SLA - App & API Protector with Advanced Security Management Plus DSA

Akamai Cloud Security Solutions Service Level Agreements

(SLA) DEFINITIONS

"Akamai Network" means the distributed network owned and operated by Akamai.

"Akamai Prolexic Network" means the distributed network of specialized network of scrubbing centers owned and operated by Akamai.

"Attack Monitoring Services - Failure to Notify Event" is an event in which Akamai fails to take the defined steps to notify Customer within a period of 15 minutes from the time that Akamai's Security Operations Center (SOC) receives a Critical alert (applicable only to Prolexic Application-Based Monitoring and Prolexic Flow-Based Monitoring Services deployed at the Customer site).

"Availability Outage" (applicable only to App and API Protector, Kona Site Defender, Kona DDoS Defender, Web Application Protector, Web Application Firewall, Bot Manager Standard, Bot Manager Premier, Account Protector, and Site Shield) is defined as a period of at least two consecutive failed attempts six (6) minutes apart by a single agent to GET the Customer test file from the Service while succeeding to GET the test file from the Customer Origin Server (directly, or via a Site Shield region if applicable). If an outage is identified by this method, the Customer will receive (as its sole remedy) a credit equal to Customer's or such domain's committed monthly service fee

"Emergency Maintenance" means any activity that Akamai, in its sole discretion, deems necessary to correct an immediate threat to the ongoing availability and quality of Akamai's Service offerings.

"Facilitated Route-On – Failure to Redirect Event" is an event in which Akamai fails to initiate a BGP route change for a Facilitated Route-On Customer within a period of 15 minutes as measured from either (i) the time that Akamai's Security Operations Command Center (SOCC) receives a Critical FBM alert that is defined in the Customer's runbook as an event that would qualify for traffic redirection for one or more protected network(s) or (ii) Akamai's receipt of Customer's confirmation that Akamai may implement the BGP route change, if such Customer confirmation is required by Customer's runbook.

"Managed Security Service 2.0 Response Times" - Akamai Security Operations Command Center Support Initial Response Times:

1. 30 minutes or less for Priority 1 issues (must be opened via phone)
2. 1 hour or less for Priority 2 issues
3. 1 business day for Priority 3 issues

All Support Requests reported via e-mail will be considered as Priority 3

Initial Response Times apply only to Support Requests filed against a currently contracted security Service.
Akamai security analysts will perform an analysis of the Security Event.

Whether or not a Security Event is considered an attack is determined solely by Akamai. Identified attacks will be classified, prioritized, and escalated as Akamai deems appropriate in accordance with the severity classifications under Product Support for Akamai security Services.

"Preconfigured Mitigation Control" – (applicable only to Prolexic Routed Service) is a proactive measure deployed in peacetime, offering the ability to block malicious layer 3 DDoS traffic abuses that are destined to a Customer's network.

"Security Severity Levels"

● **"Severity 1"** -- Critical Impact: This class exhibits: a) loss or outage on any portion of a protected property, b) data breach (exfiltration or infiltration) confirmed in progress, or c) defacement of a protected property.

● **"Severity 2"** – Major Impact: This class exhibits: a) degradation in performance on any portion of a protected property, b) suspected data breach, or c) excessive bot activity that may lead to intellectual property compromise.

● **"Severity 3"** – Low Impact: This class exhibits: a) signs of a potential small-scale security incident (log event evidence of malicious traffic that does not impact the origin and may be false positive, b) is a proactive action; "heightened attention" in response to a public threat, for instance, c) includes a possible fraud investigation without immediate evidence of data breach, or d) low-level site scraping activity.

"Service Ready"– means the point at which the Prolexic Service can be accessed and consumed by the Customer via SOCC and support teams. If the integration or provisioning of the Prolexic Service are fully-managed, Akamai will issue to the Customer a letter confirming that the Prolexic Service is Service Ready. If the managed services include customer-provisioned or customer-managed configurations, the Prolexic Service will not be considered "Service Ready" until the creation of the runbook and the completion of included training on self-provisioning component(s).

"Service Outage" (applicable only to Prolexic Routed, Prolexic Connect, and Prolexic Proxy) means that Akamai's Prolexic Network did not respond to DNS or HTTP queries or the forwarding of IP traffic for more than sixty (60) consecutive seconds.

"Service Validation" is a process which tests Customer's environment and service performance, and is required for all Customers of Prolexic Routed (i.e. GRE or Connect Option).

Akamai's Time To Mitigate Service Level (applicable only to Prolexic Routed, Prolexic Connect, Prolexic Proxy, and Prolexic IP Protect)

With respect to Customers subscribing to Prolexic Routed, Prolexic Connect, Prolexic Proxy, and Prolexic IP Protect, Akamai offers a service level ("Service Level") committing to the length of time that it will take Akamai to effectively deploy mitigation.

The Service Level begins at the time that a critical alert is generated by Akamai for Customers subscribed to the standard Always-On mitigation service or for Customers who are otherwise permitted to be running traffic through Akamai's Prolexic Network when a DDoS attack is identified. The time of the critical alert will be determined by relevant ticket correspondence and/or critical alerts in the Akamai portal.

The Service Level for Customers subscribed to an On-Demand mitigation service, if not currently routed through the Akamai Prolexic Network, begins after a Customer notifies Akamai and properly routes traffic through Akamai's Prolexic Network during a DDoS attack. The Time to Mitigate ("TTM") value for these On-Demand Customers depends upon the length of time for the Customer to properly route traffic through Akamai's Prolexic Network, and the length of time it takes for routes to propagate to the Internet at large.

Akamai's Service Level for the following attack types is available exclusively to Prolexic Routed, Prolexic Connect, Prolexic Proxy, and Prolexic IP Protect Services Customers. Akamai commits to the following TTM, for each DDoS attack type, as categorized per following:

Attack Type	TTM - Time to Mitigate (typical)	TTM - Time to Mitigate Guaranteed (Service Level)
Any attack matching a Preconfigured Mitigation Control	1 Seconds	0 Seconds
UDP/ICMP Floods	2 minute or less	5 minutes
SYN Floods	1 minute or less	5 minutes
TCP Flag Abuses	1 minute or less	5 minutes
GET/POST Floods	10 minutes or less*	20 minutes
DNS Reflection	5 minutes or less**	10 minutes
DNS Attack	5 minutes or less**	10 minutes

* Mitigation requiring traf ic analysis and custom signature deployment
** Applies to DNS attacks targeting Akamai IP addresses

Akamai's Time To Mitigate Service Levels (applicable only to App and API Protector, Kona Site Defender and Web Application Protector)

With respect to Customers subscribing to App and API Protector, Kona Site Defender, or Web Application Protector, Akamai offers a service level ("Service Level") committing to the length of time that it will take Akamai to effectively mitigate an attack, meaning initial mitigations have been deployed and have been effective at mitigating the impact of the immediate attack.

Akamai's Service Level is available exclusively to App and API Protector, Kona Site Defender, and Web Application Protector Customers and applies only to attack traffic routed through the Akamai platform.

Akamai commits to the following TTM for each of the specified DDoS attack types:

Attack Type	TTM - Time to Mitigate (typical)	TTM - Time to Mitigate Guaranteed (Service Level)
UDP/ICMP Floods	0 seconds	0 seconds
SYN Floods	0 seconds	0 seconds
TCP Flag Abuses	0 seconds	0 seconds
DNS Reflection	0 seconds	0 seconds
DNS Attack	0 seconds	0 seconds

Akamai's Time To Mitigate Service Level (applicable only to Kona DDoS Defender and Managed Kona Site Defender Service)

With respect to Customers subscribing to Kona DDoS Defender and Managed Kona Site Defender Service, Akamai offers a service level ("Service Level") committing to the length of time that it will take Akamai to effectively deploy mitigation, meaning:

- Initial mitigations have been deployed
- They have been effective at mitigating the impact of the immediate attack.
- The benefits of the mitigation were evident within the time window of the SLA.

The Service Level begins at the time that a critical alert is generated by Akamai for Customers subscribed and integrated to the standard Always-On mitigation service when a DDoS attack is identified. The time of the critical alert will be determined by relevant ticket correspondence and/or critical alerts in the Akamai portal.

Akamai's Service Level only for the following attack types is available exclusively to Kona DDoS Defender and Managed Kona Site Defender Service Customers. At a minimum, a Table Top Drill for Kona DDoS Defender, or a Threat Update Review and a Table Top Drill for Managed Kona

Site Defender Service is required once annually and Akamai's Security Specialist recommendations must have been applied to the configuration. Akamai commits to the following TTM, for each DDoS attack type, as categorized per following:

Attack Type	TTM - Time to Mitigate (typical)	TTM - Time to Mitigate Guaranteed (Service Level)
UDP/ICMP Floods	0 seconds	0 seconds
SYN Floods	0 seconds	0 seconds
TCP Flag Abuses	0 seconds	0 seconds
DNS Reflection	10 minutes or less	20 minutes
DNS Attack	0 seconds	0 seconds

Akamai's Consistency of Mitigation Service Level (applicable only to Prolexic Routed, Prolexic Connect, Prolexic Proxy, Kona DDoS Defender and Managed Kona Site Defender Service)

Akamai offers a 95% Consistency of Mitigation Service Level. Consistency of Mitigation is measured by analyzing the ratio of clean traffic to attack traffic that is forwarded to the Customer. Measurement of the Consistency of Mitigation parameter begins after the committed TTM has elapsed. Claims against the Consistency of Mitigation Service Level must be submitted with a packet capture of at least one hour in duration, identifying the total amount of attack traffic forwarded during the event envelope. The event envelope is defined as all or part of the period between the TTM Service Level period and the end of the attack. Evidence of forwarding of attack traffic in excess of 5% of the total traffic volume qualifies for a credit under this Service Level clause. This SLA shall not apply to Prolexic Services until those Services are Service Ready.

Remedy for Time to Mitigate and Consistency of Mitigation Service Levels

The TTM is based from the time that traffic is properly routed through Akamai's Prolexic Network or Akamai Network for On-Demand Customers or from the time that a critical alert is generated for services that are Always On or already routed through Akamai's Prolexic Network or Akamai Network. The TTM is measured based upon the Consistency of Mitigation Service Level terms. During any given calendar month, if Akamai fails to meet the TTM Service Level as measured by the Consistency of Mitigation parameters set forth above, the following credits will be issued:

● Single event – in the event that the TTM Service Level is exceeded – with mitigation not meeting the Consistency of Mitigation Service Level, Akamai will credit Customer's account for such month for the pro rated charges as follows:

o Less than one hour: for (1) day of Monthly Service Fees due in respect of the affected Network Protection Services; o For one hour or more, and less than 6 hours: two (2) days of Monthly Service Fees payable in respect of the affected DDoS Mitigation Services; and

● Multiple Events or Single Event lasting more than 6 hours – in the event that the Time to Mitigate Service Level is exceeded – with mitigation not meeting the Consistency of Mitigation Service Level for a period of six (6) hours or more, or during four (4) or more events within a calendar month, Customer will be credited with seven (7) days of Monthly Service Fees payable in respect of the affected DDoS Mitigation, or Managed Kona Site Defender Services,

All Customers must have successfully completed a Table Top Drill, with any prefix(es) affected, within the previous twelve months in order to qualify for remedy credit under the Time to Mitigate and Consistency of Mitigation Service Levels.

In order to qualify for any applicable Service Level Agreements for Prolexic Routed (GRE or Connect Option),Service Validation must have been successfully completed by Customer, for any prefix(es) affected, within the previous twelve (12) months.

Akamai's Service Availability Service Level (applicable to Prolexic Connect, Prolexic Routed, Prolexic Proxy, and Prolexic IP Protect Service Outage)

Akamai offers a service level ("Service Level") committing to 100% availability of the Prolexic platform. The service level begins at the time the Customer has successfully completed integration and Service Validation for the protected properties, or the contract Billing Effective Date, whichever is later.

This Availability SLA does not guarantee the availability of all scrubbing centers concurrently. All Prolexic Customers are required to have resilience via 2 or more GRE tunnels per provisioned router or 2 or more VLLs per provisioned router connected to 2 or more scrubbing centers (Prolexic Routed with Connect option). Additional resilience is available to all Customers, optionally.

Akamai will provide any credits to Customer (or to Reseller for transfer to Customer, if Reseller is the contracting entity) per the following: Provided Customer reports a Service Outage to Akamai promptly following the occurrence of an event of interruption in Service that Customer believes is a Service Outage, but in any event no later than five (5) days after the event took place, Customer shall be entitled to receive a service credit for Customer's benefit in accordance with the schedule below. Whether an interruption in Services constitutes a Service Outage shall be determined solely by Akamai in its sole good faith discretion supported by records, data and other evidence. If a Service Outage has taken place and Customer notifies Akamai as provided in this Section, Akamai shall provide a credit to Customer as follows:

(i) If a particular Service Outage reported by Customer lasted for more than one minute but less than four (4) consecutive hours during a calendar month, Akamai will credit Customer for such month, the pro-rated charges for one (1) day of Monthly Service Fees of the amount of revenue Akamai receives from Customer with respect to the affected DDoS Mitigation Service(s); or

(ii) If a particular Service Outage reported by Customer lasted for four (4) or more consecutive hours during a calendar month, a credit equal to two (2) days of the Monthly Service Fees payable of the amount of revenue Akamai receives from Customer with respect to the affected DDoS Mitigation Service(s).

The above provision sets forth Customer's sole and exclusive remedy for Service Outages and any other interruptions or failures of Akamai's Managed DDoS Mitigation Service. This SLA shall not apply to Prolexic

Services until those Services are Service Ready.

Remedy for Availability (applicable only to Prolexic Connect, Prolexic Routed, Prolexic Proxy, and Prolexic IP Protect Service Outage)

The following methodology will be employed to measure the availability and performance of the Service: Any reported or known incident that a Customer believes violates the Prolexic Availability SLA must be reported to Akamai via Akamai SOCC ticket for investigation, within (7) calendar days of the event. In reporting the incident to

Akamai, Customer should specify the date of the observed incident(s), the affected Service(s), the approximate event start and stop times, and general information about the observed impact of the event. Akamai will acknowledge receipt and investigate, providing a documented response to the Customer within (14) calendar days. Akamai will determine, in its sole good faith discretion and based on records, data and other evidence, whether a Customer-reported event constitutes a failure of the Availability and/or Performance Service Level Agreements. For each incident determined by Akamai to have violated the Availability SLA, the Customer will receive (as its sole remedy) a credit equal to Customer's fees for two (2) days of committed monthly service fees for the day(s) in which the failure occurs.

Remedy – Akamai Attack Monitoring Services (applicable only to Application-Based and Flow-Based Monitoring Services)

A Customer subscribing to the Akamai Application-Based Monitoring or Flow-Based Monitoring Service is entitled to remedy credit in accordance with this subsection should an Attack Monitoring Services - Failure to Notify Event occur, provided Customer reports the incident to Akamai promptly following the occurrence of an event that Customer believes is an Attack Monitoring Services - Failure to Notify Event, but in any event no later than five (5) calendar days after the event. Whether an incident constitutes an Attack Monitoring Services - Failure to Notify Event shall be determined by Akamai in its sole good faith discretion supported by records, data and other evidence.

(i) If an Attack Monitoring Services - Failure to Notify Event occurs once or more times during a calendar month, Akamai will credit Customer's account for the pro-rated charges for one (1) day's Monthly Service Fees due for each incident, in respect of the affected site(s)' Services; and

(ii) In addition to Customer being entitled to the above credits, in the event that three or more Attack Monitoring Services - Failure to Notify Events occur during a calendar month, Customer shall have the right, for 30 days following the start of such incident, to terminate the affected Service, without liability.

Akamai's Availability and Performance Service Level (applicable only to App and API Protector, Kona Site Defender, Kona DDoS Defender, Web Application Protector, Web Application Firewall, Bot Manager, Bot Manager Premier, Account Protector, and Site Shield)

● **Availability SLA:** Akamai offers a service level ("Service Level") committing to 100% availability of the contracted security service.
The Service Level begins at the time the Customer has successfully completed integration and Service Validation for the protected properties, or the contract Billing Effective Date, whichever is later.

● **Performance SLA:** Akamai offers a service level ("Service Level") committing that the security service will not impede origin performance in any period that the protected digital property is not under attack. The Service Level begins at the time the Customer has successfully completed integration and Service Validation for the protected properties, or the contract Billing Effective Date, whichever is later.

Activation of the Availability and Performance Service Level Agreements occurs once the Customer has successfully completed the following: Customer must enter and indicate the location of two valid test files for thesame object (as described in II(c) and (d) above) into the SLAActivation Tool located in the Provisioning Center on https://control.akamai.com (Akamai's Customer Portal). Detailed instructions are provided with the SLA Activation Tool on https://control.akamai.com; in addition, assistance is available from the Customer's Account Manager and, for Customers using the optional Site Shield solution, Akamai Professional Services. Customers using Remote Site

Shield must ensure that their firewall configurations are updated to reflect changes made by Akamai to the Site Shield access control list no later than 60 days following notification by Akamai, via email or the https://control.akamai.com customer portal, of such a change. Failure to timely update such firewall configurations will invalidate the performance portion of this SLA. The SLA will go into effect five (5) business days after the Customer enters valid test files into the SLAActivation Tool.

Remedy for Availability and Performance Service Levels (applicable only to App and API Protector, Kona Site Defender, Kona DDoS Defender, Web Application Protector, Web Application Firewall, Bot Manager Standard, Bot Manager Premier, Account Protector, and Site Shield)

If the Service fails to meet the defined service levels, the Customer will receive (as its sole remedy) a credit equal to Customer's or such domain's committed monthly security service fee for the day for the protected origin(s) in which the failure occurs, not to exceed 30 days of fees.

The following methodology will be employed to measure the availability and performance of the security service:

Agents and Polling Frequency

(a) From at least six (6) geographically and network-diverse locations in major metropolitan areas, Akamai will simultaneously poll a test file residing on the Customer's protected origin servers and on Akamai's network. The polling mechanism will perform two (2) simultaneous http GET operations using a test file on the Customer's protected origin server (ie, origin.customer.com).

One GET operation will be performed to retrieve the file directly from the protected origin server (ie, http://origin.customer.com/testobject), or via an Akamai Site Shield region if the Customer is using the Kona Site Defender or the optional Site Shield solution.

The other GET operation will be performed to retrieve the file through the Service, by requesting the object from the protected origin server (ie, http://www.customer.com/testobject,

where www.customer.com is CNAMEd to Akamai and configured to pull content from origin.customer.com)

(b) The Akamaized test content must use a TTL of 2 hours or greater.

(c) The test content will be a file of approximately 10 KB in size.

(d) Polling will occur at approximately 6-minute intervals.

(e) Based on the http GET operations described in II(b) above, the response times received from the two sources, (a) the protected Customer server (directly, or via a Site Shield region if applicable), and (b) the Akamai network, will be compared for the purpose of measuring performance metrics and outages.

Performance Metric

The performance metric will be based on a daily average of performance for the Service and the Customer's protected production origin (measured directly, or via a Site Shield region if applicable), computed from data captured across all regions and hits. If on a given day the Akamai daily average time exceeds the Customer's daily average time, then the Customer will receive (as its sole remedy) a credit equal to Customer's or such domain's committed monthly service fee for the protected property,for that day in which the failure occurs, not to exceed 30 days of fees.

Akamai's Prolexic Service Response Service Level Agreement (applicable only to the Prolexic Service)

Akamai agrees to provide a level of service to Customers purchasing the Prolexic Service as follows: a. Response Time

- For issues reported to Akamai by phone, the time to access an Akamai technical resource for DDoS or Customer-specific service emergencies shall be ≤ 5 minutes
- For issues reported to Akamai other than by telephone (e.g. email), Akamai's response time shall depend on the severity of the reported issue and shall be as follows:
- Severity 1 ≤ 30 minutes (must be opened via phone)
- Severity 2 ≤ 1 hour
- Severity 3 ≤ 1 business day

b. Live Support Availability: An Akamai representative will be available live on the phone to respond to Severity 1 (Critical Impact) and Severity 2 (Major Impact) Service issues 24 hours a day, 7 days a week and 365 days a year. Live Support Availability for severity 3 (Low Impact) cases will be available during

normal business hours, Monday through Friday, excluding local holidays, in the following geographies as follows:

- North America (GMT – 05:00): 9:00 am to 9:00 pm ET
- Europe (GMT): 08:00 am to 5:00 pm
- Asia-India (GMT + 05:30): 9:00 am to 6:00 pm
- Asia-Japan/Singapore (GMT + 08:30): 9:00 am to 6:00 pm

Remedy for Prolexic Service Response SLA Violation

In the event of a Prolexic Service Response SLA Violation, Customer must submit a written request for a credit (email request acceptable) to Customer's applicable Akamai relationship manager within seven days of the allegedSLA Violation. For acknowledged SLA Violations, Customer will receive (as its sole remedy) a credit equal to one day's worth of Customer's monthly Prolexic Service fee (for each day in which a failure occurs), not toexceed 30 days of fees per month.

Remedy Terms – General

In order for Akamai to issue a credit in accordance with this SLA, Customer must have an account that is current with payments and in good standing with Akamai, and must be able to confirm that Customer has successfully completed required integration, Provisioning, and/or Service Validation process(es) for the applicable Service and, if applicable, all Prior Competing Mitigation Techniques, Fixes and Gear have been disabled or removed during any mitigation services.

Credits shall only apply for Services provided pursuant to the Monthly Service Fee and/or Monthly Service Overage Fee, and will not apply to any other Service. Customers with subscriptions for more than one DDoS Mitigation Service will only receive credits for affected portion of DDoS Mitigation Service(s). The aggregate credits to be provided in any calendar month shall not exceed 25% of the Monthly Service Fee in respect of the affected Service(s).