SERVICE DESCRIPTION

FORTISASE™

1. Introduction

The FortiSASE™ service allows a Customer to apply cyber security controls in a cloud environment (the "Service") extending the network perimeter, and providing secure access for end-points. The Service provides security features and flexible technical solutions for secure access, as outlined in the FortiSASE™ Administration Guide ("FSAG") which is available at https://docs.fortinet.com/product/FortiSASE.

The Service is made available with three (3) user subscription levels dependent on the purchased Service SKU:

- FortiSASE™ Standard Tier
- FortiSASE™ Advanced Tier
- FortiSASE™ Comprehensive Tier

2. Service Options and Deliverables

Through the registration and activation of applicable Service contract(s), the Service provides the Customer with:

FortiSASE™ Standard Tier

The Standard Tier includes the following features:

2.1. Security Services

- The Security control features as defined in the FSAG.

2.2. Cloud Services

- Connectivity to any of the entitled Security Point of Presence ("PoP") as communicated by Fortinet based on the purchased Service Tier. This Tier provides connectivity for up to four (4) PoPs, additional PoP locations are available for purchase (as outlined in Section 7).
- Management portal for Customer's administration of the Service through application of appropriate security controls or policies to the provided PoP.
- Logging collector, where logs generated from the PoP will be sent and captured within the management portal.

2.3. End-Point Services

- Provision of agent-based software (*currently FortiClient™*).

2.4. Technical Support

- FortiCare™ Premium Technical Support as outlined in the then current Fortinet support policies and service description, which are posted and visible on the Support Portal.

FortiSASE™ Advanced Tier

The Advanced Tier includes the following features in addition to the FortiSASE™ Standard Tier:

2.5. Advanced Tier Service Options

- *FortiCloud Security Operation Center-as-a-Service* ("SOCaaS") a cloud-based managed security monitoring service that analyzes security events generated from Customer's FortiGate™, performing alert triage, and escalating verified threat notifications to the Customer, as outlined in the then-current Fortinet support policies and service description, which are posted and visible on the Support Portal.
- Provision of up to four (4) *Dedicated IP* public addresses, where one (1) public IP address will be assigned to each PoP selected by default.
- *Assisted Onboarding* a technical self-service experience which provides the Customer with structured guidance and resources to learn and configure the Service.
- *Digital Experience Monitoring* which provides end-point performance information within the management portal.
- *FortiGuard Forensics (Response) Service*: which provides remote end-point analysis, to respond to and recover from cyber incidents.

FortiSASE™ Comprehensive Tier

The Comprehensive Tier includes the following features in addition to the FortiSASE™ Advanced Tier:

2.6. Public Cloud Locations

- Connectivity to any of the entitled Security Point of Presence ("PoP"), including those located in the Public Cloud, as communicated by Fortinet based on the purchased Service Tier. This Tier provides connectivity for; up to four (4) PoPs for greater than two hundred (200) active user subscriptions; up to two (2) PoPs for up to one hundred and ninety nine (199) active user subscriptions and; one (1) PoP for up to ninety-nine (99) active user subscriptions. Additional PoP locations are available for purchase (as outlined in Section 7).
- For details on Public Cloud locations refer to the FSAG. It is possible to combine Fortinet Cloud, Regional Public Cloud and Public Cloud locations.

For further information on the features described above refer to the FSAG.

3. Service Measurements

FortiSASE™ is managed and monitored by Fortinet on a twenty-four (24) hours per day, seven (7) days a week basis. Fortinet measures and will use commercially reasonable efforts to achieve the following targets.

3.1. *Security Processing*

The "Processing Latency" for the Service, is the time to apply security controls, which is measured from the point at which the Service receives a qualified data packet for a particular transaction, to the point the packet is transmitted. The latency is a factor of the security posture configured by the Customer and the associated requirement for packet inspection. The target is 10 (ten) milliseconds or less.

3.2. *Third Party SAAS Applications*

The "Third Party SaaS Application Latency" is the time measured from the service edge in a Fortinet PoP to a chosen point on the third party SaaS network. The following SaaS applications are measured; Google G Suite, Microsoft O365, Salesforce with the following Service targets.

Security PoP Region	SaaS Latency Targets
North America	35ms
EMEA	45ms
APAC & LATAM	75ms

3.3 *Data Transfer*

The Service provides an annual Data Transfer entitlement per Customer tenant of bytes received and sent (the "Data Transfer Entitlement"). The Customer's Data Transfer Entitlement is calculated from the combined value of each active Subscription .

Per Subscription	Gigabytes Per Annum
FortiSASE™ User	250
FortiAP	500
FortiBranchSASE	500
FortiExtender	500
FortiSASE™ Branch OnRamp	50000

The Entitlement Period ("Entitlement Period") is 365 (three hundred and sixty-five) days running concurrent with the Customer's annual FortiSASE subscription. At the end of the Entitlement Period all calculations described herein are reset.

Fortinet will provide Customer with notifications once their Data Transfer Entitlement reaches 80 (eighty) percent, 90 (ninety) percent and, 100 (one-hundred) percent.

Comprehensive Tier- Excess Usage: If the Customer exceeds the Data Transfer Entitlement, for the Comprehensive Tier only, Fortinet reserves the right to limit the Customer's Data Transfer Usage for the remainder of their subscription. Customer will receive a limited daily allocation (the "Daily Enforcement Allocation") and Customer will be notified of the value of the Daily Enforcement Allocation. Once the Daily Enforcement Allocation is exceeded during any

subsequent 24 (twenty four) hour period, the Service will not accept new data packets until the next day. All notifications will be visible to Customer on login to the FortiSASE portal.

The Daily Enforcement Allocation is calculated as follows: every 30 (thirty) days during the Entitlement Period, on a rolling basis, the Customer's Data Transfer cumulative usage is tracked. The maximum sample value is recorded (the "30 Day Maximum Observed Cumulative Value"). The Daily Enforcement Allocation is a thirtieth of the 30 Day Maximum Observed Value. For example,

30 Day Maximum Value = 300 Gigabytes / 30 = Daily Enforcement Allocation = 10 Gigabytes

Additional Data Transfer is available for purchase, in increments of 250 (two hundred and fifty) gigabytes (as outlined in Section 7) and activation of same, removes any Daily Enforcement Allocation then in effect.

4. Service Level Agreement

The Service Level Agreement "SLA" covers Fortinet's uptime commitment, for the availability of the Service, subject to the terms of this document. Fortinet maintains a "Status Page" https://status.fortisase.com for overall Service availability as well as individual PoP locations.

4.1 *Availability*

Fortinet's uptime target is 100% availability of the Service. Available or the "Availability" of the Service is defined as the ability to accept the Customer's qualified packets, apply customer configured security controls (as delivered by the in-line hardware and software hosted in Fortinet's Data Centers) and transmit processed packets to the Internet.

The Availability is calculated as the "Average Percentage" of time during a calendar month the Service is available to the Customer excluding any time covered by the "Availability Exclusions". It is subject to the Customer's configuration assuring continuous service by the provisioning and use of at least 3 (three) PoP locations as well as alignment with Fortinet best practice (as outlined in Section 5).

4.2 *Availability Exclusions*

- Problems caused by the Customer's implementation including equipment failure, misconfiguration, non-adherence to Fortinet's design recommendations (as outlined in Section 5), failure to implement any support recommendations for workarounds or software upgrades, as well as assuring the correct number of subscriptions for the amount for users/traffic being sent to the Service.
- Failure or degradation of performance of intermediate internet service providers providing connectivity between the Customer network and Fortinet PoPs, including routing disruptions.
- Maintenance Activities (as outlined in Section 6).
- Any event outside "Fortinet's Control" such as: a) a third party is unable or refuses or delays supplying a service or product to Fortinet and there is no alternative available to Fortinet at reasonable cost; (b) Fortinet is prevented by legal or regulatory restrictions from supplying the Service or a Product; (c) Force Majeure events; (d) availability of third party DNS services; or (e) any item beyond Fortinet's reasonable control.
- Any time associated with suspension of the Service to the Customer implemented for security reasons (as outlined in Section 6).

4.3 *Service Credit*

If the Service does not meet the Service "Availability Percentage" during a calendar month, Fortinet will provide a "Service Credit" equivalent to a value in "Credit Days" according to the following table.

Service Availability %	>=99.999%	<99.999% but >= 99.9%	<99.9% but >=99%	<99% but >=98%	<98%
Credit Days	None	2 days	5 days	10 days	30 days

- To receive Service Credits, the Customer must; (a) submit a credit request via a customer service ticket within ten (10 days) of the incident; and (b) provide the necessary information and evidence to support the claim including reference to the relevant technical support ticket, details on impact to Customer and any other pertinent information from the incident.
- Fortinet will review the Service Credit request and provide a response to Customer no later than thirty (30) days after the claim was submitted. A Service Credit will be issued if the claim has been validated.
- Applied Credits are considered extensions of the existing Service and measured in individual days. Credits are capped at a maximum sixty (60) credit days per calendar year for the Service as described herein.

- When a Service Credit extension is provided, it shall be eligible for Service Credit as if it were part of the original term and subject to the same maximum cap.

5. Customer Requirements and Responsibilities

As a required prerequisite for Service performance, the Customer must:

- Assist with all reasonable requests to provide the information requested by Fortinet including, without limitation, any information required to resolve incidents or evaluate Service Credits.
- Implement; (a) best practice design as outlined in Fortinet's 4-D Design Guidelines available at https://docs.fortinet.com/4d-resources/SASE; and; (b) any corrective configuration changes or workarounds or software updates required to resolve or mitigate an incident as reasonably requested.
- Assure the appropriate Service coverage which includes: users, appliances which may connect to the Service, Point of Presence locations as described in the "FSAG", and, any add-on services, as outlined herein.
- Guarantee appropriate agreement within Customers organization for change requests, when non-standard configurations are applied at the Customer´s request, as these may impact entitlement to Service Credits.
- Agree to use the Service for legitimate and lawful business purposes only. In particular, the Customer is responsible for ensuring that its usage of the Service shall be in accordance with all applicable laws (including, but not limited, privacy and security laws) and that it has all necessary subscriptions, permissions, clearances, rights and has in place proper controls and processes, implemented and maintained in this respect. Therefore, Fortinet explicitly advises the Customer to always assess and ensure that the usage of the Service complies with local legislation prior to any deployment. Should Fortinet discover illegal activity, the Service may be terminated without notice and the relevant authorities may be notified regardless of intent.

6. Scope and Conditions

The Service is subject to the following terms and conditions:

- To assure the evolution and proper functioning of the Service "Maintenance Activities" take place, which are defined as the period of time when features and patches are applied to the Service platforms. Advanced notification of maintenance activities is provided on the Status Page and Customer may subscribe to receive updates. There are two types of "Maintenance Activity"; (a) "Scheduled Maintenance" is planned and in general take places on a monthly cadence and; (b) "Emergency Maintenance" which takes place if Fortinet judge that the integrity of the Service is at risk. Fortinet will endeavor to provide notification of same at least one (1) hour prior.
- In the event, that the continued provision of the Service to the Customer may compromise the security of the Service or Fortinet's systems, networks or reputation, the Customer agrees that Fortinet may temporarily or permanently suspend the Service to the Customer at Fortinet's sole discretion without any liability whatsoever for Fortinet. The Customer accepts and acknowledges that; (a) Fortinet shall not be liable for any damages, fines, claims, costs or expenses incurred or suffered by the Customer or any third parties as a result of or in connection with the breach of these warranties; and (b) it shall fully indemnify and hold Fortinet harmless from and against any and all claims, liabilities, losses, damages, penalties or fines, including all reasonable legal fees, arisen directly or indirectly as a consequence of the breach of these warranties.
- The Customer acknowledges and agrees that the Service helps to prevent, find or eliminate malware and security breaches but it is technically impossible to guarantee 100% email or network security as no security device or service can guarantee full or unbreakable security or the blocking of all known malicious activity. Fortinet accepts no liability for any damage or loss resulting directly or indirectly from any failure of the Service to detect malware, malicious activity or for false positives including security breach, data loss, data corruption, and service interruptions and/or degradations of the Company's network, systems.
- The Customer acknowledges and agrees that:
    - Logs are retained for seven (7) days.
    - Each FortiSASE™ Security PoP can support up to seven (7) seven dedicated IP addresses.
- Service Credits are provided according to the following conditions:
    - Credits are applicable; a) where all payments owed to Fortinet for the applicable services are fulfilled; b) there has been a complete calendar month of Service delivery; c) Customer appropriately logged a technical support ticket to allow timely resolution of the incident; and c) to the subscription Tiers described herein.

- Fortinet will have no liability for Service Credits if; a) the Customer has failed to meet their obligations under applicable terms; b) during a calendar month when a non-standard Customer requested configuration or a Data Transfer Daily Enforcement Allocation is in place; c) for any Service provided free of charge, for evaluation or proof of concept purposes, or bundled as part of another Service with the intention of being a sample or seed.
- Credits are the Customers sole and exclusive remedy for any claim of non-compliance of Availability and Fortinet reserves the right to deny a Service Credit if Customer does not qualify.
- Any claim to Service Credits shall immediately cease with the expiry or the Service including when a renewal event does not occur in advance of such expiry.

- For the first five (5) days following the expiration of the Service subscription, Fortinet will provide a grace period for use of the Service before termination. Fortinet will retain the configuration and any associated data for a period of fourteen (14) days from the date of expiration to allow data collection or service re-initiation following termination or expiration of the Service subscription. Once the grace period has elapsed, the Customer's instance will be deleted along with any associated data. Deleted data will not be recoverable.
- Unless otherwise specified, the Service will be delivered in English language and remotely.
- Activation of the Service takes place in accordance with Fortinet's Service Contract Activation and Grace Period Policy, made available at: https://www.fortinet.com/corporate/about-us/legal/service-contract-activation-grace-period-policy.
- The Service is subject to the terms of then-current Fortinet's Service Terms & Conditions located at https://www.fortinet.com/content/dam/fortinet/assets/legal/Fortinet-Service-Offering-Terms.pdf

7. Eligibility, Purchasing and Start Date

The Service is available for purchase by an end-customer including, as the case may be, a Fortinet authorized MSSP solely through authorized Fortinet resellers and distributors ("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. This Service is separate from any purchase of other Fortinet's products or other services.

All sales are final.

8. Purchasing Information:

FortiSASE™ User Subscriptions		
Per User Bands	**Standard Tier**	**Advanced Tier**
50-499	FC2-10-EMS05-547-02-DD	FC2-10-EMS05-676-02-DD
500-1,999	FC3-10-EMS05-547-02-DD	FC3-10-EMS05-676-02-DD
2,000-9,999	FC4-10-EMS05-547-02-DD	FC4-10-EMS05-676-02-DD
10,000+	FC5-10-EMS05-547-02-DD	FC5-10-EMS05-676-02-DD
Per User Bands	**Comprehensive Tier**	
50-499	FC2-10-EMS05-759-02-DD	
500-1,999	FC3-10-EMS05-759-02-DD	
2,000-9,999	FC4-10-EMS05-759-02-DD	
10,000+	FC5-10-EMS05-759-02-DD	

Account Level Subscription Add-Ons		
Dedicated IP Address	4 Public IPs	FC1-10-EMS05-658-02-DD
	32 Public IPs	FC2-10-EMS05-658-02-DD
Region Add-On Locations	Fortinet	FC1-10-EMS05-752-02-DD
	Public Cloud	FC2-10-EMS05-766-02-DD
	Global	FC-10-EMS05-1136-02-DD
Data Transfer	250GB	FC1-10-EMS05-471-02-DD