# **Configure a autenticação de dois fatores do Duo para o acesso de gerenciamento do FMC**

### Contents

Introdução Pré-requisitos Requisitos Componentes Utilizados Informações de Apoio Fluxo de autenticação Fluxo de autenticação explicado Configurar Etapas de configuração no FMC Etapas de configuração no ISE Etapas de configuração no Portal de administração Duo Verificar Troubleshooting Informações Relacionadas

# Introdução

Este documento descreve as etapas necessárias para configurar a autenticação externa de dois fatores para acesso de gerenciamento no Firepower Management Center (FMC).

### **Pré-requisitos**

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de objeto do Firepower Management Center (FMC)
- Administração do Identity Services Engine (ISE)

#### **Componentes Utilizados**

- Cisco Firepower Management Center (FMC) executando a versão 6.3.0
- Cisco Identity Services Engine (ISE) executando a versão 2.6.0.156
- Versão suportada do Windows (<u>https://duo.com/docs/authproxy-reference#new-proxy-install</u>) com conectividade para FMC, ISE e Internet para atuar como o servidor proxy de autenticação Duo
- Computador Windows para acessar o portal de administração do FMC, ISE e Duo
- Conta da Web do Duo

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

# Informações de Apoio

O administrador do FMC autentica-se no servidor ISE, e uma autenticação adicional sob a forma de notificação por envio é enviada pelo servidor Duo Authentication Proxy para o dispositivo móvel do administrador.

# Fluxo de autenticação



#### Fluxo de autenticação explicado

- 1. Autenticação primária iniciada no Cisco FMC.
- 2. O Cisco FMC envia uma solicitação de autenticação ao Duo Authentication Proxy.
- 3. A autenticação primária deve usar o Ative Diretory ou o RADIUS.
- 4. Conexão de Proxy de Autenticação Duo estabelecida para Segurança Duo sobre a porta TCP 443.
- 5. Autenticação secundária por meio do serviço Duo Security.
- 6. O proxy de autenticação Duo recebe a resposta de autenticação.
- 7. O acesso à GUI do Cisco FMC é concedido.

# Configurar

Para concluir a configuração, leve em consideração estas seções:

### Etapas de configuração no FMC

**Etapa 1. Navegue até System > Users > External Authentication**. Crie um Objeto de Autenticação Externa e defina o Método de Autenticação como RADIUS. Verifique se Administrador está selecionado em

Função de usuário padrão, conforme mostrado na imagem:

**Observação**: 10.106.44.177 é o endereço IP de exemplo do servidor de proxy de autenticação Duo.

UsersUser RolesExternal AuthenticationObjectAuthentication ObjectAuthentication MethodRADIUSImage: Constraint of the constraint of	Overview Analysis Policies Devic	es Objects AMP Intelli	gence					
Users       User Roles       External Authentication Object         Authentication Method       RADIUS       •         Authentication Method       RADIUS       •         Name *       DuoAuthProxy       •         Description       •       •         Primary Server       •       •         Host Name/IP Address *       10:106:44.177       ex. IP or hostname         Port *       1812       •         RADIUS Secret Key       •       •         Port       1812       •         RADIUS Secret Key       •       •         Port       1812       •         RADIUS Secret Key       •       •         Port       1812       •         RADIUS Secret Key       •       •         RADIUS Secret Key       •       •         RADIUS Secret Key       •       •         RADIUS Secret Key       30       •         Ratries       3       •         Access Admin       •       •				Configuration	Users	Domains	Integration	Update
External Authentication Object   Authentication Method   Authentication Method   Authentication Method   Name *   Description   Description   Primary Server   Most Name/IP Address *   10.106.44.177   ex. IP or hostname   Port *   1812   RADIUS Secret Key   Port   1812   RADIUS Secret Key   Port   1812   RADIUS Secret Key   Immout (Seconds)   30   Retries   3   Access Admin	Users User Roles External A	uthentication						
External Addition Coject   Authentication Method   RADIUS   Name *   Description     Primary Server   Host Name/IP Address *   10.106.44.177   ex. IP or hostname   Port *   1812   RADIUS Secret Key   Port   1812   RADIUS Secret Key     ex. IP or hostname   Port   1812   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Immeout (Seconds)   30   Retries   3   Access Admin		External Authenticati	ion Object					
Authentication Method RADIUS RADIUS RADIUS Primary Server Post Server 10:106.44.177 ex. IP or hostname Port * 1812 RADIUS Secret Key *****  Backup Server (Optional) Host Name/IP Address (		External Authenticat						
Name • DuoAuthProxy   Description     Primary Server   Host Name/IP Address •   10.106.44.177   ex. IP or hostname   Port *   1812   RADIUS Secret Key   Port   1812   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Post Secret Key     Post Admin		Authentication Method	RADIUS 💟					
Description   Primary Server   Host Name/IP Address *   10.106.44.177   ex. IP or hostname   Port *   Backup Server (Optional)   Host Name/IP Address   Port   1812   RADIUS Secret Key   Port   1812   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Port   Sala   Access Admin		Name *	DuoAuthProxy					
Primary Server   Host Name/IP Address *   10:106.44.177   ex. IP or hostname   Port *   1812   RADIUS Secret Key   Host Name/IP Address   Port   1812   RADIUS Secret Key   Port   1812   RADIUS Secret Key   Exclus Secret Key   Port   1812   RADIUS Secret Key   Exclus Secret Key   Port   1812   RADIUS Secret Key   Exclus Secret Key   Secret Key   Secret Key   Secret Key		Description						
Host Name/IP Address * 10.106.44.177 ex. IP or hostname   Port * 1812   RADIUS Secret Key •••••   Backup Server (Optional)   Host Name/IP Address   Port   1812   RADIUS Secret Key   Port   1812   RADIUS Secret Key   Port   1812   RADIUS Secret Key   RADIUS Secret Key   Secret Key   Access Admin		Primary Server						
Host Name/IP Address 10.106.44.177   Port 1812   RADIUS Secret Key •••••     Backup Server (Optional)   Host Name/IP Address   Port   1812   Port   1812   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Part   RADIUS Secret Key     Port   1812   RADIUS Secret Key     Part   RADIUS Secret Key     Partimeout (Seconds)   30   Retries   3   Access Admin		Finally Server				_		
Port 1812   RADIUS Secret Key •••••   Backup Server (Optional)   Host Name/IP Address   Port   1812   RADIUS Secret Key     RADIUS Secret Key     RADIUS Secret Key     Immout (Seconds)   30   Retries   3   Access Admin		Host Name/IP Address *	10.106.44.177		ex. 1	P or hostname		
RADIUS Secret Key   Backup Server (Optional)   Host Name/IP Address   Port   1812   RADIUS Secret Key     RADIUS Secret Key     RADIUS-Specific Parameters   Timeout (Seconds)   30   Retries   3		Port *	1812					
Backup Server (Optional)   Host Name/IP Address   Port   1812   RADIUS Secret Key     RADIUS-Specific Parateters   Timeout (Seconds)   30   Retries   3   Access Admin		RADIUS Secret Key						
Host Name/IP Addressex. IP or hostnamePort1812RADIUS Secret KeyFADIUS-Specific ParatersTimeout (Seconds)30Retries3Access Admin		Backup Server (Optio	onal)					
Port1812RADIUS Secret KeyRADIUS-Specific ParametersTimeout (Seconds)30Retries3Access Admin		Host Name/IP Address			ex. 1	P or hostname		
RADIUS Secret Key     RADIUS-Specific Parameters     Timeout (Seconds)   30   Retries   3     Access Admin		Port	1812					
RADIUS-Specific Parameters         Timeout (Seconds)       30         Retries       3         Access Admin		RADIUS Secret Key						
RADIUS-Specific Parameters         Timeout (Seconds)       30         Retries       3         Access Admin								
Timeout (Seconds)     30       Retries     3       Access Admin		RADIUS-Specific Para	ameters					
Retries     3       Access Admin		Timeout (Seconds)	30					
Access Admin		Retries	3					
		Access Admin						
		- Access Partition						
Administrator		Administrator						

Security Analyst		
Security Analyst (Read Only)		
Security Approver		
Threat Intelligence Director (TID) User		
Default User Role	Access Admin Administrator Discovery Admin External Database User	To specify the default user role if user is not for any group
Shell Access Filter		
Administrator Shell Access User List 🛈 (Mandatory for FTD devices)		ex. user1, user2, user3
Define Custom RADIU	S Attributes	
Additional Test Parame	ters	
User Name		
Password		
*Required Field	Save Test Cancel	

Clique em Salvar e Aplicar. Ignore o aviso conforme mostrado na imagem:

Overvi	ew Analysis	Policies	Devices	Objec	ts	AMP	Intelligence								
										Configuration	Users	Domains	Integration	Updates	Lice
								0	One or more en don't have defin	abled external authe ed user roles.	ntication obj	ects			
Users	User Roles	External	Authentic	ation											
Default Us	er Role: None			Shell Auti	hentica	ation [	Disabled	0							
Name															
1. DuoA	thProxy														

**Etapa 2.** Navegue até **Sistema > Usuários > Usuários**. Crie um usuário e marque o Método de autenticação como Externo, conforme mostrado na imagem:

User Configura	ition				
User Name	cpiplani				
Authentication	Use External Authentication Method				
Options	Exempt from Browser Session Timeout				
User Role Conf	figuration				
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>Access Admin</li> <li>Network Admin</li> <li>Maintenance User</li> <li>Discovery Admin</li> <li>Threat Intelligence Director (TID) User</li> <li>Save</li> <li>Cancel</li> </ul>				

Etapa 1. Baixe e instale o servidor proxy de autenticação Duo.

Faça login na máquina Windows e instale o servidor proxy de autenticação Duo

É recomendável usar um sistema com pelo menos 1 CPU, 200 MB de espaço em disco e 4 GB de RAM

Observação: esta máquina deve ter acesso a FMC, servidor RADIUS (ISE no nosso caso) e Duo Cloud (Internet)

#### Etapa 2. Configure o arquivo authproxy.cfg.

Abra esse arquivo em um editor de texto, como o Notepad++ ou o WordPad.

Observação: o local padrão é C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg

Edite o arquivo authproxy.cfg e adicione esta configuração:

<#root>
[radius\_client]
host=10.197.223.23 satisfying the second se

Sample IP Address of the ISE server

secret=cisco

O endereço IP do FMC deve ser configurado junto com a chave secreta RADIUS.

<#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=

Certifique-se de configurar os parâmetros ikey, skey e api\_host. Para obter esses valores, faça login na sua conta Duo (<u>Duo Admin Login</u>) e navegue para **Aplicativos > Proteger** um aplicativo. Em seguida, selecione o aplicativo de autenticação RADIUS como mostrado na imagem:

# 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 anyon	ne.
API hostname		select

Chave de integração = ikey

chave secreta = chave

nome de host da API = api\_host

**Etapa 3.** Reinicie o Serviço de Proxy de Autenticação de Segurança Duo. **Salve** o arquivo e **reinicie** o serviço Duo na máquina Windows.

Abra o console de Serviços do Windows (services.msc). Localize **Duo Security Authentication Proxy Service** na lista de serviços e clique em **Restart** conforme mostrado na imagem:

			Services				- 0 1
file Action Ves	. Help						
e + 💼 🗉 i	4 🖬 🖬 💷 🕨 🖬 🖬 🖬						
Service (Local)	Services (Local)						
	Oue Security Authentication Proxy Service	Name A	Description The DCORE BORCH as	Status Remotes	Statup Type Advender	Log-On As Logid Tusteen	
	Ing the service	Q-Device Association Service Q-Device Install Service	Enables pairing between. Enables a computer to	- and	Manual (Tripper Start) Manual (Tripper Start)	Local System Local System	
	failed the service	C, Device Setup Manager C, DPS Namespace	Enables the detection,	Running	Manual (Trigger Stat) Automatic	Local System Local System	
		G, DYS Replication G, DHCP Clant	Enables yes to synchro Registers and updates L.	Running Running	Automatic Automatic	Local System Local Service	
		C. Diagnostic Policy Service	The Diagnostic Policy S., The Diagnostic Policy S., The Diagnostic Tencion	Running	Automatic Delayed Manual	Local Service Local Service	
		Diagnostic System Host     Diagnostics Tracking Service	The Diagnostic System The Diagnostics Tracki	Ranning	Manual Automatic	Local System Local System	
		Contributed Link Tracking CL.	Maintains links between	Renina .	Manual Automatic Dalaced	Local System Network Service	
		C. DNS Clant	The DNS Client service	Running	Automatic (Trigger S., Automatic	Network Service Local System	
		CLOI Role Server	This service hosts the D		Manual	Local System	
		Q Due Security Buthenticatie		Ranning	Automatic	Local System	
		G. Encrypting Ale System (US) G. Extensible Authentication P.,	Provides the core file e The Extensible Authenti		Manual (Trigger Stat) Manual	Local System Local System	
		C. Fieldle Server FTP server	Synchronizes folders at	Running	Automatic	Local System Local System	
	Estended (Standard /						

#### Etapas de configuração no ISE

**Etapa 1.** Navegue para **Administração > Dispositivos de rede,** Clique em **Adicionar** para configurar o dispositivo de rede como mostrado na imagem:

<b>Observação:</b> 10.106.44.177 é o	o endereco IP	de exemplo do servid	or de proxy de	autenticação Duo.
3	5	1	1 2	3

Identity Services Engine	Home ► Conte	xt Visibility	Operations	▶ Policy	<del>▼</del> Adm	inistration
System     Identity Management	✓ Network Resources	► Device P	ortal Management	pxGrid S	Services	▶ Feed Se
Network Devices Network Device	Groups Network De	vice Profiles	External RADIUS	Servers	RADIUS	Server Sequ
Network Devices	Network Devices	List > <b>DuoAuth</b>	proxy			
Default Device	Network Devi	ces				
Device Security Settings	IP Addre	* Name   Description   ss • * II	DuoAuthproxy P: 10.106.44.17	27		
	* I Sof	Device Profile [ Model Name [ ware Version [	det Cisco V 🕀	]		

Configure o **segredo compartilhado** como mencionado em **authproxy.cfg** em **secret** como mostrado na imagem:

cisco	Identity Serv	ices Engine	Home	Context	Visibility	<ul> <li>Operations</li> </ul>	Policy	<del>▼</del> Adn	ninistration
► Sys	stem 🕨 Identi	ity Management	✓ Networ	rk Resources	Device	Portal Management	pxGrid S	ervices	Feed Ser
✓ Net	work Devices	Network Device	Groups	Network Devi	ce Profiles	External RADIUS	Servers	RADIUS	Server Seque
			3						
Networ	k Devices		✓	▼ RADIUS A	Authenticatio	n Settings			
Default	Device								
Device	Security Setting	js		RADIUS	UDP Settin	gs			
							Pr	otocol	RADIUS
							* Shared	Secret [	•••••
						Use Seco	ond Shared	Secret [	<b>i</b>
								[	
							Co	A Port	1700

Etapa 2. Navegue até Administração > Identidades. Clique em Add para configurar o usuário de

identidade como mostrado na imagem:

dentity Services Engine	Home	▸ Context Visit	ibility → Op	erations	▶ Policy	▼ Admi	inistration
► System	Network R	Resources +	Device Portal N	lanagement	pxGrid	Services	Feed Serv
✓ Identities Groups External Iden	tity Sources	Identity Sour	ce Sequences	<ul> <li>Settings</li> </ul>			
	Network	Access Users	List > <b>cpiplani</b>				
Users	v Not	work Acces	llear				
Latest Manual Network Scan Results	· Net	WOIR ACCESS	o oser				
	* Nan	ne cpiplani					
	Chat						
	Stat	us 🗹 Enab	oled -				
	Em	ail					
	▼ Pa	sswords					
	Pas	sword Type:	Internal User	S	•		
			Password			Re-Enter F	Password
	* Lo	gin Password	•••••			•••••	
	Ena	ble Password					

### Etapas de configuração no Portal de administração Duo

Etapa 1. Crie um nome de usuário e ative o Duo Mobile no dispositivo final.

Adicione o usuário na página da Web de administração de nuvem do Duo. Navegue até **Usuários** > **Adicionar usuários** conforme mostrado na imagem:

<b>&gt;u</b> ÷	<ol> <li>Search for users, grou</li> </ol>	ips, applications, or devices
Dashboard Policies	Dashboard > Users > Ad Add User	id User
Users Add User	Adding Users Most applications allo Learn more about add	w users to enroll themselves after they complete primary authentication. Ing users ${\rm G}$
Pending Envollments Buik Enroll Users Import Users Directory Sync Bypass Codes	Username	cpiplani Should match the primary authentication username.
2FA Devices Groups Administrators		Add User

Observação: certifique-se de que o usuário final tenha o aplicativo Duo instalado.

Instalação Manual do Aplicativo Duo para Dispositivos IOS

Instalação manual do aplicativo Duo para dispositivos Android

Etapa 2. Geração automática de código.

Adicione o número de telefone do usuário conforme mostrado na imagem:

Phones You may reamange the phones by dr	agging and dropping in the table.		Add Phone				
This user has no phones. Add one.							
	_						
Due	<ol> <li>Search for users, gr</li> </ol>	oups, applications, or devices					
Dashboard	Dashboard > Users > 1	piplani > Add Phone					
Policies	Add Bhon	0					
Applications	Add Phon	e					
Users	Type	Phone					
Add User		<ul> <li>Tablet</li> </ul>					
Pending Enrolments							
Buk Errol Users	Phone number	* +1 201-555-5555	ow extension field				
Directory Sync							
Bypass Codes		Add Phone					
2FA Devices							

Escolha Ativate Duo Mobile como mostrado na imagem:

Device Info					
	Not using Duo Mobile Activate Duo Mobile		<b>Model</b> Unknown	$\bigcirc$	<b>OS</b> Generic Smartp

Escolha Generate Duo Mobile Ativation Code como mostrado na imagem:

Dashboard			
	Dattors > those	Deneto Smartphone 3: Activate Duo Motole	
Potom	Activate	Duo Mobile	
Applications			
Users	This form allows yo mobile decise or as	to 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 attenticate do Duo Root.	
2FA Devices			
Planes	Note: Constanting a	In activation code will invalidate any existing Duo Motore oredentars for this device until it is activated with the new activation code.	
Hardware Tollera			
Michael & UDF	Prote	Generic Smartphone	
Groupe			
Administrations	Expiration	24 hours • after generation	
Reports			
owned a		Generale Dus Mobile Autoration Code	

Escolha Send Instructions by SMS como mostrado na imagem:

Dashboard Pulicies Applications Users	Activate Du	Stratighter 3 Ariterie Dur Made IO Mobile In code has been generated, and any oil oredentais have been invalidated. You now have the option to deliver the installation instructions and or
2FA Devices Prove Technol Technol	activation instructions to 1 Plane	e uaer by BMS. Generic Smartphone
Grisge Administrators Reports Settings	Installation Instructions	<ul> <li>Sand installation instructions via BMS</li> <li>Wetcome to Duct Please install Duo-Mobile from your app store.</li> </ul>
Dilling Report Signals processor for sequent. Account D Deployment D	Autoration Instructions	Band activation instructions via BMS     Is activate the spo. top and spon the link with Duo Mobile:
Regist Loss Reconstration (7 Uner Guide 17		Sand Instructions by SMS and align this step

**Clique** no link no aplicativo SMS e Duo é vinculado à conta de usuário na seção Informações do dispositivo, como mostrado na imagem:

Dashboard Policies Applications	Dashboard > Phones > Phone	•	
Users	cpiplani (Chakahu Piplani)	S <sub>2</sub> Attach a user	
2FA Devices Phones Hardware Tokens		Authentication devices can share multiple users	
WebAuthin & UDF			
Groups	Device Info		
Administrators	Using Duo Mobile 3.29.0	Model	05
Reports	PUO Reactivate Duo Mobile		( 💭 ) Android 9
Settings	O Last Seen 1 hour ago	$\smile$	$\smile$

### Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Faça login no FMC usando suas credenciais de usuário que foram adicionadas na página de identidade de usuário do ISE. Você deve receber uma notificação Duo PUSH em seu endpoint para Autenticação de dois fatores (2FA), aprová-la e o FMC fará login conforme mostrado na imagem:



No servidor ISE, navegue para **Operations > RADIUS > Live Logs**. Localize o nome de usuário usado para autenticação no FMC e selecione o relatório de autenticação detalhado na coluna de detalhes. Aqui, você deve verificar se a autenticação foi bem-sucedida, conforme mostrado na imagem:

Identity Services Engine

cisco

Overview		Steps	
Event	5200 Authentication succeeded	11001	Received RADIUS Access-Request
Username	coinlani	11017	RADIUS created a new session
Caernanie	Grippen ii	11117	Generated a new session ID
Endpoint Id		15049	Evaluating Policy Group
Endpoint Profile		15008	Evaluating Service Selection Policy
Lindpointertoine		15041	Evaluating Identity Policy
Authentication Policy	Default >> Default	15048	Queried PIP - Normalised Radius.RadiusFlo
Authorization Policy	Default >> Basic_Authenticated_Access	22072	Selected identity source sequence - All_Use
		15013	Selected Identity Source - Internal Users
Authorization Result	PermitAccess	24210	Looking up User in Internal Users IDStore -
		24212	Found User in Internal Users IDStore
		22037	Authentication Passed
with continuations. Brate the		15036	Evaluating Authorization Policy
uthentication Details		15048	Queried PIP - Radius.NAS-Port-Type
Source Timestamp	2019-07-11 03-50:38 694	15048	Queried PIP - Network Access.UserName
oodioo minootamp		15048	Queried PIP - IdentityGroup.Name
Received Timestamp	2019-07-11 03:50:38.694	15048	Queried PIP - EndPoints.LogicalProfile
Policy Server	ROHAN-ISE	15048	Queried PIP - Network Access.Authentication
		15016	Selected Authorization Profile - PermitAcces
Event	5200 Authentication succeeded	22081	Max sessions policy passed
Username	cpiplani	22080	New accounting session created in Session
User Type	User	11002	Returned RADIUS Access-Accept
Authentication Identity Store	Internal Users		

### Troubleshooting

Esta seção fornece as informações que você pode usar para solucionar problemas da sua configuração.

• Verifique as depurações no servidor proxy de autenticação Duo. Os logs estão localizados neste local:

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

Abra o arquivo **authproxy.log** em um editor de texto como o Notepad++ ou o WordPad.

Registra trechos de código quando credenciais incorretas são inseridas e a autenticação é rejeitada pelo servidor ISE.

<#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

No ISE, navegue até Operations > RADIUS > Live Logs para verificar os detalhes da autenticação.

Registre trechos de autenticação bem-sucedida com ISE e 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): 5 2019-08-04T18:56:30+0530 [duoauthproxy.lib.http.\_DuoHTTPClientFactory#info] Stopping factory <\_DuoHTTPC

### **Informações Relacionadas**

- <u>Autenticação de VPN RA usando Duo</u>
- <u>Suporte Técnico e Documentação Cisco Systems</u>

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.