Microsoft SSO Setup - Komplette Anleitung

📋 Übersicht

Diese Anleitung führt dich durch die komplette Einrichtung von **Microsoft Single Sign-On (SSO)** für deine Gross ICT Website. Benutzer können sich dann mit ihrem Microsoft-Konto anmelden (Office 365, Outlook.com, Azure AD).

🎯 Was du erreichen wirst

- ✅ Benutzer können sich mit Microsoft-Konto anmelden
- ✅ Automatische Profildaten-Synchronisation (Name, E-Mail, Profilbild)
- ✅ Sichere OAuth 2.0 Authentifizierung
- ✅ Unterstützung für Office 365 und persönliche Microsoft-Konten

---

📦 Voraussetzungen

- [ ] Microsoft-Konto mit Azure-Zugriff (Office 365 Admin oder persönliches Konto)
- [ ] Zugriff auf https://portal.azure.com
- [ ] Deine Website läuft auf https://gross-ict.ch

Teil 1: Azure AD App Registration

Schritt 1: Azure Portal öffnen

1. **Öffne deinen Browser** und gehe zu:

   ```
   https://portal.azure.com
   ```

2. **Melde dich an** mit deinem Microsoft-Konto
   - Verwende dein Office 365 Admin-Konto ODER
   - Verwende dein persönliches Microsoft-Konto
3. **Warte**, bis das Azure Portal vollständig geladen ist

Schritt 2: Azure Active Directory finden

Option A: Über die Suche (Empfohlen)

1. Klicke auf die **Suchleiste** oben im Portal
2. Tippe ein: `Azure Active Directory` oder `Microsoft Entra ID`
3. Klicke auf das Suchergebnis **"Azure Active Directory"**

Option B: Über das Menü

1. Klicke auf das ☰ **Hamburger-Menü** (oben links)
2. Scrolle nach unten zu **"Azure Active Directory"**
3. Klicke darauf

Schritt 3: App Registrations öffnen

1. Du bist jetzt in **Azure Active Directory**
2. Schaue im **linken Menü** nach **"App registrations"** (App-Registrierungen)
3. Klicke auf **"App registrations"**

Schritt 4: Neue App registrieren

1. Klicke oben auf den Button **" + New registration"** (+ Neue Registrierung)
2. **Fülle das Formular aus:**

Name:

```
Gross ICT Website
```

Supported account types: (Unterstützte Kontotypen)

- ✅ Wähle: **"Accounts in any organizational directory and personal Microsoft accounts"**
- (Konten in allen Organisationsverzeichnissen und persönliche Microsoft-Konten)
- Das ermöglicht sowohl Office 365 als auch private Microsoft-Konten

Redirect URI: (Umleitungs-URI)

- Platform: Wähle **"Web"** aus dem Dropdown
- URI: Gib ein:

```
https://gross-ict.ch/api/auth/microsoft/callback
```

1. Klicke auf **"Register"** (Registrieren) am unteren Rand
2. **Warte** 2-3 Sekunden, bis die App erstellt wurde

Schritt 5: Application ID und Tenant ID kopieren

Du siehst jetzt die **Overview-Seite** deiner neuen App.

Application (client) ID kopieren:

1. Suche das Feld **"Application (client) ID"**
2. Es sieht so aus: `a1b2c3d4-e5f6-7890-abcd-ef1234567890`
3. Klicke auf das 📋 **Kopier-Symbol** rechts neben der ID
4. **Speichere diese ID** in einem Textdokument:

```
Application (client) ID: [hier einfügen]
```

Directory (tenant) ID kopieren:

1. Suche das Feld **"Directory (tenant) ID"**
2. Es sieht so aus: `x9y8z7w6-v5u4-3210-zyxw-vu9876543210`
3. Klicke auf das 📋 **Kopier-Symbol** rechts neben der ID
4. **Speichere diese ID** in deinem Textdokument:

```
Directory (tenant) ID: [hier einfügen]
```

Schritt 6: Client Secret erstellen

1. Schaue im **linken Menü** nach **"Certificates & secrets"** (Zertifikate & Geheimnisse)
2. Klicke auf **"Certificates & secrets"**
3. Du siehst jetzt zwei Tabs: **"Certificates"** und **"Client secrets"**

4. Stelle sicher, dass du im Tab **"Client secrets"** bist
5. Klicke auf **"+ New client secret"** (+ Neuer geheimer Clientschlüssel)
6. **Fülle das Formular aus:**
   - **Description:** (Beschreibung)

     ```
     Gross ICT Website Secret
     ```

   - **Expires:** (Läuft ab)
     - Wähle: **"24 months"** (24 Monate) - Empfohlen
     - Oder: **"Custom"** für ein spezifisches Datum
7. Klicke auf **"Add"** (Hinzufügen)
8. ⚠ **SEHR WICHTIG - NUR EINMAL SICHTBAR:**
   - Du siehst jetzt eine neue Zeile mit deinem Secret
   - In der Spalte **"Value"** steht ein langer String
   - **Klicke auf das 📋 Kopier-Symbol** und kopiere den **Value** (NICHT die Secret ID!)
   - **Speichere diesen Wert SOFORT** in deinem Textdokument:

     ```
     Client Secret Value: [hier einfügen]
     ```

   - ⚠ **Dieser Wert wird nie wieder angezeigt!** Wenn du ihn verlierst, musst du einen neuen erstellen.

Schritt 7: API Permissions konfigurieren

1. Schaue im **linken Menü** nach **"API permissions"** (API-Berechtigungen)
2. Klicke auf **"API permissions"**

3. Du siehst bereits eine Permission: **"User.Read"** - das ist gut!
4. Klicke auf **"+ Add a permission"** (+ Berechtigung hinzufügen)
5. **Wähle Microsoft Graph:**
    - Im Popup-Fenster siehst du verschiedene APIs
    - Klicke auf **"Microsoft Graph"**
6. **Wähle Delegated permissions:**
    - Klicke auf **"Delegated permissions"**
7. **Füge diese Permissions hinzu:**

Suche nach **"email"**:

- ✅ Aktiviere die Checkbox bei **"email"**

Suche nach **"profile"**:

- ✅ Aktiviere die Checkbox bei **"profile"**

Suche nach **"openid"**:

- ✅ Aktiviere die Checkbox bei **"openid"**

1. Klicke auf **"Add permissions"** (Berechtigungen hinzufügen) am unteren Rand
2. **Optional - Admin Consent:**
    - Wenn du ein Admin-Konto hast, siehst du einen Button: **"Grant admin consent for [Your Organization]"**
    - Klicke darauf, wenn verfügbar
    - Das erspart Benutzern die Zustimmung beim ersten Login

Schritt 8: Überprüfung

Du solltest jetzt folgende **API permissions** sehen:

- ✅ **User.Read** (Microsoft Graph, Delegated)

- ✅ **email** (Microsoft Graph, Delegated)
- ✅ **profile** (Microsoft Graph, Delegated)
- ✅ **openid** (Microsoft Graph, Delegated)

Status sollte sein:

- **Granted for [Your Organization]** (grüner Haken) ODER
- **Not granted** (dann müssen Benutzer beim ersten Login zustimmen)

✅ Checkliste - Teil 1 abgeschlossen

Du solltest jetzt diese **3 Werte** haben:

```
Application (client) ID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Directory (tenant) ID: yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy
Client Secret Value: zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
```

⚠ **Bewahre diese Werte sicher auf!** Sie sind wie Passwörter.

Teil 2: Backend-Integration (Automatisch)

Sobald du mir die 3 Werte gibst, implementiere ich automatisch:

Was implementiert wird:

1. Datenbank-Schema

- Neue Tabelle `oauth_providers` für Microsoft-Tokens
- Verknüpfung mit bestehenden Benutzern

2. Backend-API

- **OAuth-Flow-Handler:** `/api/auth/microsoft`
- **Callback-Handler:** `/api/auth/microsoft/callback`
- **Token-Refresh-Logik:** Automatische Erneuerung abgelaufener Tokens
- **User-Profile-Sync:** Automatisches Abrufen von Microsoft-Profildaten

3. Sicherheit

- Sichere Token-Speicherung (verschlüsselt)
- CSRF-Protection
- State-Parameter-Validierung
- Scope-Validierung

4. Frontend-Integration

- **"Mit Microsoft anmelden" -Button** auf der Login-Seite
- Microsoft-Logo und Branding
- Automatische Weiterleitung nach erfolgreicher Anmeldung
- Fehlerbehandlung mit benutzerfreundlichen Meldungen

Teil 3: Konfiguration in der Website

Nach der Implementierung musst du die Credentials in der Website hinterlegen:

Schritt 1: Admin-Dashboard öffnen

1. Gehe zu: `https://gross-ict.ch/admin`
2. Melde dich mit deinem Admin-Konto an

Schritt 2: OAuth-Einstellungen öffnen

1. Klicke im Admin-Dashboard auf **"Einstellungen"**
2. Klicke auf **"OAuth-Provider"** (neuer Menüpunkt)

Schritt 3: Microsoft SSO konfigurieren

1. Klicke auf **"Microsoft hinzufügen"**
2. Fülle das Formular aus:
   - **Provider Name:** `Microsoft`
   - **Client ID:** [Deine Application (client) ID]
   - **Client Secret:** [Dein Client Secret Value]
   - **Tenant ID:** [Deine Directory (tenant) ID]
   - **Status:** `Aktiv` ✅
3. Klicke auf **"Speichern"**

Teil 4: Testen

Schritt 1: Ausloggen

1. Logge dich aus deinem Admin-Account aus
2. Gehe zur Login-Seite: `https://gross-ict.ch/login`

Schritt 2: Microsoft-Login testen

1. Du siehst jetzt einen neuen Button: **"Mit Microsoft anmelden"**
2. Klicke auf den Button

3. Du wirst zu Microsoft weitergeleitet
4. **Melde dich mit deinem Microsoft-Konto an**
5. **Erlaube die Berechtigungen** (wenn gefragt)
6. Du wirst zurück zu gross-ict.ch weitergeleitet
7. **Du bist jetzt eingeloggt!** ✅

Schritt 3: Profil überprüfen

1. Gehe zu deinem Benutzerprofil
2. Überprüfe, dass folgende Daten korrekt sind:
   - ✅ Name
   - ✅ E-Mail-Adresse
   - ✅ Profilbild (falls vorhanden)

Häufige Probleme und Lösungen

Problem 1: "Redirect URI mismatch"

Fehler: `AADSTS50011: The redirect URI specified in the request does not match`

Lösung:

1. Gehe zurück zu Azure Portal → App registrations
2. Klicke auf deine App "Gross ICT Website"
3. Klicke auf "Authentication" im linken Menü
4. Überprüfe, dass die Redirect URI **exakt** so lautet:

```
https://gross-ict.ch/api/auth/microsoft/callback
```

5. Achte auf:
   - ✅ `https://` (nicht `http://`)
   - ✅ Keine Leerzeichen
   - ✅ Kein `/` am Ende

Problem 2: "Invalid client secret"

Fehler: `AADSTS7000215: Invalid client secret provided`

Lösung:

1. Das Client Secret ist abgelaufen oder falsch kopiert
2. Gehe zu Azure Portal → App registrations → Certificates & secrets
3. Erstelle ein **neues Client Secret**
4. Kopiere den neuen Value
5. Update die Konfiguration in der Website

Problem 3: "Insufficient privileges"

Fehler: `AADSTS65001: The user or administrator has not consented`

Lösung:

1. Gehe zu Azure Portal → App registrations → API permissions
2. Klicke auf "Grant admin consent for [Your Organization]"
3. Bestätige mit "Yes"

Problem 4: Login funktioniert, aber keine Profildaten

Lösung:

1. Überprüfe, dass alle API Permissions gewährt wurden:
    - User.Read
    - email
    - profile
    - openid
2. Klicke auf “Grant admin consent” in Azure Portal

Sicherheitshinweise

✅ Best Practices

1. **Client Secret sicher aufbewahren:**
    - Niemals im Code speichern
    - Niemals in Git committen
    - Nur in der Datenbank (verschlüsselt) oder Umgebungsvariablen
2. **Regelmäßige Rotation:**
    - Erneuere das Client Secret alle 12-24 Monate
    - Azure warnt dich 30 Tage vor Ablauf
3. **Monitoring:**
    - Überwache fehlgeschlagene Login-Versuche
    - Überprüfe regelmäßig die Azure AD Sign-in Logs
4. **Least Privilege:**
    - Fordere nur die Permissions an, die du wirklich brauchst
    - Aktuell: User.Read, email, profile, openid

Support und Hilfe

Microsoft-Dokumentation

- **Azure AD OAuth:** https://learn.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow
- **Microsoft Graph API:** https://learn.microsoft.com/en-us/graph/overview

Bei Problemen

1. **Überprüfe die Azure AD Sign-in Logs:**
    - Azure Portal → Azure Active Directory → Sign-in logs
    - Filtere nach deiner App "Gross ICT Website"
2. **Überprüfe die Error Codes:**
    - https://learn.microsoft.com/en-us/azure/active-directory/develop/reference-error-codes
3. **Kontaktiere mich:**
    - Sende mir Screenshots von Fehlermeldungen
    - Sende mir die Error Codes aus den Azure Logs

Nächste Schritte

Nach erfolgreicher Einrichtung kannst du:

1. **Weitere OAuth-Provider hinzufügen:**
    - Google SSO
    - GitHub SSO

    - LinkedIn SSO

2. **Multi-Factor Authentication (MFA):**
    - Azure AD unterstützt MFA automatisch
    - Benutzer können MFA in ihrem Microsoft-Konto aktivieren
3. **Conditional Access:**
    - Definiere Regeln für den Zugriff (z.B. nur aus bestimmten Ländern)
    - Erfordert Azure AD Premium

Zusammenfassung

✅ Was du gemacht hast:

- Azure AD App Registration erstellt
- Client ID, Tenant ID und Client Secret erhalten
- API Permissions konfiguriert

✅ Was ich implementiere:

- Backend OAuth-Flow
- Token-Management
- User-Profile-Sync
- Frontend Microsoft-Login-Button

✅ Ergebnis:

- Benutzer können sich mit Microsoft-Konto anmelden
- Automatische Profildaten-Synchronisation
- Sichere OAuth 2.0 Authentifizierung

Bereit für die Implementierung?

Sende mir die 3 Werte:

```
Application (client) ID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Directory (tenant) ID: yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy
Client Secret Value: zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
```

Dann starte ich mit der Backend-Integration! 🚀