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

목차

소개 <u>사전 요구 사항</u> 요구 사항 <u>사용되는 구성 요소</u> 배경 정보 네트워크 다이어그램 및 시나리오 <u>통신 과정</u> <u>Active Directory 구성</u> <u>Duo 구성</u> Duo 인증 프록시 컨피그레이션 Cisco ISE 컨피그레이션 Cisco ASA RADIUS/ISE 컨피그레이션 Cisco ASA Remote Access VPN 구성 <u>테스트</u> 문제 해결 <u>작업 디버그</u>

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 디바 이스는 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 모 든 세부 정보를 만들거나 수집해야 합니다.

주요 값은 다음과 같습니다.

- 도메인 이름. 서버의 도메인 이름입니다. 이 컨피그레이션 가이드에서는 agarciam.cisco가 도 메인 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 서 명하는 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.

=	Recently	added	Windows Server		
	<u> N</u>	lotepad++			
	<u>8</u> 6	uTTYgen		Σ	2
	P	SFTP	Server Manager	Windows PowerShell	Windows PowerShell ISE
	Expand \	· · · · · · · · · · · · · · · · · · ·			
	Most use	d	Nindaur		<u>e</u> e
	Des D	Ouo Authentication Proxy Manager	Administrativ	Task Manager	Control Panel
	e 🔤	ommand Prompt	-	_	
	🤗 s	nipping Tool	Remote	0	
	<u>/</u> v	Vireshark	Desktop	Event Viewer	File Explorer
	🧭 P	aint			
	9 a	oogle Chrome			
	D				
		Duo Security 🗸 🗸			
8	G				
0	S S	ioogle Chrome lew			
¢	N				
\sim	- 1	lotepad++			
H	مر	o 🤅 📮 🗾	🥙 🔼 🚦	•	

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.

Shortcut Tools Administrative Too View Manage	ls				- □ × ~ ()				
ntrol Panel > System and Security > Administra	tive Tools			Active Directory Users and Comp	puters		-		×
ntrol Panel > System and Security > Administra Name Terminal Services Active Directory Administrative Center Active Directory Domains for Windows Po Active Directory Users and Computers Active Directory Sites and Services Active Directory Sites and Services Computer Manager Administration Kit Defragment and Optimize Drives Director Names Administration Kit Defragment and Optimize Drives Director Viewer	tive Tools Date modified 7/16/2016 6:23 AM 7/16/2016 6:29 AM 7/16/2016 6:19 AM 7/16/2016 6:18 AM 7/16/2016 6:18 AM 7/16/2016 6:19 AM 7/16	Type File folder Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut	Size 2 K8 2 K3 2 K3 2 K8 2 K8 2 K8 2 K8 2 K8 2 K8 2 K8 2 K8	Active Directory Users and Comp File Action View Help File Action View Help File Action View Help Active Directory Users and Com Saved Queries Sa	Name Type Aaministro User Aaministro Security Group Consable De. Security Group Donalamin Security Group Donalamin Security Group Domain Co Security Group	Description Built-in account for ad Members in this group c Members of this group Members of this group L. A user account manage Members in this group c DNS Administrators Gro DNS Clients who are permit Designated administrator All workstations and ser All domain controllers i All domain quests	ted to perform dynam	ic updat	× tes on
Group Policy Management Services (IIS) Manager As Construction Services (IIS) Manager As Construction Local Security Policy Microsoft Azure Services COBC One Services	7/16/2016 & 19 AM 7/16/2016 & 19 AM 7/16/2016 & 18 AM 7/16/2016 & 18 AM 7/16/2016 & 19 AM 7/16/2016 & 19 AM	Shortcut Shortcut Shortcut Shortcut Shortcut	2 KB 2 KB 2 KB 2 KB 2 KB 2 KB	< >>	Domain Users Struity Group Domain Users Struity Group DUO-USERS St unity Group duo2 see Enterprise Security Group Enterprise Security Group Enterprise Security Group	All domain guests All domain users Designated administrato Members of this group Members of this group			
	Shortcut Tools View Manage Introl Panel > System and Security > Administrative Too Manage Introl Panel > System and Security > Administrative Terminal Services Active Directory Administrative Center Active Directory Domains and Trusts Active Directory Domains and Trusts Active Directory Stea and Services Active Directory Users and Computers Active Directory Users and Computers Active Directory Users and Computers Composer Services Connection Manager Administration Kit Disk Cleanup Disk Cleanup Disk Cleanup Disk Cleanup Disk Cleanup Store Viewer Score Viewer Scor	Shortcut Tools Administrative Tools View Manage Date modified Introl Panel > System and Security > Administrative Tools Date modified Terminal Services 7/16/2016 623 AM Active Directory Administrative Center 7/16/2016 620 AM Active Directory Domains and Trusts 7/16/2016 621 AM Active Directory Domains and Trusts 7/16/2016 621 AM Active Directory Stess and Services 7/16/2016 619 AM Active Directory Users and Computers 7/16/2016 619 AM Cernfication Values and Computers 7/16/2016 619 AM Compouter Management 7/16/2016 619 AM Connection Manager Administration Kt 7/16/2016 619 AM Disk Cleanup 7/16/2016 619 AM Struct Viewer 7/16/2016 619 AM Microsoft Azure Services 7/16/2016 619 AM	Shortcut Tools Manage Administrative Tools Introl Panel > System and Security > Administrative Tools Date modified Type Introl Panel > System and Security > Administrative Tools Date modified Type Terminal Services 7/16/2016 6/23 AM File folder Active Directory Administrative Center 7/16/2016 6/29 AM Shortcut Active Directory Administrative Center 7/16/2016 6/19 AM Shortcut Active Directory Commiss and Trusts 7/16/2016 6/19 AM Shortcut Active Directory Stess and Services 7/16/2016 6/19 AM Shortcut Active Directory Users and Computers 7/16/2016 6/19 AM Shortcut Compouter Management 7/16/2016 6/18 AM Shortcut Connection Manager Administration Kit 7/16/2016 6/18 AM Shortcut Disk Cleanup 7/16/2016 6/18 AM Shortcut Shortcut Disk Cleanup 7/16/2016 6/19 AM Shortcut Shortcut Disk Cleanup 7/16/2016 6/18 AM Shortcut Shortcut Shortcut Through for Shortcut Through for Shortcut Shortcut Shortcut Through f	Shortcut Tools Manage Administrative Tools Introl Panel > System and Security > Administrative Tools Name Date modified Type Size Terminal Services 7/16/2016 6/23 AM File folder Active Directory Administrative Center 7/16/2016 6/23 AM File folder Active Directory Administrative Center 7/16/2016 6/29 AM Shortcut 2 KB Active Directory Administrative Center 7/16/2016 6/19 AM Shortcut 2 KB Active Directory Joens and Trusts 7/16/2016 6/19 AM Shortcut 2 KB Active Directory Sites and Services 7/16/2016 6/19 AM Shortcut 2 KB Active Directory Users and Computers 7/16/2016 6/19 AM Shortcut 2 KB Computer Management 7/16/2016 6/18 AM Shortcut 2 KB Connection Manager Administration Kit 7/16/2016 6/18 AM Shortcut 2 KB Disk Cleanup 7/16/2016 6/19 AM Shortcut 2 KB Disk Cleanup 7/16/2016 6/18 AM Shortcut 2 KB Disk Cleanup 7/16/2016 6/18 AM Shortcut 2 KB	Shortcut Tools Administrative Tools Manage Active Directory Users and Comp Introl Panel > System and Security > Administrative Tools If active Directory Users and Comp Terminal Services 7/16/2016 6/23 AM File folder Active Directory Administrative Center 7/16/2016 6/29 AM Shortcut 2 KB Active Directory Administrative Center 7/16/2016 6/19 AM Shortcut 2 KB Active Directory Chronis and Trusts 7/16/2016 6/19 AM Shortcut 2 KB Active Directory Sites and Services 7/16/2016 6/19 AM Shortcut 2 KB Active Directory Users and Computers 7/16/2016 6/19 AM Shortcut 2 KB Centification Reviews 7/16/2016 6/19 AM Shortcut 2 KB Computer Management 7/16/2016 6/18 AM Shortcut 2 KB Connection Manager Administration Kit 7/16/2016 6/18 AM Shortcut 2 KB Disk Cleanup 7/16/2016 6/18 AM	Shortcut Tools Administrative Tools View Manage Intel Panel > System and Security > Administrative Tools Name Date modified Terminal Services 716/2016 6:23 AM Active Directory Administrative Centry 716/2016 6:23 AM Active Directory Administrative Centry 716/2016 6:23 AM Active Directory Administrative Centry 716/2016 6:19 AM Active Directory Domain and Trusts 716/2016 6:19 AM Active Directory Users and Computers 716/2016 6:19 AM Active Directory Users and Computers 716/2016 6:19 AM Active Directory Users and Computers 716/2016 6:19 AM Societ Circla Directory Users and Computers 716/2016 6:19 AM Societ Circla Directory Users and Computers 716/2016 6:19 AM Societ Circla Directory Users and Computers 716/2016 6:18 AM Societ Circla Directory Users and Computers 716/2016 6:18 AM Socintry Group 716/2016 6:19 AM <th>Shertcut Roots Administrative Tools View Manage Intel Panel > System and Security > Administrative Tools Terminal Services 716/2016 623 AM Active Directory Users and Computers File Active Directory Users and Computers Active Directory Administrative Center 716/2016 619 AM Active Directory Users and Computers 716/2016 619 AM Social Directory Users and Computers 716/2016 619 AM Active Directory Users and Computers 716/2016 619 AM Social Directory Users and Computers 716/2016 619 AM Social Directory Users and Computers 8 danduo Weed Points Conflored Social So</th> <th>Spectra Tools Administrative Tools Name Date modified Type Size Terminal Services 716/2016 623 AM File folder Active Directory Users and Computers 716/2016 623 AM File folder Active Directory Users and Computers 716/2016 623 AM Shortout 248 Active Directory Users and Computers 716/2016 623 AM Shortout 248 Active Directory Users and Computers 716/2016 619 AM Shortout 248 Active Directory Users and Computers 716/2016 619 AM Shortout 248 Computer Services 716/2016 619 AM Shortout 248 Computer Mindels Administrative Concert 716/2016 619 AM Shortout 248 Computer Mindels Administration Ka 716/2016 619 AM Shortout 248 Computer Mindels Administration Ka 716/2016 619 AM Shortout 248 Computer Mindels Administration Ka 716/2016 619 AM Shortout 248 Computer Mindels Administration Ka 716/2016 619 AM Shortout 248 Data Charaper Administration Ka 716/2016 619 AM Shortout 248 Datak Charape</th> <th>Shertcut Tools Administrative Tools Image Name Date modified Type Size Terminal Services Date modified Type Size Active Directory Administrative Center T/16/2016 6139.AM Shortcut 248 Active Directory Model Gas Minoson Poor T/16/2016 6139.AM Shortcut 248 Active Directory Model Gas Minoson Poor T/16/2016 6139.AM Shortcut 248 Active Directory Model Gas Minoson Poor T/16/2016 6139.AM Shortcut 248 Active Directory Stress and Services T/16/2016 6139.AM Shortcut 248 Active Directory Stress and Services T/16/2016 6139.AM Shortcut 248 Component Services T/16/2016 613.AM Shortcut 248 Disk Centrus T/16/2016 613.AM Shortcut 248 Disk Centrus <</th>	Shertcut Roots Administrative Tools View Manage Intel Panel > System and Security > Administrative Tools Terminal Services 716/2016 623 AM Active Directory Users and Computers File Active Directory Users and Computers Active Directory Administrative Center 716/2016 619 AM Active Directory Users and Computers 716/2016 619 AM Social Directory Users and Computers 716/2016 619 AM Active Directory Users and Computers 716/2016 619 AM Social Directory Users and Computers 716/2016 619 AM Social Directory Users and Computers 8 danduo Weed Points Conflored Social So	Spectra Tools Administrative Tools Name Date modified Type Size Terminal Services 716/2016 623 AM File folder Active Directory Users and Computers 716/2016 623 AM File folder Active Directory Users and Computers 716/2016 623 AM Shortout 248 Active Directory Users and Computers 716/2016 623 AM Shortout 248 Active Directory Users and Computers 716/2016 619 AM Shortout 248 Active Directory Users and Computers 716/2016 619 AM Shortout 248 Computer Services 716/2016 619 AM Shortout 248 Computer Mindels Administrative Concert 716/2016 619 AM Shortout 248 Computer Mindels Administration Ka 716/2016 619 AM Shortout 248 Computer Mindels Administration Ka 716/2016 619 AM Shortout 248 Computer Mindels Administration Ka 716/2016 619 AM Shortout 248 Computer Mindels Administration Ka 716/2016 619 AM Shortout 248 Data Charaper Administration Ka 716/2016 619 AM Shortout 248 Datak Charape	Shertcut Tools Administrative Tools Image Name Date modified Type Size Terminal Services Date modified Type Size Active Directory Administrative Center T/16/2016 6139.AM Shortcut 248 Active Directory Model Gas Minoson Poor T/16/2016 6139.AM Shortcut 248 Active Directory Model Gas Minoson Poor T/16/2016 6139.AM Shortcut 248 Active Directory Model Gas Minoson Poor T/16/2016 6139.AM Shortcut 248 Active Directory Stress and Services T/16/2016 6139.AM Shortcut 248 Active Directory Stress and Services T/16/2016 6139.AM Shortcut 248 Component Services T/16/2016 613.AM Shortcut 248 Disk Centrus T/16/2016 613.AM Shortcut 248 Disk Centrus <

 이미지에 표시된 대로 사용자 폴더를 마우스 오른쪽 버튼으로 클릭하고 신규 > 사용자를 선택합 니다.

Active Directory Users and Com	puters			-	×
File Action View Help					
🗢 🔿 🙍 🚾 🔏 🖬 🗙 🛙	i 🖬 🛃 🚺 🖬	1 🙎 🔌 🛍 🍸 🗕 🐍			
Active Directory Users and Com Saved Queries Saved Queries Saved Queries Builtin Computers Domain Controllers Sim Domain Controllers Managed Service Accour Users Delegate Con Find	Name Administrator agarciam alanad alanduo Allowed RO Cert Publish Cloneable D trol D	Type Description User Built-in accourt User User User Security Group Members in th Security Group Members of th User A user accourt Security Group Members of th	is group c is group c is group is group t t manage is group c		^
New All Tasks View Refresh Export List Properties Help	>	Computer Contact Group InetOrgPerson msDS-KeyCredential msDS-ResourcePropertyList msDS-ShadowPrincipalContainer msImaging-PSPs			
< >> Create a new object	Enterprise Enterprise	MSMQ Queue Alias Printer User			~
		Shared Folder			

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

릭합니다.

New Object - User	×
Create in: agarciam.cisco/Users	0
First name: duovpn Initials:	30
Last name:	
Full name: duovpn	s
	s
User logon name:	s
eagarciam.cisco v	s
User logon name (pre-Windows 2000):	n
AGARCIAM\ duovpn	n
	e
	— st
< Back Next > Cancel	ai
	ai

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

New Object - User	\times
Create in: agarciam.cisco/Users	0
Password:	ac
Confirm password:	
User must change password at next logon	s
User cannot change password	5
Password never expires	c
Account is disabled	s
	n
	e
	st
< Back Next > Canc	el air

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

Active Directory Users and Com	puters			-	×
File Action View Help					
(⇔ ⇒) 2 📰 🔏 🗈 🗙 🗄	1 🗟 🗟 🔽 🗖	1 🗏 🐮 🕯 🦷	7 🧕 💐		
Active Directory Users and Com Saved Queries Saved Queries Builtin Builtin Computers Domain Controllers Sim ForeignSecurityPrincipal: Managed Service Accour Users	Name Administrator agarciam alanad alanduo Allowed RO Cert Publish Cloneable D DefaultAcco DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Co Domain Co Domain Gue Domain Gue Domain Users duo2 R DUO-USERS	Type User User User Security Group Security Group	Description Built-in account for ad Members in this group c Members of this group Members of this group t A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users		
	Linterprise	Copy Add to a group	d administrato		
Allows you to add the selected object	s to a group yc	Disable Account	of this group		*

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

그런 다음 기준과 일치하는 이름을 선택하고 확인을 클릭합니다.

Select Groups	×	
Select this object type:		_
Groups or Built-in security principals	Object Types	ľ
From this location:		:01
agarciam.cisco	Locations	
Enter the object names to select (examples):		
DUO-USERS	Check Names) †
		of t
		of 1
Advanced OK	Cancel	bu
		n t

8. 이 문서에서 예로 사용되는 사용자입니다.

Duo 구성

1. Dudo 관리 포털에 로그인합니다.

Admin Login	
Enter your admin credentials	
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.

	Q Search for users, groups, a	applications, or devices
Dashboard	Dashboard > Users > Add Us	er
Device Insight	Add Usor	
Policies	Add USEI	s to anroll themselves after they complete primary authentication
Applications	Learn more about adding use	ers 🗹
Single Sign-On		
Users ┥	Username	duovpn
Add User		Should match the primary authentication username.
Pending Enrollments		
Bulk Enroll Users		\frown
Import Users	(
Directory Sync		Add User

3. 새 사용자 패널에서 필요한 모든 정보를 빈 칸에 입력합니다.

Policies	Uasnboard > Users > duovpn		
Applications	duovpn		Logs Send Enrollment Email
Single Sign-On			
Users Add User Pending Enroliments Bulk Enroll Users	Username	duovpn	
Directory Sync Bypass Codes	Username aliases	+ Add a username alias Users can have up to 8 aliases.	
Groups		(e.g., Username alias 1 should only be used for Employee ID).	
Endpoints 2FA Devices Trusted Endpoints	Full name	test <u>xpn</u> user	
Trust Monitor	-		
Reports	Email	com	
Settings	Status	Active	
Need Help? Chat with Tech Support C Email Support Call us at 1-855-386-2884 Versioning Core Authentication Service: D235.6 Admin Panel: D255.6		Require multi-factor authentication (default). Bypass Allow users to skip two-factor authentication and log in with only a password. Passwordless. Disabled Automatically deny access This controls the user's two-factor authentication process.	authentication is not skipped.
Read Release Notes C Account ID 2910-6030-53	Groups	You don't have any editable groups. Add one. Groups can be used for management, reporting, and policy. Learn more about groups 🗗	
Deployment ID DUO63 C Helpful Links Documentation C User Guide C Knowledge Base C	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.

Nesse		
rnones ou may rearrange the phones by draggi	ng and dropping in the table. Learn more about activating a replacement phone ⊡.	Add Phone
	This user has no phones. Add one.	
Indpoints		
	This user has no devices.	
lardware 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.	
VebAuthn & U2F		Add Security Key

5. 사용자 전화 번호를 입력하고 전화 추가를 클릭합니다.

Dashboard > Users > duovpn > Add Phone

Add Phone



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

Dashboard	Dashboard > Users						
Device Insight	lleore			Directory	Sync I Import L	Jsers Bulk Fr	roll Users Add User
Policies	03613			,	-,		
Applications	i You have users w	ho have not activated Duo I	Mobile. Click here to send them as	ctivation links.			
Single Sign-On	Need to activate a	a replacement phone? Lear	n more about Reactivating Duo Me	obile 🖆.			
Users 🗲							
Add User	5	0	2	1	0		0
Pending Enrollments	Total Users	Not Enrolled	Inactive Users	Trash	Bypass I	Users	Locked Out
Import Users							
Directory Sync	Select (0) ✓ ····				Export ~	Q Search	
Bypass Codes	Username 🔺	Name	Email	Phones	Tokens	Status	Last Login
Groups							
Endpoints				1		Active	Mar 8, 2022 6:50 PM
2FA Devices	-			1		Active	Mar 5, 2022 7:04 PM
Trusted Endpoints							
Trust Monitor				1		Active	Never authenticated
Reports	duovpn).com	1		Active	Never authenticated
Settings			.com	1		Active	Mar 5, 2022 7:16 PM
Need Help? Chat with Tech Support 🗅							

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 dro	pping in the table. L	earn more about activating a rej	placement phone ⊡.		Add Phone
Alias	Device	Platform	Model	Security Warnings		
phone1	1000	Android 10	1.00 × 10	✓ No warnings	Activate Duo Mobile	Ē

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

Dashboard Device Insight Policies Applications Single Sign-On Users Groups Phone Phone Phone Phone Phone Phone Phone Phone Phone Phone Phone Phone P		 Search for users, groups, applications, or devices
Applications This form allows you to generate a new activation code for this phone's Duo Mobile applimobile device or authenticate via Duo Push. Single Sign-On Note: Generating an activation code will invalidate any existing Duo Mobile credentials for the second s	Dashboard Device Insight Policies	Activate Duo Mobile
Groups Phone Endpoints	Applications Single Sign-On Users	This form allows you to generate a new activation code for this phone's Duo Mobile appli mobile device or authenticate via Duo Push. Note: Generating an activation code will invalidate any existing Duo Mobile credentials for
	Groups Endpoints	Phone
2FA Devices Expiration 24 hours after generation Phones Hardware Tokens WebAuthn & U2F Generate Duo Mobile Activation Code	2FA Devices Phones Hardware Tokens WebAuthn & U2F	Expiration 24 hours after generation Generate Duo Mobile Activation Code

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

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allow: mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the r

Phone	a di ka 1760 Mili 1966.
Send links via	SMS Email
Email	ag i miner line vers a ver

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 + r copy and paste it into Duo Mobile manually:

If you're not reading this from +



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-reference에서 Duo Auth Proxy Manager를 다운로드하여 <u>설치합</u> <u>니다.</u>

✤ 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.

DUO	Q Search for users, groups, applications, or devices		Cisco ID: 314 8-6008-65 alan	Ŷ
Dashboard Device Insight Policies	Applications		Protect an Application	
Applications	_		X	
Single Sign-On	Manage your update to the new Universal Prompt experience, all in one place.		×	
Groups	Get Started Get More Information			
Endpoints				
2FA Devices			O Search	
Trusted Endpoints		EX	C Search	

3. 검색 표시줄에서 Cisco ISE Radius를 찾습니다.

Protect an Application

0	Add an application that you'd like to protect with Duo two-factor You can start with a small "proof-of-concept" installation — it to Documentation: Getting Started C Choose an application below to get started.	or authentication. akes just a few minutes, and y	rou're the only one that will see it, until you decide to add others.
isel Applica	tion	Protection Type	
Cakamai	Akamai Enterprise Application Access	2FA	Documentation E [*] Protect
altalta cisco	Cisco ISE RADIUS	2FA	Documentation C Protect

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

Successfully added Cisco ISE RADIUS to protected applications. Add another.

Dashboard > Applications > Cisco ISE RADIUS 1

Cisco ISE RADIUS 1

Follow the Cisco ISE RADIUS instructions ⊡.

Details

~

Integration key	5.00040a.00001/10120a.047	Сору
Secret key	•••••W6ho	Сору
	Don't write down your secret key or share it with an	yone.
API hostname	(24.3 0/00 / 2010/00/14/0 / 14/5 2017 /	Сору

5. Duo Authentication Proxy Manager 애플리케이션을 실행하고 Active Directory 클라이언트와 ISE Radius 서버 모두에 대한 컨피그레이션을 완료한 후 Validate(검증)를 클릭합니다.

참고: 검증에 성공하지 못한 경우 자세한 내용은 디버그 탭을 참조하고 그에 따라 수정하십시 오.

Duo Authentication Proxy Manager		- 🗆 X
Authentication Proxy is running Up since: 3/5/2022, 9:2:	3:04 AM AM	0 Restart Service Stop Service
Validation passed Configuration has passed validation and is ready to be saved	←	
Configure: authproxy.cfg	Unsaved Changes Output	
<pre>18 ; number to the section name (e.g. [ad_client2]) 19 20 [ad_client] 21 host=10.28.17.107 22 service_account_username=Administrator 23 service_account_password= HEAMTLATL 24 search_dn=DC=agarciam,DC=cisco 25 26 [radius_server_auto] 27 ikey=Umptrimit_HATMINLC? 28 skey=K0n07rtBjAZD1HTTp77i6A165arh1V2paper/Cdg 29 api_host=aji_0fT047B0.cUmptrumityAtcm 30 radius_ip_1=10.28.17.101 31 radius_secret_1=Wmxmph117! 32 failmode=safe 33 client=ad_client 34 port=1812 35 36 Validate Save</pre>	Running [info] [info] [info] [info] [info] [info] [info] [info] [info]	The Duo Authentication Proxy Connectivity Tool. This may take several minutes Testing section 'main' with configuration: {'debug': 'True', 'log_max_files': '10', 'log_max_size': '20971520', 'test_connectivity_on_startup': 'true'} There are no configuration problems
Validate		Learn how to configure the Authentication Proxy

Cisco ISE 컨피그레이션

1. ISE 관리 포털에 로그인합니다.

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

Cisco ISE -	Q What page are you looking	lor?			
Dashboard	Context Visibility Operations		-Policy-	Administration	
Recent Pages External Identity Sources Policy Sets Network Device Profiles External RADIUS Servers RADIUS Server Sequences	System Deployment Licensing Certificates Logging		Network Resources Network Devices Network Device Croups Network Device Profiles		
Live Logs	Maintenance Upgrade Health Checks Backup & Restore		RADIUS Server Sequences NAC Managers External MDM Location Services		

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

■ Cisco ISE		Administration · Network Resources					
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences			
External R	ADIUS Servers		1				
C Edit + Add	🗍 Duplicate 🍵 Delete						
Name Name:	Currently Sorted	Description					

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

Network Devices Networ	rk Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	More
* Name	DUO_NEW						
Description			E				
* Host IP	10.28.17.107						
* Shared Secret	······· -	Show					
Enable KeyWrap	0						
* Key Encryption Key		Show					
* Message Authenticator Code Key		Show					
Key Input Format	• ASCII O HEXADE	CIMAL					
* Authentication Port	1812	(Valid Range 1 to 6	65535)				
* Accounting Port	1813	(Valid Range 1 to 6	65535)				
* Server Timeout	5	Seconds (Valid Ra	ange 1 to 120)				
* Connection Attempts	3	(Valid Range 1 to	9)				
Radius ProxyFailover Expiration	300	(i)(valid Range 1	to 600)				

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

≡ Cisco ISE	Administration • Network Resources					
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				1		

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

RADIUS Server Sequences List > New RADIUS Server Sequence

RADIUS Server Sequence



✓ 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



7. 대시보드 메뉴에서 정책으로 이동하고 정책 세트를 클릭합니다.



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

Policy S	Sets					Reset	t Policyset Hi	count
÷ :	Status	Policy Set Name	Description	Con	nditions	Allowed Protocols / Serv	er Sequence	Hits
Q	Search							
	0	87.979		1	Radius-User-Name EQUALS Isevpn	Default Network Access	<u> </u>	3
	0	1 1		Ð	Radius-NAS-Port-Type EQUALS Virtual	DUO_Sequence	<u>∞</u> +	22
	0	Default	Default policy set		>	Default Network Access	⊠ ^ +	0
		T				<u>=q</u>		
		1				Allowed Protocols		eset
						Default Network Ac	cess	
						Proxy Sequence		
						DUO_Sequence)	

Cisco ASA RADIUS/ISE 컨피그레이션

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

o t avi	Home Configuration Monitoring Save Device Liss Bookmarks Bookmarks bookmark a page, right-click on a node in the agation tree and select "Add to bookmarks".	Refresh Ba AAA Server Group Server Group ISE LOCAL ad-agarciam	ack () ation : ips Pro RA LO
0	O O Device Management		
>	Management Access		
>	8 Licensing		
>	System Image/Configuration		
>	High Availability and Scalability		
>	Logging	Find:	
	Smart Call-Home		
	Security	Servers in the Se	elected
	Service Module Settings	Server Name or IP	Addres
0	W Users/AAA	10.28.17.101	Addie:
	AAA Server Groups		
	Se LDAP Attribute Map		
	🔓 AAA Kerberos		
	Authentication Prompt		
	📭 AAA Access		
	Dynamic Access Policies		
	🐨 User Accounts		
	A Password Policy		
	🚮 Change My Password		
	Login History		
>	Certificate Management		
>	P DHCP		
	B DNS		
>	MATERIA CONTRACTOR AND A DESCRIPTION OF A		

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 번 역 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.