Nexus Core API

Version: v2.4.0

Base URL: https://api.nexus-cloud.com/v2

1. General Overview

The Nexus Core API is the central integration layer of the Nexus Ecosystem. It exposes a RESTful interface designed for secure authentication, enterprise resource management, and business analytics. The API uses JSON as its primary data exchange format and communicates exclusively over HTTPS.

This document provides a comprehensive technical reference intended for software developers, system integrators, and solution architects.

2. Architecture Overview

Nexus Core API follows a stateless client-server architecture. All authenticated requests require a valid JSON Web Token (JWT) issued by the authentication service.

Authorization is enforced using role-based access control (RBAC), ensuring that each user can only access permitted resources.

3. Authentication and Security

Authentication within Nexus Core API is implemented using JWT-based access tokens. Access tokens have a limited lifespan and can be renewed using refresh tokens.

3.1 Generate Access Token

Method: POST

Endpoint: /auth/login

Description: Authenticates a user and returns an access token along with user metadata.

Parameters

email (string, required): Registered user email address.

password (string, required): User password in plain text.

client_id (string, required): Identifier of the consuming application.

ip_address (string, optional): Origin IP address of the login request.

3.2 Refresh Access Token

Method: POST

Endpoint: /auth/refresh

Description: Issues a new access token using a valid refresh token.

Parameters

refresh_token (string, required): Persistent refresh token.

client_id (string, required): Application identifier.

device_id (string, optional): Unique identifier of the client device.

4. User Management

User-related endpoints allow administrators and authorized systems to retrieve and manage users within an organization.

4.1 List All Users

Method: GET

Endpoint: /users

Description: Returns a paginated list of users associated with the organization.

Parameters

limit (integer, optional): Maximum number of records to return.

offset (integer, optional): Number of records to skip.

status (string, optional): Filter users by status (active, inactive).

role (string, optional): Filter users by assigned role.

4.2 Retrieve Specific User

Method: GET

Endpoint: /users/{userId}

Description: Retrieves detailed information for a specific user.

Parameters

userId (string, required): Unique user identifier.

include_permissions (boolean, optional): Whether to include permission details.

include_activity (boolean, optional): Whether to include recent activity summary.

5. Analytics and Events

The analytics module enables clients to record custom telemetry events for monitoring, auditing, and business intelligence purposes.

5.1 Track Custom Event

Method: POST

Endpoint: /analytics/events

Description: Records a custom analytics event for asynchronous processing.

Parameters

event_name (string, required): Name of the event.

event_category (string, required): Logical grouping of the event.

timestamp (string, optional): ISO 8601 timestamp of the event.

properties (object, optional): Custom metadata associated with the event.

user_id (string, optional): User associated with the event.

source (string, optional): Originating system or application.

6. Error Handling

The API uses standard HTTP status codes to indicate success or failure. Error responses are returned in JSON format with descriptive messages to facilitate troubleshooting.

7. Best Practices

Clients should store access tokens securely and avoid persisting them in unencrypted storage. Refresh tokens should be rotated periodically.

It is recommended to implement proper retry strategies and handle rate-limiting responses to ensure system stability.

8. Conclusion

Nexus Core API provides a scalable, secure, and extensible foundation for building modern enterprise integrations within the Nexus Ecosystem.