

ORDERING GUIDE

# FortiSIEM

## Product Offerings

	LICENSING OPTIONS		
	CAPEX/PERPETUAL	OPEX/SUBSCRIPTION	MSSP PAYG
<b>Device Monitoring and Analytics</b>			
Device and Application Discovery	☑	☑	☑
On-Premise and Cloud Monitoring	☑	☑	☑
Configuration Monitoring	☑	☑	☑
Event Collection and Normalization	☑	☑	☑
Advanced Event Correlation	☑	☑	☑
Compliance Monitoring and Reporting	☑	☑	☑
<b>Performance and Digital Experience Monitoring</b>			
Synthetic Transactions	☑	☑	☑
Performance and Availability	☑	☑	☑
SD-WAN/Interface Monitoring	☑	☑	☑
Custom Monitoring (SNMP, SQL)	☑	☑	☑
Netflow Analytics	☑	☑	☑
<b>Security Automation and Response</b>			
Case Management	☑	☑	☑
MITRE ATT&CK Alert Mapping	☑	☑	☑
Automated Response Actions	☑	☑	☑
Two-Way Integration with FortiSOAR	☑	☑	☑
Multitenant Support	☑	☑	☑
<b>Agent-based Monitoring*</b>			
File Integrity Monitoring (FIM)			
Windows Registry Monitoring	Add-on	Add-on	Add-on
Active Directory Integration			
<b>Insider Threat Monitoring</b>			
Log-based UEBA	☑	☑	☑
Endpoint-based UEBA			
Remote Worker Monitoring	Add-on	Add-on	Add-on
On- and Off-network Endpoint Monitoring			
<b>Threat Intelligence</b>			
Indicators of Compromise (IOC)	Add-on	Add-on	☑
<b>EPS</b>			
Additional Events per Second (EPS)	Add-on	Add-on	Unlimited
<b>Training Services</b>			
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	

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

## 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.



## ORDER INFORMATION

LICENSING OPTIONS		
FortiGuard IOC Service Points	IOC Point-based SKU*	MSSP PAYG
1-50	FC1-10-FSM98-149-02-DD	
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	Included
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*	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	Included
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 "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 24x7 FortiCare Contract*	Support Point-based SKU**		MSSP PAYG
1-50	FC1-10-FSM97-248-02-DD		
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		
HARDWARE APPLIANCES			
Hardware Model	FSM-500F collector Up to 5000 EPS supported	FSM-2000F Up to 15000 EPS supported***	FSM-3500G Up to 40000 EPS supported***
HW Product	FSM-500F	FSM-2000F	FSM-3500G
24x7 FortiCare Contract	FC-10-FSM04-247-02-DD	FC-10-FSM02-247-02-DD	FC-10-FSM3G-247-02-DD
Next Day Delivery Premium RMA Service (Requires 24x7 or ASE FortiCare)	FC-10-FSM04-210-02-DD	FC-10-FSM02-210-02-DD	FC-10-FSM3G-210-02-DD
4-Hour Hardware Delivery Premium RMA Service (Requires 24x7 or ASE FortiCare)	FC-10-FSM04-211-02-DD	FC-10-FSM02-211-02-DD	FC-10-FSM3G-211-02-DD
4-Hour Hardware and Onsite Engineer Premium RMA Service (Requires 24x7 or ASE FortiCare)	FC-10-FSM04-212-02-DD	FC-10-FSM02-212-02-DD	FC-10-FSM3G-212-02-DD
Secure RMA Service	FC-10-FSM04-301-02-DD	FC-10-FSM02-301-02-DD	FC-10-FSM3G-301-02-DD
Perpetual Base License SKU**	N/A	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-2000F. Does not include Maintenance & Support	FSM-AIO-2000-BASE		
500 devices and 5000 EPS all-in-one perpetual license for FortiSIEM FSM-3500 series. Does not include Maintenance & 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 24x7 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 and FSM-3500G requires collectors. Refer to the [FortiSIEM Sizing Guide](#) for more information.



## 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 to calculate FortiSIEM support points?

FortiSIEM uses a simple formula to calculate the points needed for Support and the IOC service:

1 Support Point = 1 × 10 EPS Device

1 Support Point = 2 × 2 EPS Device

1 Support Point = 3 x Agents

1 Support Point = 10 x UEBA

1 Support Point = Additional EPS does not require additional support points.

The following provides an example support point calculation and SKUs:

**Bill of Material Requirements:** 150 devices, 200 endpoint devices, 100 agents, 550 UEBA, 5K EPS. 1 year software support and 1 year 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
<b>TOTAL</b>			<b>5000</b>		<b>TOTAL</b>	<b>339</b>
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	EPS	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
<b>TOTAL</b>			<b>5000</b>		<b>TOTAL</b>	<b>339</b>
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						
<b>Support SKU for 339 points</b>	FC5-10-FSM97-248-02-DD	24x7 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.				
<b>IOC Service SKU for 339 points</b>	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, 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 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.

### Where to Find More Info

- [FortiSIEM and MITRE ATT&CK Demo](#)
- [Public UEBA Demo](#)
- [Public Overview Video](#)
- [What's New in 6.2.0](#)

### 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).

### 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.

### Main Competitors

- **Splunk:** flexible platform but also complex. Does not have a scalable real-time correlation engine. Lacks out-the-box content, CMDB, and performance monitoring. Expensive.
- **IBM QRadar:** complex architecture with multiple databases. Expensive. No NOC or CMDB features.
- **Exabeam:** moved from UEBA space to SIEM. Strong on UEBA. Expensive. Complex architecture. Device support depth is not comprehensive.



[www.fortinet.com](http://www.fortinet.com)