Txlog Portal

Endpoints Summary

Method	Path	Swagger
`GET`	`/txlog_portal/`	Swagger ↗

> The Portal Transaction Log API provides access to detailed transaction records from the Zequenze portal authentication system. This endpoint allows you to retrieve, filter, and analyze user authentication events, session activities, and system interactions for monitoring, auditing, and troubleshooting purposes.

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

Authentication: All endpoints require a Bearer token:

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

Overview

The Portal Transaction Log API is designed for system administrators, security analysts, and developers who need to monitor and audit portal authentication activities. This API provides comprehensive access to transaction logs that capture every user interaction with the authentication portal, including logins, logouts, registrations, password changes, and various system events.

Key Features:

- **Comprehensive Transaction Types**: Track 26 different transaction types from user authentication to payment processing
- **Advanced Filtering**: Filter by date ranges, user, location, access point, and transaction type
- **Real-time Monitoring**: Access up-to-date transaction data for live monitoring dashboards

- **Audit Compliance**: Maintain detailed audit trails for security and compliance requirements
- **Troubleshooting Support**: Identify authentication issues and user experience problems

Common Use Cases:

- Security monitoring and intrusion detection
- User behavior analysis and session tracking
- Compliance reporting and audit trail generation
- System performance monitoring and troubleshooting
- Customer support and user assistance

The transaction logs include detailed metadata such as IP addresses, user agents, session IDs, location information, and status codes, providing a complete picture of portal activity.

Endpoints

GET /txlog_portal/

Description: Retrieves a paginated list of portal transaction records with comprehensive filtering capabilities. This endpoint is essential for monitoring user authentication activities, analyzing login patterns, troubleshooting authentication issues, and generating audit reports. Each transaction record contains detailed information about user interactions with the portal authentication system.

Use Cases:

- Monitor failed authentication attempts for security analysis
- Generate compliance reports showing user access patterns
- Troubleshoot authentication issues by filtering specific user sessions
- Analyze portal usage statistics across different locations and access points
- Track registration and user management activities

Full URL Example:

```
https://gate.zequenze.com/api/v1/txlog_portal/?type=ui&start_date=2024-01-01&end_date=2024-01-31&limit=50
```

Parameters:

Parameter	Type	In	Required	Description

type	string	query	No	Filter by transaction type. Use 'ui' for login, 'uo' for logout, 'ur' for registration, etc.
start_date	string	query	No	Start date for filtering (ISO format: 2024-01-01 or 2024-01-01T00:00:00Z)
end_date	string	query	No	End date for filtering (ISO format: 2024-01-31 or 2024-01-31T23:59:59Z)
user	integer	query	No	Filter transactions for a specific user ID
page	integer	query	No	Filter transactions from a specific page ID
access_point	integer	query	No	Filter by access point ID (WiFi hotspot, portal location)
location	integer	query	No	Filter by location ID (physical location or site)
cursor	string	query	No	Pagination cursor for efficient large dataset traversal
limit	integer	query	No	Number of results per page (default: 20, max: 100)

cURL Example:

```
curl -X GET "https://gate.zequenze.com/api/v1/txlog_portal/?type=ui&start_date=2024-01-01&limit=25" \
  -H "Authorization: Bearer YOUR_API_TOKEN" \
  -H "Content-Type: application/json"
```

Example Response:


```
{
  "next":
"https://gate.zequenze.com/api/v1/txlog_portal/?cursor=eyJpZCI6MTAwfQ%3D%3D&limit=25",
  "previous": null,
  "results": [
```

```
{
  "id": 12345,
  "datetime": "2024-01-15T14:30:25.123456Z",
  "type": "ui",
  "organization": 1,
  "source": "u",
  "status": "h200",
  "message": "User login successful",
  "service": 101,
  "service_name": "Corporate WiFi Portal",
  "authservice": 201,
  "authservice_name": "LDAP Authentication",
  "user": 5432,
  "username": "john.doe",
  "email": "john.doe@company.com",
  "external_id": "emp_12345",
  "new_user": false,
  "session_id": "sess_abc123xyz789",
  "external_session": "ldap_session_456",
  "payment_transaction_log": null,
  "site": "corporate-portal.company.com",
  "page": 10,
  "page_url": "https://corporate-portal.company.com/login",
  "action": "li",
  "location": 15,
  "location_name": "Headquarters Building A",
  "access_point": 42,
  "access_point_name": "AP-Floor3-West",
  "ssid": "Corporate_WiFi",
  "user_agent": 301,
  "remote_ip_addr": 987654321,
  "captured_ip_addr": 987654321,
  "mac_addr": 123456789,
  "http_referer": 501
},
{
  "id": 12344,
  "datetime": "2024-01-15T14:28:15.789012Z",
  "type": "ur",
  "organization": 1,
```

```
      "source": "u",
      "status": "h201",
      "message": "User registration completed",
      "service": 101,
      "service_name": "Corporate WiFi Portal",
      "authservice": null,
      "authservice_name": null,
      "user": 5433,
      "username": "jane.smith",
      "email": "jane.smith@company.com",
      "external_id": null,
      "new_user": true,
      "session_id": "sess_def456uvw012",
      "external_session": null,
      "payment_transaction_log": null,
      "site": "corporate-portal.company.com",
      "page": 12,
      "page_url": "https://corporate-portal.company.com/register",
      "action": "rg",
      "location": 15,
      "location_name": "Headquarters Building A",
      "access_point": 43,
      "access_point_name": "AP-Floor2-East",
      "ssid": "Guest_WiFi",
      "user_agent": 302,
      "remote_ip_addr": 987654322,
      "captured_ip_addr": 987654322,
      "mac_addr": 123456790,
      "http_referer": 502
    }
  ]
}
```


Transaction Types Reference:

Code	Description	Use Case
ua	Authenticate	Initial authentication attempts
ui	Login	Successful user logins
ue	Re-authenticate	Session re-authentication

Code	Description	Use Case
uo	Logout	User logout events
uc	User capture	Data capture during registration
ur	User registration	New user account creation
uu	User update	Profile or account updates
un	User activation	Account activation events
up	Password change	Password modification
um	User activated API	API-triggered user activation
ai	Auto-login	Automatic login processes
aa	Auto-authenticate	Automatic authentication
st	Session timeout	Session expiration events
si	Idle timeout	Idle session termination
di	Disconnect	Manual or forced disconnections

Response Codes:

Status	Description
200	Success - Returns filtered transaction records
400	Bad Request - Invalid filter parameters or date format
401	Unauthorized - Invalid or missing API token
403	Forbidden - Insufficient permissions to access transaction logs
429	Too Many Requests - Rate limit exceeded

Common Use Cases

Use Case 1: Security Monitoring Dashboard

Monitor failed authentication attempts and suspicious login patterns by filtering for specific status codes and authentication types.

```
# Get failed login attempts in the last 24 hours
curl -X GET
"https://gate.zequenze.com/api/v1/txlog_portal/?type=ui&status=u401&start_date=2024-01-
```

```
15T00:00:00Z&end_date=2024-01-15T23:59:59Z" \
  -H "Authorization: Bearer YOUR_API_TOKEN"
```

Use Case 2: User Session Analysis

Track a specific user's authentication journey by filtering their transactions across different session activities.

```
# Get all transactions for user ID 5432 in January 2024
curl -X GET "https://gate.zequenze.com/api/v1/txlog_portal/?user=5432&start_date=2024-01-01&end_date=2024-01-31" \
  -H "Authorization: Bearer YOUR_API_TOKEN"
```

Use Case 3: Location-Based Usage Reports

Generate usage statistics for specific locations or access points to understand traffic patterns and capacity planning.

```
# Get all transactions from a specific access point
curl -X GET "https://gate.zequenze.com/api/v1/txlog_portal/?access_point=42&start_date=2024-01-01&limit=100" \
  -H "Authorization: Bearer YOUR_API_TOKEN"
```

Use Case 4: Registration and User Management Audit

Track user registration activities and account management operations for compliance reporting.

```
# Get all registration-related transactions
curl -X GET "https://gate.zequenze.com/api/v1/txlog_portal/?type=ur,uu,un&start_date=2024-01-01&end_date=2024-01-31" \
  -H "Authorization: Bearer YOUR_API_TOKEN"
```

Use Case 5: Payment Transaction Monitoring

Monitor payment-related portal activities for e-commerce or paid access scenarios.

```
# Get payment process transactions
curl -X GET "https://gate.zequenze.com/api/v1/txlog_portal/?type=pp&start_date=2024-01-01" \
  -H "Authorization: Bearer YOUR_API_TOKEN"
```

Best Practices

- **Use Date Filtering**: Always apply date ranges to limit result sets and improve query performance. Large unbounded queries may timeout or hit rate limits.
- **Implement Pagination**: Use the cursor-based pagination for large datasets rather than requesting all records at once. The cursor parameter provides better performance than offset-based pagination.
- **Cache Common Queries**: Cache frequently accessed data like daily statistics or user lookup results to reduce API calls and improve application performance.
- **Monitor Rate Limits**: Transaction log endpoints may have strict rate limits. Implement exponential backoff and respect HTTP 429 responses.
- **Secure Token Storage**: Store API tokens securely and rotate them regularly. Transaction logs contain sensitive user information and require proper authentication.
- **Filter Efficiently**: Use specific filters (type, user, location) to reduce payload size and improve response times. Avoid broad queries during peak hours.
- **Error Handling**: Implement robust error handling for network timeouts, API errors, and malformed responses. Transaction logs are critical for security monitoring.
- **Data Retention Awareness**: Understand your organization's log retention policies. Historical data may not be available beyond certain time periods.

Revision #4
Created 2026-02-04 05:15:53 UTC by ipena@zequenze.com
Updated 2026-02-11 03:20:50 UTC by ipena@zequenze.com