API Specification

API Specification

> **Project:** {{PROJECT_NAME}} **API Name:** {{API_NAME}} **Version:** {{API_VERSION}} **Date:** {{DATE}} **Author:** {{AUTHOR}} **Status:** Draft | In Review | Approved **Reviewers:** {{REVIEWERS}} **Spec Format:** OpenAPI 3.1

Document History

Version	Date	Author	Changes
0.1	{{DATE}}	{{AUTHOR}}	Initial draft
{{VERSION}}	{{DATE}}	{{AUTHOR}}	{{CHANGE_SUMMARY}}

---

1. API Overview

Purpose: {{API_PURPOSE}} **Primary Consumers:** {{CONSUMER_DESCRIPTION}} (e.g., internal frontend, partner systems, public developers) **Design Philosophy:** REST + JSON | Resource-oriented | Stateless | Idempotent where possible

Base URLs:

Environment	Base URL
Production	`https://api.{{DOMAIN}}/v{{MAJOR_VERSION}}`
Staging	`https://api.staging.{{DOMAIN}}/v{{MAJOR_VERSION}}`
Development	`http://localhost:{{PORT}}/api/v{{MAJOR_VERSION}}`

---

2. API Versioning Strategy

Strategy: URL path versioning — `/api/v{MAJOR}`

Versioning rules:

- **MAJOR** version (v1 → v2): Breaking changes — new base path, deprecation notice ≥ 6 months
- **MINOR** additions: Non-breaking — new optional fields, new endpoints — no version bump
- **Patch**: Bug fixes — no schema changes

Deprecation Policy:

- Deprecated endpoints marked with `Deprecation` and `Sunset` headers
- Minimum {{DEPRECATION_PERIOD}} notice before removing deprecated endpoints
- Deprecation notices sent to: {{NOTIFICATION_CHANNEL}}

Sunset Header Example:

```
Deprecation: Sat, 01 Jan 2025 00:00:00 GMT
Sunset: Sat, 01 Jul 2025 00:00:00 GMT
Link: <https://api.{{DOMAIN}}/v2/{{resource}}>; rel="successor-version"
```

---

3. Authentication & Authorization

3.1 Authentication Methods

Primary: Bearer JWT (OAuth2 / OIDC)

```
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9...
```

JWT Claims:

```
{
  "sub": "user-uuid",
  "email": "user@example.com",
  "tenant_id": "tenant-uuid",
  "roles": ["{{ROLE_1}}", "{{ROLE_2}}"],
  "scopes": ["{{SCOPE_1}}:read", "{{SCOPE_1}}:write"],
  "iat": 1700000000,
  "exp": 1700003600
}
```

Token Lifetimes:

Token Type	Lifetime	Storage
Access Token	{{ACCESS_TTL}} (e.g., 1h)	Memory only (not localStorage)
Refresh Token	{{REFRESH_TTL}} (e.g., 30d)	HttpOnly cookie
API Key	Non-expiring (rotatable)	Secure vault

Refresh Flow:

```
POST /auth/refresh
Cookie: refresh_token={{REFRESH_TOKEN}}
→ 200: { "access_token": "...", "expires_in": 3600 }
→ 401: Refresh token expired — re-authenticate
```

3.2 API Keys (for server-to-server)

```
X-API-Key: ak_live_{{KEY_PREFIX_SHOWN_TO_USER}}
```

- API keys scoped to specific permissions
- Prefixed: `ak_live_` (production), `ak_test_` (test)
- Rotate via: `POST /api-keys/{id}/rotate`

3.3 OAuth2 Scopes

Scope	Description	Grantable to
`{{resource}}:read`	Read {{resource}} data	All auth users
`{{resource}}:write`	Create/update {{resource}}	{{ROLE_REQUIRED}}
`{{resource}}:delete`	Delete {{resource}}	{{ROLE_REQUIRED}}
`admin:*`	Full admin access	Admin users only

---

4. Common Headers

Request Headers

Header	Required	Description

`Authorization`	Yes (except public endpoints)	`Bearer {JWT}` or N/A
`Content-Type`	Yes (POST/PUT/PATCH)	`application/json`
`Accept`	No	`application/json` (default)
`X-Request-ID`	Recommended	UUID v4 — echoed in response for tracing
`X-Idempotency-Key`	Yes (POST mutations)	UUID v4 — prevents duplicate operations
`Accept-Language`	No	`en`, `no`, `de` — for localized error messages

Response Headers

Header	Description
`X-Request-ID`	Echo of request ID (or generated if not provided)
`X-RateLimit-Limit`	Rate limit ceiling
`X-RateLimit-Remaining`	Remaining requests in current window
`X-RateLimit-Reset`	Unix timestamp when rate limit resets
`X-Response-Time`	Server processing time in ms
`Cache-Control`	Caching directives
`ETag`	Entity tag for conditional requests

---

5. Error Response Format (RFC 7807)

```
{
  "type": "https://api.{{DOMAIN}}/errors/{{ERROR_CODE}}",
  "title": "Human-readable error title",
  "status": 400,
  "detail": "Specific, actionable error description",
  "instance": "/api/v1/{{resource}}/{{id}}",
  "traceId": "{{TRACE_ID}}",
  "errors": [
    {
      "field": "{{FIELD_NAME}}",
      "code": "{{VALIDATION_CODE}}",
      "message": "{{FIELD_SPECIFIC_MESSAGE}}"
```

```
    }
  ]
}
```

Standard Error Codes

HTTP Status	Error Type	When to Use
`400`	`validation-error`	Request body/params fail validation
`401`	`unauthorized`	Missing or invalid authentication
`403`	`forbidden`	Authenticated but lacks permission
`404`	`not-found`	Resource does not exist
`405`	`method-not-allowed`	HTTP method not supported
`409`	`conflict`	Duplicate or state conflict
`410`	`gone`	Resource permanently deleted
`422`	`business-rule-violation`	Business logic rejection
`429`	`rate-limit-exceeded`	Too many requests
`500`	`internal-error`	Unexpected server error
`502`	`bad-gateway`	Upstream service failure
`503`	`service-unavailable`	Planned downtime or overload

---

6. Pagination Strategy

Strategy: Cursor-based (preferred) | Offset-based (legacy support)

Cursor-Based (default for all new endpoints)

Request:

```
GET /api/v1/{{resource}}?limit=20&after={{CURSOR}}
```

Response:

```
{
  "data": [],
  "pagination": {
```

```
    "hasNextPage": true,
    "hasPreviousPage": false,
    "startCursor": "{{BASE64_CURSOR}}",
    "endCursor": "{{BASE64_CURSOR}}",
    "limit": 20
  }
}
```

Offset-Based (legacy)

Request:

```
GET /api/v1/{{resource}}?page=1&limit=20
```

Response:

```
{
  "data": [],
  "pagination": {
    "page": 1,
    "limit": 20,
    "total": 500,
    "totalPages": 25
  }
}
```

Limits: Minimum 1, Maximum 100 items per request.

---

7. Rate Limiting

Tier	Limit	Window	Scope
Anonymous	{{N}} req	per minute	Per IP
Authenticated (free)	{{N}} req	per minute	Per API key
Authenticated (paid)	{{N}} req	per minute	Per API key
Admin	{{N}} req	per minute	Per user

Rate limit exceeded response:

```
HTTP/1.1 429 Too Many Requests
X-RateLimit-Limit: {{LIMIT}}
X-RateLimit-Remaining: 0
X-RateLimit-Reset: 1700003600
Retry-After: 37

{
  "type": "https://api.{{DOMAIN}}/errors/rate-limit-exceeded",
  "title": "Rate Limit Exceeded",
  "status": 429,
  "detail": "You have exceeded {{N}} requests per minute. Retry after 37 seconds."
}
```

---

8. Endpoint Documentation

Resource: {{Resource Name}}

`POST /{{resource}}`

Summary: Create a new {{entity}} **Auth:** Required | Scope: `{{resource}}:write` **Idempotency:** Required — provide `X-Idempotency-Key`

Request:

```
POST /api/v1/{{resource}} HTTP/1.1
Authorization: Bearer {{TOKEN}}
Content-Type: application/json
X-Idempotency-Key: 550e8400-e29b-41d4-a716-446655440000

{
  "{{field1}}": "string (required)",
  "{{field2}}": 123,
  "{{field3}}": "ENUM_VALUE_A | ENUM_VALUE_B"
}
```

Response `201 Created`:

```
{
  "id": "550e8400-e29b-41d4-a716-446655440000",
  "{{field1}}": "value",
  "{{field2}}": 123,
  "{{field3}}": "ENUM_VALUE_A",
  "createdAt": "2024-01-01T00:00:00.000Z",
  "updatedAt": "2024-01-01T00:00:00.000Z"
}
```

Error scenarios:

Scenario	Status	Error Code
Missing required `{{field1}}`	400	`validation-error`
`{{field1}}` exceeds max length	400	`validation-error`
Duplicate `{{unique_field}}`	409	`conflict`
Invalid enum value	400	`validation-error`
Business rule: {{RULE_DESCRIPTION}}	422	`business-rule-violation`

`GET /{{resource}}/:id`

Summary: Retrieve a {{entity}} by ID **Auth:** Required | Scope: `{{resource}}:read` **Cache:** `ETag` + `Last-Modified` supported

Path Parameters:

Parameter	Type	Description
`id`	`UUID`	The {{entity}} unique identifier

Response `200 OK`:

```
{
  "id": "550e8400-e29b-41d4-a716-446655440000",
  "{{field1}}": "value",
  "createdAt": "2024-01-01T00:00:00.000Z"
}
```

Error scenarios:

Scenario	Status	Error Code

Invalid UUID format	400	`validation-error`
{{entity}} not found	404	`not-found`
Access to other tenant's data	403	`forbidden`

`GET /{{resource}}`

Summary: List {{entities}} with filtering and pagination **Auth:** Required | Scope: `{{resource}}:read`

Query Parameters:

Parameter	Type	Default	Description
`limit`	`integer [1-100]`	`20`	Items per page
`after`	`string`	—	Cursor for next page
`before`	`string`	—	Cursor for previous page
`sort`	`string`	`createdAt:desc`	Sort: `{field}:{asc|desc}`
`{{FILTER_1}}`	`string`	—	Filter by {{FILTER_1}}
`{{FILTER_2}}`	`string (ISO8601)`	—	Filter by date range: `after:DATE`
`search`	`string`	—	Full-text search

Response `200 OK`:

```
{
  "data": [
    { "id": "...", "{{field1}}": "..." }
  ],
  "pagination": {
    "hasNextPage": true,
    "endCursor": "{{CURSOR}}"
  }
}
```

---

9. Webhook Documentation

9.1 Webhook Configuration

Register endpoint: `POST /webhooks` **Test endpoint:** `POST /webhooks/{id}/test` **Signature verification:** HMAC-SHA256

9.2 Signature Verification

```
// Verify webhook authenticity
const payload = request.rawBody;
const signature = request.headers['X-Webhook-Signature'];
const secret = process.env.WEBHOOK_SECRET;

const expected = 'sha256=' + crypto
  .createHmac('sha256', secret)
  .update(payload)
  .digest('hex');

const isValid = crypto.timingSafeEqual(
  Buffer.from(signature),
  Buffer.from(expected)
);
```

9.3 Webhook Events

Event	Description	Payload
`{{entity}}.created`	{{entity}} created	`{id, ...}`
`{{entity}}.updated`	{{entity}} updated	`{id, changes: {...}}`
`{{entity}}.deleted`	{{entity}} deleted	`{id, deletedAt}`

9.4 Webhook Delivery

- **Timeout:** 30 seconds per delivery attempt
- **Retries:** 5 attempts with exponential backoff (1min, 5min, 30min, 2h, 12h)
- **Success:** Any 2xx response
- **Dead delivery:** Alert and suspend after 5 consecutive failures

---

10. OpenAPI 3.1 YAML Skeleton

```yaml
openapi: '3.1.0'

info:
  title: '{{API_NAME}}'
  description: '{{API_DESCRIPTION}}'
  version: '{{API_VERSION}}'
  contact:
    name: '{{TEAM_NAME}}'
    email: '{{TEAM_EMAIL}}'
  license:
    name: 'Proprietary'

servers:
  - url: 'https://api.{{DOMAIN}}/v{{MAJOR_VERSION}}'
    description: 'Production'
  - url: 'https://api.staging.{{DOMAIN}}/v{{MAJOR_VERSION}}'
    description: 'Staging'

security:
  - bearerAuth: []

tags:
  - name: '{{Resource}}'
    description: 'Operations on {{resource}}'

paths:
  /{{resource}}:
    post:
      tags: ['{{Resource}}']
      summary: 'Create {{entity}}'
      operationId: 'create{{Entity}}'
      security:
        - bearerAuth: ['{{resource}}:write']
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/Create{{Entity}}Request'
      responses:
```

```
        '201':
          description: 'Created'
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/{{Entity}}'
        '400':
          $ref: '#/components/responses/ValidationError'
        '401':
          $ref: '#/components/responses/Unauthorized'
        '409':
          $ref: '#/components/responses/Conflict'

    get:
      tags: ['{{Resource}}']
      summary: 'List {{entities}}'
      operationId: 'list{{Entities}}'
      parameters:
        - $ref: '#/components/parameters/limit'
        - $ref: '#/components/parameters/after'
      responses:
        '200':
          description: 'OK'
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/Paginated{{Entity}}Response'

components:
  securitySchemes:
    bearerAuth:
      type: http
      scheme: bearer
      bearerFormat: JWT

  parameters:
    limit:
      name: limit
      in: query
      schema:
```

```
      type: integer
      minimum: 1
      maximum: 100
      default: 20

  after:
    name: after
    in: query
    schema:
      type: string

schemas:
  {{Entity}}:
    type: object
    required: [id, {{field1}}, createdAt]
    properties:
      id:
        type: string
        format: uuid
      {{field1}}:
        type: string
      createdAt:
        type: string
        format: date-time

  Create{{Entity}}Request:
    type: object
    required: [{{field1}}]
    properties:
      {{field1}}:
        type: string
        minLength: 1
        maxLength: 255

  ProblemDetails:
    type: object
    properties:
      type:
        type: string
        format: uri
```

```
        title:
          type: string
        status:
          type: integer
        detail:
          type: string
        instance:
          type: string
        traceId:
          type: string

    Paginated{{Entity}}Response:
      type: object
      properties:
        data:
          type: array
          items:
            $ref: '#/components/schemas/{{Entity}}'
        pagination:
          type: object
          properties:
            hasNextPage:
              type: boolean
            endCursor:
              type: string

  responses:
    ValidationError:
      description: 'Validation Error'
      content:
        application/problem+json:
          schema:
            $ref: '#/components/schemas/ProblemDetails'
    Unauthorized:
      description: 'Unauthorized'
      content:
        application/problem+json:
          schema:
            $ref: '#/components/schemas/ProblemDetails'
    Conflict:
```

```
      description: 'Conflict'
      content:
        application/problem+json:
          schema:
            $ref: '#/components/schemas/ProblemDetails'
```

---

11. SDK Generation Notes

Generation tool: {{SDK_TOOL}} (e.g., openapi-generator, Speakeasy, Fern) **Generated SDKs:**

Language	Package	Registry
TypeScript/JS	`@{{ORG}}/{{sdk-name}}`	npm
Python	`{{org}}-{{sdk-name}}`	PyPI
Go	`github.com/{{org}}/{{sdk-name}}`	pkg.go.dev

Generation command:

```
openapi-generator-cli generate \
  -i ./api-specification.yaml \
  -g typescript-fetch \
  -o ./sdk/typescript \
  --additional-properties=npmName=@{{org}}/{{sdk-name}}
```

---

12. API Changelog

Version	Date	Change Type	Description
`{{API_VERSION}}`	{{DATE}}	Added	`POST /{{resource}}` endpoint
`{{API_VERSION}}`	{{DATE}}	Changed	`{{FIELD}}` is now optional (was required)
`{{API_VERSION}}`	{{DATE}}	Deprecated	`GET /{{old-resource}}` — use `GET /{{new-resource}}`
`{{API_VERSION}}`	{{DATE}}	Removed	`DELETE /{{old-resource}}` — deprecated since {{DATE}}

Approval

Role	Name	Date	Signature
Author			
API Consumer Rep			
Security Review			
Tech Lead			

Revision #7
Created 2026-02-23 12:05:05 UTC by John
Updated 2026-05-25 07:32:09 UTC by John