LACEWORK FORTICNAPP CUSTOMER
SUPPORT SERVICE LEVEL AGREEMENT

Fortinet's Lacework FortiCNAPP Customer Support Service Level Agreement ("**Customer SLA**") details the Support Levels available to Fortinet's software-as-a-service customers, as identified in the applicable Order. This Customer SLA supplements the Fortinet Lacework FortiCNAPP Terms of Service (or other written agreement covering the same subject matter executed by Fortinet) for the Service purchased by Customer (the "**Agreement**"). Capitalized terms not specifically defined in this Customer SLA shall have the meaning as in the Agreement. Fortinet reserves the right to update this Customer SLA from time to time, as indicated by the "Last Updated" date below.

1. Maintenance and Support. During the Subscription Term, Fortinet will make available to Customer as part of the Service all generally available updates and bug fixes to the Service. For technical information and support regarding Customer's use of the Service, Customer can reach Fortinet through Fortinet's support portal, and Fortinet will respond to support issues during regional working hours in accordance with the Initial Response Times below ("**Support Hours**").

	STANDARD/FORTICARE PREMIUM	**PREMIUM/FORTICARE ELITE**
Initial Response Times*	**P1 (Urgent):** 1 Hour **P2 (High):** 1 Hour **P3 (Medium)Critical:** Next Business Day **P4 (Low):** 2 Business Days	**P1 (Urgent):** 15 minutes **P2 (High):** 15 minutes **P3 (Medium):** 2 Business Hours **P4 (Low):** 4 Business Hours
Update Frequency	**P1 (Urgent):** 6 Hours **P2 (High):** Daily **P3 (Medium)Critical:** Every 3 Business Days **P4 (Low):** Every 5 Business Days	**P1 (Urgent):** 3 Hours **P2 (High):** 12 Hours **P3 (Medium):** Each Business Day **P4 (Low):** Every 3 Business Days

*Lacework Standard Support is equivalent to Fortinet's FortiCare Premium, and Lacework Premium is equivalent to FortiCare Elite.

2. Customer Responsibilities. In addition to other responsibilities contained in the Agreement, Customer will be responsible for the maintenance, management and accuracy of its customer account data, as well as all software, hardware and services it uses to access the Service. By default, Fortinet auto-updates all Agent Software; provided, however, that if Customer turns off the auto-update feature, then Customer shall be responsible for updating the Agent Software.

3. Exclusions. Fortinet will have no liability for any failure to meet the Uptime Commitment (defined below) in this Customer SLA arising or resulting from: (i) factors outside of Fortinet's reasonable control, including any force majeure event, Customer's Internet access, or other problems beyond the scope of the Service; (ii) Customer's failure to promptly notify Fortinet of the alleged non-conformity to the extent Fortinet is materially prejudiced from resolving the same due to Customer's failure to promptly notify; (iii) misuse, unauthorized modification, or Customer or third party equipment, software, services, or technology not within Fortinet's direct control; (iv) Customer's failure to update the Agent Software under Section 2 above; (v) any unavailability, suspension, or termination of any Cloud Provider Account, or any other cloud service provider performance issues; (vi) evaluation or Trial use of the Service; (vii) Fortinet's pre-release or beta functionality not intended for production use; or (viii) Fortinet's suspension or termination of Customer's right to use the Service in accordance with the Agreement (collectively, the "**Uptime Exclusions**").

4. Classification of Problems. Fortinet shall work with Customer to classify each problem based on the business impact reported by Customer and will address the problem in accordance with such classification during the Support Hours, according to the table below:

Priority	**Priority Description**	**Initial Response Times**	
		Standard/FortiCare Premium	**Premium/FortiCare Elite**
P1 Urgent	An incident that causes a total loss or continuous instability of mission-critical functionality in a live or production environment of the Lacework FortiCNAPP Platform	Fortinet will provide a status update by email within 1 hours of Customer's notification.	Fortinet will provide a status update by email within 15 minutes of Customer's notification.

P2 High	An issue that causes significant impact to mission-critical functionality in a live or production environment of the Lacework FortiCNAPP Platform	Fortinet will provide a status update by email within 1 hour of Customer's notification.	Fortinet will provide a status update by email within 15 minutes of Customer's notification.
P3 Medium	An issue in the platform that has minimal impact to business operations.	Fortinet will provide a status update by email within the next business day of Customer's notification.	Fortinet will provide a status update by email within 2 business hours of Customer's notification.
P4 Low	Request by the Customer for additional information, including basic configuration assistance, errors in documentation, or minor defects that do not impact business services.	Fortinet will provide a status update by email within the next 2 business days of Customer's notification.	Fortinet will provide a status update by email within 4 business hours of Customer's notification.

5. Service Levels. If Customer is receiving the Premium/FortiCare Elite tier of Support, Customer shall be entitled to receive Service Credits based on Fortinet's failure to meet the Service Levels, all in accordance with the Service Level table below. "**Service Levels**" means the uptime availability of the Service as identified in the Service Level table below for all Scheduled Availability Time, calculated on a monthly basis for all Users. "**Scheduled Availability Time**" means 24 hours a day, 7 days a week, exclusive of the Uptime Exclusions above. Scheduled Availability Time excludes downtime as a result of (a) Customer exceeding subscribed service capacity, (b) misconfiguration or action that is of a non-standard nature, (c) integrations and use of unapproved third party products, (d) loss of service or connectivity relating to configuration of third party products interacting with the service or internet service provision, (e) usage of "Beta" features of the Subscription which are not made generally available, (f) negligence or any malicious acts of the Customer, its employees, agents, third party contractors or vendors, or (g) component or infrastructure that are not reasonably accessible to Fortinet in the resolution of any incident.

Premium/FortiCare Elite Service Levels	**Service Credits**
<99.999% but greater than or equal to 99.9%	2-Day Extension
<99.9 but greater than or equal to 99.0%	5-Day Extension
<99% but greater than or equal to 98%	10-Day Extension
<98%	30-Day Extension

6. Service Credits. If Fortinet fails to meet the Service Levels in any month during the Term, Customer shall be entitled to a an extension of the Subscription Term, being applied at the current service expiry date (each, a "**Service Credit**").

To benefit from a Service Credit the Customer shall be responsible for and perform the following:

- Raise a Priority 1 technical support ticket (or by a Fortinet recognized managed service partner operating on behalf of the Customer) with Fortinet within 24 hours of the start of the downtime clearly describing the impact experienced by the Customer.
- Submit a Service Credit request in writing and through agreed procedures within five (5) days following the end of the month during which the breach occurred.
- Provide all supporting information required by Fortinet for the sole purpose of evaluating the claim and its compliance with these terms which may include dates, ticket references related to the service incident.
- Comply with: all Fortinet documentation related to appropriate use of the service and expected performance parameters made available in respective product datasheets, deployments guides or other technical documents; and the applicable Service terms. Except for remedies associated with any breach of warranty under the Agreement, the remedies set forth in this section shall be Fortinet's sole obligation and Customer's exclusive remedy with respect to any failure by Fortinet to meet the Service Levels.

7. Scope and Conditions

- Fortinet will use reasonable efforts to perform the maintenance of its infrastructure, aiming at minimizing or mitigating any Service disruption to the extent reasonably feasible. In particular, Fortinet will use reasonable efforts to provide the Customer with forty-eight (48) hours advanced notice in the event that any planned maintenance activity may cause Service disruption. For any planned maintenance, Fortinet will use reasonable efforts not to perform it between the hours of 8 am and 6 pm in the time zone where the infrastructure subject to maintenance is located, and not for more than eight (8) hours in any given

calendar month. Notification will be made through the most appropriate means at the discretion of Fortinet which may include email, portal messages or other means.

- In the event that the integrity of the Service is at risk, Fortinet may perform emergency maintenance actions at its sole discretion and will use reasonable efforts to inform all affected parties within one (1) hour of the start of the maintenance activity.
- During any maintenance activity that requires the Service to be unavailable, Fortinet will use reasonable efforts to configure the bypass traffic directly to origin web servers to minimize Service availability impact.
- The Service may help to enhance the security of the Customer's networks but are subject to intrinsic reliability and technical limitations. It is therefore technically impossible to guarantee that malicious activity will be effectively blocked or prevented. Fortinet accepts no liability for any damage or loss resulting directly or indirectly from any failure of the Service to detect, prevent or block malicious activity.
- All service levels described in this document are targets which Fortinet will use reasonable efforts to achieve. Any loss of network connection, telecommunication links or internet connection is the responsibility of the Customer with the Service continuing to be considered as being utilized. The availability target only applies to the Service infrastructure and will exclude delays related to unavailability or disruption caused by any of following events, without limitation:
    - scheduled maintenance or emergency maintenance;
    - unauthorized user changes;
    - Customer initiated changes whether implemented by Customer or Fortinet or a third party on behalf of Customer;
    - Customer exceeding the subscribed Service entitlement;
    - Customer's failure to adhere to Fortinet implementation, support processes and procedures;
    - acts or omissions of the Customer, its employees, agents, third party contractors or vendors or any third party accessing the Service;
    - any violations of the Customer responsibilities defined herein;
    - any event not wholly within the control of Fortinet;
    - negligence or willful misconduct of the Customer, or others authorized by the Customer to use the Services provided by Fortinet;
    - any failure of any component for which Fortinet is not responsible, including but not limited to all Customer´s infrastructure, internet access, electrical power sources, networking equipment, computer hardware, computer software or data;
    - any failures that cannot be corrected because the Customer, personnel, its systems or networks are not reasonably accessible to Fortinet. It is the Customer's responsibility to ensure that technical contact details are kept up to date by submitting a request ticket to confirm or update the existing the technical contact details;
    - high Availability events and scaling events
- The Service is available in English.

Last Updated: September 2024