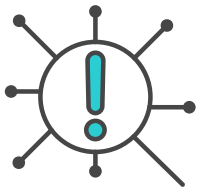

FortiSIEM

Available in

Appliance Virtual Cloud

FortiSIEM is designed to be the backbone of your security operations team, offering capabilities to automatically build an inventory of assets, apply behavioural analytics, and rapidly detect and respond to threats. Its native multi-tenancy architecture, management features, and scalability make it a leading solution for MSSPs. FortiSIEM caters to various customer requirements through different licensing and deployment models, whether on-premise using virtual/hardware appliances or as a cloud-delivered service.

Key aspects of FortiSIEM include:

- Deployment Options: Available in Appliance, Virtual, and Cloud forms.
- Licensing Models: Each licensing model is mutually exclusive and cannot be combined with another:
  - GB Per Day: Licensed by Gigabytes per day, Agent, UEBA, and IOC.
  - Device + EPS: Licensed by Device, Endpoint, Agent, UEBA, IOC, and High Availability.
  - Cloud (SaaS): Licensed by “FortiSIEM Compute Units (FCU)”, Online Storage, and Archive Storage.
  - MSSP PAYG: Licensed by Devices, Agents, and UEBA.
- Capabilities: FortiSIEM offers a wide range of features including:
  - Event Collection and Normalization.
  - Advanced Event Correlation and Compliance Monitoring and Reporting.
  - Security Automation and Response, including Case Management, MITRE ATT&CK Alert Mapping, and Automated Response Actions.
  - Threat Intelligence, including Indicators of Compromise (IOC).
  - Device and Application Discovery.
  - Device Monitoring and Analytics.
  - On-premise and Cloud Monitoring.
  - Configuration Monitoring.
  - Multitenant Support.
- Add-on Features: Certain features like FortiSIEM Automaton Service, advanced agent based Windows / Linux Agent monitoring, UEBA, High Availability and Threat Intelligence can be added on.
- FortiSIEM Manager: Requires FortiSIEM version 6.5.0 or greater

Licensing Options

	CAPEX/PERPETUAL	OPEX/SUBSCRIPTION		FORTISIEM CLOUD	MSSP PAYG
	DEVICE + EPS	DEVICE + EPS	GB PER DAY	SUBSCRIPTION	
DEVICE MONITORING AND ANALYTICS					
Device and Application Discovery	✓	✓	✓	✓	✓
On-premise and Cloud Monitoring	✓	✓	✓	✓	✓
Configuration Monitoring	✓	✓	✓	✓	✓
Event Collection and Normalization	✓	✓	✓	✓	✓
Advanced Event Correlation	✓	✓	✓	✓	✓
Compliance Monitoring and Reporting	✓	✓	✓	✓	✓
PERFORMANCE AND DIGITAL EXPERIENCE MONITORING					
Synthetic Transations	✓	✓	✓	✓	✓
Performance and Availability	✓	✓	✓	✓	✓
SD-WAN/Interface Monitoring	✓	✓	✓	✓	✓
Custom Monitoring (SNMP, SQL)	✓	✓	✓	✓	✓
Netflow Analytics	✓	✓	✓	✓	✓
SECURITY AUTOMATION AND RESPONSE					
Case Management	✓	✓	✓	✓	✓
MITRE ATT&CK Alert Mapping	✓	✓	✓	✓	✓
Remediation Actions	✓	✓	✓	✓	✓
Two-Way Integration with FortiSOAR	✓	✓	✓	✓	✓
Multitenant Support	✓	✓	✓	✓	✓
Security Automation Service	✓	✓	✓		✓
AGENT-BASED MONITORING[1]					
File Integrity Monitoring (FIM)					
Windows Registry Monitoring	Add-on	Add-on	Add-on	✓	Add-on
Active Directory Integration					
INSIDER THREAT MONITORING					
Log-based UEBA	✓	✓	✓	✓	✓
Endpoint-based UEBA					
Remote Worker Monitoring	Add-on	Add-on	Add-on	✓	Add-on
On- and Off-network Endpoint Monitoring					
THREAT INTELLIGENCE					
Indicators of Compromise (IOC)	Add-on	Add-on	Add-on	✓	✓
EPS					
Additional Events per Second (EPS)	Add-on	Add-on	N/A	N/A[2]	Unlimited
TRAINING SERVICES					
NSE 5/FortiSIEM Basic Training - 3 days			FT-FSM		
NSE 7/Advanced Analytics Training (FortiSIEM Advanced - MSSP) - 3 days			FT-ADA		
FortiSIEM Parser Training - 2 days			FT-FSM-PSR		
MULTI-INSTANCE VISIBILITY					
FortiSIEM Manager[3]	Separate Product	Separate Product		Separate Product	Separate Product

1 Agent license requires a device or endpoint license. For example, one Windows Server with FIM requires one device and one agent license.

2 FortiSIEM Cloud EPS is restricted by FortiSIEM Compute Unit resources that has been subscribed to as part of the FortiSIEM Cloud.

3 FortSIEM Manager requires FortiSIEM 6.5.0 or greater. All instances of FortiSIEM managed by FortiSIEM Manager require FortiSIEM 6.5.0 or greater.

GB PER DAY LICENSING	
FORTISIEM GB PER DAY	
FC1-10-SMGS1-1026-02-DD	FortiSIEM Subscription license for 40GB - 99GB Logs per day. Increments of additional 1GB Logs per day. Includes HA Super, FortiCare Premium support.
FC2-10-SMGS1-1026-02-DD	FortiSIEM Subscription license for 100GB - 249GB Logs per day. Increments of additional 1GB Logs per day. Includes HA Super, FortiCare Premium support.
FC3-10-SMGS1-1026-02-DD	FortiSIEM Subscription license for 250GB - 499GB Logs per day. Increments of additional 1GB Logs per day. Includes HA Super, FortiCare Premium support.
FC4-10-SMGS1-1026-02-DD	FortiSIEM Subscription license for 500GB - 999GB Logs per day. Increments of additional 1GB Logs per day. Includes HA Super, FortiCare Premium support.
FC5-10-SMGS1-1026-02-DD	FortiSIEM Subscription license for 1000GB - 1999GB Logs per day. Increments of additional 1GB Logs per day. Includes HA Super, FortiCare Premium support.
FC6-10-SMGS1-1026-02-DD	FortiSIEM Subscription license for 2000GB+ Logs per day. Increments of additional 1GB Logs per day. Includes HA Super, FortiCare Premium support.
FORTISIEM GB UEBA SUBSCRIPTION LICENSE	
FC1-10-SMGS1-334-02-DD	Per UEBA Agent based telemetry Subscription License for 25 - 499 Agents
FC2-10-SMGS1-334-02-DD	Per UEBA Agent based telemetry Subscription License for 500 - 999 Agents
FC3-10-SMGS1-334-02-DD	Per UEBA Agent based telemetry Subscription License for 1000+ Agents
FORTISIEM GB ADVANCED AGENT SUBSCRIPTION LICENSE	
FC1-10-SMGS1-182-02-DD	Per Advanced Agent Subscription License for 25 - 499 Agents. Providing File Integrity Monitoring (Windows, Linux), advanced monitoring and forensics.
FC2-10-SMGS1-182-02-DD	Per Advanced Agent Subscription License for 500 - 999 Agents. Providing File Integrity Monitoring (Windows, Linux), advanced monitoring and forensics.
FC3-10-SMGS1-182-02-DD	Per Advanced Agent Subscription License for 1000+ Agents. Providing File Integrity Monitoring (Windows, Linux), advanced monitoring and forensics.
FORTISIEM GB INDICATORS OF COMPROMISE (IOC) SERVICE	
FC1-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 50GB/Day of Logs)
FC2-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 100GB/Day of Logs)
FC3-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 200GB/Day of Logs)
FC4-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 300GB/Day of Logs)
FC5-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 400GB/Day of Logs)
FC6-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 500GB/Day of Logs)
FC7-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 700GB/Day of Logs)
FC8-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 1000GB/Day of Logs)
FC9-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 2000GB/Day of Logs)
FCA-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 3000GB/Day of Logs)
FCB-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 4000GB/Day of Logs)
FCC-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 5000GB/Day of Logs)
FCD-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 6000GB/Day of Logs)
FCE-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 7000GB/Day of Logs)
FCF-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 8000GB/Day of Logs)
FCG-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 9000GB/Day of Logs)
FCH-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 10000GB/Day of Logs)
FCI-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 15000GB/Day of Logs)
FCJ-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 20000GB/Day of Logs)
FCK-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - 25000GB/Day of Logs)
FCL-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for 1 - Unlimited GB/Day of Logs)

Order Information

Subscription/OPEX SKUs are not stackable. The device, endpoint, agent, and UEBA subscription SKUs are for minimum quantities.

DEVICE + EPS LICENSING				
DEVICES (PLUS 10 EPS POOLED E.G. 10 DEVICE PROVIDES 100 EPS)				
CAPEX		OPEX		MSSP PAYG
QUANTITY	SKU	QUANTITY	SKU	
50	FSM-AIO-BASE[1]	50	FC1-10-FSM98-180-02-DD[2]	
100	FSM-AIO-100-UG	150	FC1-10-FSM98-180-02-DD	
250	FSM-AIO-250-UG	300	FC2-10-FSM98-180-02-DD	
450	FSM-AIO-450-UG	500	FC3-10-FSM98-180-02-DD	See MSSP agreement
950	FSM-AIO-950-UG	1000	FC4-10-FSM98-180-02-DD	
1950	FSM-AIO-1950-UG	2000	FC5-10-FSM98-180-02-DD	
3950	FSM-AIO-3950-UG	4000	FC6-10-FSM98-180-02-DD	
ENDPOINTS (PLUS 2 EPS POOLED E.G. 100 ENDPOINTS PROVIDES 200 EPS)				
CAPEX		OPEX		MSSP PAYG
QUANTITY	SKU	QUANTITY	SKU	
50	FSM-EPD-50-UG	50	FC1-10-FSM98-184-02-DD	
100	FSM-EPD-100-UG	150	FC2-10-FSM98-184-02-DD	
250	FSM-EPD-250-UG	300	FC3-10-FSM98-184-02-DD	
450	FSM-EPD-450-UG	500	FC4-10-FSM98-184-02-DD	
950	FSM-EPD-950-UG	100	FC5-10-FSM98-184-02-DD	See MSSP agreement
1950	FSM-EPD-1950-UG	200	FC6-10-FSM98-184-02-DD	
3950	FSM-EPD-3950-UG	4000	FC7-10-FSM98-184-02-DD	
4950	FSM-EPD-4950-UG	5000	FC8-10-FSM98-184-02-DD	
AGENTS (LOGS AND FIM)				
CAPEX		OPEX		MSSP PAYG
QUANTITY	SKU	QUANTITY	SKU	
50	FSM-AGT-ADV-50-UG	50	FC1-10-FSM98-182-02-DD	
100	FSM-AGT-ADV-100-UG	100	FC2-10-FSM98-182-02-DD	
200	FSM-AGT-ADV-200-UG	200	FC3-10-FSM98-182-02-DD	See MSSP agreement
500	FSM-AGT-ADV-500-UG	500	FC4-10-FSM98-182-02-DD	
1000	FSM-AGT-ADV-1000-UG	1000	FC5-10-FSM98-182-02-DD	
UEBA AGENT TELEMETRY				
CAPEX		OPEX		MSSP PAYG
QUANTITY	SKU	QUANTITY	SKU	
25	FSM-UEBA-25-UG	25	FC1-10-FSM98-334-02-DD	
500	FSM-UEBA-500-UG	500	FC4-10-FSM98-334-02-DD	See MSSP agreement
10000	FSM-UEBA-10000-UG	10000	FC9-10-FSM98-334-02-DD	
ADDITIONAL EPS				
CAPEX		OPEX		MSSP PAYG
QUANTITY	SKU	QUANTITY	SKU	
1	FSM-EPS-100-UG	1	FC1-10-FSM98-183-02-DD	Included

1 You must include FSM-AIO-BASE with all CAPEX/perpetual licenses.

2 A minimum quantity of 50 x FC1-10-FSM98-180-02-DD is required per subscription/OPEX licenses.

Order Information

DEVICE + EPS LICENSING		
FORTIGUARD IOC SERVICE POINTS	**IOC POINT-BASED SKU[1]**	**MSSP PAYG**
1-50	FC1-10-FSM98-149-02-DD	Included
1-100	FC2-10-FSM98-149-02-DD	
1-200	FC3-10-FSM98-149-02-DD	
1-300	FC4-10-FSM98-149-02-DD	
1-400	FC5-10-FSM98-149-02-DD	
1-500	FC6-10-FSM98-149-02-DD	
1-750	FC7-10-FSM98-149-02-DD	
1-1000	FC8-10-FSM98-149-02-DD	
1-1500	FC9-10-FSM98-149-02-DD	
1-2000	FCA-10-FSM98-149-02-DD	
1-3000	FCB-10-FSM98-149-02-DD	
1-4000	FCC-10-FSM98-149-02-DD	
1-4500	FCD-10-FSM98-149-02-DD	
1-5000	FCE-10-FSM98-149-02-DD	
VM-BASED DEPLOYMENT 24X7 FORTICARE CONTRACT	**SUPPORT POINT-BASED SKU[1]**	**MSSP PAYG**
1-50	FC1-10-FSM97-248-02-DD	Included
1-100	FC2-10-FSM97-248-02-DD	
1-200	FC3-10-FSM97-248-02-DD	
1-300	FC4-10-FSM97-248-02-DD	
1-400	FC5-10-FSM97-248-02-DD	
1-500	FC6-10-FSM97-248-02-DD	
1-750	FC7-10-FSM97-248-02-DD	
1-1000	FC8-10-FSM97-248-02-DD	
1-1500	FC9-10-FSM97-248-02-DD	
1-2000	FCA-10-FSM97-248-02-DD	
1-3000	FCB-10-FSM97-248-02-DD	
1-4000	FCC-10-FSM97-248-02-DD	
1-4500	FCD-10-FSM97-248-02-DD	
1-5000	FCE-10-FSM97-248-02-DD	

1 One “device” or 2 “endpoints” or 3 “Advanced Agents – Log & FIM” or 10 “Advanced Agents - UEBA Telemetry” equals 1 point. Additional EPS does not require additional points.

DEVICE + EPS LICENSING		
FORTISIEM HIGH AVAILABILITY SUPER	HA SUPER POINT-BASED SKU[1]	MSSP PAYG
1-50	FC1-10-FSM98-593-02-DD	Included
1-100	FC2-10-FSM98-593-02-DD	
1-200	FC3-10-FSM98-593-02-DD	
1-300	FC4-10-FSM98-593-02-DD	
1-400	FC5-10-FSM98-593-02-DD	
1-500	FC6-10-FSM98-593-02-DD	
1-750	FC7-10-FSM98-593-02-DD	
1-1000	FC8-10-FSM98-593-02-DD	
1-1500	FC9-10-FSM98-593-02-DD	
1-2000	FCA-10-FSM98-593-02-DD	
1-3000	FCB-10-FSM98-593-02-DD	
1-4000	FCC-10-FSM98-593-02-DD	
1-4500	FCD-10-FSM98-593-02-DD	
1-5000	FCE-10-FSM98-593-02-DD	
1-7500	FCF-10-FSM98-593-02-DD	
1-10000	FCG-10-FSM98-593-02-DD	
1-20000	FCK-10-FSM98-593-02-DD	
1-50000	FCP-10-FSM98-593-02-DD	
1-100000	FCU-10-FSM98-593-02-DD	
1-100000+	FCY-10-FSM98-593-02-DD	
HARDWARE-BASED DEPLOYMENT 24X7 FORTICARE CONTRACT[2]	SUPPORT POINT-BASED SKU[1]	MSSP PAYG
1-50	FC1-10-FSM99-240-02-DD	
1-100	FC2-10-FSM99-240-02-DD	
1-200	FC3-10-FSM99-240-02-DD	
1-300	FC4-10-FSM99-240-02-DD	
1-400	FC5-10-FSM99-240-02-DD	
1-500	FC6-10-FSM99-240-02-DD	
1-750	FC7-10-FSM99-240-02-DD	
1-1000	FC8-10-FSM99-240-02-DD	
1-1500	FC9-10-FSM99-240-02-DD	
1-2000	FCA-10-FSM99-240-02-DD	
1-3000	FCB-10-FSM99-240-02-DD	
1-4000	FCC-10-FSM99-240-02-DD	
1-4500	FCD-10-FSM99-240-02-DD	
1-5000	FCE-10-FSM99-240-02-DD	

1 One “device” or 2 “endpoints” or 3 “Advanced Agents – Log & FIM” or 10 “Advanced Agents - UEBA Telemetry” equals 1 point. Additional EPS does not require additional points.

2 When purchased with perpetual license SKUs, hardware appliances require a hardware base license SKU for the appropriate appliance. For example, if ordering the FSM-3600G, the base SKU would be FSM-AIO-3600-BASE instead of the FSM-AIO-BASE (VM perpetual base license). The 500F/500G Collector Hardware Appliance does not require a base license SKU. Only use the Hardware-based Deployment 24×7 FortiCare Contract” if applied to license on a FSM-2000F/G, FSM-2200G, FSM-3500G, or FSM-3600G hardware appliance.

HARDWARE APPLIANCES			
HARDWARE MODEL	**FSM-500G COLLECTOR**	**FSM-2200G**	**FSM-3600G**
EPS Supported	5000	20000[1]	50000[1]
HW Product	FSM-500G	FSM-2200G	FSM-3600G
FortiCare Premium Support[2]	FC-10-FSM5G-247-02-DD	FC-10-FM22G-247-02-DD	FC-10-FM36G-247-02-DD
Next Day Delivery Premium RMA Service (Requires FortiCare Premium or FortiCare Elite)	FC-10-FSM5G-210-02-DD	FC-10-FM22G-210-02-DD	FC-10-FM36G-210-02-DD
4-Hour Hardware Delivery Premium RMA Service (Requires FortiCare Premium or FortiCare Elite)	FC-10-FSM5G-211-02-DD	FC-10-FM22G-211-02-DD	FC-10-FM36G-211-02-DD
4-Hour Hardware and Onsite Engineer Premium RMA Service (Requires FortiCare Premium or FortiCare Elite)	FC-10-FSM5G-212-02-DD	FC-10-FM22G-212-02-DD	FC-10-FM36G-212-02-DD
Secure RMA Service	FC-10-FSM5G-301-02-DD	FC-10-FM22G-301-02-DD	FC-10-FM36G-301-02-DD
Perpetual Base License SKU**	N/A	FSM-AIO-2200-BASE	FSM-AIO-3600-BASE
HARDWARE BASE LICENSE[3]	**CAPEX**	**OPEX**	**MSSP PAYG**
100 devices and 1000 EPS all-in-one perpetual license for FortiSIEM FSM-2000. Does not include Maintenance and Support.	FSM-AIO-2000-BASE		
100 devices and 1000 EPS all-in-one perpetual license for FortiSIEM FSM-2200G. Does not include Maintenance and Support.	FSM-AIO-2200-BASE		
500 devices and 5000 EPS all-in-one perpetual license for FortiSIEM FSM-3500 series. Does not include Maintenance and Support.	FSM-AIO-3500-BASE		
500 devices and 5000 EPS all-in-one perpetual license for FortiSIEM FSM-3600 series. Does not include Maintenance and Support.	FSM-AIO-3600-BASE		

1 Supported maximum EPS on FSM-2000G, FSM-2200G, FSM-3500G, and FSM-3600G requires collectors. Refer to the FortiSIEM Sizing Guide for more information.

2 FortiCare Support on Hardware Appliances FC10-FSM[XX]-247-02-DD does not include FortiSIEM Product support. FortiCare Product support is required for VM based deployments (FC[X]-10-FSM97-248-02-DD) and HW based deployments (FC[X]-10-FSM99-240-02-DD).

3 One “device” or 2 “endpoints” or 3 “Advanced Agents – Log & FIM” or 10 “Advanced Agents - UEBA Telemetry” equals 1 point. Additional EPS does not require additional points.

FORTISIEM MANAGER		
FortiSIEM Manager	FC1-10-SMMGR-574-02-DD	Subscription license for FortiSIEM Manager providing centralized incident, management, and status of independent FortiSIEM instances. Requires a Minimum Qty. of five to monitor five separate FortiSIEM Instances, max of 50 Instances. Includes Maintenance & Support.

FORTISIEM CLOUD			
REGION	**PRODUCT**	**SKU**	**DESCRIPTION**
Region A	**FortiSIEM Compute Units**	FC2-10-SMCLD-543-02-DD	10 FortiSIEM Compute Units (FCU). Quantity 1 only. Deployment regions A, refer to datasheet for region locations. Annual Subscription. Includes FortiCare Premium Support.
		FC3-10-SMCLD-543-02-DD	10 FortiSIEM Compute Units (FCU). Minimum quantity of 2 and maximum 4. Deployment regions A, refer to datasheet for region locations. Region A Annual Subscription. Includes FortiCare Premium Support.
		FC4-10-SMCLD-543-02-DD	10 FortiSIEM Compute Units (FCU). Minimum quantity of 5 and maximum 60. Deployment regions A, refer to datasheet for region locations. Annual Subscription. Includes FortiCare Premium Support.
	FortiSIEM Cloud Online Storage	FC-10-SMCLD-541-02-DD	500GB Online storage. Deployment regions A, refer to datasheet for region locations. Requires minimum quantity of 1 with initial FortiSIEM Compute Unit order. Annual Subscription.
	FortiSIEM Cloud Archive Storage	FC-10-SMCLD-542-02-DD	Optional Archive storage. 500GB of Archive storage per unit. Deployment regions A, refer to datasheet for region locations. Annual Subscription.
Region B	**FortiSIEM Compute Units**	FC2-10-SMCLB-543-02-DD	10 FortiSIEM Compute Units (FCU). Deployment regions B, refer to datasheet for region locations. Quantity 1 only. Annual Subscription. Includes FortiCare Premium Support.
		FC3-10-SMCLB-543-02-DD	10 FortiSIEM Compute Units (FCU). Deployment regions B, refer to datasheet for region locations. Minimum quantity of 2 and maximum 4. Annual Subscription. Includes FortiCare Premium Support.
		FC4-10-SMCLB-543-02-DD	10 FortiSIEM Compute Units (FCU). Deployment regions B, refer to datasheet for region locations. Minimum quantity of 5 and maximum 60. Annual Subscription. Includes FortiCare Premium Support.
	FortiSIEM Cloud Online Storage	FC-10-SMCLB-541-02-DD	500GB online storage. Deployment regions B, refer to datasheet for region locations. Requires minimum quantity of 1 with initial FortiSIEM Compute Unit order. Annual Subscription.
	FortiSIEM Cloud Archive Storage	FC-10-SMCLB-542-02-DD	Archive 500GB storage. Deployment regions B, refer to datasheet for region locations. Annual Subscription.

SECURITY AUTOMATION SERVICE	
SKU	**DESCRIPTION**
FC1-10-SIMPC-1055-02-DD	FortiSIEM Automation Service providing one concurrent playbook execution capacity. Increase quantity to enable additional concurrent playbook processing. Maximum quantity of 10.

Example Calculations of FortiSIEM Points

If using the "Device + EPS" licensing model, the below tables provide examples of how to calculate the number of points that are required for FortiCare Support and the FortiGuard IOC service.

CAPEX						
QUANTITY	SKU	ENTITLEMENT	EPS	TOTAL ENTITLEMENT	CALCULATION	POINTS
1	FSM-AIO-BASE	50	500	150 Devices	150 * 1 =	150
1	FSM-AIO-100-UG	100	1000			
2	FSM-EPD-50-UG	100	200	200 Endpoints	200 / 2 =	100
1	FSM-EPD-100-UG	100	200			
1	FSM-AGT-ADV-100-UG	100	0	100 Agents	100 / 3 =	34
2	FSM-UEBA-25-UG	50	0	550 UEBA	550 / 10 =	55
1	FSM-UEBA-500-UG	500	0			
3100	FSM-EPS-100-UG	3100	3100	3100 EPS + 1900 EPS = 5000	0	0
		TOTAL	**5000**		**TOTAL**	**339**
1	FC5-10-FSM97-248-02-DD	Support for up to 400 points				
1	FC5-10-FSM98-149-02-DD	IOC Service for up to 400 points				

OPEX						
QUANTITY	SKU	ENTITLEMENT		TOTAL ENTITLEMENT	CALCULATION	POINTS
150	FC2-10-FSM98-180-02-DD	150	1500	150 Devices	150 * 1 =	150
200	FC2-10-FSM98-184-02-DD	200	400	200 Endpoints	200 / 2 =	100
100	FC2-10-FSM98-182-02-DD	100	0	100 Agents	100 / 3 =	34
550	FC4-10-FSM98-334-02-DD	50	0	550 UEBA	550 / 10 =	55
3100	FC1-10-FSM98-183-02-DD	3100	3100	3100 EPS + 1900 EPS = 5000	0	0
		TOTAL	**5000**		**TOTAL**	**339**
1	FC5-10-FSM97-248-02-DD	Support for up to 400 points				
1	FC5-10-FSM98-149-02-DD	IOC Service for up to 400 points				

SUPPORT AND IOC SERVICE		
Support SKU for 339 points	FC5-10-FSM97-248-02-DD	24×7 FortiCare Contract (1 - 400 points) for FortiSIEM Software deployments. 1 "Device" or 2 "End points" or 3 "Advanced Agents – Log & FIM" or 10 "Advanced Agents - UEBA Telemetry" equals 1 point.
IOC Service SKU for 339 points	FC5-10-FSM98-149-02-DD	(1 - 400 Points) FortiSIEM Indicators of Compromise

Fortinet Training and Certification

FCP – FortiSIEM Analyst Training and Certification

Learn how to use FortiSIEM to search, enrich, and analyze events from customers in a managed security service provider (MSSP) organization. You will learn how to perform real-time and historical searches and build advanced queries. You will also learn how to perform analysis and remediation of security incidents.

Other Technical:

FortiSIEM Administrator Training

Learn about FortiSIEM initial configurations and architecture, and the discovery of devices on the network. You will also learn how to collect performance information and aggregate it with syslog data to enrich the overall view of the health of your environment, use the configuration database to greatly facilitate compliance audits, and integrate FortiSIEM into your network awareness infrastructure.

FortiSIEM Parser Training

Learn how to create custom parsers to extend the integration capability of FortiSIEM to a wider range of devices and custom applications. You will learn how parsers recognize the type of device or application that sent the data, extract and save key information from the log, and map the device type and log information to an event type.

Course Details

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

FortiSIEM Analyst: https://training.fortinet.com/local/staticpage/view.php?page=library_fortisiem-analyst

FortiSIEM Administrator: https://training.fortinet.com/local/staticpage/view.php?page=library_fortisiem-administrator

FortiSIEM Parser: https://training.fortinet.com/local/staticpage/view.php?page=library_fortisiem-parser

Training Offering

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

Frequently Asked Questions

How is FortiSIEM licensed?

FortiSIEM provides OPEX (Subscription), CAPEX (Perpetual) and MSSP PAYG options.

CAPEX has one licensing model that is based on Devices & EPS and is available both as software and hardware deployments.

OPEX has three licensing models, one based on Devices & EPS, the other based on GB per day. The third licensing model is the MSSP PAYG option, available to qualifying MSSP's, please contact your local Fortinet Sales Team.

The FortiSIEM Cloud is licensed on FortiSIEM Compute Units (FCU), Online and Archive storage.

With the "Device + EPS" licensing model, what is the difference between a Devices and an Endpoint?

A Device provides 10 EPS and an Endpoint provides 2 EPS, however FortiSIEM does not differentiate what type of device, service or application the Device or Endpoint license is used to monitor.

Can the different license models be combined?

No, the license models are mutually exclusive.

For example GB per day cannot be used with the MSSP PAYG licensing, nor can Agents purchased on one model cannot be used with another model.

Is the GB per day licensing model available as a Perpetual License?

No, the GB per day licensing is available as Subscription only.

Is the GB per day licensing model supported on HW Appliances?

No, the GB per day licensing is not supported with the FortiSIEM HW appliances.

Is High Availability Super available with the GB per day licensing?

High Availability is included with the price of the GB per day licensing, this feature does not need to be licensed separately.

What version of FortiSIEM supports the GB per day licensing?

Please check the FortiSIEM 7.2.x release note for support of GB per day licensing. All version of FortiSIEM 7.3.0 onwards support GB per day licensing.

How many monitored devices does the GB per day licensing support?

The number of devices monitored or in the FortiSIEM CMDB is not limited by the GB per day licensing.

Is the GB per day based on the compressed storage or raw logs?

GB per day calculation is based on the uncompressed, raw log size within FortiSIEM.

Does the GB per day license include support?

Yes, FortiCare Support is included with the GB per day license.

What version of FortiSIEM supports the Automation Service?

Version 7.4.0 or later.

Is FortiSIEM Automation Service available for on-premises and FortiSIEM Cloud?

FortiSIEM on-premises is currently supported. FortiSIEM Cloud will be supported at a later date.

Where is FortiSIEM Automation Service hosted?

FortiSIEM Automation Service is serviced from within FortiCloud and from the US region.

What ports does FortiSIEM Automation Service use?

FortiSIEM communicated over HTTPS port 443 to FortiSIEM Automation Service. No inbound communication is required. Because the FortiSIEM Automation Service requires Internet connectivity, it will not work with offline/air gapped FortiSIEM deployments. A separate FortiSOAR is recommended for these scenarios.

How is the Automation Service licensed?

The Automation Service is licensed by playbook execution capacity and concurrency. Each increment can support approximately 3000 playbooks per day (assuming a 24 hour day and a 30-second playbook average runtime) using a single FortiSIEM Automation Service concurrency. Additional concurrency and capacity can be added by increasing the quantity.

What is FortiSIEM Cloud?

FortiSIEM Cloud is a hosted and dedicated FortiSIEM cluster where the platform availability and upgrades are managed by Fortinet.

What is an FCU in FortiSIEM Cloud?

FortiSIEM Compute Units (FCU) provide a licensed daily average of 10 FCU to 1K Events Per Second (EPS). A FCU provides platform capacity for FortiSIEM Cloud instance, which is dedicated to a specific customer.

How do I size FortiSIEM Cloud with FCU's?

FortiSIEM Cloud is licensed using FortiSIEM Compute Units (FCU) and provides the performance characteristics needed to meet customer's Events Per Second (EPS) ingest requirements. FortiSIEM Compute Units (FCU), where 10 FCU (1 x FC[1-3]-10-SMCLD-543-02-DD) provides 1000 EPS ingestion of events, therefore 50 FCU provides an ingestion rate of 5000 EPS. A range of other factors may affect performance, such as custom rules; reporting overhead; third-party integrations; and user interface processing. Customers can purchase additional FCU to provide additional system performance to meet their requirements.

What is the minimum FortiSIEM Cloud?

The minimum requirement is quantity 1 x FC2-10-SMCLD-543-02-DD (10 FortiSIEM Compute Units (FCU) and quantity 1 x FC-10-SMCLD-541-02-12 (500GB online storage). The minimum recommended FortiSIEM Compute Units (FCU) is 20 (qty >= 2 x FC-10-SMCLD-543-02-12).

Is there a maximum FCU count?

Yes, there is a maximum of 600 FCU (quantity 60 x FC4-10-SMCLD-543-02-DD).

Is there a maximum Online Storage count?

Yes, there is a maximum of 60TB of online storage (quantity 120 x FC-10-SMCLD-541-02-12).

What regions can FortiSIEM Cloud be deployed to?

Region A:

North America	Europe	Middle East	Asia Pacific
Canada Central	France - Paris	United Arab Emirates	Australia - Sydney
USA East - Northern Virginia	Germany - Frankfurt		India - Mumbai
USA East - Ohio	Ireland		Singapore
USA West - Oregon	Italy - Milan		
	UK - London		
	Sweden - Stockholm		

Region B:

South America	Africa	Europe	Middle East	Asia Pacific
Brazil - Sao Paolo	South Africa	Zurich	Bahrain	Hong Kong

Cheat Sheet

The Space

SIEM (Security Information and Event Management) space is a dynamic landscape that empowers organizations to proactively detect cyber threats. SIEM solutions provide centralized monitoring, analysis, and correlation of security event data from various sources, including network devices, applications, and endpoints. Leveraging advanced analytics, SIEM helps identify anomalous behavior, potential breaches, and threats. By streamlining incident detection and compliance efforts, SIEM solutions offer comprehensive security intelligence to help safeguard against evolving cyber risks.

Ordering Guide

Product Offerings:

- **OPEX:** There are two licensing models; the "Device + EPS" and "GB per day" are subscription/term licenses. Typically used with VM deployments.
- **CAPEX:** HW appliances selected by EPS and event retention requirements. Device, endpoints, agents, UEBA, and EPS can be purchased with a perpetual license. IoC, Manager, and support are on subscription/term licenses. Typically used with VM and HW deployments.
- **MSSP PAYG:** Annual program fee. Device, agents, and UEBA usage are billed in arrears. Support, IoC, and unlimited EPS are included with annual program fee. VM-based deployments.
- **Cloud:** Licensed by "FortiSIEM Compute Units", Online storage and Archived storage rather than devices, endpoints, agents, UEBA, EPS used by the VM or HW licensing. Support is included as part of the "FortiSIEM Compute Units" license. As more features are used within FortiSIEM, this will produce more event logs, increase the load, and consume licensed compute and storage resources.

Product Lineup

FortiSIEM is a single product with licensed features. It is not licensed on number of VMs deployed, rather devices and number of events monitored.

- **HW appliances** require a software base license.
- **VM appliances** are not licensed and customers can deploy as many VMs as needed.
- **Product license** is based on devices, endpoints, agents, UEBA telemetry via an agent, and events per second (EPS).
- **FortiSIEM Cloud** provides a turnkey solution allowing customers to use the platform without any of the overhead of platform management or upgrades. Each FortiSIEM Cloud provides an isolated instance of FortiSIEM and is available in select geographical regions. Licensing is simplified, providing an all-in-one license with no separate Device, EPS, Agents or UEBA licensing requirements.

Major Highlights

- Scalable platform with distributed real-time correlation (patented).
- Thousands of built-in rules and reports for fast return on investment.
- Built-in NOC and SOC capabilities. Discovers the device and applications and starts to monitor device for performance as well as events (security).
- Built-in CMDB providing understanding of devices and their configuration on the network.
- Integrated UEBA capabilities using agent telemetry to monitor devices on and off the network.
- Strong support for the Fortinet portfolio of products.

FSM-OG-R23-20250818