

Anyconnect/원격 액세스 VPN 클라이언트에서 2단계 인증을 위해 Active Directory 및 ISE와 Duo 통합 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[네트워크 다이어그램 및 시나리오](#)

[통신 과정](#)

[Active Directory 구성](#)

[Duo 구성](#)

[Duo 인증 프록시 컨피그레이션](#)

[Cisco ISE 컨피그레이션](#)

[Cisco ASA RADIUS/ISE 컨피그레이션](#)

[Cisco ASA Remote Access VPN 구성](#)

[테스트](#)

[문제 해결](#)

[작업 디버그](#)

소개

이 문서에서는 ASA에 연결된 AnyConnect 클라이언트에 대한 2단계 인증으로서 AD 및 ISE와의 Duo Push 통합에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA의 RA VPN 컨피그레이션
- ASA의 RADIUS 컨피그레이션
- ISE
- 액티브 디렉토리
- Duo 애플리케이션

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

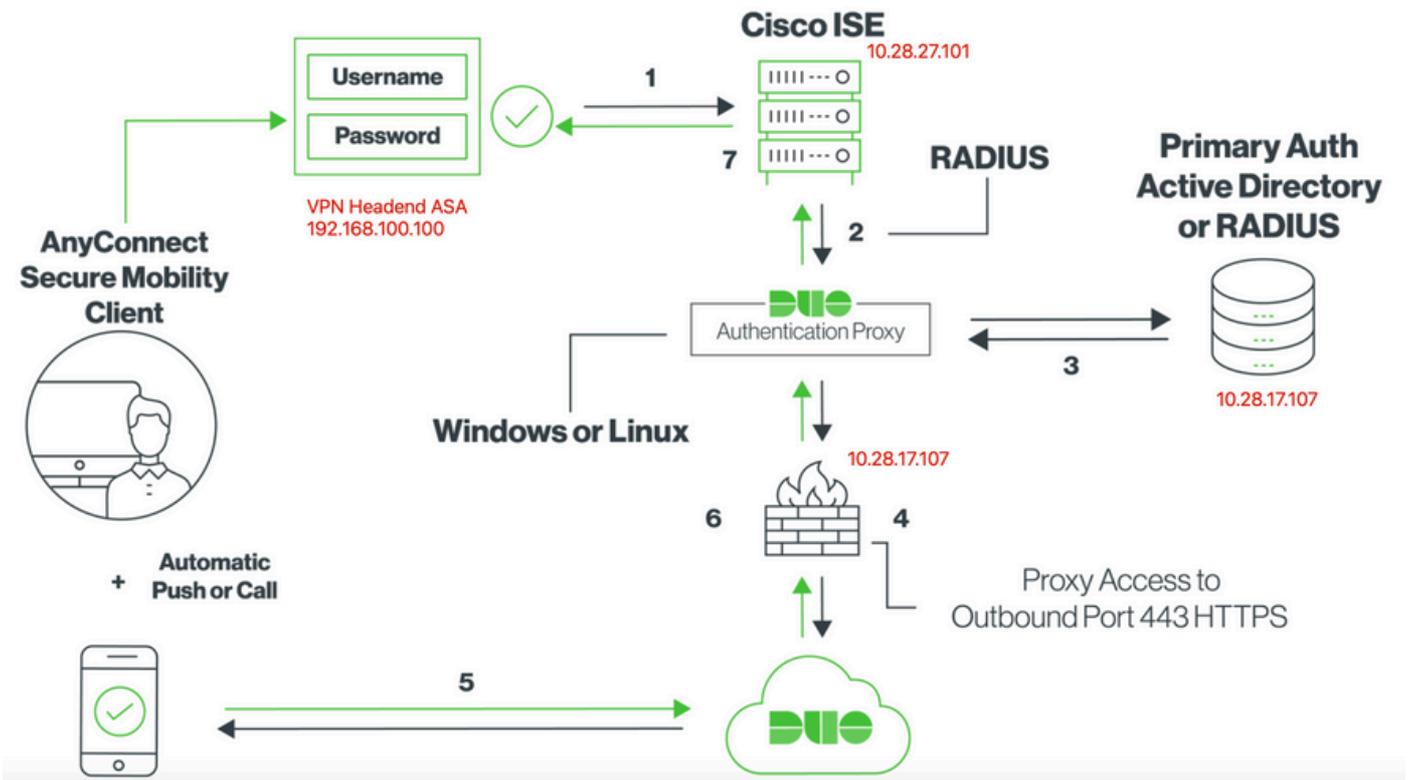
- Microsoft 2016 서버
- ASA 9.14(3)18
- ISE Server 3.0
- Duo 서버
- Duo 인증 프록시 관리자

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 Cisco ASA(Adaptive Security Appliance)에 연결하는 AnyConnect 클라이언트에 대해 AD(Active Directory) 및 Cisco ISE(Identity Service Engine)와의 Duo Push 통합을 2단계 인증으로 구성하는 방법에 대해 설명합니다.

네트워크 다이어그램 및 시나리오



통신 과정

<https://duo.com/docs/ciscoise-radius>

1. Cisco ISE에 대한 기본 인증 시작
2. Cisco ASA가 Duo 인증 프록시에 인증 요청 전송
3. 기본 인증에서는 Active Directory 또는 RADIUS를 사용합니다.
4. Duo 인증 프록시 연결이 TCP 포트 443을 통해 Duo 보안에 설정됨

5. Duo Security 서비스를 통한 2차 인증
6. Duo 인증 프록시가 인증 응답을 수신함
7. Cisco ISE 액세스 권한 부여됨

사용자 계정:

- Active Directory Admin(Active Directory 관리자): 이 옵션은 Duo 인증 프록시가 기본 인증을 위해 Active Directory 서버에 바인딩할 수 있도록 디렉토리 계정으로 사용됩니다.
- Active Directory 테스트 사용자
- Duo 보조 인증을 위한 테스트 사용자

Active Directory 구성

Windows 서버가 Active Directory 도메인 서비스와 함께 미리 구성되어 있습니다.

 참고:RADIUS 듀오 인증 프록시 관리자가 동일한 Active Directory 호스트 시스템에서 실행되는 경우 NPS(네트워크 정책 서버) 역할을 제거/삭제해야 합니다. 두 RADIUS 서비스가 모두 실행되는 경우 충돌하여 성능에 영향을 줄 수 있습니다.

원격 액세스 VPN 사용자의 인증 및 사용자 ID에 대한 AD 컨피그레이션을 수행하려면 몇 가지 값이 필요합니다.

ASA 및 Duo 인증 프록시 서버에서 컨피그레이션을 수행하려면 먼저 Microsoft 서버에서 이러한 모든 세부 정보를 만들거나 수집해야 합니다.

주요 값은 다음과 같습니다.

- 도메인 이름. 서버의 도메인 이름입니다. 이 컨피그레이션 가이드에서는 agarciam.cisco가 도메인 이름입니다.
- 서버 IP/FQDN 주소입니다. Microsoft 서버에 연결하는 데 사용되는 IP 주소 또는 FQDN. FQDN을 사용하는 경우 FQDN을 확인하려면 ASA 및 Duo 인증 프록시 내에서 DNS 서버를 구성해야 합니다.

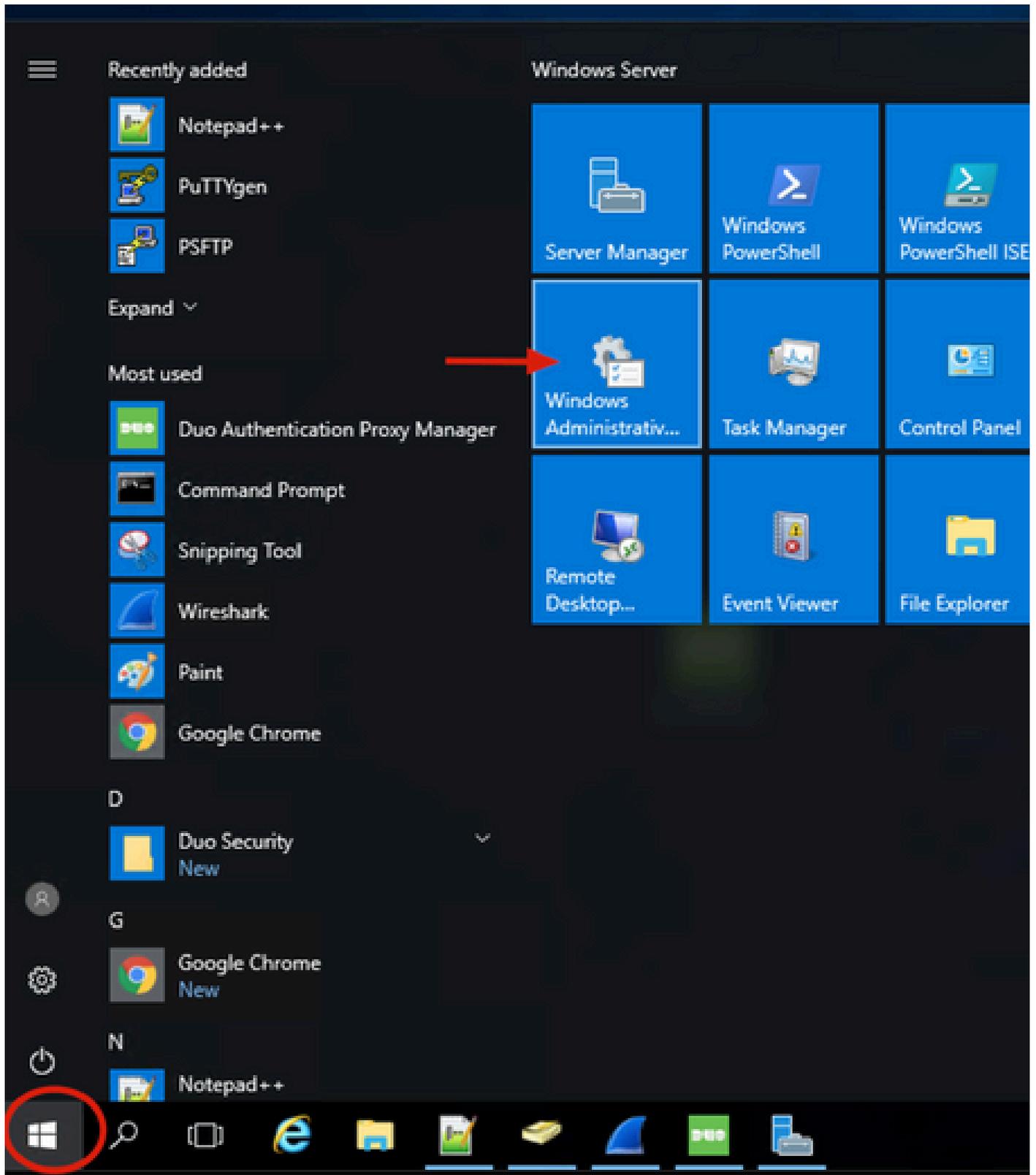
이 컨피그레이션 가이드에서 이 값은 agarciam.cisco(10.28.17.107로 확인됨)입니다.

- 서버 포트. LDAP 서비스에서 사용하는 포트. 기본적으로 LDAP 및 STARTTLS는 LDAP에 TCP 포트 389를 사용하고 LDAP over SSL(LDAPS)은 TCP 포트 636을 사용합니다.
- 루트 CA. LDAPS 또는 STARTTLS를 사용하는 경우 LDAPS에서 사용하는 SSL 인증서에 서명하는 데 사용되는 루트 CA가 필요합니다.
- 디렉토리 사용자 이름 및 비밀번호. Duo Auth 프록시 서버에서 LDAP 서버에 바인딩하고 사용자를 인증하며 사용자 및 그룹을 검색하는 데 사용되는 계정입니다.
- 기본 및 그룹 DN(고유 이름)입니다. Base DN은 Duo Auth 프록시의 출발점이며 Active Directory에 사용자 검색 및 인증을 시작하도록 지시합니다.

이 컨피그레이션 가이드에서 루트 도메인 agarciam.cisco는 기본 DN으로 사용되며 그룹 DN은

Duo-USERS입니다.

1. 새 Duo 사용자를 추가하려면 Windows Server에서 왼쪽 하단의 Windows 아이콘으로 이동하여 이미지에 표시된 대로 Windows 관리 도구를 클릭합니다.

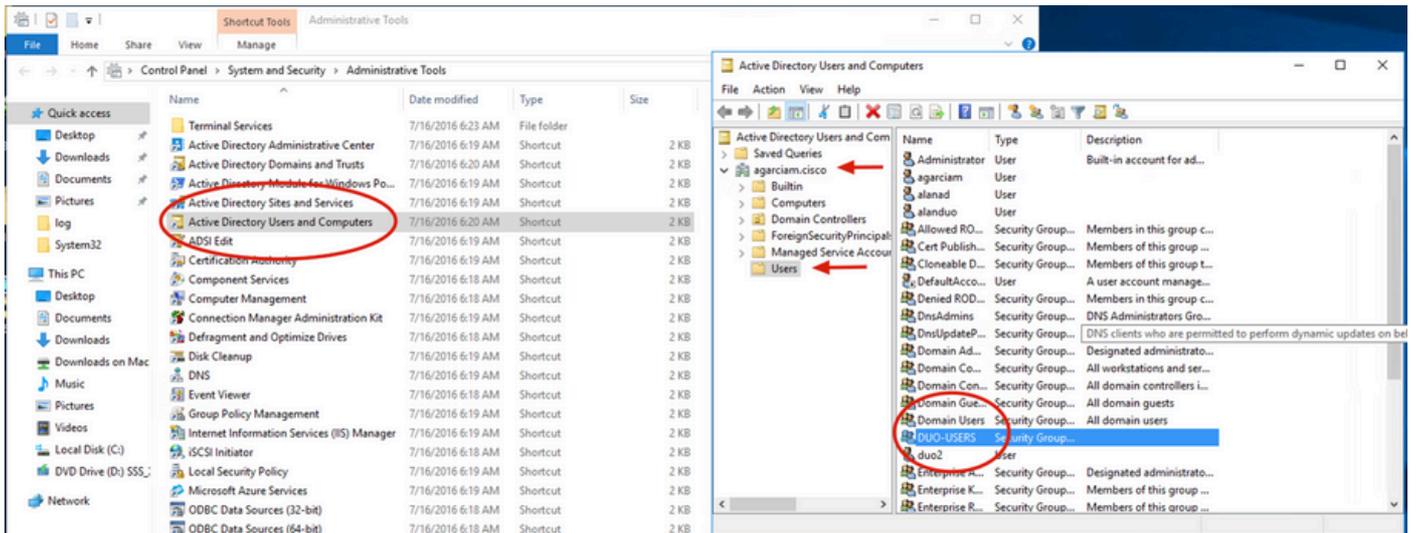


2. Windows 관리 도구 창에서 Active Directory 사용자 및 컴퓨터로 이동합니다.

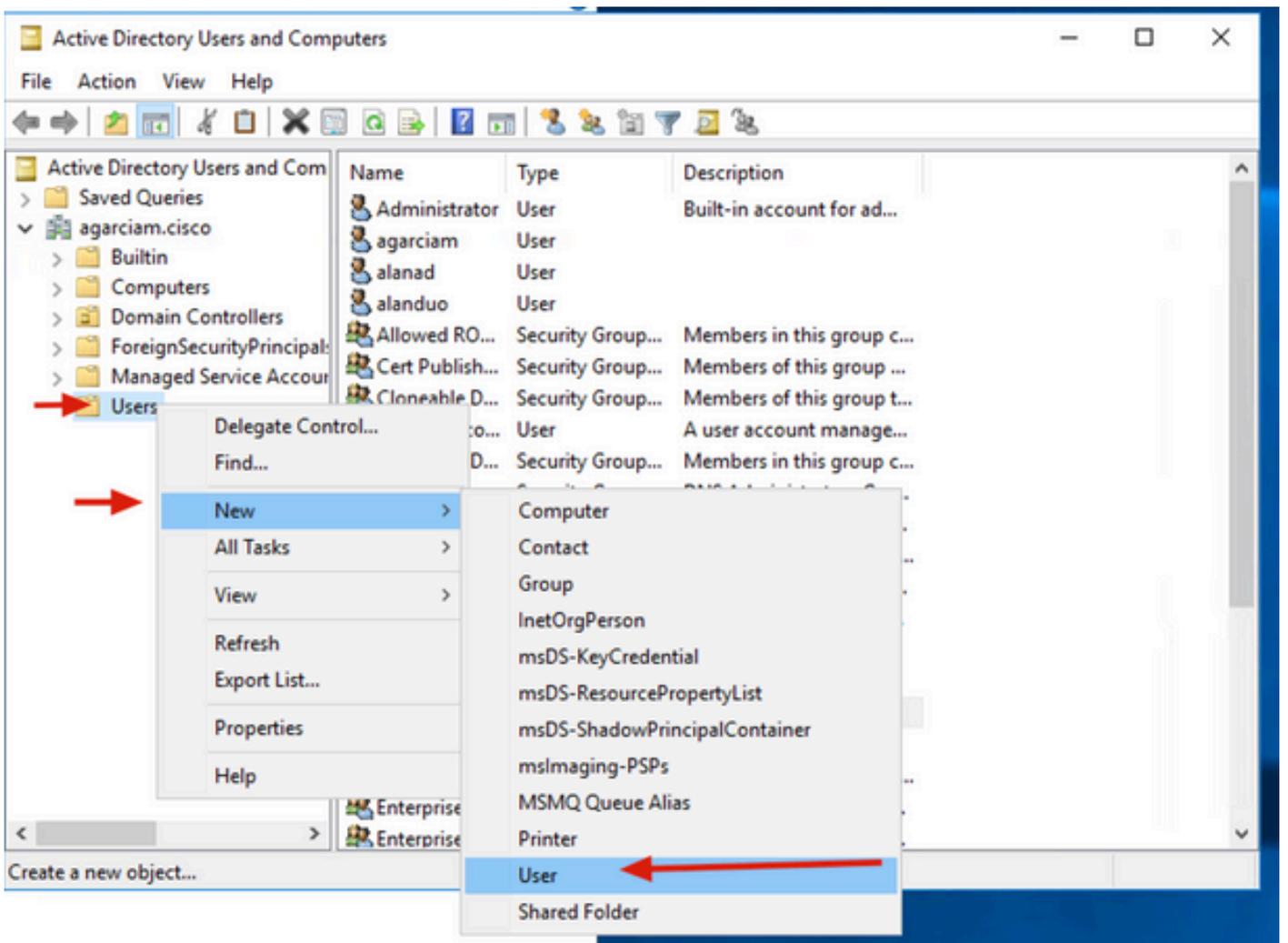
Active Directory Users and Computers(Active Directory 사용자 및 컴퓨터) 패널에서 domain(도메

인) 옵션을 확장하고 Users(사용자) 폴더로 이동합니다.

이 컨피그레이션에서는 Duo-USERS가 보조 인증을 위한 대상 그룹으로 사용됩니다.



3. 이미지에 표시된 대로 사용자 폴더를 마우스 오른쪽 버튼으로 클릭하고 신규 > 사용자를 선택합니다.



4. 새 객체 사용자 창에서 이 새 사용자에게 대한 ID 속성을 지정하고 이미지에 표시된 대로 다음을 클

릭합니다.

New Object - User

Create in: agarciam.cisco/Users

First name: duovpn Initials:

Last name:

Full name: duovpn

User logon name: duovpn @agarciam.cisco

User logon name (pre-Windows 2000): AGARCIAM\ duovpn

< Back Next > Cancel

5. 비밀번호를 확인하고 다음, 사용자 정보가 확인되면 마침을 클릭합니다.

New Object - User X

 Create in: agarciam.cisco/Users

Password: ←

Confirm password: ←

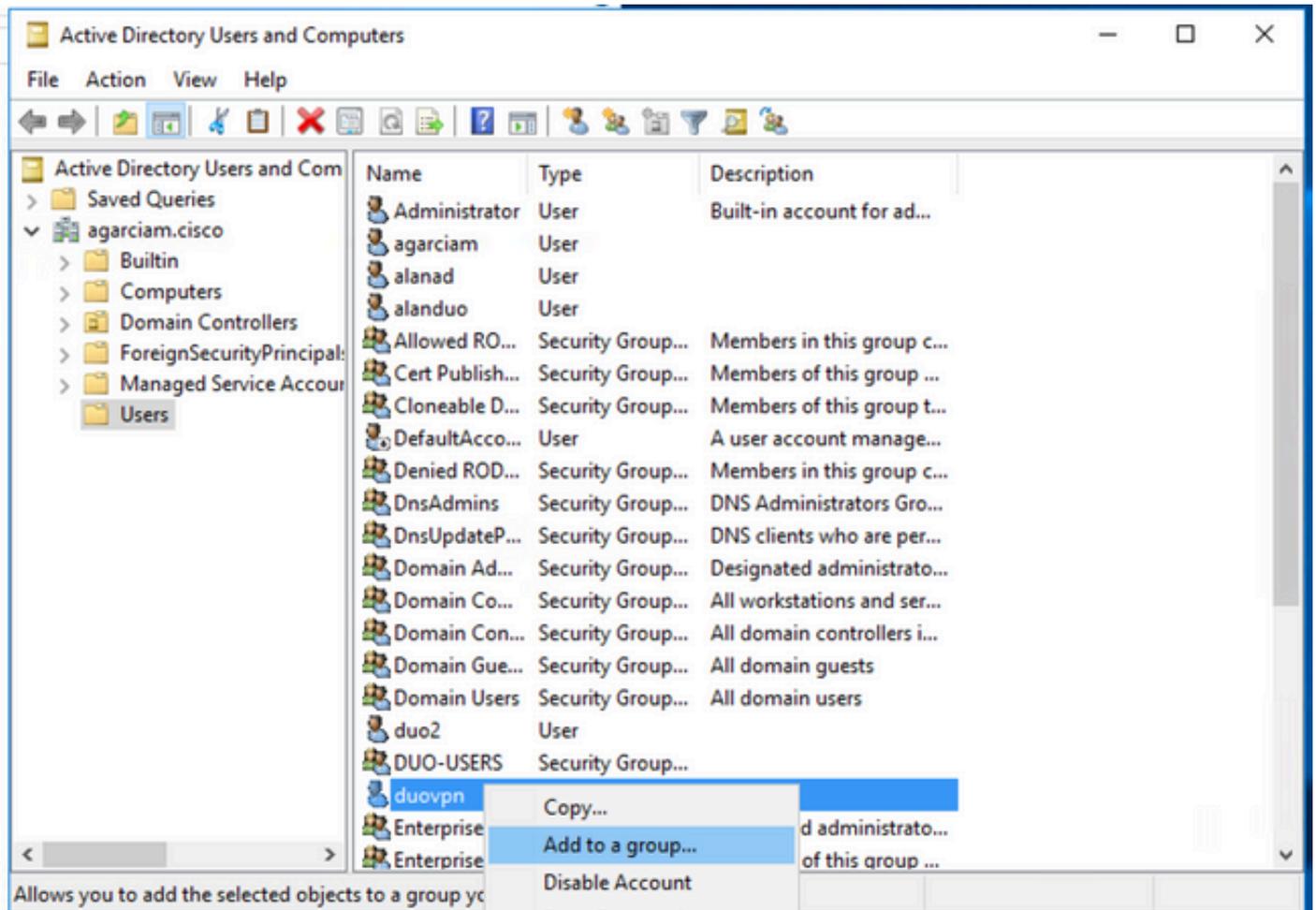
User must change password at next logon

User cannot change password

Password never expires

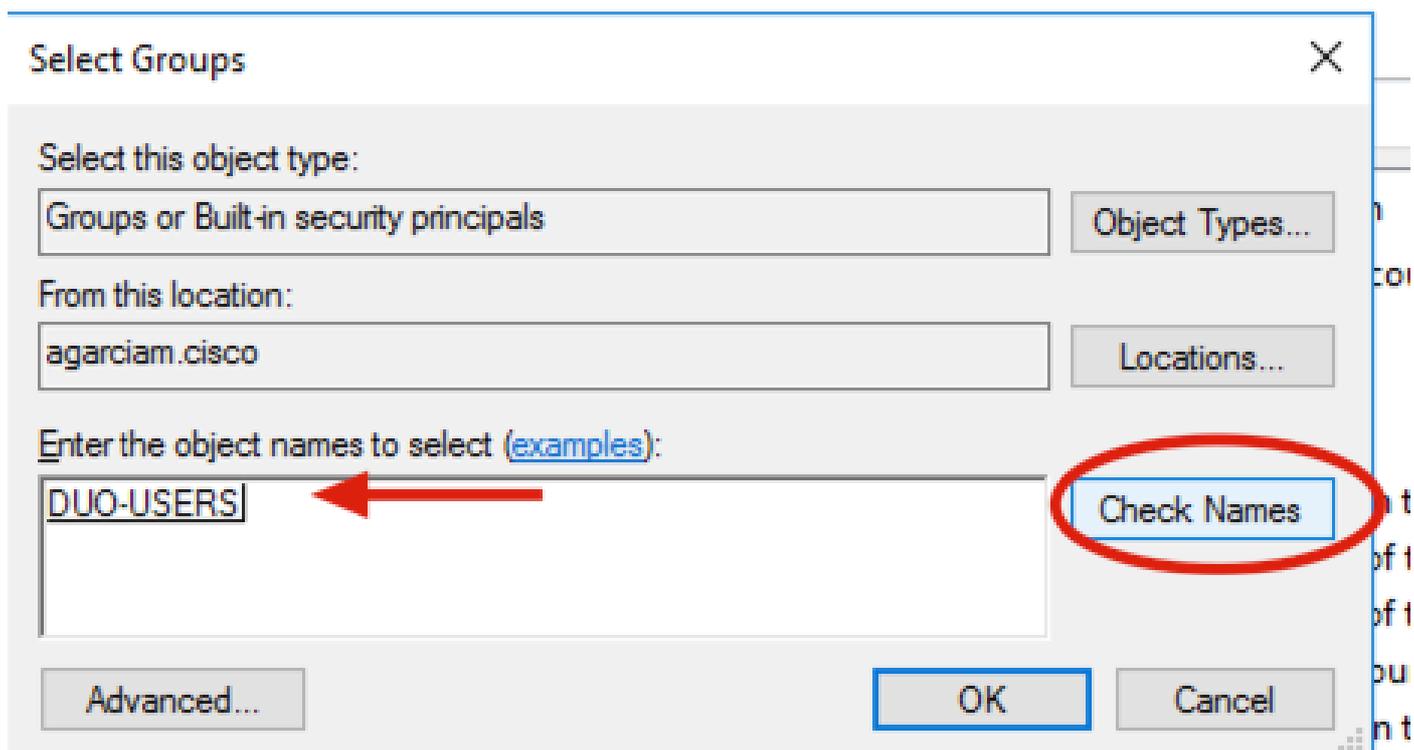
Account is disabled

6. 이미지에 표시된 대로 특정 그룹에 새 사용자를 지정하고 마우스 오른쪽 단추로 누른 다음 그룹에 추가를 선택합니다.



7. [그룹 선택] 패널에서 원하는 그룹의 이름을 입력하고 이름 확인을 클릭합니다.

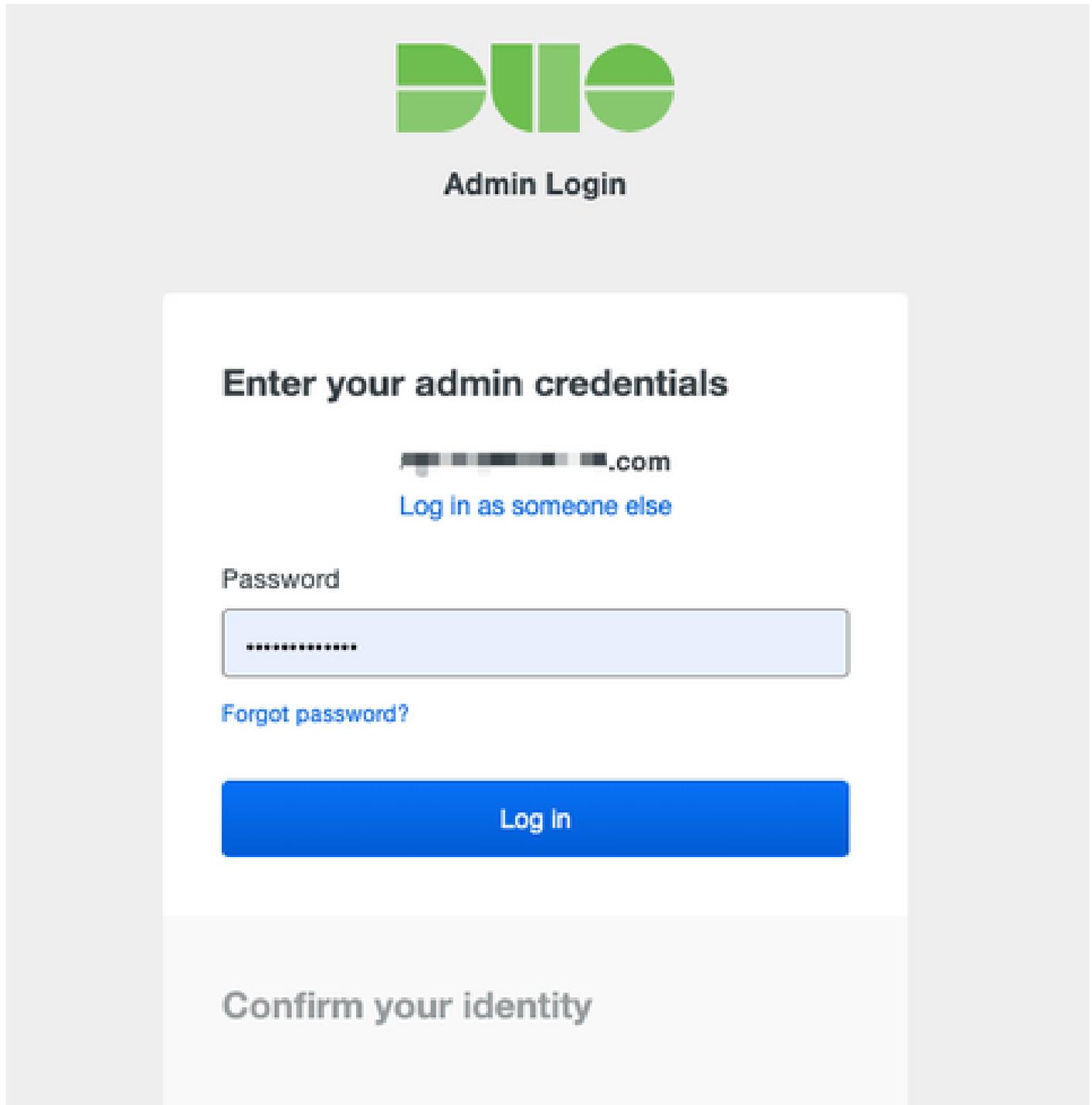
그런 다음 기준과 일치하는 이름을 선택하고 확인을 클릭합니다.



8. 이 문서에서 예로 사용되는 사용자입니다.

Duo 구성

1. Dudo 관리 포털에 로그인합니다.



Duo

Admin Login

Enter your admin credentials

██████████.com

[Log in as someone else](#)

Password

.....

[Forgot password?](#)

Log In

Confirm your identity

2. 왼쪽 패널에서 Users(사용자)로 이동하고 Add User(사용자 추가)를 클릭한 다음 Active Domain 사용자 이름과 일치하는 사용자 이름을 입력하고 Add User(사용자 추가)를 클릭합니다.

DUO

Search for users, groups, applications, or devices

Dashboard > Users > Add User

Add User

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

3. 새 사용자 패널에서 필요한 모든 정보를 빈 칸에 입력합니다.

duovpn

i This user has not enrolled yet. See our [enrollment documentation](#) to learn more about enrolling users.

Username

Username aliases [+ Add a username alias](#)
 Users can have up to 8 aliases. Optionally, you may choose to reserve using an alias number for a specific alias (e.g., Username alias 1 should only be used for Employee ID).

Full name

Email

Status **Active** ←
 Require multi-factor authentication (default).
 Bypass
 Allow users to skip two-factor authentication and log in with only a password. Passwordless authentication is not skipped.
 Disabled
 Automatically deny access
 This controls the user's two-factor authentication process.

Groups You don't have any editable groups. [Add one.](#)
 Groups can be used for management, reporting, and policy. [Learn more about groups](#)

Notes
 For internal use.

4. 사용자 장치에서 보조 인증 방법을 지정합니다.

참고: 이 문서에서는 Duo push for mobile devices 방법을 사용하므로 전화 장치를 추가해야 합니다.

Add Phone(전화기 추가)을 클릭합니다.

Phones

You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#) ↗.

Add Phone

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

Endpoints

This user has no devices.

Hardware Tokens

Add Hardware Token

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

Bypass Codes

Add Bypass Code

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

WebAuthn & U2F

Add Security Key

5. 사용자 전화 번호를 입력하고 전화 추가를 클릭합니다.

Add Phone



[Learn more about Activating Duo Mobile](#)

Type

- Phone
 Tablet

Phone number



[Show extension field](#)

Optional. Example: "+52 1 222 123 4567"



6. 왼쪽 Duo Admin(듀오 관리자) 패널에서 Users(사용자)로 이동하여 새 사용자를 클릭합니다.

Dashboard > Users

Users

Directory Sync | Import Users | Bulk Enroll Users [Add User](#)

5 Total Users **0** Not Enrolled **2** Inactive Users **1** Trash **0** Bypass Users **0** Locked Out

Select (0) [...](#) [Export](#) Search

Username	Name	Email	Phones	Tokens	Status	Last Login
<input type="checkbox"/>			1		Active	Mar 8, 2022 6:50 PM
<input type="checkbox"/>			1		Active	Mar 5, 2022 7:04 PM
<input type="checkbox"/>			1		Active	Never authenticated
<input type="checkbox"/> duovpn		...@... .com	1		Active	Never authenticated
<input type="checkbox"/>		...@... o.com	1		Active	Mar 5, 2022 7:16 PM

참고: 현재 전화기에 액세스할 수 없는 경우 이메일 옵션을 선택할 수 있습니다.

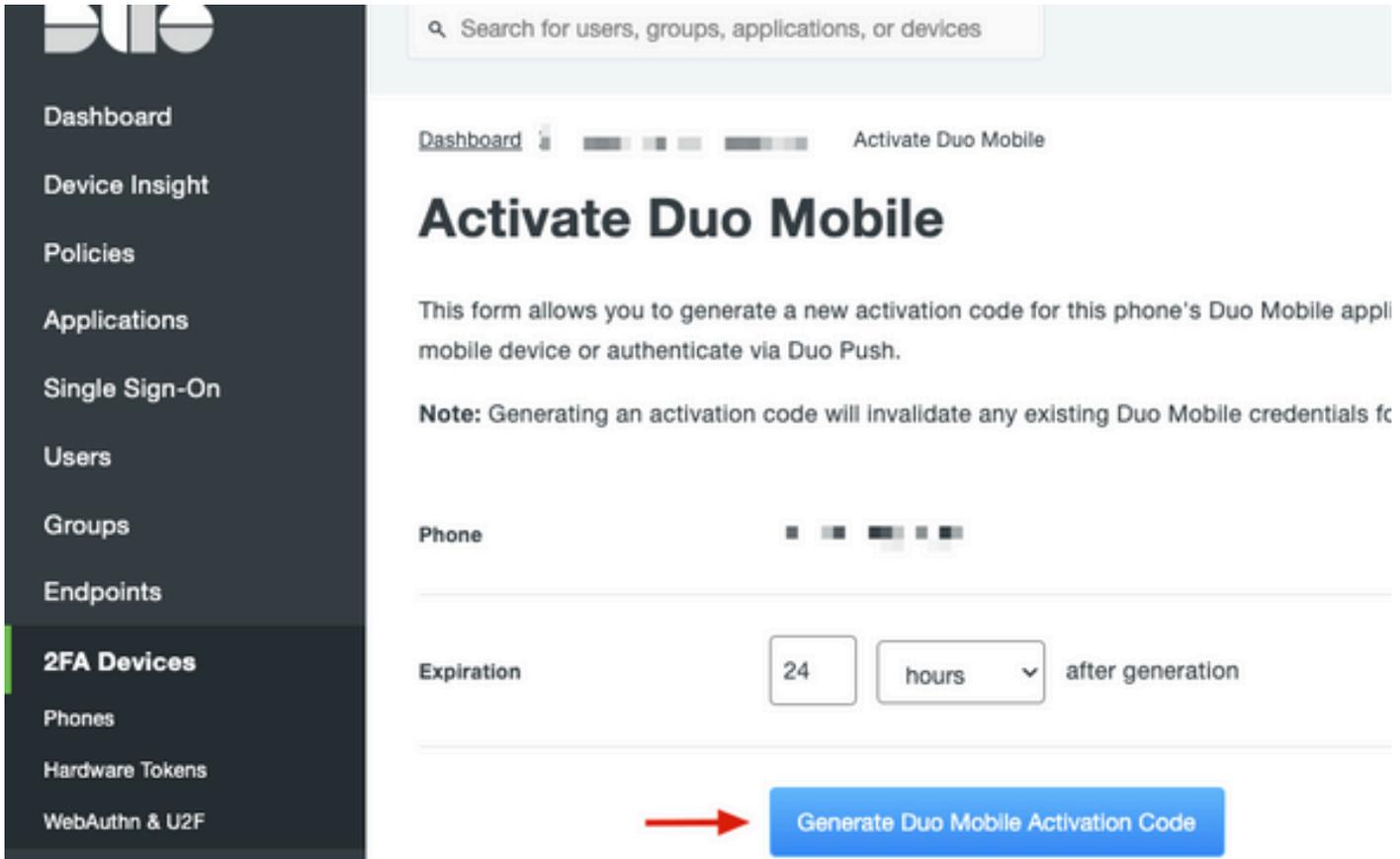
7. Phones(전화기) 섹션으로 이동하고 Activate Duo Mobile(Duo Mobile 활성화)을 클릭합니다.

Phones

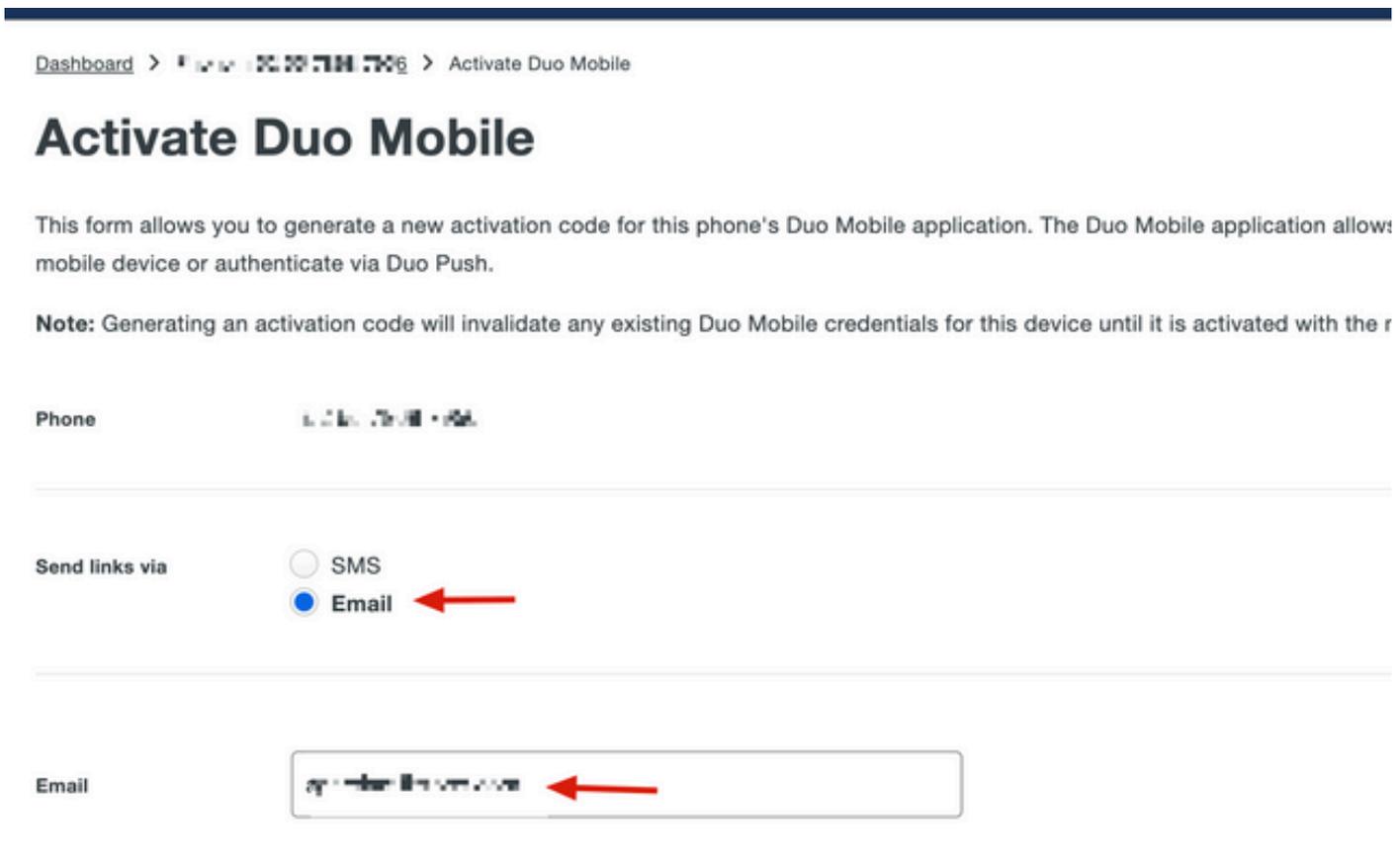
You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#) [...](#) [Add Phone](#)

Alias	Device	Platform	Model	Security Warnings	
phone1		Android 10		✓ No warnings	Activate Duo Mobile

8. Generate Duo Mobile Activation Code(Duo Mobile 활성화 코드 생성)를 클릭합니다.



9. 전자메일을 통해 지시사항을 수신하려면 전자메일을 선택하고 전자메일 주소를 입력한 후 전자메일로 지시사항 발송을 클릭합니다.



10. 이미지에 표시된 대로 지침이 포함된 이메일을 수신합니다.

This is an automated email from Duo Security.

Your organization invites you to set up Duo Mobile on your phone. You will find instructions from your Duo administrator below. If you have questions, please reach out to your organization's IT or help desk team.

This email will help you add your Cisco account to Duo Mobile on this device:



Just tap this link from + [redacted] or copy and paste it into Duo Mobile manually:



If you're not reading this from + [redacted] Duo Mobile on your phone and scan this barcode:



Don't have Duo Mobile yet? Install it first:

iPhone: <https://itunes.apple.com/us/app/duo-mobile/id422663827>

Android: <https://play.google.com/store/apps/details?id=com.duosecurity.duomobile>

11. 모바일 장치에서 Duo Mobile App을 열고 [추가]를 클릭한 다음 [QR 코드 사용]을 선택하고 지침 전자 메일에서 코드를 스캔합니다.

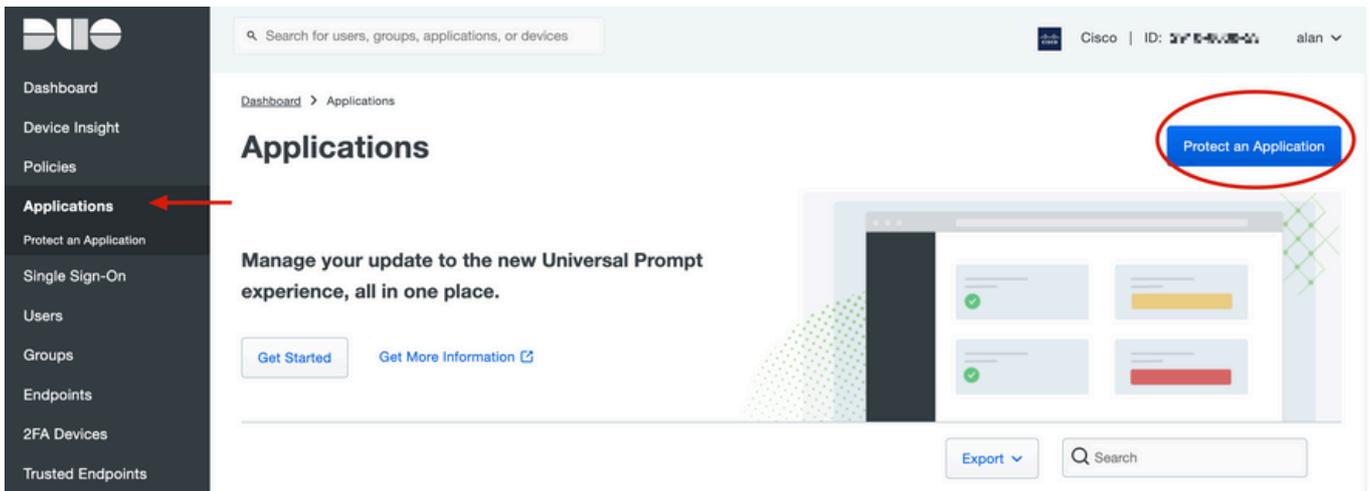
12. Duo Mobile App에 새 사용자가 추가되었습니다.

Duo 인증 프록시 컨피그레이션

1. <https://duo.com/docs/authproxy-reference>에서 Duo Auth Proxy Manager를 다운로드하여 [설치합니다.](#)

 참고: 이 문서에서는 Duo Auth Proxy Manager가 Active Directory 서비스를 호스트하는 Windows Server에 설치됩니다.

2. Duo Admin(듀오 관리) 패널에서 Applications(애플리케이션)로 이동하고 Protect an Application(애플리케이션 보호)을 클릭합니다.



3. 검색 표시줄에서 Cisco ISE Radius를 찾습니다.

Protect an Application

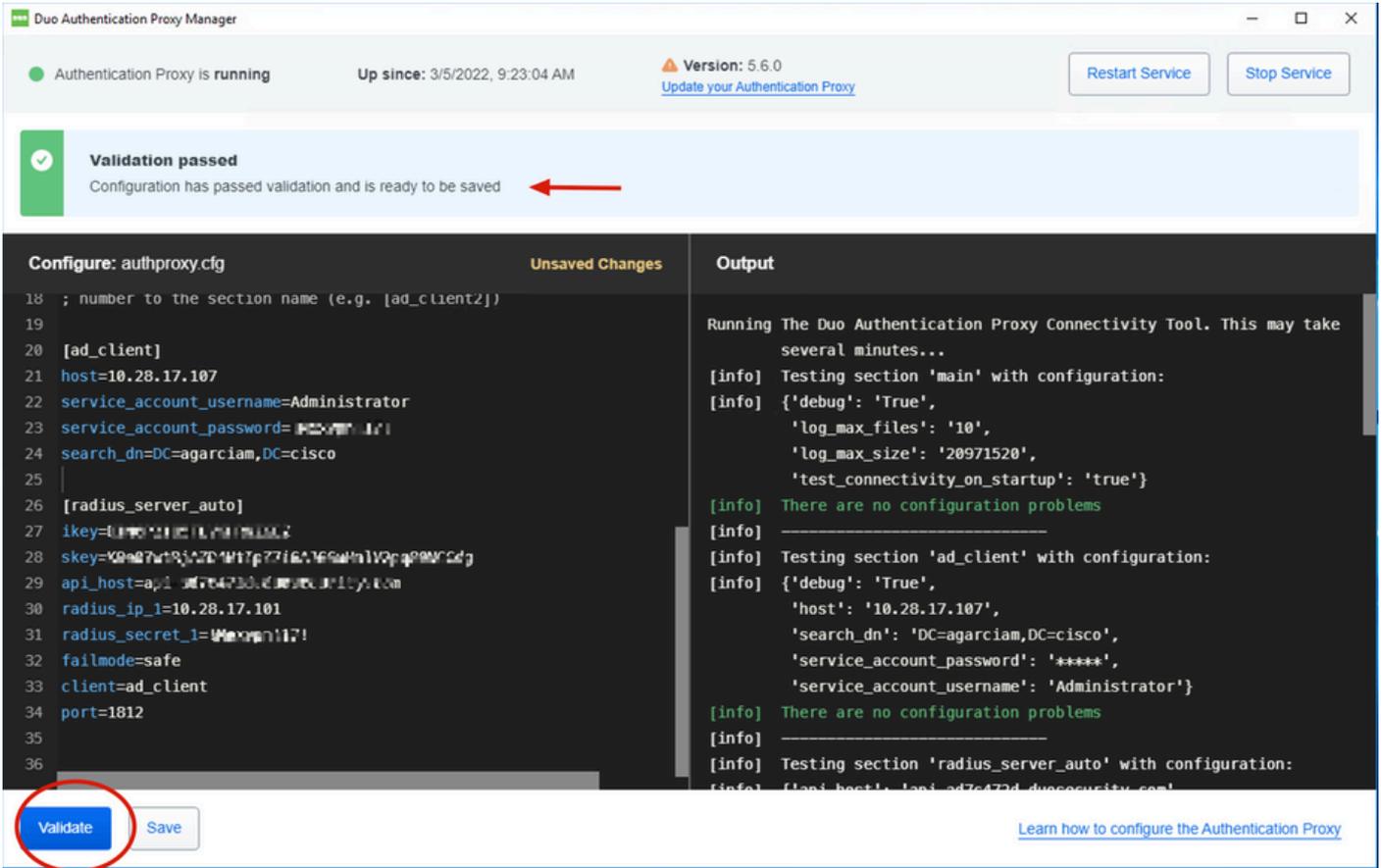
 Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others.

Documentation: [Getting Started](#)

Choose an application below to get started.

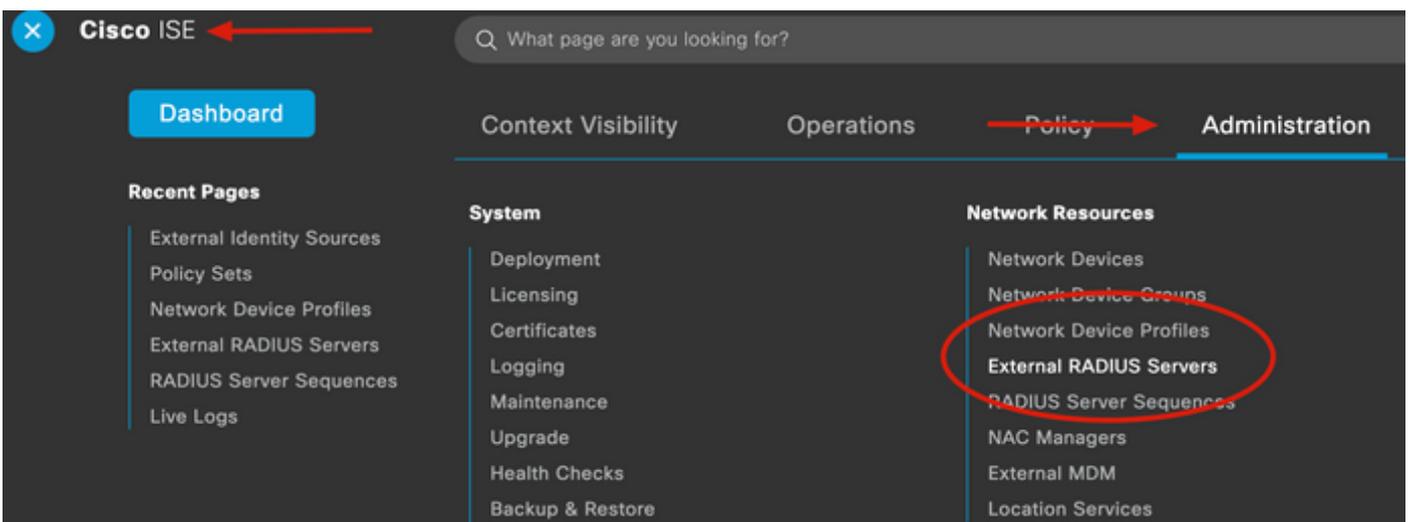
Application	Protection Type	
 Akamai Enterprise Application Access	2FA	Documentation Protect
 Cisco ISE RADIUS 	2FA	Documentation Protect

4. 통합 키, 보안 키 및 API 호스트 이름을 복사합니다. Duo Authentication Proxy 컨피그레이션에 이 정보가 필요합니다.



Cisco ISE 컨피그레이션

1. ISE 관리 포털에 로그인합니다.
2. Cisco ISE 탭을 확장하고 Administration(관리)으로 이동한 다음 Network Resources(네트워크 리소스)를 클릭하고 External RADIUS Servers(외부 RADIUS 서버)를 클릭합니다.



3. External Radius Servers(외부 Radius 서버) 탭에서 Add(추가)를 클릭합니다.

External RADIUS Servers

Edit **+ Add** Duplicate Delete

Name: Currently Sorted Description

4. Duo Authentication Proxy Manager에서 사용되는 RADIUS 컨피그레이션으로 빈 칸을 채우고 Submit(제출)을 클릭합니다.

Network Devices Network Device Groups Network Device Profiles **External RADIUS Servers** RADIUS Server Sequences NAC Managers External MDM More

* Name DUO_NEW

Description

* Host IP 10.28.17.107

* Shared Secret Show

Enable KeyWrap

* Key Encryption Key Show

* Message Authenticator Code Key Show

Key Input Format ASCII HEXADECIMAL

* Authentication Port 1812 (Valid Range 1 to 65535)

* Accounting Port 1813 (Valid Range 1 to 65535)

* Server Timeout 5 Seconds (Valid Range 1 to 120)

* Connection Attempts 3 (Valid Range 1 to 9)

Radius ProxyFailover Expiration 300 (Valid Range 1 to 600)

Submit

5. RADIUS Server Sequences(RADIUS 서버 시퀀스) 탭으로 이동하고 Add(추가)를 클릭합니다.

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers **RADIUS Server Sequences**

RADIUS Server Sequences

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit **+ Add** Duplicate Delete

6. 시퀀스의 이름을 지정하고 새 RADIUS 외부 서버를 할당한 후 제출을 클릭합니다.

RADIUS Server Sequence

General

Advanced Attribute Settings

* Name

DUO_Sequence

Description

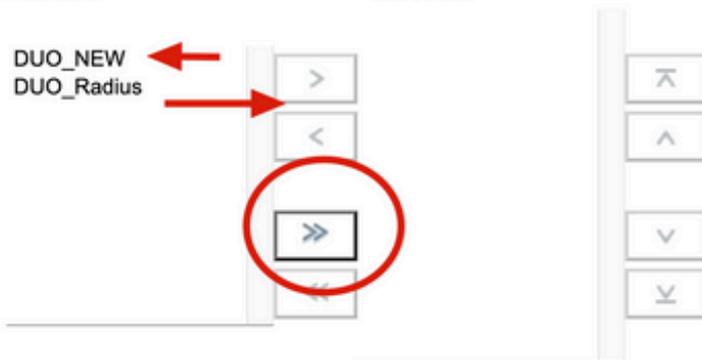
∨ User Selected Service Type

Select the set of external RADIUS servers to use to process requests. Servers are accessed in sequence until a response is r

Available

* Selected

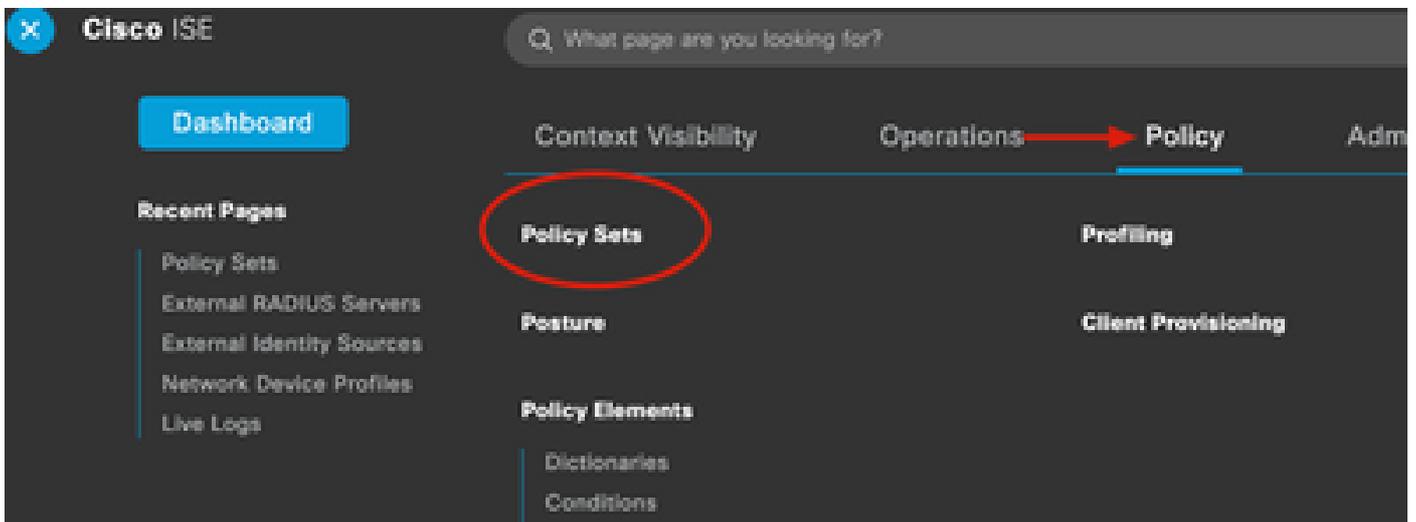
DUO_NEW
DUO_Radius



Remote accounting

Local accounting

7. 대시보드 메뉴에서 정책으로 이동하고 정책 세트를 클릭합니다.



8. RADIUS 시퀀스를 기본 정책에 할당합니다.

 참고: 이 문서에서는 모든 연결에 대한 Duo 시퀀스가 적용되므로 기본 정책이 사용됩니다. 정책 할당은 요구 사항에 따라 달라질 수 있습니다.

Policy Sets Reset Reset Policyset Hitcount

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
			Radius-User-Name EQUALS isevpn	Default Network Access	3
			Radius-NAS-Port-Type EQUALS Virtual	DUO_Sequence	22
	Default	Default policy set		Default Network Access	0

EQ |

Allowed Protocols

- Default Network Access

Proxy Sequence

- DUO_NEW
- DUO_Sequence**

Cisco ASA RADIUS/ISE 컨피그레이션

1. AAA Server groups(AAA 서버 그룹)에서 ISE RADIUS 서버를 구성하고 Configuration(컨피그레이션)으로 이동한 다음 Device Management(디바이스 관리)를 클릭하고 Users/AAA(사용자/AAA) 섹션을 확장하고 AAA Server Groups(AAA 서버 그룹)를 선택합니다.

Bookmarks

To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks".

Go Delete

Configuration

AAA Server Groups

Server Group	Pro
ISE	RA
LOCAL	LO
ad-agarciam	LD

Device Management

- > Management Access
- > Licensing
- > System Image/Configuration
- > High Availability and Scalability
- > Logging
- Smart Call-Home
- Cloud Web Security
- Service Module Settings
- Users/AAA
 - AAA Server Groups
 - LDAP Attribute Map
 - AAA Kerberos
 - Authentication Prompt
 - AAA Access
 - Dynamic Access Policies
 - User Accounts
 - Password Policy
 - Change My Password
 - Login History
- > Certificate Management
- > DHCP
- > DNS
- REST API Agent

Find:

Servers in the Selected

Server Name or IP Address
10.28.17.101

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.