

FMC 관리 액세스를 위한 듀오 2단계 인증 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[인증 흐름](#)

[인증 흐름 설명](#)

[구성](#)

[FMC의 컨피그레이션 단계](#)

[ISE의 컨피그레이션 단계](#)

[Duo 관리 포털의 컨피그레이션 단계](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 FMC(Firepower Management Center)에서 관리 액세스를 위한 외부 2단계 인증을 구성하는 데 필요한 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FMC(firepower 관리 센터) 개체 컨피그레이션
- ISE(Identity Services Engine) 관리

사용되는 구성 요소

- 버전 6.3.0을 실행하는 Cisco FMC(Firepower Management Center)
- 버전 2.6.0.156을 실행하는 Cisco ISE(Identity Services Engine)
- Duo 인증 프록시 서버 역할을 할 수 있도록 FMC, ISE 및 인터넷에 연결되어 있는 지원되는 Windows 버전(<https://duo.com/docs/authproxy-reference#new-proxy-install>)
- FMC, ISE 및 Duo 관리 포털에 액세스하기 위한 Windows 머신
- Duo 웹 계정

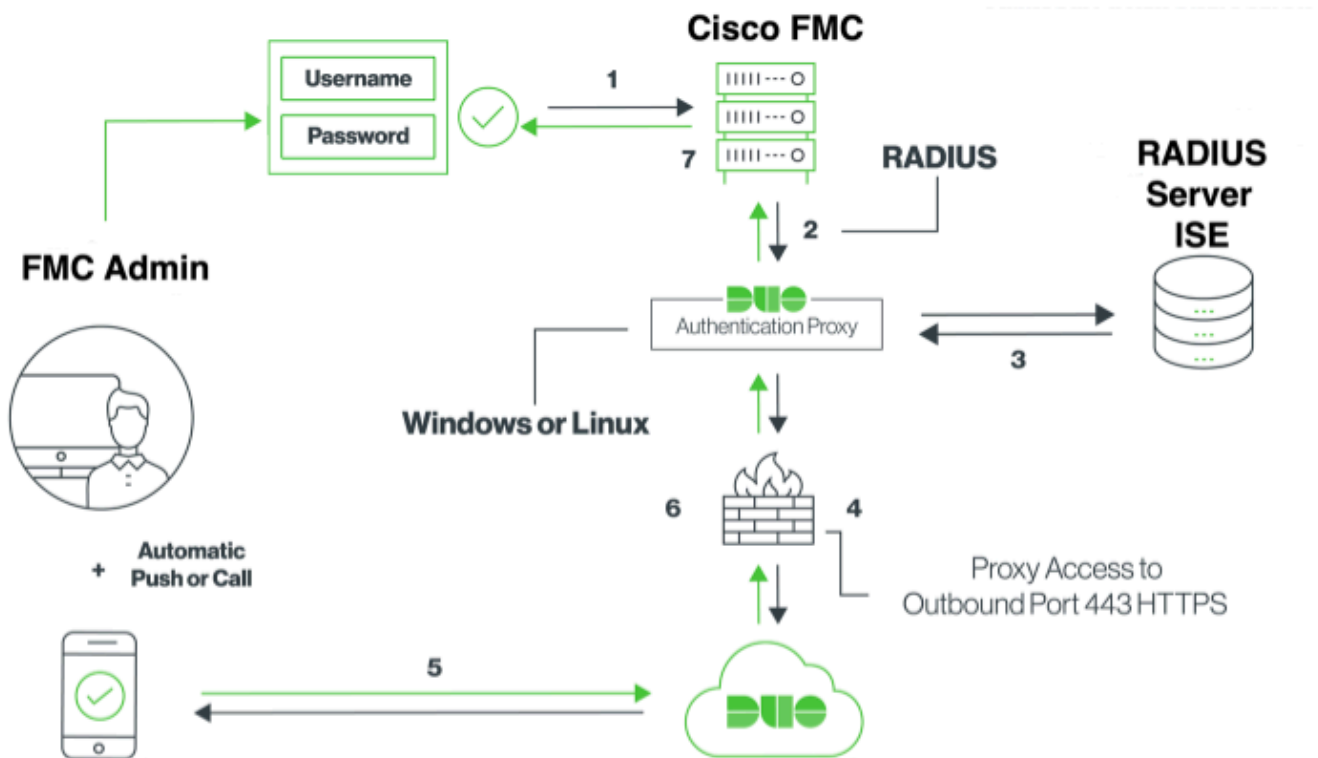
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

FMC 관리자가 ISE 서버에 대해 인증하고 Duo Authentication Proxy 서버에서 푸시 알림 형태의 추가 인증을 관리자의 모바일 디바이스로 전송합니다.

인증 흐름



인증 흐름 설명


1. Cisco FMC에 대한 기본 인증이 시작되었습니다.
2. Cisco FMC는 Duo 인증 프록시에 인증 요청을 보냅니다.
3. 기본 인증에서는 Active Directory 또는 RADIUS를 사용해야 합니다.
4. Duo 인증 프록시 연결이 TCP 포트 443을 통해 Duo 보안에 설정되었습니다.
5. Duo Security 서비스를 통한 2차 인증
6. Duo 인증 프록시가 인증 응답을 수신합니다.
7. Cisco FMC GUI 액세스 권한이 부여됩니다.

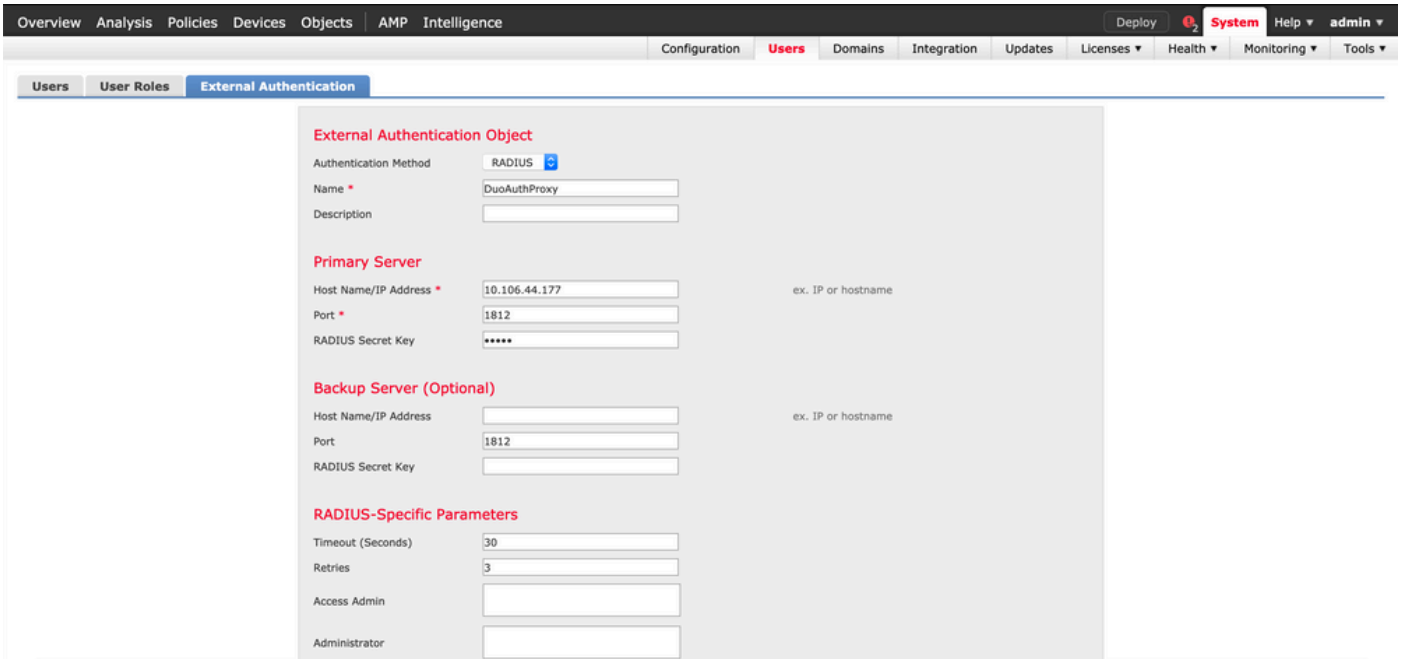
구성

컨피그레이션을 완료하려면 다음 섹션을 고려하십시오.

FMC의 컨피그레이션 단계

1단계. System(시스템) > Users(사용자) > External Authentication(외부 인증)으로 이동합니다. 외부 인증 객체를 생성하고 인증 방법을 RADIUS로 설정합니다. 이미지에 표시된 대로 Default User Role(기본 사용자 역할)에서 Administrator(관리자)가 선택되었는지 확인합니다.

 참고: 10.106.44.177은 Duo 인증 프록시 서버의 샘플 IP 주소입니다.



External Authentication Object

Authentication Method: RADIUS

Name: DuoAuthProxy

Description:

Primary Server

Host Name/IP Address: 10.106.44.177 (ex. IP or hostname)

Port: 1812

RADIUS Secret Key: *****

Backup Server (Optional)

Host Name/IP Address: (ex. IP or hostname)

Port: 1812

RADIUS Secret Key:

RADIUS-Specific Parameters

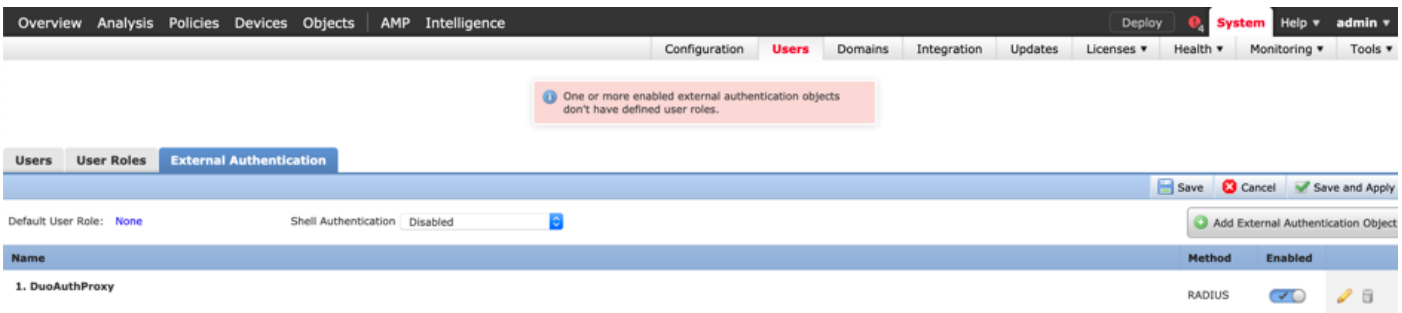
Timeout (Seconds): 30

Retries: 3

Access Admin:

Administrator:

Save and Apply를 클릭합니다. 그림과 같이 경고를 무시합니다.



One or more enabled external authentication objects don't have defined user roles.

Save Cancel Save and Apply

Default User Role: None Shell Authentication: Disabled

Add External Authentication Object

Name	Method	Enabled
1. DuoAuthProxy	RADIUS	<input checked="" type="checkbox"/>

2단계. System(시스템) > Users(사용자) > Users(사용자)로 이동합니다. 사용자를 생성하고 이미지에 표시된 대로 Authentication Method(인증 방법)를 External(외부)로 선택합니다.

User Configuration

User Name

Authentication



Use External Authentication Method

Options



Exempt from Browser Session Timeout

User Role Configuration

Default User Roles



Administrator



External Database User



Security Analyst



Security Analyst (Read Only)



Security Approver



Intrusion Admin



Access Admin



Network Admin



Maintenance User



Discovery Admin



Threat Intelligence Director (TID) User


Save

Cancel

1단계. Duo 인증 프록시 서버를 다운로드하고 설치합니다.


Windows 시스템에 로그인하고 [Duo 인증 프록시 서버](#) 설치

최소 1개의 CPU, 200MB의 디스크 공간 및 4GB RAM이 있는 시스템을 사용하는 것이 좋습니다

 참고: 이 시스템은 FMC, RADIUS 서버(여기서는 ISE) 및 듀오 클라우드(인터넷)에 액세스할 수 있어야 합니다.

2단계. authproxy.cfg 파일을 구성합니다.

Notepad++ 또는 WordPad와 같은 텍스트 편집기에서 이 파일을 엽니다.

 참고: 기본 위치는 C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg입니다.

authproxy.cfg 파일을 편집하고 이 구성을 추가합니다.

```
<#root>
```

```
[radius_client]
```

```
host=10.197.223.23          Sample IP Address of the ISE server
```

```
secret=cisco
```

Password configured on the ISE server in order to register the network device

FMC의 IP 주소는 RADIUS 비밀 키와 함께 구성되어야 합니다.

```
<#root>
```

```
[radius_server_auto]
```

```
ikey=xxxxxxxxxxxxxxxxxx
```

```
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

```
api_host=api-xxxxxxx.duosecurity.com
```

```
radius_ip_1=10.197.223.76
```

```
IP of FMC
```

```
radius_secret_1=cisco
```

Radius secret key used on the FMC

```
failmode=safe
```

```
client=radius_client
```

```
port=1812
```

```
api_timeout=
```

ikey, skey 및 api_host 매개변수를 구성해야 합니다. 이러한 값을 가져오려면 Duo 계정(Duo 관리자 로그인)에 로그인하고 Applications(애플리케이션) > Protect an Application(애플리케이션 보호)으로 이동합니다. 그런 다음 이미지에 표시된 대로 RADIUS 인증 애플리케이션을 선택합니다.

RADIUS

See the [RADIUS documentation](#) to integrate Duo into your RADIUS-enabled platform.

Details

Integration key	<input type="text" value="REDACTED"/>	select
Secret key	Click to view.	select
Don't write down your secret key or share it with anyone.		
API hostname	<input type="text" value="REDACTED"/>	select

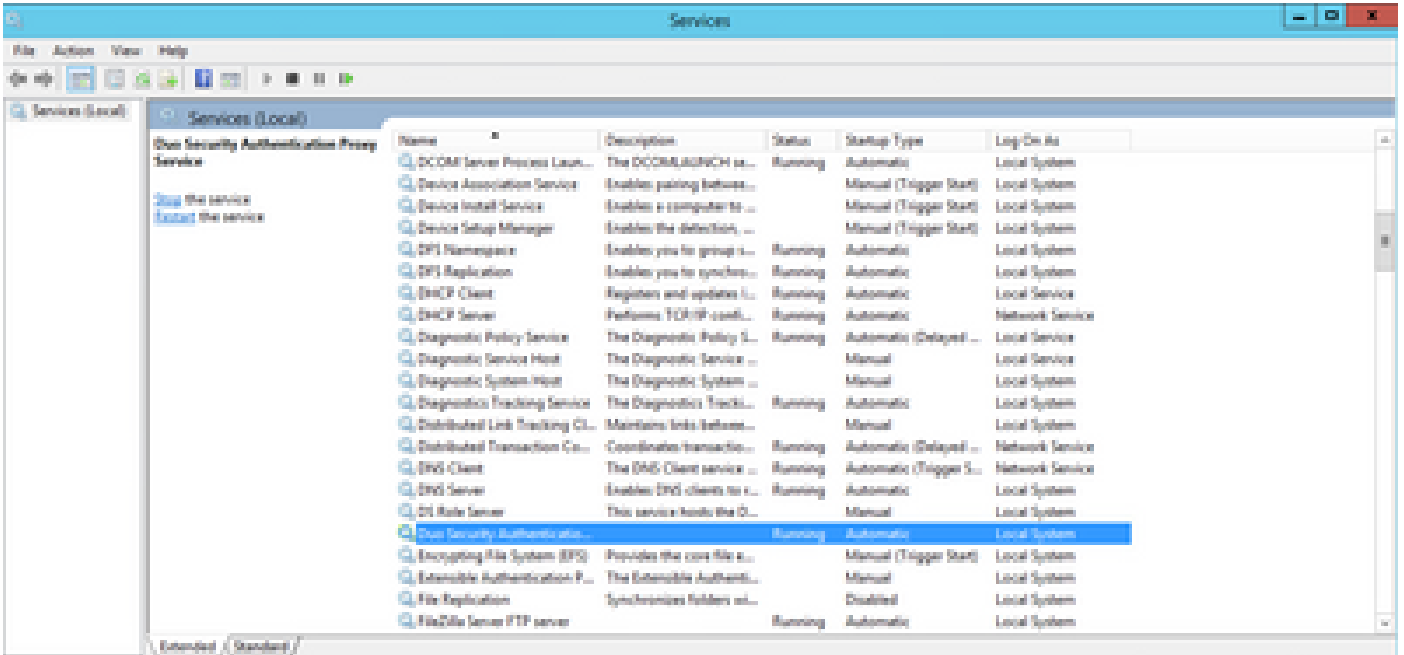
통합 키 = ikey

비밀 키 = skey

API 호스트 이름 = api_host


3단계. Duo Security Authentication Proxy 서비스를 다시 시작합니다. 파일을 저장하고 Windows 시스템에서 Duo 서비스를 다시 시작합니다.

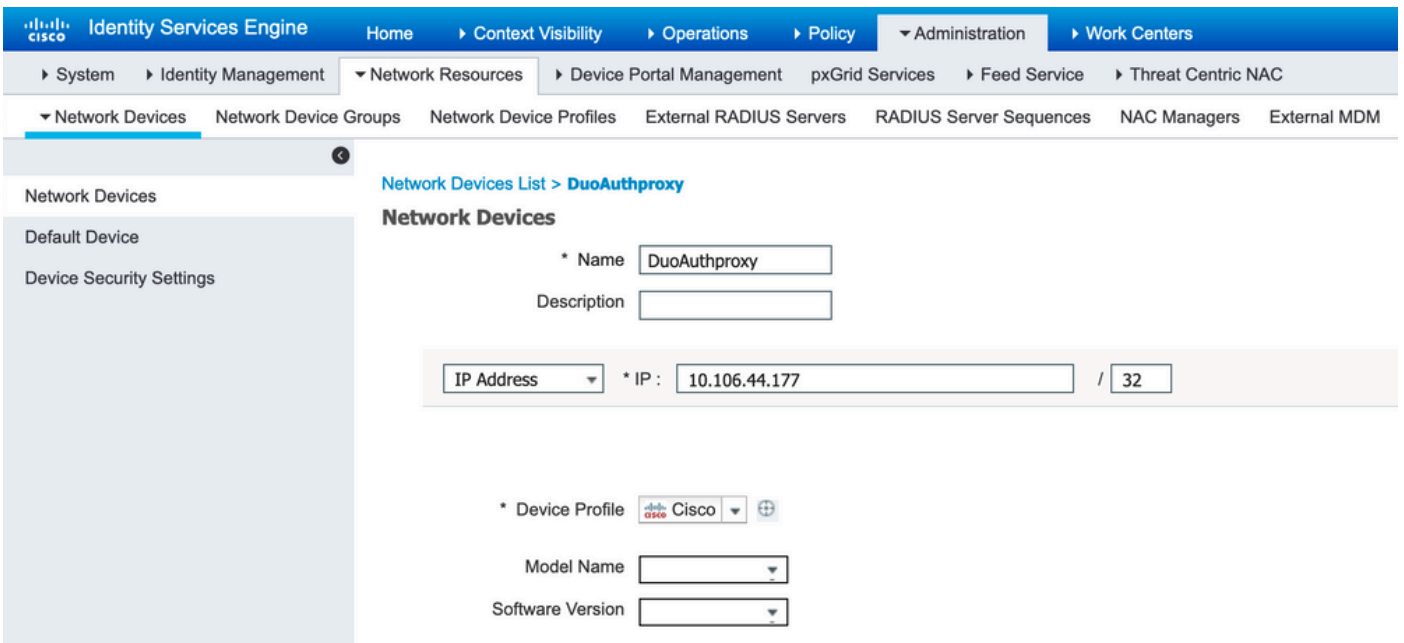
Windows 서비스 콘솔(services.msc)을 엽니다. 서비스 목록에서 Duo Security Authentication Proxy Service(Duo 보안 인증 프록시 서비스)를 찾고 이미지에 표시된 대로 Restart(재시작)를 클릭합니다.



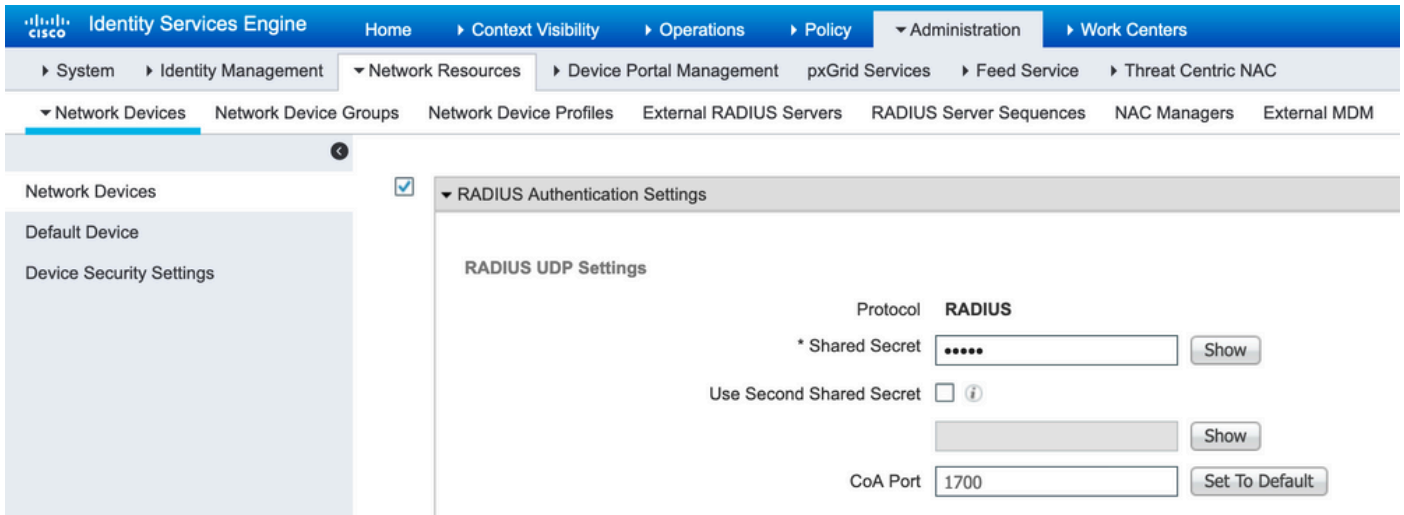
ISE의 컨피그레이션 단계

1단계. 이미지에 표시된 것처럼 네트워크 디바이스를 구성하려면 Administration(관리) > Network Devices(네트워크 디바이스)로 이동하고 Add(추가)를 클릭합니다.

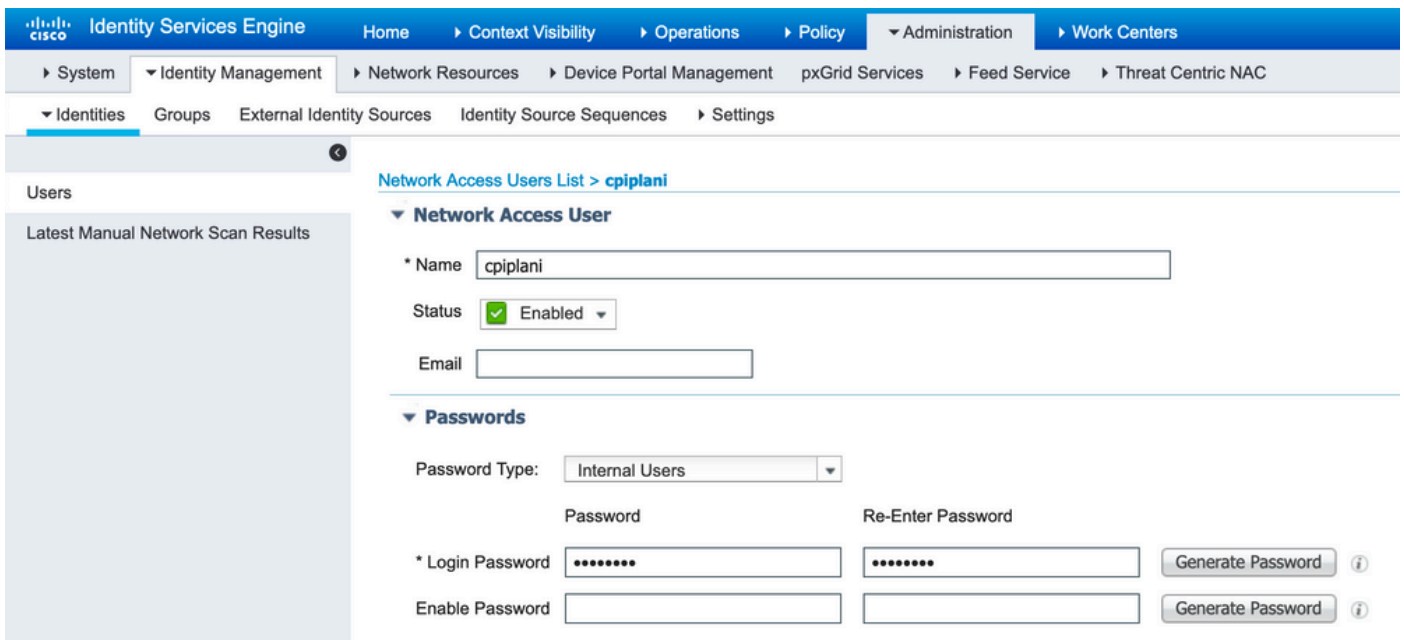
 참고: 10.106.44.177은 Duo 인증 프록시 서버의 샘플 IP 주소입니다.



authproxy.cfg에 설명된 대로 공유 암호를 이미지에 표시된 대로 암호로 구성합니다.



2단계. Administration(관리) > Identities(ID)로 이동합니다. 이미지에 표시된 대로 Identity 사용자를 구성하려면 Add를 클릭합니다.



Duo 관리 포털의 컨피그레이션 단계

1단계. 사용자 이름을 생성하고 엔드 디바이스에서 Duo Mobile을 활성화합니다.

Duo 클라우드 관리 웹 페이지에서 사용자를 추가합니다. 이미지에 표시된 대로 Users(사용자) > Add users(사용자 추가)로 이동합니다.


Dashboard > Users > Add User

Add User

Adding Users
Most applications allow users to enroll themselves after they complete primary authentication.
[Learn more about adding users](#)

Username:
Should match the primary authentication username.

[Add User](#)

 참고: 최종 사용자에게 Duo 앱이 설치되어 있는지 확인하십시오.

[iOS 디바이스용 Duo 애플리케이션 수동 설치](#)

[Android 디바이스용 Duo 애플리케이션 수동 설치](#)

2단계. 코드를 자동으로 생성합니다.

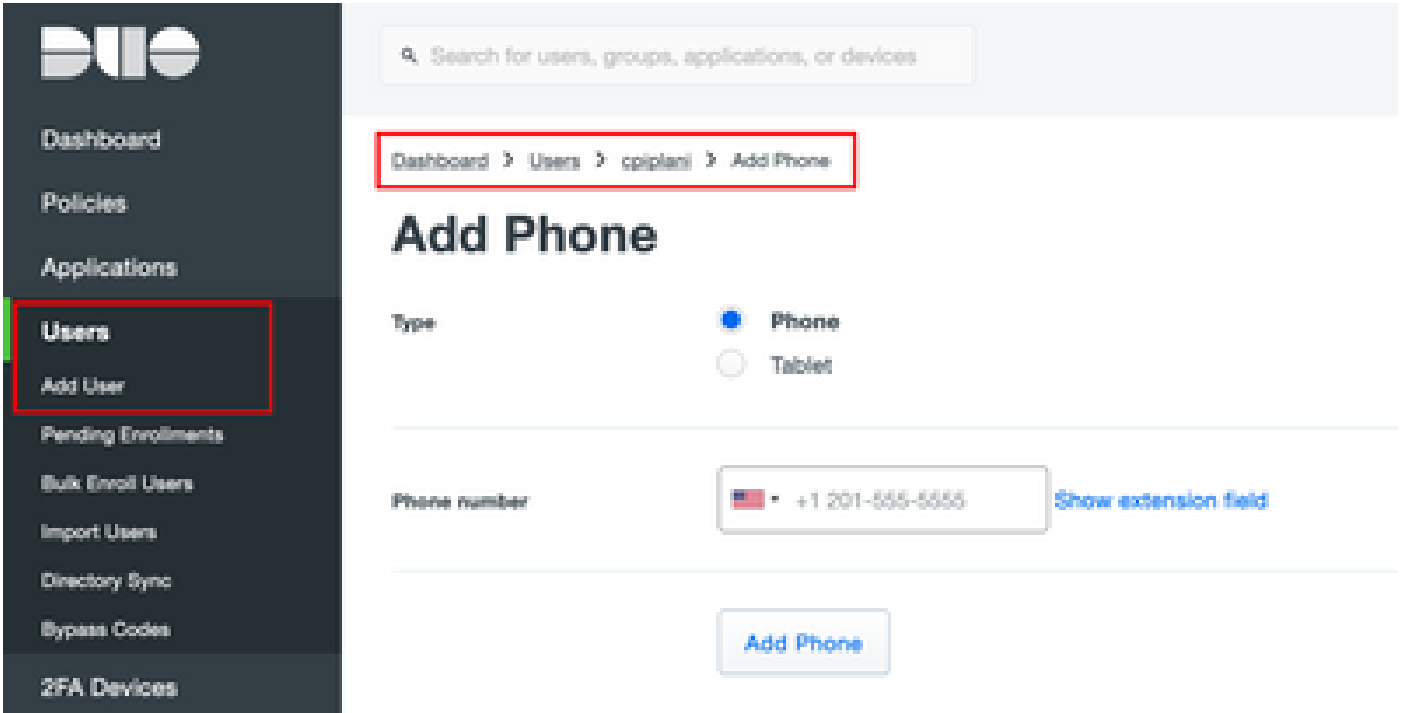
이미지에 표시된 대로 사용자의 전화 번호를 추가합니다.

Add one.' To the right of the heading is a blue 'Add Phone' button."/>

Phones
You may rearrange the phones by dragging and dropping in the table.

This user has no phones. [Add one.](#)

[Add Phone](#)



이미지에 표시된 대로 Activate Duo Mobile(듀오 모바일 활성화)을 선택합니다.

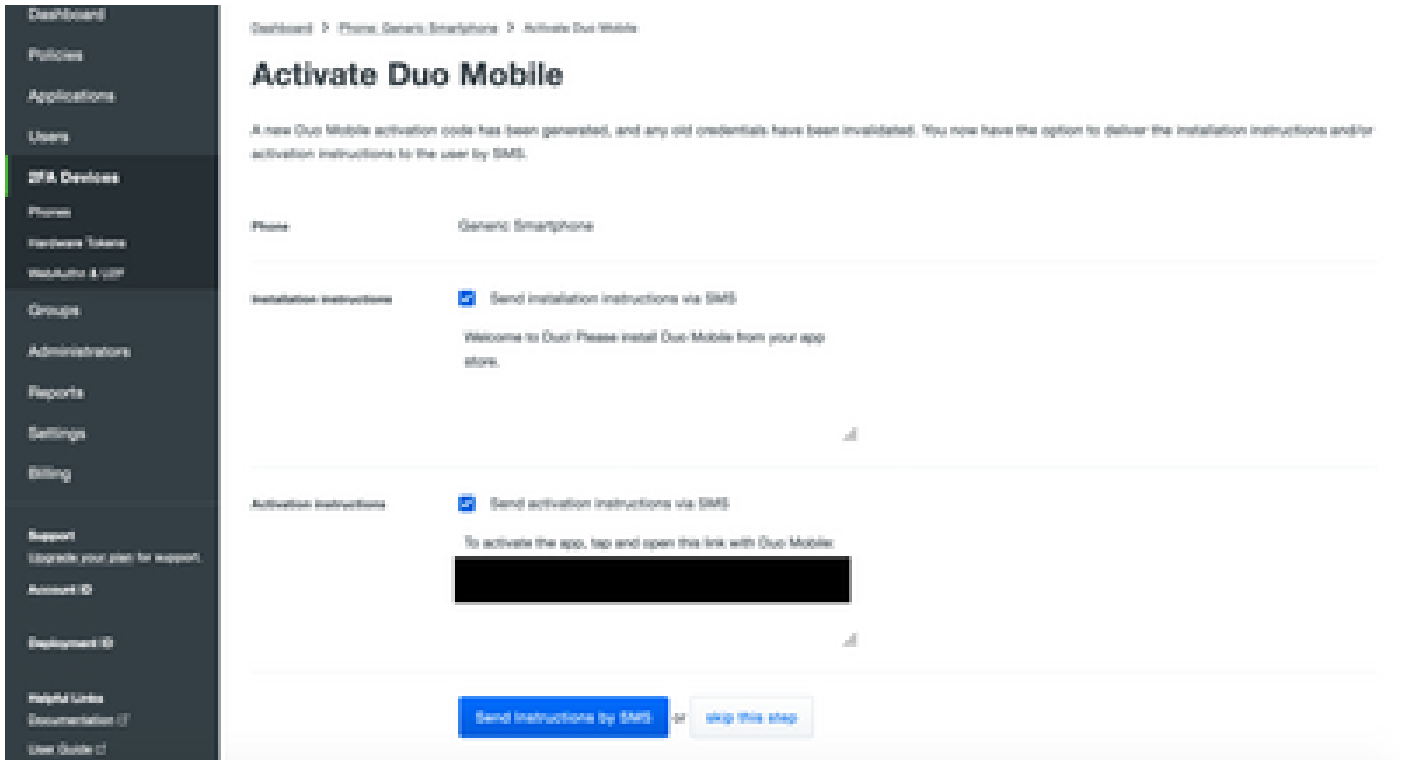
Device Info



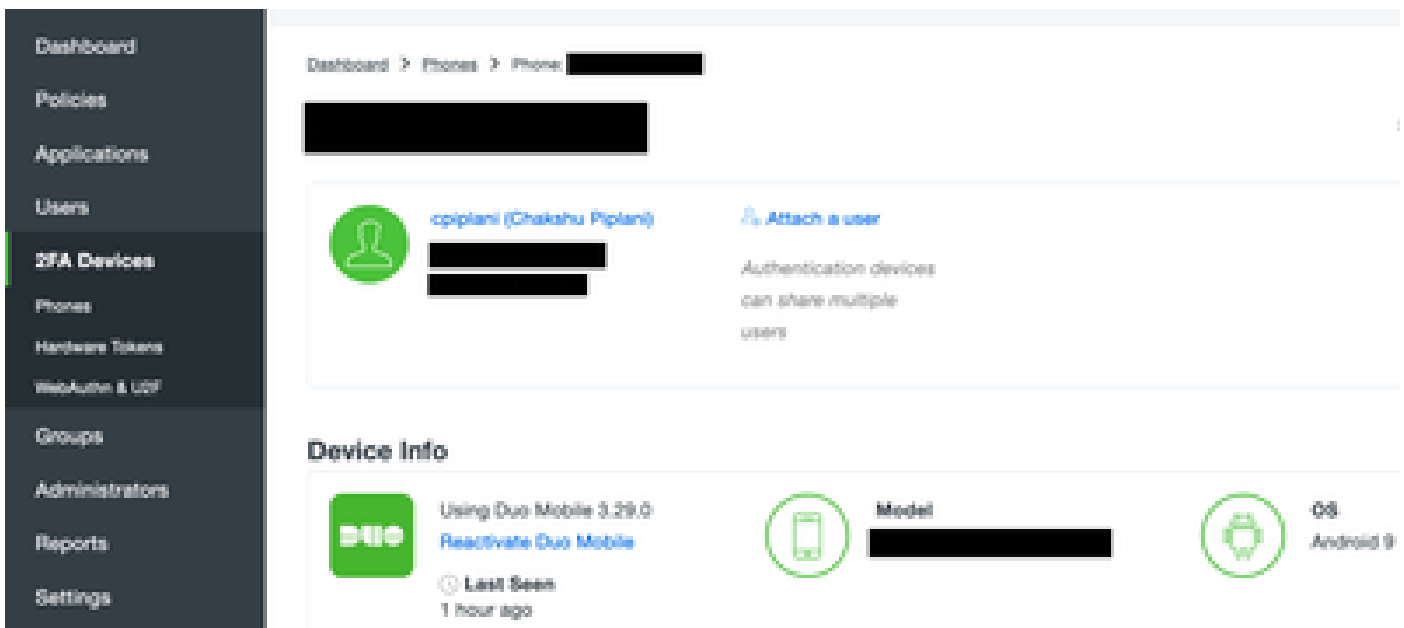
이미지에 표시된 대로 Generate Duo Mobile Activation Code(Duo Mobile 활성화 코드 생성)를 선택합니다.



이미지에 표시된 대로 Send Instructions by SMS(SMS로 지침 보내기)를 선택합니다.



이미지에 표시된 대로 SMS에서 링크를 클릭하면 Duo 앱이 Device Info(디바이스 정보) 섹션의 사용자 계정에 연결됩니다.



다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

ISE 사용자 ID 페이지에 추가된 사용자 자격 증명을 사용하여 FMC에 로그인합니다. Two Factor Authentication(2FA)을 위해 엔드포인트에서 Duo PUSH 알림을 받고 승인해야 하며, FMC는 이미지에 표시된 대로 로그인합니다.

Login Request



CISCO SYSTEMS



cpiplani



August 2, 2019, 7:37 PM



에서 인증에 사용되는 사용자 이름을 찾고 세부 정보 열에서 세부 정보 인증 보고서를 선택합니다. 여기에서 이미지에 표시된 대로 인증이 성공했는지 확인해야 합니다.

The screenshot displays the Cisco Identity Services Engine (ISE) interface. On the left, there are two main sections: 'Overview' and 'Authentication Details'. The 'Overview' section shows a successful authentication event for user 'cpiplani' with a '5200 Authentication succeeded' status. The 'Authentication Details' section provides further information, including the source and received timestamps (2019-07-11 03:50:38.694), the policy server (ROHAN-ISE), and the user type (User). On the right side, a 'Steps' section lists a series of log events with their corresponding IDs and descriptions, such as 'Received RADIUS Access-Request', 'RADIUS created a new session', and 'Authentication Passed'.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

- Duo Authentication Proxy Server(Duo 인증 프록시 서버)의 디버그를 확인합니다. 로그는 이 위치 아래에 있습니다.

C:\Program 파일(x86)\Duo 보안 인증 프록시\log

Notepad++ 또는 WordPad와 같은 텍스트 편집기에서 authproxy.log 파일을 엽니다.

잘못된 자격 증명이 입력되고 ISE 서버에서 인증이 거부될 경우 스니펫을 기록합니다.

<#root>

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Sending request from
```

```
10.197.223.76
```

```
to radius_server_auto
```

```
10.197.223.76 is the IP of the FMC
```

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Received new request id 4 from ('10.197.223.76', 3452)
```

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] (('10.197.223.76', 34524), 4):
```

```
login attempt for username u'cpiplani'
```

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.76', 34524)
```

```
2019-08-04T18:54:17+0530 [RadiusClient (UDP)]
```

```
Got response
```

for id 199 from ('

10.197.223.23

', 1812);

code 3 10.197.223.23 is the IP of the ISE Server.

2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4): Primary credentials reject

2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4):

Returning response code 3: AccessReject

2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4): Sending response

- ISE에서 Operations(운영) > RADIUS > Live Logs(라이브 로그)로 이동하여 인증 세부사항을 확인합니다.

ISE 및 Duo를 사용한 성공적인 인증의 조각 기록:

<#root>

2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Sending request from

10.197.223.76

to radius_server_auto

2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Received new request id 5 from ('10.197.223.76', 34095)

2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] (('10.197.223.76', 34095), 5): login attempt for user

2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.

2019-08-04T18:56:16+0530 [RadiusClient (UDP)] Got response for id 137 from ('

10.197.223.23

', 1812);

code 2 <<<< At this point we have got successful authentication from ISE Server.

2019-08-04T18:56:16+0530 [RadiusClient (UDP)] http POST to https://api-f754c261.duosecurity.com:443/res

2019-08-04T18:56:16+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPC

2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):

2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] Invalid ip. Ip was None

2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] http POST to https://api-f754c2

2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPC

2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPC

2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):

Duo authentication returned 'allow': 'Success. Logging you in...

2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):

Returning response code 2: AccessAccept <<<< At this point, user has hit the approve button

2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):

2019-08-04T18:56:30+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPC

관련 정보

- [Duo를 사용하는 RA VPN 인증](#)
- [기술 지원 및 문서 - Cisco Systems](#)

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.