

CUSTOMER PORTAL WEB APP TO AZURE AD INTEGRATION

AZURE APPLICATION REGISTRATION PROJECT PLAN

Project Name: Customer Support Portal to Azure AD Integration

Source Application: Customer Portal Web App v3.2

Target Application: Azure Active Directory

Connection Type: Microsoft Graph API via OAuth 2.0

Date: December 15, 2024

Author: Customer Experience Team

Classification: Customer Confidential

CONNECTION OVERVIEW

Customer Portal Web App (source application) connects to Azure Active Directory (target application) to authenticate customers, manage support tickets, access knowledge base articles, and enable single sign-on for integrated services. This integration provides seamless customer authentication and personalized support experiences.

APPLICATIONS INVOLVED

1. Customer Portal Web Application
 - Platform: ASP.NET Core 6.0
 - Framework: React 18.x frontend
 - Deployment: Azure App Service
 - Authentication: Azure AD B2C
2. Azure Active Directory
 - Service: Microsoft 365 Azure AD
 - Tenant: Customer organization tenant
 - User Types: External customers and support staff
 - Authentication: OAuth 2.0 with PKCE flow

REQUIRED AZURE APPLICATION PERMISSIONS

Critical Risk Permissions:

- User.ReadWrite.All: Manage customer profiles and authentication settings
- Directory.ReadWrite.All: Access customer organization directory information

High Risk Permissions:

- User.Read.All: Read customer profile information for personalization
- Group.ReadWrite.All: Manage customer support groups and access levels
- Application.ReadWrite.All: Manage integrated application access

Medium Risk Permissions:

- User.Read: Basic customer profile access for authentication
- Directory.Read.All: Read directory information for customer organization

mapping

- Group.Read.All: Read customer group memberships for access control

Low Risk Permissions:

- User.ReadBasic.All: Basic customer information for support tickets
- Profile.Read: Customer profile photos and basic information
- OpenId: Basic authentication and identity verification

DATA INTEGRATION FLOWS

Customer Authentication

Direction: Bidirectional (Customer Portal ↔ Azure AD)

- Customer login and authentication
- Single sign-on token management
- Multi-factor authentication coordination

Support Ticket Management

Direction: Read-only (Azure AD → Customer Portal)

- Customer identity verification for support requests
- Access level determination for knowledge base
- Support staff authentication and authorization

Customer Profile Synchronization

Direction: Bidirectional (Customer Portal ↔ Azure AD)

- Customer profile updates and preferences
- Contact information synchronization
- Support history and case management

COMPLIANCE AND SECURITY

- All customer data encrypted in transit and at rest
- GDPR compliance for European customer data
- Customer consent management for data processing
- Regular security audits and penetration testing
- SOC 2 Type II compliance for customer data handling