SERVICE DESCRIPTION
FORTISIEM™ CLOUD

1. Introduction

FortiSIEM Cloud is a cloud-based SaaS-hosted analytics-powered security and log management service (the "Service") for supported Fortinet security products (the "Supported Products"), as communicated by Fortinet in applicable product data sheets, release notes and the FortiSIEM "External System Configuration Guide" documentation.

The Service is hosted on the FortiCloud™ service portal whose features, deliverables and terms of use are described in the then-current FortiCloud service description made available at https://support.fortinet.com/Information/DocumentList.aspx (the "FortiCloud Service Description"). The terms of the FortiCloud Service Description are incorporated herein by reference and in the event of a conflict, this service description shall prevail over the FortiCloud Service Description.

2. Service Features and Deliverables

The Service will be made available twenty-four (24) hours a day, seven (7) days a week and available in various regional secure datacenters that enable Customers to keep their data within defined geographic boundaries. The Service does not share any Customer logs or configurations between regional datacenter instances.

The following Service features are included:

- Dedicated FortiSIEM cloud instance.
- Service availability target of 99.9% of the FortiSIEM Cloud instance
- Dashboarding of event/log data.
- Analytical reporting of event/log data.
- Incident detection based on FortiSIEM rules.
- Configuration Management Database (CMDB) of supported and discovered devices and applications.
- Log retention based on storage subscription levels.
- Indicators of compromise from FortiGuard service.
- FortiCare™ Premium support, as outlined in the then-current Fortinet support policies and service description, available on the Support Portal or other site as designated by Fortinet.

Customer may benefit from said features for the Supported Products without the need for additional hardware, software, or management overhead to be deployed on premise.

The Service is licensed based on FortiSIEM Compute Units ("FCU"),where 10 FCU (1 x FC-10-SMCLD-543-02-DD) provides 1000 EPS ingestion of events, therefore 50 FCU provides an ingestion rate of 5000 EPS.

The licensed FCUs provide an entitlement of system resources (e.g. CPUs, memory, disk throughput and IOPS) that will be applied by Fortinet in a combination that they deem will provide performance capable of ingesting EPS at the typical rate of 1,000 EPS with an average 700 bytes per event per 10 FCU.

Events per Second ("EPS") of ingested data is often used as a metric for estimating the total FCU requirements expected to maintain system performance. Many factors contribute to the resource load on a FortiSIEM instance including average event size, custom rules, reporting overhead, third party integrations, number of users modelled within User and Entity Behavior Analytics ("UEBA"), Machine Learning jobs, number of agents deployed and concurrent number of interactive users using the Service. Additionally, system performance is subjective. Therefore EPS-to-FCU ratios are provided for guidance and are not a guarantee of performance or responsiveness in your environment. You may need to purchase a greater ratio of FCU to ingested EPS to maintain system performance.

3. Customer Requirements and Responsibilities

In addition to the Customer required contributions and responsibilities included in the FortiCloud Service Description, Customer agrees with the following for the duration of the Service:

- FCU sizing: The customer is responsible for ensuring registration of the appropriate FCU requirements to meet the EPS level experienced. If the average daily EPS exceeds the FCU to EPS ratio 20 times in a rolling thirty (30) day period, then upon notification from Fortinet the Customer will:
    - Reduce the EPS to the FCU to EPS ratio and not exceed this ratio 20 times in a rolling thirty (30) day period, for the next 180 days. or;
    - Purchase and register additional FCUs within the next thirty (30) days following the communication by Fortinet.
- Administration: Customer is solely responsible for the administration of all end user login names and passwords for the purpose of authenticating and authorizing access to the Service. Customer shall take reasonable steps to prevent unauthorized access to the Service, including without limitation, by protecting its passwords and account information. Customer shall notify Fortinet immediately of any known or suspected unauthorized use of the Service or breach of its security and shall use best efforts to stop said breach. Fortinet cannot and will not be liable for any loss or damage arising from failure by Customer to protect their passwords or account information.
- Unacceptable Uses: Customer shall only use the Service for internal business purposes and not: (1) share non-public features or content of the Services with any third party; (2) access the Services in order to build a competitive product or service, to build a product using similar ideas, features, functions or graphics of the Service, or to copy any ideas, features, functions or graphics of the Service; or (3) engage in web scraping or data scraping on or related to the Service, including without limitation, collection of information through any software that simulates human activity or any bot or web crawler. In the event that Fortinet suspects any breach of this requirements, Fortinet may suspend Customer's access to the Service without advanced notice, in addition to such other remedies as Fortinet may have.
- Customer Infrastructure: Customer is solely responsible for – and shall bear all cost including and not limited to, network devices, services, workstations and applications within the customer infrastructure – its internal infrastructure (the "Infrastructure") as well as any maintenance, updates, patches, upgrades and other modifications to ensure uninterrupted and effective access to the Service. In particular, the Customer agrees and acknowledges that Fortinet will not be providing any infrastructure that resides on Customer's network other than FortiSIEM collector and agent capabilities as provided under the Service. Customer further agrees and acknowledges that it is solely responsible to roll out the FortiSIEM collector and agent in its Infrastructure.
- FortiSIEM collectors are required to collect events from customer devices or applications and FortiSIEM agents upload events to a FortiSIEM collector. FortiSIEM collectors upload events to the FortiSIEM Cloud. FortiSIEM agents and collectors must also be able to communicate with FortiSIEM Cloud.
- Network Bandwidth: The Customer must (a) ensure suitable and uninterrupted internet connectivity and bandwidth for accessing the Service and (b) manage the network bandwidth used for the transfer of logs from the Customer deployed FortiSIEM collectors to the FortiSIEM Cloud. For instance, the FortiSIEM collector may consume all available bandwidth across its network and may significantly impact the performance of the Customer network, unless the Customer actively manages the bandwidth assigned to the FortiSIEM collector by configuring the FortiSIEM cloud instance or otherwise.
- Suggested Maintenance, Upgrades, and Modifications to Infrastructure: Fortinet may notify the Customer of upgrades, configuration, or other modifications to Customer's network infrastructure which may improve the security, quality, stability or reliability of the Service. Notification via email or through the support portal shall be deemed sufficient for this purpose. Customer shall be under no obligation to implement Fortinet suggestions but Customer acknowledges and accepts that all risk related to the lack of implementation of said suggestions in the infrastructure exclusively lies with Customer including for any performance issues, vulnerabilities, Service interruption or malfunctioning, or other technical issues.
- Service and Infrastructure sizing: The Customer is solely responsible for the appropriate sizing of the Service and Infrastructure as necessary to meet its requirements.

4. Scope and Conditions

- Fortinet will not be obligated to provide the Service Features or deliverables if the Customer fails to perform or complete the Customer Requirements and Responsibilities.
- Fortinet will use reasonable efforts to ensure the configuration of the Customer FortiSIEM cloud instance is reasonably available to the Customer by performing a backup and making available the most recent

backup only for restoration of the Service. The backup will be typically performed every twenty four (24)-hour period as deemed necessary by Fortinet.

- Fortinet will use reasonable efforts to schedule upgrades of FortiSIEM cloud instances to occur within a three (3) month period of the FortiSIEM software release being available to upgrade on FortiSIEM Cloud. Upon Customer request and risk, Fortinet may bring forward the upgrade schedule to an earlier date. If the upgrade has not been scheduled to occur within three (3) months by the Customer, Customer accepts that Fortinet may initiate the upgrade of the FortiSIEM cloud instance to ensure that the FortiSIEM Cloud instance is operating on the current generally available version as approved by Fortinet.
- At least thirty (30) days prior to the Service expiration, the Customer will receive a renewal notification email from the cloud portal on a weekly basis. The Service expiration date will be displayed within the FortiSIEM Cloud portal where the Customer will also be prompted with daily notifications for renewal. Upon Service expiration, the FortiSIEM Cloud instance will be shut down and an email notification will be sent to the Customer. The Customer then has fourteen (14) days to contact Fortinet to renew their license and regain access to the FortiSIEM instance. After fourteen (14) days of the expiration, the instance will be deleted and a notification email sent to the Customer. For clarity, the Customer is explicitly advised that, once the instance is deleted, the data will be no longer recoverable.
- Service performance (including any equivalence between FCU and EPS) are tested under reproducible laboratory conditions and might vary in live environments. Therefore, Fortinet cannot guarantee these in any other environment.
- FortiSIEM Cloud log data cannot exceed more than the subscribed storage.
- Customer is solely responsible for configuring the data retention period in the FortiSIEM cloud instance and monitoring and managing the subscribed storage. The log data will be purged upon the expiration of the retention period or in the event that the subscribed storage (online or archive) is full. The Service will purge Customer data on a first in first out basis to ensure that there is space to store the latest logs received. Typically, Fortinet will purge data from online storage when less than ten percent (10%) of subscribed storage is available. Data will be purged until a minimum of twenty percent (20%) of subscribed storage space is available. If archive storage has been subscribed to, online data will be moved to archive as a result the online data becoming full or thresholds reached. If archive storage has not been subscribed to then data will be purged from online storage when full. When data is in the archive storage and all subscribed storage space is consumed, the archive will purge the oldest data to allow for new data to be stored.
- Fortinet will use reasonable efforts to monitor the utilization of the Service including EPS rate, agents, UEBA usage and other metrics.
- Fortinet may recommend enabling of controls to maintain the availability of the instance, this may include enabling of EPS limiting functions.
- FortiSIEM Cloud evaluations may be terminated by Fortinet prior to the evaluation expiry date. Fortinet will email the primary contact designated in FortiCare to inform of the termination date and provide at least 1 business day (Monday to Friday) notice. Upon termination, the instance is deleted, and the data will be no longer recoverable.
- In the event that the integrity or availability of the Service is at risk, Fortinet may perform emergency maintenance actions at its sole discretion and Fortinet will inform the customer via FortiCare as soon as reasonably possible.
- Service availability target is measured on the ability for users to access the FortiSIEM Cloud instance, storage of newly received events and operation of real-time correlation rules with subsequent generation of incidents.
- Fortinet will exclude delays related to Service unavailability or disruption caused by any of following events, without limitation:
  i) Customer's ability or inability to operate the FortiSIEM collectors, agents or integrations with third party technologies.
  ii) FortiSIEM collectors and agents.
  iii) Scheduled and emergency service changes including upgrades of FortiSIEM Cloud instances and application of additional FortiSIEM Compute Units to an instance.

5. Eligibility & Purchasing

The Service is available for purchase by an end-customer including, as the case may be, Fortinet's authorized MSSPs (the "Customer") through authorized Fortinet resellers and distributors globally ("Channel Partners"). Channel Partners are independent third parties that conduct business in their own name and account and, consequently, cannot bind Fortinet in any way. The Service is delivered to the Customer as referenced in the purchase order placed with Fortinet by a Customer or Channel Partner.

The date of the Service registration determines the start date of the Service which will run for the period determined by the Service SKU purchased by Customer notwithstanding if the Service entitlements are not fully consumed. The registration and delivery of the Service covered by this service description must commence in accordance with the terms outlined in Fortinet's Standard Terms and Conditions. In no circumstances will the duration of the Service be extended or any right to obtain a refund apply if the commencement terms are not met. All sales are final.

Purchasing Information:

SKU	Description
FC-10-SMCLD-543-02-DD	10 FortiSIEM Compute Units (FCU). Minimum quantity of 10 FCU. Annual Subscription. Includes FortiCare Premium Support.
FC-10-SMCLD-541-02-DD	Additional 500GB online storage. Requires minimum quantity of 1 with initial FortiSIEM Compute Unit order. Annual Subscription.
FC-10-SMCLD-542-02-DD	Archive 500GB storage. Annual Subscription.

With “DD” indicating length of the Service in number of months. Currently, terms of 12, 24, 36, 48 and 60 months are offered.

Note: FortiSIEM Cloud supports a minimum of 10 FCU. Recommended is 20 FCU.