

Mitigation Portal API

KNOWLEDGE BASE - NOVEMBER 2026

IN THIS GUIDE

01 Scope and applicability
02 API design
03 API documentation
04 Access and authentication
05 Authorization and account context
06 Functional scope
07 Requests and responses
08 Fair and acceptable use
09 Versioning and compatibility
10 Responsibilities
11 Service levels and support

> This document is an informative description of the standard Inter.link Mitigation Portal API. The applicable service order, Service Level Agreement (SLA), and Master Services Agreement (MSA) prevail in the event of any conflict.

01

Scope and applicability

The Inter.link Mitigation Portal API (the 'API') provides programmatic access to the DDoS mitigation controls available in the Mitigation Portal. It allows the customer to read mitigation configuration, traffic and attack data, and to manage supported mitigation settings from their own tools, monitoring systems, and automation.

The API is an interface to the Inter.link DDoS Protection service and does not change its technical definition, eligibility requirements, availability, commercial terms, or billing. Those matters remain governed by the DDoS Protection specification and the applicable service order.

The API is separate from the Inter.link Portal API. Ordering, changing, and deleting Inter.link services, including DDoS Protection itself, is handled through the Inter.link Portal API, the customer portal, or Sales, and is outside the scope of this specification.

02

API design

The API is a RESTful interface. All requests are made over HTTPS, and request and response bodies use JSON. The API uses the HTTP methods `GET`, `POST`, `PUT`, and `DELETE`.

Every function of the Mitigation Portal web interface is implemented on top of the API. A control that the customer can use in the Mitigation Portal is therefore also available through the API, subject to the same permissions.

The API is intended for automated systems and scripts. It is not designed to be browsed with a web browser.

03

API documentation

The Mitigation Portal is built on the RioRey rWeb platform. The rWeb API developer guide documents the available resources and methods, request and response schemas, fields, and endpoint-specific examples. Resources described there that are reserved for platform administration are not available to customers; see Authorization and account context.

The API reference defines the currently deployed interface and the operations it exposes. The DDoS Protection specification defines the technical behaviour and limitations of the underlying mitigation service.

04

Access and authentication

The API uses API keys. A Mitigation Portal user can create a key from their user profile in the Mitigation Portal. Each key belongs to the user who created it and carries the same roles and permissions as that user.

The token value is displayed once, when the key is created. It cannot be retrieved afterwards. A lost key must be deleted and replaced with a new key. API keys do not expire automatically. A user revokes a key by deleting it.

The key is supplied on every request in the `Authorization` header, using the `token` scheme:

```
Authorization: token <API key>
```

The scheme name is not case-sensitive. API key authentication does not create a session or set session cookies, so the header must be included in each request.

An API key is an authentication credential and must be protected accordingly. It must not be embedded in public source code, included in tickets or logs without redaction, or shared with an unauthorized party. A key that is no longer required or is suspected of exposure must be deleted and, where needed, replaced.

05

Authorization and account context

Mitigation Portal access is organised by group. A customer's protected prefixes are arranged into zones within the customer's group, and each user holds one or more roles that define what they can view and change in that group. API requests are subject to the same roles, permissions, and validation as the Mitigation Portal web interface. Changes to a user's roles also apply to that user's API keys.

Platform-level functions, such as mitigation device, cluster, and backup management, are operated by Inter.link and are not available to customers.

06

Functional scope

The API reference organises the customer-available operations into resource groups.

RESOURCE GROUP	PURPOSE
Authentication and roles	Identify the authenticated user and the roles and permissions enabled for them
Groups	Read the customer's group and its users and roles
Zones	Read and configure zones, including zone configuration, revisions, subnets, rulesets, and filter lists
Zone traffic and victims	Read traffic statistics for a zone and the victim addresses detected within it
Victims	Read details of an individual victim address
Lists	Manage block lists, source allow lists, and destination allow lists

Typical uses include retrieving zone traffic statistics, listing zones with historical attacks above a threshold, retrieving top attacking sources, maintaining block and allow lists, and changing a zone's filter mode as part of an automated response.

Configuration changes made through the API take effect on live mitigation in the same way as changes made in the Mitigation Portal. Zone configuration is revisioned, and the current revision of a zone can be read through the API.

07

Requests and responses

Paged queries

Resources that return lists support paging and sorting through query parameters, in addition to each resource's own parameters.

PARAMETER	DESCRIPTION
`start_row`	First row to return. The first row is row 1.
`number_of_rows`	Number of rows to return. Must be greater than 0. All rows are returned when omitted.
`sort_name`	Column to sort by.
`sort_order`	`ASC` or `DESC`. Ascending is the default.
`sort_list`	URL-encoded list of `sort_name` and `sort_order` pairs, for resources that support multi-column sorting.

Paged responses wrap the results in a `data` array, together with `rows` and `start` fields.

Background jobs

Some requests take longer to process. These return `202 Accepted` together with a job status resource. The customer polls the job status with `GET /delayed_job_statuses/{id}` until the job is finished. The response contains a human-readable `message` and the boolean fields `finished` and `failed`. Once a job is finished, its status does not change. Job statuses are removed automatically after a period and can also be deleted with `DELETE /delayed_job_statuses/{id}`.

Response codes

CODE	MEANING
`200 OK`	The request was processed successfully.
`201 Created`	The request created a resource.
`202 Accepted`	The request was accepted, but processing is not yet complete. See Background jobs.
`400 Bad Request`	The request is invalid. The response body describes the problem.
`401 Unauthorized`	Authentication failed, or the user does not have the permission required for the request.
`422 Unprocessable Entity`	The request is well-formed, but the combination of parameters is not valid. The body lists errors by field name.
`500 Internal Server Error`	An unexpected error occurred while processing the request.

A `422` response body has the form:

```
{
  "field_name": ["error", "another_error"],
  "next_field": ["error"]
}
```

08

Fair and acceptable use

API access is subject to fair and acceptable use. The customer must design automation and polling intervals to avoid excessive request volume and unnecessary load on the mitigation platform.

09

Versioning and compatibility

The Mitigation Portal API follows the release of the Mitigation Portal. The interface can change when the Mitigation Portal is upgraded. The customer is responsible for monitoring the API documentation and validating its integrations after a Mitigation Portal upgrade.

10

Responsibilities

ACTIVITY	INTER.LINK	CUSTOMER
API platform and reference	Operates the Mitigation Portal and its API and provides the API reference	Uses only documented operations and validates integrations against the current reference
Authentication	Allows Mitigation Portal users to create and delete non-expiring per-user API keys	Protects keys, stores the token securely at creation, deletes keys that are no longer required or may be exposed, and redacts keys from diagnostic material
Authorization	Assigns customer groups and applies each user's roles and permissions to their API keys	Controls which users have Mitigation Portal access and ensures that automation targets the intended zones and resources
Mitigation configuration	Applies valid configuration changes to live mitigation	Validates changes before applying them and prevents unintended or duplicate changes
Requests and automation	Processes valid requests and exposes background job status	Selects reasonable polling intervals and checks responses and resulting state
Platform operation	Operates mitigation devices, clusters, and platform backups	Raises platform issues through Inter.link Support
Troubleshooting	Investigates API behaviour within the Inter.link support boundary	Provides timestamps, affected zones or resources, endpoint and method details, response codes, and redacted request and response evidence

11

Service levels and support

API questions and suspected faults may be submitted to Inter.link Support through the published support channels. Credentials and other secrets must be removed from all support material.

The Mitigation Portal API is not covered by an availability or performance SLA. Availability and performance commitments, incident priorities, response and restoration targets, maintenance rules, exclusions, remedies, and service credits for DDoS Protection are defined exclusively in its applicable SLA. Nothing in this informative specification changes those terms.

Need a hand?

Our network engineers are happy to help — reach out through the Inter.link Portal or visit inter.link.