Authentication API

1. Overview

The Authentication endpoint is the gateway to the Kamion API. It allows you to exchange a valid username and password for a short-lived **JSON Web Token (JWT)**.

The returned JWT (token) must be included as a Bearer token in the “Authorization” header for all subsequent API calls to authenticated endpoints.

Token Expiration: For security, the token expire **10 minutes** after being generated. You must implement a token refresh strategy to maintain an active session beyond 10 minutes.

2. Authentication

This endpoint authenticates a user's session. The authentication method is a POST request containing the user's credentials in a JSON body.

All communication must be over HTTPS to ensure credentials are encrypted in transit.

3. Endpoint

Environment	Endpoint
UAT	`https://customer-integration-api-uat.kamion.com.au/api/authentication/login`
Production	`https://customer-integration-api.kamion.com.au/api/authentication/login`

4. Data Model

Request Body

The body of the POST request must be a JSON object containing the user's credentials. These will be provided during initial set up (UAT) and before go-live (Production).

Field	Type	Required	Description
username	string	Yes	The user's registered email address.
password	string	Yes	The user's password.

Response Body

A successful request will return a 200 OK status and a JSON body containing the authentication token.

Field	Type	Description
token	string (JWT)	A JSON Web Token (JWT) to be used as a Bearer token in the “Authorization” header of subsequent API requests.

5. Example Request and Response

Example Request (cURL)

```
curl --location --request POST 'https://customer-integration-api-
uat.kamion.com.au/api/authentication/login' \
-H 'Content-Type: application/json' \
-d '{
  "username": "YOUR_USERNAME",
  "password": "YOUR_PASSWORD"
}'

```

Example Success Response

Status: 200 OK

```
{
  "token": "eyJraWQiOiJB..."
}

```

How to Use the Token

The returned token must be sent in the Authorization header of subsequent requests to protected endpoints.

Example cURL request to another endpoint:

```
curl -X 'POST' \
  'https://customer-integration-api-uat.kamion.com.au/api/consignment' \
  -H 'accept: */*' \
  -H 'Authorization: Bearer eyJraWQiOiJB...'
```

6. Error Handling

When an API call fails, the response body will contain a JSON object with details about the error.

Error Response Format

Generated json

```
{
  "type": "ApiException",
  "title": "An error occurred",
  "status": 401,
  "detail": "Response status code does not indicate success: 401 (Unauthorized).",
```

```
  "instance": "POST /api/authentication/login",
  "content": "{\"message\":\"Incorrect username or password. Please contact KAMION support.\"}",
  "trace-id": "0HNA1TRBMIQ65:00000001"
}
```

7. Status Codes

Code	Meaning	Description
200	OK	The credentials are valid and tokens have been returned.
400	Bad Request	The request body is malformed, or username/password is missing.
401	Unauthorized	The provided username or password is incorrect.
429	Too Many Requests	You have exceeded the rate limit. See the Retry-After header.
500	Internal Server Error	A generic error occurred on our end. Please contact Kamion Support.

8. Rate Limits

To protect against brute-force attacks, this endpoint has a strict rate limit.

- **10 requests per minute** per IP address.
- Repeated failed attempts from the same IP address **will** result in a temporary block.

9. Terms of Use

- This API is provided for use by authorised customers and partners only.
- You are responsible for the secure storage of usernames, passwords, and returned tokens.
- By using this API, you agree to our full Terms of Service.

10. Changelog

- **2024-04-01 - v1.4.0**
  - **NEW:** Initial release of the Authentication API.