FortiAnalyzer™

Unified Data Lake, Visibility, and Automation

FortiAnalyzer is a fully integrated SecOps platform, purpose-built to simplify and modernize security operations. It combines SIEM and SOAR capabilities with a scalable data lake, native threat intelligence integration, and built-in Generative AI—all in one unified solution. Designed to be XDR-ready, FortiAnalyzer enables end-to-end visibility and faster, more coordinated responses across the entire security environment. By eliminating the need for multiple disconnected tools, it streamlines workflows, reduces SOC fatigue, and improves detection and response times.

Product Offerings

FortiAnalyzer delivers a rich set of SecOps capabilities from data ingestion, detection and response, designed for scale, automation, and efficiency. A detailed breakdown of features is illustrated in the diagram below. FortiAnalyzer supports both Capex and Opex models—available as perpetual licenses for on-prem deployments or subscription-based for cloud and hosted environments to fit diverse customer needs.

	On-Prem		Cloud
	Appliance	VM	FortiAnalyzer Cloud
Ingestion Based License	✓	✓	—
Per-Device Based License	—	—	✓
GB/Day Usage Expansion	—	✓	✓
Fortinet Logging Sources	✓	✓	✓
3rd-party Logging Sources	✓	✓	✓ *
Multi-tenancy (ADOM)	✓	✓	via FortiCloud OU
FortiAI Assist	✓	✓	✓
Security Automation	✓	✓	✓
IOC & Outbreak Detection	✓	✓	✓
FortiTiP Integration	✓	—	—
OT Service	✓	✓	✓
Attack Surface Rating & Compliance	✓	✓	✓
FortiCare Premium	✓	✓	✓
FortiCare Elite	✓	✓	N/A
Log Forwarding	✓	✓	—
Collector mode	✓	✓	N/A
High Availability	✓	✓	N/A
Fabric of FortiAnalyzer	✓	✓	—
FortiPoints	N/A	✓ **	✓ **
FortiFlex	N/A	✓	N/A
FAZaaS	✓	N/A	N/A

** 3rd-party logs sources are supported via on-prem FortiAnlayzer Cloud Connector.*
*** FortiPoints are used to renew or upgrade SKUs for FortiAnalyzer VM or FortiAnalyzer Cloud.*

Hardware Bundle
Best Value for Hardware Based Deployment

- FortiAnalyzer Appliance
- FortiCare Premium
- Indicators of Compromise Service
- FortiGuard Outbreak Detection Service
- Security Automation Service
- FortiTIP SaaS Extension

FAZ-[Hardware Model]-BDL-1263-DD

VM Subscription Bundle
Best Value for VM Based Deployment

- FortiAnalyzer VM S-series
- FortiCare Premium
- Indicators of Compromise Service
- FortiGuard Outbreak Detection Service
- Security Automation Service

FCx-10-AZVMS-465-01-DD

Per Device Subscription
Commonly Purchased

- ✓ FortiAnalyzer Cloud Central Logging & Analytics
- ✓ Indicator of Compromise Service
- ✓ FortiGuard Outbreak Detection Service
- ✓ Security Automation Service

FC-10-[FORTIGATE MODEL CODE]-585-02-DD

FC-10-[FORTIWEB MODEL CODE]-585-02-DD

GB/Day Subscription*
Storage Expansion and 3rd-Party Support

FortiAnalyzer Cloud Base Subscription

- ✓ FortiAnalyzer Cloud Central Logging & Analytics
- ✓ Indicator of Compromise Service
- ✓ FortiGuard Outbreak Detection Service
- ✓ Security Automation Service
- ✓ FortiCare Premium

FCx-10-AZCLD-463-01-DD

** This option has two main uses: 1) Expands cloud storage. 2) Ingests logs from devices that don't have a per-device subscription license.*

Service Add-On

SERVICE NAME	DESCRIPTION	ORDER INFO
Security Automation Service	FortiAnalyzer Security Automation Service including premium reports, event handlers, SIEM correlation rules for advanced threat detection and SOAR playbooks.	FCx-10-xxxxx-335-0x-DD
IoC & Outbreak Detection Service	FortiGuard Indicators of Compromise and Outbreak Detection Service including daily updates of IOCs and automated outbreak alerts and predefined event handlers to detect and respond to wide spread malware outbreaks.	FCx-10-xxxxx-661-0x-DD
FortiTIP	FortiGuard Threat Intel Platform (TIP) SaaS Service Extension	FC-10-xxxxx-1034-02-DD
OT Service	OT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules.	FCx-10-xxxxx-159-0x-DD
Attack Surface Rating & Compliance	The service provides a centralized way to measure security posture, identify misconfigurations, and monitor compliance against best practices using telemetry from Fortinet devices. It helps reduce cyber risk and supports audit readiness through automated scoring, reporting, and remediation guidance.	FCx-10-xxxxx-175-0x-DD
Backup to Public Cloud Service	FortiAnalyzer storage connector service for 10TB data transfer to public cloud.	FC-10-FAZ00-286-02-DD
Managed FortiAnalyzer Service	A light-touch service delivered by SOCaaS for monitoring FortiAnalyzer's health, availability, performance, and event rule efficiency.	FC-10-xxxxx-464-02-DD
FortiAI Service	Generative AI powered security service utilizing large language models (LLMs) for real-time assistance in SOC analysis, incident investigation, triage and response.	FCx-10-xxxxx-1118-0x-DD

Use Cases

Network Operations

USE CASES	DESCRIPTION
Network & Application Monitoring	Collect and analyze logs from firewalls, routers, load balancers, web/app servers. Visibility into traffic patterns, performance, and service health.
Connectivity Troubleshooting	Use real-time search and dashboards to identify issues. Faster root cause analysis and resolution.
Capacity Planning	Trend reports on resource usage (disk, memory, bandwidth). Supports infrastructure scaling and budget forecasting.
Compliance & Audit	Store logs for regulatory and IT audit readiness (e.g., PCI, HIPAA). Simplifies audit process and meets retention policies. Archive high-volumn logs from various sources data retention
Low-Cost Log Forwarding	Use FAZ to ingest and store logs, then forward filtered data to expensive SIEMs. Reduces SIEM ingestion volume and costs.

Security Operations

USE CASES	DESCRIPTION
Theat Detection	Detect Known and unknown threats using correlation rules, anomaly detection, and AI/ML. Improves detection accuracy and speed.
Alert Triage	Normalize, enrich, and prioritize alerts using AI and automation. Reduces analyst fatigue, accelerates decision-making.
Incident Investigation	Auto-build incident timelines, investigate related logs, and visualize attack paths. Reduces mean time to investigate (MTTI) and improves context.
Response Automation	Execute playbooks to block IPs, isolate hosts, disable accounts, or notify teams. Speeds up containment, reduces manual work.
Threat Intelligence Integration	Ingest threat feeds, perform reputation checks, enrich IOCs across multiple layers. Enhances situational awareness and proactive defenses.
MITRE ATT&CK Mapping	Align detections and investigations with MITRE ATT&CK techniques. Provides structured defense analysis and coverage gap visibility.
Security Reporting & Dashboards	Auto-generate compliance and executive-level reports.

Hardware Order Information

	150G	300G	810G	1000G
Product				
Hardware	FAZ-150G	FAZ-300G	FAZ-810G	FAZ-1000G
Hardware Bundle	FAZ-150G-BDL-1263-DD	FAZ-300G-BDL-1263-DD	FAZ-810G-BDL-1263-DD	FAZ-1000G-BDL-1263-DD
Renew Bundle	FC-10-L150G-1263-02-DD	FC-10-L03HG-1263-02-DD	FC-10-AZ81G-1263-02-DD	FC-10-AZ1KG-1263-02-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
Service Add-On				
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
Attack Surface Rating & Compliance	FC-10-L150G-175-02-DD	FC-10-L03HG-175-02-DD	FC-10-AZ81G-175-02-DD	FC-10-AZ1KG-175-02-DD
FortiAI Service	FC-10-L150G-1118-02-DD	FC-10-L03HG-1118-02-DD	FC-10-AZ81G-1118-02-DD	FC-10-AZ1KG-1118-02-DD
FortiAI Token Top-up	FC1-10-AITAZ-1089-02-DD	FC1-10-AITAZ-1089-02-DD	FC1-10-AITAZ-1089-02-DD	FC1-10-AITAZ-1089-02-DD
Managed FortiAnalyzer Service	FC-10-L150G-464-02-DD	FC-10-L03HG-464-02-DD	FC-10-AZ81G-464-02-DD	FC-10-AZ1KG-464-02-DD
Backup to Public Cloud Service	FC-10-FAZ00-286-02-DD	FC-10-FAZ00-286-02-DD	FC-10-FAZ00-286-02-DD	FC-10-FAZ00-286-02-DD
FortiCare Elite Upgrade	FC-10-L150G-204-02-DD	FC-10-L03HG-204-02-DD	FC-10-AZ81G-204-02-DD	FC-10-AZ1KG-204-02-DD
Replacement Disks				
Replacement Disk SKU	—	—	—	—
Replacement PSUs				
Replacement PSU SKU	—	SP-FAD400F-PS	SP-FAZ800G-PS	—

	3100G	3510G	3750G
Product			
Hardware	FAZ- 3100G	FAZ- 3510G	FAZ- 3750G
Hardware Bundle	FAZ-3100G-BDL-1263-DD	FAZ-3510G-BDL-1263-DD	FAZ-3750G-BDL-1263-DD
Renew Bundle	FC-10-AZ31G-1263-02-DD	FC-10-AZ3AG-1263-02-DD	FC-10-L375G-1263-02-DD
Support-only Renewal	FC-10-AZ31G-247-02-DD	FC-10-AZ3AG-247-02-DD	FC-10-L375G-247-02-DD
Service Add-On			
OT Service	FC-10-AZ31G-159-02-DD	FC-10-AZ3AG-159-02-DD	FC-10-L375G-159-02-DD
Attack Surface Rating & Compliance	FC-10-AZ31G-175-02-DD	FC-10-AZ3AG-175-02-DD	FC-10-L375G-175-02-DD
FortiAI Service	FC-10-AZ31G-1118-02-DD	FC-10-AZ3AG-1118-02-DD	FC-10-L375G-1118-02-DD
FortiAI Token Top-up	FC1-10-AITAZ-1089-02-DD	FC1-10-AITAZ-1089-02-DD	FC1-10-AITAZ-1089-02-DD
Managed FortiAnalyzer Service	FC-10-AZ31G-464-02-DD	FC-10-AZ3AG-464-02-DD	FC-10-L375G-464-02-DD
Backup to Public Cloud Service	FC-10-FAZ00-286-02-DD	FC-10-FAZ00-286-02-DD	FC-10-FAZ00-286-02-DD
FortiCare Elite Upgrade	FC-10-AZ31G-204-02-DD	FC-10-AZ3AG-204-02-DD	FC-10-L375G-204-02-DD
Replacement Disks			
Replacement Disk SKU	—	—	—
Replacement PSUs			
Replacement PSU SKU	—	—	—

VM Order Information

1. VM Subscription - All in one subscription including 24×7 FortiCare Premium support, IOC, Outbreak Alert Detection, Security Automation Service. Fully stackable.

	5GB/DAY	50GB/DAY	500GB/DAY
Product			
VM Subscription Bundle	FC1-10-AZVMS-465-01-DD	FC2-10-AZVMS-465-01-DD	FC3-10-AZVMS-465-01-DD
Service Add-On			
OT Service *	FC1-10-AZVMS-159-01-DD	FC2-10-AZVMS-159-01-DD	FC3-10-AZVMS-159-01-DD
Attack Surface Rating & Compliance *	FC1-10-AZVMS-175-01-DD	FC2-10-AZVMS-175-01-DD	FC3-10-AZVMS-175-01-DD
FortiAI Service *	FC1-10-AZVMS-1118-01-DD	FC2-10-AZVMS-1118-01-DD	FC3-10-AZVMS-1118-01-DD
FortiAI Token Top-up	FC1-10-AITAZ-1089-02-DD	FC1-10-AITAZ-1089-02-DD	FC1-10-AITAZ-1089-02-DD
Backup to Public Cloud Service	FC-10-FAZ00-286-02-DD	FC-10-FAZ00-286-02-DD	FC-10-FAZ00-286-02-DD
FortiCare Elite Upgrade *	FC1-10-AZVMS-1137-01-DD	FC2-10-AZVMS-1137-01-DD	FC3-10-AZVMS-1137-01-DD

** The add-on service tier must match the GB/day ingestion subscription. For example, a 5 GB/day ingestion license requires a 5 GB/day FortiAI Service tier.*

2. VM Perpetual - With a la carte service options. Perpetual license. Purchase 24×7 FortiCare Premium Support, IOC, Security Automation Service, and FortiGuard Outbreak Detection Service separately. Only GB/Day is stackable.

	1GB/Day	5GB/DAY	25GB/Day	100GB/Day	500GB/Day	2000GB/Day
Product						
Perpetual License	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000
Service Add-On						
OT Service *	FCx-10-LV0VM-159-02-DD					
Attack Surface Rating & 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 Service *	FCx-10-LV0VM-1118-02-DD					
FortiAI Token Top-up	FC1-10-AITAZ-1089-02-DD					
FortiCare Premium *	FCx-10-LV0VM-248-02-DD					
FortiCare Elite *	FCx-10-LV0VM-285-02-DD					
Backup to Public Cloud Service	FC-10-FAZ00-286-02-DD					
FortiCare Elite Upgrade *	FCx-10-LV0VM-204-02-DD					

** The add-on service tier must match the GB/day ingestion subscription. For example, a 5 GB/day ingestion license requires a 5 GB/day Security Automation Service tier.*

VM Information for Private and Public Cloud

PRIVATE AND PUBLIC CLOUD SUPPORT		
	Private Cloud	Public Cloud
VMware	✓	—
Citrix Xen	✓	—
KVM	✓	—
Microsoft Hyper-V	✓	—
Nutanix AHV	✓	—
Oracle Private Cloud	✓	—
OpenSource Xen	✓	—
Amazon AWS	—	✓
Microsoft Azure	—	✓
Google GCP	—	✓
Oracle OCI / OPC	—	✓

FortiAnalyzer Cloud Order Information

FortiAnalyzer Cloud provides cloud-based central logging and analytics, including IOC service, FortiGuard Outbreak Detection Service and Security Automation Service. FortiAnalyzer Cloud Support the following license models:

1. Per-Device Subscription: Each logging device must have its own license. Applies to FortiGate and FortiWeb.

How it works:

- You must first purchase the -585 device subscription SKU to enable logging to FortiAnalyzer Cloud.
- This license is required and includes a default log ingestion volume. The daily log volume varies depending on the size of the devices. https://docs.fortinet.com/document/fortianalyzer-cloud/7.6.4/release-notes/140964/logging-support-and-daily-log-limits

If more cloud storage is needed, you add a GB/Day Subscription to extend the cloud storage. This is separate from the per-device subscription. You don't need to this GB/Day license if the default log ingestion volume is sufficient.

Note that FortiGate and FortiWeb logs must be sent directly to FortiAnalyzer Cloud. These logs cannot be forwarded via an on-prem FortiAnalyzer using a GB/day subscription.

2. GB/Day Subscription: A shared capacity model based on the expected daily log ingestion volume. The licensed capacity is pooled and shared across all the devices under the same support account.

How it works:

- Based on daily log ingestion volume (GB/day).
- Shared across all supported devices within the same FortiCloud account.

When GB/day license is required:

- *Integrated Fortinet Devices that do not offer Per-Device subscription.*
  - Applies to FortiClient, FortiEndpoint, FortiMail and FortiNDR.
  - These devices can send logs directly to FortiAnalyzer Cloud with GB/day license.
  - No on-prem FortiAnalyzer collector is required.

- *3rd-Party Devices.*
  - Third-party logs must use a GB/day license.
  - An on-prem FAZ is required to collect and forward logs to FortiAnalyzer Cloud via the FortiAnalyzer Cloud Connector.
  - The on-prem FortiAnalyzer must run OS 7.6.3 https://docs.fortinet.com/document/fortianalyzer/7.6.0/new-features/185893/fortianalyzer-cloud-connector-7-6-3
  - Note that If the customer is already using an on-prem FortiAnalyzer, other Fortinet device except FortiGate and FortiWeb logs can also be forwarded through it using the same GB/day subscription license.

FORTIANALYZER CLOUD			
Per-Device Subscription			
FortiGate	FC-10-[FORTIGATE MODEL CODE]-585-02-DD		
FortiWeb	FC-10-[FORTIWEB MODEL CODE]-585-02-DD		
GB/Day Subscription	**5GB/Day**	**50GB/Day**	**500GB/Day**
	FC1-10-AZCLD-463-01-DD	FC2-10-AZCLD-463-01-DD	FC3-10-AZCLD-463-01-DD
Service Add-On			
OT Service *	FC1-10-AZCLD-159-01-DD	FC2-10-AZCLD-159-01-DD	FC3-10-AZCLD-159-01-DD
Attack Surface Rating & Compliance *	FC1-10-AZCLD-175-01-DD	FC2-10-AZCLD-175-01-DD	FC3-10-AZCLD-175-01-DD
FortiAI Service *	FC1-10-AZCLD-1118-01-DD	FC2-10-AZCLD-1118-01-DD	FC3-10-AZCLD-1118-01-DD
FortiAI Token Top-up	FC1-10-AITAZ-1089-02-DD	FC1-10-AITAZ-1089-02-DD	FC1-10-AITAZ-1089-02-DD
Backup to Public Cloud Service	FC-10-FAZ00-286-02-DD	FC-10-FAZ00-286-02-DD	FC-10-FAZ00-286-02-DD
FortiCare Elite Upgrade *	—	—	—

** The add-on service tier must match the GB/day ingestion subscription. For example, a 5 GB/day ingestion license requires a 5 GB/day FortiAI Service Tier.*

Fortinet 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

Course Details

For prerequisites, agenda topics, and learning objectives, visit:

- 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

Training Offering

For training SKUs, purchasing, and delivery options, visit:
https://training.fortinet.com/local/staticpage/view.php?page=purchasing_process

Order Examples

FortiAnalyzer Cloud Order Example 1

Scenario: A customer has **3×FortiGate-70G** devices and wants to send logs to **FortiAnalyzer Cloud**.

1. FortiAnalyzer Cloud – Device License

- SKU: FC-10-GT70G-585-02-DD
- Quantity: 3
- One FortiAnalyzer Cloud device license is required **per FortiGate**.

What this provides:

- Direct logging from each FortiGate-70G to FortiAnalyzer Cloud.
- **Default log ingestion entitlement of 200 MB/day per device**.
- Built-in logging, analytics, reporting, dashboards and SIEM/SOAR capabilities.
- No on-prem FortiAnalyzer required.

2. (Optional) GB/Day Subscription Add-On

A GB/day ingestion add-on is only required if the customer needs:

- Log volume **beyond the default 200 MB/day per FortiGate**.

Notes

- GB/day add-on capacity is **shared across all licensed FortiGates** within the same FortiCloud account.
- Add-on capacity supplements (does not replace) the per-device entitlement.

FortiAnalyzer Cloud Order Example 2

Scenario: A customer does **not** have FortiGate or FortiWeb devices. They want to send logs from **FortiClient** and **FortiMail** to **FortiAnalyzer Cloud**.

1. FortiAnalyzer Cloud – GB/Day Subscription

- SKU: FC1-10-AZCLD-463-01-DD – 5GB/day ingestion license
- Quantity: Based on required daily log volume (GB/day) - if you need more than 5GB/day, you purchase multiple.
- A GB/day subscription is required to ingest logs from FortiClient and FortiMail into FortiAnalyzer Cloud.

What this provides:

- Log ingestion for FortiClient and FortiMail.
- Shared ingestion capacity across all supported devices in the same FortiCloud account.
- Built-in logging, analytics, reporting, dashboards and SIEM/SOAR capabilities.
- No on-prem FortiAnalyzer required.

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 (GB/DAY)	FORTICARE PREMIUM	SECURITY AUTOMATION SERVICE	IOC AND OUTBREAK SERVICE	FORTICARE ELITE	FORTICARE PREMIUM TO ELITE UPGRADE
1-6 GB/Day	FC1-10-LV0VM-248-02-DD	FC1-10-LV0VM-335-02-DD	FC1-10-LV0VM-661-02-DD	FC1-10-LV0VM-285-02-DD	FC1-10-LV0VM-204-02-DD
1-11 GB/Day	FC2-10-LV0VM-248-02-DD	FC2-10-LV0VM-335-02-DD	FC2-10-LV0VM-661-02-DD	FC2-10-LV0VM-285-02-DD	FC2-10-LV0VM-204-02-DD
1-26 GB/Day	FC3-10-LV0VM-248-02-DD	FC3-10-LV0VM-335-02-DD	FC3-10-LV0VM-661-02-DD	FC3-10-LV0VM-285-02-DD	FC3-10-LV0VM-204-02-DD
1-101 GB/Day	FC5-10-LV0VM-248-02-DD	FC5-10-LV0VM-335-02-DD	FC5-10-LV0VM-661-02-DD	FC5-10-LV0VM-285-02-DD	FC5-10-LV0VM-204-02-DD
1-501 GB/Day	FC6-10-LV0VM-248-02-DD	FC6-10-LV0VM-335-02-DD	FC6-10-LV0VM-661-02-DD	FC6-10-LV0VM-285-02-DD	FC6-10-LV0VM-204-02-DD
1-2001 GB/Day	FC7-10-LV0VM-248-02-DD	FC7-10-LV0VM-335-02-DD	FC7-10-LV0VM-661-02-DD	FC7-10-LV0VM-285-02-DD	FC7-10-LV0VM-204-02-DD
1-unlimited GB/Day	FC4-10-LV0VM-248-02-DD	FC4-10-LV0VM-335-02-DD	FC4-10-LV0VM-661-02-DD	FC4-10-LV0VM-285-02-DD	FC4-10-LV0VM-204-02-DD

New Order Example

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

Purchase the following SKU

- 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 Example

Add immediately **15 GB/Day** of Logs for a total of **25 GB/Day** of Logs

As net new

3x FAZ-VM-GB5 (License for adding 5 GB/Day Logs)

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.*

Frequently Asked Questions

When should I use device-based licensing for FortiAnalyzer Cloud?

Use **device-based licensing** when the customer has **FortiGate or FortiWeb** devices. Each device requires **one FortiAnalyzer Cloud device license**.

What is included with a FortiAnalyzer Cloud device license?

A device-based FortiAnalyzer Cloud license includes:

- Log ingestion entitlement (for example, 200 MB/day per FortiGate-70G).
- Default cloud log retention: 3 months for analytics and 12 months for archive.
- Built-in central logging, analytics, reports, dashboards, and SIEM/SOAR capabilities.
- Direct logging to FortiAnalyzer Cloud.
- FortiAnalyzer Cloud automatically allocates the required storage and system resources based on the licensed devices.

When is a GB/day ingestion license required?

A GB/day ingestion license is required when:

- The customer does not have FortiGate or FortiWeb devices.
- Logs are generated by FortiClient, FortiMail, or other supported Fortinet products.
- Logs are generated by third-party devices.
- Additional ingestion capacity is needed beyond the device-based entitlement.

Can device-based and GB/day licenses be used together?

Yes. Device-based licenses and GB/day ingestion licenses can be used together within the same FortiCloud account.

Typical use cases include:

- FortiGate logs using device-based licensing.
- FortiClient, FortiMail, or third-party logs using a shared GB/day ingestion license.
- When FortiGate or FortiWeb logs exceed the default device-based entitlement, the excess log volume is consumed from the shared GB/day ingestion pool.

How do I order more storage for my FortiAnalyzer Cloud?

You do not order additional storage directly. Instead, you increase the log ingestion rate by purchasing a GB/day ingestion subscription (-AZCLD-463). FortiAnalyzer Cloud automatically scales backend storage based on the total licensed ingestion rate to ensure logs are retained according to the configured retention period.

What is the default FortiAnalyzer Cloud storage? Do I need to purchase the FortiAnalyzer Cloud - 463 SKU from the beginning?

The smallest FortiAnalyzer Cloud instance has 500 GB of storage. However, the instance storage size should not be a concern. FortiAnalyzer Cloud automatically scales backend storage based on the entitled log ingestion rate.

You do not need to purchase the -463 (GB/day ingestion) SKU if your devices do not exceed the default log ingestion entitlement.

Is the GB/day ingestion license shared?

Yes. GB/day ingestion capacity is **Shared across all supported log sources** in the same FortiCloud account, not tied to a specific device.

What happens if the customer exceeds their licensed ingestion volume?

If log ingestion exceeds the licensed capacity, logs may be throttled or dropped. Customers should upgrade their device-based entitlement or GB/day subscription ensure continuous and complete logging.

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

Each FortiGate requires its own FAZ cloud subscription.

Do we need to purchase a FortiAI subscription for both FortiAnalyzer HA active and standby units?

Yes. Each device in an HA deployment, including both the active and standby units, must have its own FortiAI subscription.

How does FortiAnalyzer FortiAI Top-Up license work?

The FortiAI base subscription license must be purchased first before you can purchase the FortiAI Top-up license. Without this base subscription, the Top-Up license cannot be activated.

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	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.

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.

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.

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.

When expanding the FortiAnalyzer Cloud entitlement (e.g., from 15GB/day to 50GB/day), will there be any service interruption or data loss?

No. The expansion to support increased log ingestion (measured in GB/day) is carefully managed by the FortiAnalyzer Cloud operations team. There is no need to migrate platforms, so there is no risk of data loss or service disruption.

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

To add FortiAnalyzer High Availability, you can purchase 2 of the same FortiAnalyzer. Each FortiAnalyzer in the HA cluser should also:

- 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 cluser should also:

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

What does Managed FortiAnalyzer Service Provide?

The Managed FortiAnalyzer Service provides proactive operational oversight of the customer's FortiAnalyzer platform. SOCaaS experts continuously monitor and reveiw FortiAnalyzer system health, configuration, and performance to help ensure the platform is running optimally and aligned with best practices.

The service includes:

- Monitoring of FortiAnalyzer system health, capacity, and performance.
- Review of platform configurations to identify misconfigurations or optimization opportunities.
- Expert guidance and recommendations for configuration tuning and operational improvements.
- Proactive identification of issues that could impact stability, scalability, or usability.

The customer's team retains full control of FortiAnalyzer for their own log monitoring and alert triage. Only FortiAnalyzer local system event logs and telemetry are shared for the purpose of this service. Logs collected and stored by FortiAnalyzer from connected devices are not shared, monitored, or analyzed.

This service does not provide security log monitoring, threat detection, investigation, or incident response. Its purpose is to keep the FortiAnalyzer platform itself healthy, properly configured, and operationally ready.

How do I order FortiAnalyzer Supervisor?

There is no separate or special license for FortiAnalyzer Supervisor. You only need a valid FortiCare contract.

Hardware platform guidance:

- A FortiAnalyzer 1000G can typically support up to 12 high-end FortiAnalyzer appliances (3000 series and above).
- For environments with mid- to low-end FortiAnalyzer appliances, a FortiAnalyzer 300G is generally sufficient.

VM platform guidance:

- For supervising high-end FortiAnalyzer appliances, provision at least **16 vCPUs and 64 GB RAM**.
- For mid- to low-end FortiAnalyzer appliances, provision at least **16 vCPUs and 32 GB RAM**.

No additional licenses are required beyond FortiCare.

December 18, 2025 1:05 AM

FAZ-OG-R24-20251218