Microsoft

tech·days Korea 2014
개발자 컨퍼런스

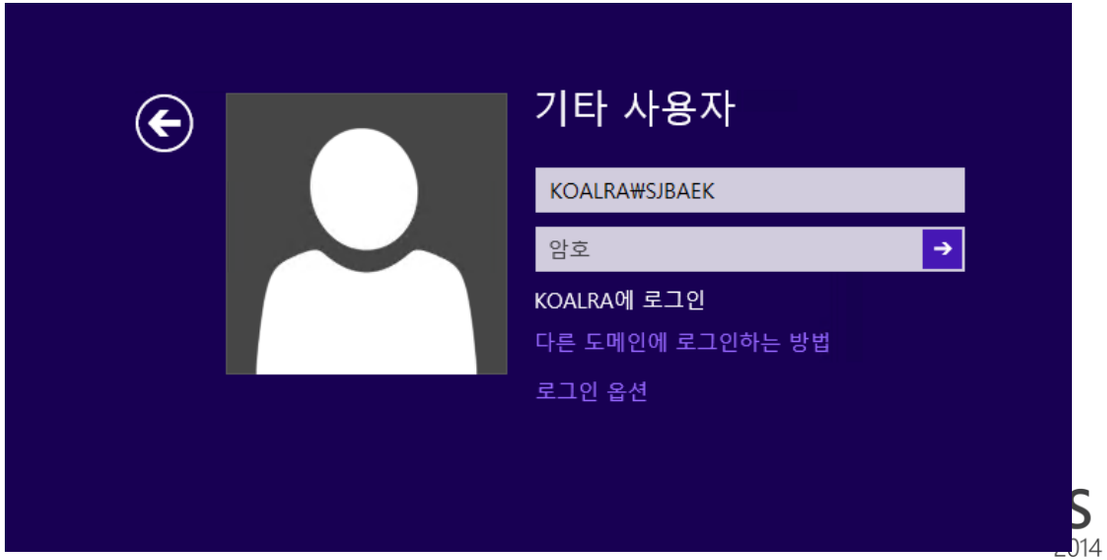
SSO를 위한 IDentity 일원화를 꿈꾸며 :
부제 : Azure Active Directory와 서비스(앱)인증

백 승 주
Sr. Technical Evangelist for IT Pro
Microsoft Korea

www.koalra.com
www.facebook.com/koalra

IDENTITY

넌 누구니? ^_^;;



AUTHENTICATION

인증

AUTHORIZATION

허가


Microsoft Azure
가입
koalra@outlook.com
2
CDN
0
사용화
0
스케줄러
0
API 관리
0
active directory
디렉터리
ACCESS CONTROL 네임스페이스
다단계 인증 공급자
권한 관리
이름
상태
역할
가입
데이터 센터 지역
국가 또는...
KOALRA
활성
전역 관리자
모든 KOALRA 가입에서 공유
아시아, 유럽, 미국
한국
KoalraKorea
활성
전역 관리자
모든 KoalraKorea 가입에서 공유
아시아, 유럽, 미국
한국
KOALRA CLOUD
활성
전역 관리자
모든 KOALRA CLOUD 가입에서 공유
아시아, 유럽, 미국
한국

Azure Active Directory (AAD)

클라우드 기반의 ID 및 액세스 관리

표준 프로토콜 및 서비스 지원 – 잠시 후에 ☺

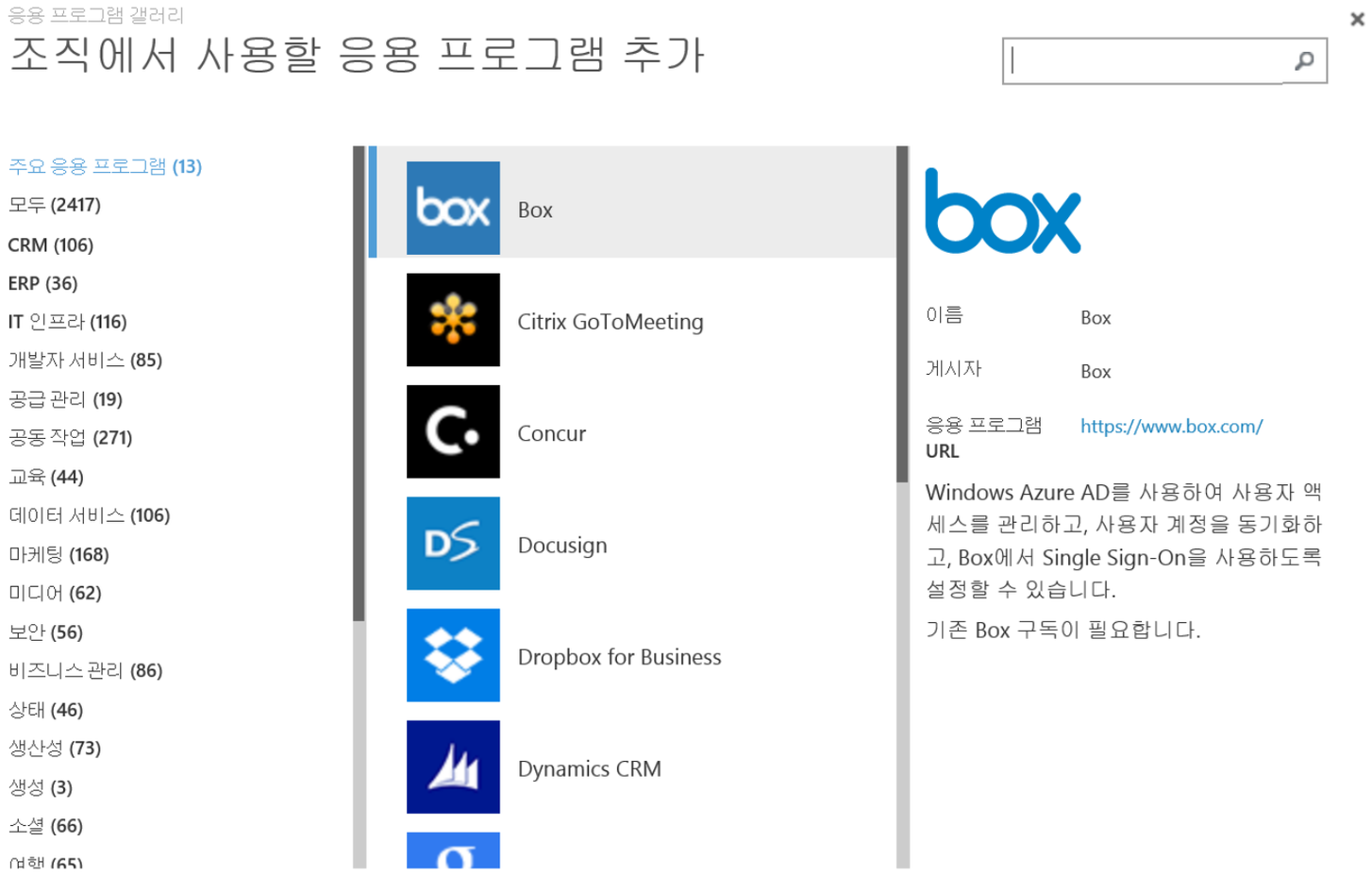
- WS-Federation, WS-Trust, WS-MetadataExchange
- SAML-P
- OpenID Connect
- Oauth 2.0
- STS(Security Token Service) 기반의 페더레이션 서비스
  - Office 365, Windows Intune, Microsoft Azure, Dynamic CRM

도메인 가입 안됨

- Windows Server의 Active Directory가 아닙니다.

미리 구성된 응용 프로그램 (Cloud App Discovery)

2400+



DEMO

1. Azure Active Directory의 기본 구성 및 사용자 생성
2. 미리 구성된 응용 프로그램

Microsoft

tech·days Korea 2014
개발자 컨퍼런스

Azure AD를 활용하는 서비스/앱 개발

최 한 홍
Technical Evangelist for Developer
Microsoft Korea

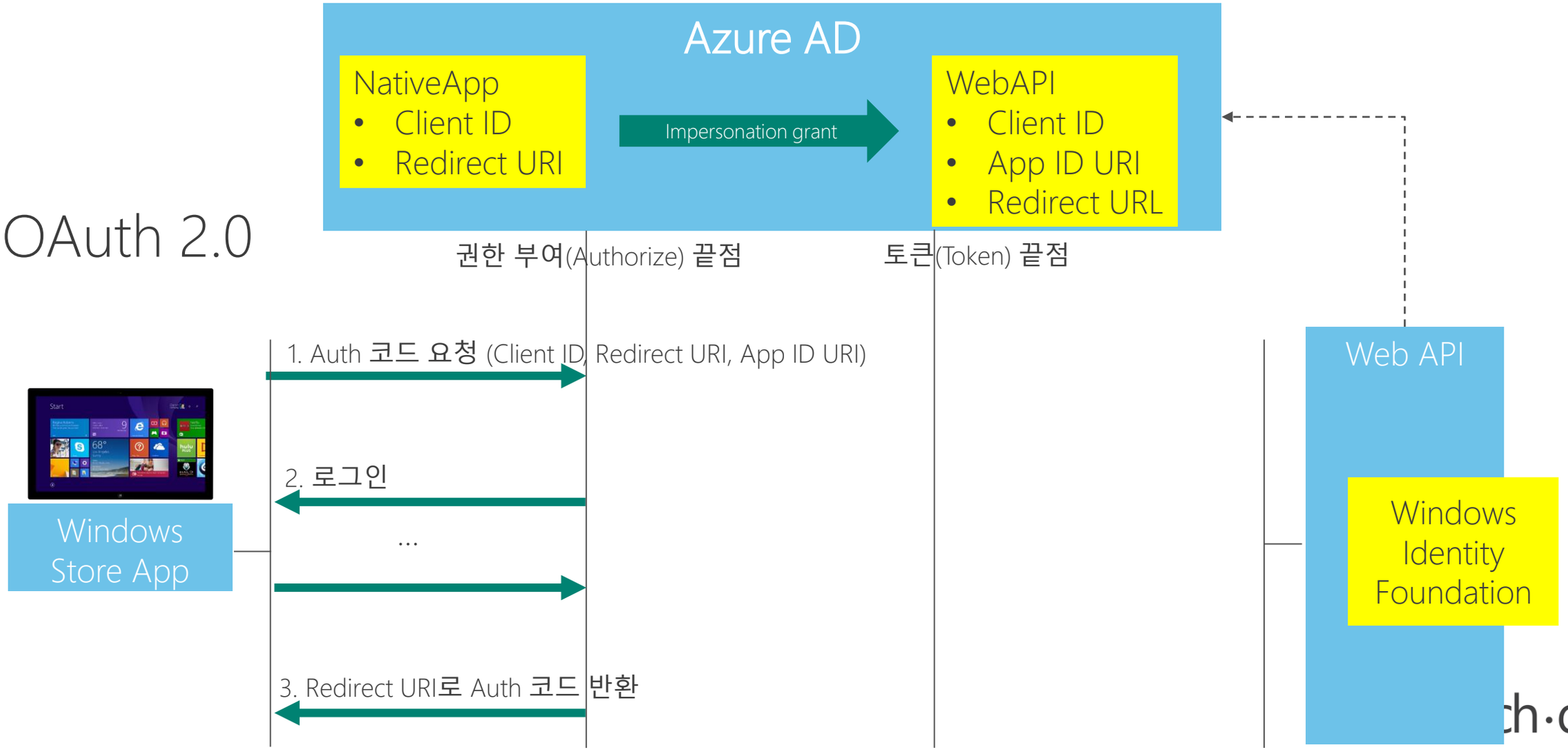
http://www.facebook.com/james.choi.3760

DEMO

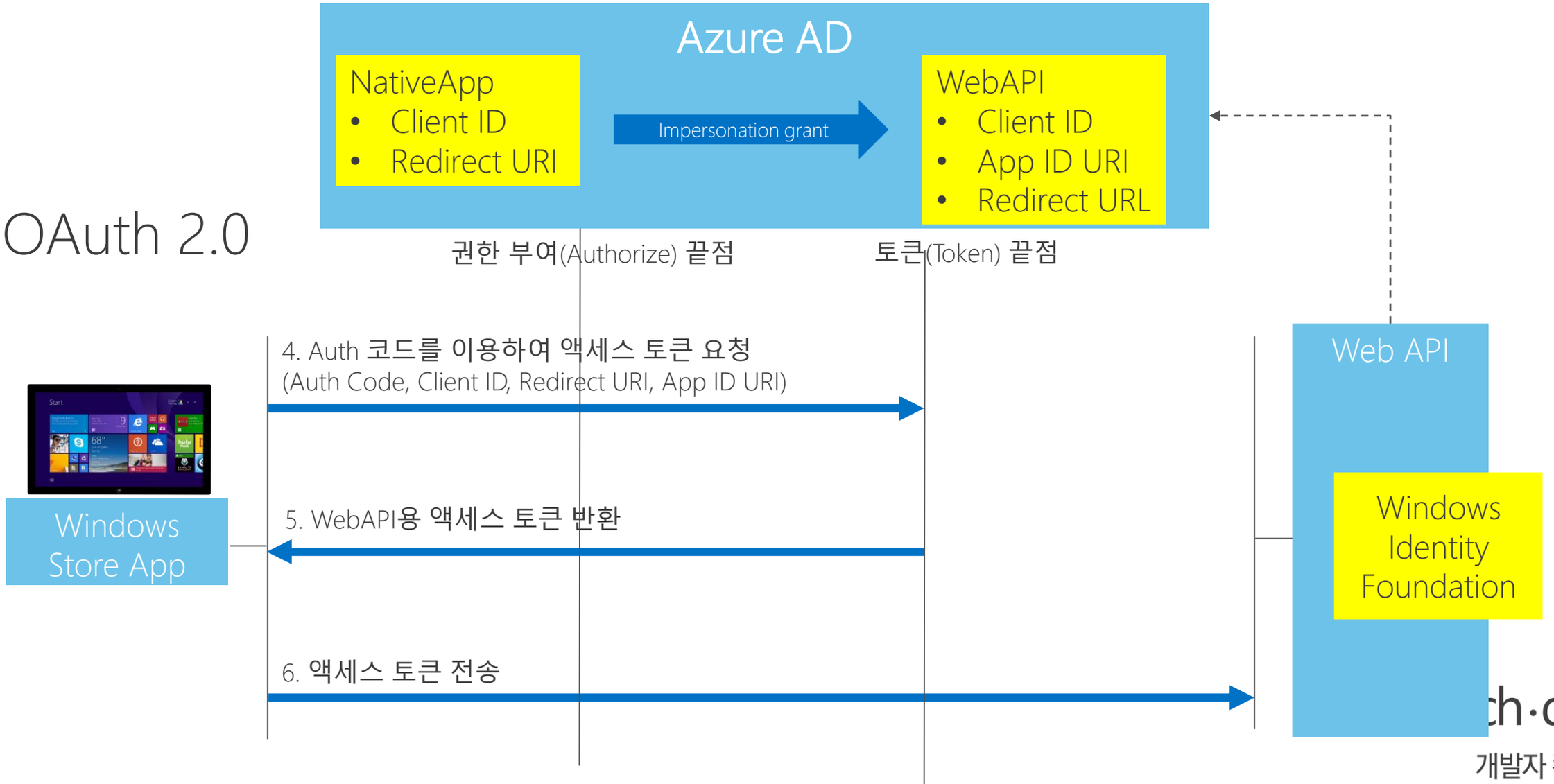
ASP.NET 응용 프로그램에서의 Azure AD를 통한 사용자 인증

인증 : 브라우저에서 ASP.NET 응용 프로그램

인증 : Windows Store App



인증 : Windows Store App (계속)



DEMO

Windows Store App 에서의 Azure AD를 통한 사용자 인증

참고 자료

- Azure AD Authentication Libraries 사용 개요 : http://msdn.microsoft.com/en-us/library/azure/dn499820.aspx

- Azure AD 인증 Sample Code : https://github.com/AzureADSamples

- Windows Identity Foundation : http://msdn.microsoft.com/en-us/library/ee748475.aspx

- Store App 인증 시나리오 참조 블로그 : http://www.nimbo.com/blog/use-azure-active-directory-adal-windows-store-app/

왜!!

Windows Server에도 Active Directory가 있는데... Azure AD가 ...

Windows Server Active Directory (WSAD)

SSO(Single Sign On)

- Kerberos, NTLM

데이터베이스

- LDAP

클라이언트/서버의 중앙 관리

- 그룹 정책

트렌드 변화에 따른 WSAD 확장 필요

DMZ 네트워크에 배치된 LOB 서버의 SSO 처리

- 보안 책임 소재

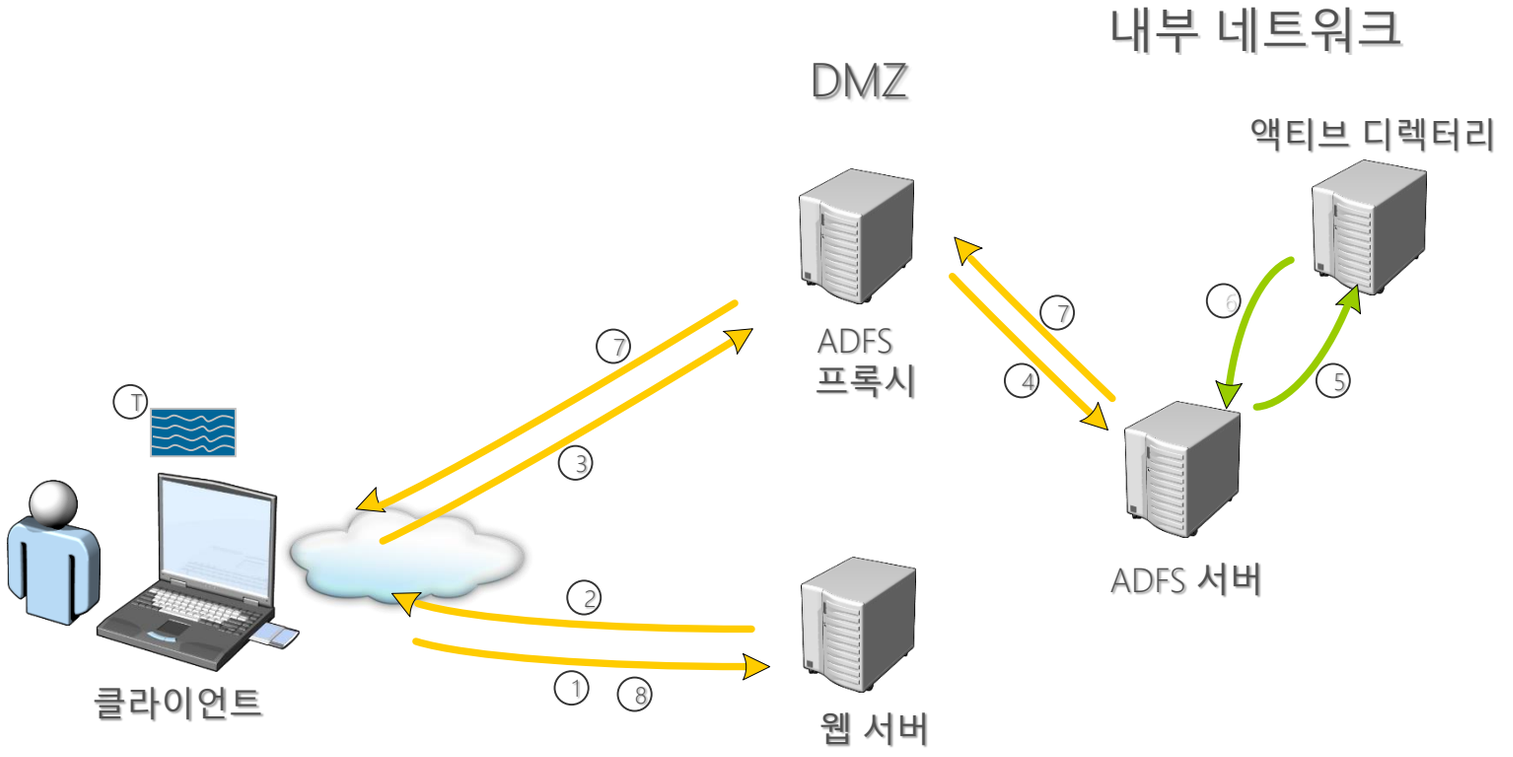
Windows 기반의 PC가 아닌 디바이스에서의 SSO 처리

- 도메인 가입 기술 제공 유무
- 프로토콜 제한

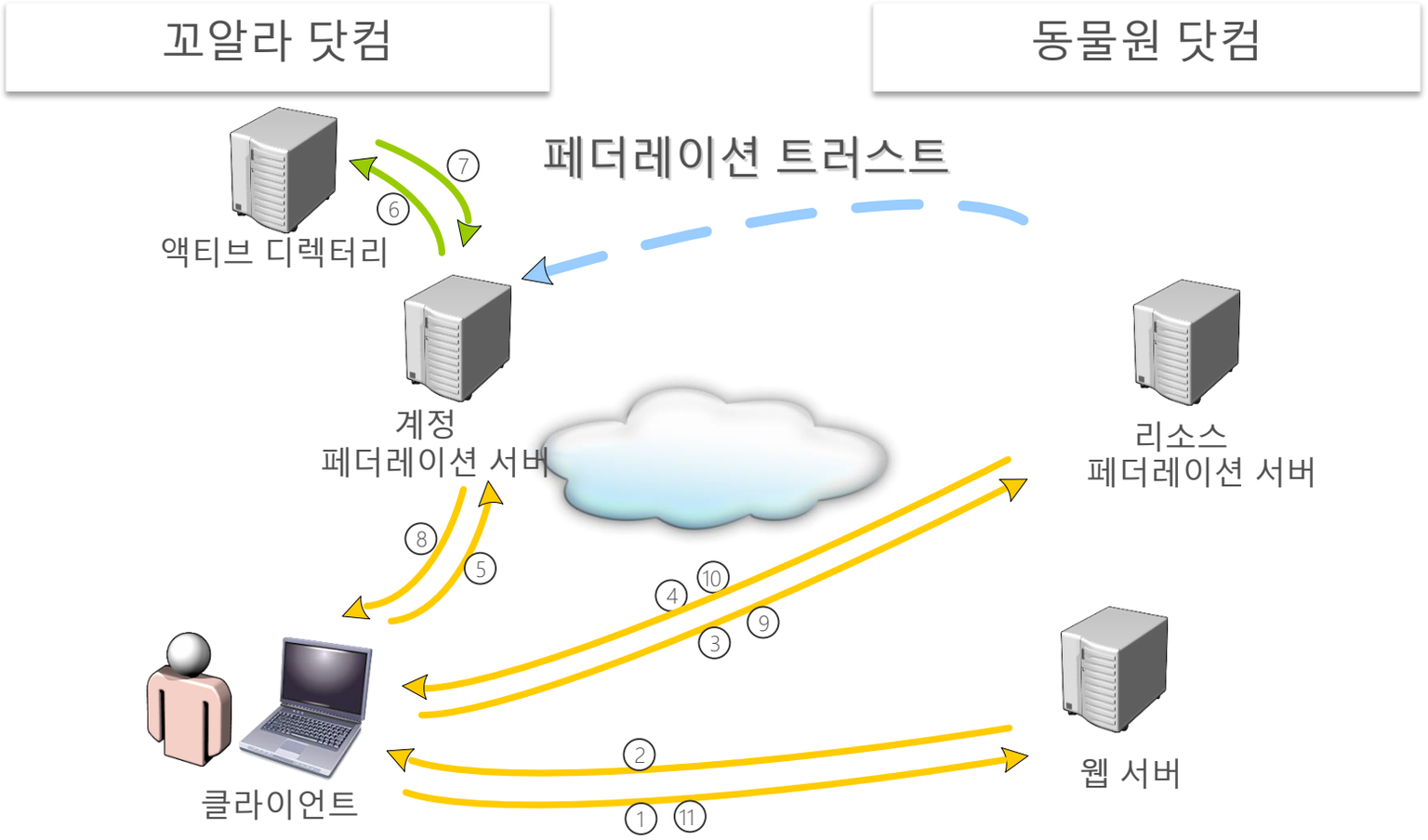
다른 조직의 사용자에게 사내 리소스 접근 권한 허가

- 계정에 대한 제공 위치 및 관리 이슈

Windows Server Active Directory Federation Services (ADFS) #1



Windows Server Active Directory Federation Services (ADFS) #2



ADFS의 표준 지원

ADFS 1.x

- WS-Federation Passive Requestor Profile (PRP, browser)
- SAML 1.0 Tokens

ADFS 2.0, AD FS @ Windows Server 2012

- WS-Federation PRP
- WS-Trust (active applications)
- SAML 1.1 Token
- SAML 2.0 Token (only with SAML Relying Party)
- SAML 2.0 Operational Modes

ADFS @ Windows Server 2012 R2

- 기존 Active Directory Federation Services 2.x의 지원
- OAuth Authorization Code Flow Profile
- JSON (JavaScript Object Notation) Web Token (JWT)

DEMO

Active Directory Federation Services
빠르게 살펴보기

ㅜㅜ

우리는 WSAD가 있는데...
AAD까지?!

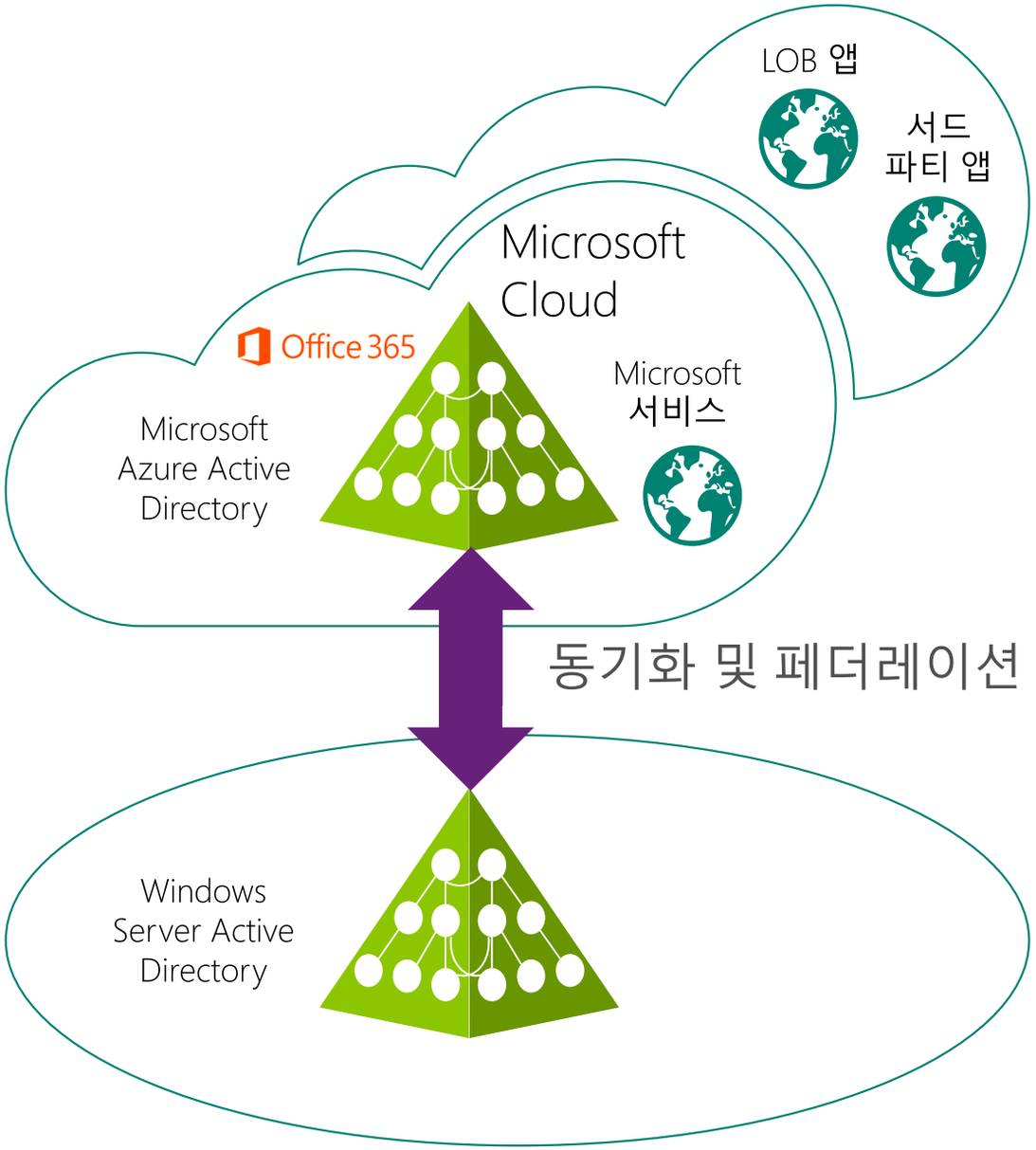
AAD와 WSAD의 관계

WSAD와 AAD 통합 가능

디렉터리 정보에 대한 동기화를 통해, AAD 인증 또는 ADFS 인증을 사용하는 서비스에서 활용

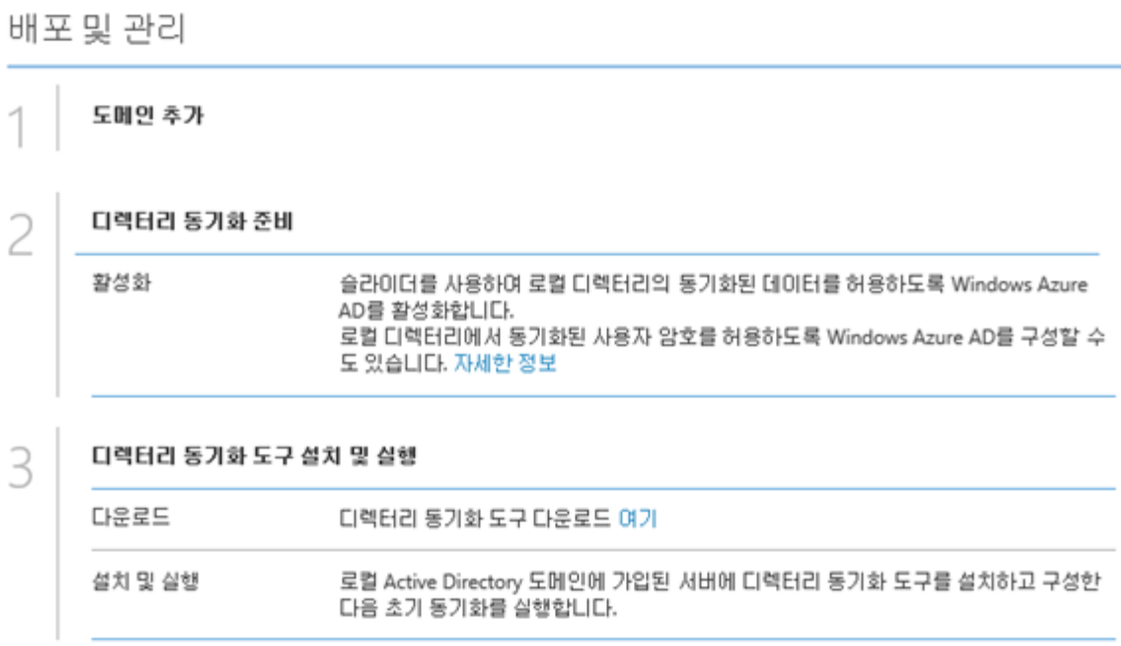
인증 영역 위치에 대한 결정 필요

- WS의 ADFS 인증
- AAD 인증



디렉터리 동기화 (DirSync)

Microsoft Azure AD 디렉터리 통합 페이지에서 동기화 설정



페이지내 링크를 통해 다운로드

AAD PowerShell

디렉터리 연동 옵션

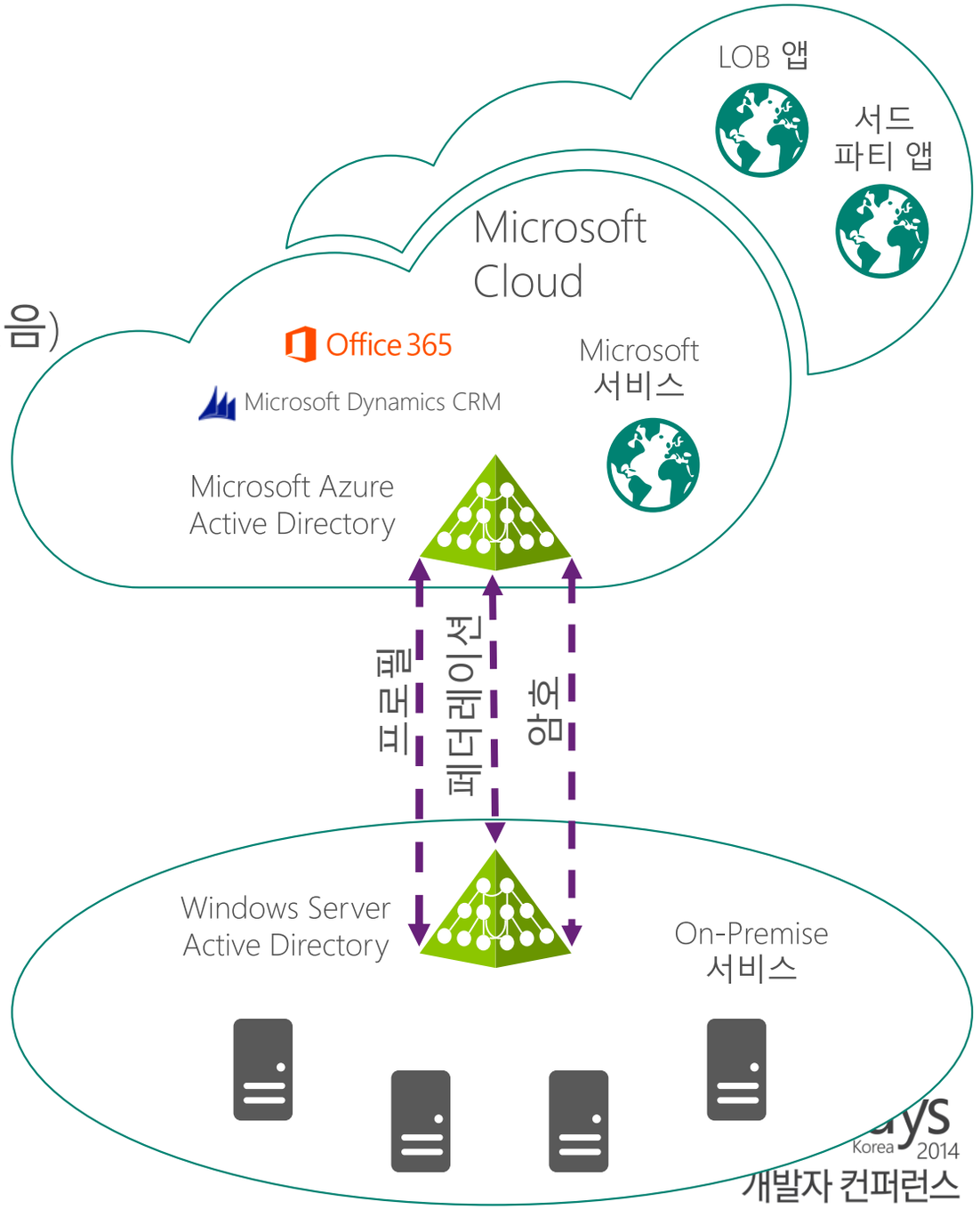
개별 사용

프로필 데이터만 (아직 미지원, 암호 동기화 없음)

프로필 및 ID 데이터만 (암호 동기화 없음)

프로필 및 ID 데이터, 그리고 ADFS 인증 연계 (SSO) (암호 동기화 없음)

프로필 및 ID 데이터, 그리고 AAD 인증 연계 (SSO) (암호 동기화)



DEMO

디렉터리 동기화 및 인증 위치 결정

AAD 인증 및 ADFS 인증 상호 변경

AAD 인증

- Standard Domain

ADFS 인증

- Federated Domain

```
PS C:\> Get-MsolDomain

Name                                    Status          Authentication
----                                    ------          --------------
cloud.koalra.com                        Verified        Federated
korea.koalra.com                        Verified        Managed
KOALRAAZURE.mail.onmicrosoft.com        Verified        Managed
KOALRAAZURE.onmicrosoft.com             Verified        Managed
```

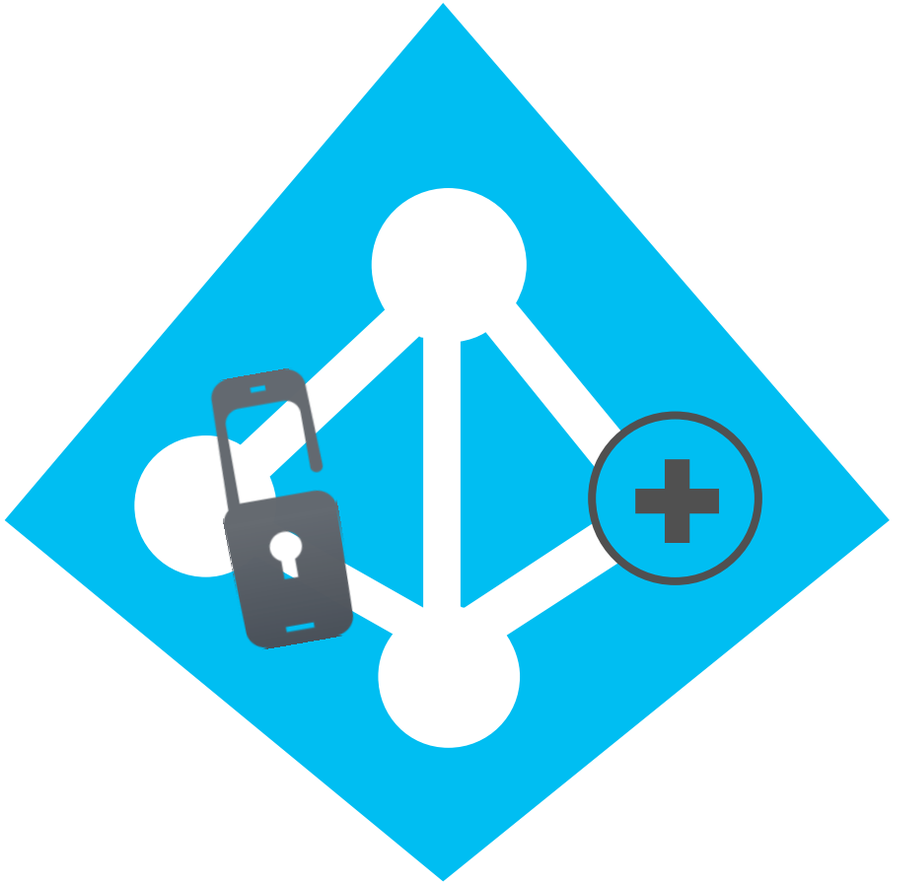
Convert-MsolDomainToStandard

- 암호 동기화 필요
  - Enable-MSOnlinePasswordSync
  - Set-FullPasswordSync
  - FIMSynchronizationService 서비스 재시작

Convert-MsolDomainToFederated

AAD에도 프리미엄 버전이!

Azure Active Directory Premium (AADP)



99.9%, 엔터프라이즈급 SLA

조직에서 필요한 추가 기술 제공

- 로그인 페이지 커스터마이징
- 셀프 서비스 사용자 암호 재설정 및 WSAD로 동기화
- 셀프 서비스 그룹 관리
- 다단계 인증(MFA) 등

Forefront Identity Manager 서버 및 CAL 제공

Microsoft EA 라이선스 프로그램에 포함, 90일 평가판

AAD vs. AADP

	Azure AD	Azure AD **프리미엄**
디렉터리 서비스	✓최대 50만개 개체까지	✓ 제한 없음
사용자 및 그룹 관리	✓	✓
미리 구성된 SAAS 응용 프로그램 및 조직 서비스에 대한 SSO	✓사용자당 최대 10개까지	✓ 제한 없음
디렉터리 동기화 도구	✓	✓
사용자 기반 접근 관리	✓	✓
그룹 기반 접근 관리		✓
셀프 서비스 그룹 관리		✓
셀프 서비스 암호 변경	✓	✓
셀프 서비스 암호 재설정 및 WSAD 동기화		✓
보안 보고서	✓	✓
Machine Learning 기반 고급 보안 보고서		✓
사용량 보고서		✓
조직 브랜딩 (로그온 페이지 및 접근 패널 커스터마이징		✓
MFA (Microsoft Azure/Windows Server)		✓
SLA		✓
FIM CAL + FIM Server		✓

사용자 암호 재설정

사무실 전화

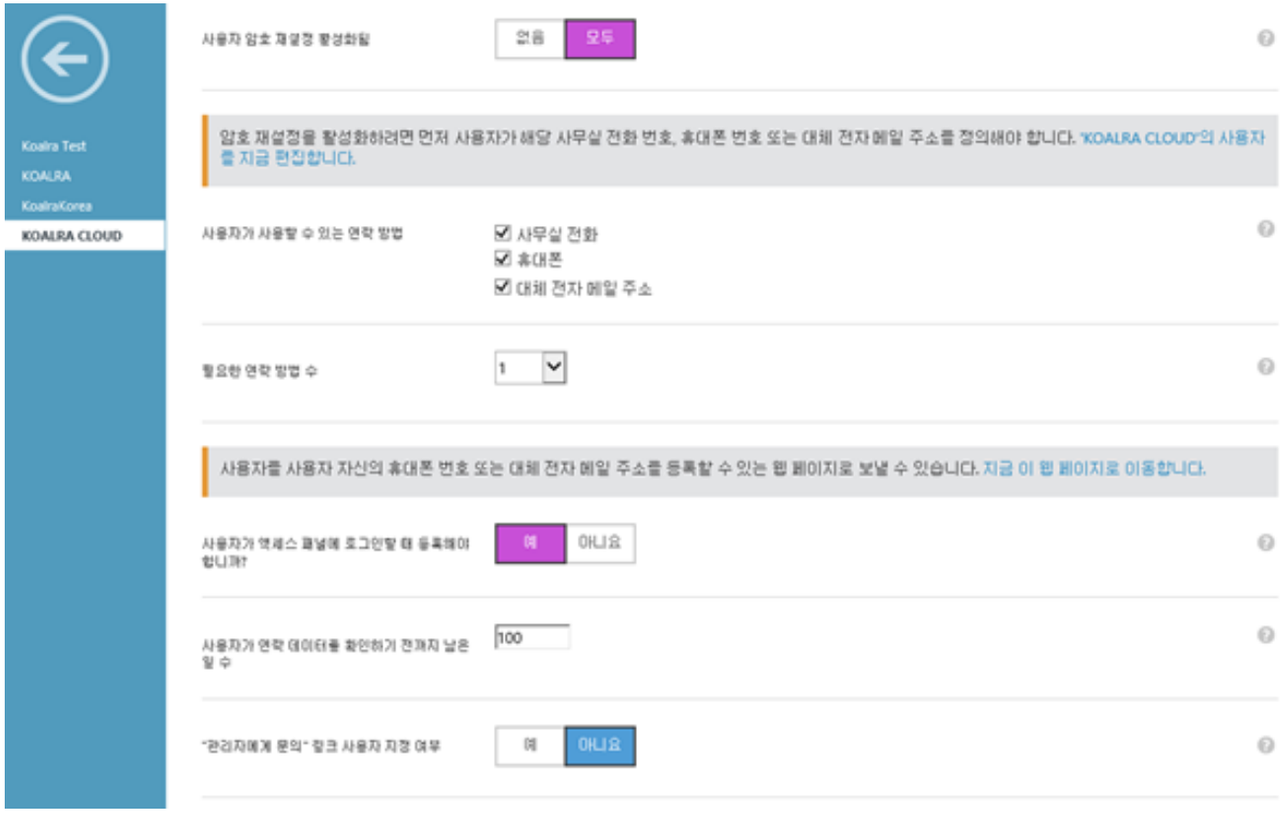
- 전화로 확인(대한민국 지원 안함)

휴대폰

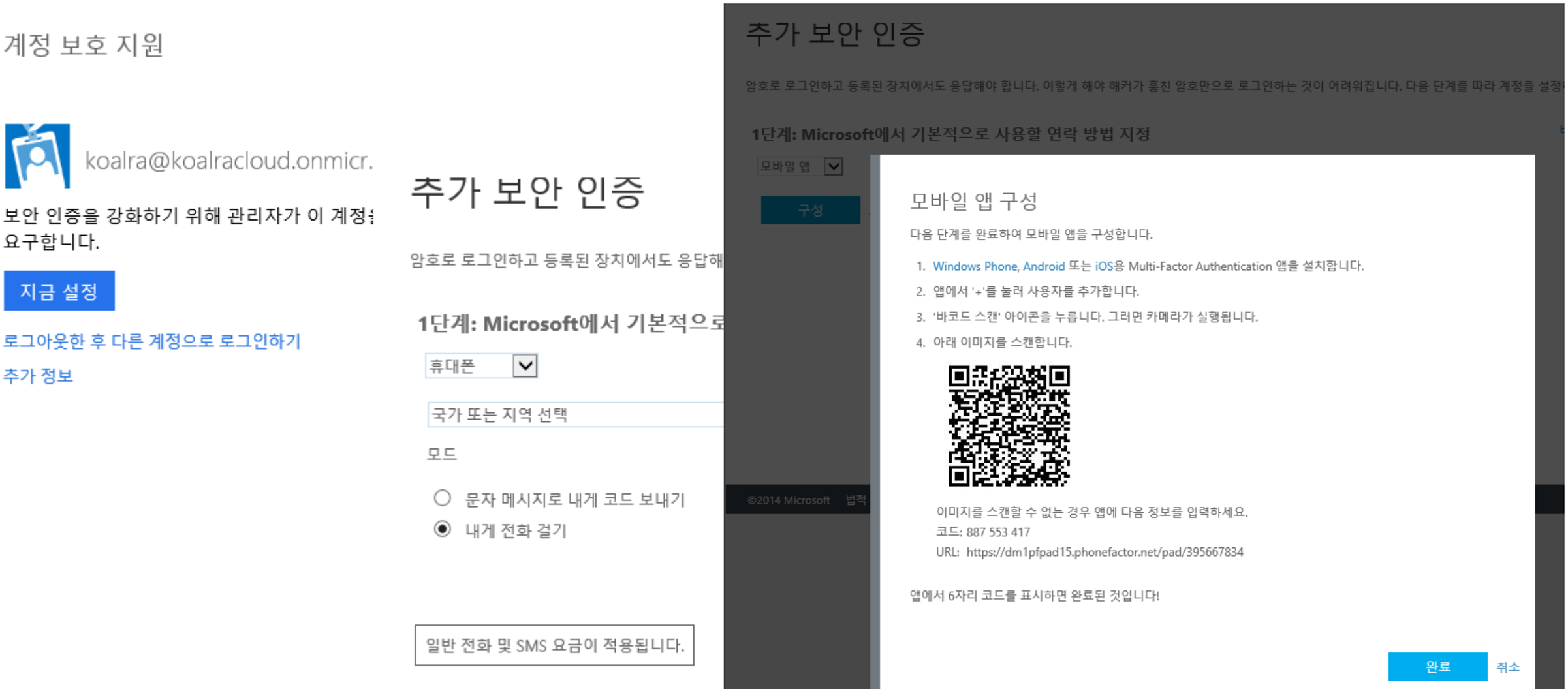
- 코드 확인

대체 전자 메일 주소

- 코드 확인



다단계 인증
(Multi-Factor Authentication, MFA)

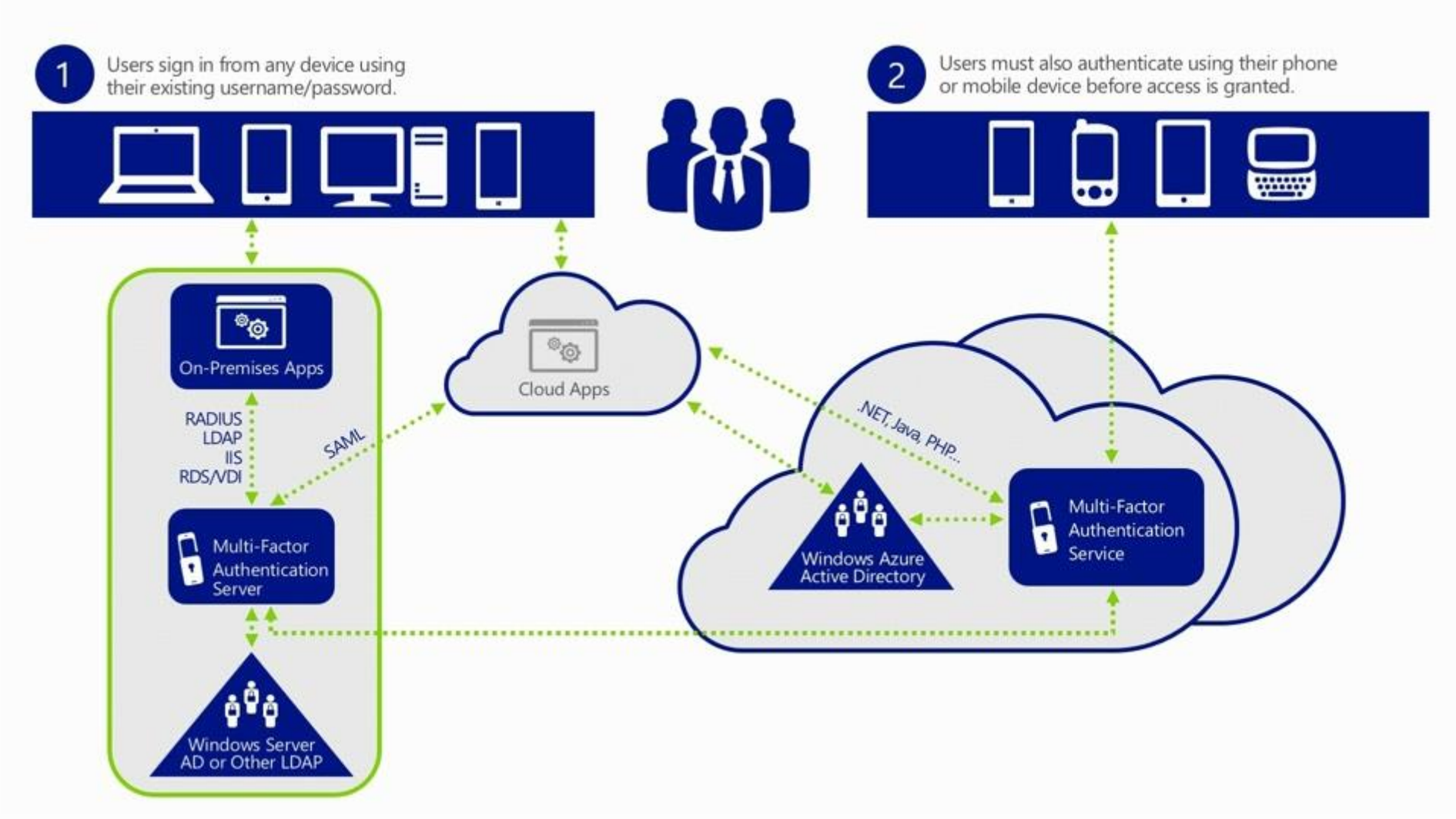


DEMO

Azure Active Directory Premium

1. 사용자 암호 재설정 구성
2. 다단계 인증

온 프레미스와 Azure MFA 연동



Azure Active Directory (AAD)

1. WSAD와 비슷하지만, 동작 및 활용은 완전히 다름
2. 기존 WSAD가 있을 경우에 대한 구성 시나리오 고려
3. AADP 기술 시나리오 고려
4. 다양한 디바이스에 대한 SSO 및 클라우드 시대에 적절한 인증 기술