Microsoft ID 배포(2부)

- 인증 구현
- 권한 부여 구현

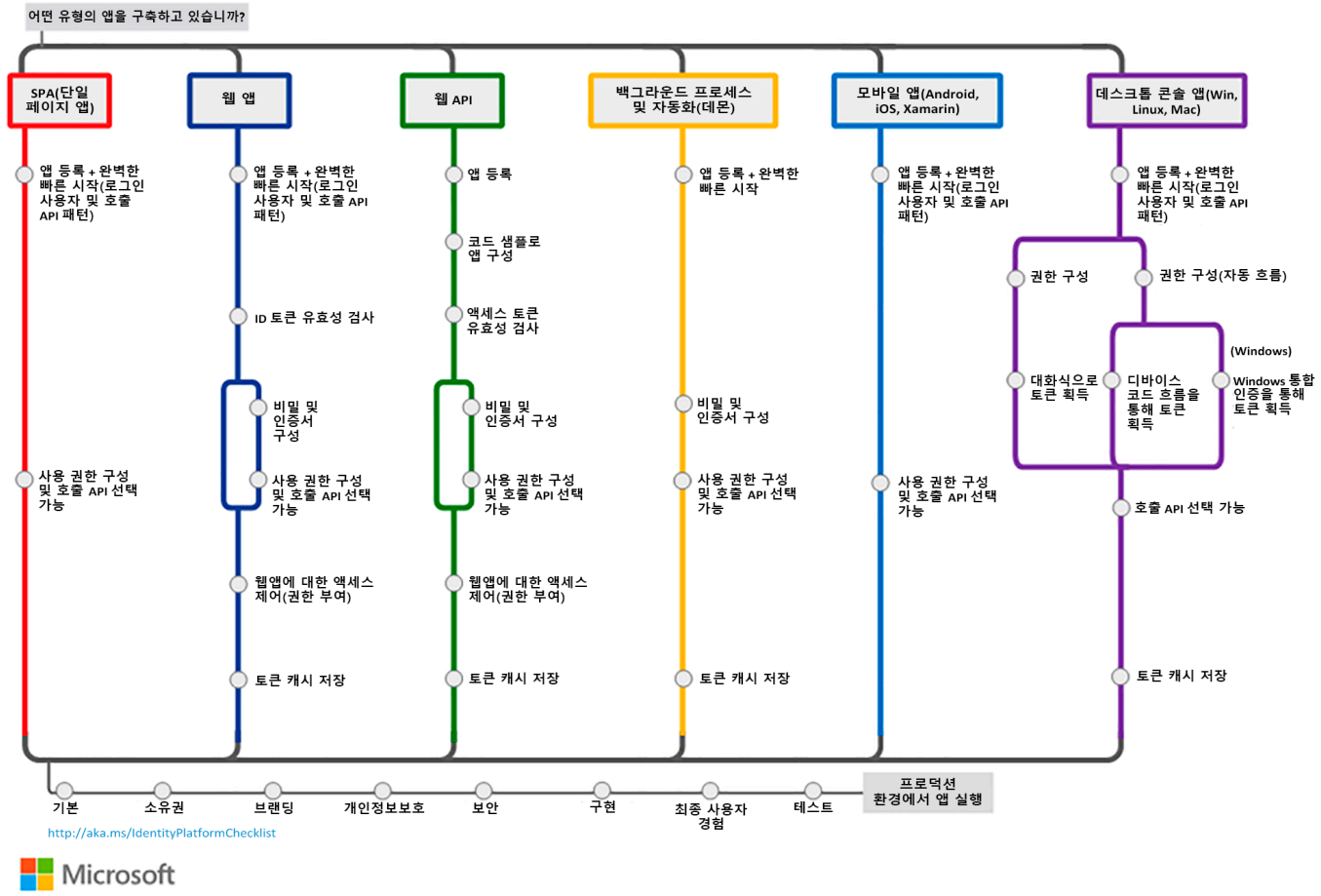
Microsoft

인증 구현

인증 흐름 및 애플리케이션 시나리오

인증 범주

- 보호된 리소스와 클라이언트 애플리케이션 비교
- 사용자 포함 또는 사용자 제외
- 단일 페이지, 공용 클라이언트 및 기밀 클라이언트 애플리케이션
- 로그인 고객
- 지원되는 OAuth 2.0 흐름
- 지원되는 플랫폼



Microsoft Authentication Library(MSAL)

Microsoft Authentication Library(MSAL)를 사용하면 개발자가 보안된 웹 API에 액세스하기 위해 Microsoft ID 플랫폼 끝점에서 토큰을 획득할 수 있습니다.

- 애플리케이션 유형 및 시나리오
- 언어 및 프레임워크

Microsoft ID용 보안 토큰

- ID 토큰

ID 토큰은 클라이언트가 사용자의 ID를 확인할 수 있는 보안 토큰입니다.

- 액세스 토큰

액세스 토큰을 사용하면 클라이언트가 Azure AD에 의해 보호되는 API를 안전하게 호출할 수 있습니다. 액세스 토큰은 "사용자+앱" 또는 "앱 전용"이라고도 합니다.

데모

인증 구현

Microsoft

권한 부여 구현

권한 부여 모델 개요

Microsoft ID 플랫폼과 통합되는 애플리케이션은 사용자와 관리자가 데이터에 액세스하는 방법을 제어하도록 허용하는 권한 부여 모델을 따릅니다.

- OAuth 2.0 권한 부여 코드 흐름
- 범위 및 권한
- 위임된 권한과 애플리케이션 권한 비교
  - 유효 권한
- 전체 테넌트에 대한 동의 요청
- 관리 제한 권한

관리자 동의

- 일부 권한은 테넌트 내에서 부여되기 이전에 관리자의 동의가 필요합니다. 관리자 동의 끝점을 사용하여 전체 테넌트에 권한을 부여할 수도 있습니다.
- 앱 등록 UI에는 앱에 부여된 권한 및 관리자 동의가 표시됩니다. 다음 섹션이 있습니다.
  - 구성된 권한
  - 부여된 기타 권한
  - 관리자 동의 단추
- 디렉터리 관리자에게 권한을 요청합니다.
- 애플리케이션 승인 동의 이해

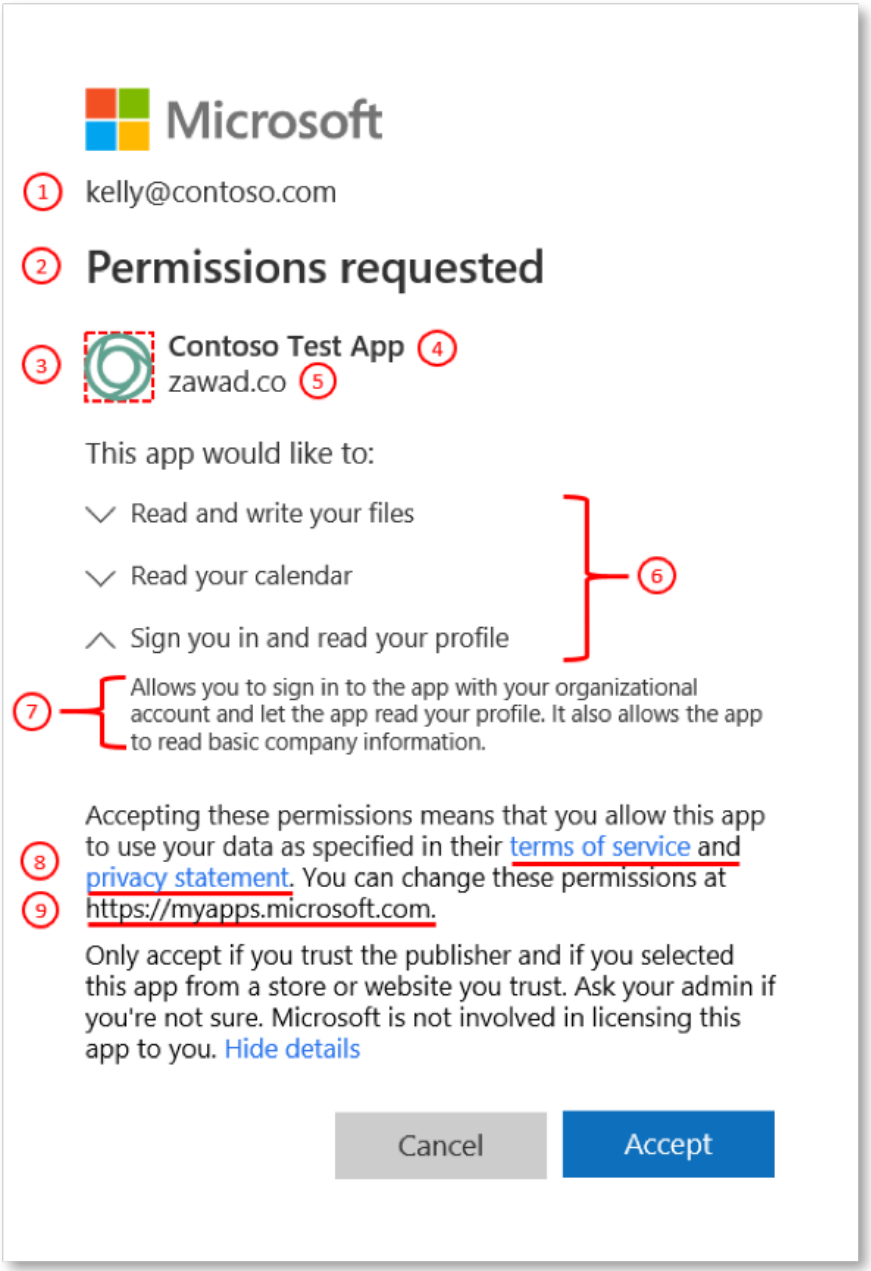
애플리케이션 동의 환경

- 사용자 동의 흐름

애플리케이션 개발자가 현재 사용자에 대해서만 동의를 기록하려는 의도로 사용자를 권한 부여 끝점으로 안내하는 경우

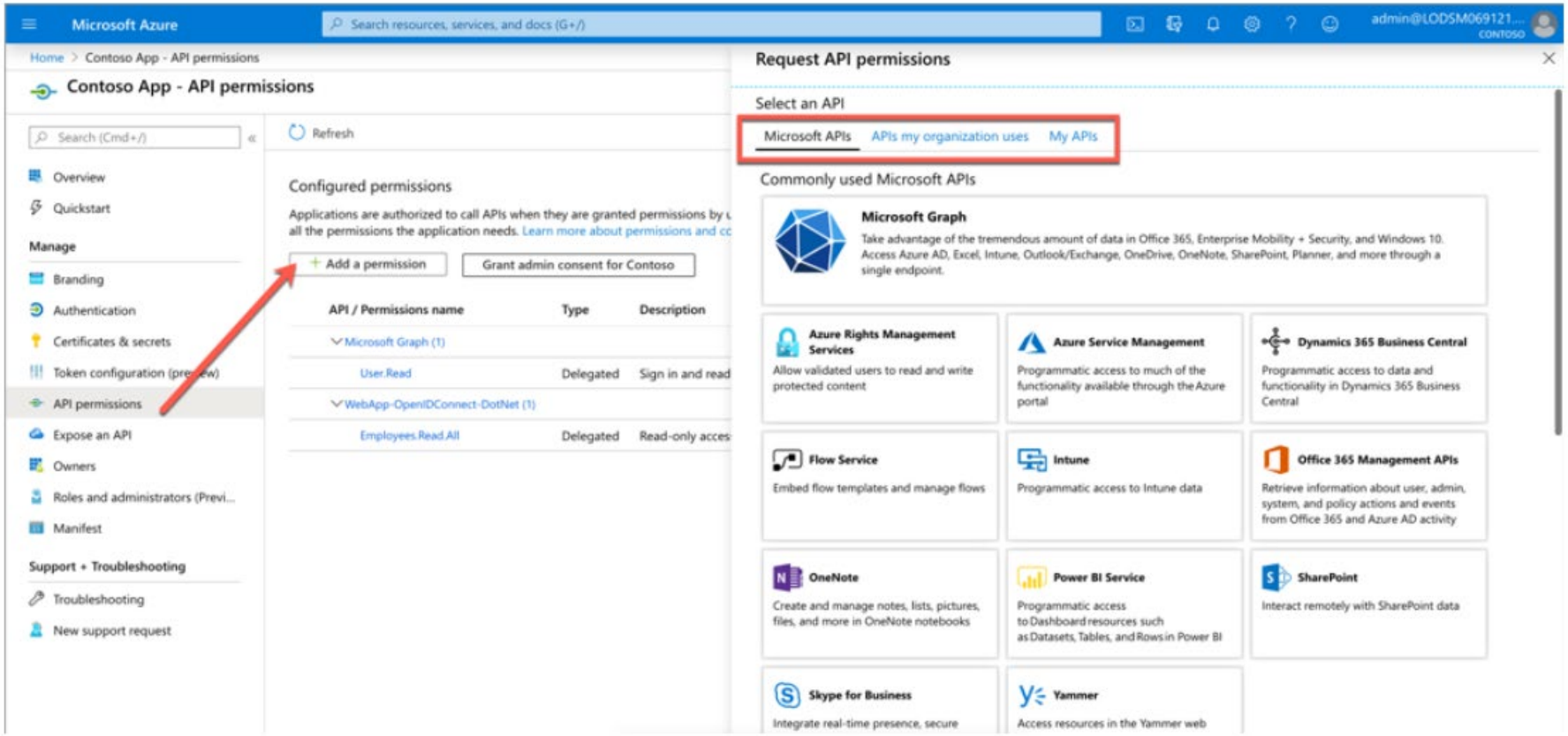
- 관리자 동의 흐름

애플리케이션 개발자가 전체 테넌트에 대해 동의를 기록하려는 의도로 사용자를 관리자 동의 끝점으로 안내하는 경우. 관리자 동의 흐름이 제대로 작동하는지 확인하려면 애플리케이션 개발자는 애플리케이션 매니페스트의 RequiredResourceAccess 속성에 모든 권한을 나열해야 합니다.



웹 API에 액세스할 수 있는 권한 추가

- Microsoft API
- 조직에서 사용하는 API
- 내 API



Microsoft ID로 사용자 지정 API 보호

다른 애플리케이션에서 호출될 수 있는 Microsoft ID로 웹 API를 보호하는 과정에는 다음 두 가지 주요 작업이 포함됩니다.

- Azure AD 애플리케이션 등록 및 구성
  - 범위 정의
- Microsoft ID를 지원하도록 구성된 웹 API 프로젝트 코드 작성
  - 현재 요청에 필요한 범위가 있는지 검사하기 위한 지원 추가

Microsoft Graph API 호출

Microsoft Graph API는 REST API 끝점을 통해 Azure AD에 프로그래밍 방식으로 액세스할 수 있습니다. 애플리케이션에서 Microsoft Graph API를 사용하여 디렉터리 데이터 및 개체에 대한 CRUD(만들기, 읽기, 업데이트 및 삭제) 작업을 수행할 수 있습니다.

- 제공되는 기능은 다음과 같습니다.
  - REST API 끝점
  - Azure AD로 인증
  - RBAC(역할 기반 권한 부여)
  - 차등 쿼리
  - 디렉터리 확장
  - 권한 범위로 보호
- 다음과 같은 애플리케이션 시나리오를 사용합니다.
  - 업무용(단일 테넌트) 애플리케이션
  - SaaS(Software as a Service)(다중 테넌트) 애플리케이션

데모

API 사용 권한 구현