Authentication — Microsoft Entra ID

This document describes the authentication flow used by the BI Dashboard Web platform, based on Microsoft corporate login.

Authentication Strategy

The platform uses federated authentication via Microsoft Entra ID (formerly Azure Active Directory).

Users authenticate using their corporate Microsoft accounts.
The system does not store or manage user passwords.

Authentication Flow (High Level)

1. User accesses the frontend application
2. User clicks “Sign in with Microsoft”
3. Frontend redirects the user to Microsoft login
4. Microsoft authenticates the user
5. Microsoft returns an identity token (JWT)
6. Frontend sends the token to the backend
7. Backend validates the token
8. User access is granted

Frontend Responsibilities

- Trigger Microsoft login
- Handle redirect after login
- Store authentication token securely
- Send token in every API request

Authentication library:
- Microsoft Authentication Library (MSAL)

Backend Responsibilities

- Validate received JWT tokens
- Verify token signature and issuer
- Extract user identity information
- Enforce access rules and permissions

The backend never trusts the frontend without token validation.

Token Information Used

The backend may extract the following information from the token:
- User name
- Email address
- Unique user identifier
- Tenant identifier
- Group or role claims (if enabled)

Access Control Strategy

Access control can be based on:
- User identity
- Microsoft Entra ID groups
- Application roles

Examples:
- BI_Admin → Full access
- BI_Manager → Manager dashboards
- BI_Operator → Operational dashboards

Security Considerations

- No user passwords are stored
- Tokens have limited lifetime
- Token validation is mandatory on every request
- Secure storage of client secrets
- HTTPS enforced for all environments

Authentication Goals

- Single Sign-On (SSO)
- Corporate security compliance
- Centralized user management
- Minimal authentication complexity