

Configurar a autenticação VPN SSL através de FTD, ISE, DUO e Active Directory

Contents

[Introdução](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configurações de FTD.](#)

[Integrar um servidor RADIUS no Firepower Management Center \(FMC\)](#)

[Configure a VPN remota.](#)

[Configurações do ISE.](#)

[Integre o DUO como um Servidor Radius Externo.](#)

[Integre o FTD como um dispositivo de acesso à rede.](#)

[Configurações DUO.](#)

[Instalação do Proxy DUO.](#)

[Integre o DUO Proxy com o ISE e o DUO Cloud.](#)

[Integrar o DUO com o Active Directory.](#)

[Exportar contas de usuário do Active Directory \(AD\) via Nuvem do DUO.](#)

[Inscreva usuários na nuvem do Cisco DUO.](#)

[Procedimento de validação da configuração.](#)

[Problemas comuns.](#)

[Cenário de trabalho.](#)

[Erro11353 Não há mais servidores RADIUS externos: não é possível executar failover](#)

[As sessões RADIUS não são exibidas nos registros ao vivo do ISE.](#)

[Troubleshooting Adicional.](#)

Introdução

Este documento descreve a integração de SSLVPN no Firepower Threat Defense usando o Cisco ISE e o DUO Security para AAA.

Requisitos

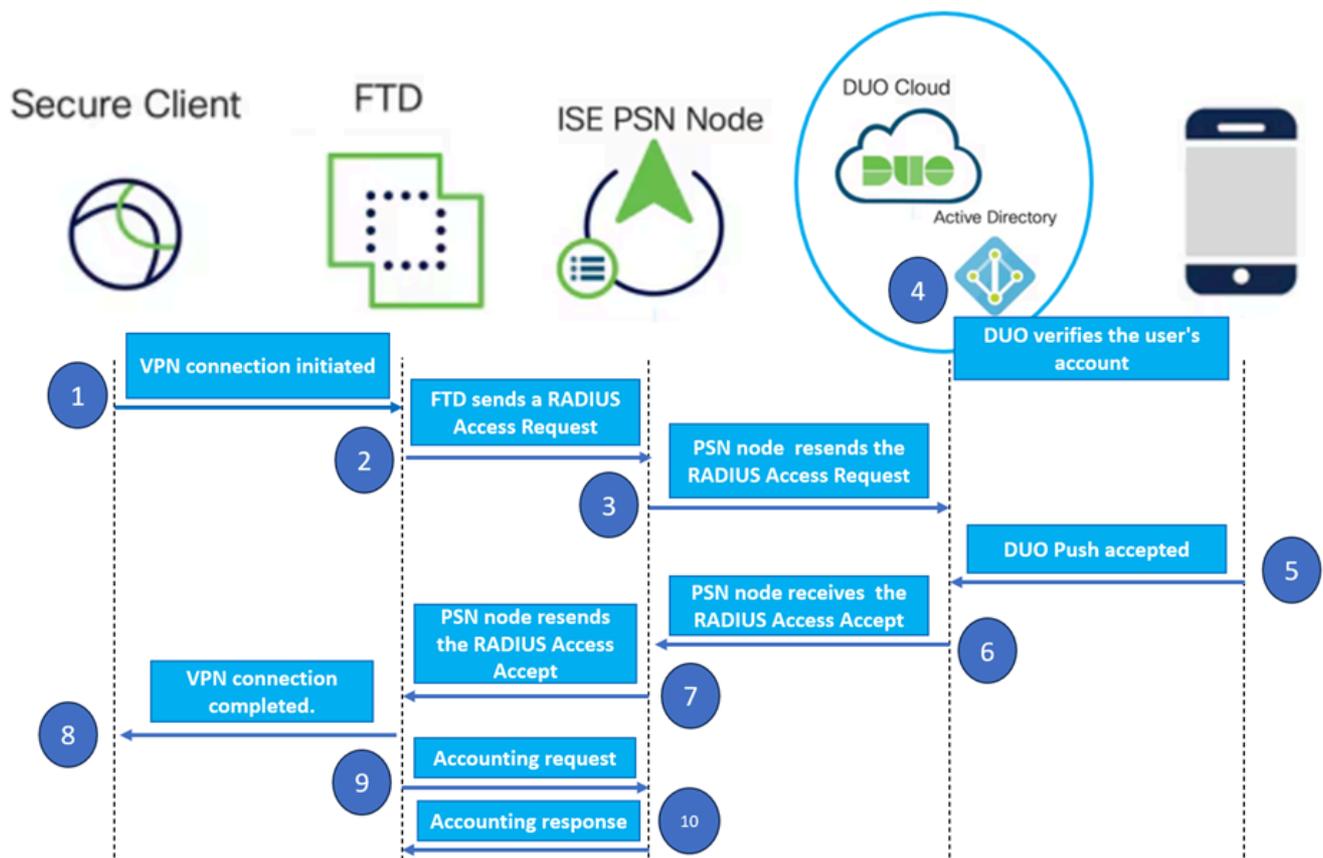
- ISE 3.0 ou posterior.
- FMC 7.0 ou superior.
- FTD 7.0 ou superior.
- Proxy de autenticação DUO.
- Licenciamento do ISE Essentials
- Licenciamento do DUO Essentials.

Componentes Utilizados

- Patch 3 do ISE 3.2
- CVP 7.2.5
- FTD 7.2.5
- Proxy DUO 6.3.0
- Any Connect 4.10.08029

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.

Diagrama de Rede



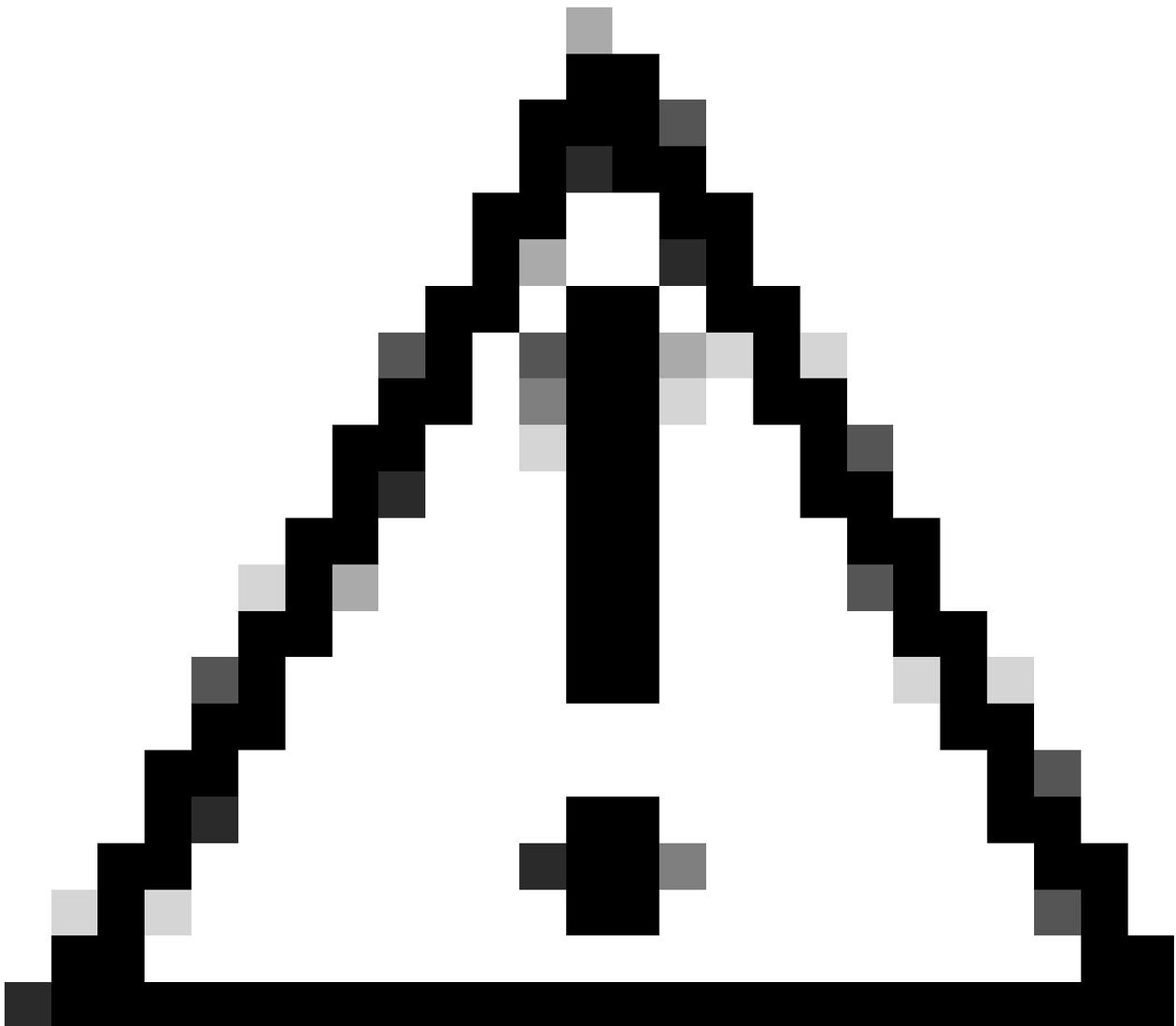
Topologia.

Em nossa solução proposta, o Cisco ISE é um proxy de servidor RADIUS crucial. Em vez de avaliar diretamente as políticas de autenticação ou autorização, o ISE é configurado para encaminhar os pacotes RADIUS do FTD para o Proxy de Autenticação DUO.

O Proxy de Autenticação DUO opera como um intermediário dedicado dentro deste fluxo de autenticação. Instalado em um servidor Windows, ele preenche a lacuna entre o Cisco ISE e a nuvem do DUOs. A função principal do proxy é transmitir solicitações de autenticação - encapsuladas dentro de pacotes RADIUS - para a nuvem DUO. Em última análise, a nuvem DUO

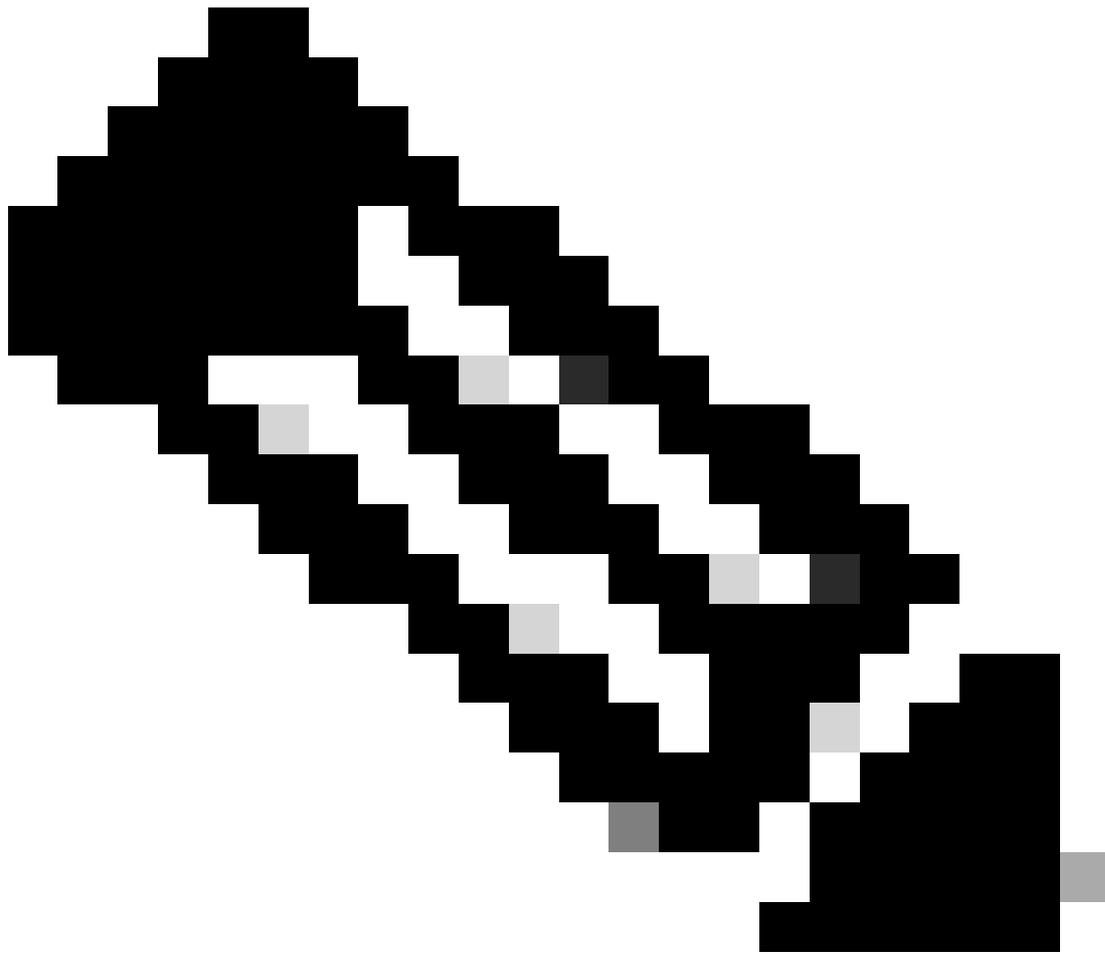
permite ou nega o acesso à rede com base nas configurações de autenticação de dois fatores.

1. O usuário inicia o processo de autenticação da VPN inserindo seu nome de usuário e senha exclusivos.
2. O Firewall Threat Defense (FTD) envia a solicitação de autenticação ao Cisco Identity Services Engine (ISE).
3. O Nó de Serviços de Política (PSN) encaminha a solicitação de autenticação ao Servidor Proxy de Autenticação DUO. Subsequentemente, o Servidor de Autenticação DUO valida as credenciais por meio do serviço de Nuvem DUO.
4. O DUO Cloud valida o nome de usuário e a senha em relação ao seu banco de dados sincronizado.



Cuidado: a sincronização entre a nuvem do DUO e as organizações do Active Directory precisa estar ativa para manter um banco de dados de usuário atualizado na nuvem do DUO.

5. Após a autenticação bem-sucedida, a nuvem DUO inicia um Push DUO para os usuários registrados no dispositivo móvel por meio de uma notificação de push criptografada segura. O usuário deve aprovar o Push DUO para confirmar sua identidade e continuar.
6. Depois que o usuário aprova o Push DUO, o Servidor Proxy de Autenticação DUO envia uma confirmação de volta ao PSN para indicar que a solicitação de autenticação foi aceita pelo usuário.
7. O nó PSN envia a confirmação ao FTD para informar que o usuário foi autenticado.
8. O FTD recebe a confirmação de autenticação e estabelece a conexão VPN ao terminal com as medidas de segurança apropriadas em vigor.
9. O FTD registra os detalhes da conexão VPN bem-sucedida e transmite com segurança os dados de contabilidade de volta ao nó ISE para fins de manutenção de registros e auditoria.
10. O nó do ISE registra as informações de contabilidade nos seus registros, garantindo que todos os registros sejam armazenados de forma segura e estejam acessíveis para futuras auditorias ou verificações de conformidade.



Note:

A configuração neste guia utiliza os próximos parâmetros de rede:

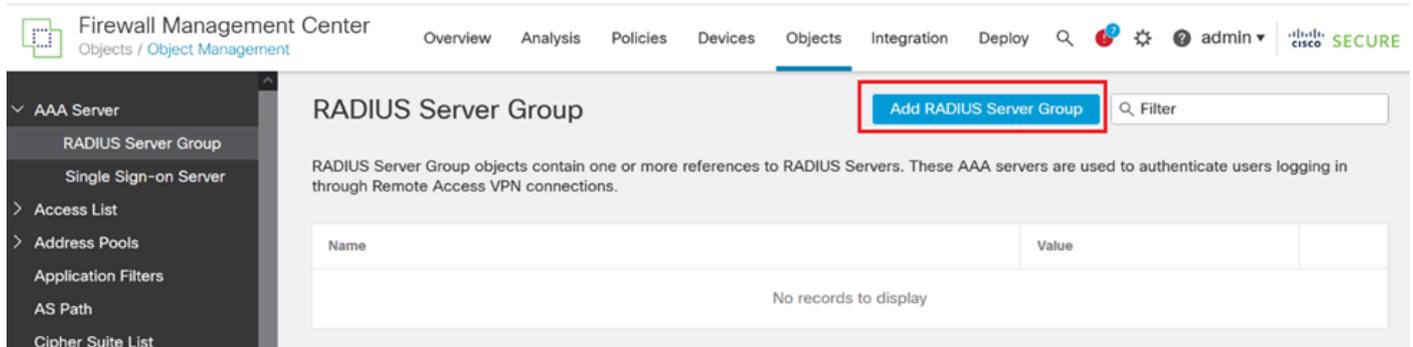
- IP do nó do servidor de rede primário (PNS): 10.4.23.21
- IP Firepower Threat Defense (FTD) para VPN de mesmo nível: 10.4.23.53
- IP do proxy de autenticação DUO: 10.31.126.207
- Nome do domínio: testlab.local

Configurações

Configurações de FTD.

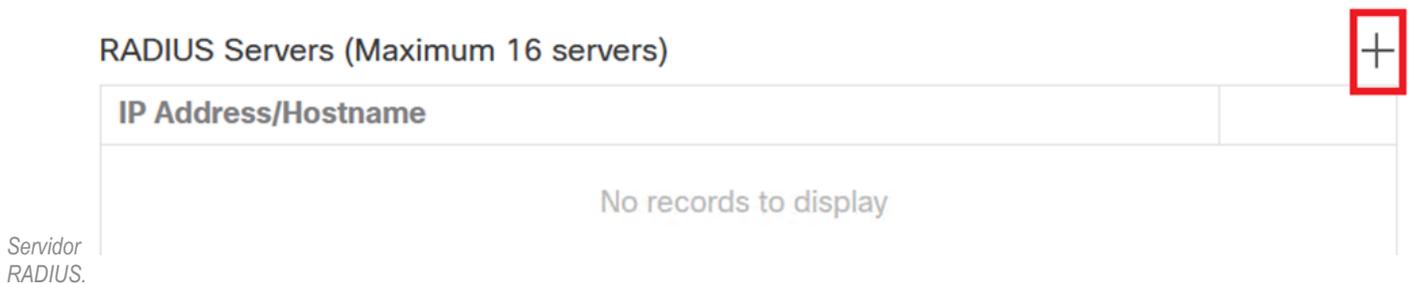
Integrar um servidor RADIUS no Firepower Management Center (FMC)

1. Para acessar ao FMC, abra o browser e introduza o endereço IP do FMC para abrir a Interface Gráfica do Utilizador (GUI).
2. Navegue até o menu Objects, selecione AAA Server e prossiga para a opção RADIUS Server Group.
3. Clique no botão Add RADIUS Server Group para criar um novo grupo para servidores RADIUS.



RADIUS Server Group (Grupo de servidores RADIUS).

4. Insira um nome descritivo para o novo grupo de servidores AAA RADIUS para garantir uma identificação clara dentro da sua infraestrutura de rede.
5. Continue para adicionar um novo Servidor RADIUS selecionando a opção apropriada na configuração do grupo.



6. Especifique o endereço IP dos servidores RADIUS e insira a chave secreta compartilhada.



Nota: É essencial garantir que essa chave secreta seja compartilhada com segurança com o servidor ISE para estabelecer uma conexão RADIUS bem-sucedida.

New RADIUS Server



IP Address/Hostname:*

10.4.23.21

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)

1812

Key:*

●●●●●●●●

Confirm Key:*

●●●●●●●●

Accounting Port: (1-65535)

1813

Timeout: (1-300) Seconds

10

Connect using:

Routing Specific Interface 

Cancel

Save

Novo servidor RADIUS.

7. Após configurar os detalhes do servidor RADIUS, clique em Salvar para preservar as configurações do grupo de servidores RADIUS.

Add RADIUS Server Group



Enable authorize only

Enable interim account update

Interval:* (1-120) hours

24

Enable dynamic authorization

Port:* (1024-65535)

1700

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname

10.4.23.21



Cancel

Save

Detalhes do Grupo de Servidores.

8. Para finalizar e implementar a configuração do Servidor AAA em sua rede, navegue para o menu Deploy e selecione Deploy All para aplicar as configurações.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration **Deploy** admin **SECURE**

AAA Server
RADIUS Server Group
Single Sign-on Server
Access List
Address Pools
Application Filters
AS Path

RADIUS Server Group

RADIUS Server Group objects contain one or through Remote Access VPN connections.

Name
ISE

FTD_01 | Ready for Deployment

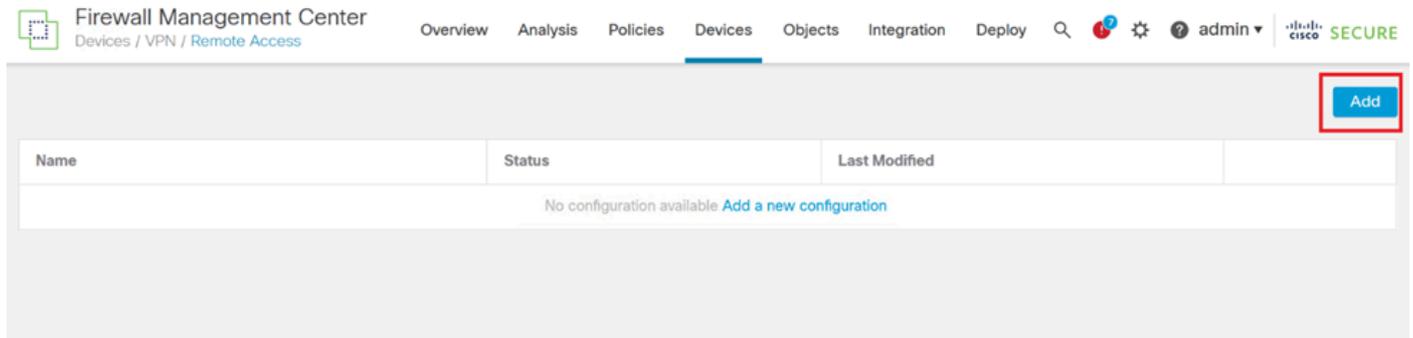
[Advanced Deploy](#) **Deploy All**

Implantando o servidor AAA.

Configure a VPN remota.

1. Navegue até Devices > VPN > Remote Access na GUI do FMC para iniciar o processo de configuração da VPN.

2. Clique no botão Add para criar um novo perfil de conexão VPN.

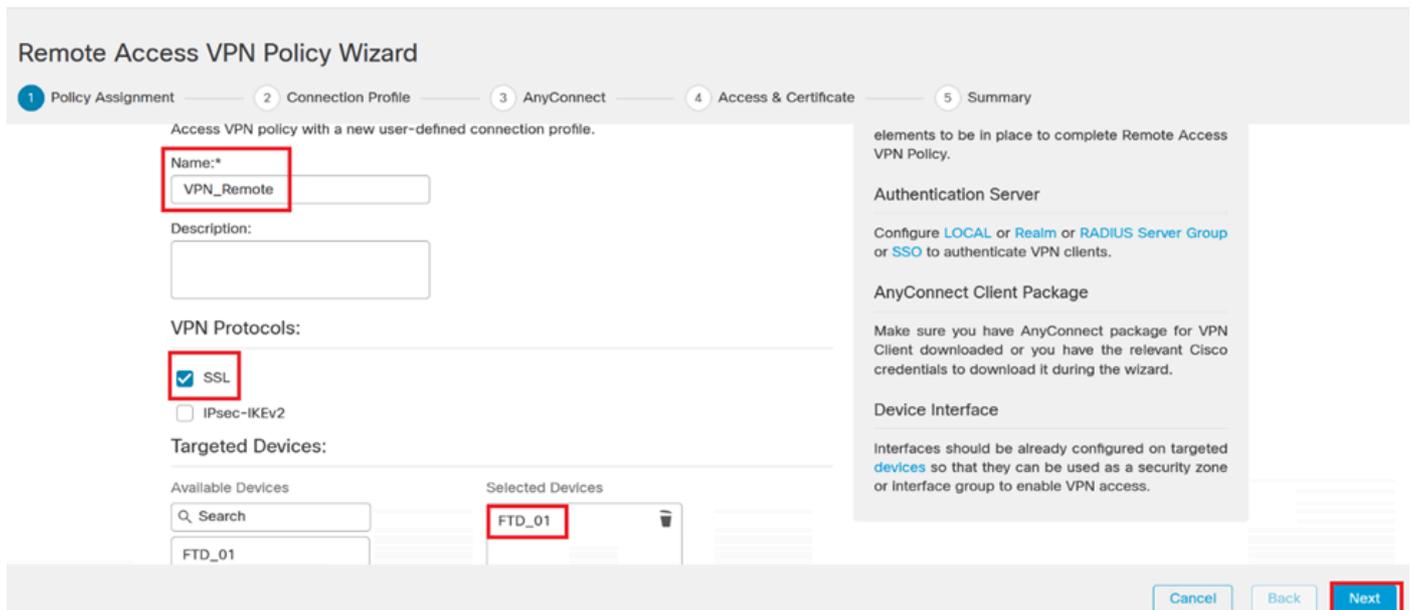


Perfil de conexão VPN.

3. Insira um nome exclusivo e descritivo para a VPN para ajudar a identificá-la nas configurações de rede.

4. Escolha a opção SSL para garantir uma conexão segura usando o protocolo VPN SSL.

5. Na lista de dispositivos, selecione o dispositivo FTD específico.



Configurações de VPN.

6. Configure o método AAA para utilizar o nó PSN nas configurações de autenticação.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: **AAA Only** ▼

Authentication Server:* **ISE** ▼ +

(LOCAL or Realm or RADIUS)

Fallback to LOCAL Authentication

Authorization Server: **Use same authentication server** ▼ +

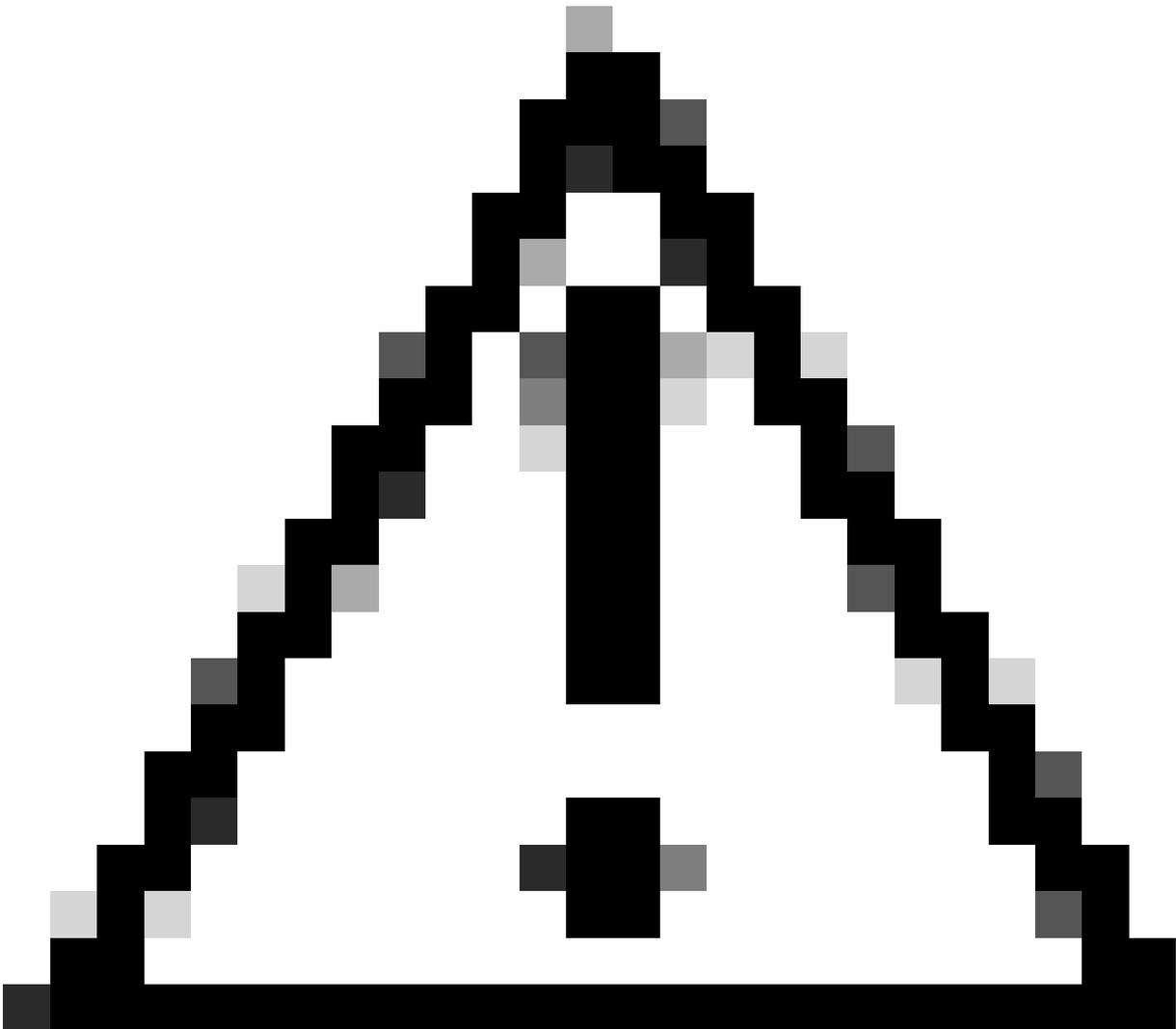
(realm or RADIUS)

Accounting Server: **ISE** ▼ +

(RADIUS)

Perfil de conexão.

7. Configure a atribuição dinâmica de endereço IP para VPN.



Cuidado: Por exemplo, o pool de VPNs DHCP foi selecionado.

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ⓘ

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: 

IPv6 Address Pools: 

Pool de endereços IP.

8. Continue para criar uma nova Política de Grupo.

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* 

[Edit Group Policy](#)

Política de grupo.

9. Nas configurações de Diretiva de Grupo, verifique se o protocolo SSL está selecionado.

Add Group Policy



Name:*

VPN_Remote_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

Cancel

Save

Protocolos VPN.

10. Crie um novo Pool VPN ou selecione um existente para definir o intervalo de endereços IP disponíveis para clientes VPN.

Add Group Policy



Name:*

VPN_Remote_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IP Address Pools:



Name

IP Address Range

Cancel

Save

Pool VPN.

11. Especifique os detalhes do servidor DNS para a conexão VPN.

Add Group Policy



Name:*

VPN_Remote_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Primary DNS Server:

+

Secondary DNS Server:

+

Primary WINS Server:

+

Secondary WINS Server:

+

DHCP Network Scope:

+

Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

Cancel

Save

Configurações DNS.



Aviso: observe que recursos adicionais como as opções Banner, Split Tunneling, AnyConnect e Advanced são consideradas opcionais para esta configuração.

12. Depois de configurar os detalhes necessários, clique em Próximo para prosseguir para a próxima fase da configuração.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Use AAA Server (Realm or RADIUS only)

 Use DHCP Servers

 Use IP Address Pools

IPv4 Address Pools:

IPv6 Address Pools:

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* +

[Edit Group Policy](#)

Cancel Back **Next**

Política de grupo.

13. Selecione o pacote AnyConnect apropriado para os usuários VPN. Se o pacote necessário não estiver listado, você tem a opção de adicionar o pacote necessário neste estágio.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

Select at least one AnyConnect Client image

[Show Re-order buttons](#) +

<input type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input type="checkbox"/>	anyconnect-win-4.10.08029-we...	anyconnect-win-4.10.08029-webdeploy-k9...	Windows

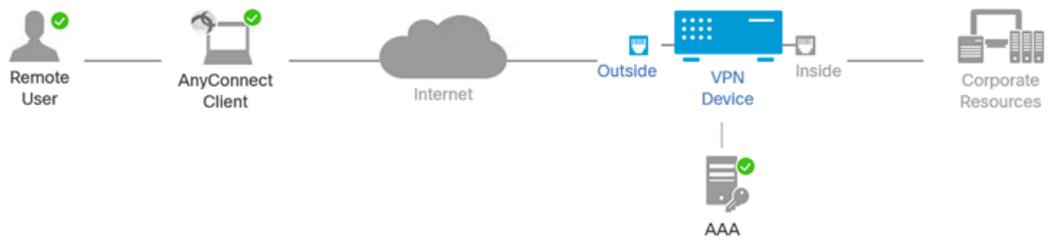
Cancel Back **Next**

Instalação do pacote.

14. Escolha a interface de rede no dispositivo FTD no qual deseja ativar o recurso remoto de VPN.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary



Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

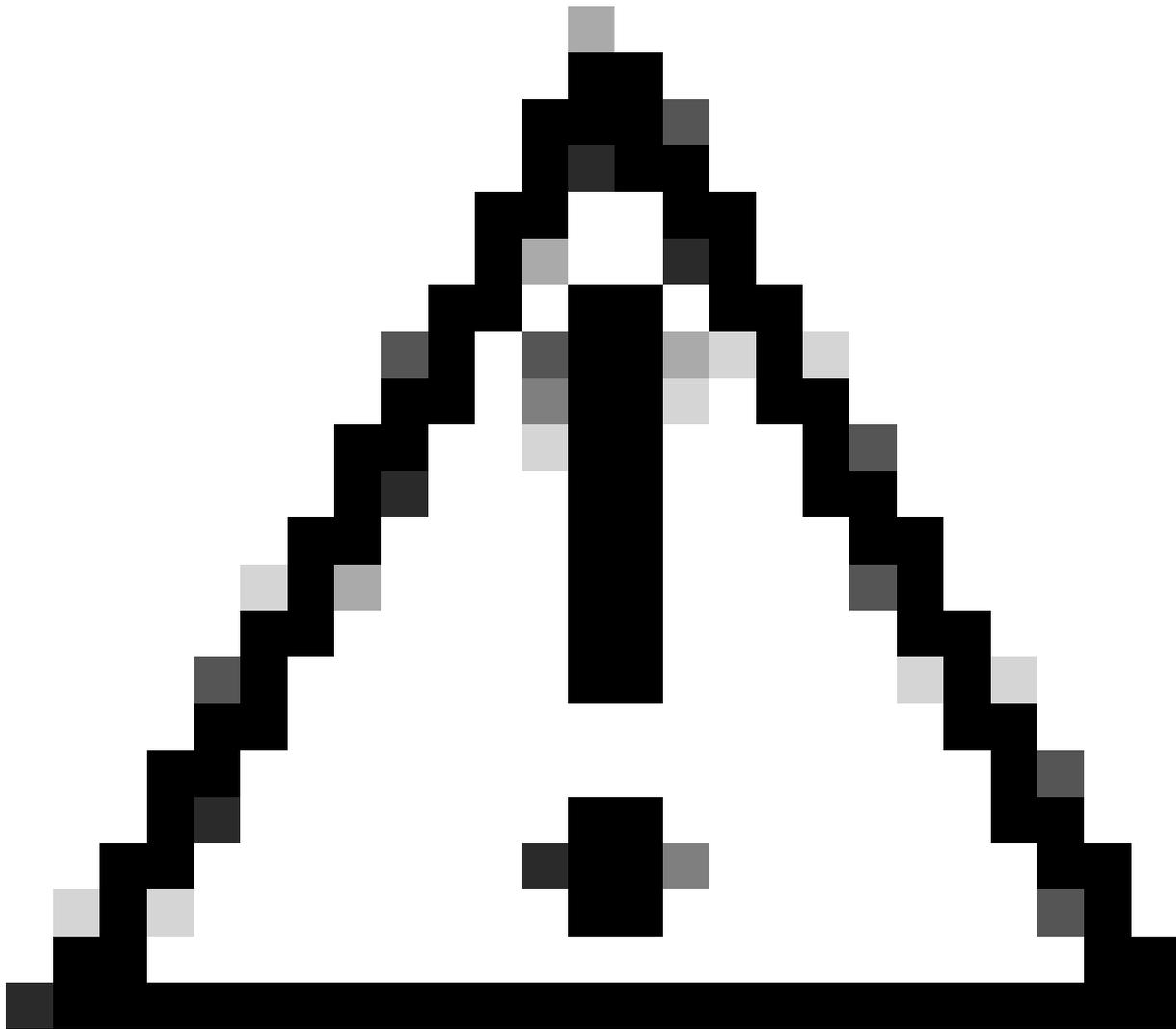
Interface group/Security Zone:* +

Enable DTLS on member interfaces

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Interface VPN

15. Estabeleça um processo de registro de Certificado selecionando um dos métodos disponíveis para criar e instalar o certificado no firewall, que é crucial para conexões VPN seguras.



Cuidado: por exemplo, um certificado autoassinado foi selecionado neste guia.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:*

 +

Certificado do dispositivo.

Add Cert Enrollment



Name*

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

SCEP

Enrollment URL:*

Self Signed Certificate

EST

Challenge Password:

SCEP

Confirm Password:

Manual

PKCS12 File

Retry Period:

1 (Range 1-60)

Retry Count:

10 (Range 0-100)

Fingerprint:

Cancel

Save

Inscrição no Cert.

16. Clique em Próximo quando a inscrição de certificado estiver configurada.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

will access for VPN connections.

Interface group/Security Zone:* +

Enable DTLS on member interfaces

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Resumo de acesso e serviços

17. Revise o resumo de todas as suas configurações para garantir que elas sejam precisas e reflitam a configuração pretendida.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Firepower Management Center will configure an RA VPN Policy with the following settings

Name:	VPN_Remote
Device Targets:	FTD_01
Connection Profile:	VPN_Remote
Connection Alias:	VPN_Remote
AAA:	
Authentication Method:	AAA Only
Authentication Server:	ISE (RADIUS)
Authorization Server:	ISE (RADIUS)
Accounting Server:	ISE
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	Pool_VPN
Address Pools (IPv6):	-
Group Policy:	VPN_Remote_Policy
AnyConnect Images:	anyconnect-win-4.10.08029-webdeploy-k9.pkg
Interface Objects:	Outside
Device Certificates:	Cert_Enrollment

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update

An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption

If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- DNS Configuration

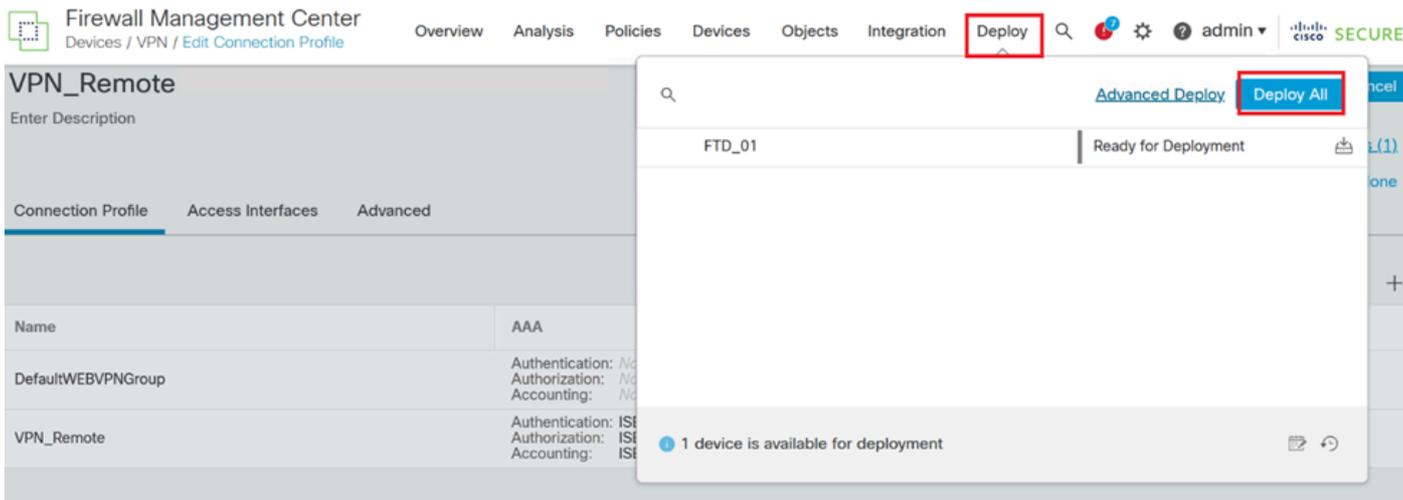
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- Port Configuration

SSL will be enabled on port 443. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.
- ▲ Network Interface Configuration

Make sure to add interface from targeted

Resumo das configurações de VPN.

18. Para aplicar e ativar a configuração de acesso remoto VPN, navegue para Implantar > Implantar Tudo e execute a implantação para o dispositivo FTD selecionado.



Implantando configurações de VPN.

Configurações do ISE.

Integre o DUO como um Servidor Radius Externo.

1. Navegue até Administration > Network Resources > External RADIUS Servers na interface administrativa do Cisco ISE.
2. Clique no botão Add para configurar um novo servidor RADIUS externo.



Servidores Radius Externos

3. Informe um nome para o Servidor Proxy DUO.
4. Insira o endereço IP correto para o servidor Proxy DUO para garantir a comunicação adequada entre o ISE e o servidor DUO.
5. Defina a chave secreta compartilhada.

Observação: esta chave secreta compartilhada deve ser configurada no Servidor Proxy DUO para estabelecer uma conexão RADIUS com êxito.

6. Depois que todos os detalhes forem inseridos corretamente, clique em **Enviar** para salvar a nova configuração do Servidor Proxy DUO.

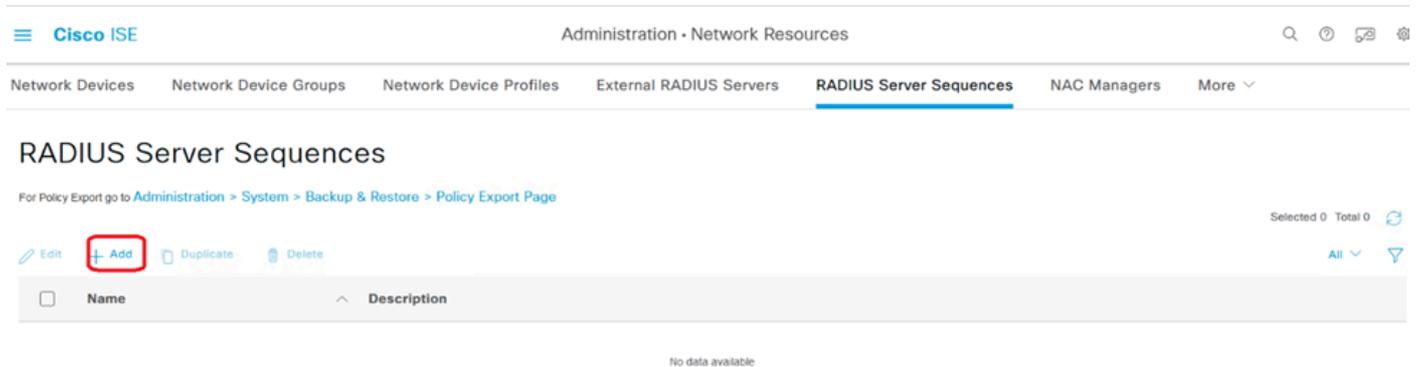
The screenshot shows the Cisco ISE Administration interface for configuring an External RADIUS Server. The breadcrumb path is Administration > Network Resources > External RADIUS Servers. The configuration form includes the following fields:

- Name:** DUO_Server
- Description:** (Empty text area)
- Host IP:** 10.31.126.207
- Shared Secret:** (Masked with 8 dots)

A "Show" button is located next to the Shared Secret field.

7. Continue em Administração > Sequências do Servidor RADIUS.

8. Clique em Adicionar para criar uma nova sequência de servidor RADIUS.

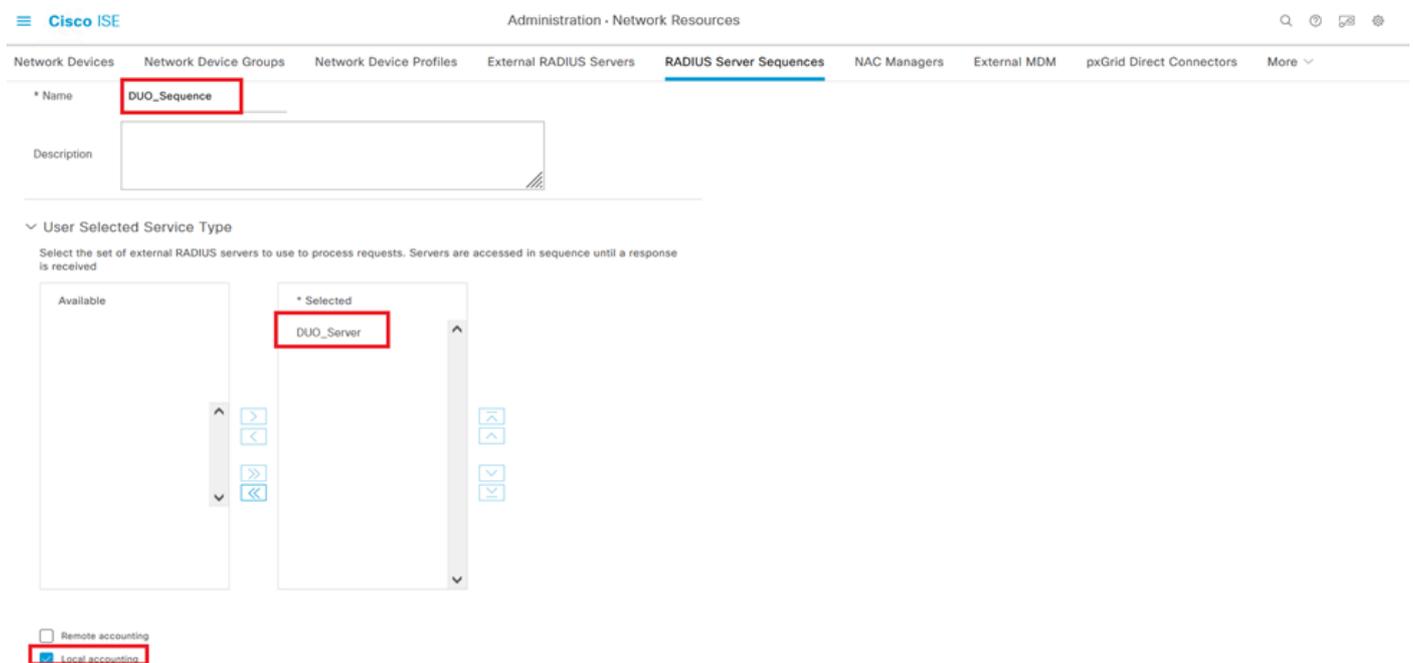


Sequências do servidor RADIUS

9. Forneça um nome distinto para a Sequência de Servidores RADIUS para facilitar a identificação.

10. Localize o Servidor RADIUS DUO previamente configurado, conhecido como DUO_Server neste guia e mova-o para a lista selecionada à direita para incluí-lo na sequência.

11. Clique em Submit para finalizar e salvar a configuração da Sequência de Servidor RADIUS.



Configuração de sequências de servidor Radius.

Integre o FTD como um dispositivo de acesso à rede.

1. Navegue até a seção Administração na interface do sistema e, a partir dela, selecione Recursos de Rede para acessar a área de configuração para dispositivos de rede.

2. Na seção Recursos de Rede, localize e clique no botão Adicionar para iniciar o processo de adição de um novo Dispositivo de Acesso à Rede.

Network Devices

Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers More ▾

Network Devices

Default Device

Device Security Settings

Selected 0 Total 0 🔄 ⚙

✎ Edit **+ Add** 📄 Duplicate 📄 Import 📄 Export ▾ 📄 Generate PAC 🗑 Delete ▾ All ▾ 🔍

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
No data available						

Network Access Devices (Dispositivos de acesso à rede).

3. Nos campos fornecidos, digite o nome do dispositivo de acesso à rede para identificá-lo na rede.
4. Continue para especificar o endereço IP do dispositivo FTD (Firepower Threat Defense).
5. Insira a chave previamente estabelecida durante a configuração do FMC (Firepower Management Center). Essa chave é essencial para a comunicação segura entre dispositivos.
6. Conclua o processo clicando no botão Submeter.

[Network Devices List](#) > **FTD**

Network Devices

Name

FTD

Description

IP Address ▾

* IP :

10.4.23.53

/

32



Adicionando FTD como NAD.

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret

••••••••

Show

Use Second Shared Secret ⓘ

Second Shared Secret

Show

CoA Port **1700**

Set To Default

Configurações de RADIUS

Configurações DUO.

Instalação do Proxy DUO.

Acesse o Guia de download e instalação do DUO Proxy clicando no próximo link:

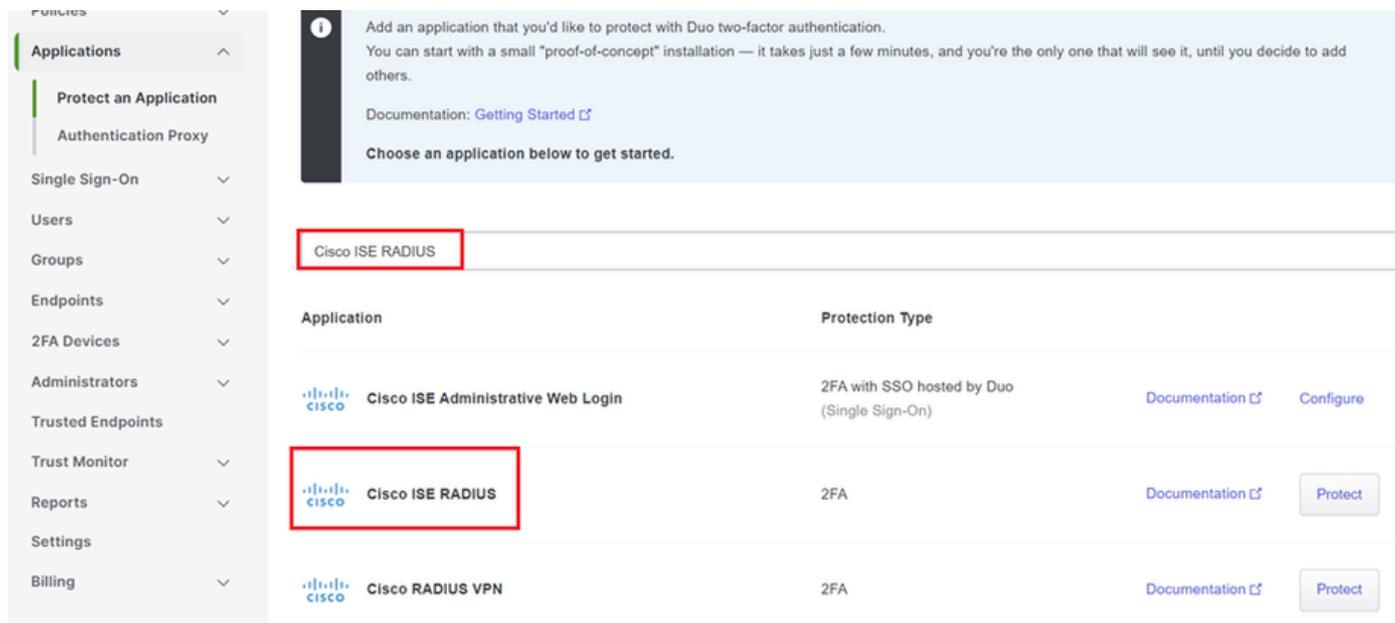
<https://duo.com/docs/authproxy-reference>

Integre o DUO Proxy com o ISE e o DUO Cloud.

1. Faça login no site do DUO Security em <https://duo.com/> usando suas credenciais.
2. Navegue até a seção Aplicações e selecione Proteger uma aplicação para continuar.

The screenshot displays the DUO Security dashboard. On the left is a navigation sidebar with the following items: Dashboard, Device Insight, Policies, Applications (highlighted with a red box), Protect an Application, Authentication Proxy, Single Sign-On, Users, Groups, Endpoints, and 2FA Devices. The main content area is titled 'Applications' and includes a 'Protect an Application' button in the top right corner. Below the title, there is a message: 'Manage your update to the new Universal Prompt experience, all in one place.' with buttons for 'See My Progress' and 'Get More Information'. At the bottom of the main area, there are two statistics: '0 All Applications' and '0 End of Support'. On the right side, there is a preview of a user interface with several cards. At the bottom right, there are 'Export' and 'Search' buttons.

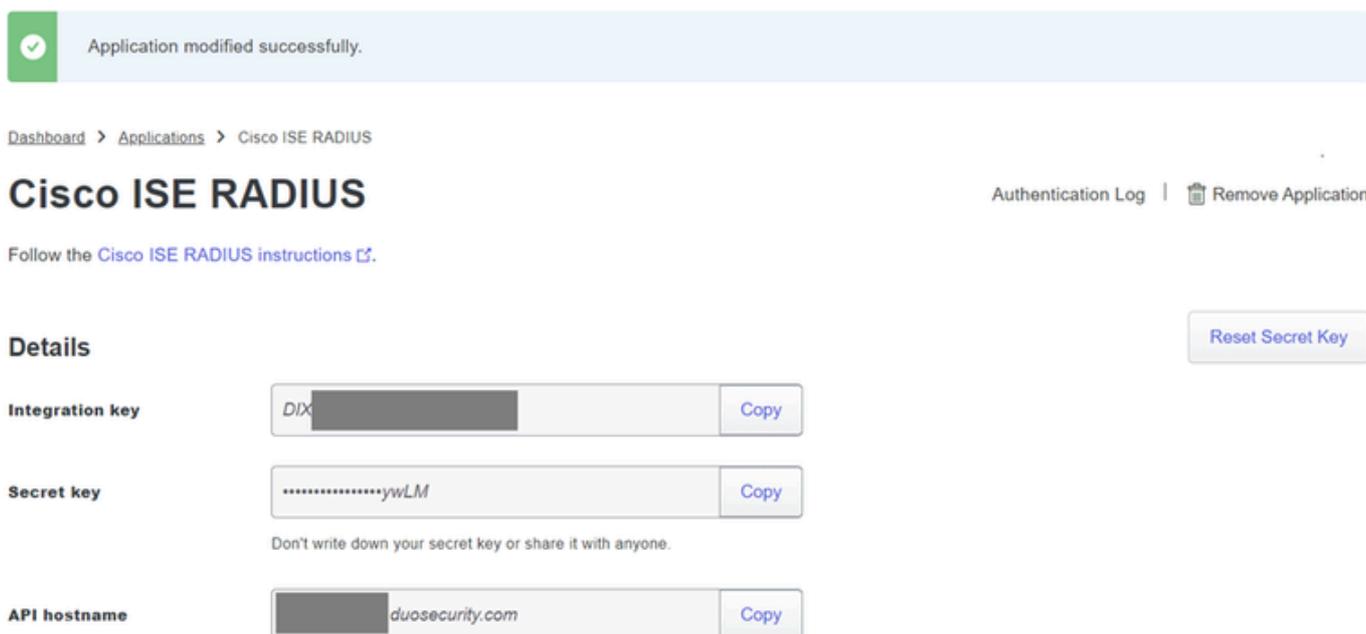
3. Procure a opção "Cisco ISE RADIUS" na lista e clique em Proteger para adicioná-la aos seus aplicativos.



opção ISE RADIUS

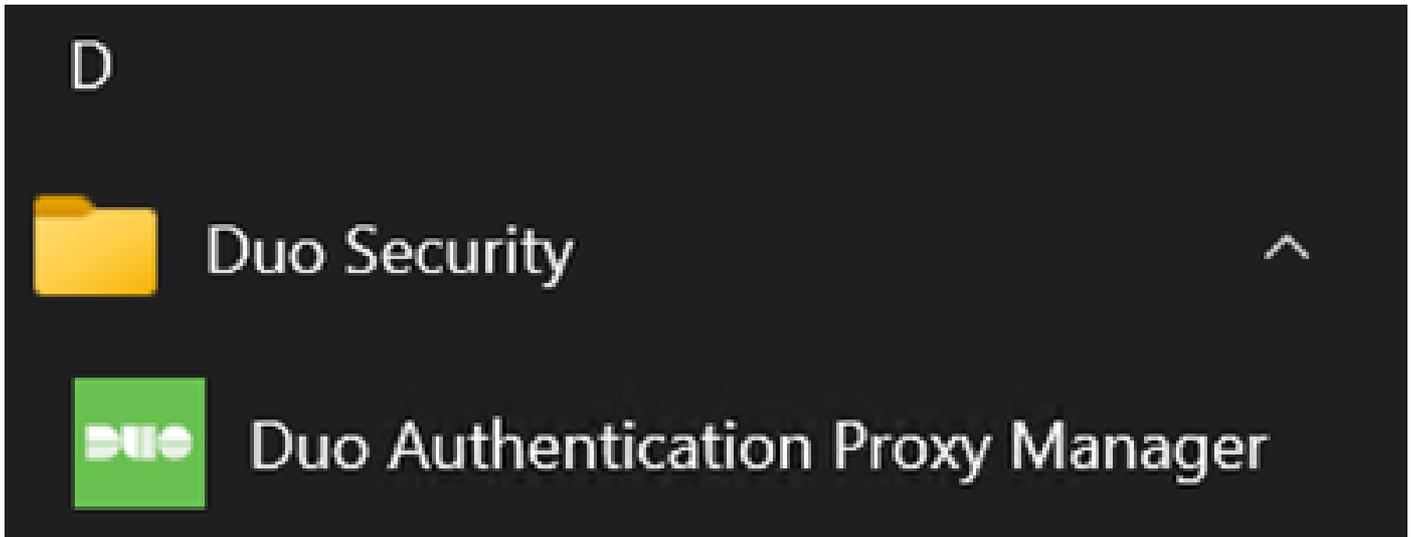
4. Após a adição bem-sucedida, você verá os detalhes do aplicativo DUO. Role para baixo e clique em Save.

5. Copie a chave de integração, a chave secreta e o nome do host da API fornecidos; esses itens são cruciais para as próximas etapas.



Detalhes do servidor ISE

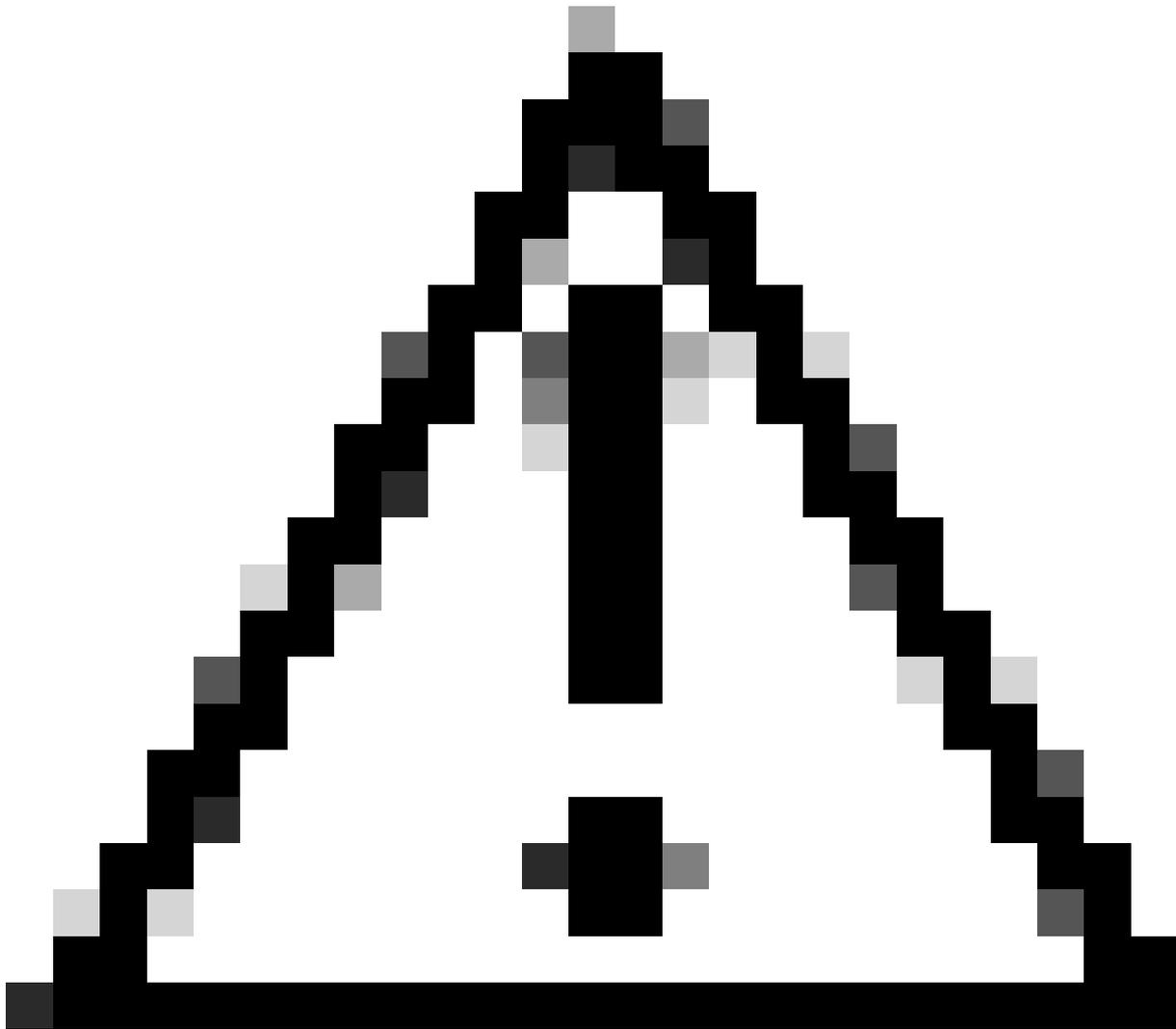
6. Inicie o DUO Proxy Manager em seu sistema para continuar com a configuração.



Gerenciador de proxy DUO

7. (Opcional) Se o Servidor Proxy DUO exigir uma configuração de proxy para se conectar à Nuvem DUO, insira os próximos parâmetros:

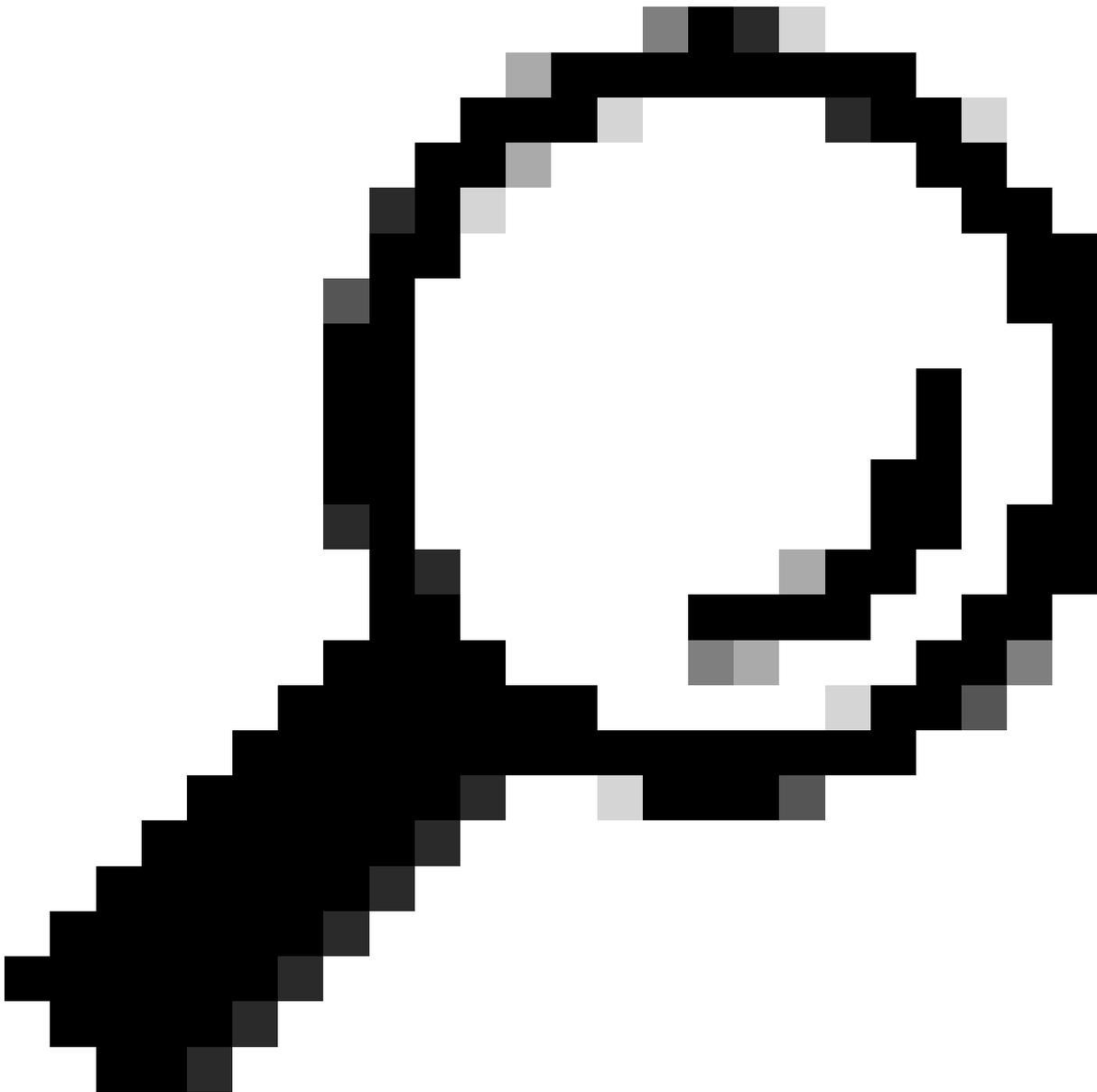
```
[main]
http_proxy_host=<Proxy IP Address or FQDN >
http_proxy_port=<port>
```



Cuidado: certifique-se de substituir e pelos detalhes reais do proxy.

8. Agora, utilize as informações copiadas anteriormente para concluir a configuração de integração.

```
[radius_server_auto]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
radius_ip_1=<ISE IP address>
radius_secret_1=<secret key configured in the external RADIUS server section>
failmode=safe
port=1812
client=ad_client
```



Dica: A linha `client=ad_client` é uma indicação de que o Proxy DUO autentica usando uma conta do Active Directory. Verifique se essas informações estão corretas para concluir a sincronização com o Active Directory.

Integrar o DUO com o Active Directory.

1. Integre o Proxy de Autenticação DUO ao seu Active Directory.

```
[ad_client]
host=<AD IP Address>
service_account_username=<service_account_username>
service_account_password=<service_account_password>
search_dn=DC=<domain>,DC=<TLD>
```

2. Junte-se ao seu Ative Directory com os serviços em nuvem DUO. Faça login em <https://duo.com/>.

3. Navegue até "Users" e selecione "Directory Sync" para gerenciar as configurações de sincronização.

Dashboard > Users

Users

Directory Sync | Import Users | Bulk Enroll Users | Add User

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).

0 Total Users | 0 Not Enrolled | 0 Inactive Users | 0 Trash | 0 Bypass Users | 0 Locked Out

Select (0) | ... | Export | Search

No users shown based on your search.

Sincronização de Diretórios

4. Clique em "Adicionar nova sincronização" e escolha "Ative Directory" entre as opções fornecidas.

Dashboard > Users > Directory Sync

Directory Sync

Add New Sync

Directory Syncs | Connections

You don't have any directories yet.

Adicionar Nova Sincronização

5. Selecione Adicionar nova conexão e clique em Continuar.

Adicionando novo Ative Diretory

6. Copie a chave de integração gerada, a chave secreta e o nome de host da API.

Detalhes do proxy de autenticação

7. Retorne à configuração do Proxy de Autenticação DUO e configure a seção [cloud] com os novos parâmetros obtidos, bem como as credenciais da conta de serviço para um administrador do Active Directory:

```
[cloud]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
service_account_username=<your domain>\<service_account_username>
service_account_password=<service_account_password>
```

8. Valide sua configuração selecionando a opção "validar" para garantir que todas as configurações estejam corretas.

```
1 [main]
2 http_proxy_host=cx[redacted]
3 http_proxy_port=3128
4
5 [radius_server_auto]
6 ikey=DIX[redacted]
7 skey=[redacted]uXWYwLM
8 api_host=a[redacted].duosecurity.com
9 radius_ip_1=10.4.23.21
10 radius_secret_1=po[redacted]
11 failmode=safe
12 port=1812
13 client=ad_client
14
15 [ad_client]
16 host=10.4.23.42
17 service_account_username=administrator
18 service_account_password=[redacted]
```

Configuração do Proxy DUO.

9. Após a validação, salve sua configuração e reinicie o serviço Proxy de Autenticação DUO para aplicar as alterações.

```
Running The Duo Authentication Proxy Connectivity Tool. This may take
several minutes...
[info] Testing section 'main' with configuration:
[info] {'http_proxy_host': 'cx[redacted]',
'http_proxy_port': '3128'}
[info] There are no configuration problems
[info]
[info] Testing section 'radius_server_auto' with configuration:
[info] {'api_host': '[redacted].duosecurity.com',
'client': 'ad_client',
'failmode': 'safe',
'http_proxy_host': '[redacted]',
'http_proxy_port': '3128',
'key': 'DIX[redacted]',
```

opção Reiniciar serviço.

10. De volta ao painel de administração do DUO, insira o endereço IP do servidor do Active Directory junto com o DN base para sincronização de usuário.

Directory Configuration

Domain controller(s)

Hostname or IP address (1) *

10.4.23.42

Port (1) *

389

[+ Add Domain controller](#)

The port is typically 389 for cleartext LDAP or STARTTLS, and 636 for LDAPS.

Base DN *

DC=testlab,DC=local

Enter the full distinguished name (DN) of the directory location to search for users and groups. We recommend setting this to the directory root (example: DC=domain,DC=local). If specifying the DN of an OU or container, ensure it is **above both the users and groups to sync**.

Configurações do diretório.

11. Selecione a opção Plain para configurar o sistema para autenticação não-NTLMv2.

Authentication type



Integrated

Performs Windows authentication from a domain-joined system.



NTLMv2

Performs Windows NTLMv2 authentication.



Plain

Performs username-password authentication.

Tipo de autenticação.

12. Salve suas novas configurações para garantir que a configuração seja atualizada.

 Delete Connection

Save

Status

Not connected

Add Authentication Proxy



Configure Directory

Connected Directory Syncs

User Syncs

[AD Sync](#)

opção Salvar

13. Utilize o recurso "testar conexão" para verificar se o serviço DUO Cloud pode se comunicar

com seu Ative Directory.

Authentication Proxy

1. To set up this directory, you need to install the Duo Authentication Proxy software on a machine that Duo can connect to and that can connect to your LDAP server. [View instructions](#)
2. Configure your Authentication Proxy. Update the `ikey`, `skey`, and `api_host` entries in the `[cloud]` section of your configuration, or [download a pre-configured file](#).

Integration key [Copy](#)

Secret key [Copy](#)

Don't write down your secret key or share it with anyone.

[Reset Secret Key](#)

API hostname [Copy](#)

3. If you are using NTLM or plain authentication, update the `[cloud]` section of your configuration with the username and password for the LDAP account that has read access for your LDAP directory.

```
service_account_username=myusername  
service_account_password=mypassword
```

4. Restart your Authentication Proxy.

5. [Test Connection](#).

Opção de conexão de teste.

14. Confirme se o status do Ative Directory é exibido como "Connected", indicando uma integração bem-sucedida.

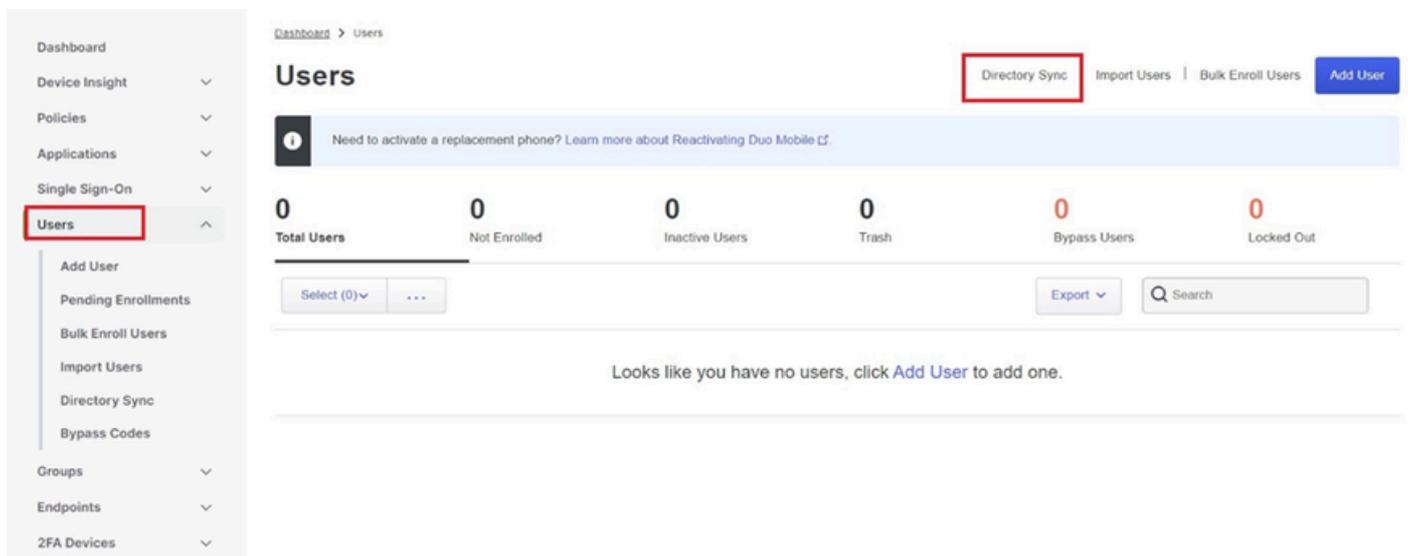
Status

Connected

Status bem-sucedido.

Exportar contas de usuário do Ative Directory (AD) via Nuvem do DUO.

1. Navegue até Users > Directory Sync no Duo Admin Panel para localizar as configurações relacionadas à sincronização de diretórios com o Ative Directory.

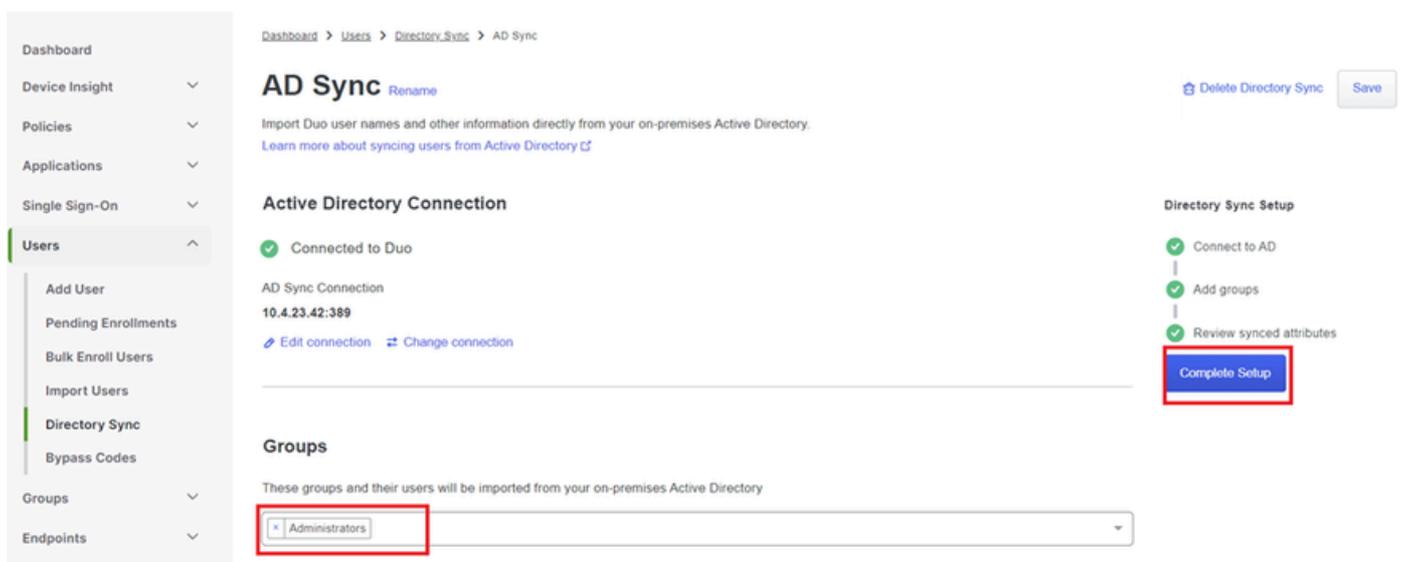


Lista de usuários.

2. Selecione a configuração do Ative Directory que deseja gerenciar.

3. Nas definições de configuração, identifique e escolha os grupos específicos no Ative Directory que deseja sincronizar com a Nuvem Duo. Considere o uso das opções de filtragem para sua seleção.

4. Clique em Concluir Configuração.



Sincronização do AD.

5. Para iniciar a sincronização imediatamente, clique em Sincronizar Agora. Isso exporta as contas de usuário dos grupos especificados no Ative Directory para a nuvem do Duo, permitindo que elas sejam gerenciadas no ambiente de segurança do Duo.

AD Sync Rename

Delete Directory Sync No Changes

Import Duo user names and other information directly from your on-premises Active Directory. [Learn more about syncing users from Active Directory](#)

Sync Controls

Sync status

Scheduled to automatically synchronize every 12 hours, next around 2:00 AM UTC [Pause automatic syncs](#)

Sync Now

Troubleshooting ▼

Active Directory Connection

✓ Connected to Duo

AD Sync Connection

10.4.23.42:389

[Edit connection](#)

[Change connection](#)

Iniciando Sincronização

Inscreva usuários na nuvem do Cisco DUO.

A inscrição do usuário permite a verificação de identidade por meio de vários métodos, como acesso a código, push DUO, códigos SMS e tokens.

1. Navegue até a seção Usuários no painel do Cisco Cloud.
2. Localize e selecione a conta do usuário que deseja inscrever.

Dashboard > Users

Users Directory Sync | Import Users | Bulk Enroll Users | Add User

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#)

1 Total Users **1** Not Enrolled **1** Inactive Users **0** Trash **0** Bypass Users **0** Locked Out

Select (0) ▼ ... Export ▼ Search

<input type="checkbox"/>	Username ▲	Name	Email	Phones	Tokens	Status	Last Login
<input checked="" type="checkbox"/>	administrator		oteg [REDACTED]			Active	Never authenticated

1 total

Lista de contas de usuário.

3. Clique no botão Enviar E-mail de Inscrição para iniciar o processo de inscrição.

administrator

Logs

Send Enrollment Email

Sync This User



This user has not enrolled yet. See our [enrollment documentation](#) to learn more about enrolling users.



This user was synced from the directory **AD Sync**. Some fields are read-only.

Username

administrator

Username aliases

[+ Add a username alias](#)

Users can have up to 8 aliases.

Optionally, you may choose to reserve using an alias number for a specific alias

(e.g., Username alias 1 should only be used for Employee ID).

Inscrição por e-mail.

4. Verifique a caixa de entrada de e-mail e abra o convite de inscrição para concluir o processo de autenticação.

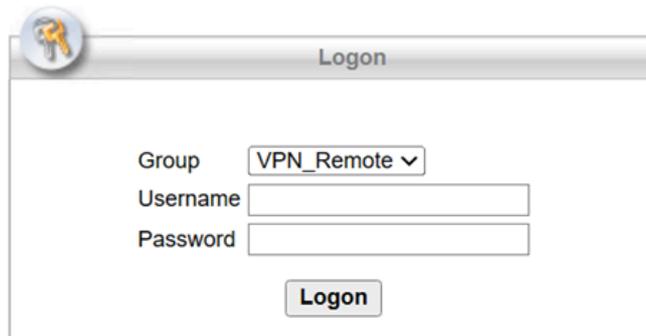
Para obter mais detalhes sobre o processo de inscrição, consulte estes recursos:

- Guia de inscrição universal: <https://guide.duo.com/universal-enrollment>
- Guia de inscrição tradicional: <https://guide.duo.com/traditional-enrollment>

Procedimento de validação da configuração.

Para garantir que suas configurações sejam precisas e operacionais, valide as próximas etapas:

1. Inicie um navegador da Web e insira o endereço IP do dispositivo Firepower Threat Defense (FTD) para acessar a interface VPN.



Logon

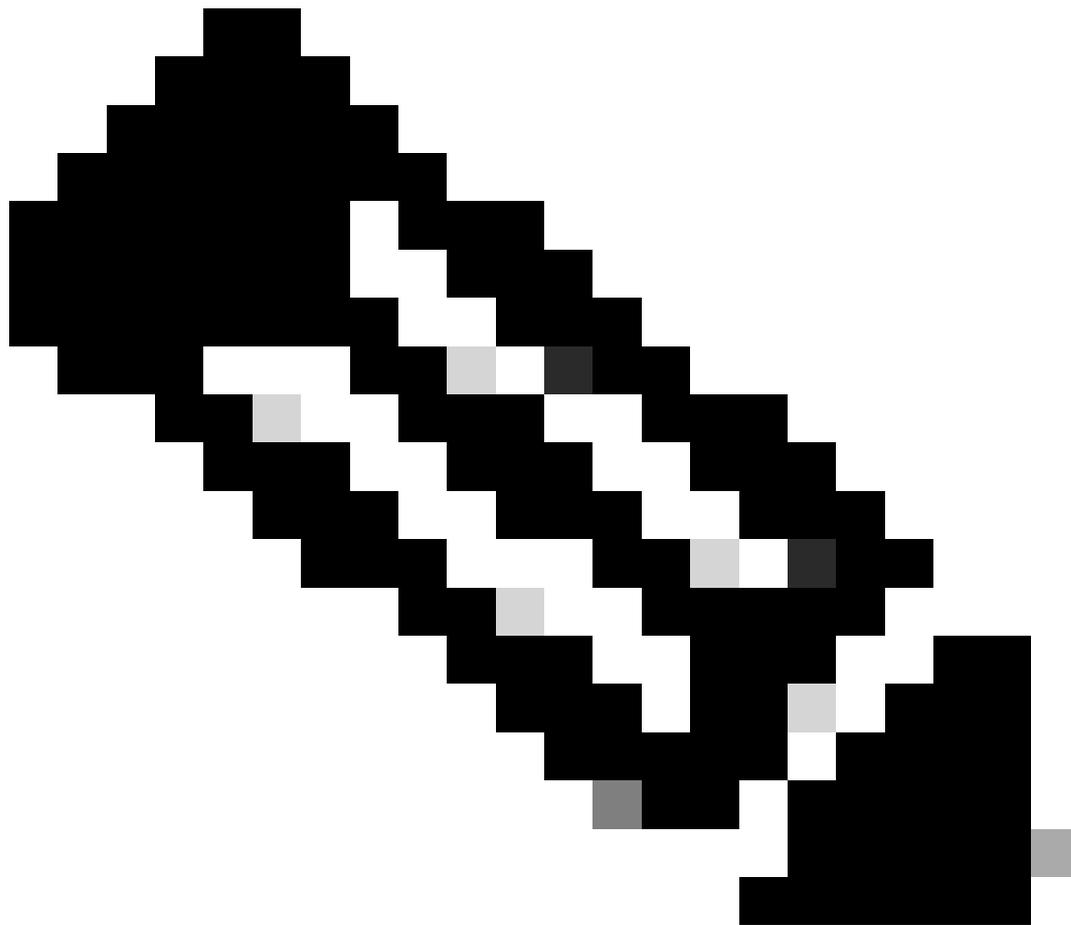
Group

Username

Password

Logon de VPN.

2. Insira seu nome de usuário e senha quando solicitado.



Observação: as credenciais fazem parte das contas do Ative Directory.

3. Quando você receber uma notificação Push DUO, aprove-a usando o Software DUO Mobile para continuar com o processo de validação.



(1) Login request waiting.

[Respond](#)



Are you logging in to Cisco ISE
RADIUS?

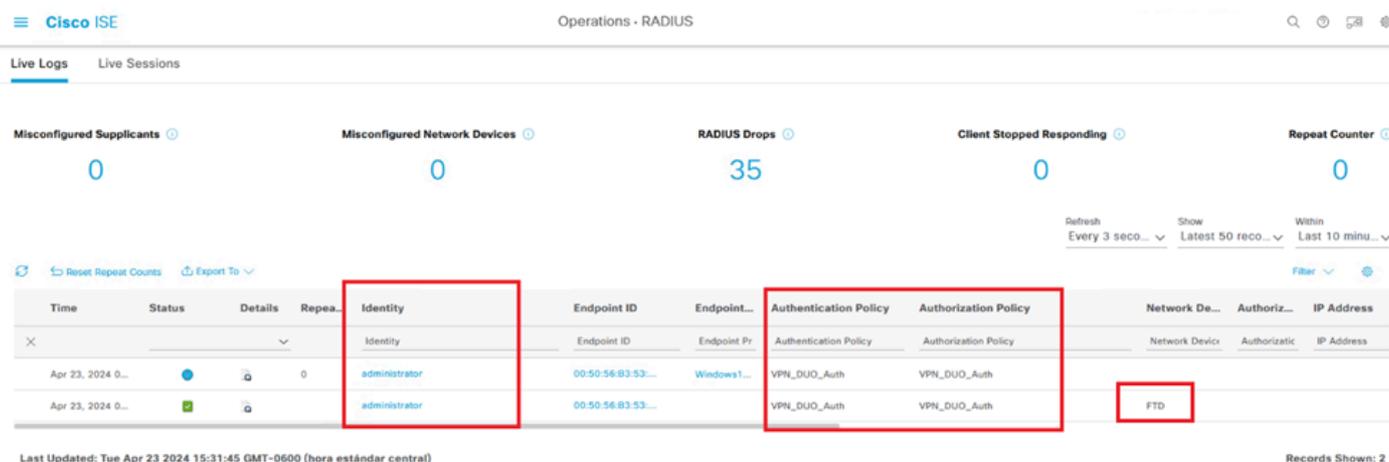


 Unknown

 3:13 PM CST

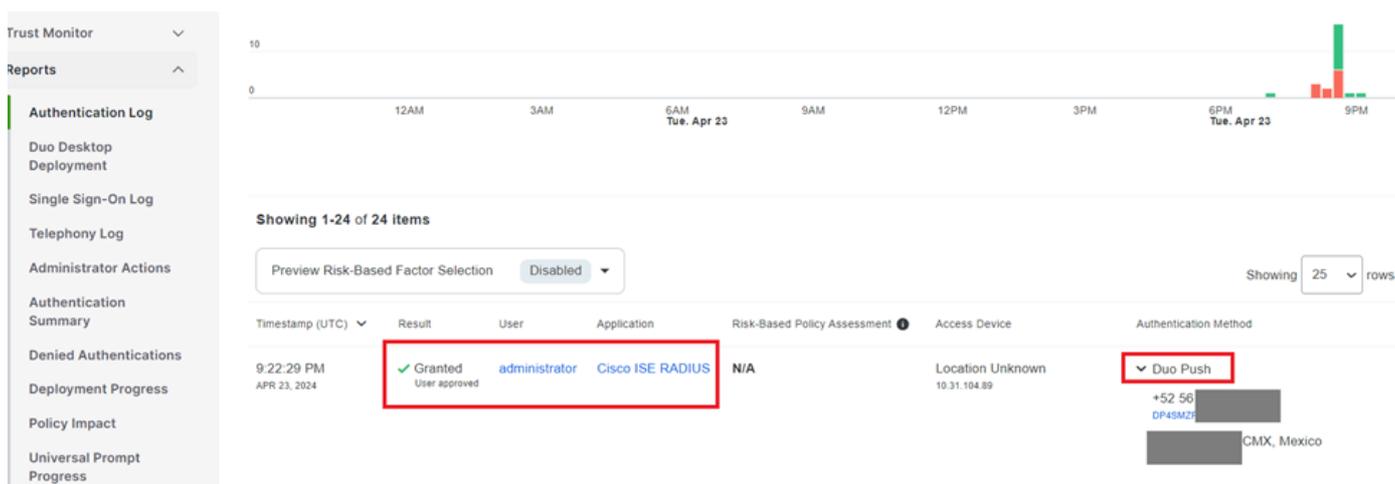
 administrator

para monitorar a atividade em tempo real e verificar a conectividade apropriada, acessar os logs ao vivo no Cisco Identity Services Engine (ISE).



Livelogs do ISE.

9. Vá para Relatórios > Logs de autenticação para revisar os logs de autenticação no Painel de Administração do DUO para confirmar as verificações bem-sucedidas.



Logs de autenticação.

Problemas comuns.

Cenário de trabalho.

Antes de explorar erros específicos relacionados a essa integração, é crucial entender o cenário geral de trabalho.

Nos livelogs do ISE, podemos confirmar que o ISE encaminhou os pacotes RADIUS para o Proxy DUO e, uma vez que o usuário aceitou o Push DUO, o RADIUS Access Accept foi recebido do Servidor Proxy DUO.

Overview

Event	5200 Authentication succeeded
Username	administrator
Endpoint Id	00:50:56:B3:53:D6
Endpoint Profile	
Authentication Policy	VPN_DUO_Auth
Authorization Policy	VPN_DUO_Auth
Authorization Result	

Authentication Details

Source Timestamp	2024-04-24 20:03:33.142
Received Timestamp	2024-04-24 20:03:33.142
Policy Server	asc-ise32p3-1300
Event	5200 Authentication succeeded
Username	administrator
Endpoint Id	00:50:56:B3:53:D6
Calling Station Id	10.31.104.89
Audit Session Id	000000000002e000662965a9
Network Device	FTD

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Network Access.NetworkDeviceName
- 11358 Received request for RADIUS server sequence.
- 11361 Valid incoming authentication request
- 11355 Start forwarding request to remote RADIUS server
- 11365 Modify attributes before sending request to external radius server
- 11100 RADIUS-Client about to send request - (port = 1812)
- 11101 RADIUS-Client received response (Step latency=5299 ms)
- 11357 Successfully forwarded request to current remote RADIUS server
- 11002 Returned RADIUS Access-Accept

Êxito na autenticação.

CiscoAVPair

mdm-tlv=device-platform=win,
mdm-tlv=device-mac=00-50-56-b3-53-d6,
mdm-tlv=device-type=VMware, Inc. VMware7,1,
mdm-tlv=device-platform-version=10.0.19045 ,
mdm-tlv=device-public-mac=00-50-56-b3-53-d6,
mdm-tlv=ac-user-agent=AnyConnect Windows 4.10.08029,
mdm-tlv=device-uid-
global=4CEBE2C21A8B81F490AC91086452CF3592593437,
mdm-tlv=device-
uid=3C5C68FF5FD3B6FA9D364DDB90E2B0BFA7E44B0EAAA
CA383D5A8CE0964A799DD,
audit-session-id=000000000002e000662965a9,
ip:source-ip=10.31.104.89
coa-push=true,
proxy-flow=[10.4.23.53,10.4.23.21]

Result

Reply-Message Success. Logging you in...

Resultado com êxito.

Uma captura de pacote do lado do ISE mostra as próximas informações:

Source	Destination	Protocol	Length	Info	
10.4.23.53	10.4.23.21	RADIUS	741	Access-Request id=138	→ The FTD sends the RADIUS request to ISE
10.4.23.21	10.31.126.207	RADIUS	883	Access-Request id=41	→ ISE resends the same RADIUS requests to the DUO Proxy
10.31.126.207	10.4.23.21	RADIUS	190	Access-Accept id=41	→ DUO Proxy sends the RADIUS accept (DUO push approved)
10.4.23.21	10.4.23.53	RADIUS	90	Access-Accept id=138	→ ISE resend the RADIUS accept to the FTD
10.4.23.53	10.4.23.21	RADIUS	739	Accounting-Request id=139	→ FTD sends the accounting for the current VPN connection
10.4.23.21	10.4.23.53	RADIUS	62	Accounting-Response id=139	→ ISE registered the accounting on its dashboard

Captura de pacotes ISE.

Erro11368 Examine os logs no servidor RADIUS externo para determinar o motivo exato da falha.

Event	5400 Authentication failed
Failure Reason	11368 Please review logs on the External RADIUS Server to determine the precise failure reason.
Resolution	Please review logs on the External RADIUS Server to determine the precise failure reason.
Root cause	Please review logs on the External RADIUS Server to determine the precise failure reason.

Erro 11368.

Troubleshooting:

- Verifique se a chave secreta compartilhada RADIUS no ISE é igual à chave configurada no FMC.

1. Abra a GUI do ISE.
2. Administração > Recursos de Rede > Dispositivos de Rede.
3. Escolha o Servidor Proxy DUO.
4. Ao lado do segredo compartilhado, clique em "Mostrar" para ver a chave em formato de texto simples.
5. Abra a GUI do FMC.
6. Objetos > Gerenciamento de Objetos > Servidor AAA > Grupo de Servidores RADIUS.
7. Escolha o Servidor ISE.
8. Reinsira a chave secreta.

- Verifique a integração do Ative Diretory no DUO.

1. Abra o Gerenciador de Proxy de Autenticação DUO.

2. Confirme o usuário e a senha na seção [ad_client].
3. Clique em validar para confirmar se as credenciais atuais estão corretas.

Erro 11353 Não há mais servidores RADIUS externos; não é possível executar failover

Event	5405 RADIUS Request dropped
Failure Reason	11353 No more external RADIUS servers; can't perform failover
Resolution	Verify the following: At least one of the remote RADIUS servers in the ISE proxy service is up and configured properly ; Shared secret specified in the ISE proxy service for every remote RADIUS server is same as the shared secret specified for the ISE server ; Port of every remote RADIUS server is properly specified in the ISE proxy service.
Root cause	Failover is not possible because no more external RADIUS servers are configured. Dropping the request.

Erro 11353.

Troubleshooting:

- Verifique se a chave secreta compartilhada RADIUS no ISE é a mesma que a chave configurada no Servidor Proxy DUO.

1. Abra a GUI do ISE.
2. Administração > Recursos de Rede > Dispositivos de Rede.
3. Escolha o Servidor Proxy DUO.
4. Ao lado do segredo compartilhado, clique em "Mostrar" para ver a chave em formato de texto simples.
5. Abra o Gerenciador de Proxy de Autenticação DUO.
6. Verifique a seção [radius_server_auto] e compare a chave secreta compartilhada.

As sessões RADIUS não são exibidas nos registros ao vivo do ISE.

Troubleshooting:

- Verifique a configuração do DUO.

1. Abra o Gerenciador de Proxy de Autenticação DUO.
2. Verifique o endereço IP do ISE na seção [radius_server_auto]

- Verifique a configuração do FMC.

1. Abra a GUI do FMC.

2. Vá para Objects > Object Management > AAA Server > RADIUS Server Group.

3. Escolha o Servidor ISE.

4. Verifique o endereço IP do ISE.

- Faça uma captura de pacote no ISE para confirmar a recepção dos pacotes RADIUS.

1. Vá para Operations > Troubleshoot > Diagnostic Tools > TCP Dump

Troubleshooting Adicional.

- Ative os próximos componentes na PSN como debug:

Mecanismo de políticas

Prrt-JNI

runtime-AAA

Para obter mais soluções de problemas no Gerenciador de Proxy de Autenticação DUO, verifique o próximo link:

https://help.duo.com/s/article/1126?language=en_US

Modelo DUO.

Você pode usar o próximo modelo para concluir a configuração no seu Servidor Proxy DUO.

```
[main] <--- OPTIONAL
http_proxy_host=<Proxy IP address or FQDN>
http_proxy_port=<Proxy port>
[radius_server_auto]
ikey=xxxxxxxxxxxxxxxx
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=xxxxxxxxxxxxxxxxxxxxxxxx
radius_ip_1=<PSN IP Address>
radius_secret_1=xxxxxxxxxx
failmode=safe
port=1812
client=ad_client
```

```
[ad_client]
host=<AD IP Address>
service_account_username=xxxxxxx
service_account_password=xxxxxxxxxx
search_dn=DC=xxxxxx,DC=xxxx
```

[cloud]

apikey=xxxxxxxxxxxxxxxxxxxx

sk=xx

api_host=xxxxxxxxxxxxxxxxxxxx

service_account_username=<your domain\username>

service_account_password=xxxxxxxxxxxx

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.