

Duo Lab v1 - Advanced with Cisco AnyConnect



미지막 업데이트: 2020 년 5 월 27 일

본 대모에 대하여

미리 구성되어 있는 본 데모는 아래 내용을 포함합니다:

[요구 사항](#)

[솔루션 소개](#)

[구성도](#)

[시작하기](#)

[시나리오 1: 새 사용자 만들기](#)

[시나리오 2: Cisco CSE Lab - RDP](#)

[시나리오 3: Duo LDAPS Cisco ASA Integration](#)

[시나리오 4: Duo RADIUS Cisco ASA Integration](#)

[부록 A. Duo 계정에 등록](#)

[부록 B. 추가 리소스](#)

요구 사항

아래 항목은 미리 구성된 본 데모를 진행하는데 필요한 구성요소 입니다.

필수	선택 사항
개인 컴퓨터	Cisco AnyConnect®
휴대폰	
Duo Mobile App (휴대폰의 앱 스토어에서 다운로드)	

솔루션 소개

Duo 의 MFA 솔루션으로 Cisco AnyConnect VPN 로그인을 보호하십시오. Duo 는 가장 사용하기 쉽고, 구축이 빠르며, 가장 유연한 MFA 솔루션을 제공합니다. 사용자 ID 를 몇 초 만에 Duo Push, OTP(One-Time Passcode), SMS, 전화 통화 또는 U2F 토큰을 포함한 몇 가지 간단한 인증 옵션을 사용하여 확인할 수 있습니다.

내부 애플리케이션에 대한 안전한 원격 접근을 제공하고, 도난당한 사용자 자격 증명을 방어하며, AnyConnect VPN 에 어떤 장치가 로그인하는지를 발견할 수 있습니다. 이러한 장치 및 보안 상태에 대한 가시성과 인사이트를 확보하여 장치 상태를 확인하고 신뢰할 수 있는 보안 장치에서만 VPN 에 접근할 수 있도록 보장하는 정책을 적용합니다.

구성도

본 데모는 Duo 솔루션의 스크립트로 작성된 시나리오 및 기능을 설명하기 위해 사전 구성된 사용자 및 구성 요소들을 포함되어 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.

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.

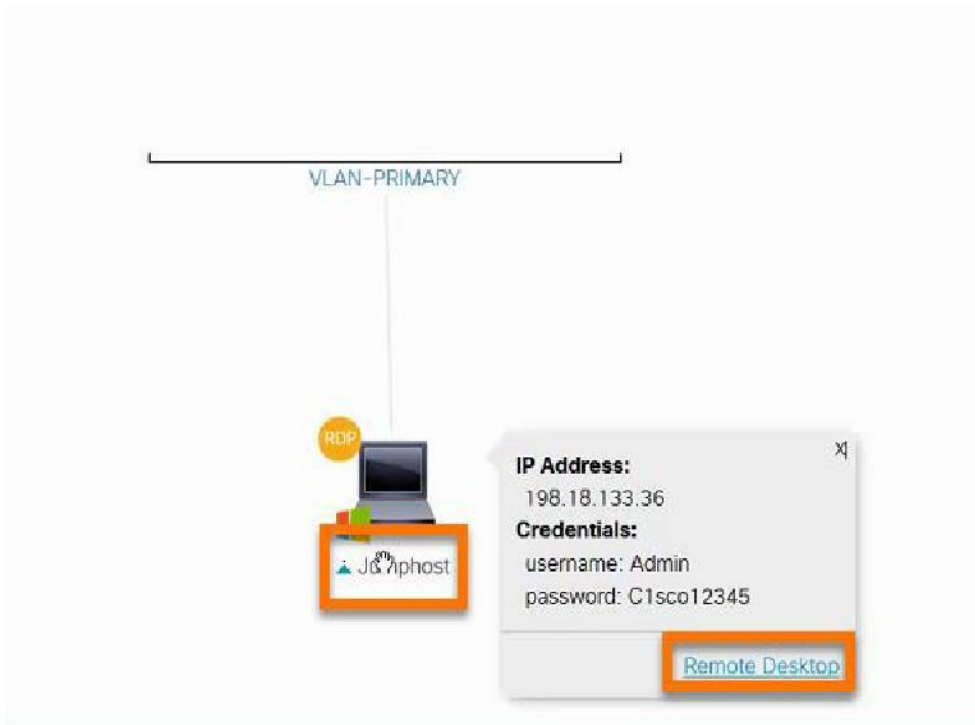
사전에 충분한 연습은 성공적 진행을 위한 필수 조건입니다.

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

1. dCloud 세션 시작합니다. [\[가이드\]](#)

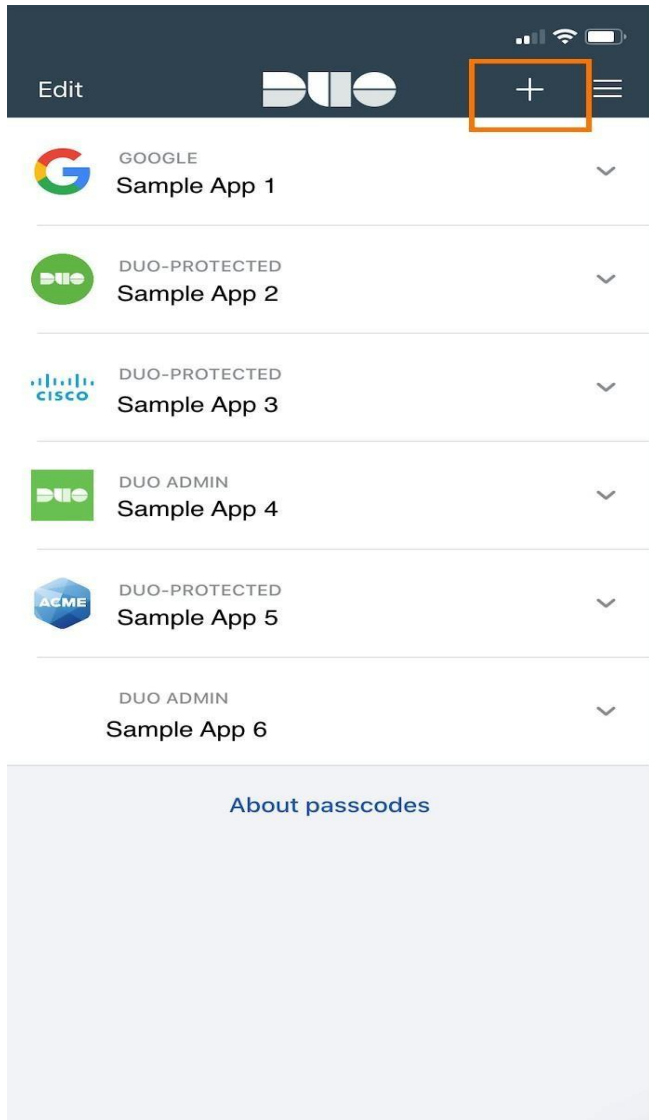
노트: 세션 예약 후 시나리오의 랩이 활성화 되기까지 최대 10 분 소요됩니다.

2. **Jumphost** 를 클릭한 다음 **Remote Desktop** 를 클릭합니다.



3. Duo Mobile 앱을 휴대폰에 다운로드합니다.

4. 휴대폰에서 Duo Mobile 앱을 열고 오른쪽 상단 모서리에 있는 + 아이콘을 클릭합니다.



5. 휴대폰으로 QR 코드를 스캔합니다.

팁: QR 코드가 스캔되지 않으면 다음을 수행합니다:


모바일 앱에서 **No Barcode?**를 누릅니다. "What type of account do you want to add? 필드에서 **Duo Security** 를 선택합니다. 그런 다음 랩톱의 자격 증명 화면에서 Launch 단추 아래를 보고 **Manual activation code** 필드에 사용 가능한 URL 을 입력합니다.

6. 노트북에서 **Launch** 를 클릭하면 웹 브라우저에서 새 **Login - Duo** 탭이 열립니다.

Cisco dCloud

Welcome to dCloud

1. Install "Duo Mobile" on your iOS or Android device.
2. Activate Duo Mobile for this demo. This allows you to log in using Duo Push as your second factor.
 - Open Duo Mobile
 - Tap "+" button to add the Duo dCloud demo account
 - Scan the QR code below (countdown indicates QR validity)
3. Launch the demo and log in to the Duo Admin Panel using the provided credentials and Duo Mobile




1h 25m 18s

Email address: [COPY](#)

Password: [COPY](#)

[Launch](#)

admin-demodemo.duosecurity.com/login?next=%2F



1. Log In

Email address

Save my email address for next time
Not recommended for public or shared computers

[Continue](#)

[Don't have an account?](#)

2. Confirm Your Identity

7. 데스크톱 하단에 있는 **DCV Automation Controller** 아이콘을 클릭하여 **Welcome to dCloud** 화면으로 돌아갑니다.



1h 25m 18s

Email address:

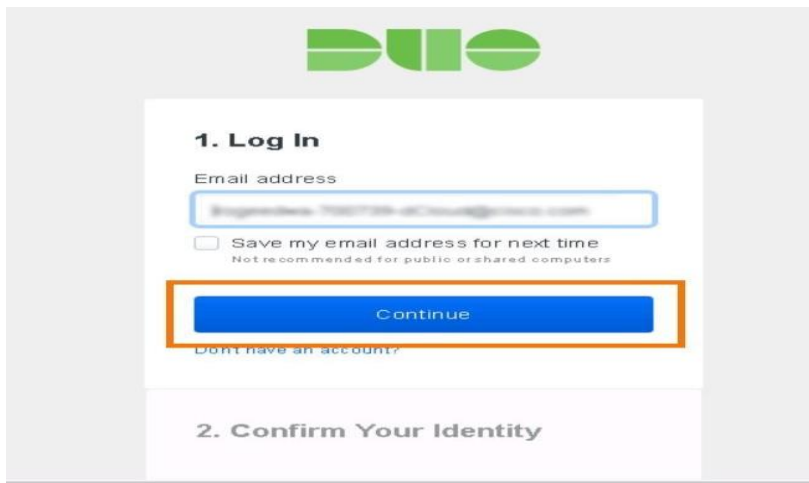
[COPY](#)

Password:

[COPY](#)

Launch

8. **Welcome to dCloud** 화면에서 이메일 주소(**Email Address**) 옆에 있는 복사(copy) 링크를 클릭합니다.
9. Google Chrome 아이콘(데스크톱 하단에)을 클릭하여 웹 브라우저의 **Login - Duo** 탭으로 돌아가 이메일 주소를 붙여넣습니다.



10. **Continue** 를 클릭합니다.

11. **DCV Automation Controller** 아이콘 (바탕 화면 하단에 있음)을 클릭하여 **Welcome to dCloud** 화면으로 돌아갑니다.



1h 25m 18s

Email address: [copy](#)

Password: [copy](#)

[Launch](#)

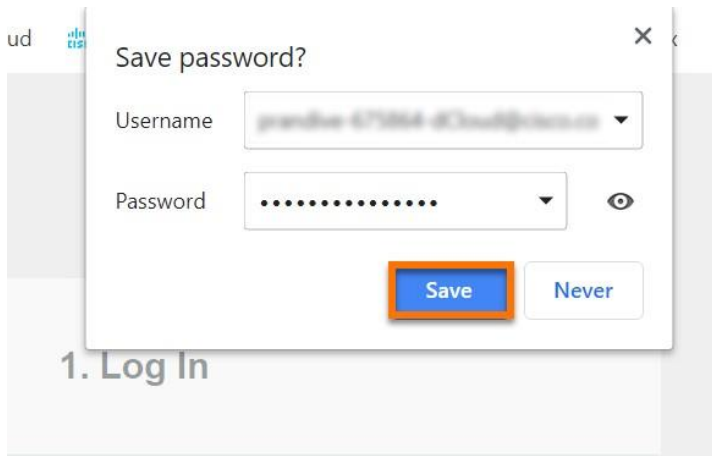
12. **Welcome to dCloud** 화면에서, 링크를 클릭합니다. (**Password** 옆에 있음).

13. 그런 다음 데스크톱 하단에 있는 Google Chrome 아이콘을 클릭하여 웹 브라우저의 **Login - Duo** 탭으로 돌아가서 비밀 번호를 붙여넣습니다.



14. **Log In** 을 클릭합니다.

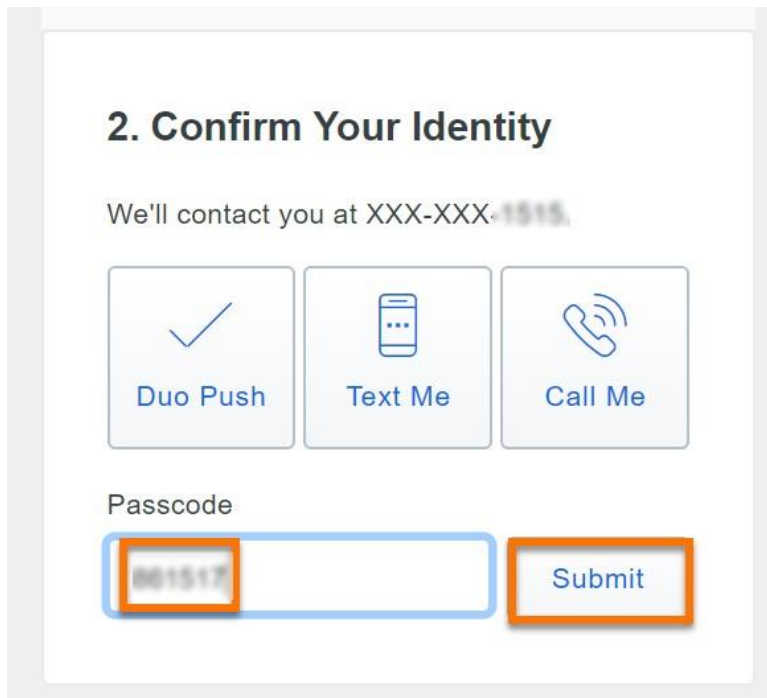
15. **Save** 를 클릭하여 자격 증명을 저장합니다.



1. Log In

2. Confirm Your Identity

16. Duo Mobile 앱의 패스코드를 Passcode 필드에 입력하여 ID 를 확인하고 **Submit** 를 클릭합니다.



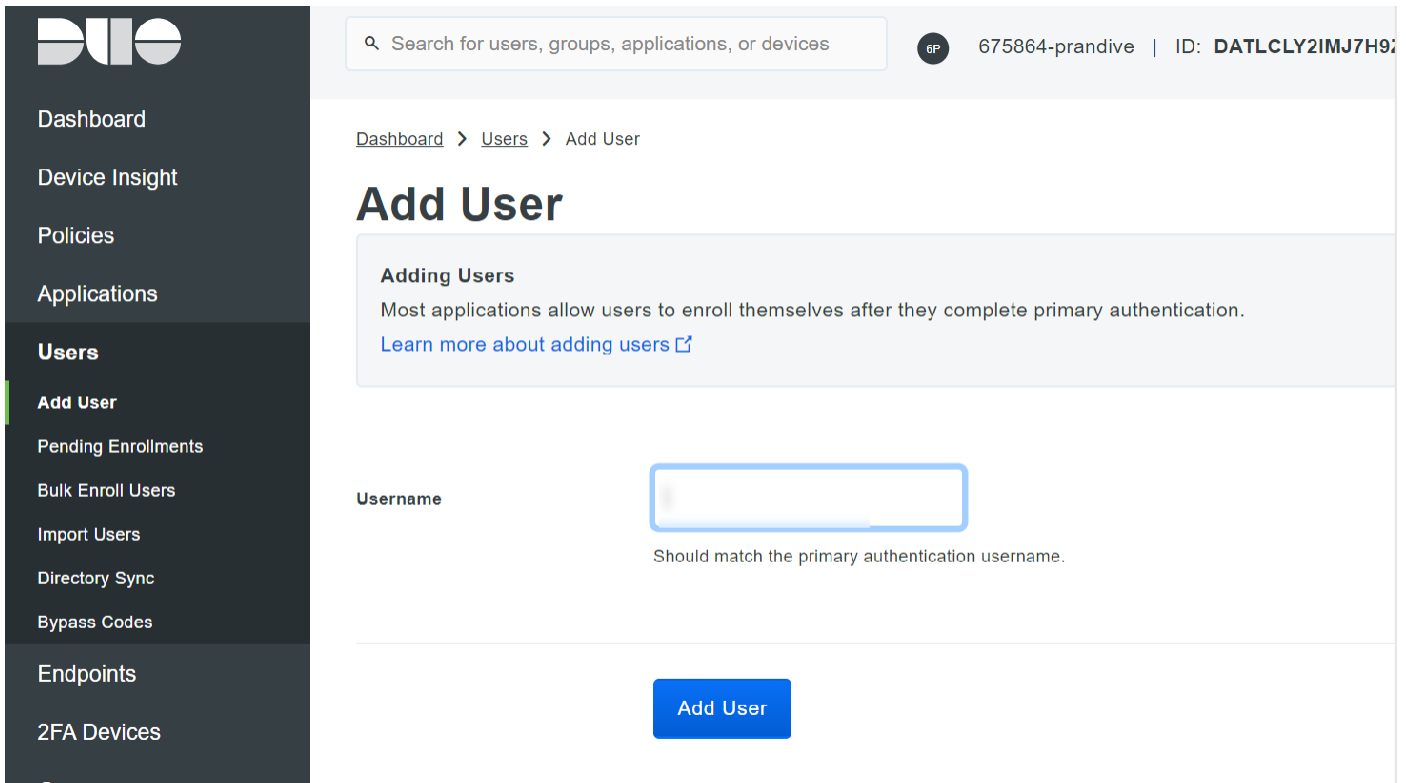
시나리오 1: 새 사용자 만들기

가치 제안: 본 실습에서는 Add User(단일 사용자) 옵션을 사용합니다. 단일 사용자를 추가하는 것은 특히 사례별로 사용자를 등록할 가능성이 높은 중소기업에서 새로운 사용자를 설정하는 것이 얼마나 쉬운지를 보여주는 데 유용합니다. 일반적으로 엔터프라이즈 클라이언트는 디렉터리 동기화, 인라인 자체 등록 또는 Duo Security 의 다른 대량 등록 방법 중 하나를 사용하여 사용자를 가져옵니다. 사용자 등록에 대한 자세한 내용은 : <https://duo.com/docs/enrolling-users> 에서 확인할 수 있습니다.

스텝

이 작업의 경우 현재 사용 중인 실제 이메일 계정을 사용할 수 있습니다. 이렇게 하면 Duo 로부터 이메일 알림을 받고 시스템에 등록할 수 있을 것입니다.

1. Duo 대시보드의 왼쪽에 있는 메뉴에서 **Users**(사용자)를 선택합니다. 그런 다음 **Add User**(사용자 추가)를 선택합니다.
2. 새 사용자를 만들려면 **username** 텍스트 상자에 이름과 성(예: **johndoe**)을 입력합니다.
노트: username 에 공백을 사용하지 마십시오.
3. **Username** 텍스트 상자 아래에 있는 **Add User** 버튼을 클릭합니다.



The screenshot displays the Duo Admin Console interface. On the left is a dark sidebar with navigation options: Dashboard, Device Insight, Policies, Applications, Users (highlighted), Add User, Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, Endpoints, and 2FA Devices. The main content area has a search bar at the top with the text 'Search for users, groups, applications, or devices'. Below the search bar is a breadcrumb trail: 'Dashboard > Users > Add User'. The main heading is 'Add User'. Underneath, there is a section titled 'Adding Users' with the text: 'Most applications allow users to enroll themselves after they complete primary authentication.' and a link 'Learn more about adding users'. Below this is a form with a 'Username' label and a text input field. A note below the field states: 'Should match the primary authentication username.' At the bottom right of the form is a blue button labeled 'Add User'.

- 이 사용자의 전체 이름 및 이메일 주소를 입력합니다. 사용자가 등록 알림을 받고 조치를 취할 수 있는 유효한 이메일 주소인지 확인하십시오.

Full Name

Email

Save Changes

- Save Changes**(변경 사항 저장)을 클릭합니다.
- 사용자의 페이지 상단에서 **Send Enrollment Email** 를 클릭합니다.

[Dashboard](#) > [Users](#) > johndoe

johndoe

Logs | [Send Enrollment Email](#) |  [Send to Trash](#)

- 받은 편지함에서 등록 이메일(enrollment email)을 찾습니다. 바로 표시되지 않으면 스팸/정크 폴더를 확인합니다.

Hello,

Your company is now rolling out Duo Security, a friendly and secure way for you to log into your organization's applications. Your manager has invited you to set up your account for Duo so you can start logging in.

To begin, click this link to enroll a phone, tablet, or other device:

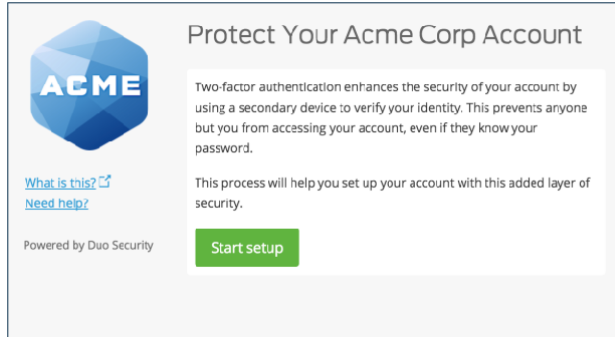
<https://api-ae380425.duosecurity.com/portal?code=3f2d5f5d7885d7b2&akey=DA9XKQEZCILVW28CB4WQ>

Duo Security is a two-factor authentication service that strives to be easy to use and secure. To learn more about Duo authentication, visit the guide here:

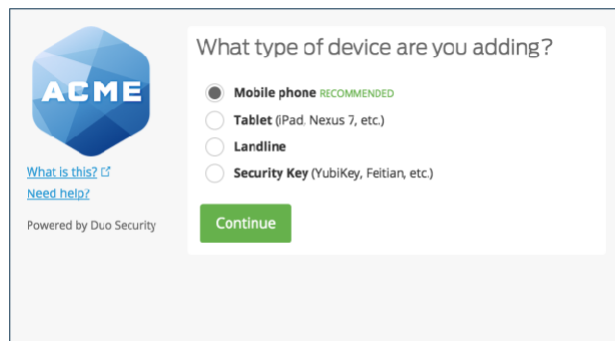
<https://guide.duo.com/enrollment>

8. enrollment(등록) 링크를 클릭하고 다음과 같이 단계별 등록 프로세스를 완료합니다:

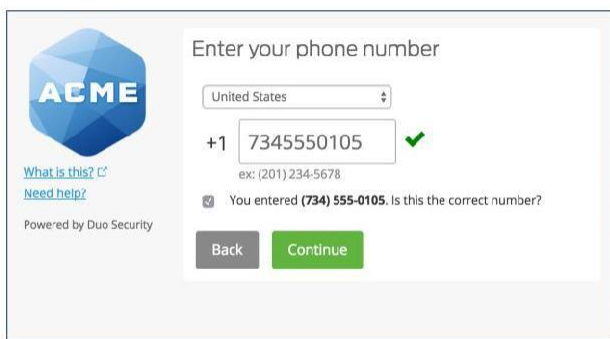
a. **Start setup** 를 클릭합니다.



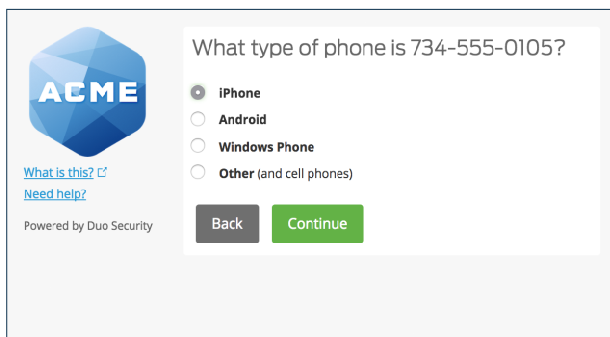
b. 추가할 디바이스 유형을 선택합니다. **Continue** 를 클릭하십시오.



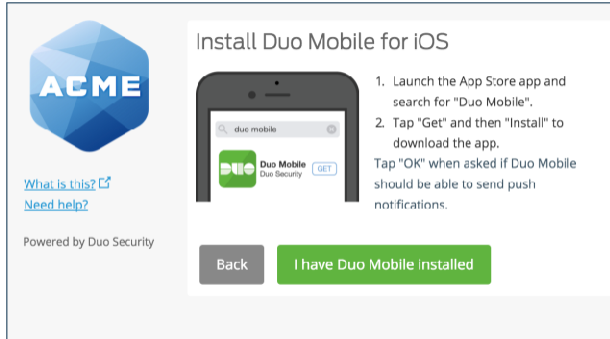
c. 전화 번호를 입력하고 **Continue** 를 클릭합니다.



d. 전화 유형을 선택하고 **Continue** 를 클릭합니다.



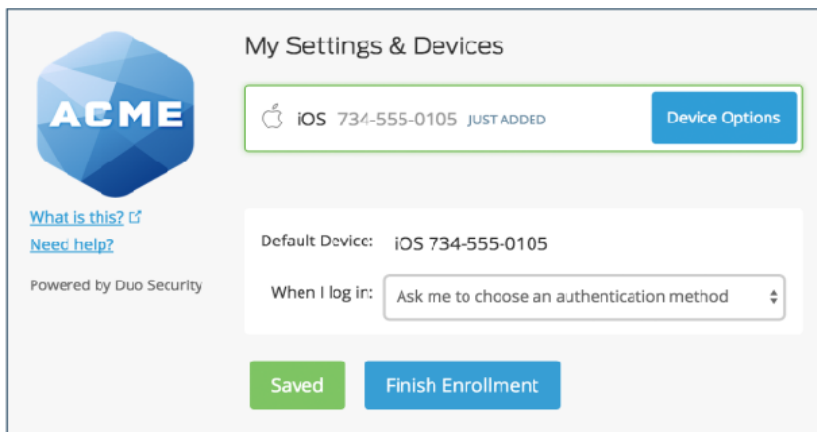
e. 다음 지침에 따라 iOS 용 Duo Mobile 을 설치하고 **I have Duo Mobile Installed** 를 클릭합니다.

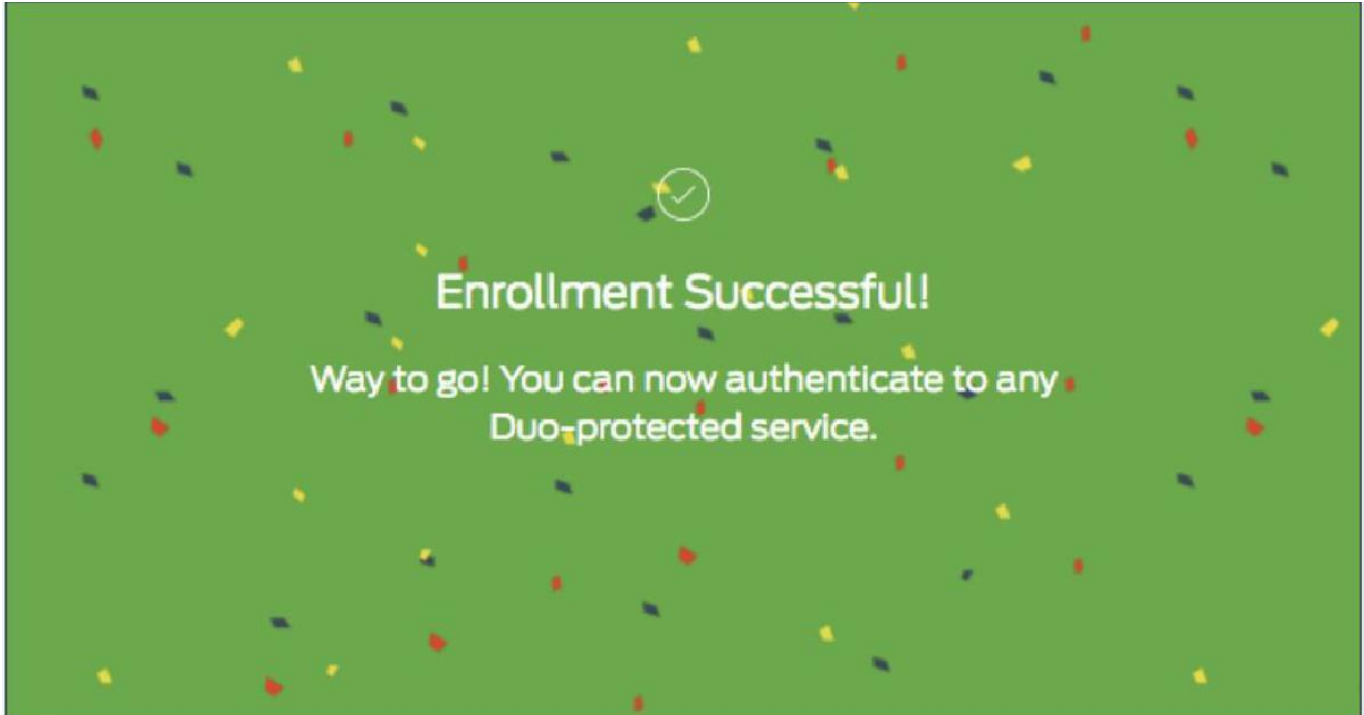


f. 다음 지침에 따라 iOS 용 Duo Mobile 을 활성화합니다. 바코드를 성공적으로 스캔 한 후 Continue 를 클릭합니다.



g. My Setting & Devices 화면에서 **Finish Enrollment** 를 클릭합니다.





시나리오 2: Cisco CSE Lab - RDP

가치 제안: 등록되지 않은 사용자 및 2FA 등록 사용자에게 대한 인증 사용 사례를 테스트하기 위해 dCloud lab 에 Duo Authentication for Windows 로그인 통합 기능을 설치합니다.

스텝

노트: Windows PC/Server 를 사용하여 이 섹션을 완료할 수 있지만, 일관성을 유지하고 문제가 발생할 경우 다른 컴퓨터에 영향을 미치지 않도록 이 dCloud 인스턴스를 사용하는 것이 권장합니다.

Provision the Cisco AnyConnect Posture with ASA, ISE, and AMP v1.2 Lab

Cisco AnyConnect Posture with ASA, ISE, and AMP v1.2

ID: 545214 Published Date: 10-Apr-2019 22:32 Demonstration Security Policy and Access VPN Security Clients English

Demonstrate the powerful capabilities of the Cisco AnyConnect and how integration with Cisco ASA Firewall, Cisco AMP, and Cisco Identity Service Engine provides seamless and secure remote access to enterprise networks.

★ Favorite [Related Documents](#) [Schedule](#)

1. 브라우저를 열고 dCloud 예정된 Duo Admin 계정에 로그인합니다.

2. Duo 계정에서 **Global New User** 정책을 **Allow Access without 2FA** 으로 설정합니다.
 - a. **Policies** 페이지로 이동하여 (**edit the global policy**) 글로벌 정책을 편집합니다.
 - b. 편집기에서 **New User Policy** 를 찾아 Allow access without 2FA 를 선택합니다.
 - c. Save Policy 버튼을 클릭합니다.
3. 아래 단계에 따라 RDP 애플리케이션을 만듭니다.
 - a. **Duo Admin Panel** 로 로그인하여 **Applications** 으로 이동합니다.
 - b. **Protect an Application** 을 클릭하고 애플리케이션 목록에서 **Microsoft RDP** 항목을 찾습니다.
 - c. 맨 오른쪽에 **Protect** 를 클릭하여 애플리케이션을 구성하고 **integration key, secret key** 및 **API hostname** 을 가져옵니다. 설치를 완료하려면 이 정보가 필요합니다.
4. Cisco AnyConnect Posture with ASA, ISE, and AMP v1.2 Lab 에서 **Wkst1** 을 열고 Windows Logon 설치자 패키지에 대한 Duo Authentication 을 다운로드합니다. <https://dl.duosecurity.com/duo-win-login-latest.exe>
 - a. 관리자 권한으로 Windows 로그온용 Duo Authentication installer 를 실행합니다.
 - b. **Duo Authentication for Windows Logon** 을 설치하고 구성을 위해서는 <https://duo.com/docs/rdp#run-the-installer> 를 참조하십시오.
5. Workstation 에서 로그 아웃하고 또 다시 로그인하십시오.

참고: Duo Admin Panel > Reports 에서 관리자는 "Granted Allow unenrolled user – Amin"인지 확인합니다.
6. 계정에 **administrator** 라는 사용자를 생성/ 등록합니다.
 - a. <https://duo.com/docs/deploying-a-proof-of-concept#proof-of-concept-deployment>
7. Workstation 에서 로그아웃하고 또 다시 로그인합니다. 이번에는 **2FA** 에 대한 메시지가 표시될 겁니다.
8. 아래 나열된 바와 같이 2FA 프롬프트에 대해 고객이 이 시나리오에서 배울 수 있는 유용한 정보와 함께 흥미로운 점을 반드시 지적하십시오.

2FA 프롬프트에 대한 주의 사항

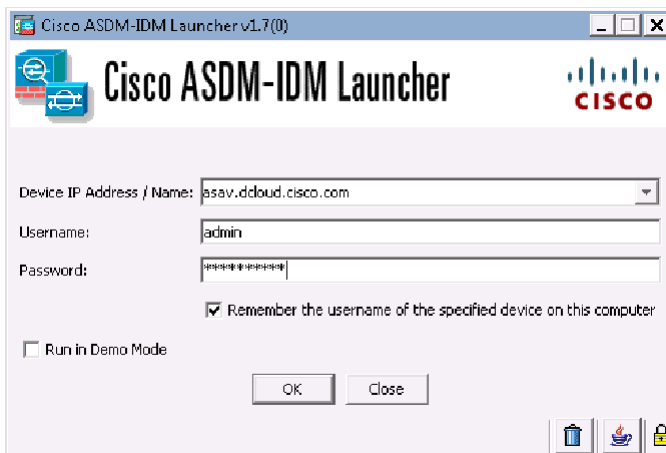
- Duo Auth Prompt 처럼 보이지만, 다릅니다.
- 기억되는 장치 없음
- 장치 데이터 없음
- RDP 전용 IP 주소, 로컬 로그인 없음(즉, Trusted Networks 정책을 사용할 수 없음)
- Q1 에 시작하는 admin panel 에서 오프라인 보고서 호스트 이름(hostname) 로컬로 보고
- 인라인 등록 없음

시사점

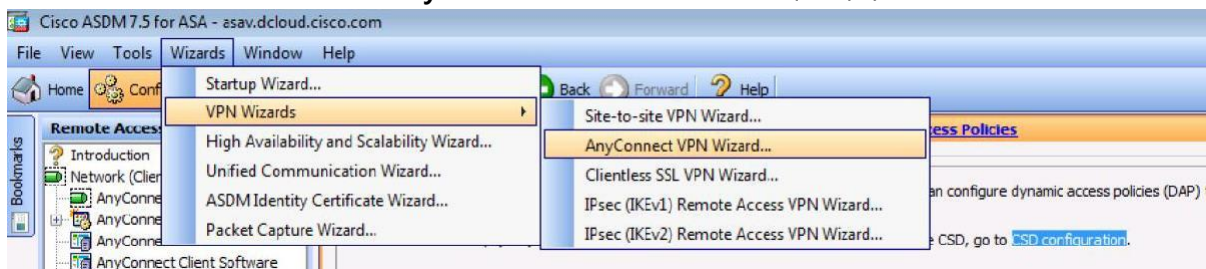
- 간편하게 설치할 수 있습니다.
- 최종 사용자 환경이 간편합니다(여러 장치를 지원).
- 등록되지 않은 사용자의 접근을 허용합니다.
- Yes! 2FA every time(적절한 기대치를 설정하도록 하십시오)
- GPO 와 같은 방법을 사용하여 푸시할 수 있습니다(문서 참조).

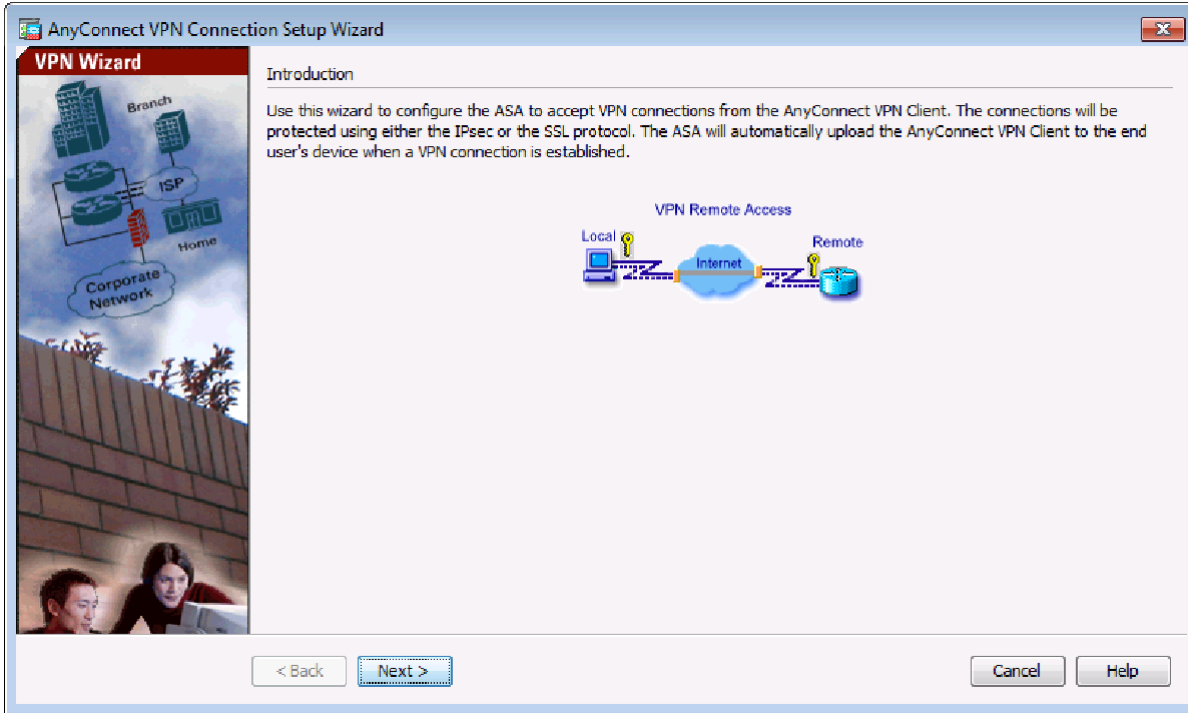
Cisco ASA + Duo

1. 이 테스트를 위해 새 AnyConnect Connection Profile, Client Profile, 및 Local User 를 만듭니다.
2. 자격 증명 **admin/C1sco12345** 를 사용하여 Workstation 에서 **Cisco-ASDM** 을 시작합니다.



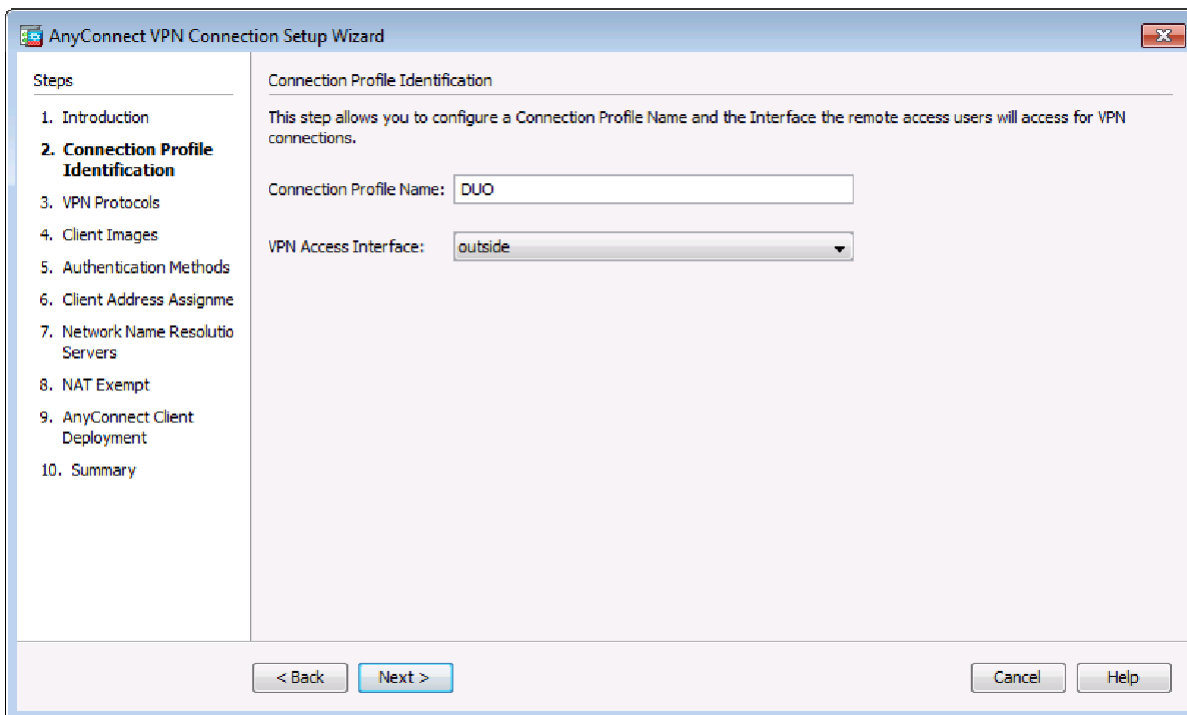
3. **Wizards > VPN Wizards > AnyConnect VPN Wizard** 를 선택합니다.



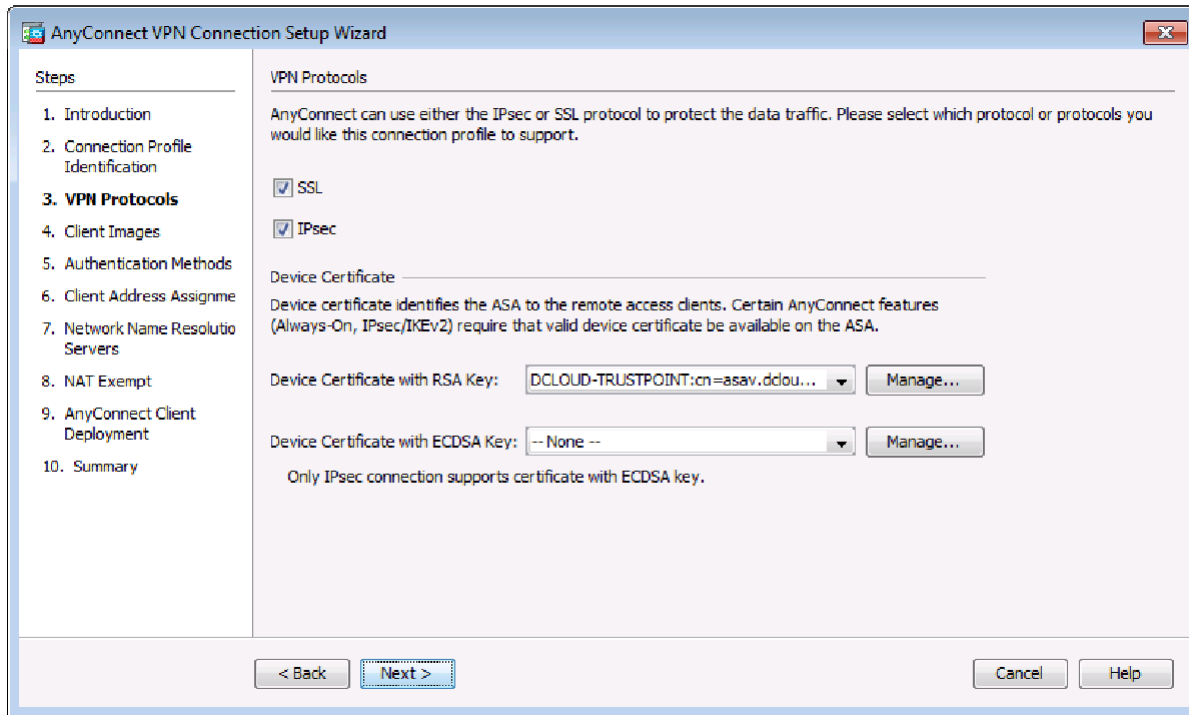


4. **Next** 를 클릭합니다.

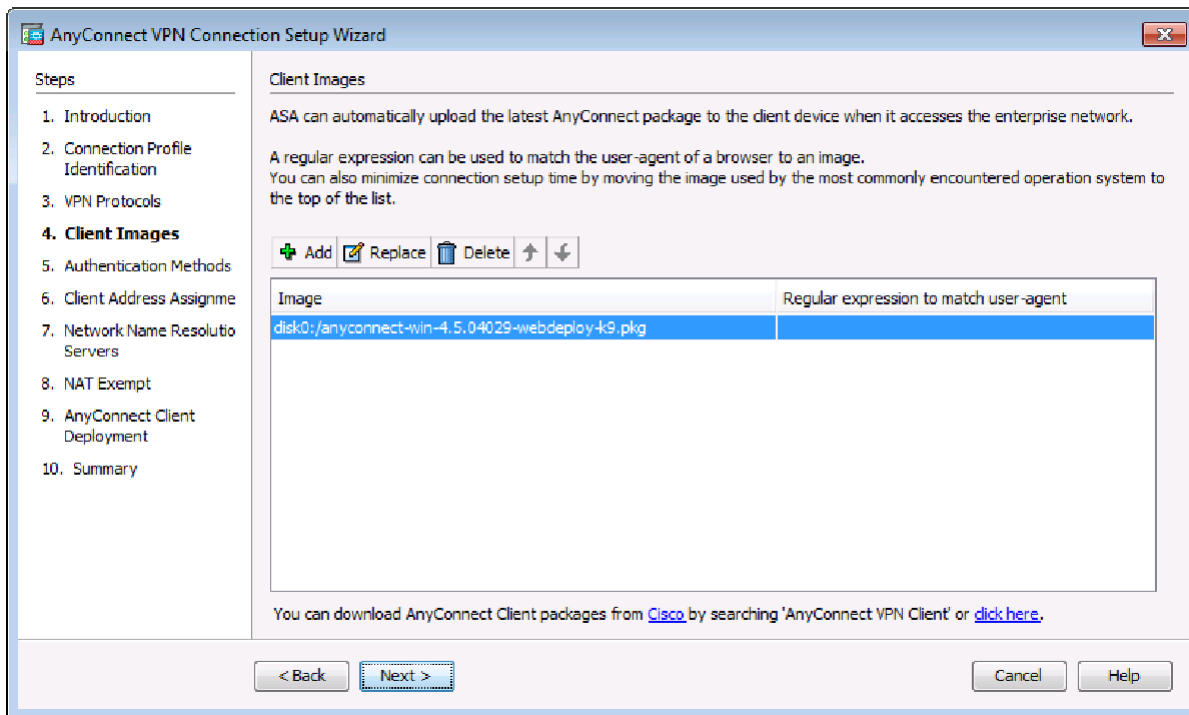
5. **Connection Profile Identification** 화면에서 프로파일 이름 (예: Duo)을 입력합니다.



6. 그런 다음, **Next** 를 클릭합니다.

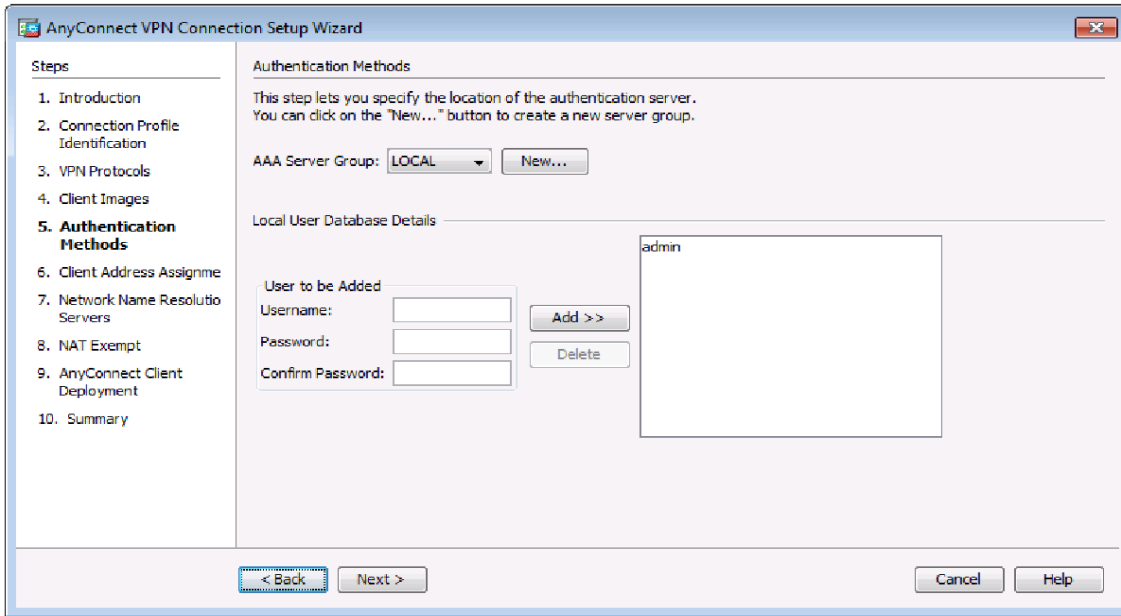


7. **Next** 를 클릭합니다.

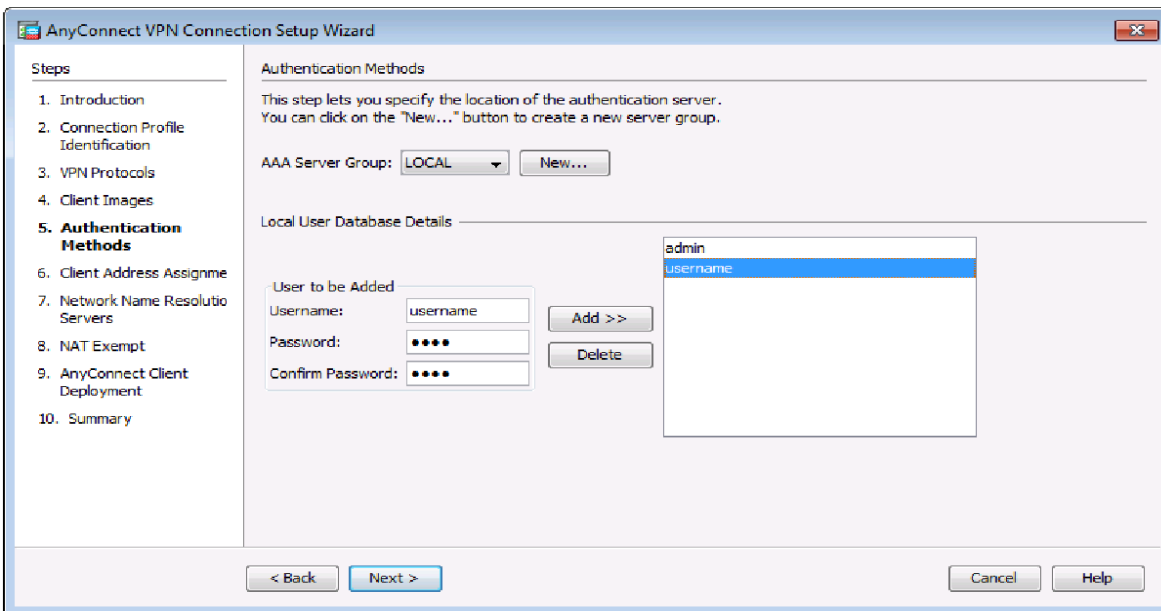


8. **Next** 를 클릭합니다.

9. **Authentication Methods** 화면을 사용하여 새 Local User 계정을 추가합니다.
10. **User to be Added** 아래에서, setup lab 에(firstnamelastname) 생성한 테스트 사용자 이름(username)을 입력한 다음 테스트 계정에 대한 비밀번호를 만듭니다.
- 참고:** 설정 랩(setup Lab)에서 사용한 것과 동일한 사용자 이름(username)이어야 합니다. 예: **firstnamelastname** (이름성)

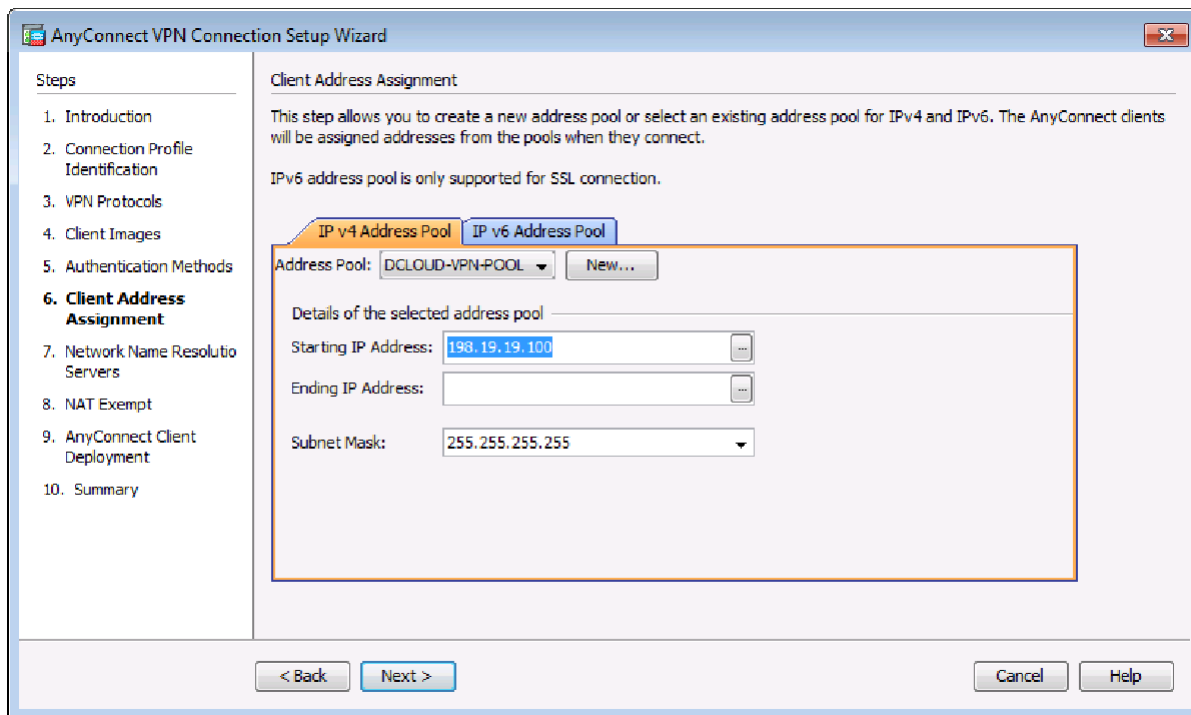
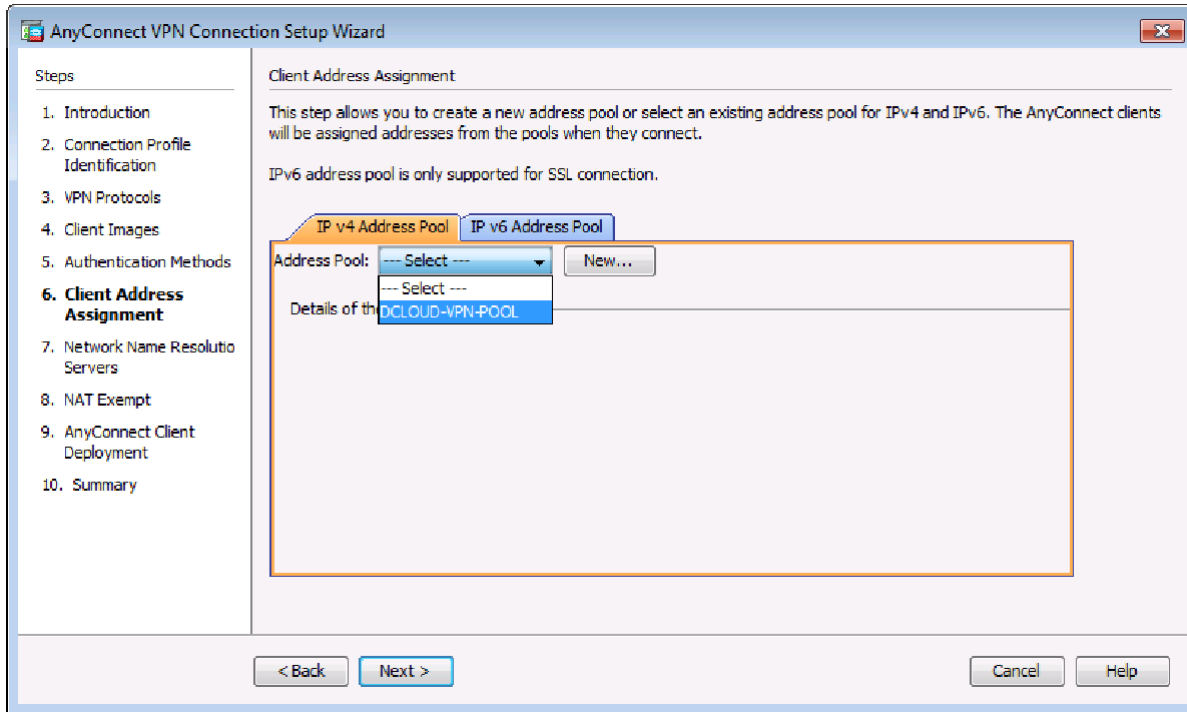


Authentication Methods(인증 방법) – User to be Added(추가 할 사용자) – Add(추가) >>

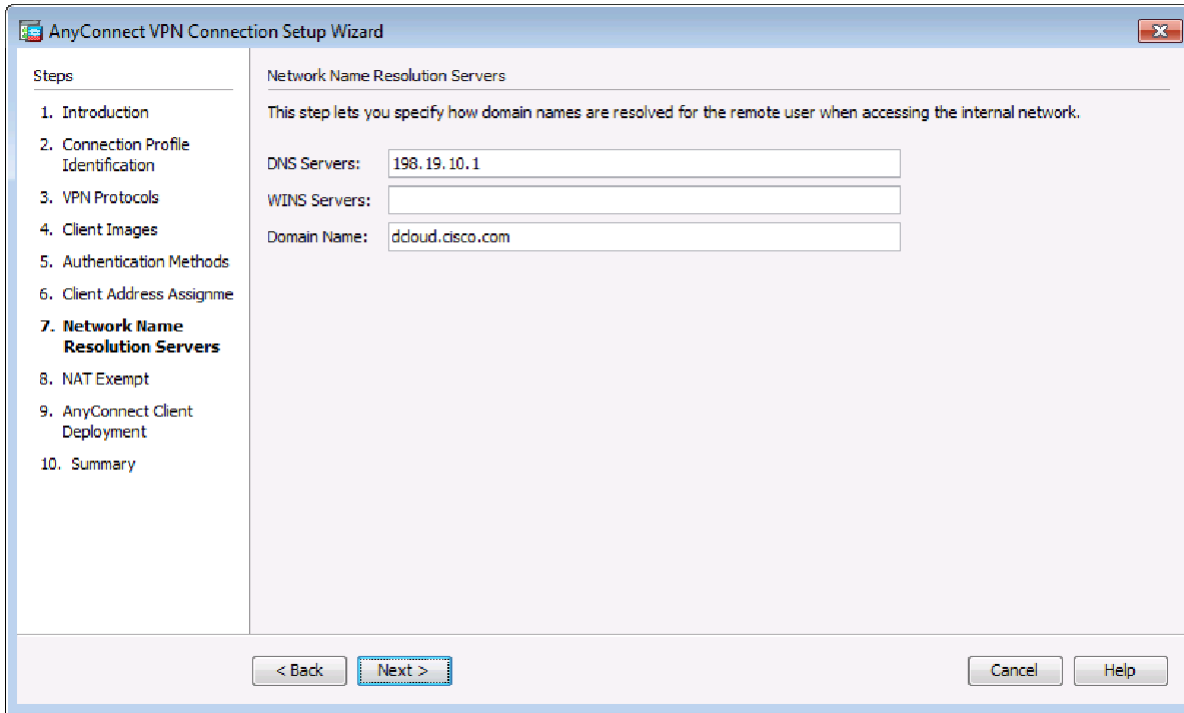


1. **Next** 를 클릭합니다.

2. **Client Address Assignment** 화면에서, IPv4 Address Pool 의 DCLLOUD-VPN-POOL 을 선택합니다.
주의 사항: DNS 서버가 풀에서 선택한 설정으로 자동 채워져야 합니다. 풀에서 이미 선택한 IP 주소 범위를 편집하지 마십시오.

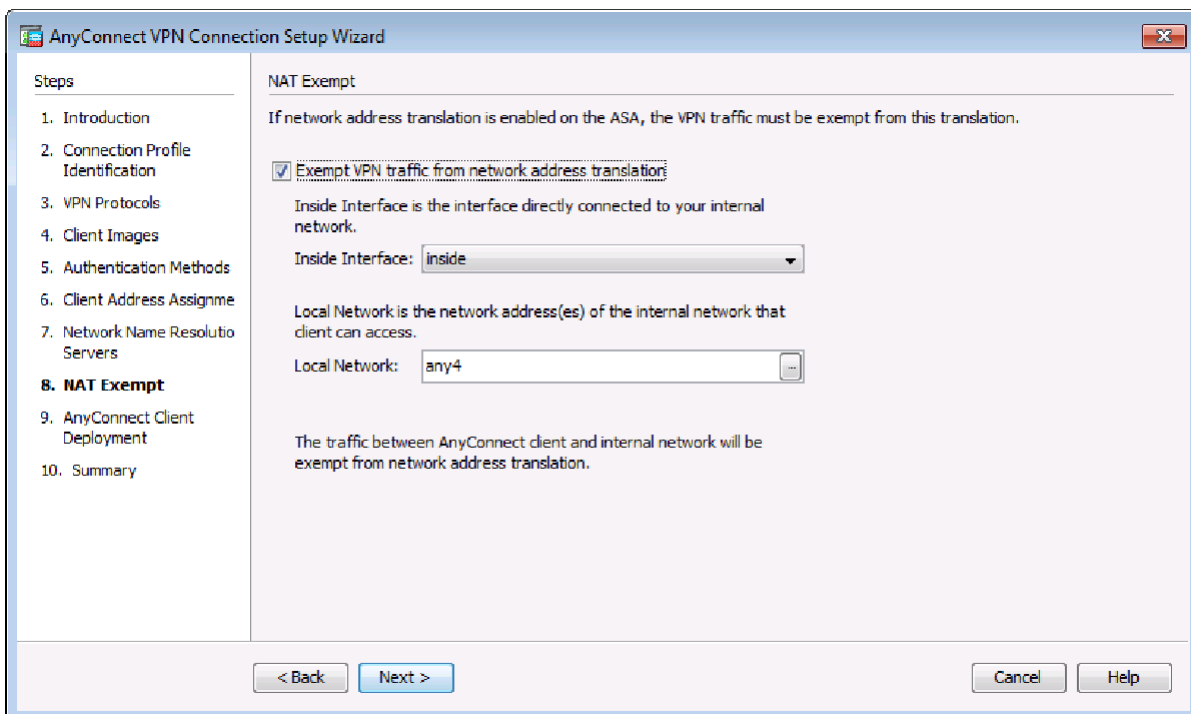


3. **Next** 를 클릭합니다.

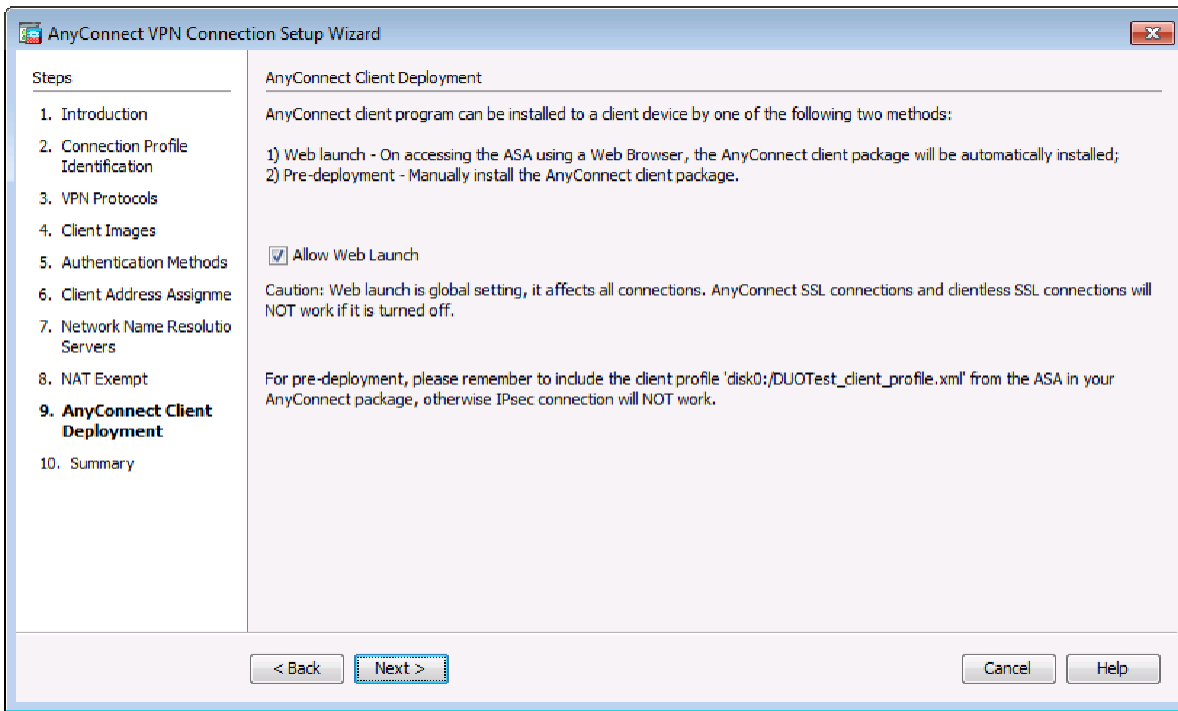


4. **Next** 를 클릭합니다.

5. NAT Exempt 화면에서, **Exempt VPN traffic from network address translation** 에 대한 확인란을 선택합니다.

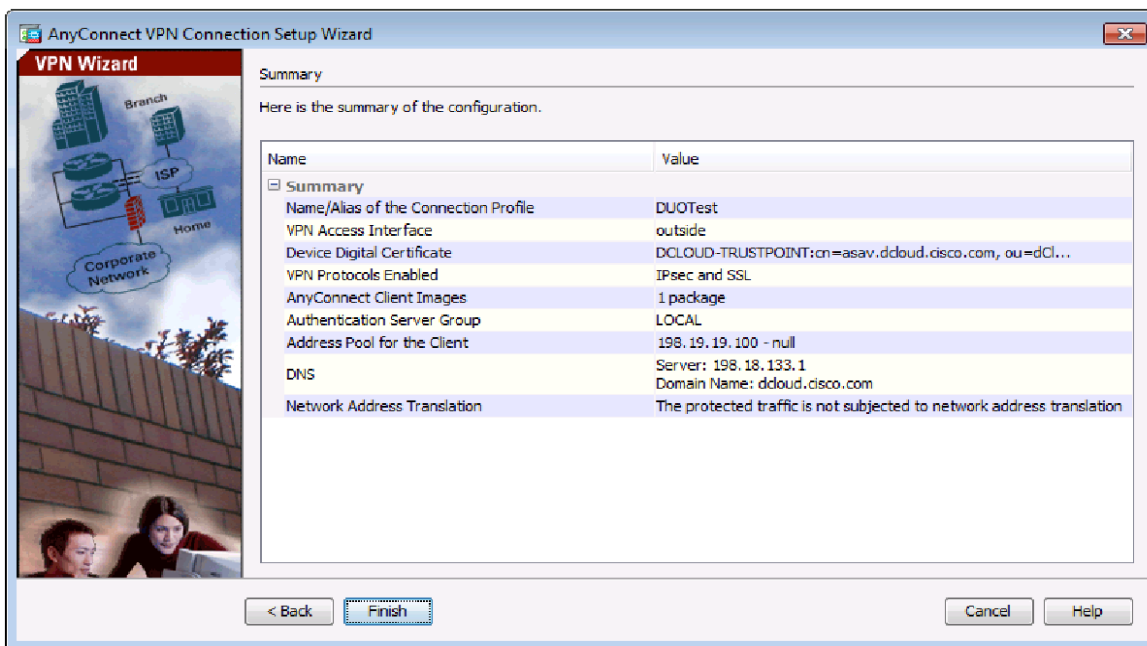


6. **Next** 를 클릭합니다.



7. **Next** 를 클릭합니다.

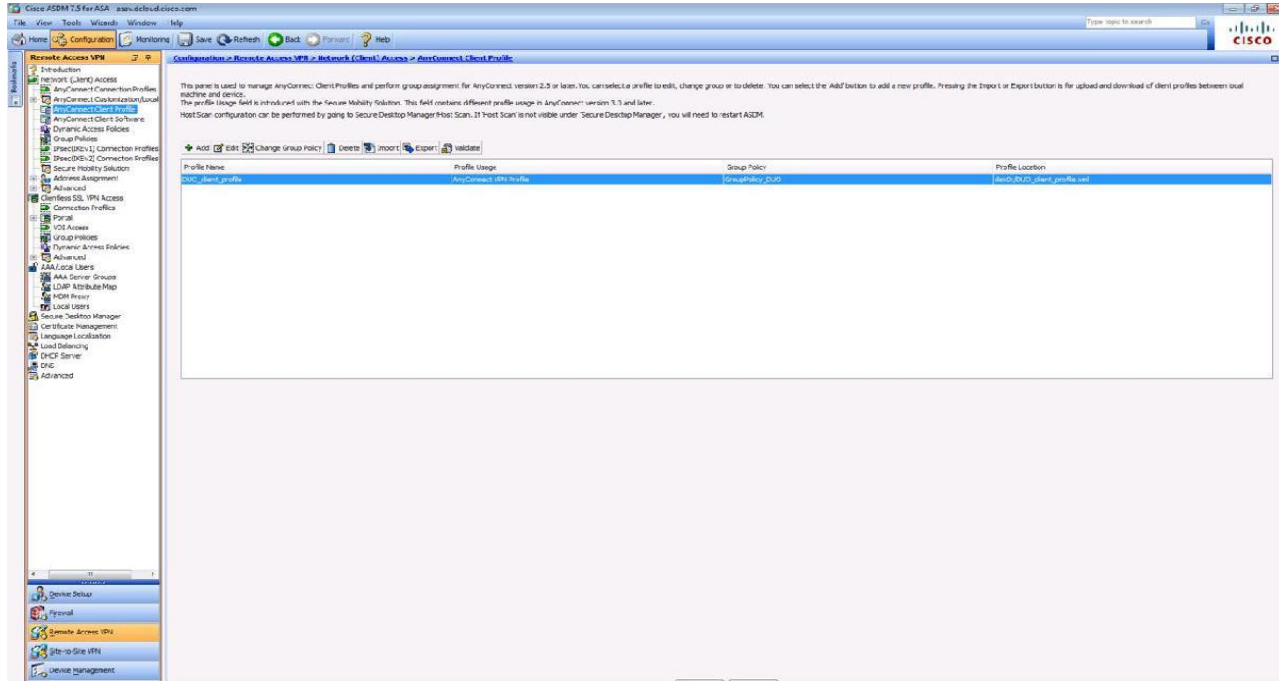
Summary – Verify (요약 – 확인)



1. **Finish** 를 클릭하고 **Send** 를 클릭합니다.

참고: 이제 ASA 에 새 테스트 Connection Profile, Client Profile, and Local User 계정이 있습니다.

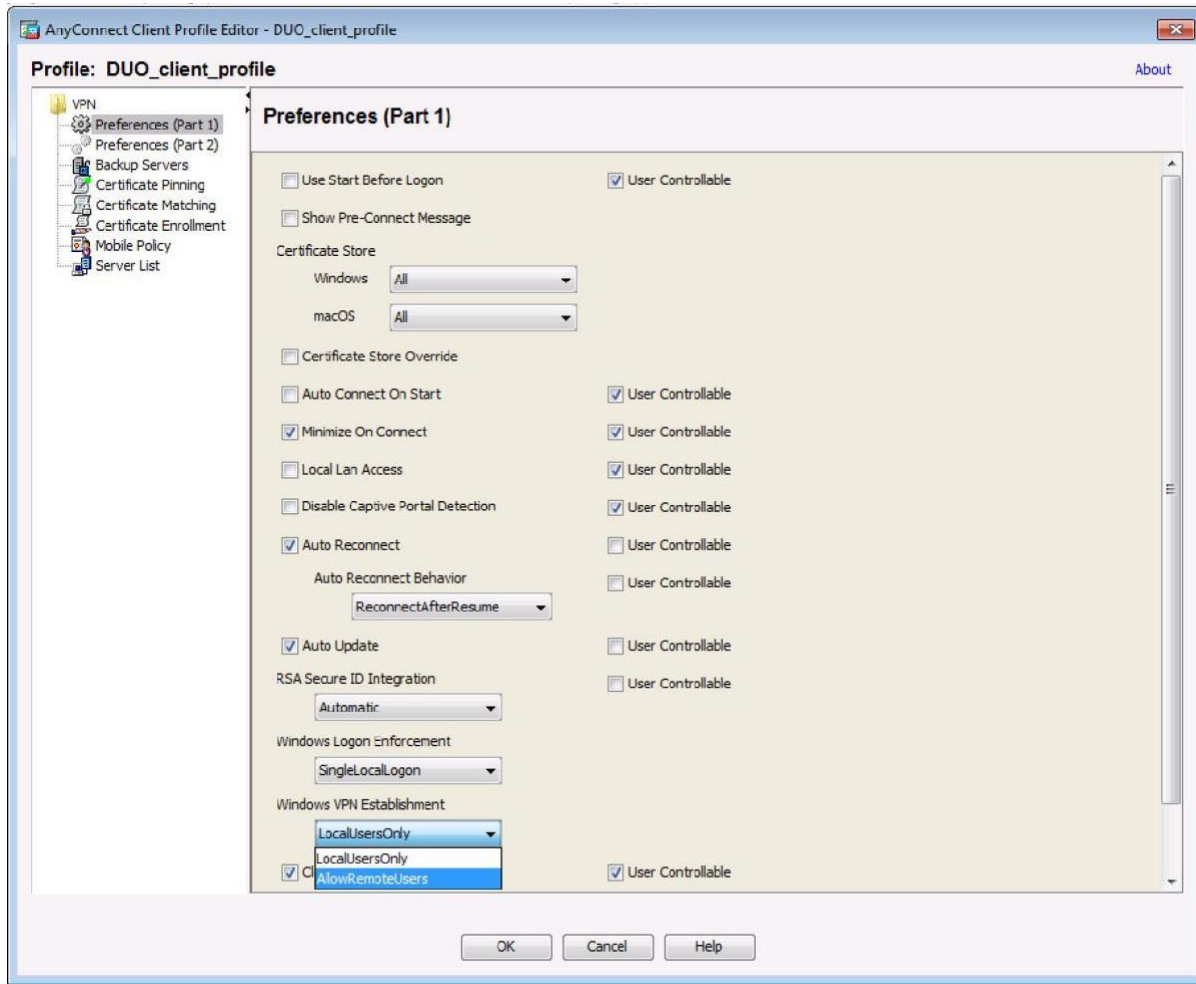
2. **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile** 로 이동합니다.



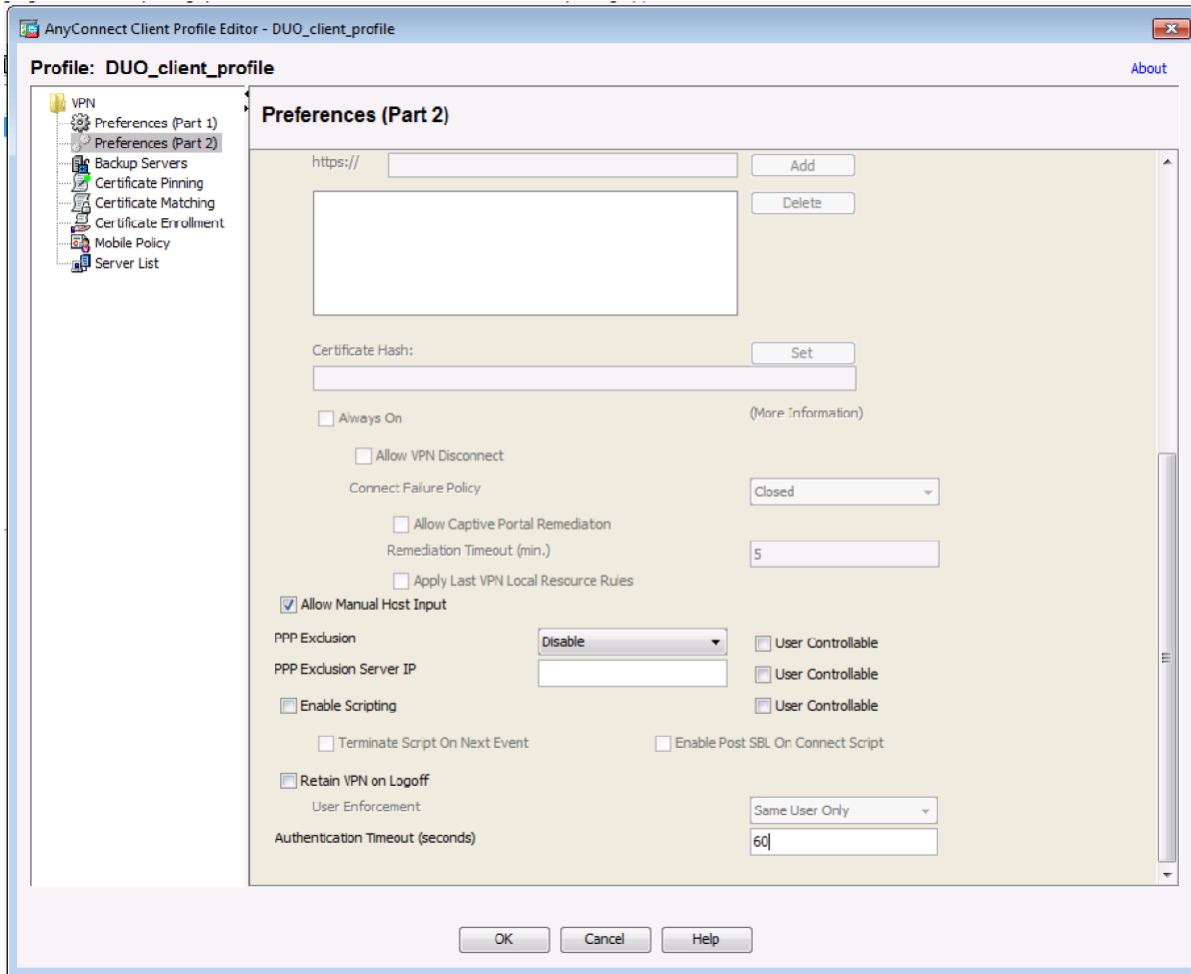
3. DUO 클라이언트 프로필을 편집합니다. 이 단계는 단순히 더 사용자 친화적인 테스트 환경을 만들어 각 테스트 연결이 실제로 오류를 렌더링하지 않고 성공하도록하는 것입니다.

Profile Name	Profile Usage	Group Policy
Duo_client_profile	AnyConnect VPN Profile	GroupPolicy_Duo
DCLLOUD-ANYCONNECT-PROFILE	AnyConnect VPN Profile	DCLLOUD-ANYCONNECT-ISE,DfltGrpP
DCLLOUD-AMP-PROFILE	AMP Enabler Service Profile	DCLLOUD-CLIENTLESS-ANYCONNECT
DCLLOUD-ISE-POSTURE-PROFILE	ISE Posture Profile	DCLLOUD-ANYCONNECT-ISE

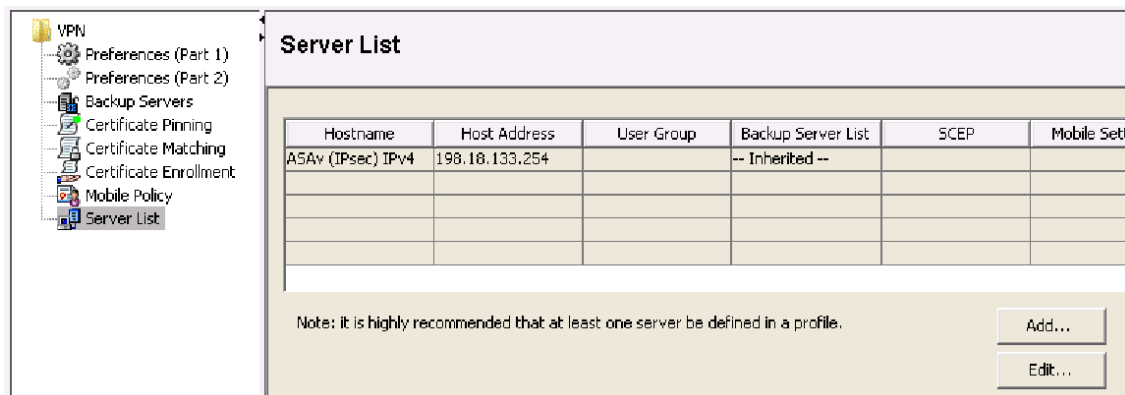
4. **Preferences (Part 1)**을 선택합니다. 그럼 다음, Windows VPN Establishment 아래에서 **Allow Remote Users** 를 선택합니다.



5. **Preferences (Part 2)**를 선택합니다. 그런 다음, 페이지 하단의 **Authentication Timeout**(인증 시간 초과)를 60 초로 조정합니다.

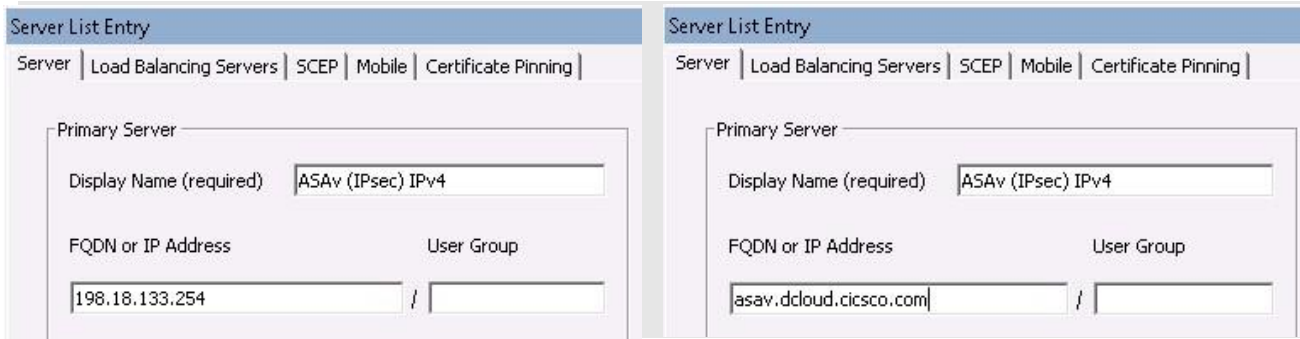


6. **Server List** 를 선택합니다.



7. 목록을 선택하고 **Edit** 를 클릭합니다.

8. IP 주소를 ASA 의 FQDN 으로 변경합니다.



Profile: Duo_client_profile

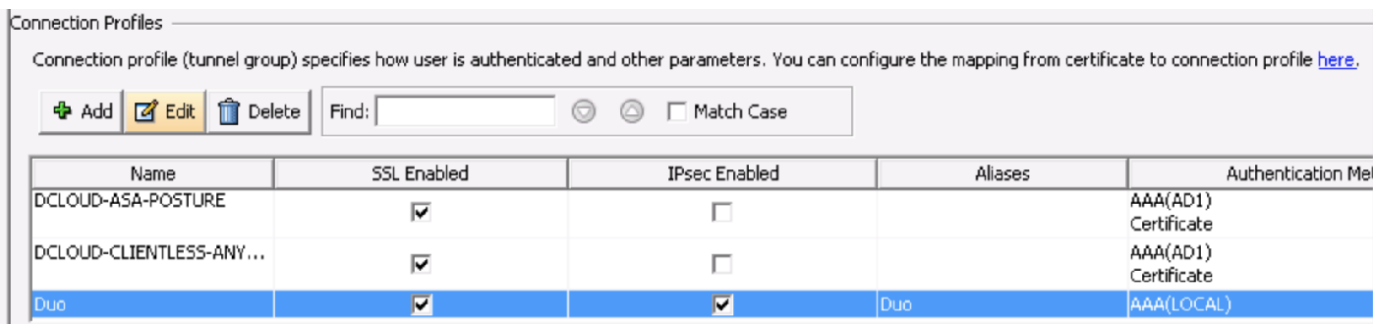
- WPM
- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List

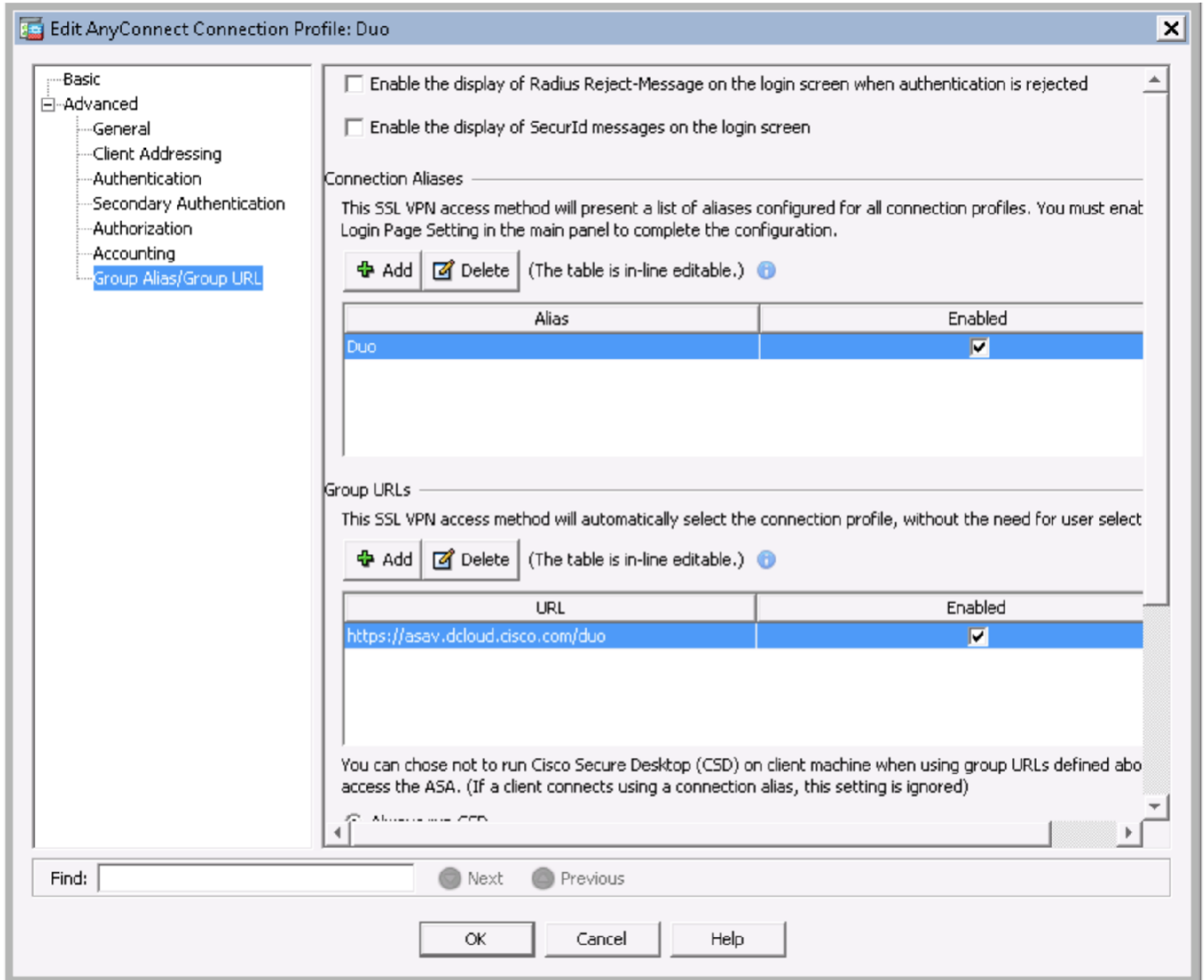
Hostname	Host Address	User Group	Backup Server List
ASAv (IPsec) IPv4	asav.dcloud.cisco...		-- Inherited --

참고: 이 단계는 60 초 제한 시간을 준수하기 위해 필요합니다. ASA 에 FQDN 의 요구 사항에 대해 알려진 버그가 있습니다. 60 초 제한 시간이 없으면 서버는 단 12 초 기본 인증 시간 제한을 계속 사용합니다.

9. **OK** 를 클릭하고 또 다시 **OK** 를 클릭합니다. 그런 다음 **Apply** 를 클릭하고 **Send** 를 누릅니다.
10. **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** 로 이동합니다.



11. **Duo** 라는 새로 생성된 프로파일을 편집합니다.
12. 왼쪽 메뉴에서 **Group Alias/Group URL (Advanced)** 아래에서)을 선택합니다.
13. 이 Connection Profile 에 대한 Group URL (예: https://asav.dcloud.cisco.com/duo)을 추가합니다.



14. **OK** 를 클릭합니다.

15. **Apply** 를 클릭합니다.

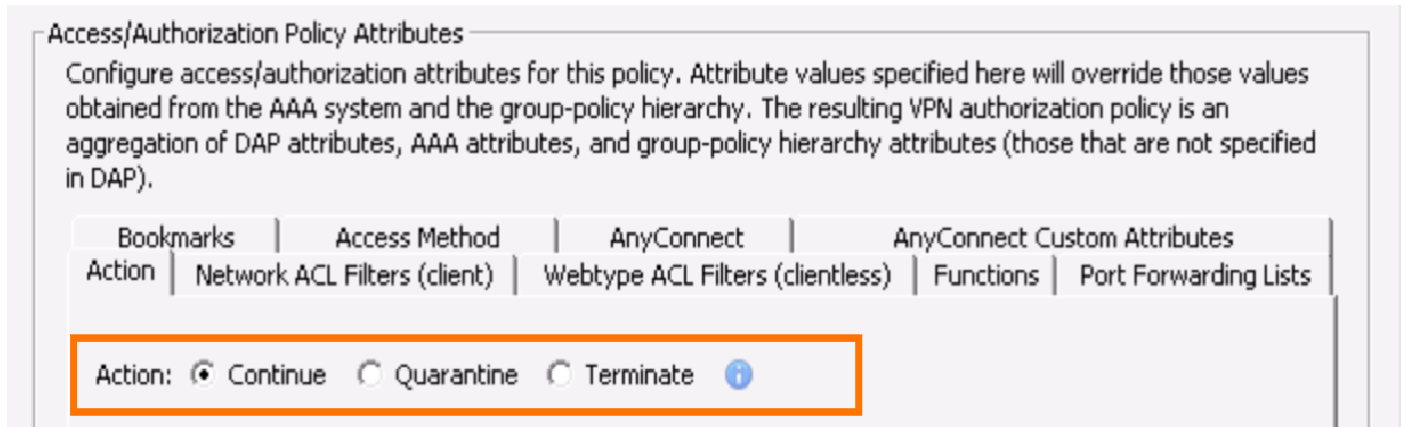
16. **Send** 를 클릭합니다.

참고: IPv6 오류가 발생하면 데모에 영향을 주지 않으므로 무시해도 됩니다.

17. **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies** 로 이동합니다.

18. 기본 액세스 정책인 **DfltAccessPolicy** 를 편집합니다.

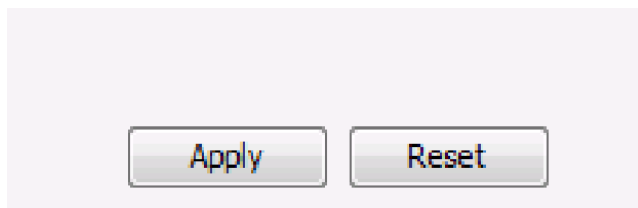
19. Action 을 **Continue** 로 선택합니다.



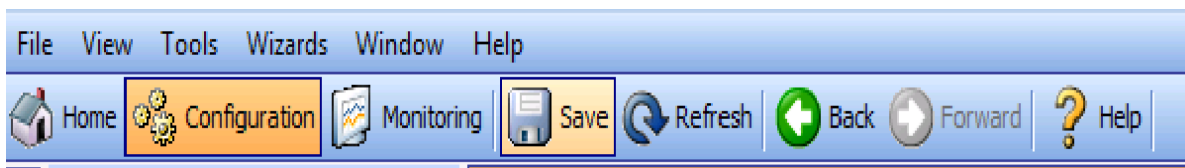
20. **OK** 를 클릭합니다.
21. **Apply** 를 클릭하고 **Send** 를 클릭합니다.
22. **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan Image** 로 이동합니다.
23. **Enable Host Scan/CSD** 확인란 선택 취소합니다.



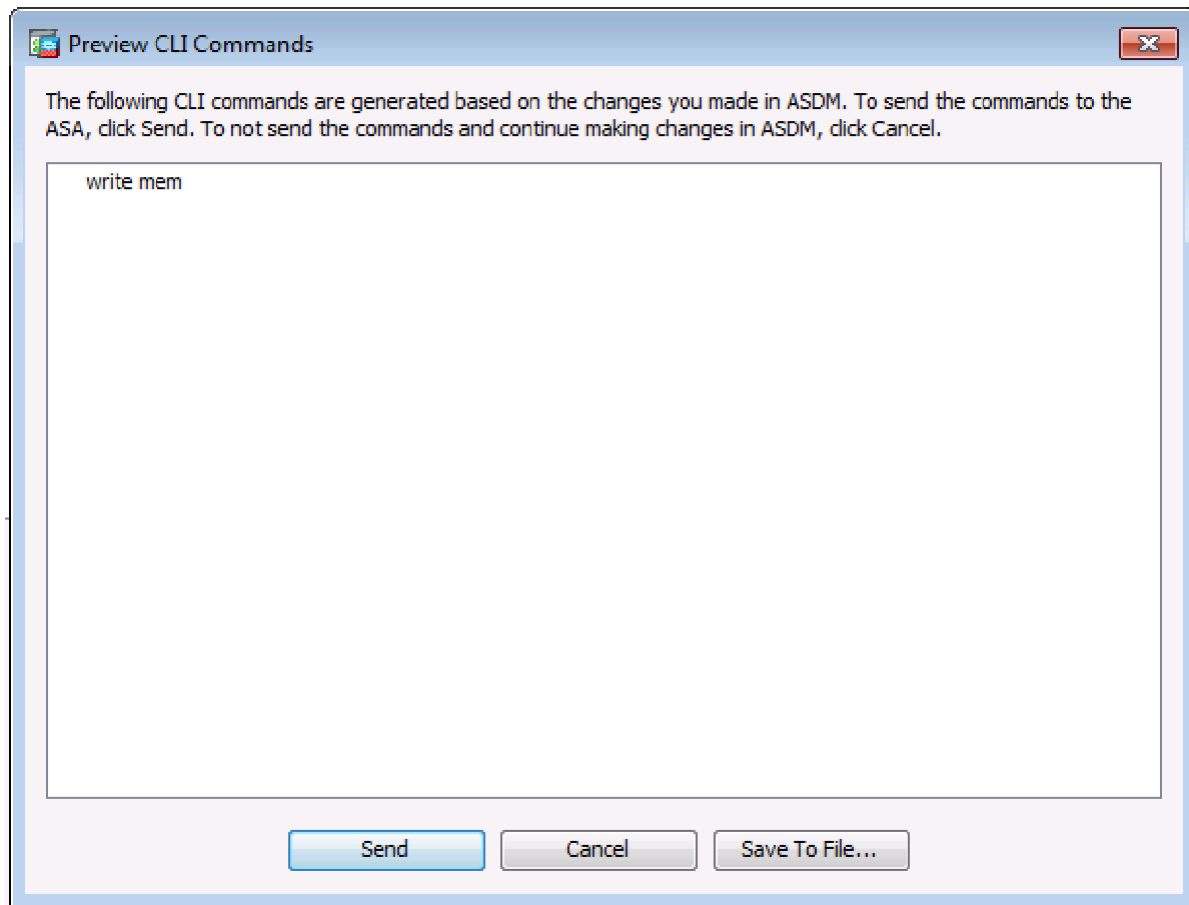
24. **Apply** 를 클릭하고 **Send** 를 클릭합니다.



25. **Save** 를 클릭합니다.



26. **Send** 를 클릭합니다.



시나리오 3: Duo LDAPS Cisco ASA Integration

가치 제안: 이 통합은 ASA 와 Duo Cloud 서비스 간에 LDAPS 연결을 생성합니다. 그런 다음 이 AAA 서버 그룹은 연결 프로파일(터널 그룹)에서 보조 인증 서버(Secondary Authentication Server)로 설정됩니다. 이 통합은 AnyConnect 클라이언트에 두 번째 패스워드(Second Password) 필드를 추가하고 SSLVPN Clientless VPN 포털에 로그인할 때 Duo 인증 프롬프트를 사용할 수 있도록 허용합니다.

스텝

1. **Duo Admin Panel** 에 로그인하여 **Applications** 로 이동합니다.
2. **Protect an Application** 을 클릭하고 애플리케이션 목록에서 **Cisco ASA SSL VPN** 을 찾습니다. **Protect this Application** 을 클릭하고 **integration key**, **secret key**, 및 **API hostname** 을 가져옵니다. (도움말을 위해서는 [Getting Started](#) 를 참고하십시오.)
중요! secret key 를 비밀번호처럼 취급하십시오. Duo 애플리케이션의 보안은 secret key (skey)의 보안과 연결되어 있습니다. 민감한 자격 증명과 마찬가지로 보안을 유지하십시오. 권한이 없는 개인과 공유하거나 어떤 상황에서도 이메일을 보내지 마십시오!
3. 링크를 클릭하여 Duo Admin Panel 의 **Cisco ASA SSL VPN** 애플리케이션 속성 페이지에서 **Duo Cisco package** 를 다운로드하고 데스크탑과 같은 편리한 위치에 압축을 풉니다.



로그인 페이지 수정 (Modify the sign-in page)

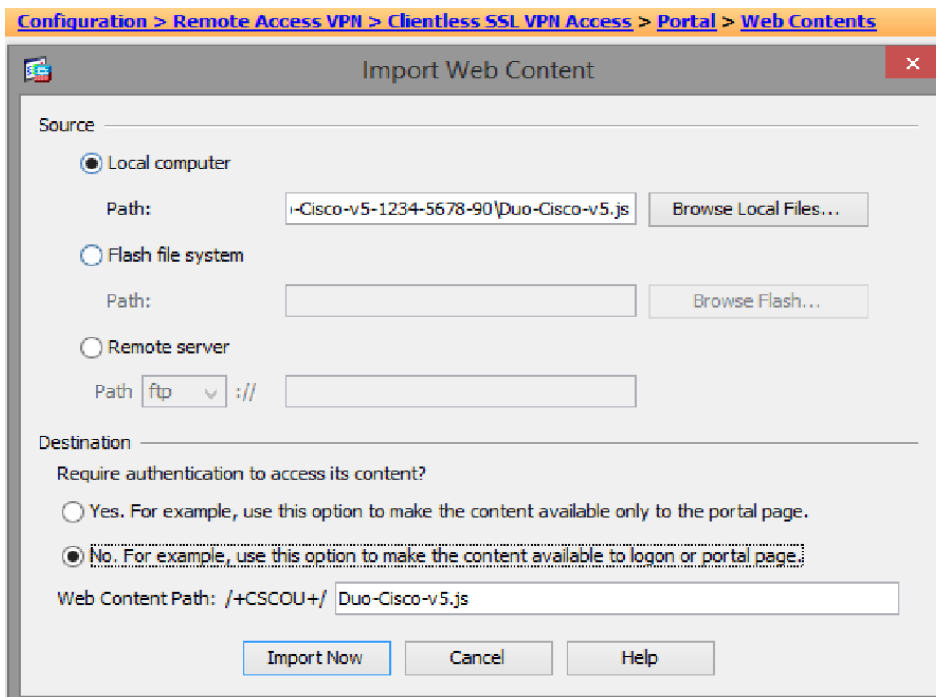
Cisco 로그인 페이지에 Duo 사용자 지정을 추가하려면:

참고: 스텝 1 은 SSLVPN Clientless Portal 에만 영향을 미칩니다. Clientless Portal 로그인 페이지의 Second Password 필드를 Duo Authentication Prompt 로 바꿉니다.

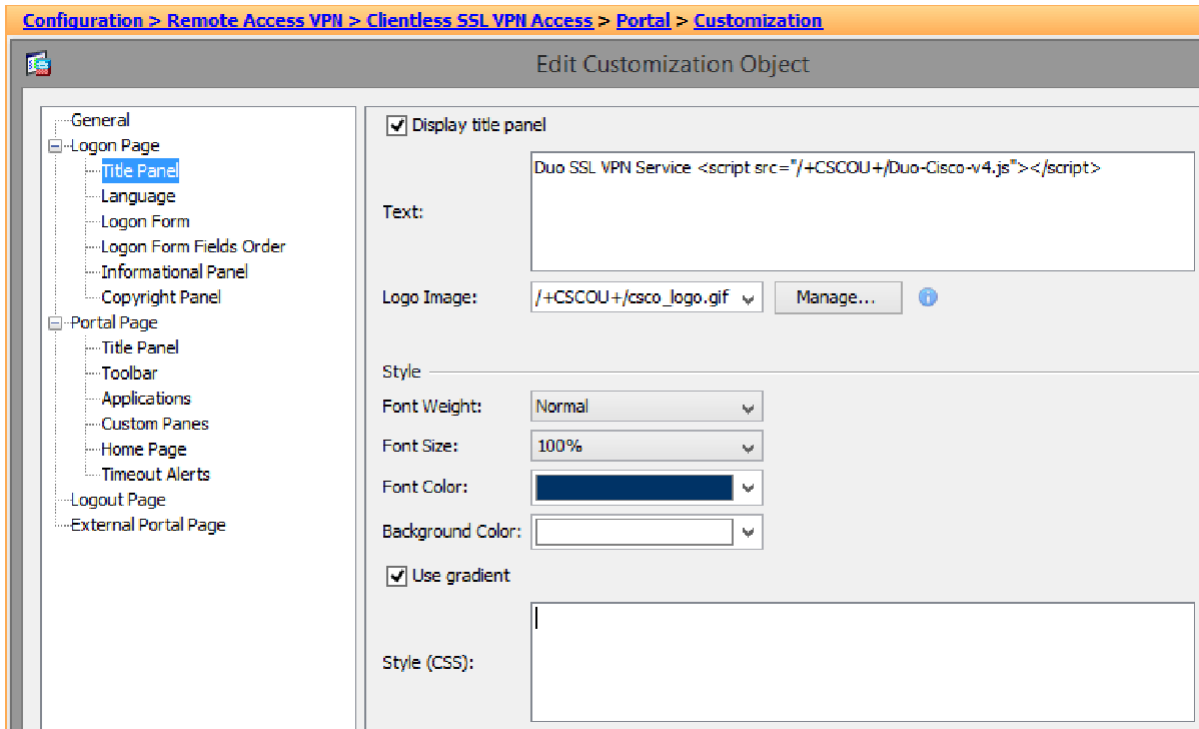
1. Cisco ASA 관리자 웹 인터페이스 (ASDM)에 로그인합니다.
2. **Configuration** 탭을 클릭합니다. 왼쪽 메뉴에서 **Remote Access VPN** 을 클릭합니다.
3. **Clientless SSL VPN Access > Portal > Web Contents** 으로 이동하고 **Import** 를 클릭합니다.
4. **Source** 섹션에서 **Local computer** 를 선택합니다.
5. **Browse Local Files...**를 클릭한 다음에 Duo admin console 에서 이전에 다운로드 한 Duo-Cisco-vX-accountid.zip 파일에서 추출한 Duo-Cisco-vX.js 파일을 찾습니다.

참고: vX 는 Duo Cisco 패키지의 실제 버전을 반영하며 accountid 는 조직의 Duo 계정 ID(Duo Admin Panel 의 Settings 탭에 표시됨), 즉 Duo-Cisco-v5-1234-5678-90.zip 입니다. 파일을 선택하면 Web Content Path 상자에 Duo-Cisco-vX.js 가 나타납니다.

6. **Destination** 섹션에서 "Require authentication to access its content?(컨텐츠에 액세스하려면 인증이 필요합니까?)"에 대한 응답으로 **No** 를 선택하십시오.
7. **Import Now** 를 클릭하고 **OK** 를 클릭합니다.



8. **Clientless SSL VPN Access > Portal>Customization** 으로 이동합니다. 그런 다음 사용자 지정 개체(Customization Object)에서 **DfltCustomization** 을 선택하고 **Edit** 를 클릭합니다.
9. 왼쪽 메뉴에서 **Title Panel (Logon Page** 아래)을 클릭합니다.
10. 그런 다음, **Text** 라는 필드에 `<script src="/+CSCOU+/Duo-Cisco-vX.js"></script>`를 입력합니다 (vX 를 실제로 다운로드한 파일 버전으로 대체). **OK** 를 클릭합니다.

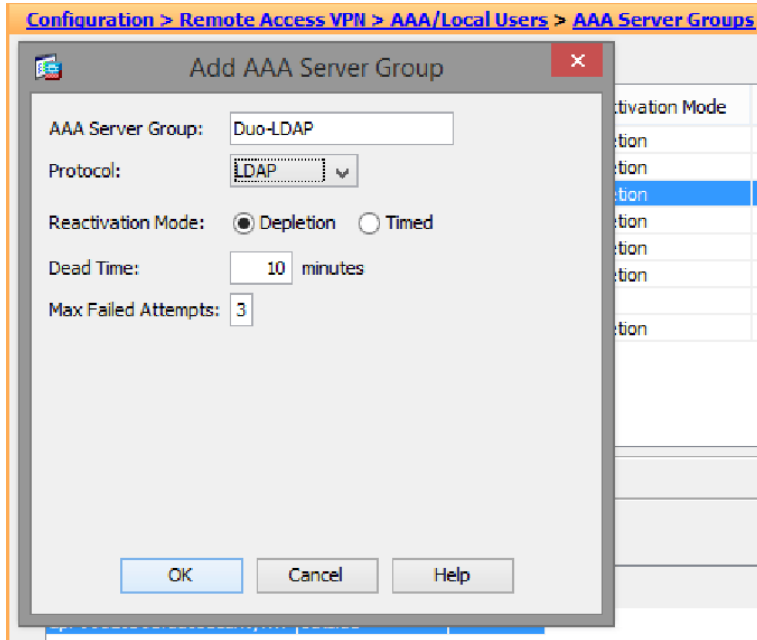


11. **Apply** (적용)을 클릭하고 **Send** 를 누릅니다.

Duo LDAP 서버 추가

1. **AAA/Local Users >AAA Server Groups** 으로 이동합니다. 그런 다음 **Add** 를 클릭하고 양식을 작성하십시오:

AAA Server Group	Duo-LDAP
Protocol	LDAP

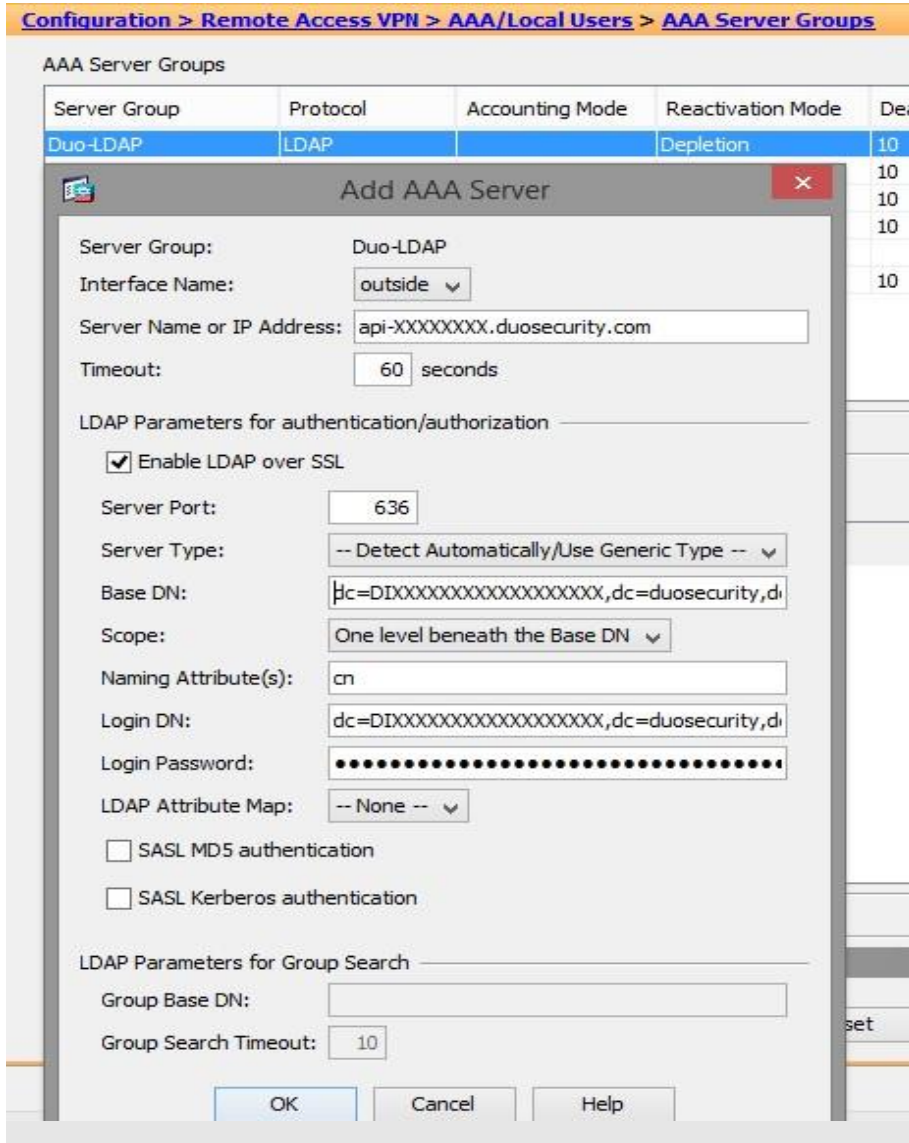


2. **OK** 를 클릭합니다.
3. 방금 추가한 **Duo-LDAP** 그룹을 선택합니다.
4. Selected Group 섹션의 Servers 에서 **Add** 를 클릭하고 다음 양식을 작성하십시오:

Interface Name (인터페이스 이름)	인터넷에 연결된 외부 인터페이스를 선택하십시오. ("outside"라고도 함).
Server Name 또는 IP Address	API hostname (i.e. api-XXXXXXXXX.duosecurity.com)
Timeout	60 초

5. **Enable LDAP over SSL** 를 선택하고 양식을 작성합니다(**INTEGRATION_KEY** 및 **SECRET_KEY** 애플리케이션 별 키로 대체):

Server Port	636
Server Type	-- Detect Automatically/Use Generic Type --
Base DN	dc= INTEGRATION_KEY ,dc=duosecurity,dc=com
Scope	One level beneath the Base DN
Naming Attribute(s)	cn
Login DN	dc= INTEGRATION_KEY ,dc=duosecurity,dc=com
Login Password	SECRET_KEY



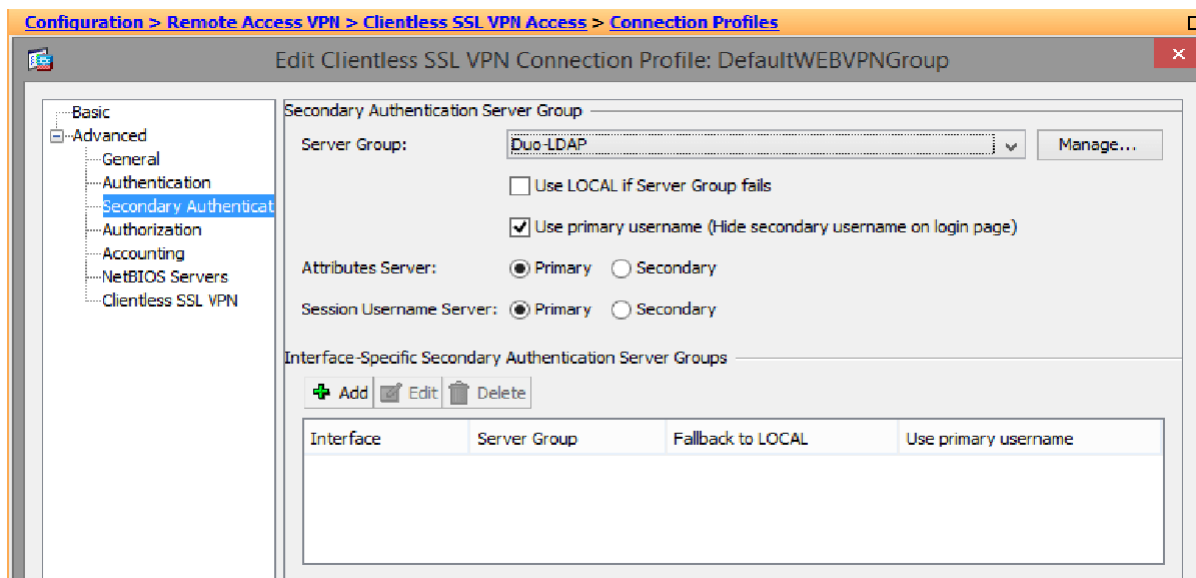
6. **OK** 를 클릭합니다.
7. **Apply** 를 클릭하고 **Send** 를 누릅니다.
8. 이제 Duo LDAP 서버에 대한 연결성을 확인할 수 있습니다. [방금 만든](#) Duo AAA 서버 그룹을 선택하고 **Test** 를 클릭합니다.
9. "Test AAA Server" 양식에서 **Authentication** 을 선택합니다.
10. Duo 에 존재하고 유효한 인증 장치(예: 전화 또는 토큰)가 있는 사용자의 username 을 입력합니다.
11. 사용자의 비밀 번호를 입력하는 대신 해당 사용자에게 유효한 인증 방법(예: **push** 또는 **phone** 또는 패스코드)의 이름을 입력합니다. 그런 다음 **OK** 를 클릭합니다.
12. **push** (푸시) 또는 **phone**(전화)를 입력하면 Duo 인증 요청을 승인합니다.
13. 테스트의 성공 여부를 알려주는 새 양식이 나타납니다.

Duo LDAP 서버 구성

1. **Clientless SSL VPN Access > Connection Profiles** 로 이동합니다.
2. 하단 근처의 연결 프로필을 선택하고 **Edit** 를 클릭합니다 (연결 프로파일은 "DefaultWEBVPNGroup"이라고 할 수 있음).

노트: 이 랩의 경우 위에서 만든 프로파일(이름: Duo)을 선택합니다. 이름이 Duo 인 것 같습니다.

3. 왼쪽 메뉴에서 **Secondary Authentication (Advanced 아래)**을 선택합니다.
4. **Server Group** 목록에서 **Duo-LDAP** 을 선택합니다.
5. **Use LOCAL if Server Group fails** 확인란 선택을 취소합니다.
6. **Use primary username** 확인란을 선택합니다.

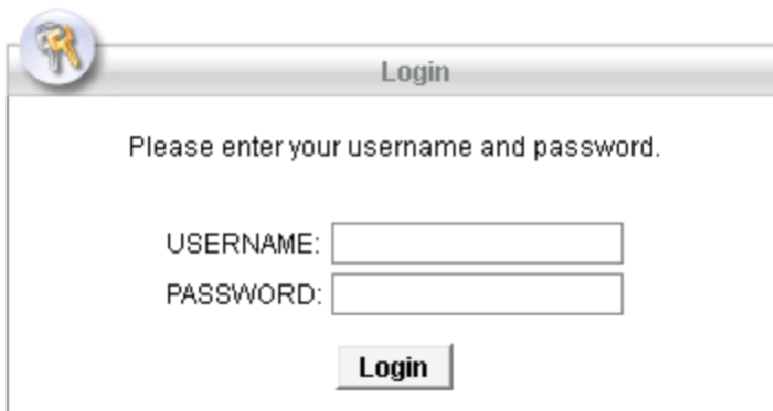


7. **OK** 를 클릭합니다.
8. **Apply** 를 클릭한 다음에 **Send** 를 클릭합니다.

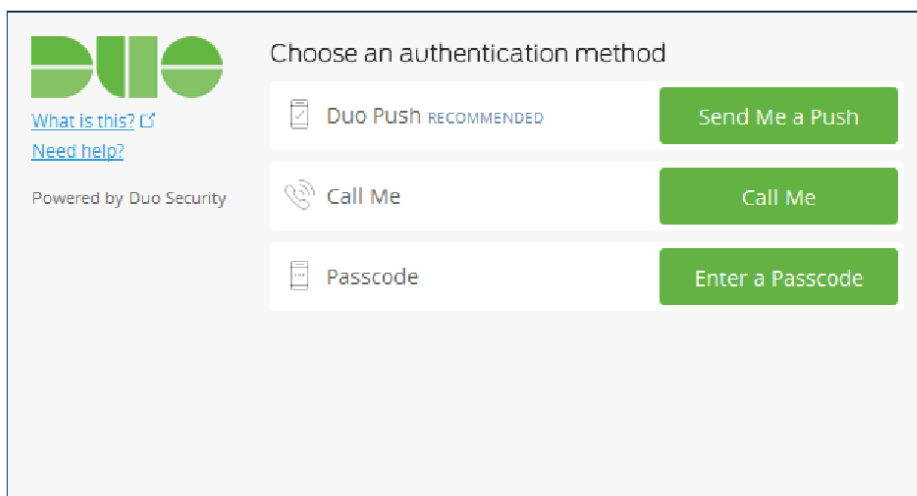
설정 테스트 (Test your setup)

SSLVPN Clientless Portal 를 통해 테스트합니다.

1. Firefox 를 엽니다.
2. 브라우저를 열고 **ASAv** url <https://asav.dcloud.cisco.com/duo> 를 입력합니다.
3. 이전에 구성한 로컬 사용자 이름(username)/ 비밀번호(password)를 입력합니다.



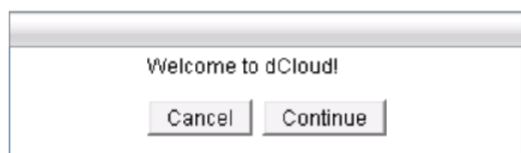
4. **Login** 을 클릭합니다.
5. **Send Me a Push** 를 클릭합니다.



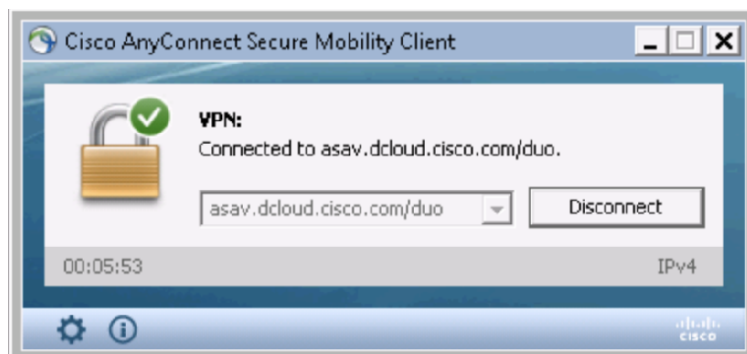
6. 휴대폰에서 **Approve** (승인)을 선택합니다.

Lab Guide

Cisco dCloud

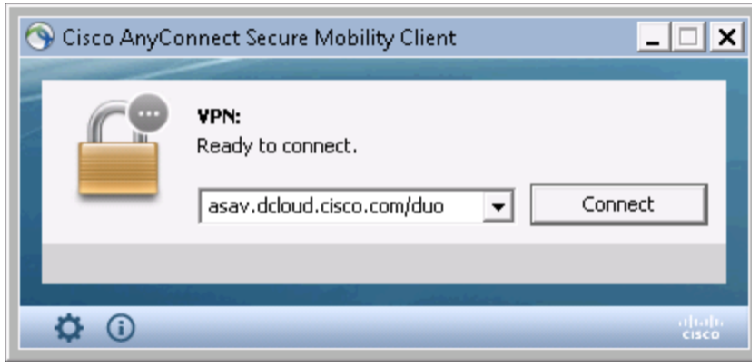


7. **AnyConnect** 를 열고 **Disconnect** 를 클릭합니다.



AnyConnect Client 를 사용하여 테스트

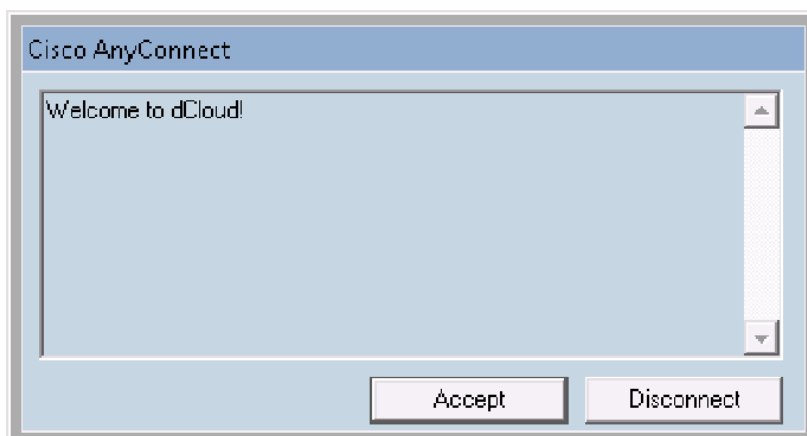
1. AnyConnect 를 엽니다.
2. URL 을 asav.dcloud.cisco.com/duo 로 변경합니다.



3. **Connect** 를 클릭합니다.
4. 이전에 구성한 로컬 사용자 이름(username)/ 비밀번호(password)를 입력합니다.
5. **Second Password** 에는: push, or phone, 또는 패스코드를 입력합니다.
(<https://guide.duo.com/anyconnect>).



6. 휴대폰에서 **Approve** (승인)을 선택합니다.



시나리오 4: Duo RADIUS Cisco ASA Integration

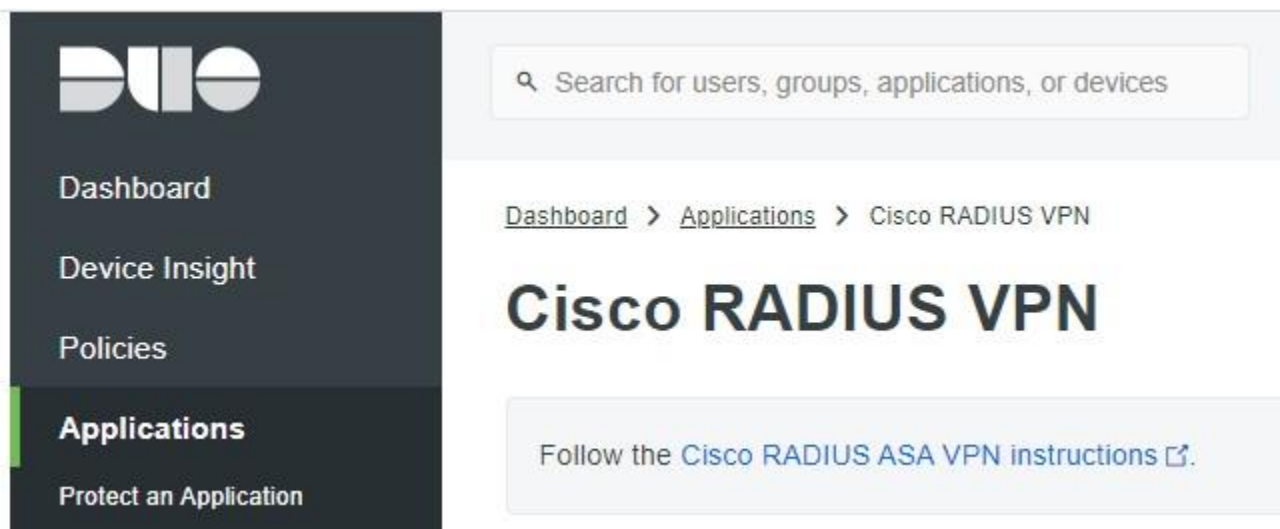
가치 제안: 이 통합은 기본 인증 요청에 따라 인라인으로 배치되는 Duo Authentication Proxy 를 사용합니다. 해당 프록시는 RADIUS AAA 서버 역할을 하고 LDAP 연결을 통해 Active Directory 에 기본 인증을 전달한 다음 Duo Cloud 서비스에 연결하여 보조 인증을 시작합니다. 기본적으로 최종 사용자는 모바일 장치에 자동 Push 기능을 제공받지만 Auth Proxy 의 추가 모드 기능을 사용하여 다른 2FA 를 선택할 수도 있습니다.

스텝

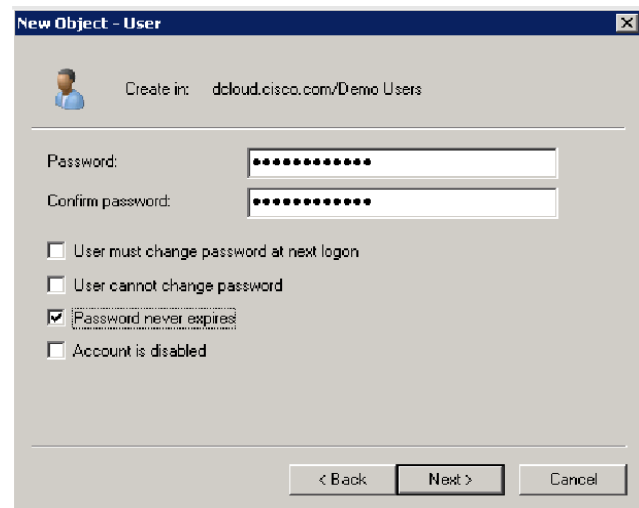
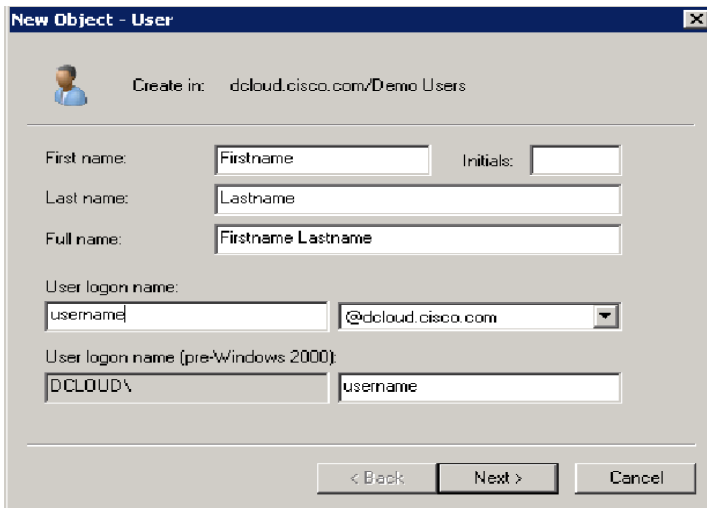
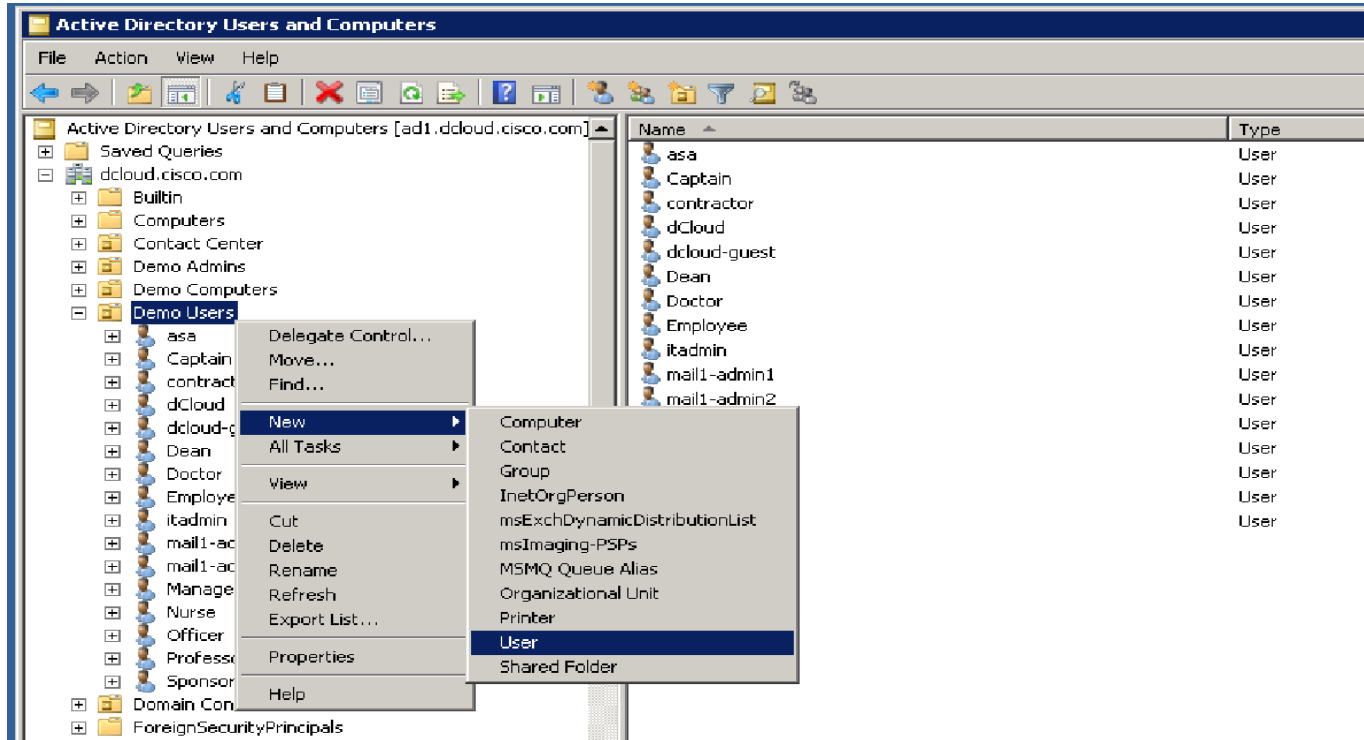
1. Duo Admin Panel 에 로그인하고 **Applications** 로 이동합니다.
2. **Protect an Application** 을 클릭하고 애플리케이션 목록에서 **Cisco RADIUS VPN** 찾습니다.
3. **Protect this Application** 을 클릭하여 **integration key**, **secret key**, 및 **API hostname** 을 가져옵니다. 도움말을 보려면 [Getting Started](#) 를 참조하십시오.

중요! **secret key** 를 비밀번호처럼 취급하십시오.

Duo 애플리케이션의 보안은 secret key (skey)의 보안과 연결되어 있습니다. 민감한 자격 증명과 마찬가지로 보안을 유지하십시오. 권한이 없는 개인과 공유하거나 어떤 상황에서도 이메일을 보내지 마십시오!



4. 데스크톱(Remote Desktop)을 통해 AD1 에 로그인하고 시작(start)을 클릭하고 **Active Directory Users** 및 **컴 Computer** 를 클릭합니다.
5. 사용자 이름 (firstnamelastname)으로 새 데모 사용자를 만듭니다.



6. 이 랩에서는 Duo Authentication Proxy 에서 사용하는 서비스 계정의 **administrator** 계정을 사용합니다. 이것은 최상의 방법은 아니지만 테스트 용도로는 좋습니다. Duo Authentication Proxy 를 설치하려면 dCloud Lab 에서 **scep server** 를 사용합니다.
7. 다음 세부 정보는 Auth Proxy 구성에서 사용되므로 확인해야 합니다:
 - AD 서버의 로컬 IP 주소: **198.19.10.1**
 - AD domain: dcloud.cisco.com
 - ASA 의 내부 IP 주소: **198.19.10.100**
 - scep server 의 IP 주소: **198.19.10.102**
8. <https://duo.com/docs/authproxy-reference#installation> 에서 Duo Authentication Proxy 설치 단계를 따르세요.

Duo Authentication Proxy 설치하기

1. dCloud 의 **scep** 서버에 로그인 합니다.
2. <https://dl.duosecurity.com/duoauthproxy-3.2.4.exe>에서 Windows 용 인증 프록시(Authentication Proxy)를 다운로드합니다. [요기](#)에서 Duo 다운로드 검사 합계(checksum)을 확인하십시오.
3. 관리자 권한이 있는 사용자로 대상 Windows 서버에서 **Authentication Proxy** 설치 프로그램을 시작하고 화면의 지시를 따릅니다.

프록시 구성하기

Duo Authentication Proxy 구성 파일의 이름은 **authproxy.cfg** 이며 프록시 설치의 **conf** subdirectory 에 있습니다. 기본 설치 경로를 사용하는 프록시 구성 파일은 다음 위치에 있습니다.

플랫폼	기본 구성 경로 (Default Configuration Path)
Windows (64-bit)	C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg
Windows (32-bit)	C:\Program Files\Duo Security Authentication Proxy\conf\authproxy.cfg
Linux	/opt/duoauthproxy/conf/authproxy.cfg

Authentication Proxy.cfg 에는 일부 예제 콘텐츠와 함께 기존 **authproxy.cfg** 가 포함될 수 있습니다. 그러나 이러한 지침을 사용하려면 기존 내용을 삭제하고 빈 텍스트 파일로 시작해야 합니다.

참고: Windows 에서 구성 파일을 편집 할 때 Notepad 대신 WordPad 또는 다른 텍스트 편집기를 사용하십시오.

기본 인증자를 위한 프록시 구성 (Configure the Proxy for Your Primary Authenticator)

이 단계에서는 프록시의 기본 인증자(Proxy's primary authenticator)를 설정합니다 (사용자의 기존 패스워드를 검증할 시스템). 대부분의 경우 이는 Active Directory 또는 RADIUS 와 통신하도록 프록시를 구성하는 것을 의미합니다.

<https://duo.com/docs/cisco-alt#configure-the-proxy-for-your-primary-authenticator>

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

Cisco ASA SSL VPN 에 대한 프록시 구성

다음으로 Cisco ASA SSL VPN 과 함께 작동하도록 Authentication Proxy 를 설정합니다. 다음 속성으로 [radius_server_auto] 섹션을 생성합니다: <https://duo.com/docs/cisco-alt#configure-the-proxy-for-your-cisco-asa-ssl-vpn>

```
[radius_server_auto]  
ikey=XXXXXXXXXXXXXXXXXXXXXXXXXXXX  
skey=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
api_host=api-XXXXXXXXXX.duosecurity.com  
radius_ip_1=198.19.10.100  
radius_secret_1=Cisco12345  
failmode=safe  
client=ad_client  
port=1812
```

Proxy 시작하기

1. Windows 서버에서 **Services** 를 엽니다.
2. Duo Security Authentication Proxy Service 를 스크롤합니다.
3. 마우스 오른쪽 버튼을 클릭하고 **Start** 를 선택합니다.

문제 해결 팁: 서비스가 시작되지 않으면 구성 파일에 구문(syntax) 문제가 있을 수 있습니다.

이 문제를 디버깅하려면 다음을 수행합니다:

- (1) Open the Application Event Viewer 를 엽니다.
- (2) 소스 DuoAuthProxy 에서 오류를 찾습니다.

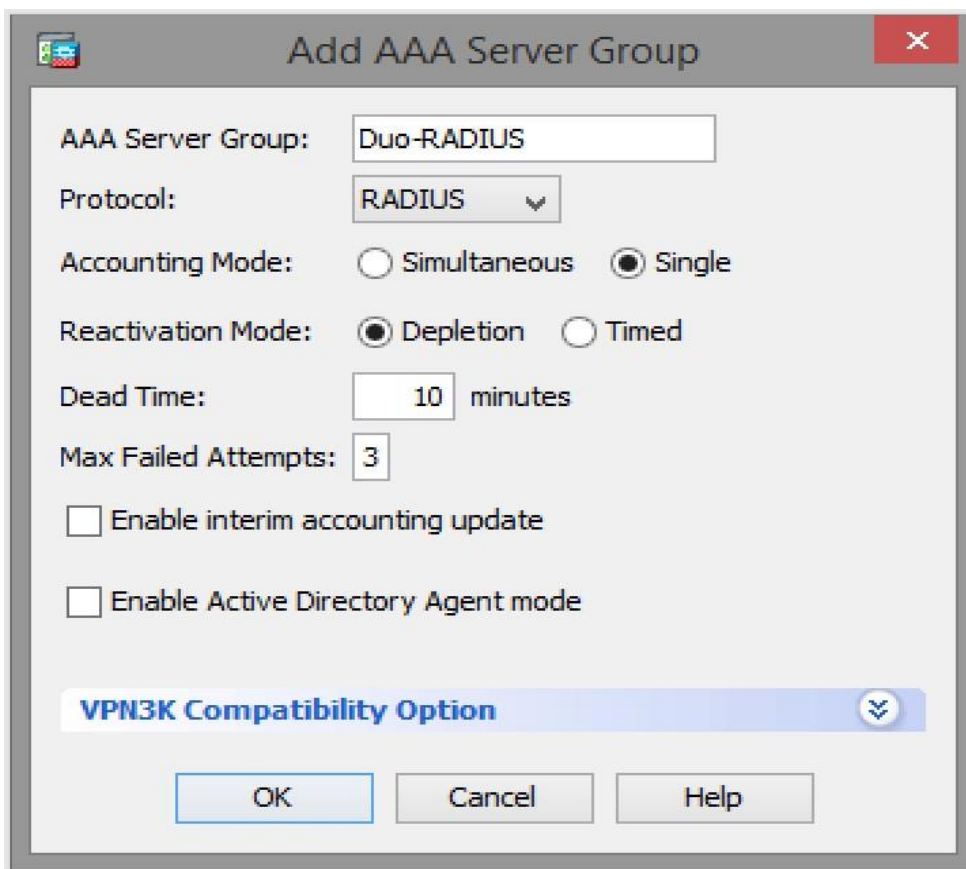
트레이스백(Traceback)에는 문제의 원인을 찾는 데 도움이 되는 "ConfigError"가 포함될 수 있습니다.

Cisco ASA 구성하기

Duo RADIUS 서버 추가

1. **AAA/Local Users > AAA Server Groups** 으로 이동합니다. **Add** 를 클릭하고 양식을 작성하십시오:

설정	가치
AAA Server Group	Duo-RADIUS
Protocol	RADIUS



Add AAA Server Group

AAA Server Group: Duo-RADIUS

Protocol: RADIUS

Accounting Mode: Simultaneous Single

Reactivation Mode: Depletion Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

Enable interim accounting update

Enable Active Directory Agent mode

VPN3K Compatibility Option

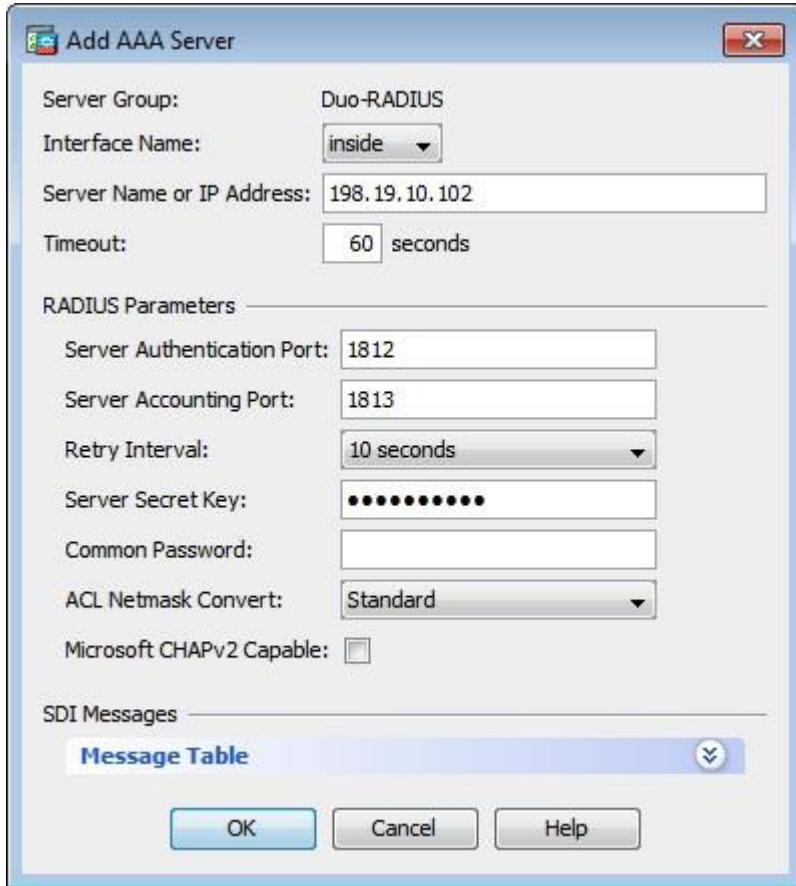
OK Cancel Help

2. **OK** 를 클릭하여 새 AAA 서버 그룹을 만듭니다.

3. 방금 추가한 Duo-RADIUS 그룹을 선택합니다.

4. **Add AAA Server** 대화상자에서 다음 정보를 입력합니다.

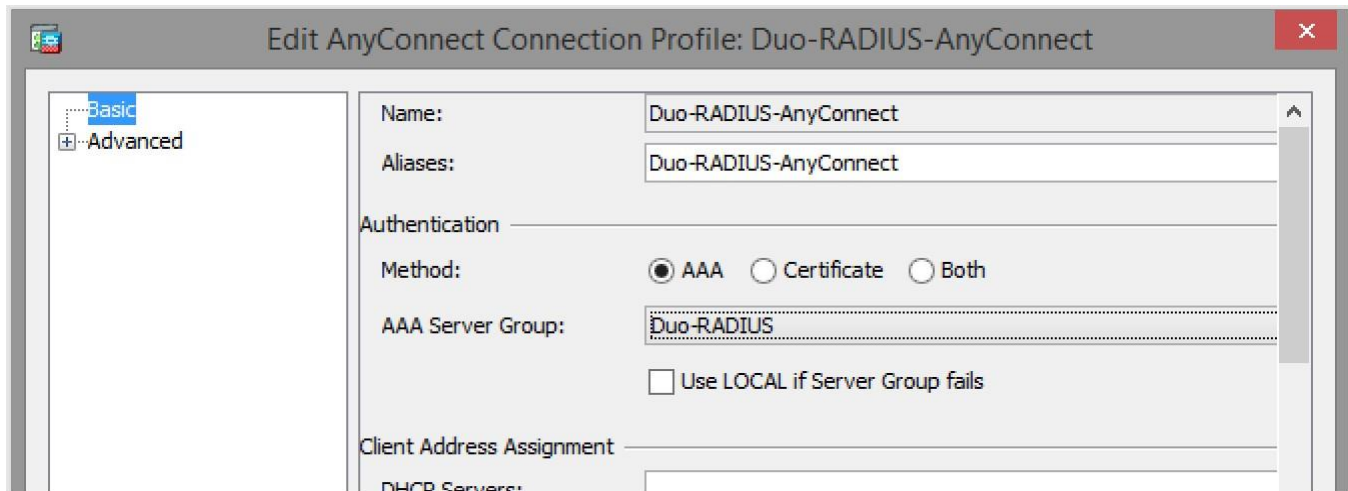
설정	가치
Interface Name (인터페이스 이름)	Duo Authentication Proxy 에 연결할 수 있는 ASA 인터페이스
Server Name 또는 IP Address	Duo Authentication Proxy 의 호스트 이름 또는 IP 주소
Timeout (시간 초과)	인증을 완료하기 위해서는 시간이 60 초면 충분합니다; FAQ 제한 시간에 대한 FAQ 항목을 참조하십시오.
Server Authentication Port	1812 (또는 authproxy.cfg 파일에 지정된 포트)
Server Accounting Port	1813 (Duo Authentication Proxy 는 RADIUS Accounting 을 지원하지 않으므로 기술적으로 이 설정은 중요하지 않습니다.)
Retry Interval (재시도 간격)	10 초
Server Secret Key	Authentication Proxy 구성에 사용되는 공유 Secret
Microsoft CHAPv2 Capable	선택 안 함



5. **OK** 를 클릭하고 또 다시 **OK** 를 클릭해서 새 서버를 저장합니다.
6. 이제 Duo RADIUS 서버에 대한 연결성을 확인할 수 있습니다. 방금 만든 Duo AAA 서버 그룹에서 **Apply** 를 클릭합니다.
7. **Send** 를 클릭하고 **Test** 를 클릭합니다.
8. Test AAA Server 양식에서 Authentication(인증)을 선택합니다.
9. 위에 있는 AD user 의 username (사용자 이름)을 입력합니다.
10. **Password** 필드에 해당 사용자의 비밀 번호를 입력합니다. 사용자에게 token authenticators 만 사용할 수 있는 경우 비밀 번호에 심표를 추가한 다음 패스코드를 추가할 수 있습니다. 예: **password,123456**.
11. **OK** 를 클릭합니다.
12. 사용자가 Duo Push 또는 전화 통화 인증을 설정한 경우 Duo 인증 요청을 승인합니다.
13. 테스트의 성공 여부를 알려주는 새 양식이 나타납니다.

SSL VPN 인증 방법을 Duo 로 변경

1. **Network (Client) Access > AnyConnect Connection Profiles** 로 이동합니다.
2. 2FA(two-factor authentication)을 추가할 연결 프로파일을 선택한 다음 **Edit** 를 클릭합니다.
3. 기본 프로파일 설정 페이지의 **Authentication** 섹션에서 **AAA Server Group** 목록에서 **Duo-RADIUS** 를 선택합니다.
4. **Use LOCAL if Server Group fails** 옵션 확인란을 선택 취소합니다.

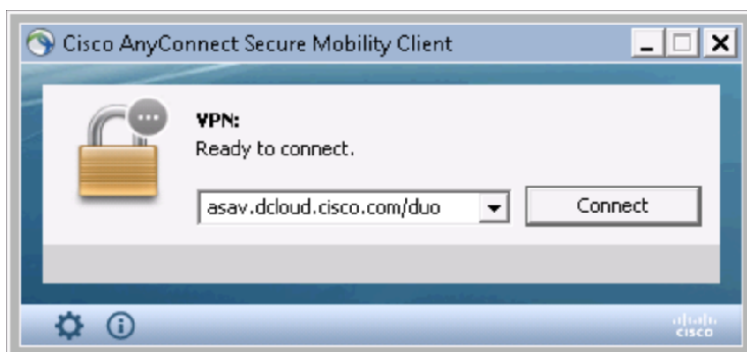


5. 왼쪽 메뉴에서 **Secondary Authentication** (Advanced 아래에)을 선택합니다.
6. **Server Group** 목록에서 -- **None** -- 을 선택합니다. (이렇게하면 위에서 한 기본 통합이 "비활성화"됩니다.)
7. **OK** 를 클릭합니다; 그런 다음 **Apply** 를 클릭하고 **Send** 를 누릅니다.

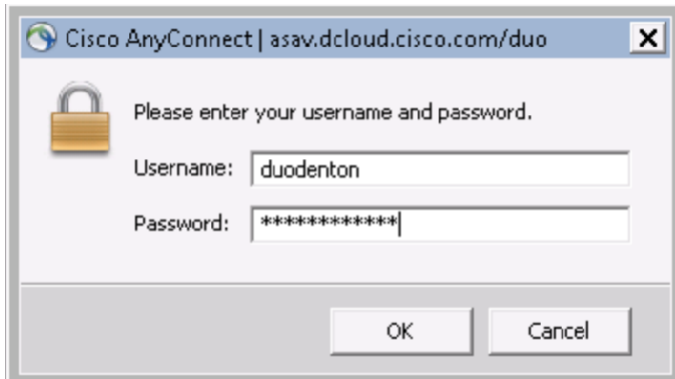
설정 테스트하기

AnyConnect client 시작: Test Auto-Push 테스트

1. URL 를 `asav.dcloud.cisco.com/duo` 로 변경합니다.



2. **Connect** 를 클릭합니다.



3. Active Directory 사용자 이름/ 비밀번호를 입력하십시오.
4. 휴대폰에서 자동 Push 를 수신해야 합니다.
5. Push 를 승인(Approve) 합니다.
6. **Disconnect** 를 누릅니다.

AnyConnect 클라이언트 시작 : 추가 모드(Append-Mode) 테스트

1. URL 을 asav.dcloud.cisco.com/duo 로 변경합니다.
2. **Connect** 를 클릭합니다.
3. Active Directory 사용자 이름을 입력합니다.
4. **Password** 필드에 AD 패스워드와 심표를 차례로 입력한 다음 추가 모드(**Append-Mode**) 옵션을 입력합니다.:
 - a. <password>,phone
 - b. <password>,<Duo Mobile Passcode>

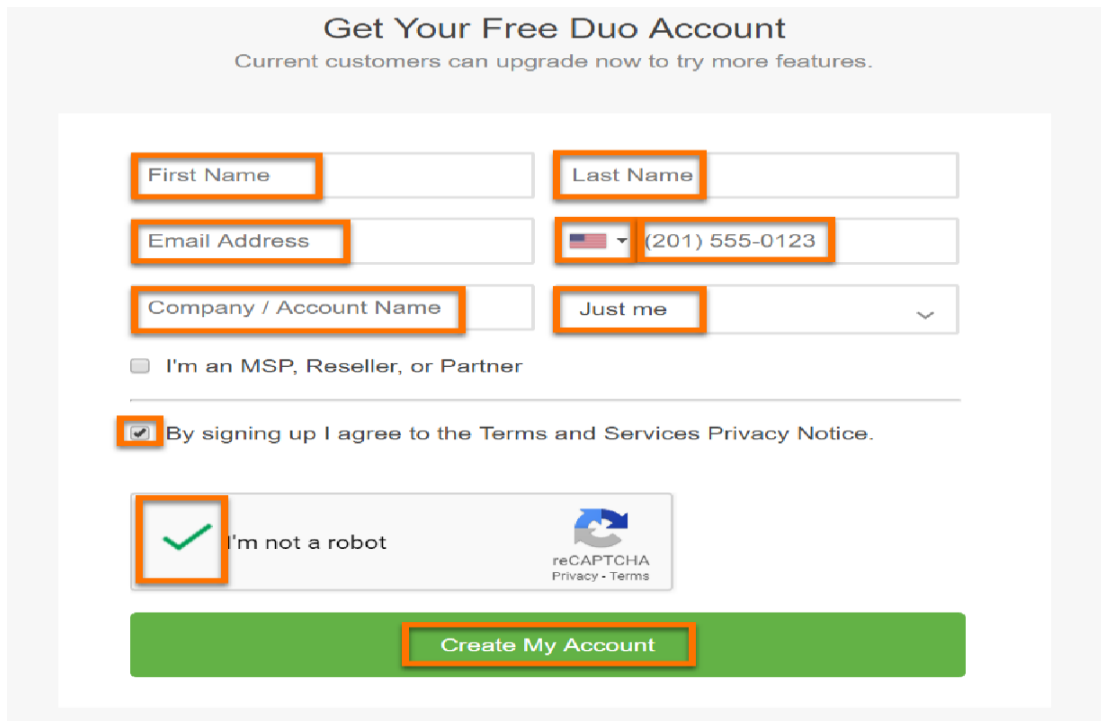
참고: 자세한 내용은 <https://guide.duo.com/append-mode> 을 참조하십시오.
5. 2FA (2-factor Authentication).
6. **Disconnect** 를 누릅니다.

부록 A. Duo 계정에 등록

가치 제안: 이 랩을 완료하려면 Duo 계정과 Duo Mobile 앱이 있어야 합니다. Duo Mobile 은 Duo Security의 모바일 인증 애플리케이션입니다.

스텝

1. 개인 Duo 계정이 없는 경우 <https://signup.duo.com/> 에서 가입하세요.
2. 모든 정보를 입력하고 **Just Me** 를 선택한 다음 **Create My Account** 를 클릭합니다.



Get Your Free Duo Account
Current customers can upgrade now to try more features.

First Name Last Name

Email Address (201) 555-0123

Company / Account Name Just me

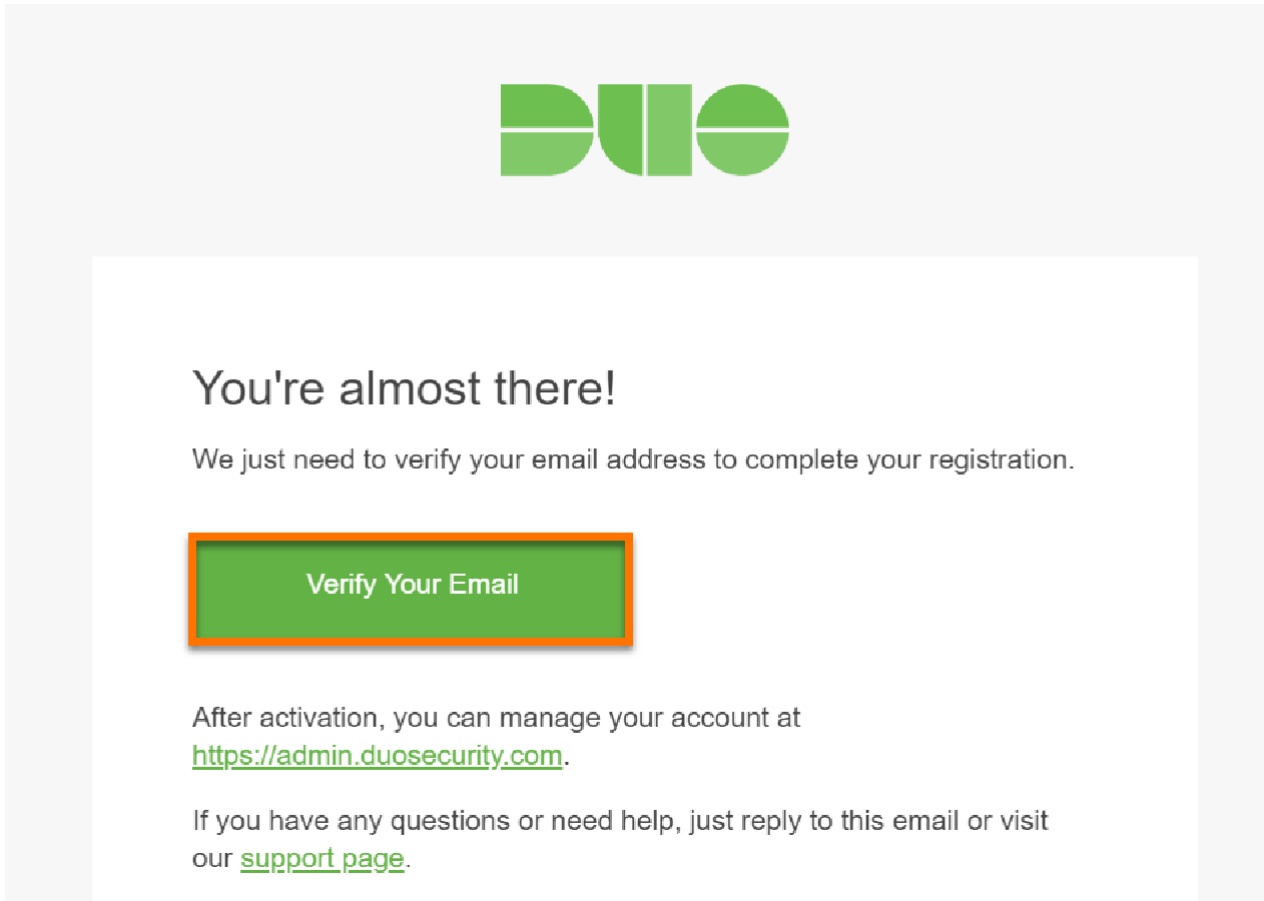
I'm an MSP, Reseller, or Partner

By signing up I agree to the Terms and Services Privacy Notice.

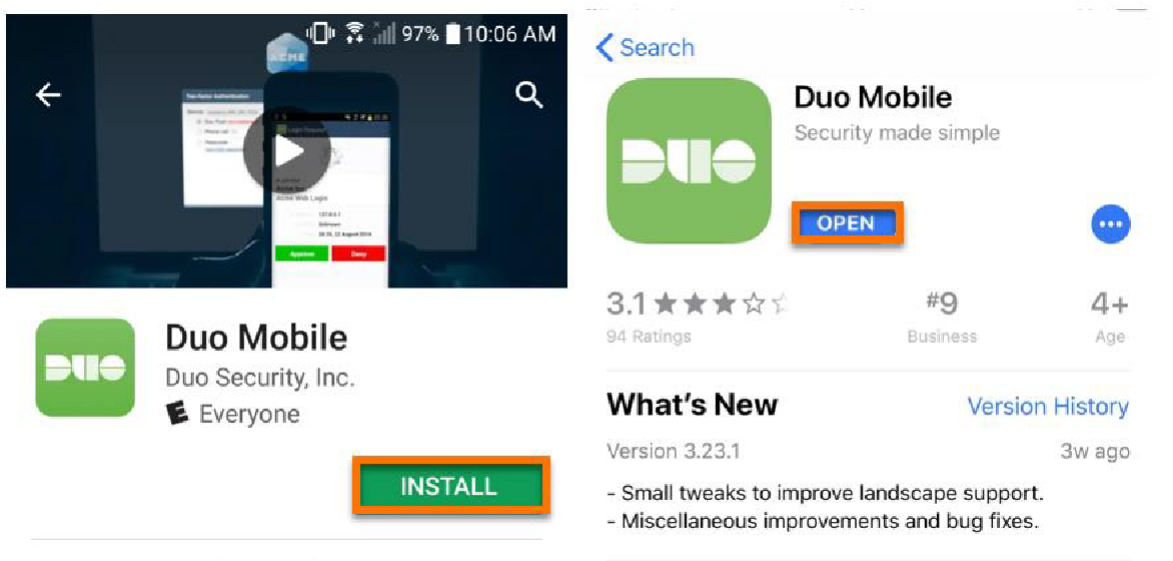
I'm not a robot reCAPTCHA Privacy - Terms

Create My Account

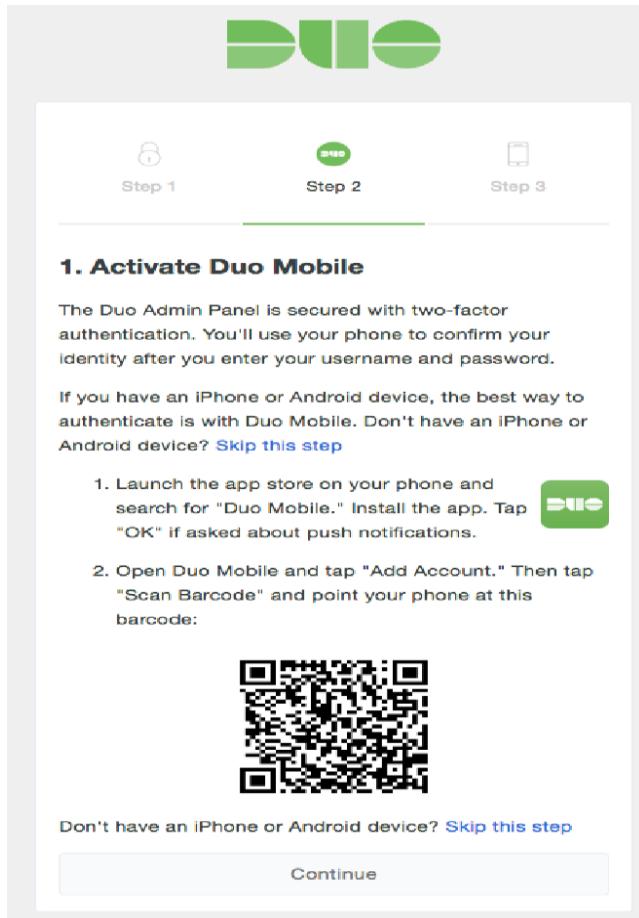
3. 이메일 계정 받은 편지함으로 이동하여 **Welcome to Duo** 이메일을 엽니다. 이메일 확인(Verify Your Email)을 클릭합니다.



- 비밀 번호를 만들려면 최소 12 자를 입력하십시오. 그런 다음 동일한 비밀번호를 다시 입력하고 **Continue** 를 클릭합니다.
- 휴대폰에서 **App Store** 또는 **Play Store** 를 열고 **Duo Mobile** 앱을 검색 한 다음 **Install** 을 탭합니다.
- Duo Mobile 설치가 완료되면 **Open** 을 눌러 휴대폰에서 앱을 시작합니다.

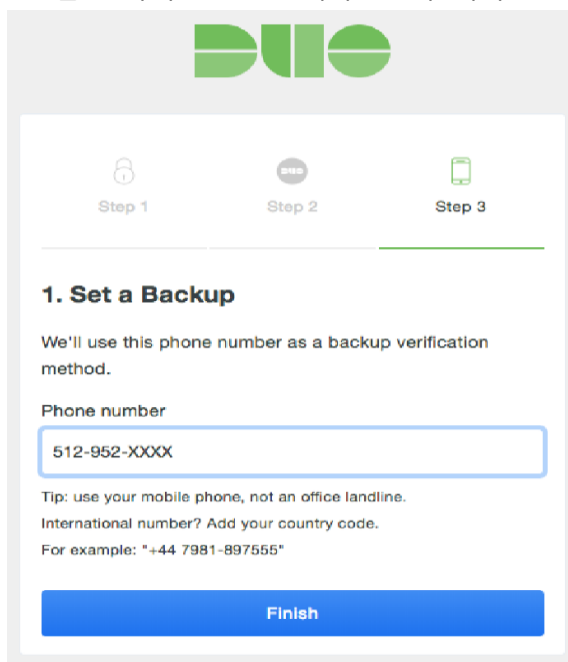


7. 브라우저에서 아래 표시된 단계에 따라 휴대폰에서 Duo Mobile 앱을 활성화(activate)하십시오.



8. 전화 번호를 입력하여 백업 확인 방법을 설정하고 **Finish** 를 클릭합니다.

참고: 국제 번호를 입력하는 경우 국가 코드를 추가하십시오.



부록 B. 추가 리소스

Getting Started: https://duo.com/docs/getting_started

Deploy a POC: <https://duo.com/docs/deploying-a-proof-of-concept>

Duo documentation: <https://duo.com/docs/>

Product editions: <https://duo.com/pricing>

Demos- live and canned: <https://demo.duo.com/>

Deployment Best Practices: <https://duo.com/assets/pdf/Duo-Liftoff-Guide.pdf>

Enrollment Process: <https://duo.com/docs/enrolling-users>

Duo Enrollment Guide: <https://guide.duo.com/enrollment>

End User Guide: <https://guide.duo.com/>

Duo Policy Guide: <https://duo.com/assets/pdf/Duo-Policy-Guide.pdf>

Add a device: <https://guide.duo.com/add-device>



What's Next?

자세한 내용은 [dCloud Community](#) 에서 알아볼 수 있습니다!



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.

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. 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)