FMC 관리 액세스를 위한 듀오 2단계 인증 구성

목	차
---	---

<u>소개</u>
<u>사전 요구 사항</u>
<u>요구 사항</u>
사용되는 구성 요소
<u>배경 정보</u>
<u>인증 흐름</u>
<u>인증 흐름 설명</u>
<u>구성</u>
<u>FMC의 컨피그레이션 단계</u>
<u>ISE의 컨피그레이션 단계</u>
<u>Duo 관리 포털의 컨피그레이션 단계</u>
<u>다음을 확인합니다.</u>
<u>문제 해결</u>
<u>관련 정보</u>

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. 외 부 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.

Overview Ana	alysis Pol	icies Devices	Objects AMP Inte	elligence						Deploy	. 0, 1	System	Help 🔻	admin 🔻
					Configuration	Users	Domains	Integration	Updates	Licenses v	Health •	Mon	nitoring 🔻	Tools v
Users Use	er Roles	External Authe	intication											
			External Authentic Authentication Method Name * Description Primary Server Host Name/IP Address * Port *	AADIUS C RADIUS C DuoAuthProxy 10.106.44.177 1812		ex. I	P or hostname							
			RADIUS Secret Key Backup Server (Op Host Name/IP Address Port RADIUS Secret Key	••••• tional) 1812		ex. I	P or hostname							
			RADIUS-Specific P Timeout (Seconds) Retries Access Admin Administrator	30 3 3										

Save and Apply를 클릭합니다. 그림과 같이 경고를 무시합니다.

Overvie	w Analysis	Policies	Devices	Objects	AMP	Intelligence							Deplo	vy 🍕	System	Help ¥	admin 🔻
								Configuration	Users	Domains	Integration	Updates	Licenses *	Health	 Mor 	itoring 🔻	Tools •
							One or more en don't have defin	abled external auther ed user roles.	itication obje	cts							
Users	User Roles	External	Authentic	ation													
														🔚 Save	😫 Cance	I 📝 Sar	ve and Apply
Default Use	Role: None			Shell Authenti	cation D	isabled	0							•	Add Extern	al Authenti	cation Object
Name														Meth	od E	nabled	
1. DuoAu	hProxy													RADI	us (10	/ 8

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	cpiplani			
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 Access Admin Network Admin Maintenance User Discovery Admin Threat Intelligence Director (TID) User 			

1단계. Duo 인증 프록시 서버를 다운로드하고 설치합니다.

Windows 시스템에 로그인하고 <u>Duo 인증 프록시 서버</u> 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_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)으 로 이동합니다. 그런 다음 이미지에 표시된 대로 RADIUS 인증 애플리케이션을 선택합니다.

RADIUS

See the RADIUS documentation I to integrate Duo into your RADIUS-enabled platform.

Details



통합 키 = ikey

비밀 키 = skey

API 호스트 이름 = api_host

3단계. Duo Security Authentication Proxy 서비스를 다시 시작합니다. 파일을 저장하고 Windows 시 스템에서 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 클릭 합니다.

		Services				- 0 -
Vev Help						
3 2 3 8 2 2 1 8 8 8 8						
4 Services (Local)						
One Security Authentication Prove	Name A	Overciption.	Status	Statup Type	Log On As	
Service	Q.0COM Server Process Laure	THE DOOMLASHON M.	Ranning	Automatic	Local System	
	Q Device Association Service	Enables pairing between		Manual (Tripper Start)	Local Suthern	
200 the parties	C. Device Install Service	Evolve a computer to		Manual (Trigger Start)	Local System	
Stated the periods	C. Device Setup Manager	Evaluation the detection,		Manual (Trigger Start)	Local System	
	C. 075 Namespace	Evaluation year to group the	Burning	Automatic	Local System	
	C. OFS Replication	Enables yes to grother	Renning	Automatic	Local System	
	G,0HCP Class	Registers and opdates it	Running	Automatic	Local Service	
	G, DHCP Server	Performs 109/IP config.	Running	Automatic	Network Service	
	C. Diagnostic Policy Service	The Disprestic Policy S.,	Running	Automatic Delayed	Local Service	
	C. Diagnostic Service Heat	The Dispersitie Service		Manual	Local Service	
	C. Diagnostic System West	The Disprostic System		Manager	Local System	
	Q Dispension Tracking Service	The Degreetics Tracking	Renning	Automatic	Local System	
	Q Distributed Link Tracking CL.	Maintains links between		Manual	Local System	
	Q Distributed Transaction Co	Condinates transaction	Rening	Automatic Delayed	Network Service	
	Q.0%S Clent	The DNS Client service	Renning	Automatic (Trippe S.,	Naturpek Samica	
	C, 010 Server	Evolve 215 client to c.	Renning	Automatic	Local System	
	CL 01 Rate Server	This service heats the D.,		Manual	Local System	
	Cue Security Buthenticatie		Annag	Automatic	Local System	
	G. Encogeting File System (EFS)	Provides the core file a		Manual (Trigger Start)	Local System	
	C. Exercible Authentication P.,	The Extensible Authentic		Manual	Local System	
	C. File Replication	Synchronizes folders with		Disabilitied	Local System	
	C. FileDille Server FTP server		Renning.	Automatic	Local System	

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.

dentity Services Engine	Home → Context Visibility → Operations → Policy → Administration → Work Centers
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
✓ Network Devices Network Device C	oups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM
C Natural Devices	Network Devices List > DuoAuthproxy
Default Devices	Network Devices
	* Name DuoAuthproxy
Device Security Settings	Description
	IP Address • IP : 10.106.44.177 / 32
	* Device Profile ditte Cisco 💌 🕀
	Model Name
	Software Version

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

dentity Services Engine	Home	Context Visibility Operations Policy Administration Work Centers
System Identity Management	- Network	Resources
Network Devices Network Device 0	Groups	etwork Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM
0		
Network Devices	✓	
Default Device		
Device Security Settings		RADIUS UDP Settings
		Protocol RADIUS
		* Shared Secret Show
		Use Second Shared Secret 🔲 🕧
		Show
		CoA Port 1700 Set To Default

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

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
► System Identity Management	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC
◄ Identities Groups External Ident	ity Sources Identity Source Sequences
Users	Network Access Users List > cpiplani
Latest Manual Network Scan Results	 Network Access User
	* Name cpiplani
	Status C Enabled -
	Email
	▼ Passwords
	Password Type: Internal Users 🔹
	Password Re-Enter Password
	* Login Password Generate Password (i)
	Enable Password Generate Password (1)

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.



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.

Phones

You may reamange the phones by dragging and dropping in the table.



This user has no phones. Add one.



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

Device Info							
Bite	Not using Duo Mobile Activate Duo Mobile		Model Unknown	?	OS Generic Smartphone		

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

Dashboard Policies Applications Users 2FA Devices Plones	Destroard > Process Senance Structures > Antivers Over Medice Activate Duo Mobile This form allows you to perversite a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to penerate passocides on their mobile device or authenticate via Duo Puel. Note: Generating an activation code will invalidate any existing Duo Mobile condentiats for this device until it is activated with the new activation code.					
Hardware Scherte Medichurter & USF	Press	Generic Smartphone				
Groups Administrators	Espreise	24 Anore after generation				
Reports Settings		Generate Duo Mobile Activation Code				

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

Deshiveri	Sectored > Prime Sectors.)	Institutes 3 Automotive Decimates							
Pulcies	Activate Duo Mobile								
Applications	Activate Du	Activate pao mobile							
Uses	A new Quo Mobile activation activation instructions to the	A new Quo Mobile activation code has been generated, and any old oredentials have been invalidated. You now have the option to deliver the installation instructions and/or -							
21A Devices									
Proven Textheore Unione	Phote	Generic Smartphone							
MARKING & VIEW	Installation instanctions	Sarot instalation instructions via \$245.							
Groups		Weinverse to Duri Peans Justel Pan Mehlin han une ann							
Administrators		alore.							
Feporta									
Settings		A							
Dilling									
	Activation instructions	Send activation instructions via SMS							
Report Linguistic your plan for support.		To activate the app, tap and open this link with Duo Mobile:							
Access 10									
Department I.									
Regelal Contra Decompositation (7		Send Instructions by SMIS or skip this step							
Uner divide of									

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

•	Dashboard Policies Applications	Dashboard >	Phone > Phone		
1	Users		cpiplani (Chakahu Piplani)	S ₆ Attach a user	
	SFA Devices	25		Authentication devices	
	Phones			can share multiple	
	tanjware Tokons			U.Pers	
-	NebAuthin & UDF				
1	Groups	Device Ir	nfo		
	Administrators		Using Duo Mobile 3.29.0	Model	05
	Reports	DUO	Reactivate Duo Mobile	(🗋)	(💮) Android 9
	Settings		O Last Seen 1 hour ago	\smile	\sim

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 이미 지에 표시된 대로 로그인합니다.

Login Request



CISCO SYSTEMS



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.

verview		
Event	5200 Authentication succeeded	
Username	cpiplani	
Endpoint Id		
Endpoint Profile		
Authentication Policy	Default >> Default	
Authorization Policy	Default >> Basic_Authenticated_Access	
Authorization Result	PermitAccess	
sthentication Details	2019-07-11 03:50:38.694	
Ithentication Details Source Timestamp Received Timestamp	2019-07-11 03:50:38.694 2019-07-11 03:50:38.694	
Ithentication Details Source Timestamp Received Timestamp Policy Server	2019-07-11 03:50:38.694 2019-07-11 03:50:38.694 ROHAN-ISE	
sthentication Details Source Timestamp Received Timestamp Policy Server Event	2019-07-11 03:50:38.694 2019-07-11 03:50:38.694 ROHAN-ISE 5200 Authentication succeeded	
Source Timestamp Received Timestamp Policy Server Event Username	2019-07-11 03:50:38.694 2019-07-11 03:50:38.694 ROHAN-ISE 5200 Authentication succeeded cpipiani	

Steps		
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	
11117	Generated a new session ID	
15049	Evaluating Policy Group	
15008	Evaluating Service Selection Policy	
15041	Evaluating Identity Policy	
15048	Queried PIP - Normalised Radius.RadiusFlowType (4 times)	
22072	Selected identity source sequence - All_User_ID_Stores	
15013	Selected Identity Source - Internal Users	
24210	Looking up User in Internal Users IDStore - cpiplani	
24212	Found User in Internal Users IDStore	
22037	Authentication Passed	
15036	Evaluating Authorization Policy	
15048	Queried PIP - Radius.NAS-Port-Type	
15048	Queried PIP - Network Access.UserName	
15048	Queried PIP - IdentityGroup.Name	
15048	Queried PIP - EndPoints.LogicalProfile	
15048	Queried PIP - Network Access AuthenticationStatus	
15016	Selected Authorization Profile - PermitAccess	
22081	Max sessions policy passed	
22080	New accounting session created in Session cache	
11002	Returned RADIUS Access-Accept	

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.) 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', 3409
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 ('10.197.223.72)
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): 0 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-f754c20 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

- <u>Duo를 사용하는 RA VPN 인증</u> <u>기술 지원 및 문서 Cisco Systems</u>

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.