ORDERING GUIDE

FortiSIEM

Product Offerings

	LICENSING OPTIONS			
	CAPEX/PERPETUAL	OPEX/SUBSCRIPTION	FORTISIEM CLOUD SUBSCRIPTION	MSSP PAYG
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	✓	✓	✓	✓
Automated Response Actions	✓	✓	✓	✓
Two-Way Integration with FortiSOAR	✓	✓	✓	✓
Multitenant Support	✓	✓	✓	✓
Agent-based Monitoring*				
File Integrity Monitoring (FIM) Windows Registry Monitoring Active Directory Integration	Add-on	Add-on	✓	Add-on
Insider Threat Monitoring				
Log-based UEBA	✓	✓	✓	✓
Endpoint-based UEBA Remote Worker Monitoring On- and Off-network Endpoint Monitoring	Add-on	Add-on	✓	Add-on
Threat Intelligence				
Indicators of Compromise (IOC)	Add-on	Add-on	✓	✓
EPS				
Additional Events per Second (EPS)	Add-on	Add-on	Unlimited***	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**	Separate Product	Separate Product	Separate Product	Separate Product

* Agent license requires a device or endpoint license. For example, one Windows Server with FIM requires one device and one agent license.
**FortSIEM Manager requires FortiSIEM 6.5.0 or greater. All instances of FortiSIEM managed by FortiSIEM Manager require FortiSIEM 6.5.0 or greater.
***FortiSIEM Cloud EPS is restricted by FortiSIEM Compute Unit resources that has been subscribed to as part of the FortiSIEM Cloud.

ORDER INFORMATION

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

LICENSING OPTIONS				
Devices (plus 10 EPS pooled e.g. 10 device provides 100 EPS)				
CAPEX		OPEX		MSSP PAYG
Quantity	SKU	Quantity	SKU	
50	FSM-AIO-BASE*	50	FC1-10-FSM98-180-02-DD**	See MSSP agreement
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	
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	See MSSP agreement
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	
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	See MSSP agreement
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	
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	See MSSP agreement
500	FSM-UEBA-500-UG	500	FC4-10-FSM98-334-02-DD	
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

* You must include FSM-AIO-BASE with all CAPEX/perpetual licenses.
** A minimum quantity of 50 x FC1-10-FSM98-180-02-DD is required per subscription/OPEX licenses.

ORDER INFORMATION

LICENSING OPTIONS		
FortiGuard IOC Service Points	**IOC Point-based SKU***	**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 24×7 FortiCare Contract	**Support Point-based SKU***	**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 “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.

ORDER INFORMATION

LICENSING OPTIONS		
Hardware-based Deployment 24×7 FortiCare Contract*	**Support Point-based SKU****	**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	

HARDWARE APPLIANCES					
Hardware Model	**FSM-500F collector**	**FSM-500G collector**	**FSM-2000F**	**FSM-2000G**	**FSM-3500G**
EPS Supported	5000	5000	15000***	15000***	40000***
HW Product	FSM-500F	FSM-500G	FSM-2000F	FSM-2000G	FSM-3500G
FortiCare Premium Support****	FC-10-FSM04-247-02-DD	FC-10-FSM5G-247-02-DD	FC-10-FSM02-247-02-DD	FC-10-FSM2G-247-02-DD	FC-10-FSM3G-247-02-DD
Next Day Delivery Premium RMA Service (Requires FortiCare Premium)	FC-10-FSM04-210-02-DD	FC-10-FSM5G-210-02-DD	FC-10-FSM02-210-02-DD	FC-10-FSM2G-210-02-DD	FC-10-FSM3G-210-02-DD
4-Hour Hardware Delivery Premium RMA Service (Requires FortiCare Premium)	FC-10-FSM04-211-02-DD	FC-10-FSM5G-211-02-DD	FC-10-FSM02-211-02-DD	FC-10-FSM2G-211-02-DD	FC-10-FSM3G-211-02-DD
4-Hour Hardware and Onsite Engineer Premium RMA Service (Requires FortiCare Premium)	FC-10-FSM04-212-02-DD	FC-10-FSM5G-212-02-DD	FC-10-FSM02-212-02-DD	FC-10-FSM2G-212-02-DD	FC-10-FSM3G-212-02-DD
Secure RMA Service	FC-10-FSM04-301-02-DD	FC-10-FSM5G-301-02-DD	FC-10-FSM02-301-02-DD	FC-10-FSM2G-301-02-DD	FC-10-FSM3G-301-02-DD
Perpetual Base License SKU**	N/A	N/A	FSM-AIO-2000-BASE	FSM-AIO-2000-BASE	FSM-AIO-3500-BASE

Hardware Base License**	**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		
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		

* When purchased with perpetual license SKUs, hardware appliances require a hardware base license SKU for the appropriate appliance. For example, if ordering the FSM-3500G, the base SKU would be FSM-AIO-3500-BASE instead of the FSM-AIO-BASE (VM perpetual base license). The 500F 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 or FSM-3500G hardware appliance.
** 1 "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.
*** Supported maximum EPS on FSM-2000F, FSM-2000G, and FSM-3500G requires collectors. Refer to the FortiSIEM Sizing Guide for more information.
**** 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).

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		
Product	**SKU**	**Description**
FortiSIEM Compute Units	FC-10-SMCLD-543-02-12	10 FortiSIEM Compute Units (FCU). Minimum quantity of 50 FCU. Annual Subscription. Includes 24×7 FortiCare Support.
FortiSIEM Cloud Online Storage	FC-10-SMCLD-541-02-12	Additional 500GB online storage. Requires minimum quantity of 1 with initial FortiSIEM Compute Unit order. Annual Subscription.
FortiSIEM Cloud Archive Storage	FC-10-SMCLD-542-02-12	Archive 500GB storage. Annual Subscription.

FREQUENTLY ASKED QUESTIONS

How is FortiSIEM licensed?

FortiSIEM provides OPEX, CAPEX and MSSP PAYG options. OPEX and CAPEX licenses are based on devices, endpoints, agents, UEBA Telemetry, and FortiGuard IOC feed. For MSSP PAYG licensing, please contact your local Fortinet Sales Team.

How is FortiSIEM licensed?

FortiSIEM provides OPEX, CAPEX and MSSP PAYG options. OPEX and CAPEX licenses are based on devices, endpoints, agents, UEBA Telemetry, and FortiGuard IOC feed. For MSSP PAYG licensing, please contact your local Fortinet Sales Team. FortiSIEM Cloud is licensed on FortiSIEM Compute Units (FCU), Online storage and Archive storage.

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?

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. 10 x FCU provides approximately 1000 EPS for ingesting. 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 5 x FC-10-SMCLD-543-02-12 (10 FortiSIEM Compute Units (FCU) and quantity 1 x FC-10-SMCLD-541-02-12 (500GB online storage).

Is there a maximum FCU count?

Yes there is a maximum of 250 x FCU (quantity 25 x FC-10-SMCLD-543-02-12).

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				

CHEAT SHEET

The Space

Visibility and threat detection in a multivendor environment becomes challenging due to multiple consoles and lack of correlation. Additionally the data (logs) generated required for compliance, audit, and investigation are not retained without a central logging solution. SIEM provides central storage, reporting, and detection of threats using logs.

More customers are choosing MSSP services rather than owning a SIEM.

Ordering Guide

Product Offerings:

- **OPEX:** device, endpoints, agents, UEBA, EPS, IoC, Manager, and support are on 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:** all features (e.g. device, endpoints, agents, UEBA, EPS) and support are included as part of "FortiSIEM Compute" license. Feature use will produce telemetry and events, which will 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.
- Multitenancy support and scalability to support MSSPs.

FORTINET

www.fortinet.com

FSM-OG-R7-20220713