

# Duo with AnyConnect SAML and ISE TACACS+ v1.1



마지막 업데이트: 2020 년 1 월 7 일

**중요!** 이 콘텐츠는 커뮤니티에서 개발되었으며 표준 dCloud 검증 또는 지원의 대상이 아닙니다. 자세한 내용은 dCloud Support 에 문의하시기 바랍니다.

## 본 데모에 대하여

미리 구성되어 있는 본 데모는 아래 내용을 포함합니다:

[본 데모에 대하여](#)

[요구 사항](#)

[솔루션 소개](#)

[토폴로지](#)

[시작하기](#)

[시나리오 1. Duo 를 사용하여 Azure Active Directory 에 대해 Cisco ASA VPN SAML 로그인 보호](#)

[시나리오 2. Duo MFA 를 통해 TACACS+ 로그인 보호](#)

[부록 A. Appendix](#)

[What's Next?](#)



## 요구 사항

아래 항목은 데모를 진행하는데 필요한 구성요소입니다.

필수	옵션
개인 컴퓨터	없음
운영하는 Duo 계정(30 일 평가판 사용 가능)	
P2 라이선싱을 포함한 운영하는 Azure AD 계정 (30 일 평가판 사용 가능)	

## 솔루션 소개

- **Cisco Duo** 는 다양한 제품에서 멀티팩터 인증을 지원합니다. 이 솔루션은 Duo MFA 를 마이크로소프트의 Azure Active Directory 에 결합되는 AnyConnect 로그인과 Cisco 의 ISE(Identity Services Engine)를 통한 TACACS+ 로그인에 적용합니다.
- Cisco Duo 에 대한 자세한 내용을 원하시면 <https://duo.com> 을 방문하십시오.

## 구성

이 데모에는 현재 멀티팩터 없이 로컬 로그인을 사용하여 미리 구성된 환경이 포함되어 있습니다. AnyConnect VPN 로그인은 로컬 사용자 데이터베이스를 사용하여 ASA 에서 직접 처리됩니다. 마찬가지로 TACACS+를 사용하여 ISE 에 라우터 로그인은 ISE 의 로컬 사용자 데이터베이스를 사용하여 처리됩니다.

테이블 1. 자격 증명 및 디바이스 레벨

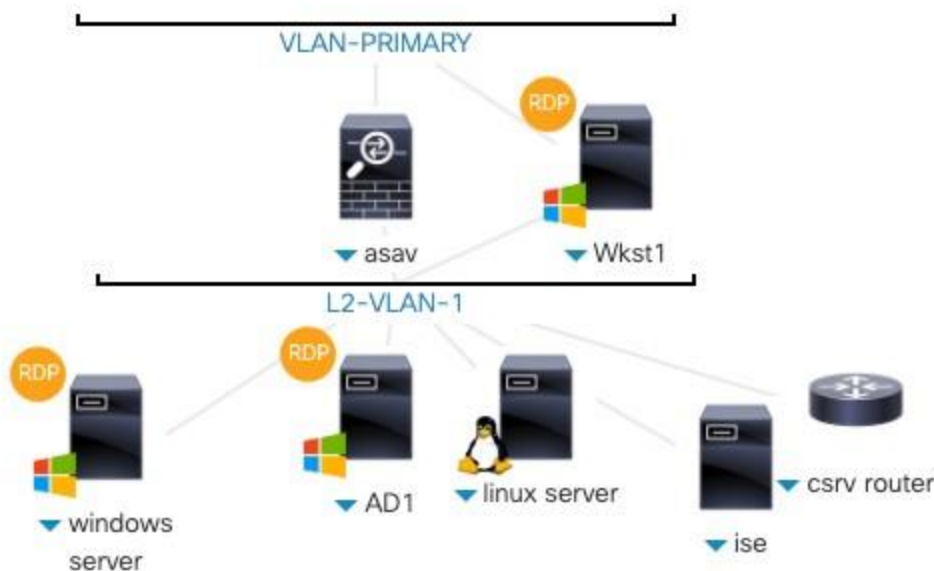
시나리오	사용자 이름	패스워드
Duo 통합 전 CSRv TACACS + 로그인	iseuser	C1sco12345
Duo 통합 후 CSRv TACACS + 로그인	routeradmin	C1sco12345
TACACS +가없는 CSRv	admin	C1sco12345
<b>AnyConnect VPN</b>	admin	C1sco12345

## 구성도

본 데모는 시나리오의 원활한 진행 및 솔루션이 제공하는 각 기능들의 동작 확인을 위해 사전 설정된 구성요소들을 포함하고 있습니다. 대부분의 구성요소들은 별도 제공되는 관리자 계정을 통해 설정이 가능하며 토폴로지 메뉴에 있는 구성요소 아이콘을 클릭하면 해당 구성요소에 접근하기 위한 IP 어드레스 및 계정 정보를 확인할 수 있습니다.

**노트:** L2-VLAN-1 에 대한 외부 연결은 ASAv 를 통과합니다. 이 ASAv 는 처리량 기능이 거의 없으며, RDP 나 L2-VLAN-1 웹 검색도 제대로 작동하지 않습니다. Windows 또는 AD1 서버의 변경이 필요한 경우 해결책으로 Wkst1 에서 필요한 서버로 RDP 연결하십시오. Wkst1 은 두 VLAN 에 모두 인터페이스가 있으므로 방화벽을 바이패스합니다.

그림 1. dCloud 토폴로지



## 시작하기

### 시작하기에 앞서

고객 및 파트너를 대상으로 데모 시연을 할 경우 원활한 진행을 위해 본 자료를 가지고 사전에 충분한 연습을 하시기를 권장합니다. 데모 완료 후 새롭게 구성을 해야 하는 경우는 세션을 다시 예약하십시오.

**사전에 충분한 연습은 성공적 진행을 위한 필수 조건입니다.**

세션 예약 및 데모 환경을 준비하기 위하여 아래 절차를 따라 주십시오.

1. dCloud 세션 시작. [\[가이드\]](#)

**노트:** 세션 예약 후 시나리오의 램이 활성화 되기까지 최대 45 분 소요됩니다.

1. 보다 빠른 환경으로 시나리오 진행을 원하는 경우는 **Cisco AnyConnect VPN** 클라이언트 [\[가이드\]](#) 및 **이용자 컴퓨터에 있는 로컬 RDP 클라이언트**를 이용해 접속하십시오. [\[가이드\]](#)

**노트:** dCloud 의 리모트 데스크탑 클라이언트 [\[가이드\]](#)를 이용한 접속도 가능합니다. dCloud Remote Desktop 클라이언트는 최소한의 상호 작용으로 활성 세션에 접속하는 데 가장 적합합니다. 그러나 많은 사용자가 이 방법으로 연결 및 성능 문제를 경험합니다.

## 시나리오 1. Duo 를 사용하여 Azure Active Directory 에 대해 Cisco ASA VPN SAML 로그인 보호

**노트:** 이 시나리오는 P2 라이선스 환경에서 Azure Active Directory 를 활용합니다. 계속하기 전에 환경이 정상으로 작동하는지 확인하십시오.

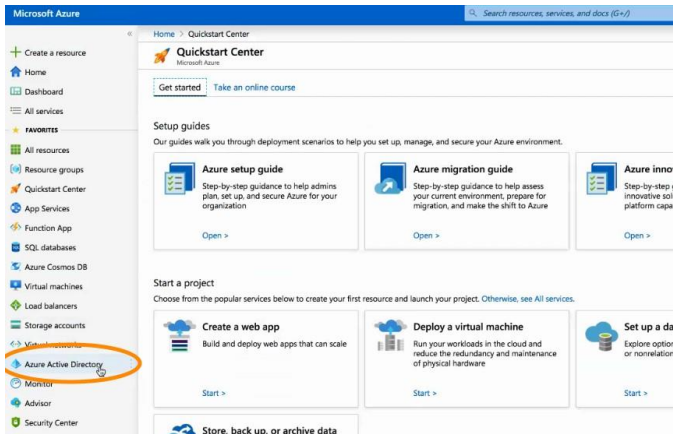
이 시나리오에서는 Azure 및 ASA 구성에 초점을 맞춰 다음 기능을 시연합니다.:

- ASA 의 인증 요청을 허용하도록 Azure AD 구성
- SAML 을 사용하여 Azure Active Directory SSO(Single Sign-On) 포털에 대해 사용자 인증을 위한 ASA 구성
- SAML 공급자 (Azure AD)를 사용하여 AnyConnect VPN 연결 인증

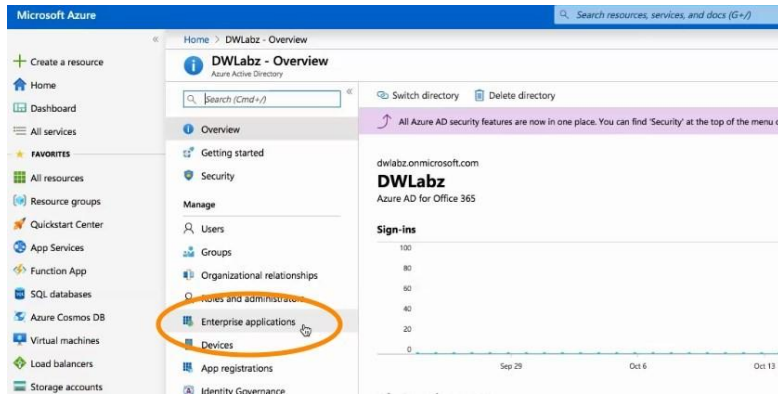
## Azure AD S 스텝

본 시나리오에서는 dCloud ASA 의 SAML 요청을 허용하도록 Azure AD 를 설정합니다. SSO 인증을 위해 Azure 에 ASA 애플리케이션을 작성합니다.

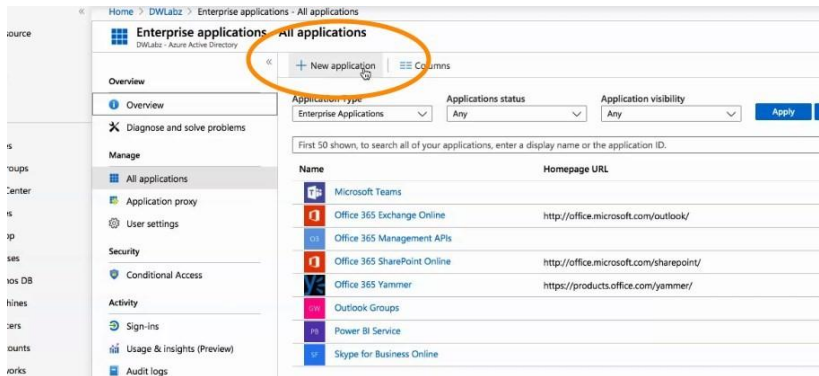
1. dCloud 워크스테이션 2 를 사용하여 <https://portal.azure.com> 의 사전 작업에서 만든 Azure Portal 에 로그인합니다. **Azure Active Directory** 를 클릭합니다.



3. Enterprise applications 에 클릭합니다.



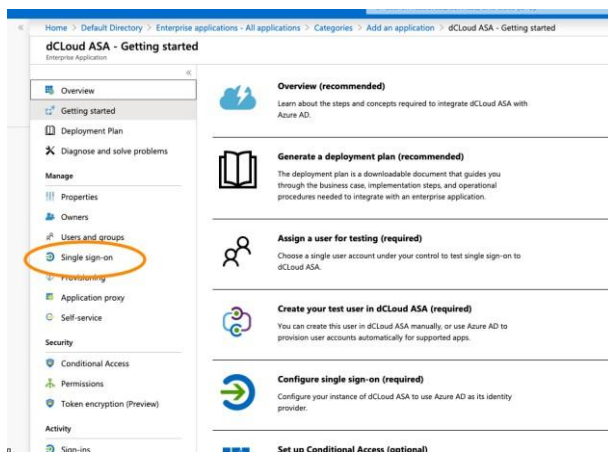
4. New application 에 클릭합니다.



5. Non-gallery application 에 클릭합니다.

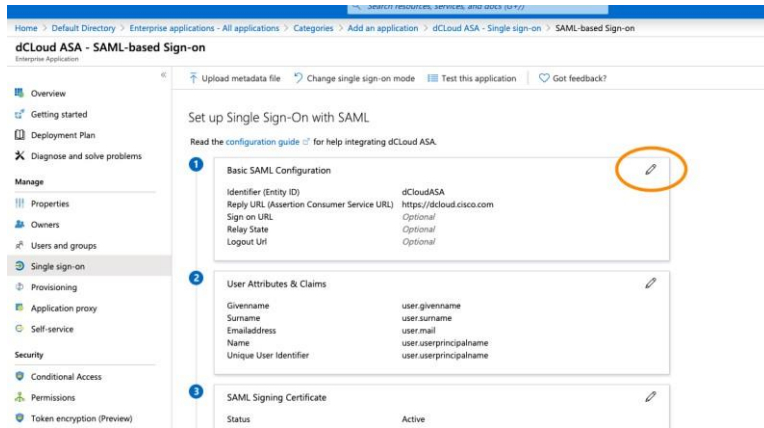
6. 애플리케이션에 이름 (예 : dCloud ASA)을 지정한 다음 Add 를 클릭합니다.

7. Single sign-on 에 클릭합니다.



8. SAML 을 클릭합니다.

9. Configuration box 1 에서 pencil(연필 아이콘)을 클릭합니다.



10. Identifier (Entity ID)를 <https://asav.dcloud.cisco.com/saml/sp/metadata/DefaultWEBVPNGroup> 으로 설정합니다.

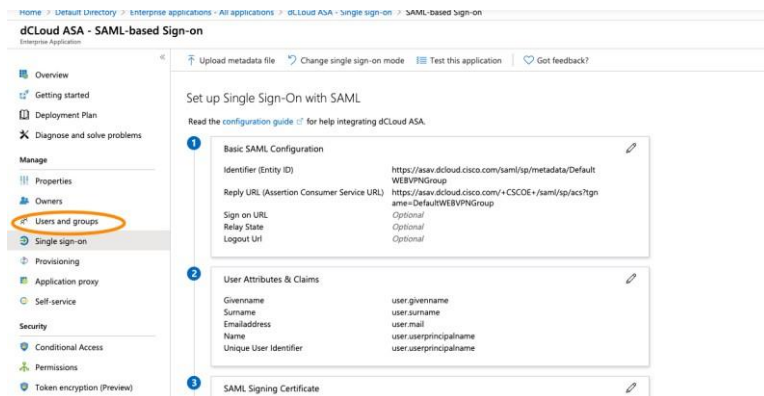
11. Reply URL (Assertion Consumer Service URL) 를 <https://asav.dcloud.cisco.com/+CSCOE+/saml/sp/acs?tgname=DefaultWEBVPNGroup> 으로 설정합니다.

12. Save 를 클릭한 다음에 No, I'll test later 를 클릭합니다.

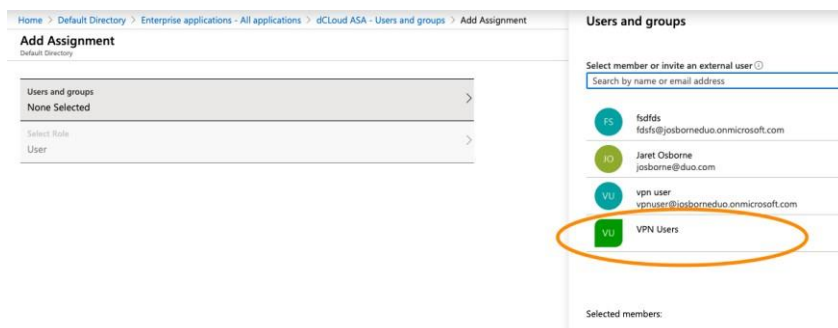
13. 섹션 3 에서 Certificate Base64 를 다운로드하고 dCloud 워크스테이션의 데스크탑에 저장합니다.

14. Login URL, Azure AD Identifier 및 Logout URL 을 dCloud 워크 스테이션 데스크톱의 텍스트 파일에 복사합니다.

15. 사전 작업에서 "VPN Users"라는 그룹을 Azure AD 에 생성했습니다. 이 그룹을 새로 만든 애플리케이션을 사용하려면 액세스 권한이 있어야 합니다. 애플리케이션에서 **Users and Groups** 를 클릭합니다.



16. Add user 를 클릭한 다음 사용자 및 그룹을 클릭하고 VPN User group (user 가 아닌)을 추가합니다.



17. **Select** 를 클릭한 다음 **Assign** 을 클릭합니다.

## ASA 스텝

다음으로, 로그인 프로세싱하는 Azure AD 를 사용하도록 ASA 를 구성해야 합니다. 이를 위해서는 ASA CLI 를 사용할 것입니다.

**노트:** ASA 에서 SAML 구성을 변경할 경우 변경 내용을 적용하려면 ASA 를 재부팅해야 하는 ASA 에 결함이 있습니다. 오타로 인해 SAML 구성을 수정해야 하는 경우, 먼저 ASA 를 저장하고 재부팅 하십시오. CSCvi23605 결함.

1. Trustpoint 를 만들고 이전에 다운로드한 인증서에서 텍스트를 가져옵니다.

a. Putty 를 사용하여 SSH 를 ASA 로 전송하고 저장된 "ASAv Outside Interface" 세션을 로드합니다.

b. admin 및 C1sco12345 를 사용하여 로그인한 다음

c. 구성 모드로 이동합니다.

i.enable

ii.Conf t

iii.Crypto ca trustpoint AzureAD\_SAML

revocation-check none

no id-usage

enrollment terminal

no ca-check

crypto ca authenticate AzureAD\_SAML

-----BEGIN CERTIFICATE-----

*다운로드한 인증서의 내용에 붙여넣습니다. Notepad 를 사용하여 인증서를 엽니다.*

-----END CERTIFICATE-----

quit

2. 다음으로 ASA 에서 Azure IdP 를 프로비저닝합니다.

a. webvpn

i. saml idp <https://sts.windows.net/.....> ← 이 값은 위 14 단계의 Azure AD Identifier 입니다.

url sign-in <https://login.microsoftonline.com/.....> ← 이 값은 위 14 단계의 Logib URL 입니다.

url sign-out <https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0>

← 이 값은 위 14 단계의 Logout URL 입니다.

trustpoint idp AzureAD\_SAML trustpoint sp

DCLLOUD-TRUSTPOINT

no force re-authentication no

signature

base-url <https://asav.dcloud.cisco.com>





3. 다음으로 터널 그룹을 수정합니다.

a. Tunnel-group DefaultWEBVPNGroup webvpn-attributes

- i. saml identity-provider <https://sts.windows.net/>..... ← 이 값은 위 14 단계의 Azure AD Identifier 입니다.  
authentication saml  
end  
write mem

4. 시점에서, prework 에서 생성된 vpnuser 를 사용하여 AnyConnect 로그인을 테스트할 수 있습니다. 전체 사용자 ID Azure AD 를 기록해 두십시오. [vpnuser@<your\\_email>.onmicrosoft.com](mailto:vpnuser@<your_email>.onmicrosoft.com) 과 같은 형식입니다.

- a. 서버 보안 인증서를 수락할지 묻는 메시지가 나타나면, Accept (동의)를 클릭하여 계속 진행하십시오.
- b. 처음 로그인 시 vpnuser 에 대한 패스워드를 변경해야 합니다. SSO 로그인을 통해 암호를 변경할 수 있습니다.

**노트:** ASA 에서 SAML 구성을 변경할 경우 변경 내용을 적용하려면 ASA 를 재부팅해야 하는 ASA 에 결함이 있습니다. 오타로 인해 SAML 구성을 수정해야 하는 경우, 먼저 ASA 를 저장하고 재부팅 하십시오. CSCvi23605 결함.

## Azure 애플리케이션에 Duo 추가하기

다음으로 VPN 로그인에 Duo Multiactor 를 추가해야 합니다. 로그인이 Azure 의 SSO IdP 를 활용하고 있으므로 Duo 기능을 Azure 에 추가한 다음 보호하려는 Azure 앱(이 예에서는 AnyConnect VPN 로그인만 해당)에 Duo 기능을 적용하면 됩니다.

**노트:** 이 단계를 완료하려면 Global Administrator 역할을 있는 Azure Active Directory 계정을 사용해야 합니다. 원래 Azure AD 평가판을 만드는 데 사용한 계정은 통합을 완료할 수 없는 Microsoft Account 일 수 있습니다. Global Admin 역할로 Azure AD 에 새 계정을 생성하고 사용할 수 있습니다.

### Azure Active Directory 사용자를 만들기(옵션, 위의 노트 참고)..

1. Azure Active Directory 에서 **User** 로 이동하십시오.
2. 새로운 User 를 추가합니다.
3. User 를 이름 및 username 을 지정합니다.
4. Azure 에서 패스워드를 할당하도록 할 수 있지만 암호를 반드시 보고 기록해야 합니다.
5. 역할을 Global administrator 로 설정합니다.



## Azure 에 Duo 통합을 추가하기

<https://duo.com/docs/azure-ca> 에서 제공한 지침에 따라 Duo 기능을 Azure 환경에 추가합니다. Azure 에 인증하라는 메시지가 표시되면 위에서 만든 Azure AD 사용자를 사용해야 합니다. "Create and Apply a Duo Conditional Access Policy"(Duo 조건부 액세스 정책 생성 및 적용) 단계에 도달하면 Duo 를 이전에 만든 "VPN User" 그룹 및 "dCloud ASA" 클라우드 애플리케이션에만 적용하도록 단계를 수정합니다.

## 시나리오 2. Duo MFA 로 TACACS + 로그인 보호

이 시나리오에서는 ISE 에 다시 TACACS+를 사용하여 라우터 로그인에 Duo MFA 를 추가하는 방법을 시연합니다. 이 예제에서 ISE 는 로컬 계정을 사용하도록 구성됩니다(디렉토리 통합 없음). 이는 ISE 에 Duo MFA 를 추가하는 여러 방법 중 하나입니다.

**노트:** 다양한 ISE 워크플로우에 Duo 보호를 추가하는 방법은 여러 가지가 있습니다. 본 시나리오는 가능한 구성 중 하나 일뿐입니다.

## Duo Admin Panel 스텝

먼저, Cisco ISE RADIUS 애플리케이션을 Duo 인스턴스에 추가하고 라우터 관리자(라우터 관리자)를 위한 해당 사용자를 추가합니다. <https://admin.duosecurity.com> 에서 Duo Admin 패널에 로그인합니다.

1. **Applications > Protect an Application** 을 클릭합니다.
2. **Cisco ISE RADIUS** 를 검색합니다.
3. **Protect this Application** 을 클릭합니다.
4. 맨 아래로 스크롤하여 이름을 **dCloud ISE RADIUS** 로 수정합니다.
5. **Save** 를 클릭합니다.

다음으로 "routeradmin"에 Duo user 를 추가합니다.

1. **User > Add User** 를 클릭합니다.
2. Username: **routeradmin**.
3. **Add User** 를 클릭합니다.

새로 만든 사용자 아래에서 설정을 변경할 필요가 없습니다. 다음으로, Duo 의 기존 2FA 장치에 "routeradmin" 사용자를 추가합니다.

1. 왼쪽 메뉴에서 **2FA Devices** 를 클릭합니다.



2. 가지고 있는 **2FA device** 를 찾아 클릭합니다.
3. **link** 를 클릭하여 사용자를 첨부합니다.
4. **routeradmin** 를 입력합니다.
5. **attach** 를 클릭합니다.

이제 Duo 의 routeradmin 사용자도 2FA 디바이스를 사용하도록 구성되었습니다.

## Duo Authentication Proxy 스텝

애플리케이션과 사용자를 추가한 후에는 Duo Auth Proxy 를 구성해야 합니다. Duo Authentication Proxy 는 dCloud 세션의 Windows Server 에 미리 설치되어 있습니다.

1. Windows Server 의 RDP (이 환경에서는 "scep"라고도 함)에 연결합니다.
  - a. 최상의 성능을 위해 DCloud web portal 에서 아닌 Jump Server/Wkst1 에서 RDP 세션을 시작합니다.
2. 데스크톱에서 바로 가기를 사용하여 **C:\Program Files (x86)\Duo Security Auth Proxy\conf** 로 이동합니다.
3. Notepad 에서 **authproxy.cfg** 를 열고 다음을 추가합니다:

- b. [radius\_server\_auto]  
ikey=*DXXXXXXXXXXXXXXXXXXXX*  
skkey=*XX*  
api\_host=*api-XXXXXXXX.duosecurity.com*  
radius\_ip\_1=198.19.10.27  
radius\_secret\_1=duoradius  
client=ad\_client  
port=1812  
failmode=safe

구성 파일은 다음과 같아야 합니다(XXXX 를 Duo 관리 패널의 값으로 대체).

```
[ad_client]
host=198.19.10.1
service_account_username=administrator
service_account_password=C1sco12345
search_dn=dn=dcloud,dc=cisco,dc=com
[radius_server_auto]
```

```
ikey=DXXXXXXXXXXXXXXXXXXXXX  
skey=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
api_host=api-XXXXXXXXX.duosecurity.com  
radius_ip_1=198.19.10.27  
radius_secret_1=duoradius  
client=ad_client  
port=1812  
failmode=safe
```

- c. 파일을 저장하고 메모장(notepad)을 닫습니다.
  - d. 데스크탑에서 서비스 아이콘을 두 번 클릭합니다.
  - e. Duo Security Authentication Proxy 를 마우스 오른쪽 버튼으로 클릭하고 재시작(restart)을 클릭합니다.
4. 마지막으로, C:\Program Files (x86)\Duo Security Authentication Proxy\bin\에서 authproxy\_connectivity\_tool.exe 를 실행하여 구성 파일에 구성을 올바르게 입력했는지 확인합니다.
- f. Start 를 클릭하여 명령 프롬프트(비 관리)를 열고 Command Prompt 아이콘을 클릭합니다 (참고: PowerShell 명령 프롬프트가 작동하지 않음, 태스크 바(Task bar)의 아이콘을 사용하지 마십시오).
  - g. 명령 프롬프트에 "C:\Program Files (x86)\Duo Security Authentication Proxy\bin\authproxy\_connectivity\_tool.exe" 따옴표를 포함해서 입력하고 Enter 키를 클릭합니다.
  - h. 인증 프록시 구성을 올바르게 구성한 경우 연결 문제 없이 **GREEN**(녹색)으로 반환되고 그렇지 않으면 스텝 3 부터 다시해야 합니다.
5. 이제 Windows Server 를 종료 할 수 있습니다.

## Active Directory 스텝

이 시나리오에서는 Duo Auth Proxy 를 사용하여 dCloud Active Directory 서버에 대해 사용자를 인증합니다. AD 사용자 그룹을 ISE 로 가져오지 않으므로 이 예제에서는 AD 를 ISE 의 JoinPoint 로 추가하지 않아도 됩니다. 이는 단순성과 데모를 위한 것입니다. 사용자가 ISE 보호 장치에 로그인하면 ISE 가 로그인 요청을 Duo Auth Proxy 로 보냅니다. Duo Auth Proxy 는 먼저 사용자를 AD 에 대해 확인한 다음 Duo MFA 를 호출합니다.

- 1. **AD1 RDP** 세션에 연결합니다.
  - a. 최상의 성능을 위해 DCloud 웹 포털이 아닌 Jump Server/Wkst1 에서 RDP 세션을 시작합니다.
- 2. 작업 표시줄의 아이콘을 클릭하여 **ADUC(Active Directory Users and Computers)** 를 엽니다.
- 3. **Users container** 를 클릭합니다.



4. 사용자 컨테이너를 마우스 오른쪽 단추로 클릭하고 New → User 를 선택하십시오.
  - b. First Name(이름): Router  
Last Name(성): Admin  
User logon name(사용자 로그인 이름): routeradmin  
Password(비밀 번호): C1sco12345  
UnCheck(체크 해제): 사용자는 다음 로그인시 비밀번호를 변경해야 합니다.  
Check(확인): Password never expires (비밀 번호가 만료되지 않음)
5. 이제 AD1 서버를 종료 할 수 있습니다.

## ISE Configuration 스텝

먼저, 로그인 처리에 Duo Authentication Proxy 를 사용하도록 ISE 를 구성해야 합니다:

1. dCloud 워크스테이션에서 Chrome 을 사용하여 사용자 admin 및 패스워드 C1sco12345 를 사용하여 <https://ise.dcloud.cisco.com> 으로 이동하여 dCloud 세션의 ISE Server 에 연결합니다. **Administration > Identity Management > External Identity Sources** 으로 이동합니다.
3. **RADIUS Token External Identity Source** 에 클릭한다음에 **Add** 를 클릭합니다.
  - a. 일반적으로, 이름 설정: **DuoAuthProxy**  
Connection 에서 IP 주소를 Duo Auth Proxy 가 실행 중인 Windows Server 로 설정합니다.  
198.19.10.102  
Shared Secret 설정: duoradius <Duo Auth Proxy.cfg 파일에서 설정한 것과 동일함>  
서버 제한 시간 설정: 60  
**Submit** 를 클릭합니다.

그런 다음 라우터 관리에 사용할 사용자를 ISE 에 추가합니다:

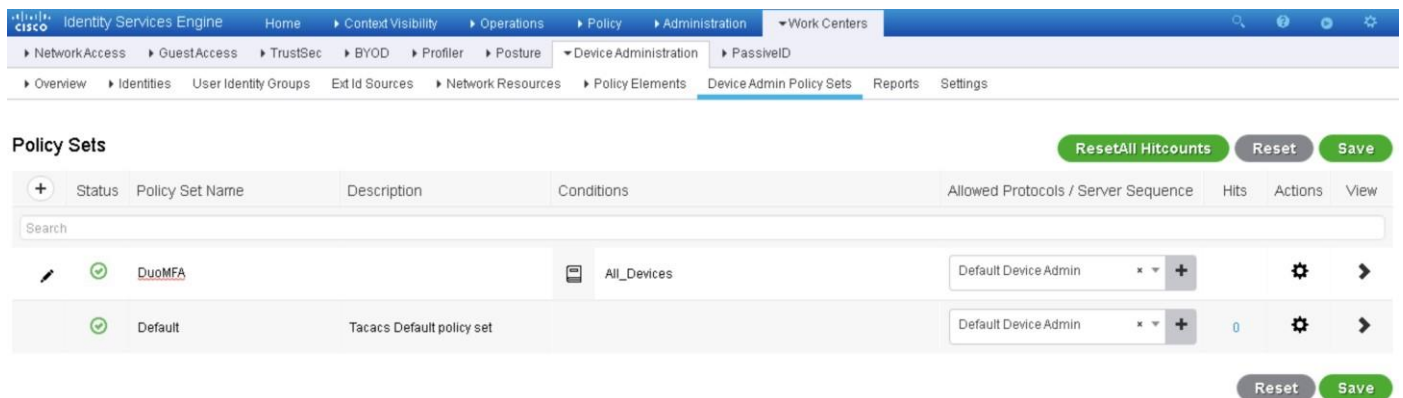
1. **Administration > Identity Management > Identities** 로 이동합니다.
2. **Add** 를 클릭합니다.
  - a. 이름 (Name): routeradmin  
패스워드 유형(Password Type): DuoAuthProxy  
사용자 그룹(User Groups): Router Admin  
Submit(제출)를 클릭합니다.

이제 Duo 와 사용자가 ISE 에 추가되었으므로 ISE 의 DeviceAdmin Policy Sets 를 구성해야 합니다. 이 설정을 Network Access Control 에 사용되는 정책 세트와 혼동하지 마십시오.

1. **Work Centers > Device Administration > DeviceAdmin Policy Sets** 로 이동합니다.



2. + 기호를 클릭합니다.
3. 정책 세트에 DuoMFA 4 와 같은 이름을 지정합니다. Duo MFA 의 조건(Conditions) 섹션에서 + 기호를 클릭합니다.
  - a. **All Devices** 로 설정합니다.  
**Use** 를 클릭합니다.
5. Allowed Protocols/Server Sequence 에서:
  - a. **Default Device Admin** 을 클릭합니다.
6. **save** 를 클릭합니다.



다음으로 구성을 완료하려면 정책을 입력해야 합니다. 방금 만든 정책 세트의 보기 열(View column)에서 > 를 클릭합니다.

1. 인증 정책 섹션에서 새 규칙을 추가합니다:
2. Name(이름): **Duo\_Auth**
3. Conditions(조건):
  - a. Device(디바이스): Location EQUALS All Location AND
  - b. Network Access Protocol EQUALS TACACS+
4. Use column(사용 열)에서:
  - a. DuoAuthProxy 를 사용하도록 설정  
Options(옵션):  
If Auth Fails(인증 실패 시): Reject(거부)  
If User Not Found(사용자를 찾을 수 없는 경우): Continue(계속)  
If Process Fail(프로세스가 실패한 경우): Continue (계속)



5. Authorization Policy 섹션에서 새 규칙을 추가합니다.
6. Name(이름): **Router\_admins**
7. Conditions(조건):
  - a. InternalUser-IdentityGroups EQUALS User Identity Groups: Router Admin
8. Shell Profiles 열에서:
  - a. CSR\_Admin\_Privilege 를 사용하도록 설정.

9. **Save** 를 클릭합니다.



## 설정 테스트하기 (Test the setup)

dCloud jump station 에서 Putty 를 사용하여 CSRv 에 SSH 세션을 시도합니다. 사용자 routeradmin 및 비밀번호 C1sco12345 로 로그인합니다. routeradmin 을 추가 한 Duo 앱에 대한 푸시를 자동으로 받을 것입니다.

대안으로, 비밀번호 끝에 침표(",") 를 추가한 다음 Duo 패스코드를 추가할 수 있습니다(패스코드는 모바일 장치의 Duo 앱에서 사용 가능합니다):

**username: routeradmin**

**password: C1sco12345,123456**

또한 패스코드 대신 out-of-band factor 이름을 입력할 수도 있습니다. 다음 목록에서 요소 이름을 선택할 수 있습니다.

<b>push</b>	Duo Push 인증 수행 디바이스에 Duo Mobile 을 설치하고 활성화한 경우 Duo Push 를 사용 가능합니다.
<b>phone</b>	전화 콜백을 통해 인증 수행
<b>sms</b>	새로운 일괄 SMS 암호 전송 인증 시도가 거부됩니다. 그런 다음 새로 제공된 패스코드 중 하나로 인증할 수 있습니다.

SMS 를 통해 새 패스코드를 전송하는 예:

**username: routeradmin**

**password: C1sco12345,sms**

## 부록 A. Appendix

본 연구소는 Azure Active Directory 를 활용하며, 참가자는 Premium P2 라이선스가 활성화된 Azure AD 환경에서 작업해야 합니다. Microsoft 는 참가자들이 Azure AD 테스트 환경에 접속할 수 없는 경우 30 일 무료 평가판을 제공합니다. 30 일 평가판을 설치하려면 유효한 신용 카드가 필요하지만 자동으로 갱신되지는 않습니다. 사용자가 30 일 이상 평가판을 계속 진행하도록 Microsoft 에 특별히 지시하지 않는 한 신용카드는 청구되지 않습니다.

참가자는 활성 Duo 인스턴스도 필요합니다.

## Duo 인스턴스에 가입하기

랩에는 Duo 작업 인스턴스가 필요합니다. 이미 가지고 계시면 그걸로 쓸 수 있습니다. 그렇지 않은 경우 Cisco.com 이메일 주소를 사용하여 등록해 주십시오.

1. <https://signup.duo.com/>으로 이동합니다.
2. Cisco.com 이메일 주소를 사용해야 합니다.

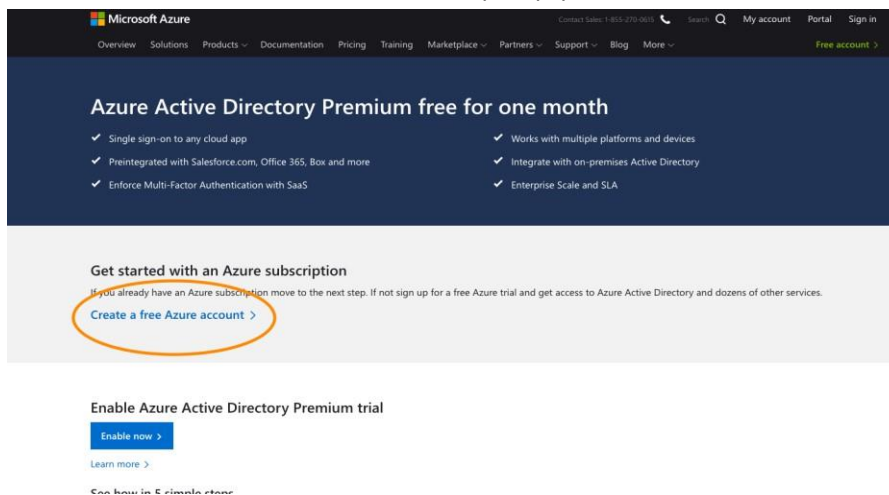


## Azure Active Directory 에 가입하기

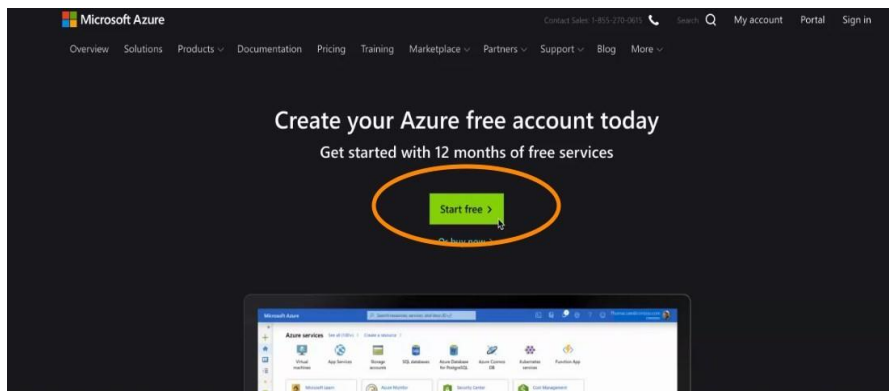
**노트:** 이 섹션의 특정 기능을 사용하도록 설정한 후 Microsoft 클라우드에서 백엔드 변경이 발생하는 데 다소의 시간이 걸립니다. 백엔드 변경이 완료될 때까지 1 시간을 소요됩니다.

이 프로세스를 수행하려면 유효한 신용 카드가 필요합니다. 평가판을 계속 진행하도록 선택하지 않은 한 신용카드는 청구되지 않습니다. Microsoft 는 요금이 청구되기 전에 문의하고 확인할 것입니다.

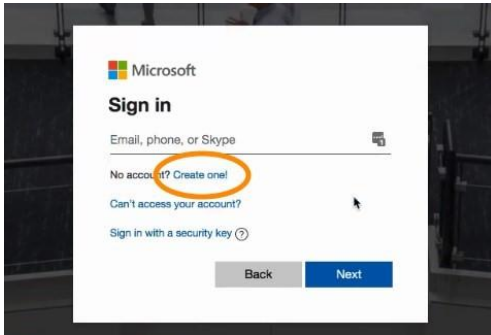
1. <https://azure.microsoft.com/en-us/trial/get-started-active-directory/>으로 이동합니다.
2. "Create a Free Azure account"를 클릭합니다.



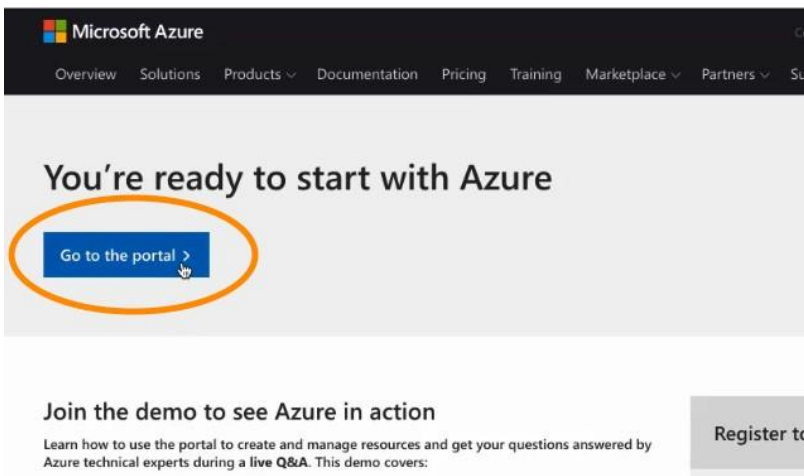
3. 그럼 다음 **Start free** 를 클릭합니다.



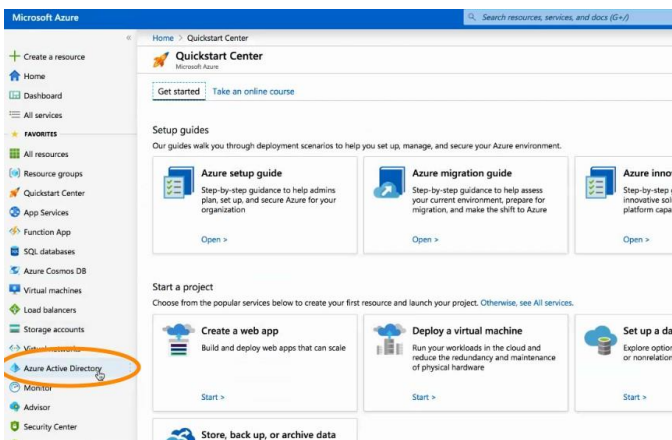
4. 이 시점에서 새 계정을 만들거나(Cisco.com 이메일을 사용하지 마십시오) 기존(Cisco.com 아닌 이메일) 계정을 사용할 수 있습니다. 새 계정을 만들 경우 **Create one!** 링크를 클릭하여 만듭니다.



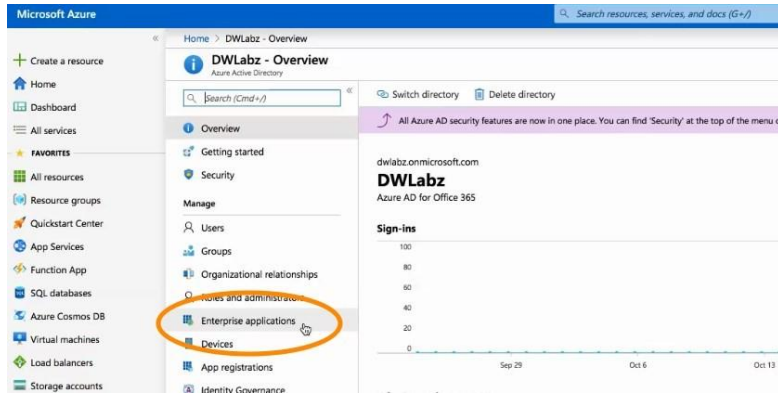
5. 계정이 있으면 About You, 계정이 있으면 About You, 전화로 신원 확인, 카드로 신원 확인(참고: 요금이 청구되지 않음)를 완료한 다음 계약 6 에 동의해야 합니다. 이제 포털로 이동할 수 있습니다.



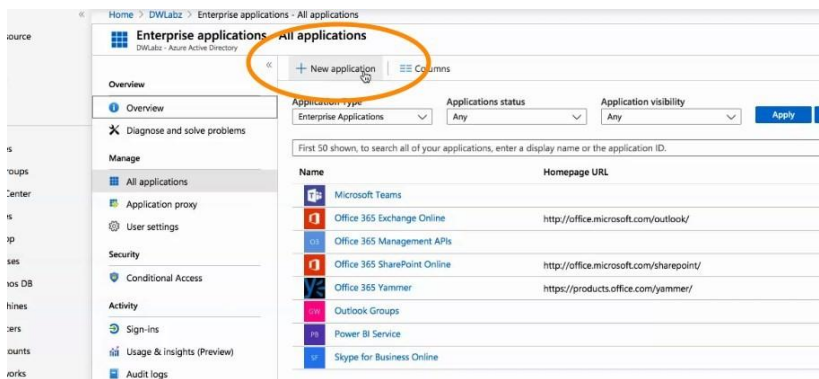
7. 다음으로 P2 평가판을 추가해야 합니다. **Azure Active Directory** 에 클릭합니다.



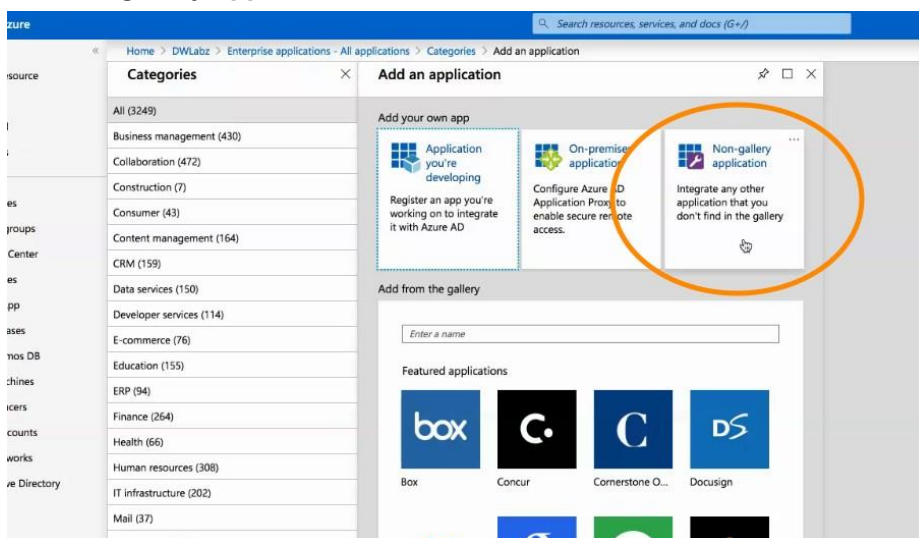
8. Enterprise applications 에 클릭합니다.



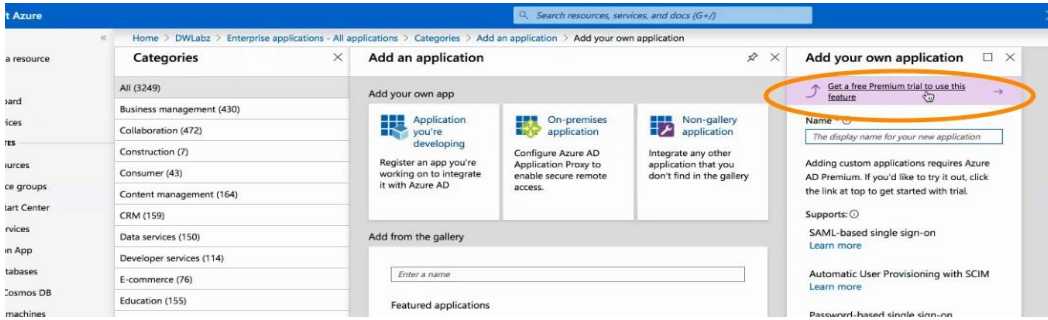
9. New Application 에 클릭합니다.



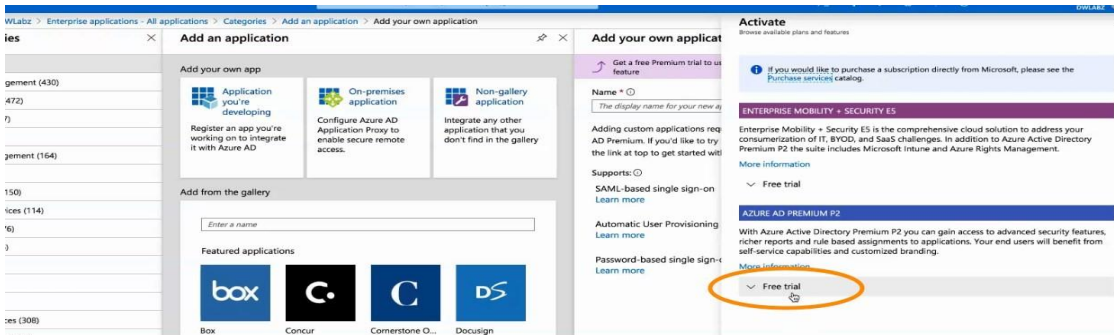
10. Non-gallery application 에 클릭합니다.



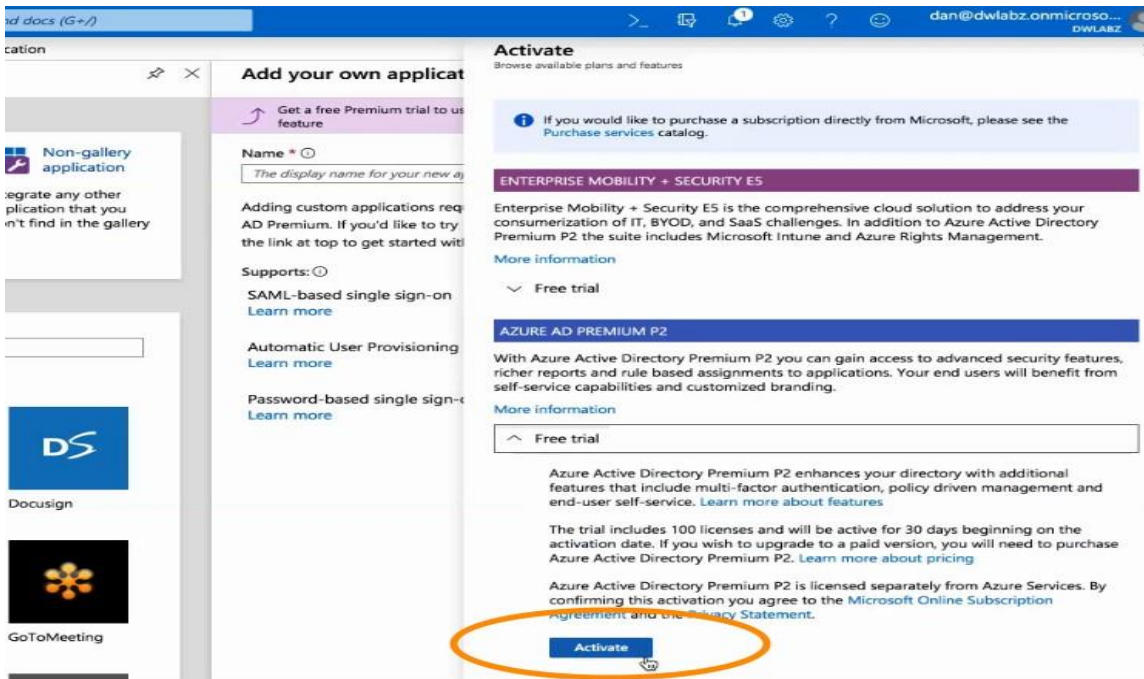
11. 이 기능을 사용하려면 purple free Premium trial (보라색 무료 프리미엄 평가판)을 클릭합니다.



12. AZURE AD PREMIUM P2 에서 Free trial 를 클릭합니다.



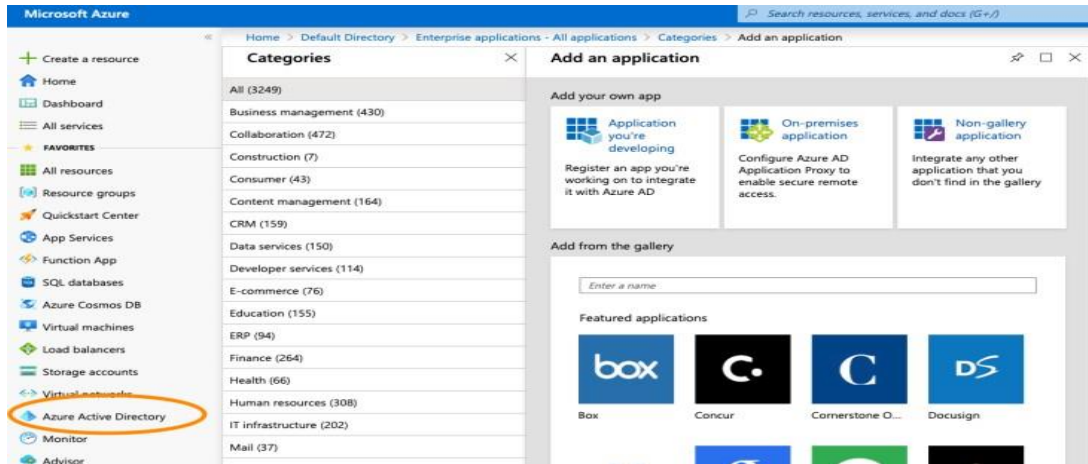
a. 그런 다음 Activate 를 클릭합니다.



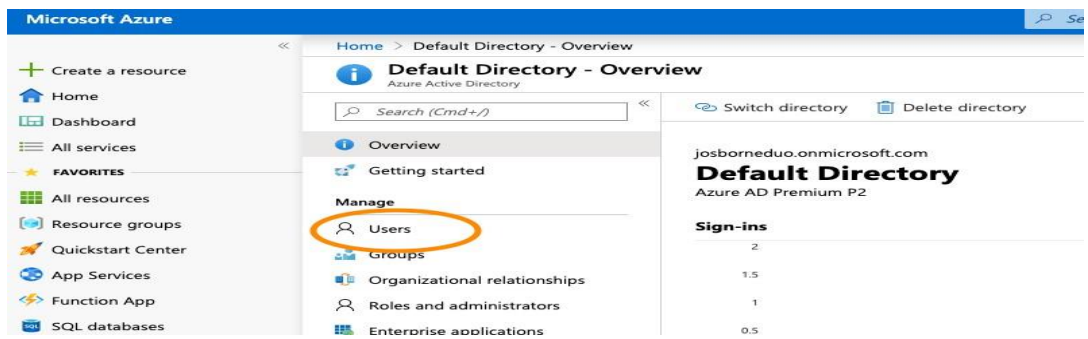
13. P2 라이선스는 백그라운드에서 추가되고 있으며 약 30 분 이상 유효하지 않습니다. 보라색 "Get free trial"(무료 평가판 받기) 상자가 한동안 그대로 있는 것은 전상입니다.

**노트:** 이 기능을 사용하도록 설정한 후 Microsoft 클라우드에서 백엔드 변경 사항이 발생하려면 시간이 좀 걸립니다. 백엔드 변경이 완료되는 데 1 시간이 소요됩니다.

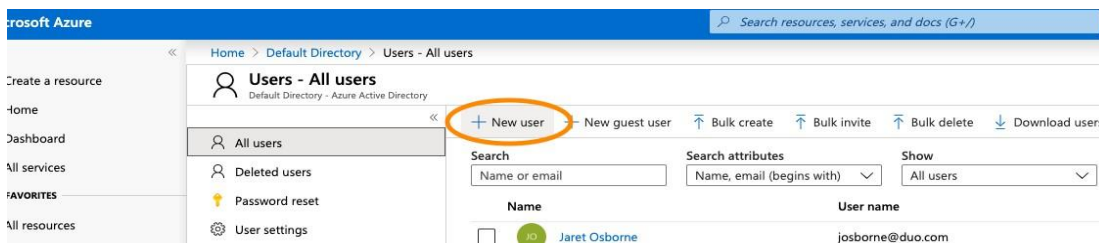
14. P2 라이선스가 백그라운드에서 추가되는 동안 잠시 시간을 내어 사용자를 Azure Active Directory 에 추가합니다.  
왼쪽 메뉴에서 **Azure Active Directory** 를 클릭합니다.



15. **Users** 를 클릭합니다.



16. **New User** 버튼을 클릭합니다.



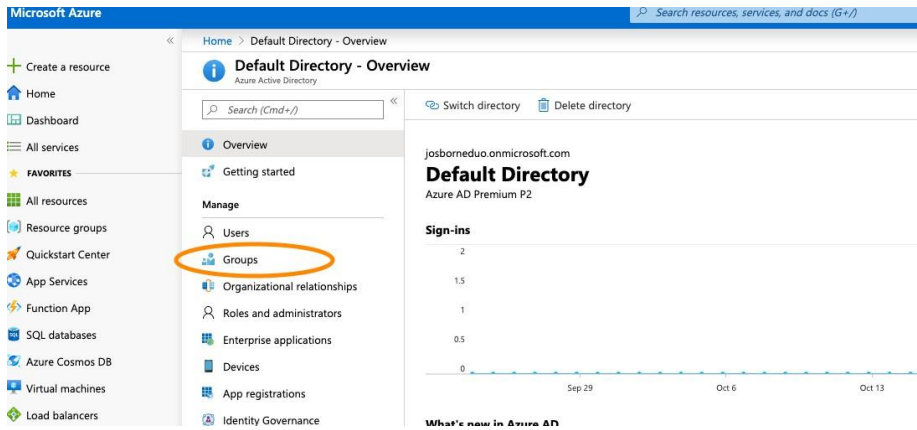
17. User name 을 **vpnuser** 로 설정합니다.

18. Password 를 **C1sco12345** 로 설정합니다.

19. 왼쪽 메뉴에서 **Azure Active Directory** 를 클릭하여 그룹을 만듭니다.

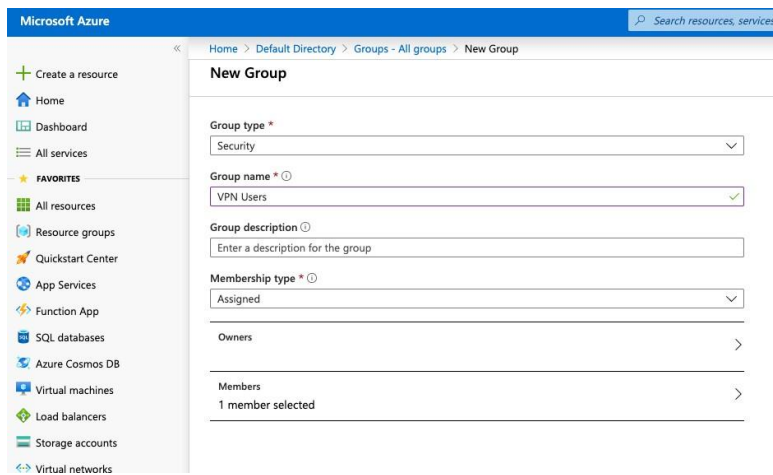
20. **Groups** 를 클릭합니다.





21. 새 그룹(group)을 생성합니다.

- a. Type(유형): Security
- b. Group name(그룹 이름): VPN Users
- c. Membership type(회원 유형): Assigned
- d. Members 클릭하고 위에서 "vpnuser"를 추가합니다.



b. **Create** 를 클릭합니다.

22. 이제 Azure AD 사전 작업(preview)이 완료되었습니다.



## What's Next?

Cisco Duo 에 대한 추가 정보를 원하시면 <https://duo.com> 을 방문하십시오.



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)