION
FT-FAZ-ADM	Instructor-led Training - 1 full day or 2 half days
FT-FAZ-ADM -LAB	On-demand Labs in self-paced
FT-FAZ-ANS	Instructor-led Training – 1 full day or 2 half days
FT-FAZ-ANS-LAB	On-demand Labs in self-paced
NSE-EX-FTE2	Certification Exam

Course Description

For more information about prerequisites, agenda topics and learning objectives, please refer to the course description at

- FortiAnalyzer Administrator- https://training.fortinet.com/local/staticpage/view.php?page=library_fortianalyzer-administrator
- FortiAnalyzer Analyst- https://training.fortinet.com/local/staticpage/view.php?page=library_fortianalyzer-analyst

FREQUENTLY ASKED QUESTIONS

What is the FortiGuard Outbreak Detection Service and how do I purchase?

What is FortiGuard Outbreak Detection Service?

- The FortiGuard Outbreak Detection Service, provides customers with content packages created in real time, to protect their networks against new malware outbreaks. The package contains reports, report templates and event handlers to handle the latest malware outbreaks identified by Fortinet's Global Threat Intelligence.

How do I purchase FortiGuard Outbreak Detection Service?

- The FortiGuard Outbreak Detection Service is included with the FortiAnalyzer Enterprise Protection bundle and is available a la carte for eligible hardware models.
- The FortiGuard Outbreak Detection Service is available a la carte for FortiAnalyzer Perpetual VM.
- The FortiGuard Outbreak Detection Service is included with FortiAnalyzer VM Subscription.

What is SOCaaS, what is included with SOCaaS (SOC as as Service) and how do I purchase?

What is SOCaaS?

- SOCaaS is a Cloud-based managed security service offering – whereas Fortinet SOC analysts monitor the customer's network for security events and threats and escalate back to customer when detected.

What does SOCaaS include?

- 7×24×365 monitoring of security events and device health for FortiGate firewalls
- Incident detection, investigation and escalation
- Preventative control review and tuning recommendation
- Weekly/Monthly reports & quarterly risk review
- Remote assistance via online chat, email, and phone
- Access to the SOCaaS Portal

How do I purchase SOCaaS?

- FortiAnalyzer Cloud with SOCaaS can be purchased for supported FortiGate models. Each FortiGate requiring the monitoring service requires a license.

How do I purchase a VM perpetual license?

A VM perpetual license can be purchased in two ways.

Start with a limited free trial (available with a FortiCloud account) then upgrade the VM by purchasing an upgrade license SKU to increase capacity.

Purchase an upgrade license SKU directly.

How do I extend my existing FAZ VM Perpetual deployment?

Customers who already have a perpetual FAZ-VM can purchase any of the below add-on SKUs to extend the capacity of their existing FAZ-VM deployment.

SKU	DESCRIPTION
FAZ-VM-GB1	Upgrade license for adding 1 GB/Day of Logs.
FAZ-VM-GB5	Upgrade license for adding 5 GB/Day of Logs.
FAZ-VM-GB25	Upgrade license for adding 25 GB/Day of Logs.
FAZ-VM-GB100	Upgrade license for adding 100 GB/Day of Logs.
FAZ-VM-GB500	Upgrade license for adding 500 GB/Day of Logs.
FAZ-VM-GB2000	Upgrade license for adding 2 TB/Day of Logs.

What is included in FAZ-VM Free Trial and how many trials can I have?

The FortiAnalyzer VM Free Trial includes the following:

- 1 GB/day logs, 3 devices, 3 ADOMs.
- Trial licenses do NOT include services or support.

How many free trials can I have?

- Customer can generate 1 free trail for a product on their account at a time.
- Only 1 free trial per product, per account, can be active at a time.
- Once the purchased add-on license is applied to the trial instance, the trial instance is converted into Production Instance.
- Only after the free trial is converted to the production instance, will a new free trial be available again for the FortiCare account.
- Once a product has no active free trial on the FortiCare account, a new free trial will be available.

*So, a customer can generate multiple Trial Licenses but not at the same time.

**For PoCs or for our Demo Labs we still have the Eval Licenses. 60-days for external or 1 Year for internal.

Can I opt-out of the FortiCare Free Trial and directly purchase a license?

Customers can opt out of the free trial and purchase only the FortiAnalyzer-VM stackable add-on SKUs.

- For FortiAnalyzer 7.0 customers will receive a license and can enter the purchased license code on the VM login page. Customers can also upload new licenses via the GUI.
- For FortiAnalyzer 6.2/6.4 customers, licenses can be uploaded via the GUI.

How many ADOMs are included with my FortiAnalyzer?

ADOM defaults and maximums information for FortiAnalyzer Hardware and VM can be found on docs.fortinet.com in the release notes for your FortiAnalyzer's firmware release under Appendix A.

How do I add ADOMs to my FortiAnalyzer?

- An ADOM add-on license can be purchased for FortiAnalyzer VM Subscriptions, and for supported FortiAnalyzer hardware models (FortiAnalyzer hardware G models 1000 Series and above)
- The ADOM add-on License SKUs for FortiAnalyzer can be found under the "VDOM & ADOM" tab of the pricelist.

How do I order FortiAnalyzer Cloud or SOCaaS?

FortiAnalyzer Cloud and SOCaaS for FortiGates are obtained via the below SKUs

SKU	DESCRIPTION
FC-10-[FortiGate Model Code]-464-02-DD	SOCaaS: 24×7 cloud-based managed log monitoring, incident triage and SOC escalation service
FC-10-[FortiGate Model Code]-585-02-DD	FortiAnalyzer Cloud: cloud-based central logging and analytics. Include all FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Detection Service.

How do I order more storage for my FortiAnalyzer cloud?

- FortiAnalyzer Cloud Storage can be increased by purchasing the stackable "FortiAnalyzer Cloud Storage" SKU in the Cloud tab of the pricelist.

How do I unlock advanced OT Security and Security Rating and Compliance Services?

Starting in version 7.4, FortiAnalyzer adds two new SKUs:

- 159 "OT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules" Unlock all OT related features such as OT security reports and event handlers.
- 175 "FortiAnalyzer Attack Surface Rating and Compliance" Unlock the newly available compliance reports (PCI, CIS) and Shadow-IT.

How do I order High Availability for FortiAnalyzer?

To add FortiAnalyzer High Availability, you can purchase 2 of the same FortiAnalyzer.

Each FortiAnalyzer in the HA cluster should also:

- Be of the same FortiAnalyzer series/platform.
- Be on the same FortiAnalyzer firmware version
- Run in the same operation mode: Analyzer or Collector
- Have the same GB/Day of Logs
- Be visible on the network

What license do I need for FAZ in Collector-Only mode?

For an appliance, you can use the lowest hardware model, e.g., FAZ-150G.

For a VM, you can choose the lowest available tier, such as FAZ-VM-GB1 or FC1-10-AZVMS-465-01-DD

How is FAZ Cloud licensed for FortiGates in an HA pair?

Each FortiGate requires its own FAZ cloud subscription.

Visit www.fortinet.com for more details