

# LDAP 및 Duo Multifactor Authentication과 IMM(Intersight Managed Mode) 디바이스 콘솔 통합 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[구성](#)

[네트워크 다이어그램](#)

[1단계.](#)

[2단계.](#)

[3단계.](#)

[4단계.](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

---

## 소개

이 문서에서는 LDAP 및 Duo 인증 프록시를 사용하여 IMM 디바이스 콘솔에서 멀티팩터 인증을 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

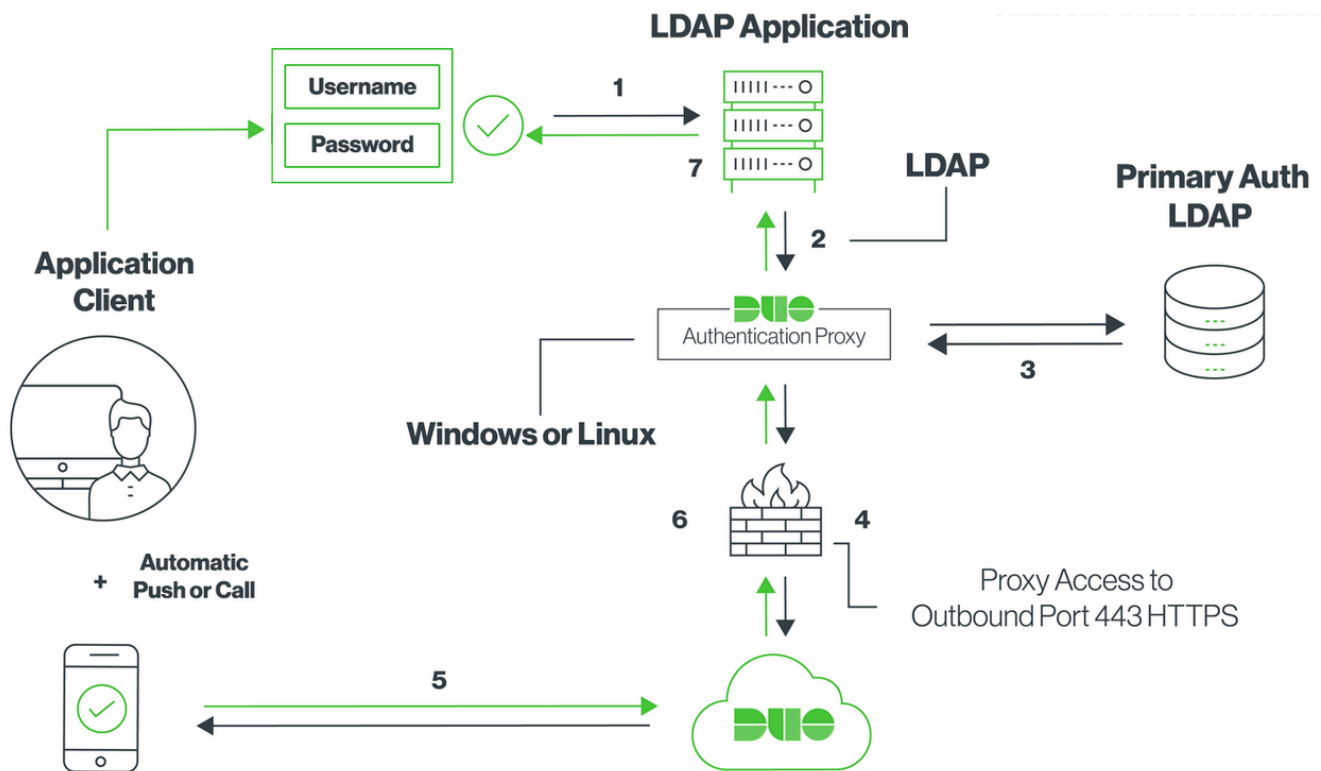
### 요구 사항

IMM(Intersight Managed Mode)의 UCS 패브릭 인터커넥트.

등록된 사용자와의 Duo 서브스크립션.

## 구성

### 네트워크 다이어그램



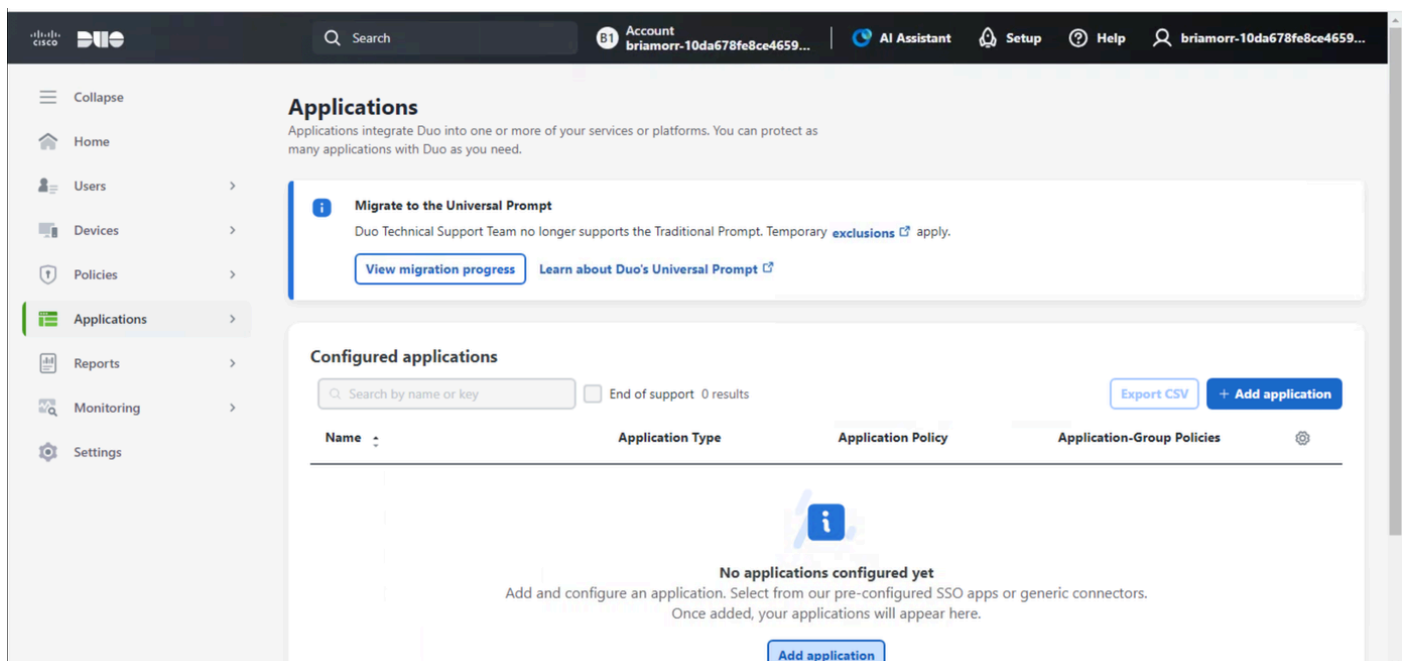
1단계.

Active Directory 및 IMM 디바이스 콘솔 모두에서 액세스할 수 있는 Windows 서버에 Duo 인증 프록시를 설치합니다.

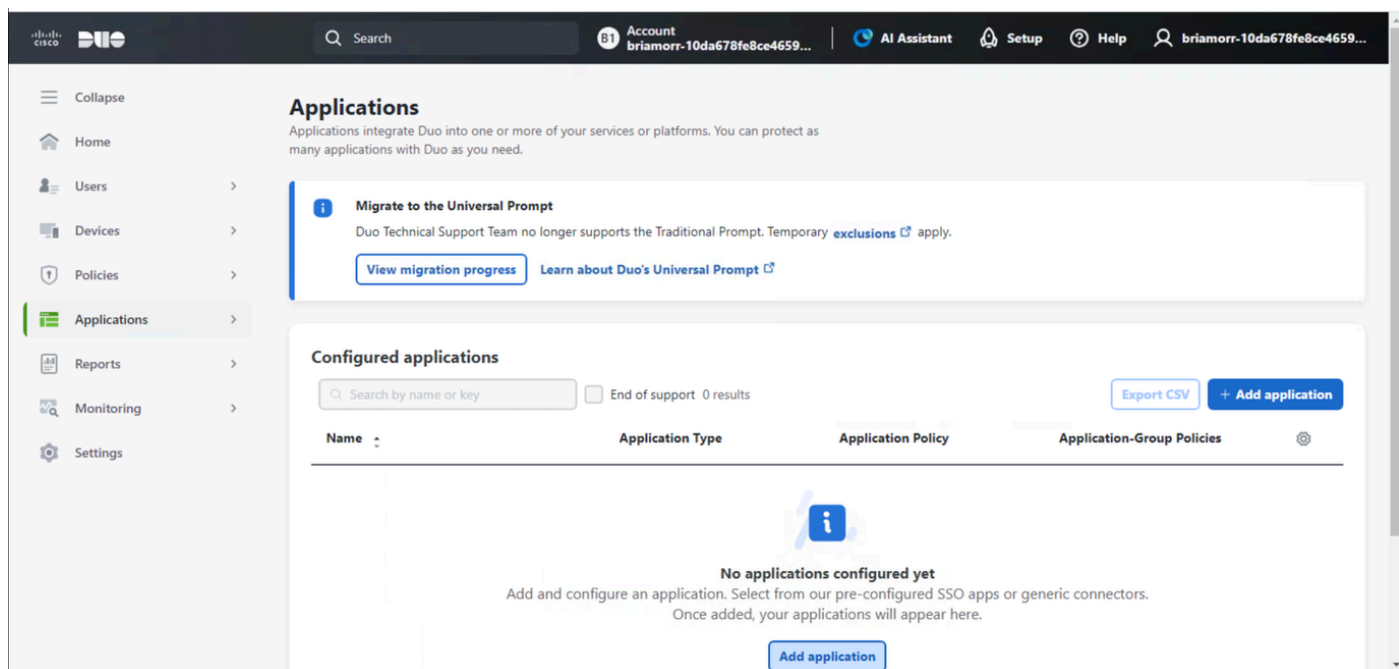
Duo 인증 프록시는 여기에서 찾을 수 [있습니다](#).

2단계.

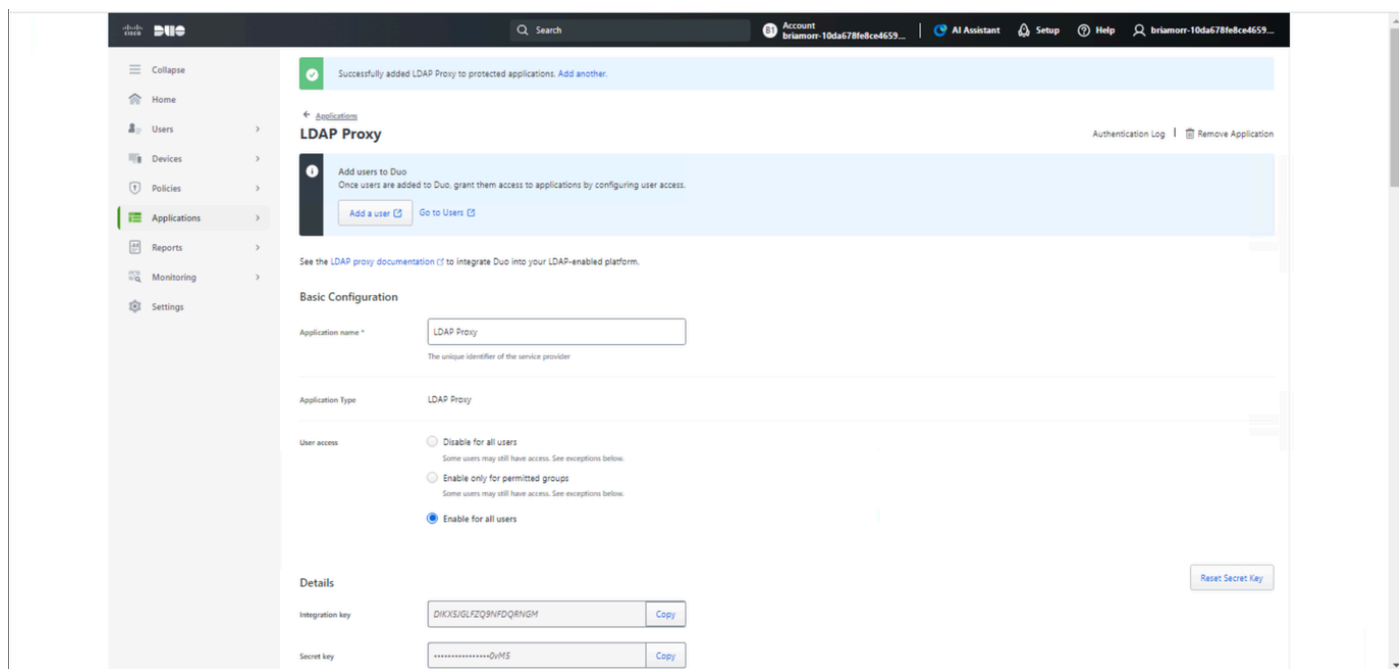
Duo 인스턴스에서 새 애플리케이션을 추가할 수 있습니다.



Idap를 검색하고 계속하려면 LDAP 프록시를 추가합니다.



LDAP 프록시 애플리케이션 아래에서 애플리케이션 이름을 구성하고 모든 사용자에게 대해 활성화하며 나중에 사용할 수 있도록 통합 키, 비밀 키 및 API 호스트 이름을 복사할 수 있습니다.



3단계.

Duo Authentication Proxy를 설치한 서버로 돌아가면 Duo Authentication Proxy Manager를 구성할 수 있습니다.

Duo Authentication Proxy Manager
Authentication Proxy is running
Uptime: 00:02:14
Version: 6.5.2
Restart Service
Stop Service

Configure: authproxy.cfg
Unsaved Changes

```

12 ; CLIENTS: Include one or more of the following configuration secti
13 ; To configure more than one client configuration of the same type,
14 ; number to the section name (e.g. [ad_client2])
15
16 [ad_client]
17 host=ad1.dcloud.cisco.com
18 service_account_username=ldap
19 service_account_password=changeme
20 search_dn=DC=dcloud,DC=cisco,DC=com
21
22
23 ; SERVERS: Include one or more of the following configuration secti
24 ; To configure more than one server configuration of the same type,
25 ; number to the section name (e.g. radius_server_auto1, radius_serv
26
27 [ldap_server_auto]
28 client=ad_client
29 ikey=DI*****
30 skey=*****
31 api_host=api-demodemo.duosecurity.com
32 failmode=safe
33 port=1389
34 exempt_ou_1=CN=ldap,CN=Users,DC=dcloud,DC=cisco,DC=com
35 exempt_primary_bind=false
36 allow_unlimited_binds=true

```

Output

Validate the configuration to view output

Validate
Save
[Learn how to configure the Authentication Proxy](#)

Duo 인증 프록시 샘플 구성:



참고: 가독성을 위해 추가된 의견 수

```

[ad_client]
host=ad1.dcloud.cisco.com    # Our Domain Controller
service_account_username=ldap # Our BIND Service Account in AD
service_account_password=changeme # Service Accounts BIND password
search_dn=DC=dcloud,DC=cisco,DC=com # LDAP Search DN

[ldap_server_auto]
client=ad_client
ikey=DI*****           # Copy from Duo LDAP Proxy App Page
skey=*****             # Copy from Duo LDAP Proxy App Page
api_host=api-demodemo.duosecurity.com # Copy from Duo LDAP Proxy App Page
failmode=safe           # If proxy cant communicate with Duo cloud, allow auth with credentials only
port=1389                # Port the LDAP Proxy listen on
exempt_ou_1=CN=ldap,CN=Users,DC=dcloud,DC=cisco,DC=com # Exempt the Service Account from MFA
exempt_primary_bind=false # Exempt the Service Account from MFA on initial bind
allow_unlimited_binds=true # Allow multiple binds, needed to prevent "Attempt to bindRequest multiple

```

4단계.

그런 다음 Intersight에서 기본 dn, 바인드 dn, LDAP 서버 ip, 비밀번호 등 필요한 Active Directory 설정으로 Duo LDAP 프록시를 가리키는 LDAP 정책을 생성할 수 있습니다. 먼저 Active Directory를 직접 가리키고 LDAP 서버를 Duo LDAP 프록시로 변경하기 전에 올바르게 작동하는지 확인하여 문제를 더 쉽게 해결할 것을 권장합니다.

Policy Details

Enable LDAP

Base Settings

Base DN: DC=dccloud,DC=ntosco,DC=com

Timeout: 180

Enable Encryption

Binding Parameters

Bind Method: Configured Credentials

Bind DN: CN=ldap,CN=Users,DC=dccloud,DC=ntosco,DC=com

Password: [redacted]

Search Parameters

Filter: SAMAccountName=\$userid

Group Attribute: memberOf

Attribute: memberOf

Group Authorization

Group Authorization: Enabled

Nested Group Search: Enabled

Nested Group Search Depth: 128

Search Parameters

Filter: SAMAccountName=\$userid

Group Attribute: memberOf

Attribute: memberOf

Group Authorization

Group Authorization: Enabled

Nested Group Search: Enabled

Nested Group Search Depth: 128

Configure LDAP Servers

Server: 3.135.250.11

Port: 12956

Vendor: MSAD

Add New LDAP Group

Name	Group DN	End Point Role
Domain Users	CN=Domain Users,CN=Users,DC=dccloud,DC=ntosco	admin

Export

다음을 확인합니다.

디바이스 콘솔에서 이전에 Duo에 등록한 LDAP 사용자로 로그인합니다.

# Device Console

Username \* ⓘ

mfauser

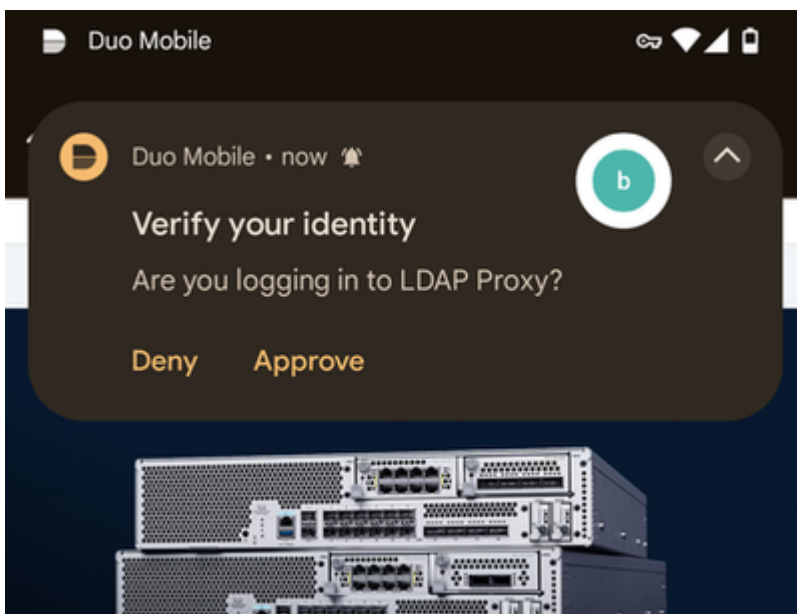
Password \*

.....

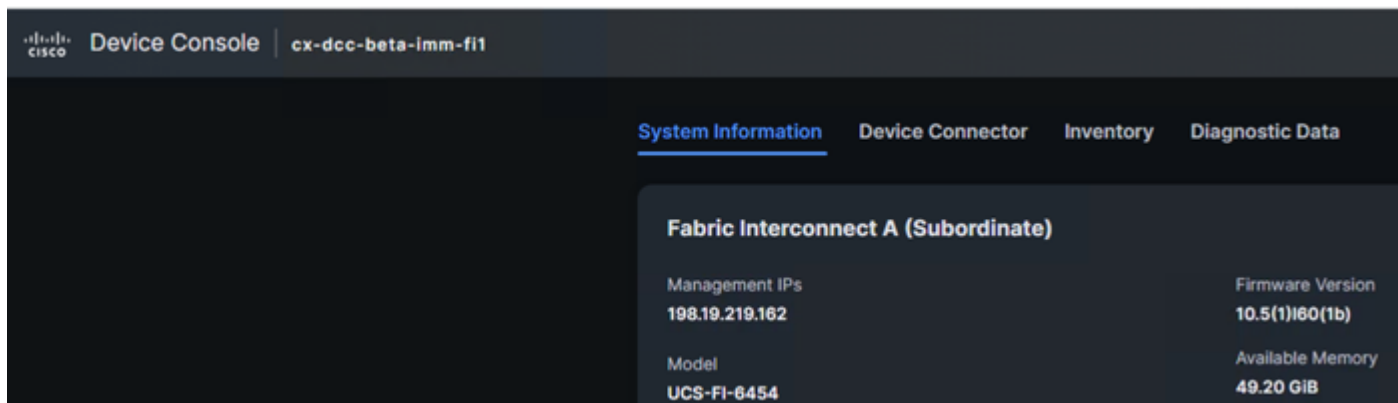
Show

Sign In

그러면 등록된 사용자는 자신의 디바이스에서 로그인하라는 프롬프트를 얻을 수 있습니다.



요청이 확인되면 2단계 인증 및 LDAP를 사용하여 디바이스 콘솔에 성공적으로 로그인할 수 있습니다.



## 문제 해결

Duo LDAP 프록시 로그는 다음 위치에 있습니다.

```
C:\Program Files\Duo Security Authentication Proxy\log\authproxy.log
```

Intersight Managed Mode Fabric Interconnect의 경우:

```
connect nxos
```

```
debug ldap
```

## 관련 정보

- [Device Console 설명서](#)
- [듀오가 뭔가요?](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.