

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

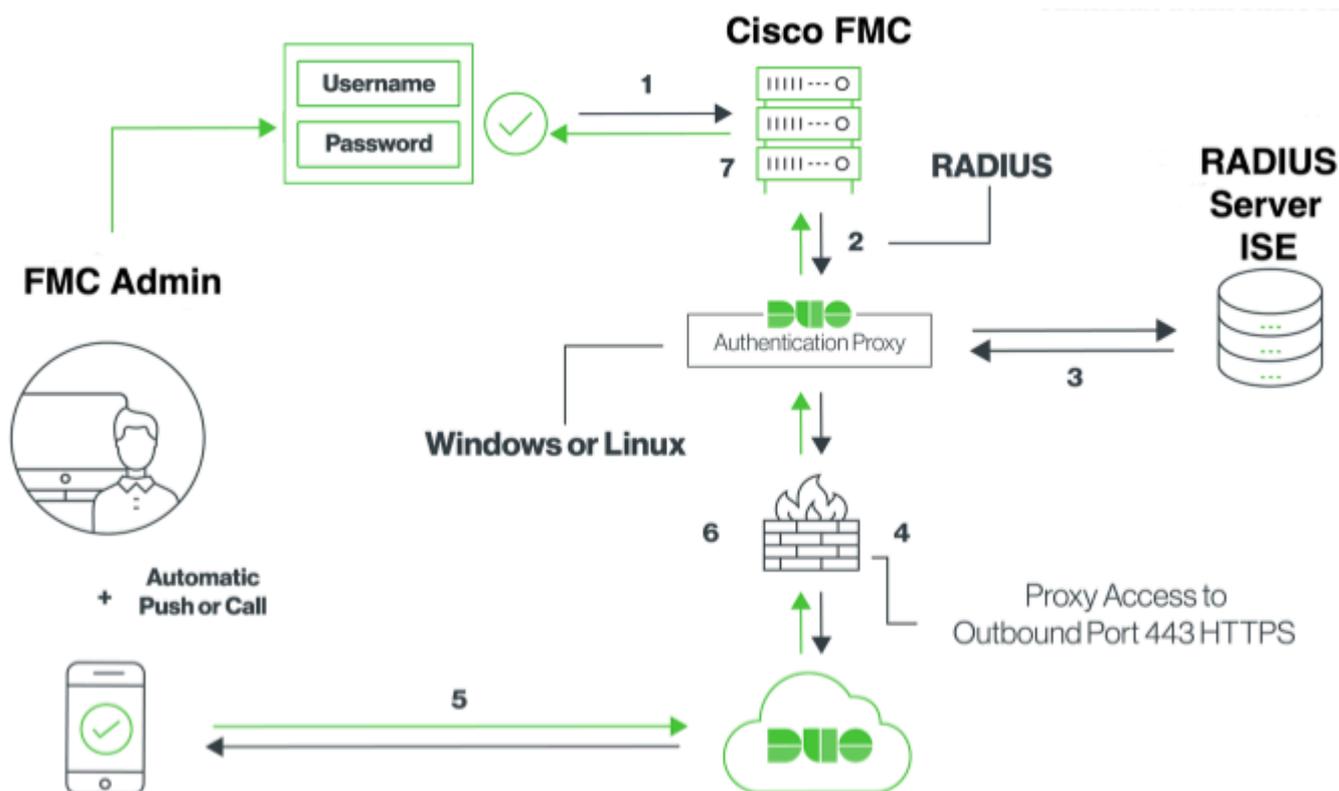
- Cisco Firepower Management Center (FMC) executando a versão 6.3.0
- Cisco Identity Services Engine (ISE) executando a versão 2.6.0.156
- Versão suportada do Windows (<https://duo.com/docs/authproxy-reference#new-proxy-install>) com conectividade para FMC, ISE e Internet para atuar como o servidor proxy 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 Active Directory 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

Etapas 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.

The screenshot shows the configuration page for External Authentication in the Palo Alto Networks management console. The navigation bar includes Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The main menu has Configuration, Users (highlighted), Domains, Integration, and Updates. The sub-menu includes Users, User Roles, and External Authentication (highlighted).

External Authentication Object

Authentication Method: RADIUS

Name: DuoAuthProxy

Description: [Empty field]

Primary Server

Host Name/IP Address: 10.106.44.177 (ex. IP or hostname)

Port: 1812

RADIUS Secret Key: [Masked with dots]

Backup Server (Optional)

Host Name/IP Address: [Empty field] (ex. IP or hostname)

Port: 1812

RADIUS Secret Key: [Empty field]

RADIUS-Specific Parameters

Timeout (Seconds): 30

Retries: 3

Access Admin: [Empty field]

Administrator: [Empty field]

Security Analyst

Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

Default User Role
To specify the default user role if user is not found in any group

Shell Access Filter

Administrator Shell Access User List
ex. user1, user2, user3
(Mandatory for FTD devices)

► **Define Custom RADIUS Attributes**

Additional Test Parameters

User Name

Password

*Required Field

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

Overview Analysis Policies Devices Objects AMP Intelligence Configuration **Users** Domains Integration Updates Licenses

Users User Roles External Authentication

Default User Role: **None** Shell Authentication: Disabled

Name

1. DuoAuthProxy

Note: One or more enabled external authentication objects don't have defined user roles.

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

User Configuration

User Name:

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
- Network Admin
- Maintenance User
- Discovery Admin
- Threat Intelligence Director (TID) User

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
```

```
Sample IP Address of the ISE server
```

```
secret=cisco
```

Password configured on the ISE server in order to register the network device

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

```
<#root>
```

```
[radius_server_auto]
ikey=xxxxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-xxxxxxx.duosecurity.com

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 ([Duo Admin Login](#)) e navegue para **Aplicativos > Proteger** um aplicativo. Em seguida, selecione o aplicativo de autenticação RADIUS como mostrado na imagem:

RADIUS

See the [RADIUS documentation](#) to integrate Duo into your RADIUS-enabled platform.

Details

Integration key	<input type="text" value="REDACTED"/>	select
Secret key	Click to view.	select
Don't write down your secret key or share it with anyone.		
API hostname	<input type="text" value="REDACTED"/>	select

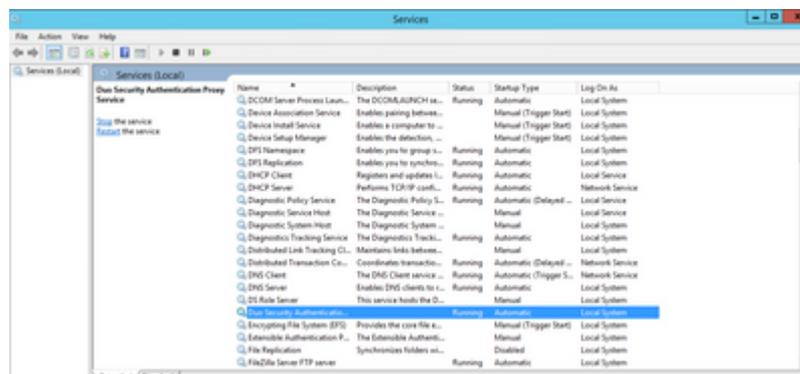
Chave de integração = ikey

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:



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:

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

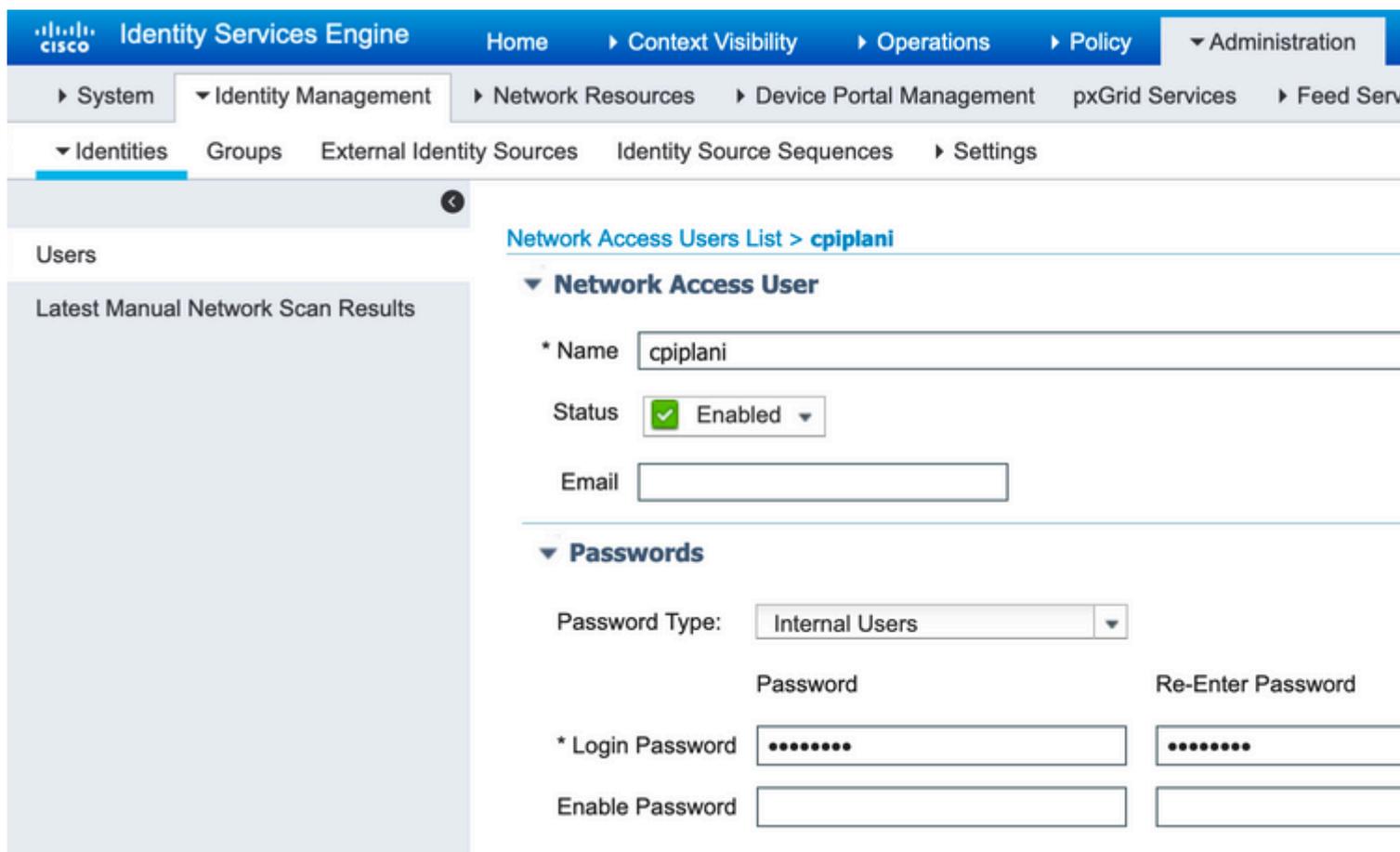
The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Network Resources > Network Devices. The left sidebar shows 'Network Devices' with sub-items 'Default Device' and 'Device Security Settings'. The main content area is titled 'Network Devices List > DuoAuthproxy' and 'Network Devices'. The configuration fields are: Name: DuoAuthproxy; Description: (empty); IP Address: (dropdown menu); * IP: 10.106.44.177; * Device Profile: Cisco; Model Name: (dropdown menu); Software Version: (dropdown menu).

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

The screenshot shows the RADIUS Authentication Settings page in the Cisco ISE interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Network Resources > Network Devices > RADIUS Authentication Settings. The left sidebar is the same as in the previous screenshot. The main content area is titled 'RADIUS Authentication Settings' and 'RADIUS UDP Settings'. The configuration fields are: Protocol: RADIUS; * Shared Secret: (masked with dots); Use Second Shared Secret: (checkbox, unchecked); CoA Port: 1700.

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

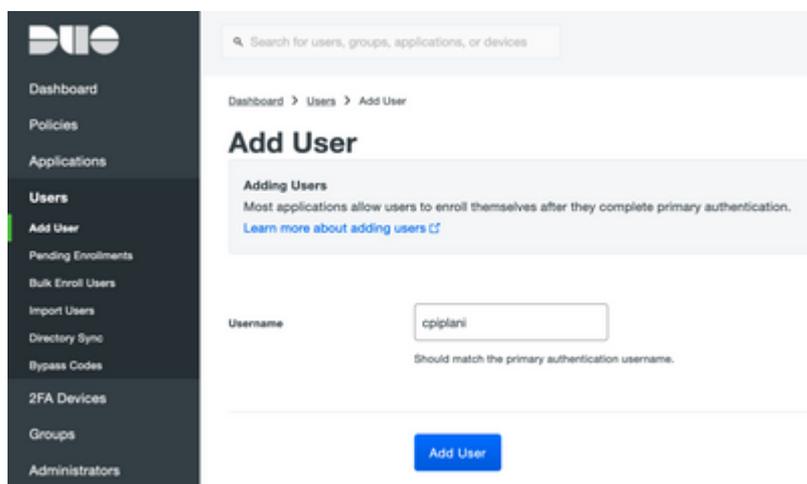
identidade como mostrado na imagem:



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:



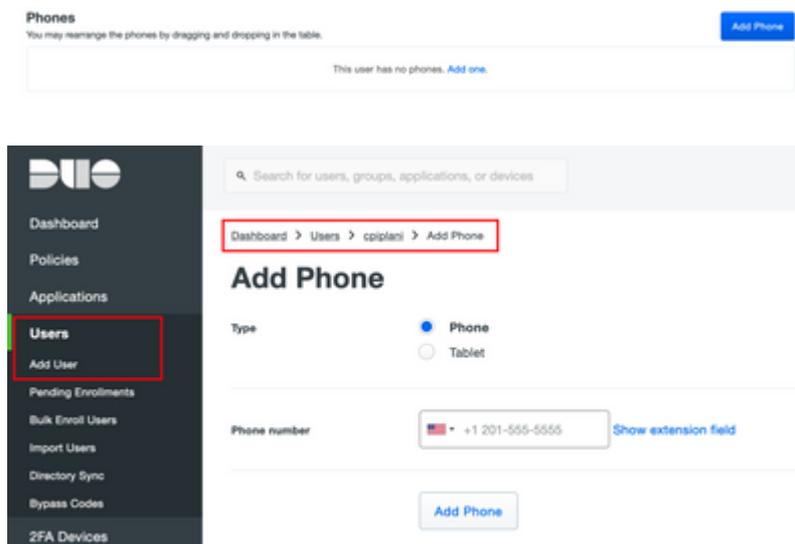
Observação: certifique-se de que o usuário final tenha o aplicativo Duo instalado.

[Instalação Manual do Aplicativo Duo para Dispositivos IOS](#)

[Instalação manual do aplicativo Duo para dispositivos Android](#)

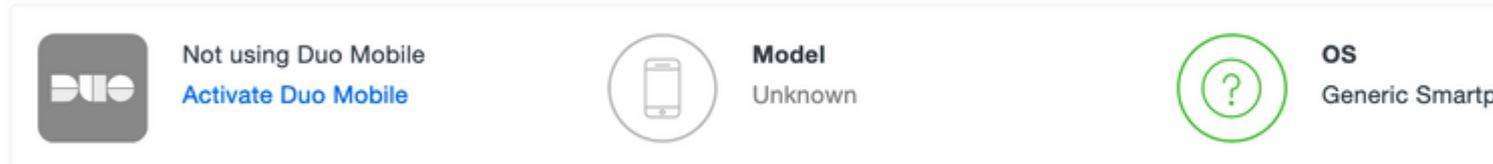
Etapa 2. Geração automática de código.

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

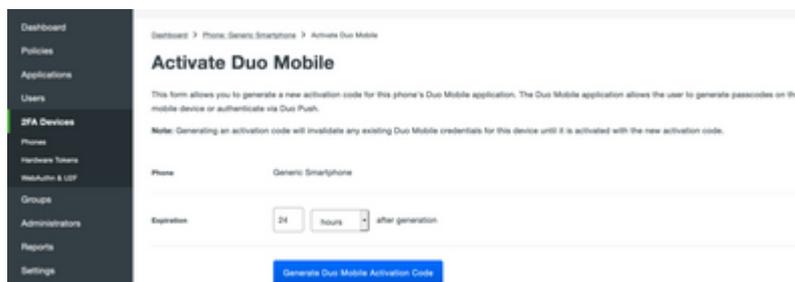


Escolha **Ativate Duo Mobile** como mostrado na imagem:

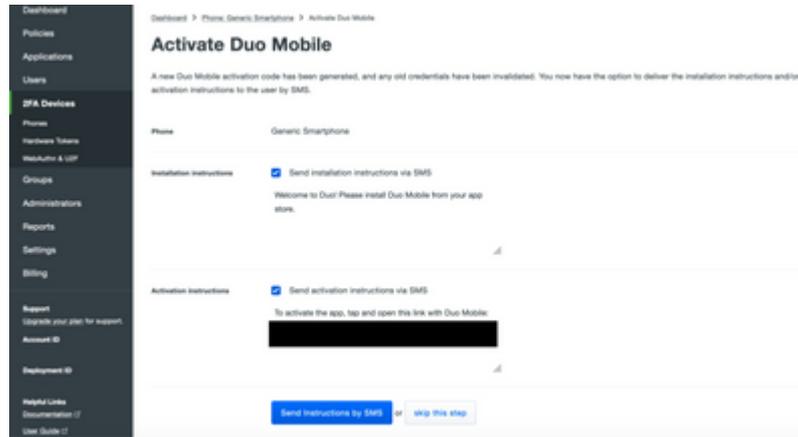
Device Info



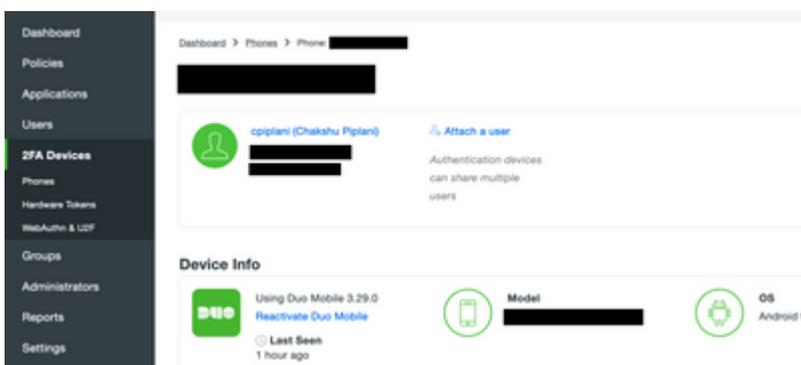
Escolha **Generate Duo Mobile Ativation Code** como mostrado na imagem:



Escolha **Send Instructions by SMS** como mostrado na imagem:



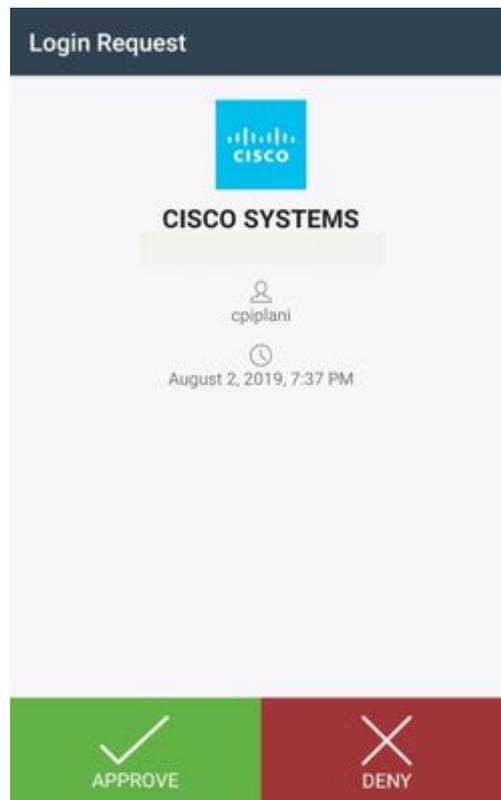
Clique no link no aplicativo SMS e Duo é vinculado à conta de usuário na seção Informações do dispositivo, como mostrado na imagem:



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

Overview

Event	5200 Authentication succeeded
Username	cpiplani
Endpoint Id	
Endpoint Profile	
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2019-07-11 03:50:38.694
Received Timestamp	2019-07-11 03:50:38.694
Policy Server	ROHAN-ISE
Event	5200 Authentication succeeded
Username	cpiplani
User Type	User
Authentication Identity Store	Internal Users

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.RadiusFlo
- 22072 Selected identity source sequence - All_Us
- 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 - PermitAcces
- 22081 Max sessions policy passed
- 22080 New accounting session created in Session
- 11002 Returned RADIUS Access-Accept

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 ('10.197.223.76', 34524)
```

```
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 rejected
```

```
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 ('10.197.223.2
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 <_DuoHTTPC
2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5): C
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 [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): S
2019-08-04T18:56:30+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPC
```

Informações Relacionadas

- [Autenticação de VPN RA usando Duo](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

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.