FortiAnalyzer

Product Offerings

F::RTINET

Available in:

Appliance   Virtual Machine   Cloud

FortiAnalyzer provides central logging and reporting, advanced analytics, and security automation for rapid detection and response against cyber threats.

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**: cloud offering through the FortiCloud Premium subscription.

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

				HARDWARE					VM	SUBSCRIPTION	
	150G	**300G**	**800G**	**1000F**	**3000G**	**3500G**	**3700G**	**4500F**	**BD-VM**	**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*	Stackable*	Stackable
Collector Mode Sustained LPS	750	3,000	6,000	30,000	60,000	90,000	150,000		Stackable*	Stackable*	Stackable
No. Days @ Max Sustained LPS	90	50	50	34	30	38	60	30	Stackable*	Stackable*	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	5	25	50	50	500	500	1,200	10,000	1,200	1,200	
Max ADOMs with add-on license					1,200		10,000				
Distributed Arch. / Horizontal Scaling								✓			✓
Container Modules Supported											
FortiSOAR				7.0	7.0	7.0	7.0		7.0	7.0	
Security Services											
Fortinet SOCaaS											✓
FortiGuard IOC Subscription	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SOC Subscription license	✓	✓	✓	✓	✓	✓	7.0	✓	✓	✓	✓
FortiGuard Outbreak Detection Subscription	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0
FortiCASB ShadowIT	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0
SIEM Database Capable	✓	✓	✓	✓	✓	✓	✓	7.0	✓	✓	✓
UEBA Database Capable	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Additional Services											
FortiCare Premium Contract				Subscription							
FortiCare Elite Contract				Subscription					✓	✓	✓
Replacement Disks				✓	✓	✓	✓	✓	✓		
How to Buy	Hardware Bundle	Hardware Bundle	Hardware Bundle	Hardware Bundle	Hardware Bundle	Hardware Bundle	Hardware Bundle	Hardware Bundle	VM Bundle	VM Subscription	FortiGate Subscription

* Depends on the VM deployment (hypervisor, number & type of CPUs, IOPS setup, amount of memory allocated, etc.). The limits for VM deployments are: 1 - 4 interfaces, 4GB RAM to unlimited, and 2 CPUs to unlimited.

ORDER INFORMATION

BUNDLES	HARDWARE DEVICES							
	150G	300G	800G	1000F	3000G	3500G	3700G	4500F (FAZ-BD)
Hardware Bundle	FAZ-150G-BDL-466-DD	FAZ-300G-BDL-466-DD	FAZ-800G-BDL-466-DD	FAZ-1000F-BDL-466-DD	FAZ-3000G-BDL-466-DD	FAZ-3500G-BDL-466-DD	FAZ-3700G-BDL-466-DD	FAZ-BD-4500F-BDL-466-DD
Renew Bundle	FC-10-L150G-466-02-DD	FC-10-L03HG-466-02-DD	FC-10-L08HG-466-02-DD	FC-10-L01KF-466-02-DD	FC-10-L03KG-466-02-DD	FC-10-L3K5G-466-02-DD	FC-10-L3K7G-466-02-DD	FC-10-BD45F-466-02-DD
Support-only Renewal	FC-10-L150G-247-02-DD	FC-10-L03HG-247-02-DD	FC-10-L08HG-247-02-DD	FC-10-L01KF-247-02-DD	FC-10-L03KG-247-02-DD	FC-10-L3K5G-247-02-DD	FC-10-L3K7G-247-02-DD	FC-10-BD45F-247-02-DD
Replacement Disks								
Replacement Disk SKU				SP-FMG1KF-HDD	SP-D4TC	SP-FAZ-3500G-SATA-HDD	SP-DAM37G4T	SP-BD4500F-SSD-B1 SP-BD4500F-SSD-B2
Replacement PSUs								
Replacement PSU SKU		SP-FAD400F-PS	SP-FAZ800G-PS	SP-FMG400E-PS	SP-FAZ3000G-PS		SP-FAZ3700F-PS	SP-BD4500F-PS (module only)

FORTIANALYZER-BD-VM		
	150,000 Logs/Sec	Description
Base License	FAZ-BD-VM	Perpetual license. Purchase 24x7 FortiCare support, IOC, SOC subscription and FortiGuard Outbreak Detection Service separately. Log rates is stackable.
	50,000 Logs/Sec	Description
Add-On License	FAZ-BD-VM-UG	Perpetual license. Multiple ADD-ONs can be stacked together to scale up the ingestion rate and storage

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 24x7 FortiCare support, IOC, SOC subscription, andFortiGuard Outbreak Detection service. Fully stackable.
	1GB/Day	5GB/Day	25GB/Day	100GB/Day	500GB/Day	2000GB/Day	Description
Perpetual License	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000	Perpetual license. Purchase 24x7 FortiCare support, IOC, SOC subscription and FortiGuard Outbreak Detection Service separately. Only GB/Day is stackable.

FORTIANALYZER CLOUD				
				Description
Per Device Subscription	FC-10-[FortiGate Model Code]-464-02-DD			FortiAnalyzer Cloud Logging and Monitoring for FortiGate logs, including FortiCloud SOCaaS.
	5GB/Day	50GB/Day	500GB/Day	Description
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 FortiGate logs and all other supported Fortinet product logs. Including FortiCloud SOCaaS. Stackable

EXTENSIONS		
EXTENSION	EXTENSION LICENSE	Description
FortiSIEM Collector	Included in FortiAnalyzer	Collect and forward FortiAnalyzer events to FortiSIEM
FortiSOAR	FC-10-SRVMS-389-02-DD	FortiSOAR Enterprise Subscription plus 24x7 FortiCare and FortiCare Best Practice Service - 2 User Logins included

TRAINING SERVICES LICENSE		
Instructor-led Training	FT-FAZ	NSE 5/FortiAnalyzer Instructor-led Training
Lab Access	FT-FAZ-LAB	NSE 5/FortiAnalyzer Lab Access
Certification Exam	NSE-EX-SPL5	NSE 5/FortiAnalyzer Exam Voucher

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.

Can I still purchase a perpetual FAZ VM license without the VM BASE SKU?

1. Can I still purchase a FortiAnalyzer Perpetual VM, now that FAZ-VM-BASE SKU has been EOL/EOO?

   FortiAnalyzer and FortiManager Perpetual VMs are still available for purchase and are NOT EOL/EOO.
   - The EOO only applies to SKU: FAZ-VM-BASE

2. Will my previously purchased FortiAnalyzer Perpetual VMs work without the FAZ-VM-BASE SKUs?

   Yes, FortiAnalyzer Perpetual VMs will still work.
   - The permanent add-on SKUs are not affected.
     Eg. FAZ-VM-GB5 or FMG-VM-10-UG etc

3. Do the VM Subscription SKUs replace the VM Perpetual SKUs?

   No. There are no plans at the moment to replace the perpetual VM model with the subscription model.

4. How do I start a purchase for the VM perpetual license now?

   The VM perpetual license purchase can be started 2 ways.

   a) Start a Free Trial, and then upgrade the VM by purchasing the VM add-on SKUs.
   - Instead of purchasing the VM BASE SKU, customers can start the purchase with the Limited Free Trial (available with a FortiCare account).
   - Once the Free Trial is activated, they can purchase add-on licenses to increase capacity. This is done the same way as before.

   b) Skip the Free Trial and purchase only the VM add-on SKUs.
   - Customers who already have the permanent FAZ-VM can continue to purchase the add-on SKUs to extend the capacity for their existing FAZ-VM.
   - Customers who do not already have a FAZ-VM but want to skip the free trial, can purchase the FAZ-VM add-on SKUs directly.

5. How do I extend my existing FAZ/FMG VM Perpetual deployment?

   Customers who already have the permanent FAZ-VM/FMG-VM can still purchase the add-on SKUs to extend the capacity for their existing FAZ/FMG-VM deployment.

   The following FortiAnalyzer VM Perpetual SKUs are still available and are NOT EOL/EOO.

   These FAZ Perpetual VM SKUs can still be purchased.

SKU	DESCRIPTION
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.

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.
- For air gapped FortiAnalyzer, connection to FDS or a FMG is required for registration, and then the license 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.

https://docs.fortinet.com/document/fortianalyzer/7.0.0/release-notes/443796/appendix-a-default-andmaximum-number-of-adoms-supported

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.

Where did the 360 Bundle go and how do I get FortiAnalyzer Cloud?

- The 360 bundle SKUs have been EOL/EOO and are no longer needed for purchasing FortiAnalyzer Cloud
- FortiAnalyzer Cloud is now purchased through ordering the FortiAnalyzer Cloud with SOCaaS SKU and FortiCloud Premium SKU.

How do I order FortiAnalyzer cloud?

- The FortiCloud Premium Account License is required for FortiAnalyzer Cloud usage. The SKU can be found in the Cloud tab of the Price List. FortiCloud Premium is required for all FortiAnalyzer Cloud licenses.
- FortiAnalyzer Cloud for FortiGate is obtained with the FortiAnalyzer Cloud SOCaaS subscription.
- FortiAnalyzer Cloud for FortiGate VM is obtained with the FortiAnalyzer Cloud SOCaaS subscription

SKU	DESCRIPTION
FC-15-CLDPS-219-02-DD	FortiCloud Premium - Access to advanced account and platform features. Per account license. See datasheet/online resources for included feature/license details.
FC-10-[FortiGate Model Code]-464-02-DD	FortiAnalyzer Cloud SOCaaS: Cloud-based Log Monitoring (PaaS), including IOC Service and FortiCloud SOCaaS.
FC-10-[FortiGate VM Model Code]-464-02-DD	FortiAnalyzer Cloud with SOCaaS: Cloud-based Log Monitoring (PaaS), including IOC Service and FortiCloud SOCaaS.

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.