Agistix API Policy

Accepting the Terms of Use

Please read these terms of use ("API Policy") carefully before using any API. If you do not agree to all the terms and conditions of this API Policy, do not use the API. An Agistix API is accessed by Customer under the following terms and conditions:

Introduction

This API Policy outlines the constraints placed on the number of requests that can be made to our API within a specific timeframe. Rate limiting is essential to ensure fair usage, protect our servers from overload, and maintain optimal performance for all users. By implementing rate limits, we can prevent abuse, ensure resource availability, and provide a consistent and reliable API experience.

Rate Limit Thresholds

The rate limits are subject to change and may vary based on the specific API endpoint or service being accessed.

The rate limits are counted per source IP and API user, whichever reaches the limit first. This means that if you have multiple users accessing the API from the same IP address, they will share the same rate limit. Similarly, if you have a single user accessing the API from multiple IP addresses, they will also share the same rate limit.

This approach ensures that all users have equal access to the API and prevents any single user or IP address from monopolizing resources. It also helps protect against abuse and malicious activity.

The current rate limits are as follows:

API Tier	Limit	Timeframe
Tier 1 (heavy requests)	10 requests per minute	1 minute
Tier 2 (light requests)	100 requests per minute	1 minute

The list of API endpoints for Tier 1 and Tier 2 (may be subject to change):

API Tier	API Endpoints
Tier 1 (heavy requests)	/api/booking-api/* /booking SOAP
Tier 2 (light requests)	Everything else

Exceeding Rate Limits

If you exceed the rate limit for a particular endpoint or service, you will receive an HTTP 429 "Too Many Requests" response status code. This indicates that you have temporarily exceeded the allowed request rate and need to wait before making additional requests. The response headers will typically include information about the rate limit, such as the remaining number of requests allowed and the time at which the limit will reset.

Rate Limit Handling

To avoid exceeding rate limits, we recommend that you:

- Monitor your API usage and track the number of requests you are making within the specified timeframes.
- Implement backoff strategies, such as exponential backoff, to handle rate limit errors gracefully.
- Consider caching frequently accessed data to reduce the number of API calls.
- Optimize your application logic to minimize unnecessary API requests.

Requesting additional API rate quota

To request additional API rate quota per source IP or user, please contact support@agistix.com.

Contact

If you have any questions or concerns about our API Policy, please contact our support team - support@agistix.com.

Updated 01/30/2025