# 為FMC管理訪問配置雙因素身份驗證

### 目錄

· · · · · · · · · · · · · · · · · · ·
<u>必要條件</u>
<u>需求</u>
採用元件
<u>背景資訊</u>
身份驗證流程
<u>驗證流程說明</u>
<u>設定</u>
FMC的配置步驟
ISE的配置步驟
Duo Administration Portal的配置步驟
<u>驗證</u>
<u>疑難排解</u>
<u>相關資訊</u>

## 簡介

本文檔介紹在Firepower管理中心(FMC)上為管理訪問配置外部雙因素身份驗證所需的步驟。

## 必要條件

#### 需求

思科建議您瞭解以下主題:

- Firepower管理中心(FMC)對象配置
- 身分識別服務引擎(ISE)管理

#### 採用元件

- 運行版本6.3.0的Cisco Firepower管理中心(FMC)
- 運行版本2.6.0.156的思科身份服務引擎(ISE)
- 支援版本的Windows(<u>https://duo.com/docs/authproxy-reference#new-proxy-install</u>),可連線 到FMC、ISE和Internet以充當Duo身份驗證代理伺服器
- Windows機器訪問FMC、ISE和Duo管理門戶
- Duo Web帳戶

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

FMC管理員根據ISE伺服器進行身份驗證,Duo Authentication Proxy伺服器向管理員的流動裝置傳送推送通知形式的附加身份驗證。

身份驗證流程



#### 驗證流程說明

- 1. 主身份驗證已啟動到Cisco FMC。
- 2. Cisco FMC向Duo Authentication Proxy傳送驗證要求。
- 3. 主身份驗證必須使用Active Directory或RADIUS。
- 4. Duo Authentication Proxy連線建立到Duo Security over TCP埠443。
- 5. 通過Duo Security的服務進行輔助身份驗證。
- 6. Duo authentication proxy接收身份驗證響應。
- 7. 已授予Cisco FMC GUI訪問許可權。

## 設定

要完成配置,請考慮以下部分:

#### FMC的配置步驟

步驟 1.導覽至System > Users > External Authentication。 建立外部身份驗證對象並將身份驗證方

♦ 註:10.106.44.177是Duo Authentication Proxy伺服器的示例IP地址。

Overview Analysis Policies Devices	Objects AMP Intellig	ence						Deploy	D 🔒 🕏	vstem Help T	admin v
ore them randyois rolleles beries	objects vin intellige		Configuration	Users	Domains	Integration	Updates	Licenses *	Health •	Monitoring •	Tools •
Heave Heav Palac External Auth	entication										
Users User Koles External Auto	entication										
	External Authenticatio	n Object									
	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	•••••									
	Paskup Conver (Ontion										
	Backup Server (Option	ai)	_								
	Host Name/IP Address	1013	-	ex. 1	r or nostname						
	RADIUS Secret Key	1015	_								
	Noto Selecting										
	RADIUS-Specific Parar	neters									
	Timeout (Seconds)	30									
	Retries	3									
	Access Admin										
			_								
	Administrator										

#### 按一下「Save」和「Apply」。忽略警告,如下圖所示:

Overview Analysis	Policies Devices	6 Objects	AMP	Intelligence							Deplo	y 🍳	System	ielp 🔻	admin 🔻
						Configuration	Users	Domains	Integration	Updates	Licenses •	Health	<ul> <li>Monit</li> </ul>	oring 🔻	Tools •
					One or more er don't have defin	abled external auther red user roles.	tication obje	ects							
Users User Roles	External Authent	ication													
												🔚 Save	😫 Cancel	🗹 Sav	e and Apply
Default User Role: None		Shell Authentic	ation D	isabled	0							0	Add External	Authentic	ation Object
Name												Meth	od Ena	bled	
1. DuoAuthProxy												RADI	us 💽		0

步驟 2. 導航到System > Users > Users。 建立使用者,並檢查外部的驗證方法,如下圖所示:

User Configuration						
User Name	cpiplani					
Authentication	Use External Authentication Method					
Options	Exempt from Browser Session Timeout					
User Role Conf	iguration					
Default User Roles	<ul> <li>Administrator</li> <li>External Database User</li> <li>Security Analyst</li> <li>Security Analyst (Read Only)</li> <li>Security Approver</li> <li>Intrusion Admin</li> <li>Access Admin</li> <li>Network Admin</li> <li>Maintenance User</li> <li>Discovery Admin</li> <li>Threat Intelligence Director (TID) User</li> </ul>					
	Save Cancel					

步驟 1.下載並安裝Duo Authentication Proxy Server。

登入到Windows機器並安裝Duo Authentication Proxy Server

建議使用至少具有1 CPU、200 MB磁碟空間和4 GB RAM的系統

✤ 注意:此電腦必須能夠訪問FMC、RADIUS伺服器(在我們的情況下為ISE)和Duo Cloud(網際網路)

步驟 2.配置authproxy.cfg檔案。

在文本編輯器(如記事本或寫字板)++開啟此檔案。

### ◆ 注意:預設位置位於C:\Program Files(x86)\Duo Security Authentication Proxy\conf\authproxy.cfg

編輯authproxy.cfg檔案並新增以下配置:

<#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

FMC的IP地址必須與RADIUS金鑰一起配置。

#### <#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=

確保配置ikey、skey和api\_host引數。要獲取這些值,請登入您的Duo帳戶(<u>Duo Admin Login</u>)並導 航至Applications > Protect an Application。接下來,選擇RADIUS驗證應用程式,如下圖所示:

# RADIUS

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

#### Details



#### 整合金鑰= ikey

secret key = skey

API主機名= api\_host

步驟 3.重新啟動Duo Security身份驗證代理服務。儲存檔案並在Windows電腦上重新啟動Duo服務。

開啟Windows服務控制檯(services.msc)。在服務清單中找到Duo Security Authentication Proxy Service,然後按一下Restart,如下圖所示:

			Services				- 0
a Action Vie	u thip						
• • 💼 🗉	86 B 20 + B B P						
Sevice (Lead)	Services (Local)						
	Over Security Authentication Prove	Name	Overlytion.	Sec.	Statup Type	LogOn As	
	Service	Q. DCOM Server Process Lauru.	The DCOMLADNON M.	Running.	Automatic	Local System	
		Q Device Association Service	Enables pairing between		Manual (Tripper Rev)	Local System	
	2mg the service	Q Device Install Service	English a computer to		Manual (Trigger Start)	Local System	
	Solari the pervice	Q. Denice Setup Manager	English the detection,		Manual (Tripper Start)	Local System	
		C. OVI Namespace	Evaluation year to group the	Burning.	Automatic	Local System	
		Q.095 Replication	Enables yes to synchrony	Burning	Automatic	Local System	
		G. DHCP Class	Registers and opdates i.e.	Rendered	Automatic	Local Service	
		G, DHCP Server	Performs TOUP config.	Running	Automatic	Network Service	
		Q. Diagnostic Policy Service	The Dispersitie Palicy S.,	Autom	Automatic Colored	Local Service	
		C. Diagnostic Service Heat	The Degratite Service		Manual	Local Service	
		Q. Diagnostic System West	The Disprovite System		Manual	Local System	
		Q. Diagnostics Tracking Service	The Disgnostics Tracki	Randog	Automatic	Local System	
		Q Distributed Link Tracking CL.	Maintains Into Informa-		Manual	Local System	
		Q. Distributed Transaction Co	Coordinates transaction	Burning	Automatic Selayed -	Network Service	
		G. (NS Clent	The DNS Client service	Rendered	Automatic (Trigger S.,	Nativork Service	
		G, 0%G Gerver	Easting 202 clients to c.,	Running	Automatic	Local System	
		Q.01 Role Server	This pervice heats the D		Manual	Local System	
		C. Due Security Buthentication		Randog	Automatic	Local System	
		C. Encrupting Alle System (EFS)	Provides the core file a		Manual (Trigger Start)	Local Suttem	
		Q Exerciple Authentication P	The Extensible Authentic.		Manual	Local System	
		C. File Replication	Synchronizes folders with		Dealited	Local System	
		C. FileDile Server #1P server		Renning.	Automatic	Local System	

## ISE的配置步驟

步驟 1.導覽至Administration > Network Devices,按一下Add以設定網路裝置,如下圖所示:

♦ 註:10.106.44.177是Duo Authentication Proxy伺服器的示例IP地址。

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 0	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM
Network Devices	Network Devices List > DuoAuthproxy
Default Device	Network Devices
Device Security Settings	* Name DuoAuthproxy Description
	IP Address • IP : 10.106.44.177 / 32
	* Device Profile 🗰 Cisco 👻 🕀
	Model Name
	Software Version

設定Shared Secret,如authproxy.cfg中的secret所述,如下圖所示:

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

#### 步驟 2.導航到Administration > Identities。 按一下Add以設定Identity使用者,如下圖所示:

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
✓ Identities Groups External Iden	tity Sources Identity Source Sequences
Users	Network Access Users List > cpiplani
Latest Manual Network Scan Results	Network Access User     Name cpiplani     Status Enabled      Email
	Passwords Password Type: Internal Users
	Password Re-Enter Password
	* Login Password Generate Password (i
	Enable Password Generate Password (i)

Duo Administration Portal的配置步驟

步驟 1.建立使用者名稱並在終端裝置上啟用Duo Mobile。

在Duo雲管理網頁上新增使用者。 導覽至Users > Add users,如下圖所示:



♦ 注意:確保終端使用者安裝了Duo應用。

<u>手動安裝IOS裝置Duo應用程式</u>

手動安裝用於Android裝置的Duo應用程式

步驟 2. 代碼的自動生成。

新增使用者的電話號碼,如下圖所示:

#### Phones

Add Phone You may reamange the phones by dragging and dropping in the table. This user has no phones. Add one.



#### 選擇Activate Duo Mobile,如下圖所示:

Device	Info

Not using Duo Mobile Activate Duo Mobile Model Unknown OS Generic Smartphone	
---	--

選擇Generate Duo Mobile Activation Code,如下圖所示:

Destilicant	Induced > Provulence	to Smartphone 3: Antivare Due Melaite							
Policies	Activate D	uo Mobile							
Users	This form allows you to p	This form allows you 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							
27A Devices	mobile device or authority Note: Constanting an activ	mobile device or authenticate via Dvo Pueh. Note: Constraints an authentics code will invalidate any activities Duo Mistile condentate for this device until it is activated with the new activation code.							
Phones Hackeys Totana									
MALAUTH & USF	Phone	Generic Smartphone							
Gноире									
Administrations	Capitalian	Lan hours and permanent							
Settings		Generale Cus Mobile Astivation Code							

選擇Send Instructions by SMS,如下圖所示:

Deshboard	Decisional 2 Phone Decesion	Institutes 2 Automotion
Policies	Activate Du	a Mabila
Applications	Activate Du	o Mobile
Uses	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	activation manufacture to the	super by Data.
Paran Tantana lakara	Plane	Generic Smartphone
Notice Elize	Installation Instancions	Send instalation instructions via \$165
<b>Groups</b>		Weinverse to Durit Please Justicel Fun. Mobile trans unor ann
Administrators		aliza.
Reports		
Settings		A
Diffing		
	Activation instructions	Send activation instructions via SMS
Report Second star in a second		To activate the app, tap and open this link with Ouo Mobile:
Accestio		
Indigment ID		4
Regional Galeria Electrometation (T		Sand Instructions by DMS or wild this step
User during of		

單擊SMS中的連結,Duo應用將連結到「Device Info(裝置資訊)」部分中的使用者帳戶,如下圖 所示:

Dashboard Policies Applications	Dashboard >	fitones > Phone		
Users 2FA Devices Ptones Hardware Tokens WebAuter & UDF	2	cpiplani (Chakahu Piplani)	Authentication devices can share multiple users	
Groups Administrators Reports Settings	Device In	fo Using Duo Mobile 3.29.0 Reactivate Duo Mobile O Last Seen 1 hour ago	Model	OS Android 9

## 驗證

使用本節內容,確認您的組態是否正常運作。

使用在ISE使用者身份頁面上新增的使用者憑據登入FMC。您必須在您的終端上獲取Duo PUSH通 知以進行二元身份驗證(2FA),請批准該通知,然後FMC將登入,如下圖所示:

# Login Request



# **CISCO SYSTEMS**



August 2, 2019, 7:37 PM





上用於身份驗證的使用者名稱,並選擇詳細列下的詳細身份驗證報告。在此處,必須驗證身份驗證 是否成功,如下圖所示:

verview		Steps	
Event	5200 Authentication succeeded	11001	F
Linu		11017	F
Username	cpiplani	11117	G
Endpoint Id		15049	E
		15008	E
Endpoint Profile		15041	E
Authentication Policy	Default >> Default	15048	C
Authorization Policy	Default>> Resin Authenticated Across	22072	S
Autorization Folicy		15013	S
Authorization Result	PermitAccess	24210	L
		0.0010	
		24212	F
		24212 22037	F
utherstication Details		24212 22037 15036	F A E
uthentication Details		22212 22037 15036 15048	F
uthentication Details	2019-07-11 03:50:38.694	24212 22037 15036 15048 15048	F A E C
uthentication Details Source Timestamp	2019-07-11 03:50:38.694	24212 22037 15036 15048 15048 15048	
uthentication Details Source Timestamp Received Timestamp	2019-07-11 03:50:38.694 2019-07-11 03:50:38.694	24212 22037 15036 15048 15048 15048	
uthentication Details Source Timestamp Received Timestamp Policy Server	2019-07-11 03:50:38.694 2019-07-11 03:50:38.694 ROHAN-ISE	24212 22037 15036 15048 15048 15048 15048	
uthentication Details Source Timestamp Received Timestamp Policy Server	2019-07-11 03:50:38.694 2019-07-11 03:50:38.694 ROHAN-ISE	24412 22037 15036 15048 15048 15048 15048 15048 15048	
uthentication 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	24212 22037 15036 15048 15048 15048 15048 15048 15048 15048	F A E C C C C C S N
uthentication Details 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	24412 22037 15036 15048 15048 15048 15048 15048 15048 15048 15016 22081 22080	

iteps	
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

## 疑難排解

tity Services F

本節提供的資訊可用於對組態進行疑難排解。

• 檢查Duo Authentication Proxy伺服器上的調試。日誌位於以下位置:

C:\Program檔案(x86)\Duo Security Authentication Proxy\log

在記事本或寫字板等文本編輯器中開啟authproxy++log檔案。

當ISE伺服器輸入不正確的憑證並拒絕身份驗證時,記錄片段。

#### <#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

▪ 在ISE上,導航到操作> RADIUS >即時日誌以驗證身份驗證詳細資訊。

使用ISE和Duo成功身份驗證的日誌片段:

<#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

相關資訊

• <u>使用Duo的RA VPN身份驗證</u>

• <u>技術支援與文件 - Cisco Systems</u>

#### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。