

API

KNOWLEDGE BASE - NOVEMBER 2026

IN THIS GUIDE

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

> This document is an informative description of the standard Inter.link 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 Portal API (the 'API') provides programmatic access to supported customer platform functions. It allows the customer to integrate service ordering and management into their own workflows, tools, and automation systems.

The API is an interface to Inter.link services and does not change their technical definitions, eligibility requirements, availability, commercial terms, validation rules, provisioning processes, or billing. Those matters remain governed by the applicable product specification and service order.

The API exposes the operations documented in its own reference; availability varies by resource and lifecycle action. A function being available in the customer portal does not by itself mean that the same function is available through the API. Some workflows remain portal-only, ticket-based, Sales-assisted, or controlled through a network protocol such as BGP.

02

API documentation

The current Inter.link API reference documents the published endpoints and methods, authentication syntax, request and response schemas, fields, response codes, and endpoint-specific examples.

The API reference defines the currently deployed interface and the operations it exposes. The applicable product specification defines the technical behaviour and limitations of the underlying service. Availability of an API operation does not change service prerequisites or third-party requirements.

03

API surfaces

This specification applies to the Inter.link Portal API documented in the public API reference.

The Mitigation Portal API, used to manage DDoS mitigation controls, is a separate interface and is outside the scope of this specification. It is described in the Mitigation Portal API specification. The DDoS Protection specification defines the service-level scope of its mitigation controls.

04

Access and authentication

The Inter.link Portal API uses API keys. Every portal user can create a named key from the API Keys section of their user profile. Each key belongs to the individual user who created it and has the same permissions and tenant access as that user. The key is displayed after creation and is supplied to API requests using the authentication method defined in the current API reference.

API keys do not expire automatically. A user can revoke their own keys. All keys belonging to a portal user are invalidated when that user is disabled or deleted.

The interactive API Explorer is part of the API reference. After authorizing the Explorer with an API key, the customer can inspect documented operations, submit requests, and view their responses. Explorer requests use the supplied API key and act on the account and resources available to its user.

Explorer requests are live: an order submitted through the Explorer creates a binding order, and changes or deletions take effect on real services. 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 disabled or replaced through the supported account or support process.

05

Authorization and account context

API requests remain subject to applicable account permissions, service prerequisites, ownership checks, and validation. Changes to the creating user's permissions or tenant access also apply to that user's API keys. An API key does not bypass an external provider's required acceptance workflow.

An authorized reseller user can select a sub-customer tenant context by supplying the tenant identifier in the `as-tenant` request header. The reseller is responsible for ensuring that its automation acts on the intended tenant and resources.

06

Functional scope and processing

The API supports the resources and lifecycle actions identified in the current API reference. Support may differ between reading a resource and ordering, changing, or deleting it. The customer must not infer an unsupported lifecycle action from the availability of another action on the same resource.

API requests are subject to the applicable technical, authorization, feasibility, and availability checks. Some orders or changes may require additional validation, external acceptance, or Inter.link provisioning after the initial API request. A successful order request creates a binding order; it is not a quotation, simulation, or confirmation that provisioning is complete. The documented response and, where applicable, subsequent resource or order state must be used to determine the provisioning outcome. Provisioning status is available through the API and is obtained by polling the applicable documented resource.

Features which customer control is defined through BGP, a support ticket, Sales, or another management surface remain governed by that workflow unless the API reference explicitly documents an API operation for them.

07

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 platform.

API activity is recorded in internal Inter.link logs. A customer-visible API audit log is not provided.

08

Versioning and compatibility

The Inter.link Portal API is versioned. A breaking interface change is introduced through a new API version. No fixed deprecation or migration period is defined as this is handled on a case-by-case basis.

The customer is responsible for selecting the intended API version, monitoring the API documentation and release notes, validating its integrations against a replacement version, and completing any required migration before the version in use is retired.

09

Responsibilities

ACTIVITY	INTER.LINK	CUSTOMER
API platform and reference	Operates the API and publishes the current interface definition	Uses only documented operations and validates integrations against the current reference
Authentication	Allows every portal user to create and revoke non-expiring per-user API keys and invalidates them when the corresponding user is disabled or deleted	Protects keys, limits their distribution, revokes or replaces them when required, and redacts them from diagnostic material
Authorization	Applies the creating user's permissions and tenant access to their API keys	Controls portal-user access and ensures that automation targets the intended tenant and resources
Requests and automation	Processes valid supported requests and exposes provisioning status for polling	Supplies accurate data, selects reasonable polling intervals, validates responses and resulting state, and prevents unintended or duplicate changes
Audit information	Retains API activity in internal logs	Maintains any customer-required audit record within the customer's own automation because no customer-visible API audit log is provided
Service prerequisites	Applies the validation and provisioning workflow for the requested service	Maintains required authorizations, dependencies, capacity, and third-party accounts or approvals
Version migration	Introduces breaking changes through a new API version and communicates changes through the release notes	Monitors published changes, tests integrations, and migrates before the version in use is retired
Troubleshooting	Investigates API behaviour within the Inter.link support boundary	Provides timestamps, affected resources, endpoint and method details, response codes, and redacted request and response evidence

10

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 Inter.link 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 the underlying ordered services are defined exclusively in their 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.