

# SSO를 위한 IDentity 일원화를 꿈꾸며 :

부제 : Azure Active Directory와 서비스(앱)인증

백 승 주

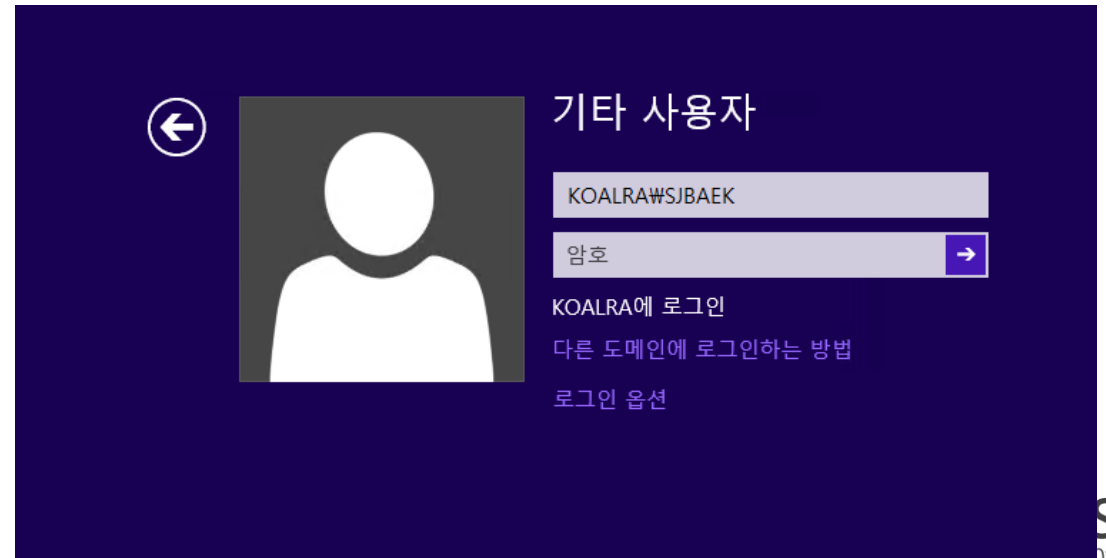
Sr. Technical Evangelist for IT Pro  
Microsoft Korea

[www.koalra.com](http://www.koalra.com)

[www.facebook.com/koalra](http://www.facebook.com/koalra)

# IDENTITY

넌 누구니? ^-^;;







# AUTHENTICATION

인증

# AUTHORIZATION

허가

-  2
-  CDN 0
-  자동화 0
-  스케일링 0
-  API 관리 0
-  MACHINE LEARNING

## active directory

디렉터리 ACCESS CONTROL 네임스페이스 다단계 인증 공급자 권한 관리

이름	상태	역할	가입	데이터 센터 지역	국가 또는...
<b>KOALRA</b> →	✓ <b>활성</b>	전역 관리자	모든 KOALRA 가입에서 공유	아시아, 유럽, 미국	한국
KoalraKorea	✓ <b>활성</b>	전역 관리자	모든 KoalraKorea 가입에서 공유	아시아, 유럽, 미국	한국
KOALRA CLOUD	✓ <b>활성</b>	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)

응용 프로그램 갤러리

조직에서 사용할 응용 프로그램 추가

2400+

주요 응용 프로그램 (13)

모두 (2417)

CRM (106)

ERP (36)

IT 인프라 (116)

개발자 서비스 (85)

공급 관리 (19)

공동 작업 (271)

교육 (44)

데이터 서비스 (106)

마케팅 (168)

미디어 (62)

보안 (56)

비즈니스 관리 (86)

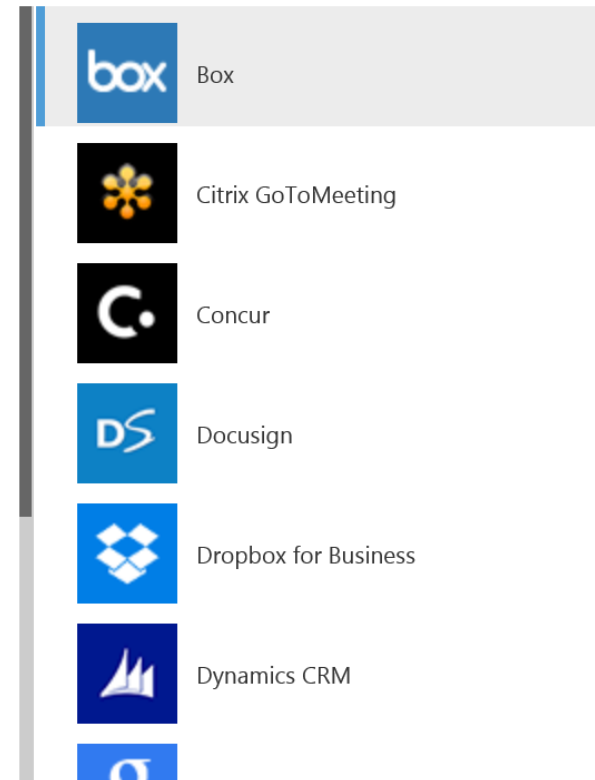
상태 (46)

생산성 (73)

생성 (3)

소셜 (66)

여행 (65)



이름 Box

게시자 Box

응용 프로그램 URL <https://www.box.com/>

Windows Azure AD를 사용하여 사용자 액세스를 관리하고, 사용자 계정을 동기화하고, Box에서 Single Sign-On을 사용하도록 설정할 수 있습니다.

기존 Box 구독이 필요합니다.



# DEMO

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



# Azure AD를 활용하는 서비스/앱 개발

최한홍

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 프로 그램

앱 ID URI

웹 브라우저



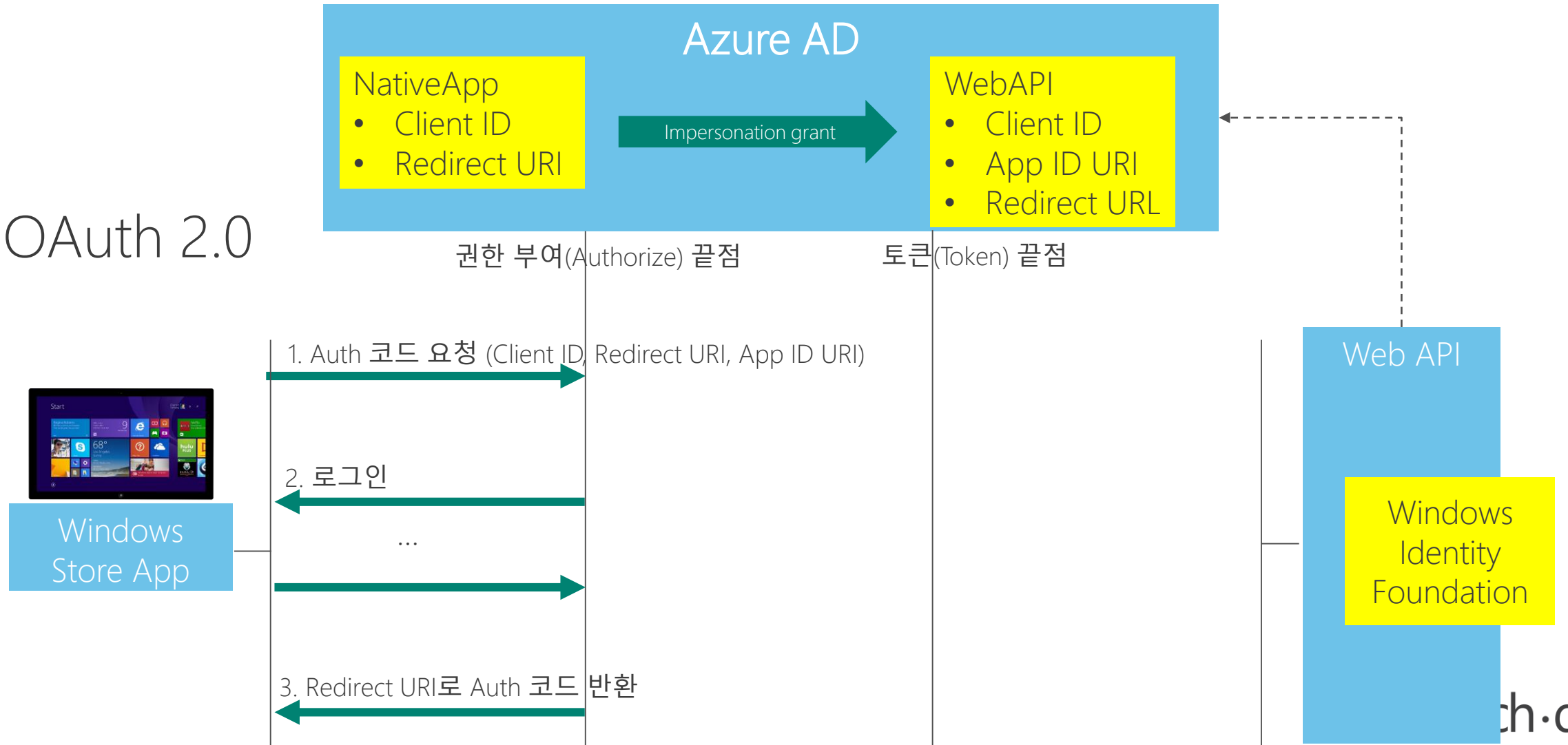
Azure AD

ASP.NET  
응용  
프로그램

Windows Identity  
Foundation

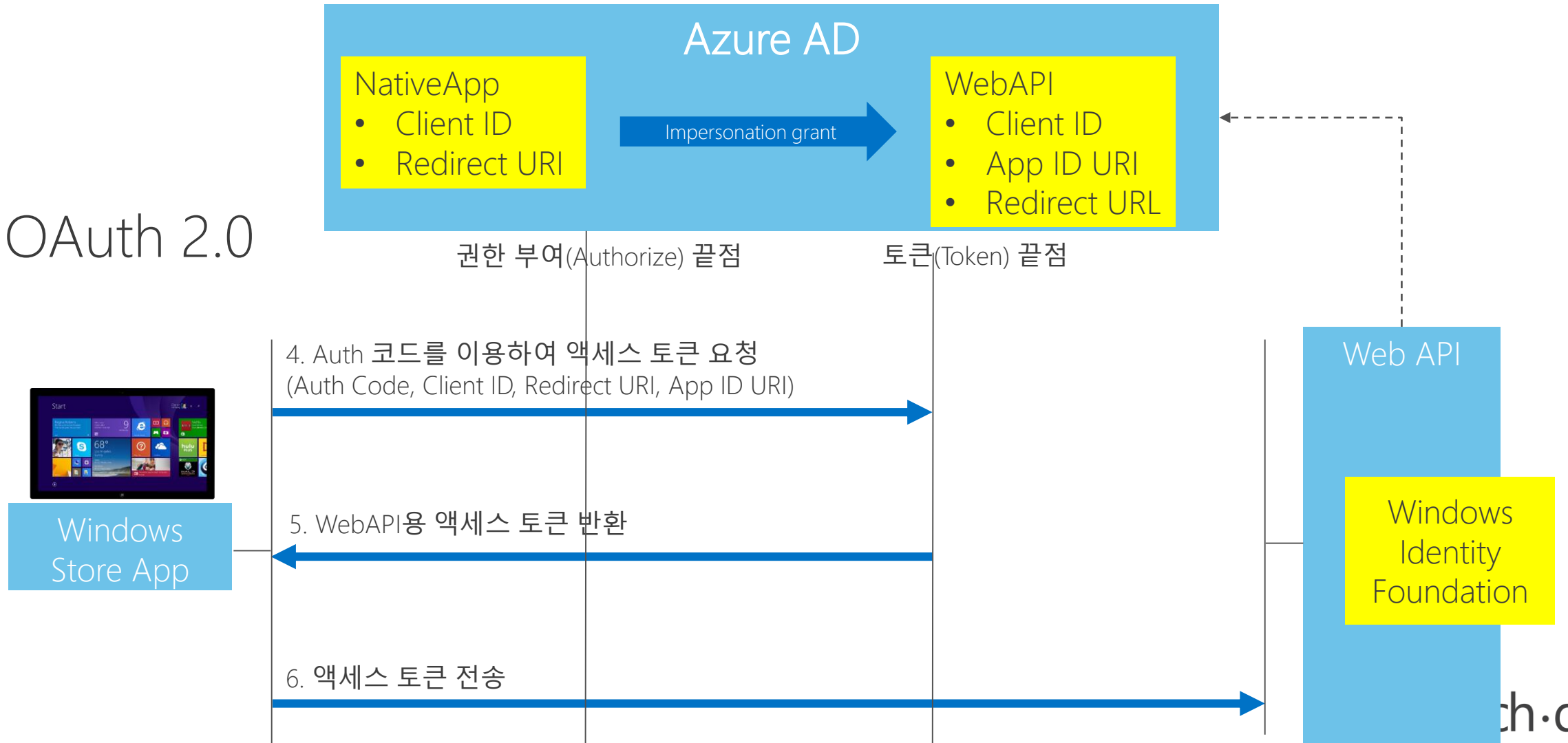
# 인증 : Windows Store App

OAuth 2.0



# 인증 : Windows Store App (계속)

OAuth 2.0



# 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

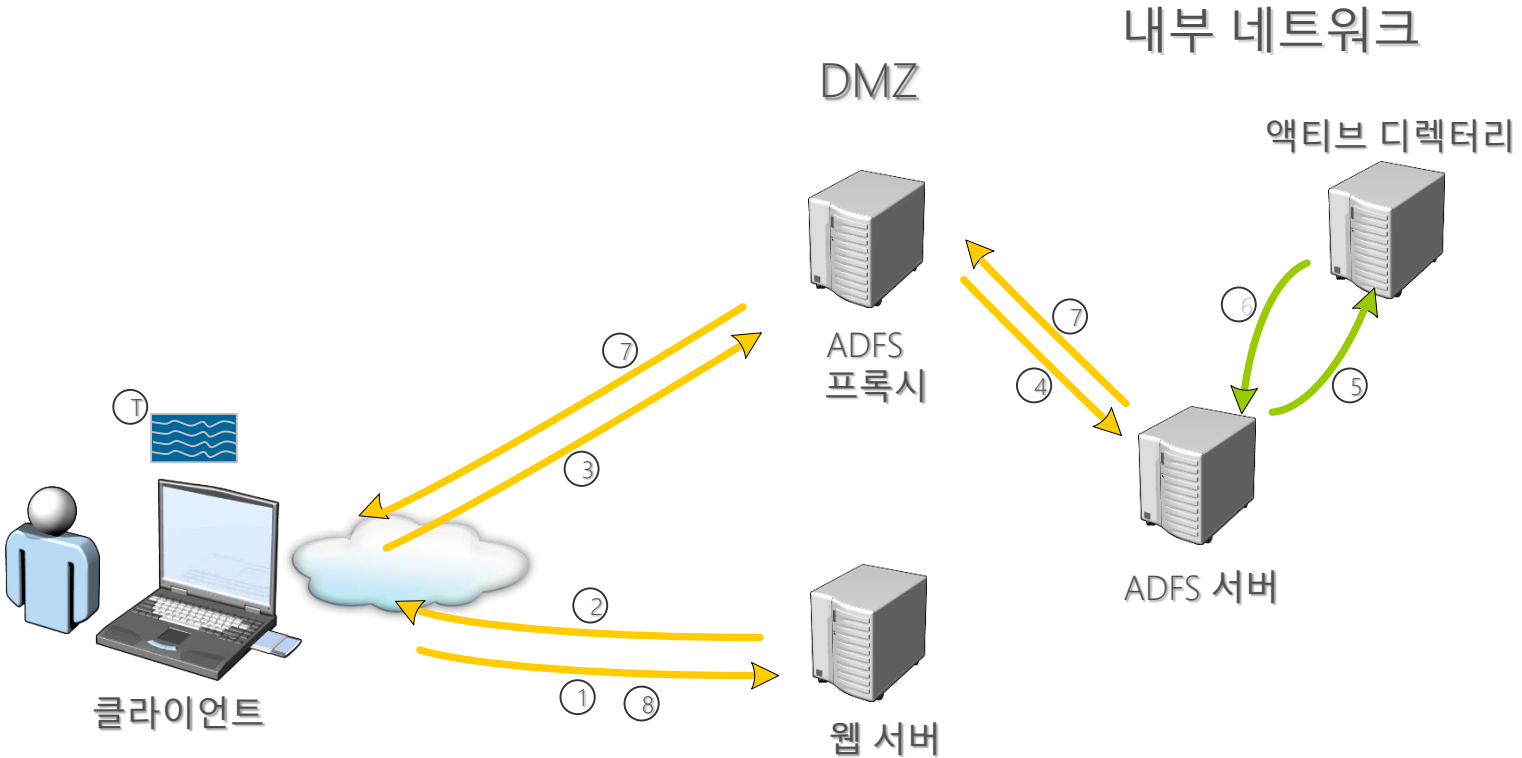
## Windows 기반의 PC가 아닌 디바이스에서의 SSO 처리

- 도메인 가입 기술 제공 유무
- 프로토콜 제한

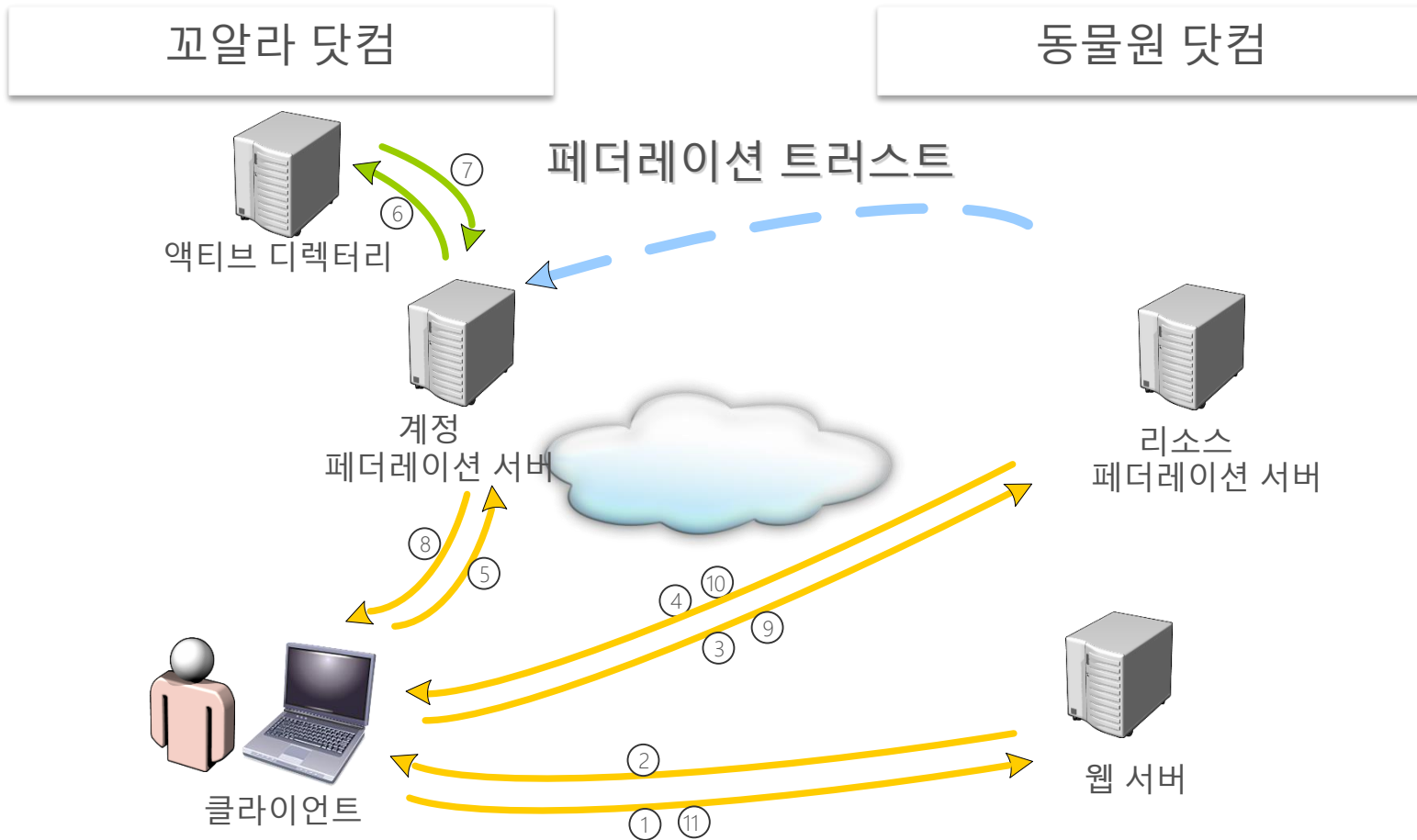
## 다른 조직의 사용자에게 사내 리소스 접근 권한 허가

- 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

TT

우리는 WSAD가 있는데...  
AAD까지?!

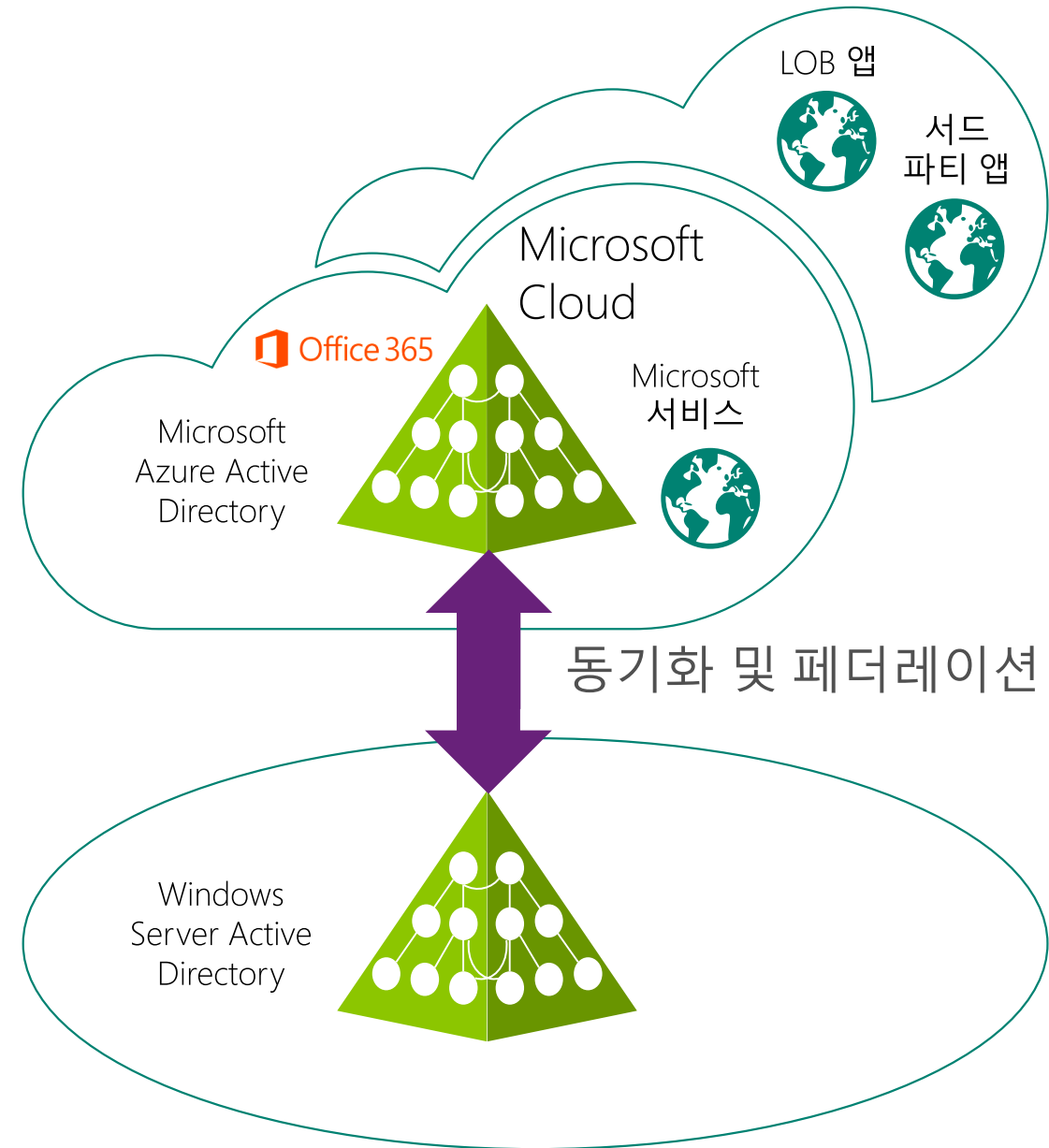
# AAD와 WSAD의 관계

## 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

koalra cloud

사용자 그룹 응용 프로그램 도메인 디렉터리 통합 구성 보고서 라이선스

### 로컬과 통합 active directory

디렉터리 동기화에 대해 확인된 도메인	1
SINGLE SIGN-ON용으로 계획된 도메인	0
디렉터리 동기화	<input checked="" type="checkbox"/> 활성화됨 <input type="checkbox"/> 비활성화됨
마지막 동기화	1시간 미만 이전

배포 및 관리

### 배포 및 관리

#### 1 | 도메인 추가

#### 2 | 디렉터리 동기화 준비

**활성화** 슬라이더를 사용하여 로컬 디렉터리의 동기화된 데이터를 허용하도록 Windows Azure AD를 활성화합니다. 로컬 디렉터리에서 동기화된 사용자 암호를 허용하도록 Windows Azure AD를 구성할 수도 있습니다. [자세한 정보](#)

#### 3 | 디렉터리 동기화 도구 설치 및 실행

**다운로드** 디렉터리 동기화 도구 다운로드 [여기](#)

**설치 및 실행** 로컬 Active Directory 도메인에 가입된 서버에 디렉터리 동기화 도구를 설치하고 구성한 다음 초기 동기화를 실행합니다.

페이지내 링크를 통해 다운로드  
AAD PowerShell

# 디렉터리 연동 옵션

개별 사용

프로필 데이터만 (아직 미지원, 암호 동기화 없음)

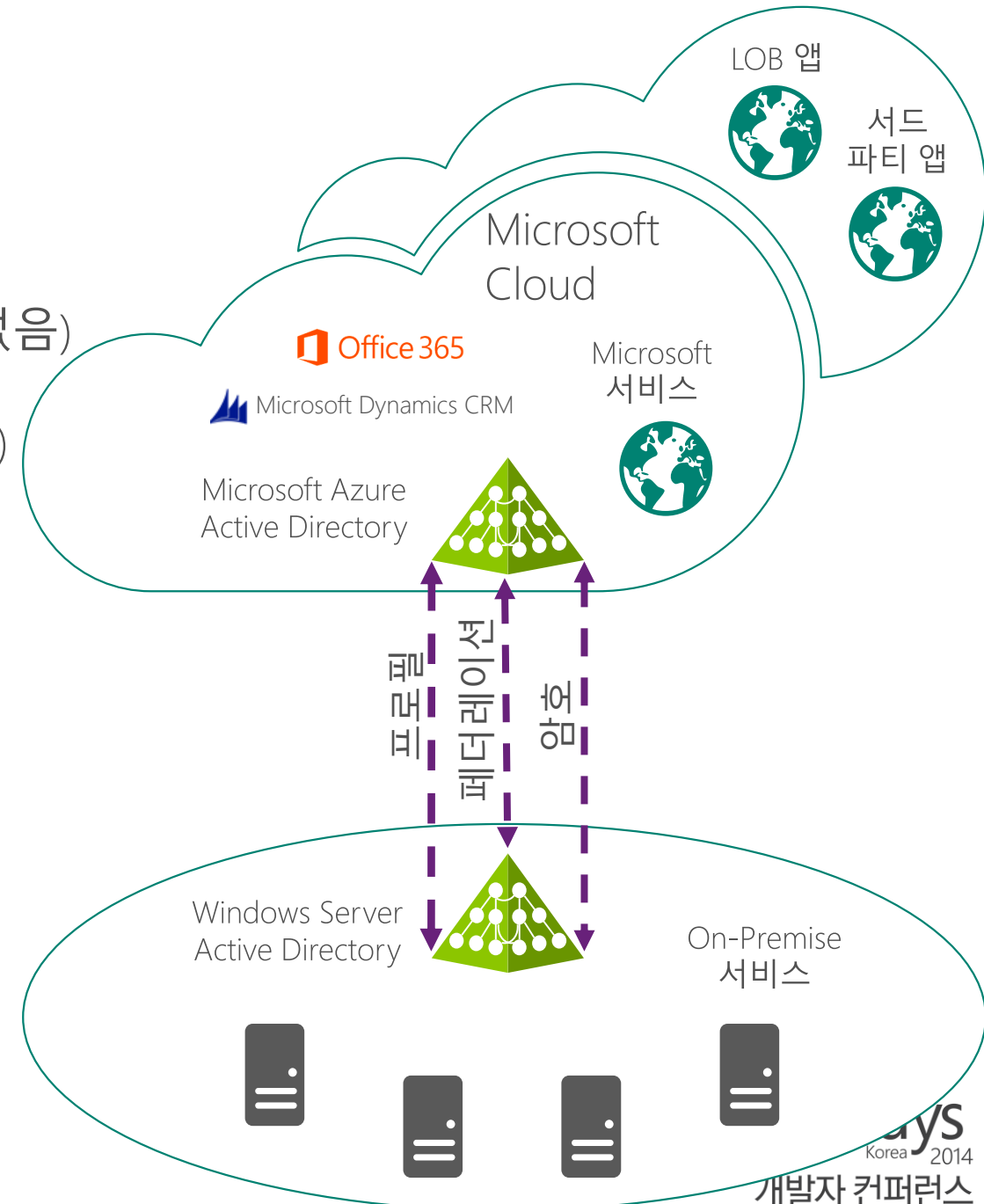
프로필 및 ID 데이터만 (암호 동기화 없음)

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 프로그램  
에 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

사용자 암호 재설정 활성화됨

암호 재설정을 활성화하려면 먼저 사용자가 해당 사무실 전화 번호, 휴대폰 번호 또는 대체 전자 메일 주소를 정의해야 합니다. 'KOALRA CLOUD'의 사용자들 지금 편집합니다.

사용자가 사용할 수 있는 연락 방법  사무실 전화  휴대폰  대체 전자 메일 주소

필요한 연락 방법 수

사용자를 사용자 자신의 휴대폰 번호 또는 대체 전자 메일 주소를 등록할 수 있는 웹 페이지로 보낼 수 있습니다. 지금 이 웹 페이지로 이동합니다.

사용자가 액세스 기록에 로그인할 때 등록해야 하나요?

사용자가 연락 데이터를 확인하기 전까지 남은 일 수

"관리자에게 문의" 링크 사용자 지정 여부



# 다단계 인증 (Multi-Factor Authentication, MFA)

계정 보호 지원



koalra@koalracloud.onmicr.

보안 인증을 강화하기 위해 관리자가 이 계정을  
요구합니다.

지금 설정

로그아웃한 후 다른 계정으로 로그인하기

추가 정보

## 추가 보안 인증

암호로 로그인하고 등록된 장치에서도 응답해

1단계: Microsoft에서 기본적으로

휴대폰

국가 또는 지역 선택

모드

- 문자 메시지로 내게 코드 보내기
- 내게 전화 걸기

일반 전화 및 SMS 요금이 적용됩니다.

## 추가 보안 인증

암호로 로그인하고 등록된 장치에서도 응답해야 합니다. 이렇게 해야 해커가 훔친 암호만으로 로그인하는 것이 어려워집니다. 다음 단계를 따라 계정을 설정

1단계: Microsoft에서 기본적으로 사용할 연락 방법 지정

모바일 앱

구성

### 모바일 앱 구성

다음 단계를 완료하여 모바일 앱을 구성합니다.

- Windows Phone, Android 또는 iOS용 Multi-Factor Authentication 앱을 설치합니다.
- 앱에서 '+'를 눌러 사용자를 추가합니다.
- '바코드 스캔' 아이콘을 누릅니다. 그러면 카메라가 실행됩니다.
- 아래 이미지를 스캔합니다.



이미지를 스캔할 수 없는 경우 앱에 다음 정보를 입력하세요.  
코드: 887 553 417  
URL: https://dm1pfpad15.phonefactor.net/pad/395667834

앱에서 6자리 코드를 표시하면 완료된 것입니다!

완료

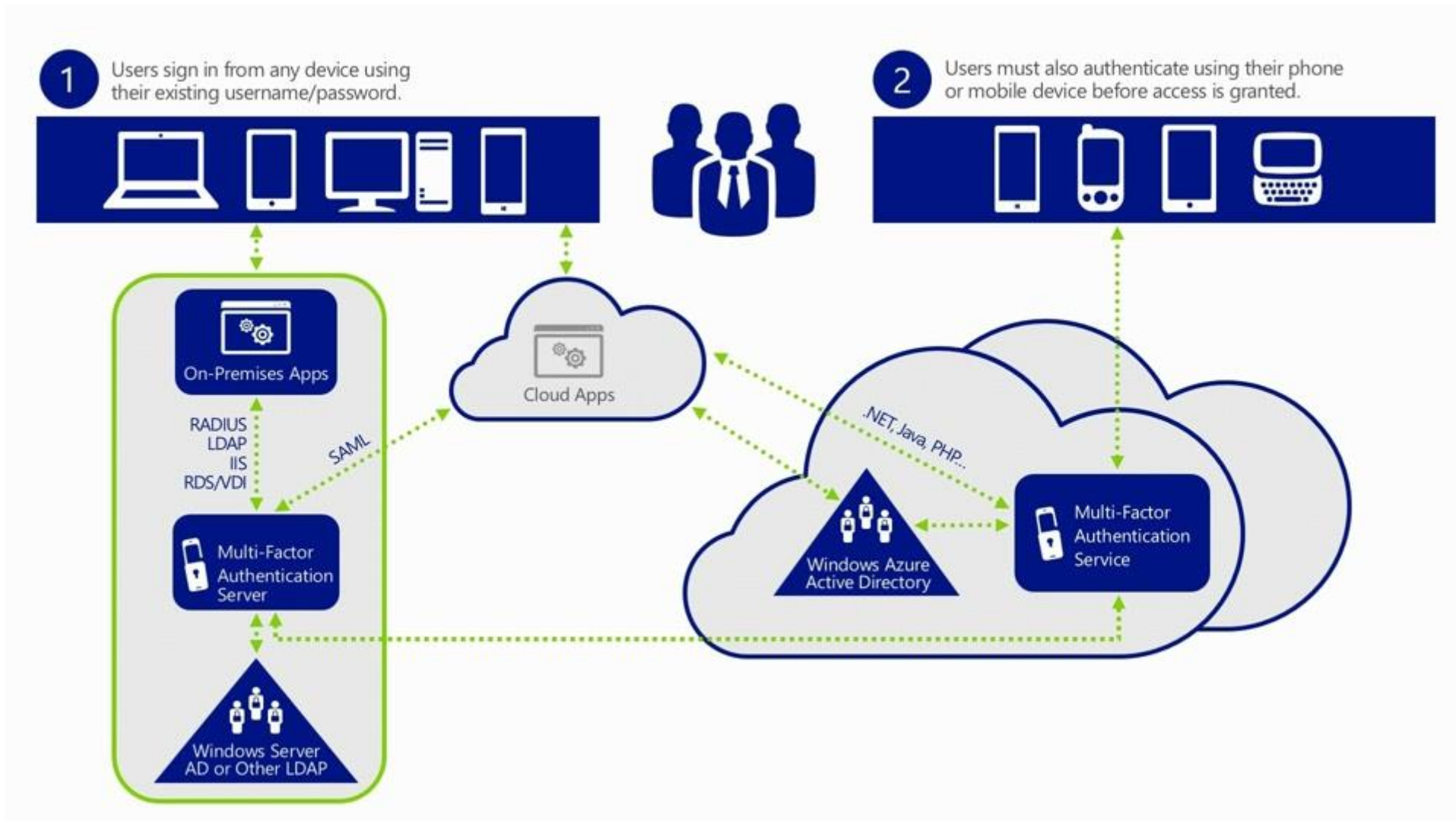
취소

# DEMO

Azure Active Directory Premium

1. 사용자 암호 재설정 구성
2. 다단계 인증

# 온프레미스와 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

