Me

Endpoints Summary

Method	Path	Swagger
`GET`	`/me/organization/`	Swagger ↗

> The User Organization API provides access to organization information for the authenticated user. This endpoint allows users to retrieve details about their organization membership, settings, and associated metadata. It's commonly used for displaying organization context in applications and implementing organization-based access controls.

Base URL: `https://gate.zequenze.com/api/v1`

Authentication: All endpoints require a Bearer token:

```
Authorization: Bearer <your-api-token>
```

Overview

The User Organization API category focuses on retrieving organization-related information for the currently authenticated user. This API is essential for applications that need to understand the organizational context of their users, implement role-based access controls, or display organization-specific information in user interfaces.

Key concepts to understand:

- **User Organization Context**: Each authenticated user belongs to one or more organizations, and this API provides access to that organizational data
- **Organization Metadata**: Includes details like organization name, settings, subscription status, and user permissions within the organization
- **Access Control**: The information returned is filtered based on the user's permissions and role within the organization

This endpoint is typically called during application initialization to establish the user's organizational context and configure the application interface accordingly.

Endpoints

GET /me/organization/

Description: Retrieves comprehensive organization information for the currently authenticated user. This endpoint returns details about the user's organization membership, including organization metadata, user permissions, subscription status, and configuration settings. Use this endpoint to establish organizational context when a user logs into your application.

Use Cases:

- Initialize application with user's organization settings and branding
- Determine user's permissions and role within their organization
- Display organization-specific dashboard elements and navigation
- Validate organization subscription status and feature access
- Configure organization-specific integrations and settings

Full URL Example:

```
https://gate.zequenze.com/api/v1/me/organization/
```

Parameters:

This endpoint does not accept any query parameters.

cURL Example:

```
curl -X GET "https://gate.zequenze.com/api/v1/me/organization/" \
  -H "Authorization: Bearer YOUR_API_TOKEN" \
  -H "Content-Type: application/json"
```

Example Response:

```
{
  "id": 12345,
  "name": "Acme Corporation",
  "slug": "acme-corp",
```

```
"display_name": "Acme Corporation",
"description": "Leading provider of industrial solutions",
"website": "https://www.acmecorp.com",
"industry": "Manufacturing",
"size": "enterprise",
"created_at": "2023-03-15T08:30:00Z",
"updated_at": "2024-01-20T14:22:00Z",
"settings": {
  "timezone": "America/New_York",
  "date_format": "MM/DD/YYYY",
  "currency": "USD",
  "language": "en-US"
},
"subscription": {
  "plan": "enterprise",
  "status": "active",
  "expires_at": "2024-12-31T23:59:59Z",
  "features": [
    "advanced_analytics",
    "api_access",
    "custom_integrations",
    "priority_support"
  ]
},
"user_role": {
  "role": "admin",
  "permissions": [
    "manage_users",
    "manage_settings",
    "view_analytics",
    "manage_integrations"
  ],
  "joined_at": "2023-04-01T09:15:00Z"
},
"limits": {
  "max_users": 500,
  "current_users": 127,
  "max_api_calls": 10000,
  "current_api_calls": 2341
},
```

```
  "branding": {
    "logo_url": "https://cdn.gate.zequenze.com/logos/acme-corp.png",
    "primary_color": "#0066CC",
    "secondary_color": "#F0F8FF"
  }
}
```

Response Codes:

Status	Description
200	Success - Returns the user's organization information
401	Unauthorized - Invalid or missing authentication token
403	Forbidden - User does not have permission to view organization details
429	Too Many Requests - Rate limit exceeded
500	Internal Server Error - Server encountered an error processing the request

---

Common Use Cases

Use Case 1: Application Initialization

When a user logs into your application, call this endpoint to retrieve their organization context and configure the user interface with appropriate branding, settings, and available features based on their subscription plan.

Use Case 2: Permission-Based Feature Access

Use the returned user role and permissions data to dynamically show or hide features in your application, ensuring users only see functionality they're authorized to access.

Use Case 3: Organization Dashboard

Display organization statistics, current usage against limits, and subscription information in an admin dashboard or settings page.

Use Case 4: Multi-Tenant Configuration

In multi-tenant applications, use the organization settings (timezone, currency, language) to customize the user experience and format data appropriately for each organization.

Use Case 5: Subscription Management

Check the subscription status and available features to guide users toward appropriate upgrade paths or notify them of upcoming subscription renewals.

Best Practices

- **Cache Organization Data**: Organization information changes infrequently, so cache the response for the duration of the user session to reduce API calls and improve performance.
- **Handle Permission Changes**: User permissions can be modified by organization administrators, so refresh organization data when users report access issues or after significant time periods.
- **Graceful Degradation**: Always handle cases where certain organization features or settings might be unavailable, and provide sensible defaults in your application.
- **Rate Limiting**: This endpoint is typically called once per session, but implement proper rate limiting and exponential backoff in case of errors to avoid hitting API limits.
- **Error Handling**: Implement robust error handling, especially for 403 errors which might indicate the user's access has been revoked or their organization status has changed.
- **Security Considerations**: Never expose sensitive organization information in client-side code or logs. Always validate user permissions server-side before performing privileged operations.

Revision #4
Created 2026-02-04 05:15:08 UTC by ipena@zequenze.com
Updated 2026-02-11 03:18:54 UTC by ipena@zequenze.com