Duo Two-Factor verificatie configureren voor FMC Management Access

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Verificatiestroom Verificatiestroom toegelicht Configureren Configuratiestappen op FMC Configuratiestappen op ISE Configuratiestappen voor Duo Management Portal Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

In dit document worden de stappen beschreven die moeten worden uitgevoerd om externe verificatie met twee factoren voor beheertoegang te configureren op Firepower Management Center (FMC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Objectconfiguratie van Firepower Management Center (FMC)
- Beheer van Identity Services Engine (ISE)

Gebruikte componenten

- Cisco Firepower Management Center (FMC) versie 6.3.0
- Cisco Identity Services Engine (ISE) actieve versie 2.6.0.156
- Ondersteunde versie van Windows (<u>https://duo.com/docs/authproxy-reference#new-proxy-install</u>) met een verbinding met FMC, ISE en het internet om te fungeren als de Duo Verificatie proxyserver
- Windows Machine om toegang te krijgen tot FMC-, ISE- en Duo-beheerportal
- Duo-webaccount

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De FMC-beheerder verifieert via de ISE-server en een extra verificatie in de vorm van een push-melding wordt door de Duo-verificatieproxy-server naar het mobiele apparaat van de beheerder gestuurd.

Verificatiestroom



Verificatiestroom toegelicht

- 1. Primaire verificatie gestart op Cisco FMC.
- 2. Cisco FMC stuurt een verificatieaanvraag naar de Duo-verificatieproxy.
- 3. Voor primaire verificatie moet Active Directory of RADIUS worden gebruikt.
- 4. Duo Authenticatie Proxy-verbinding ingesteld met Duo Security over TCP-poort 443.
- 5. Secundaire authentificatie via de dienst van Duo Security.
- 6. Duo authenticatie proxy ontvangt de authenticatiereactie.
- 7. Cisco FMC GUI-toegang wordt verleend.

Configureren

Om de configuratie te voltooien, moet u rekening houden met deze secties:

Configuratiestappen op FMC

Stap 1. Navigeer naar **Systeem > Gebruikers > Externe verificatie**. Maak een extern verificatieobject en stel de verificatiemethode in als RADIUS. Zorg ervoor dat de beheerder is geselecteerd onder de standaard gebruikersrol zoals in het afbeelding:

Opmerking: 10.106.44.177 is het voorbeeldadres van het IP-adres van de Duo-verificatieproxyserver.

				Configuration	Users	Domains	Integration	Update
Users User Roles	External Authe	ntication						
		External Authenticatio	n Obiect					
		Authentication Method	RADIUS					
		Name *	DuoAuthProxy					
		Description						
		Primary Server						
		Host Name/IP Address *	10.106.44.177		ex. I	P or hostname		
		Port •	1812					
		RADIUS Secret Key	•••••					
		Backup Server (Option	nal)					
		Host Name/IP Address			ex. I	P or hostname		
		Port	1812					
		RADIUS Secret Key						
		RADIUS-Specific Parar	neters					
		Timeout (Seconds)	30					
		Retries	3					
				_				
		Access Admin						
		Administrator						
		Security Analyst						
				_				
		Security Analyst (Read Only)						
		Security Approver						
		Threat Intelligence Director		=				
		(TID) User						
			Access Admin Administrator		To so	ecify the defau	It user role if user	r is not fou
		Default User Role	Discovery Admin External Database User		any ç	roup		
		Shell Access Filter						
		Administrator Shell Access		_				
		(Mandatory for ETD devices)			ex. u	ser1, user2, us	er3	
		(Manualory for PTD devices)						
		Define Custom RADIU	JS Attributes					
		Additional Test Parame	eters					
		User Name						
		Password						
		*Required Field						
			Save Test Cance					

Klik op **Opslaan** en **Toepassen**. Negeer de waarschuwing zoals weergegeven in het beeld:

Overvie	w Analysis	Policies	Devices	Objects	AMP	Intelligence							
								Configuration	Users	Domains	Integration	Updates	Lice
							One or more ena don't have define	bled external authe ed user roles.	ntication obje	octs			
Users	User Roles	External	Authentic	ation									
Default Use	r Role: None		:	Shell Auther	ntication	Disabled	0						
Name													
1. DuoAu	thProxy												

Stap 2. Ga naar **Systeem > Gebruikers > Gebruikers**. Maak een gebruiker en controleer de verificatiemethode als extern zoals in de afbeelding:

Liser Name	coiolani
oser nume	cpipian
Authentication	Use External Authentication Method
Options	Exempt from Browser Session Timeout
User Role Conf	figuration
	✓ Administrator
	External Database User
	Security Analyst (Read Only)
	Security Approver
Default User Roles	Intrusion Admin
	Access Admin
	Network Admin
	Maintenance User
	Jiscovery Admin
	Threat Intelligence Director (TID) User

Stap 1. Duo-verificatieproxyserver downloaden en installeren.

Log in op de Windows-machine en installeer de Duo Verificatie Proxy Server

Aanbevolen wordt een systeem te gebruiken met minimaal 1 CPU, 200 MB schijfruimte en 4 GB RAM

Opmerking: dit apparaat moet toegang hebben tot FMC, RADIUS-server (in ons geval) en Duo Cloud (internet)

Stap 2. Configureer het bestand authproxy.cfg.

Open dit bestand in een teksteditor zoals Kladblok++ of WordPad.

Opmerking: De standaardlocatie is te vinden op C:\Program Files (x86)\Duo Security Verification Proxy\conf\authproxy.cfg

Bewerk het bestand authproxy.cfg en voeg deze configuratie toe:

<#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

Het IP-adres van het VCC moet worden geconfigureerd in combinatie met de RADIUS-geheime sleutel.

<#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=

Verzeker u ervan dat u de parameters key, skey en api_host configureert. Meld u aan bij uw Duo-account (<u>Duo Admin Login</u>) en navigeer naar **Toepassingen > Bescherm een Toepassing** om deze waarden te verkrijgen. Selecteer vervolgens de RADIUS-verificatietoepassing zoals in de afbeelding:

RADIUS

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

Details

Integration key		select
Secret key	Click to view.	select
	Don't write down your secret key or share it with anyone.	
API hostname		select

Integratiesleutel = ikey

geheime sleutel = sleutel

API-hostnaam = api_host

Stap 3. Start de Duo Security Verification Proxy-service opnieuw. **Sla** het bestand op en **start** de Duoservice opnieuw op de Windows-machine.

Open de Windows Services console (services.msc). Zoek de **Duo Security Verification Proxy-service** in de lijst met services en klik op **Opnieuw starten** zoals in de afbeelding:

			Services				- 0 X
File Action Ves	r Help						
e 🔸 📰 🖂 i	4 🖬 🖬 💷 🕨 🖬 🖬 🖬						
G Service (Local)	Services (Local)						
	Duo Security Authentication Proxy	Name *	Description	Status	Statup Type	Leg On As	-
	Servers	Concord Server Process Laure.	The DOCKELIONCH SE.	Automp	Automatic Television	Local System	
	Stop the service	C period Association Service	trainer paring periods.		Manual (Logger (Mar)	Local System	
	facture the service	C Device Install Service	Endows a computer to		Manual (Trigger Start)	Local System	
		C del se segurar ager	factors on presson, -		Statute (regge star)	Local System	
		C Old Residential	Enables you to produce	and and a second	Automatic .	Local System	
		C. Shift Chart	Evaluation and condition in	Real Property lies	Automatic	Local Service	
		C day's farmer	Reduces Whith cost.		A damage	National Service	
		O Description Realized Realized	The Presents Rates 5		Adventio Palment	Local Service	
		C. Discountly Service Heat	The Dispersite Tencies	- and	Manual	Local Service	
		C. Responder Surben Haut	The Discounty Sectors		Manual	Local Sustem	
		C. Dissentics Tracking Service	The Disgnostics Tracki.	Running	Automatic	Local Sustem	
		C. Databased Link Tracking Cl.	Maintaine Into Balance		Manual	Local System	
		C. Databased Transaction Co.	Coordinates Instantion	Reprint	Adventix Coland -	Network Service	
		G. 0NS Class	The DAS Client service	Running	Automatic (Trigger S.,	Natural Service	
		G. 010 Server	Easting (W) clean to c.	Running	Automatic	Local Sustem	
		C. D1 Role Server	This service hosts the D		Manual	Local System	
		Charles Security Butheritz aton.		Running	Automatic	Local System	
		C. Excepting File System (EFS)	Provides the core file e		Manual (Tripper Start)	Local Sustem	
		C. Educable Authentication P	The Extensible Authenti		Manual	Local System	
		C. File Replication	Synchronizes folders wi		Disabiled	Local System	
		Q, FileZilla Server FTP server		Running	Automatic	Local System	
	Estended (Standard /						

Configuratiestappen op ISE

Stap 1. Blader naar **Beheer > Netwerkapparaten en** klik op **Toevoegen** om het netwerkapparaat te configureren zoals in de afbeelding:

dentity Services Engine	Home	Visibility	► Policy
System Identity Management	✓ Network Resources	Device Portal Manageme	ent pxGrid Services + Feed Se
▼ Network Devices Network Device	Groups Network Devi	ce Profiles External RADIU	IS Servers RADIUS Server Sequ
Network Devices Default Device Device Security Settings	Network Devices Lis Network Device	t > DuoAuthproxy * Name DuoAuthproxy Description * IP : 10.106.44	.177
	* De	vice Profile 🔐 Cisco 👻	Ð
	N	odel Name	T
	Softw	are Version	¥.

Configureer het **gedeelde geheim** zoals vermeld in **auteproxy.cfg** in het **geheim** zoals weergegeven in de afbeelding:

cisco	· Identity Serv	vices Engine	Home	Context	Visibility	 Operations 	Policy	▼ Adn	ninistration
► S	System Ident	ity Management	✓ Networ	rk Resources	Device I	Portal Management	pxGrid S	Services	Feed Ser
~ N	letwork Devices	Network Device	Groups	Network Devi	ce Profiles	External RADIUS	Servers	RADIUS	Server Seque
		(3						
Netw	ork Devices		✓	▼ RADIUS A	Authenticatio	n Settings			
Defa	ult Device								
Devi	ce Security Setting	gs		RADIUS	UDP Setting	gs			
							Pr	rotocol	RADIUS
							* Shared S	Secret	•••••
						Use Seco	ond Shared	Secret [i
							Co	A Port	1700

Stap 2. Ga naar Beheer > Identiteiten. Klik op Add om de Identity-gebruiker te configureren zoals in de

Opmerking: 10.106.44.177 is het voorbeeldadres van het IP-adres van de Duo-verificatieproxyserver.

afbeelding:

dentity Se	ervices Engine	Home 🔸	Context Visib	ility ► Ope	rations	Policy	▼ Adminis	stration
► System - Ide	entity Management	 Network Res 	ources 🕨 [Device Portal M	anagement	pxGrid Se	ervices)	Feed Ser
- Identities Gro	oups External Ident	tity Sources Id	dentity Source	e Sequences	 Settings 			
	0	Network Ac	cess Users Li	st > cninlani				
Users		- Notw	ork Access	lleor				
Latest Manual Netw	ork Scan Results	* Netwo	JIK ACCESS	USEI				
		* Name	cpiplani					
		Status	Enable	ad =				
		oluluo		su v				
		Email						
		▼ Pass	words					
		Passw	ord Type:	Internal Users		•		
			F	Password		R	te-Enter Pa	ssword
		* Login	Password [•••••			•••••	
		Enable	Password					

Configuratiestappen voor Duo Management Portal

Stap 1. Maak een gebruikersnaam aan en activeer Duo Mobile op het eindapparaat.

Voeg de gebruiker toe op de Duo cloud administratie webpagina. Navigeer naar **Gebruikers > Gebruikers toevoegen** zoals in de afbeelding:

DUO	9. Search for users, group	os, applications, or devices
Dashboard Policies	Add User	User
Applications Users Add User	Adding Users Most applications allow Learn more about addit	users to enroll themselves after they complete primary authentication. Ing users $\ensuremath{\mathcal{C}}$
Pending Envoluments Bulk Enroll Users Import Users Directory Sync Bypass Codes	Username	opipiani Should match the primary authentication username.
2FA Devices Groups Administrators		Add User

Opmerking: Zorg ervoor dat de eindgebruiker de Duo-app heeft geïnstalleerd.

Handmatige installatie van Duo-toepassing voor IOS-apparaten

Handmatige installatie van Duo-toepassing voor Android-apparaten

Stap 2. Automatische generatie van code.

Voeg het telefoonnummer van de gebruiker toe zoals in de afbeelding:

Phones You may reamings the phones by dragging and drapping in the table. Add Phone					
	This us	er has no phones. Add one.			
DUO	 Search for users, gr 	oups, applications, or devices			
Dashboard	Dashboard > Users >	piplani 🔰 Add Phone			
Policies	Add Phon	0			
Applications	Add Phon	e			
Users	Туре	Phone			
Add User		 Tablet 			
Pending Enrolments					
Buik Enroll Users	Phone number	+1 201-555-5555 Show extension field			
Directory Sync					
Bypass Codes		Add Bhone			
2FA Devices		AND PROPERTY			

Kies **Duo Mobile activeren** zoals in de afbeelding:

Device In	fo			
	Not using Duo Mobile Activate Duo Mobile	Model Unknown	\bigcirc	OS Generic Smartp

Kies Duo Mobile Activeringscode genereren zoals in de afbeelding:

Deshboard	Dations > Press	Jeneric Smartphone 3: Activate Duo Motelle
Policies	Antivete	Due Mahila
Applications	Activate	Duo Mobile
Users	This form allows you multiple device or aut	to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their restrictle via Duo Push.
2FA Devices	Notes formation of	and and a set of the state of the set of the
Protest	Note Construct in	accessor code en relations any external can write comparises to the device crisis is accesses with the new accessor code.
Forderere Tolere		
TRADUCTION & LIDT	Phone	Generic Smartphone
Groupe		
Administrations	Equivalue	24 hours - after generation
Reports		
Settings		Generate Due Mobile Activation Code

Kies Instructies per sms verzenden zoals in de afbeelding:

Dashboard Policies Applications Users	Destinant > Proce. Descent Activate Du Anew Duo Mobile activati activation instructions to T	Understore 3 Anima Davanders IO Mobile on code has been generated, and any old oredentials have been invalidated. Now now have the option to deliver the installation instructions and/or te and ty SML.
29% Devices Proves Tarbury Tolers Webbyth & UP	Plane	Garant Smarghove
Oroups Administrators Reports Serlines	Installation instructions	Bend initializion instructions via BMS Welcome to Duct Please instal Duc Mobile from your app atom.
Dilling Report Support for support.	Activation instructions	Eend activation instructions via BMS To activate the app, tap and speri this link with Oue Mobile:
Buyingmant () Bugingmant () Buckerstellars ()		A Send Methodown by SMI or unit this Map

Klik op de koppeling in de SMS en Duo app wordt gekoppeld aan de gebruikersaccount in het gedeelte Apparaatinfo, zoals in de afbeelding:

Dashboard Policies Applications	Dashboard > Phone: > Phone:	•	
Users	cpiplani (Chakahu Piplani)	A. Attach a user	
2FA Devices		Authentication devices	
Phones		can share multiple	
Hardware Tokens		users	
Weekumn & UDF			
Groups	Device Info		
Administrators	Uning Day Mobile 3 29.0	Model	05
Reports	PUIO Reactivate Duo Mobile	((💭) Android 9
Settings	O Last Seen 1 hour ago	\smile	\smile

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Log in bij het VCC met uw gebruikersreferenties die zijn toegevoegd op de ISE-pagina met gebruikersidentiteiten. U moet een Duo PUSH melding krijgen over uw eindpunt voor Two Factor Authenticatie (2FA), goedkeuren, en FMC zou inloggen zoals in het beeld:



Ga op de ISE-server naar **Operations > RADIUS > Live logs**. Zoek de gebruikersnaam die gebruikt wordt voor de verificatie op het VCC en selecteer het detailverificatierapport onder de kolom Details. In dit geval moet u controleren of de verificatie is geslaagd, zoals in de afbeelding:

erview		
ivent	5200 Authentication succeeded	
Jsername	cpiplani	
indpoint Id		
Indpoint Profile		
Authentication Policy	Default >> Default	
Authorization Policy	Default >> Basic_Authenticated_Access	
Authorization Result	PermitAccess	

2019-07-11 03:50:38.694

2019-07-11 03:50:38.694

5200 Authentication succeeded

ROHAN-ISE

cpiplani

Internal Users

User

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.RadiusFle
22072	Selected identity source sequence - All_Use
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore -
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 Authentication
15016	Selected Authorization Profile - PermitAcce
22081	Max sessions policy passed
22080	New accounting session created in Session
11002	Returned RADIUS Access-Accept

Authentication Identity Store

Source Timestamp

Received Timestamp

Policy Server

Event

Username

User Type

Problemen oplossen

Deze sectie bevat informatie voor het troubleshooten van de configuratie.

• Controleer de debugs op Duo Authenticatie Proxy Server. De logbestanden bevinden zich onder deze locatie:

C:\Program Files (x86)\Duo Security verificatie proxy\log

Open het bestand authproxy.log in een teksteditor zoals Notepad++ of WordPad.

Log snippets als er onjuiste referenties worden ingevoerd en verificatie wordt geweigerd door de ISE-server.

<#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', 34524' 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 ('10.197.223.2 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 rejecter 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

• Ga op ISE naar **Operations > RADIUS > Live logs** om de verificatiegegevens te verifiëren.

Log fragmenten van succesvolle verificatie met ISE en Duo:

<#root>

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

10.197.223.76

to radius_server_auto

2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Received new request id 5 from ('10.197.223.76', 34095) 2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] (('10.197.223.76', 34095), 5): login attempt for user 2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.223.2019-08-04T18:56:16+0530 [RadiusClient (UDP)] Got response for id 137 from ('

10.197.223.23

', 1812);

code 2

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

2019-08-04T18:56:16+0530 [RadiusClient (UDP)] http POST to https://api-f754c261.duosecurity.com:443/rest 2019-08-04T18:56:16+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPC2 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-f754c26 2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] http POST to https://api-f754c26 2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPC2 2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPC2 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):

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

Gerelateerde informatie

- **<u>RA VPN-verificatie met Duo</u>**
- Technische ondersteuning en documentatie Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.