SLA : Arelion DDOS Mitigation

V 3.0.1

17th May 2026

Arelion Product Team

Arelion

Service Level Agreement: Arelion Distributed Denial of Service (DDoS) Protection Service

Arelion AB
169 94 Solna, Sweden

Org nr. 556103-4249
T +46771990100

arelion.com

Arelion

Table of Contents

1 SCOPE

This Appendix is an integral part of the Arelion Master Service Agreement ("MSA" or "Agreement") and shall only apply on the terms specified herein, to the following products provided to Customer by Arelion:

- Arelion DDoS Protection Service

This Service Level Agreement ("SLA") defines levels of service and Customer's right to apply for credits in the event that the applicable service levels are not achieved. Terms not defined herein shall have the same definition as in the Agreement.

2 SERVICE DESCRIPTION

The Distributed Denial of Service (DDoS) Protection Service provides protection against the effects of DDoS attacks that target a Customer's Internet connection and Internet facing hosts. The Service provides protection against attacks based upon the TCP/UDP/IP suite of protocols that attempt to consume the resources of the target (e.g. Internet bandwidth) or to interfere with the normal operation of the target and, thereby, disrupt Customer's Internet-connected services.

The DDoS Protection Service operates by redirecting Internet traffic destined for hosts or network infrastructure that have been designated in accordance with this SLA for protection by Customer. Under normal operating conditions, Customer's traffic will flow to/from the Internet via the most direct path across Arelion's IP network. When protection is enabled, such traffic is routed through the DDoS Protection Service where it is analysed to identify and discard DDoS traffic. Legitimate traffic will be allowed to continue through the DDoS Protection Service to its destination. Customer also may define specific IP addresses that are to be considered as sources of legitimate traffic (a "White List") and that are not to be blocked or filtered by the DDoS Protection Service. IP addresses for inclusion in a White List must be defined and included in the DDoS Protection configuration form.

The hosts and infrastructure to be protected by the Service must be designated by Customer in advance and specified in a Customer specific configuration called a "Managed Object". By default, Customer is provided with a summary object and five (5) Managed Objects. Each Managed Object contains the destination IP addresses or IP

address prefixes of the hosts or infrastructure that Customer has designated for protection using a template that defines the mitigation countermeasures that will be pre-configured for a specific Managed Object and are chosen by Customer when completing the Service configuration form (the "Mitigation Template"). The Mitigation Template type is determined by the type of servers, hosts or equipment that will be protected.

3 DELIVERY

3.1 Initial Configuration

The initial configuration of the Service shall be completed by Arelion within ten (10) business days of receipt of a complete and accurate configuration sheet from Customer (the "Configuration Period"). If the initial configuration of the Service is not completed within the Configuration Period (excluding any period of delay attributable to missing, incomplete or inaccurate information), Customer is entitled to claim credits according to the table set forth below for each day of delay beyond the end of the Configuration Period, which shall be Customer's sole and exclusive remedy in connection with the delay.

Number of full working days by which Arelion fails to meet the Configuration Period	Service credits as a % of the committed monthly recurring charge (MRC)
1 to 5 days	10%
6 to 10 days	20%
11 to 20 days	30%
> 21 days	50%

The Customer shall not be entitled to any credits for RFS delays arising out of Customer's acts or omissions, a delay caused by Customer failing to provide a complete and correct configuration sheet, or an event of force majeure.

3.2 Service Changes

Standard Service changes may be made directly via the Arelion Customer Care Helpdesk without the need to engage Customer's account manager or to execute a new Service Order. Standard Service changes are listed below:

- Change IP addresses in a Managed Object:
- Add, remove, or alter an IP address.
- Move an IP address to a different Managed Object
- Whitelist changes: Add, remove or alter Whitelist entries
- Contacts: Add, remove, or alter contact details

When requesting the above change types, Arelion's Customer Care will email Customer the current DDoS Protection configuration form requesting that Customer make and highlight the required changes to the form and send it via email back to Arelion Customer Care.

All of the above listed changes will be processed during business hours and subject to standard delivery time of two business days. Customer Care is not able to make services changes to Customer's Service configuration. Customer is responsible for informing Arelion in a timely manner of any desired changes to its DDoS Protection, IP Connect or IP Transit Service that may impact Arelion's ability to provide Customer with the Service outlined in the relevant Agreement, Service Order or template, including contacts and functions/persons authorized to activate or deactivate the Service.

To implement Customer change order requests, active mitigation measures may need to be disabled during the implementation process. Change Orders may also cause an outage or disruption to Customer's IP Transit or IP Connect Service and any resulting period of unavailability will not be considered Fault time and will not give rise to service level credits for the relevant Service.

Arelion reserves the right to charge for change requests.

3.3 Urgent Service Change Requests

In the event of an active attack on unprotected resources, Customer may contact Arelion's Customer Care Helpdesk and ask for the implementation of urgent change requests. Customer Care will use commercially reasonable efforts to engage the Arelion Incident Response Team ("IRT") in order to implement emergency measures. This support is offered on a best effort basis with no service levels and is not subject to availability or Fault time service credits. To the extent that Customer requests protection for any Managed Objects not included in the Service, Customer will be responsible for the charges attributable to the addition of the Managed Object and the usage of the Service.

Arelion reserves the right to charge for all change requests, however, no charges will be made for changes established on a DDOS service whilst under attack and required to improve or restore service, with the specific exception of an upgrade to the service plan itself.

4 Availability

4.1 Service Platform Availability

The measurement period for the availability of the platform over with the Service is provided shall be coterminous with the monthly billing cycle. The availability is calculated monthly, beginning with the first full month.

$$Availability = \frac{TotalTime - \Sigma(FaultTime_n)}{TotalTime} * 100\,\%$$

where $TotalTime$ = the total time during the measurement period

and $\Sigma(FaultTime_n)$ = the sum of all fault times of the faults that occurred during the measurement period

The Service platform will be considered available as long as one or more DDoS scrubbing centers is available to receive Customer traffic when the DDoS Protection Service has been enabled.

4.2 Exclusions to Service availability

A Service Level will not be deemed to have not been achieved to the extent caused by any of the following:

- Planned maintenance.
- Customer's actions or omissions
- An event of Force Majeure
- The suspension, interruption, or termination of Service in accordance with the Agreement
- Customer's failure to adhere to any requirements, including configurations, for the use of the Service
- Measures taken to reduce potential or actual adverse impacts to Arelion's IP Network arising from the DDoS attack towards the IP addresses of the Managed Objects designated for protection under the Service, including but not limited to the "black holing" of the IP addresses being attacked or alteration of the routing of the traffic destined to the IP addresses being attacked.
- Problems such as (but not limited to) bandwidth exhaustion, IP address exposure, network jitter that arise at Customer origin sites.

Under no circumstances shall any IP Transit or IP Connect Service provided by Arelion be considered unavailable due to a fault, failure, error or omission in the DDoS Protection Service.

5 DDoS PROTECTION SERVICE LEVELS

The service levels and credits set forth in this Section shall apply to the DDoS Protection Service. The credit percentages stated in this section are applied to the monthly recurring charges ("MRC") for the usage band for the DDoS Protection Service as ordered by the Customer.

5.1 Availability Service Level and Credits

Availability of the Arelion DDoS Protection Service is **99.999%,** measured as specified in Section 4 above. Customer shall be entitled to request a credit in accordance to the table below. The Service guarantee does not apply to the extent that any unavailability is due to the exclusionary factors described in Section 4 above.

Monthly Uptime Percentage	Service Credit Percentage
< 99.999% ≥ 99.9%	10% of monthly charge
< 99.9% ≥ 99,5%	20% of monthly charge
< 99.5%	40% of monthly charge

5.2 Time to Mitigate

The DDoS Mitigation Service offers Customer a choice of Auto-Mitigation or Community (as defined below), which will be defined for each Managed Object and applied to all hosts protected by that Managed Object.

Arelion also offers, as a non-standard service, or in emergency situations, manual mitigation, where Customer will contact the Service Desk directly and request mitigation to be enabled. This is covered below.

Mitigation countermeasures will be enabled per host route. Once enabled, traffic destined for the host route to be protected will be redirected through the DDoS Protection Platform.

5.2.1 Auto-Mitigation

Auto-Mitigation automatically enables mitigation countermeasures for hosts that belong to a Managed Object with Auto-Mitigation configured. When Arelion's systems detect an attack that targets a host with Auto-Mitigation configured, traffic destined for that host will be automatically re-routed to Arelion's DDoS Protection Platform. Once Arelion's systems detect that an attack has finished, traffic destined for the host that was under attack will be automatically restored to its normal routing path.

5.2.2 Community Mitigation

When an attack is detected, Customer is responsible appending the required BGP Community to the IP prefix range that the DDoS Protection Service should be enabled with the specific pre-configured hosts that require protection. Traffic destined for that host(s) will be automatically re-routed to Arelion's DDoS Protection Platform. For hosts with Community Mitigation, a mitigation will only be activated when the BGP community is appended.

Once an attack has finished and Customer has removed the BGP Community from the IP Prefix range, traffic destined for the host that was under attack will be automatically restored to its normal routing path. Customer shall be responsible for initiating disablement of the mitigation techniques implemented in response to an attack by removing the BGP Community.

5.2.3 Manual Mitigation

When an attack is detected, Customer is responsible for either

- Logging on to the MyArelion Portal and activating mitigation against the specific alert . The mitigation can also be ceased from the MyArelion Portal

Or

- Contacting Arelion customer care, and requesting that the DDOS Protection Service be enabled for the specific pre-configurated costs that require protection. Arelion will then raise a ticket to enable DDOS protection (a "Case"). A mitigation will only be activated with Customers authorization. Once an attack has finished, DDOS protection will only be disabled upon direct request from Customer to Arelion Customer Care. Arelion aims to establish and cease DDOS mitigation within 15 minutes of the Case being opened or closed.

  For the absence of doubt, Arelion will not refund DDOS mitigation minutes incurred during this process.

5.2.4 Time to Enable Service Level

Arelion will enable DDoS Protection for each Managed Object designated by Customer for protection. If the Service is not enabled within the timeframe set forth below applicable to the method of mitigation selected by Customer (e.g., Manual or Automatic), then Customer may request a service credit for the host object affected by the delay in accordance with the table below:

Description	Time to Enable Service Level	Credit (applied as a% of the MRC for the affected service)	
Manual Mitigation (Via CSC)	15 minutes from Arelion's initiation of a case to enable DDoS Protection	>15 ≤ 30 minutes = 10% of MRC	>30 minutes = 50% of MRC
Manual Mitigation (Via MyArelion Portal)	5 minutes from activating mitigation on the DDOS Alarm	>5 ≤ 15 minutes = 50% of MRC	>15 minutes = 100% of MRC
Auto Mitigation	5 minutes from Initial DDoS Alarm	>5 ≤ 15 minutes = 50% of MRC	>15 minutes = 100% of MRC
Community Mitigation	10 minutes from the Community being appended to the Prefix	>5 ≤ 15 minutes = 50% of MRC	>15 minutes = 100% of MRC

6 CLAIM OF CREDITS

6.1 Limitation of Credits

Notwithstanding the occurrence of multiple events of unavailability or failures to meet the service levels set forth in this SLA, the maximum credit to the Customer during a monthly billing period is limited to 100% of the previous month's charges for the DDoS Protection Service.

6.2 Procedure

In order to receive credits, Customer must submit a claim utilizing Arelion's standard credit request form within thirty (30) days of the end of the calendar month in which the fault occurred. The credits will be based on the actual fault time. In the event of any dispute concerning the duration of an event of unavailability, Arelion's fault monitoring and clearance records will govern. If Customer fails to submit a claim within the applicable thirty days (30) period as defined above, Customer shall irrevocably waive the right to claim any credits for the Services affected by the failure.

Notwithstanding anything to the contrary in the Agreement, the claim and award of credits pursuant to this Service Level Agreement shall be Customer's sole and exclusive remedy in the event that the Service is unavailable or fails to meet the specified service level guarantees.