

Configurar a autenticação de certificado & Autenticação SAML DUO

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar Etapas no DUO](#)

[Criar uma Política de Proteção de Aplicativos](#)

[Criar Política de Aplicativo](#)

[Passos de configuração para o FMC](#)

[Implantar Certificado de Identidade no FTD](#)

[Implantar certificado IDP no FTD](#)

[Criando o Objeto SSO SAML](#)

[Criar Configuração de Rede Virtual Privada \(RAVPN\) de Acesso Remoto](#)

[Verificar](#)

[Troubleshooting](#)

[Problema 1: Falha na autenticação do certificado.](#)

[problema 2: Falhas de SAML](#)

Introdução

Este documento descreve um exemplo da implementação da autenticação baseada em certificado e da autenticação SAML dupla.

Pré-requisitos

As ferramentas e dispositivos usados no guia são:

- Defesa contra ameaças (FTD) do Cisco Firepower
- Firepower Management Center (FMC)
- Autoridade de Certificação Interna (CA)
- Conta Premier do Cisco DUO
- Proxy de autenticação Cisco DUO
- Cisco Secure Client (CSC)

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- VPN básica,
- SSL/TLS
- Infraestrutura de Chave Pública
- Experiência com o FMC
- Cisco Secure Client
- Código FTD 7.2.0 ou superior
- Proxy de autenticação Cisco DUO

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- FTD da Cisco (7.3.1)
- FMC da Cisco (7.3.1)
- Cisco Secure Client (5.0.02075)
- Proxy de autenticação Cisco DUO (6.0.1)
- Mac OS (13.4.1)
- Diretório ativo

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.

Configurar Etapas no DUO

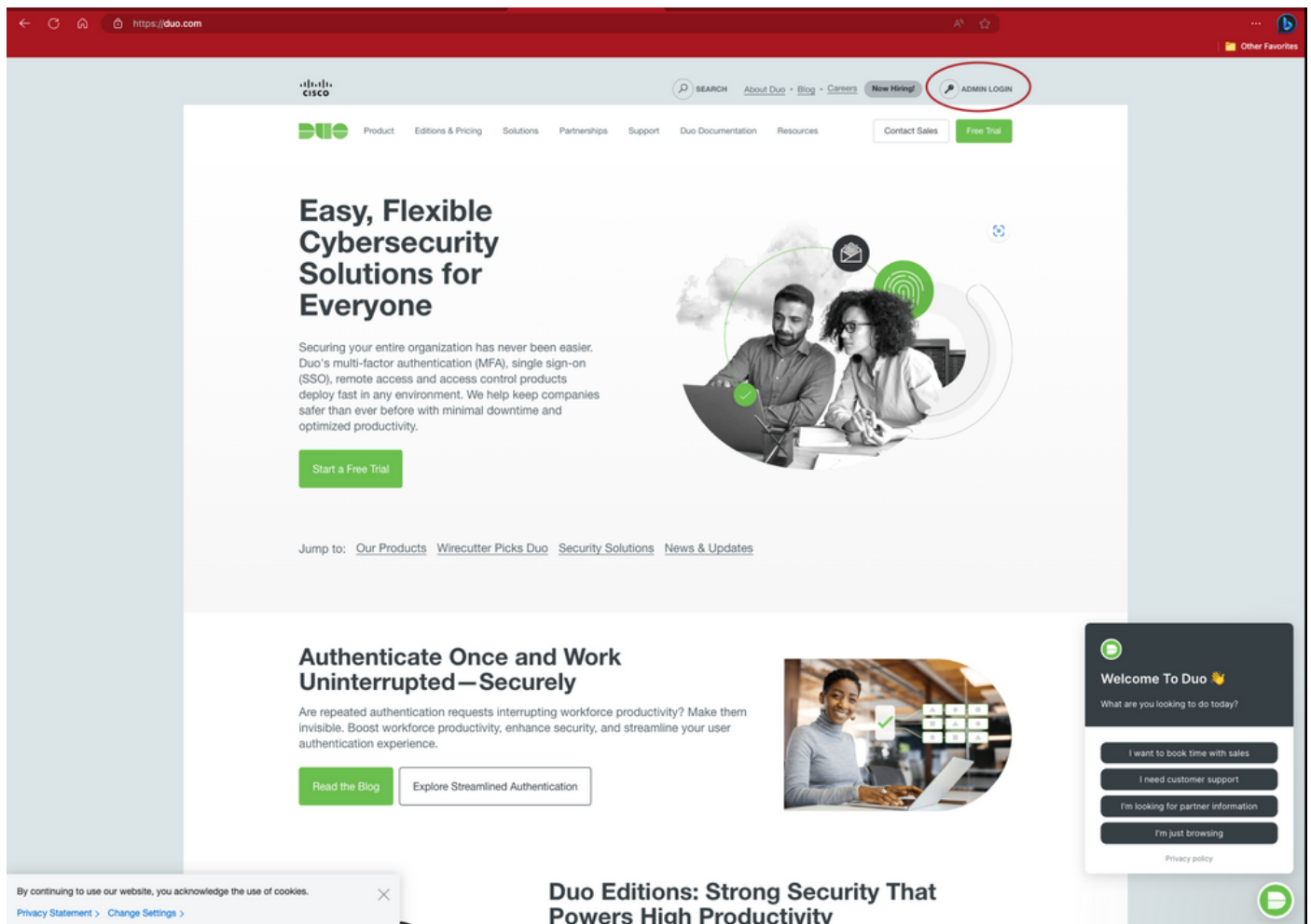
Esta seção descreve as etapas para configurar o SSO (Logon Único) do Cisco DUO. Antes de começar, certifique-se de que o proxy de autenticação esteja implementado.



aviso: Se um proxy de autenticação não tiver sido implementado, este link terá o guia para esta tarefa. [Guia de Proxy de Autenticação DUO](#)

Criar uma Política de Proteção de Aplicativos

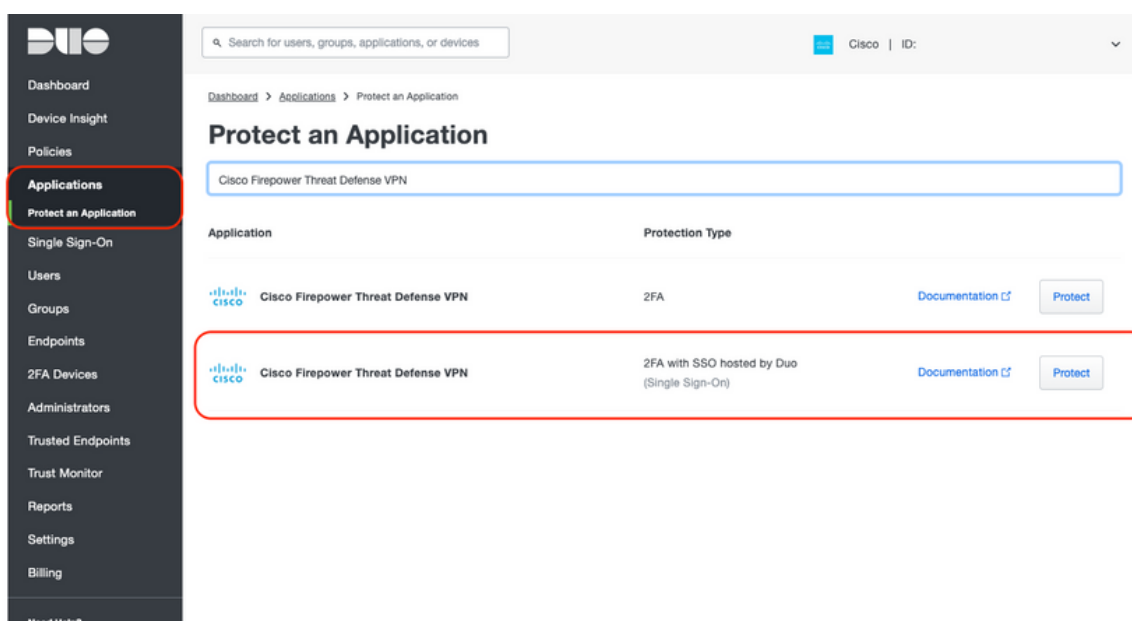
Etapa 1. Entre no painel de administração através deste link [Cisco Duo](#)



Página inicial do Cisco DUO

Etapa 2. Navegue até Painel de Controle > Aplicativos > Proteger um Aplicativo.

Na barra de pesquisa, digite "Cisco Firepower Threat Defense VPN" e selecione "Protect".



Proteger uma captura de tela do aplicativo

Selecione a opção somente com o Tipo de proteção "2FA com SSO hospedado por Duo".

Passo 3: Copie essas informações de URL em Metadados.

- ID da entidade do provedor de identidade
- URL SSO
- URL de logoff

See the [Cisco ASA SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID

Copy

Sign In URL

Copy

Sign Out URL

Copy

Exemplo de informações para copiar



Note: Os links foram omitidos da captura de tela.

Etapa 4. Selecione "Download certificate" para fazer download do Identity Provider Certificate em Downloads.

Etapa 5. Preencher as informações do provedor de serviços

URL do Cisco Firepower Base - O FQDN usado para acessar o FTD

Nome Do Perfil De Conexão- O Nome Do Grupo De Túneis

Criar Política de Aplicativo

Passo 1: Para criar uma Diretiva de aplicativo em Diretiva Selecione "Aplicar uma diretiva a todos os usuários" e selecione "Ou criar uma nova Diretiva", como mostrado na imagem.

Policy

Policy defines when and how users will authenticate when accessing this application. Your global policy always applies, but you can override its rules with custom policies.

Group policies

Apply a policy to groups of users

Application policy

Apply a policy to all users

Exemplo de criação de uma política de aplicativo

Apply a Policy



Policy

Select a Policy



[Or, create a new Policy.](#)

Apply Policy

Exemplo de criação de uma política de aplicativo

Etapa 2. Em Nome da política, insira o nome desejado, selecione "Política de autenticação" em Usuários e selecione "Aplicar 2FA." Em seguida, salve com "Criar política."

Create a New Policy

Policy name

MFA

Users

New User policy

Authentication policy

User location

Devices

Trusted Endpoints

Device Health application

Remembered devices

Operating systems

Browsers

Plugins

Networks

Authorized networks

Anonymous networks

Authenticators

Risk-based factor selection

Authentication methods

Duo Mobile app

Tampered devices

Screen lock

Full-disk encryption

Mobile device biometrics

Authentication policy

Enforce 2FA

Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

Bypass 2FA

Skip two-factor authentication and enrollment, unless there is a superseding policy configured.

Deny access

Deny authentication to all users.

When enabled, this affects all users.

Choose another rule on the left to add to this policy.

Create Policy

Exemplo de criação de uma política de aplicativo

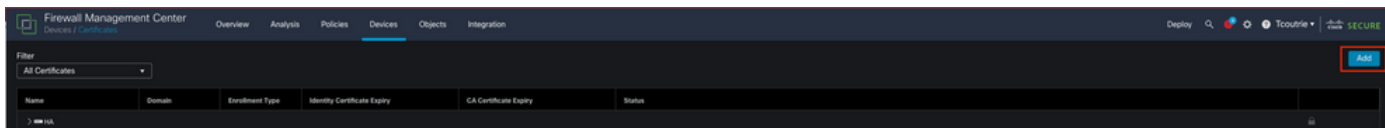
Etapa 3. Aplique a política com "Aplicar política" na próxima janela. em seguida, role até a parte inferior da página e selecione "Save" para concluir as configurações do DUO

Passos de configuração para o FMC

Implantar Certificado de Identidade no FTD

Esta seção descreve como configurar e implantar o certificado de identidade no FTD necessário para autenticação de certificado. Antes de começar, certifique-se de implantar todas as configurações.

Etapa 1. Navegue até **Devices > Certificatee** e escolha **Add**, conforme mostrado na imagem.



Captura de tela de dispositivos/certificados

Passo 2: Escolha o dispositivo FTD no menu suspenso de dispositivos. Clique no ícone + para adicionar um novo método de registro de certificado.

A screenshot of the 'Add New Certificate' dialog box. The title is 'Add New Certificate'. Below the title, there is a text box with the instruction: 'Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.' Below this, there are two dropdown menus. The first is labeled 'Device*' and has 'HA' selected. The second is labeled 'Cert Enrollment*' and has 'Select a certificate enrollment object' selected. To the right of the second dropdown is a red box around a '+' icon. At the bottom right, there are two buttons: 'Cancel' and 'Add'.

Captura de tela de Adicionar novo certificado

Etapa 3: Escolha a opção que é o método preferido para obter certificados no ambiente através do "Tipo de inscrição", como mostrado na imagem.

Add Cert Enrollment



Name*

FTD04-16

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

PKCS12 File



PKCS12 File*:

test.p12



Browse PKCS12 File

Passphrase:

.....



Validation Usage:



IPsec Client



SSL Client



SSL Server



Skip Check for CA flag in basic constraints of the CA Certificate



Allow Overrides

Cancel

Save

Captura de tela da nova página de registro de certificado



Tip: As opções disponíveis são: Certificado Autoassinado - Gere um novo certificado localmente, SCEP - Use o Simple Certificate Enrollment Protocol para obter um certificado de uma CA, Manual - Instale manualmente o certificado Raiz e Identidade, PKCS12 - Carregue o pacote de certificado criptografado com raiz, identidade e chave

privada.

Implantar certificado IDP no FTD

Esta seção descreve a configuração e a implantação do certificado IDP no FTD. Antes de começar, assegure-se de implantar todas as configurações.

Passo 1: Navegue até Devices > Certificate e escolha Add."

Passo 2: Escolha o dispositivo FTD no menu suspenso de dispositivos. Clique no ícone + para adicionar um novo método de registro de certificado.

Etapa 3: na janela Add Cert Enrollment, insira as informações necessárias, conforme mostrado na imagem, depois "Save", conforme mostrado na imagem.

- Nome: Nome do objeto
- Tipo de inscrição: Manual
- Caixa de seleção ativada: Somente CA
- Certificado CA: Formato Pem do certificado

Add Cert Enrollment

Name*

duocert

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type

Manual

☒ CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

-----BEGIN CERTIFICATE-----
OC957DUc7tc4
b79bVzOXuqz5ZpaJHqtXV8fLOH
eIPYblyYBwSstXB+k75VHs0Voz
AkeySJCWRQXF
ISSRGu8DpUIKzKu2zd55322+wd
fkyy/WMXUJWmSXKKnnHEsOqL
GCxmfd+5OsWlo
ICCMGa5gYgEv8EHF3Y++sFg=
-----END CERTIFICATE-----

Validation Usage:

☒ IPsec Client

☐ SSL Client

☒ SSL Server

☐ Skip Check for CA flag in basic constraints of the CA Certificate

☐ Allow Overrides

Cancel

Save

Exemplo de criação de um objeto de registro de certificado



Caution: "Ignorar verificação de sinalizador de CA em restrições básicas do Certificado de CA" pode ser usado se necessário. Use essa opção com cuidado.

Passo 4: Selecione o objeto de registro de certificado recém-criado em "Cert Enrollment*" e, em

seguida, selecione "Add" conforme mostrado na imagem.

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:
HA ▼

Cert Enrollment*:
duocert ▼ +

Cert Enrollment Details:

Name:	duocert
Enrollment Type:	Manual (CA Only)
Enrollment URL:	N/A

Cancel Add

Captura de tela do objeto e dispositivo de registro de certificado adicionado



Note: Depois de adicionado, o certificado é implantado imediatamente.

Criando o Objeto SSO SAML

Esta seção descreve as etapas para configurar o SAML SSO via FMC. Antes de começar, assegure-se de implantar todas as configurações.

Etapa 1. Navegue até Objects > AAA Server > Single Sign-on Server e selecione "Add Single Sign-on Server".

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? Tcourtrie | cisco SECURE

AAA Server
RADIUS Server Group
Single Sign-on Server
> Access List
> Address Pools
Application Filters
AS Path
bfd Template
Cipher Suite List
> Community List
DHCP IPv6 Pool
> Distinguished Name
DNS Server Group
> External Attributes
File List
> FlexConfig
Geolocation
Interface
Key Chain
Network
> PKI
Policy List
Port
> Prefix List
Route Map

Single Sign-on Server

[Add Single Sign-on Server](#) 🔍 Filter

Single Sign-on Server contains parameters for SAML based authentication. These Single Sign-on Servers are used to authenticate users logging in through Remote Access VPN connections.

Name	
AZ	 
DUO	 

Displaying 1 - 2 of 2 rows | < > Page 1 of 1 | 🔄

exemplo de criação de um novo objeto SSO

Etapa 2. Inserir as informações necessárias em "Criar uma política de proteção de aplicativos"

". Para continuar depois de concluído, selecione "Salvar".

- Nome*: Nome do objeto
- ID da entidade do provedor de identidade*: ID da entidade da etapa 3
- URL SSO*: URL de Entrada copiada da Etapa 3
- URL de logoff: URL de saída copiada da Etapa 3
- URL Base: Use o mesmo FQDN como "URL do Cisco Firepower Base" na Etapa 5
- Certificado do provedor de identidade*: Certificado IDP implantado
- Certificado do provedor de serviços: Certificado na interface externa do DTF

New Single Sign-on Server?

Name*

duosso

Identity Provider Entity ID*

SSO URL*

Logout URL

Base URL

https://vpn.ciscoexample.com

Identity Provider Certificate*

duocert

+

Service Provider Certificate

FTD04-16

+

Request Signature

--No Signature--

Request Timeout

Use the timeout set by the provide

seconds (1-7200)

☐ Enable IdP only accessible on Internal Network

☒ Request IdP re-authentication on Login

☐ Allow Overrides

Cancel

Save

Exemplo do novo objeto SSO.



Note: Os links ID da entidade, URL do SSO e URL de logoff foram omitidos da captura de

tela

Criar Configuração de Rede Virtual Privada (RAVPN) de Acesso Remoto

Esta seção descreve as etapas para configurar o RAVPN usando o assistente.

Etapa 1. Navegue até Devices > Remote Access Selecione "Add."

Etapa 2. No assistente, insira o nome do novo Assistente de política RAVPN, selecione SSL em Protocolos VPN: Adicione os Dispositivos de Destino, como mostrado na imagem. Selecione "Avançar" quando terminar.

Remote Access VPN Policy Wizard

Policy Assignment | Connection Profile | Secure Client | Access & Certificate | Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:

Description:

VPN Protocols:

☒ SSL

☐ IPsec-IKEv2

Targeted Devices:

Available Devices: HA

Selected Devices: HA

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy:

Authentication Server

Configure LOCAL or RADIUS or RADIUS Server Group or SSO to authenticate VPN clients.

Secure Client Package

Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

Cancel Back Next

Etapa 1 do assistente de RAVPN

Etapa 2. Para o Perfil de Conexão, defina as opções (mostradas aqui): Selecione "Próximo" quando terminar.

- Nome do perfil de conexão: Use o nome do grupo de túneis na Etapa 5 de "Criar uma política de proteção de aplicativos".

Autenticação, Autorização e Tarifação (AAA - Authentication, Authorization & Accounting):

- método de autenticação: Certificado do cliente e SAML
- Servidor de Autenticação:* Selecione o objeto SSO criado durante a "Criação do Objeto SSO SAML".

Atribuição de endereço de cliente:

- Usar servidor AAA (território ou RADIUS somente)- Radius ou LDAP
- Usar servidores DHCP - Servidor DHCP

- Usar pools de endereços IP- pool local no FTD

Firewall Management Center
Devices / VPN / Setup Wizard

Remote Access VPN Policy Wizard

Policy Assignment — Connection Profile — Secure Client — Access & Certificate — Summary

Connection Profile Name:

This name is configured as a connection alias, it can be used to connect to the VPN gateway

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:

Authentication Server:

SAML Login Experience: ☒ VPN client embedded browser ☐ Default OS Browser

☐ Allow connection only if username from certificate and SAML are the same

☐ Use username from client certificate for Authorization

Username From Certificate: Use entire DN (Distinguished Name) as username

Primary Field:

Secondary Field:

Authorization Server:

Accounting Server:

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 DHCP Servers:

☐ Use IP 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

Etapas 2 do assistente de RAVPN



Tip: Para este laboratório, um servidor DHCP é usado.

Etapas 3. Selecione "+" para carregar uma imagem de implantação na Web do Cisco Secure Client a ser implantado. Em seguida, marque a caixa de seleção da imagem do CSC a ser implantada. Conforme mostrado na imagem. Selecione "Next" quando terminar.

Firewall Management Center
Devices / VPN / Setup Wizard

Remote Access VPN Policy Wizard

Policy Assignment — Connection Profile — Secure Client — Access & Certificate — Summary

Secure Client Image

The VPN gateway can automatically download the latest Secure Client 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 Secure Client packages from [Cisco Software Download Center](#).

Secure Client File Object Name	Secure Client Package Name	Operating System
☒ cisco-secure-client-macos-5.0.02075-web...	cisco-secure-client-macos-5.0.02075-web...	Mac OS
☒ cisco-secure-client-win-5.0.02075-web...	cisco-secure-client-win-5.0.02075-web...	Windows

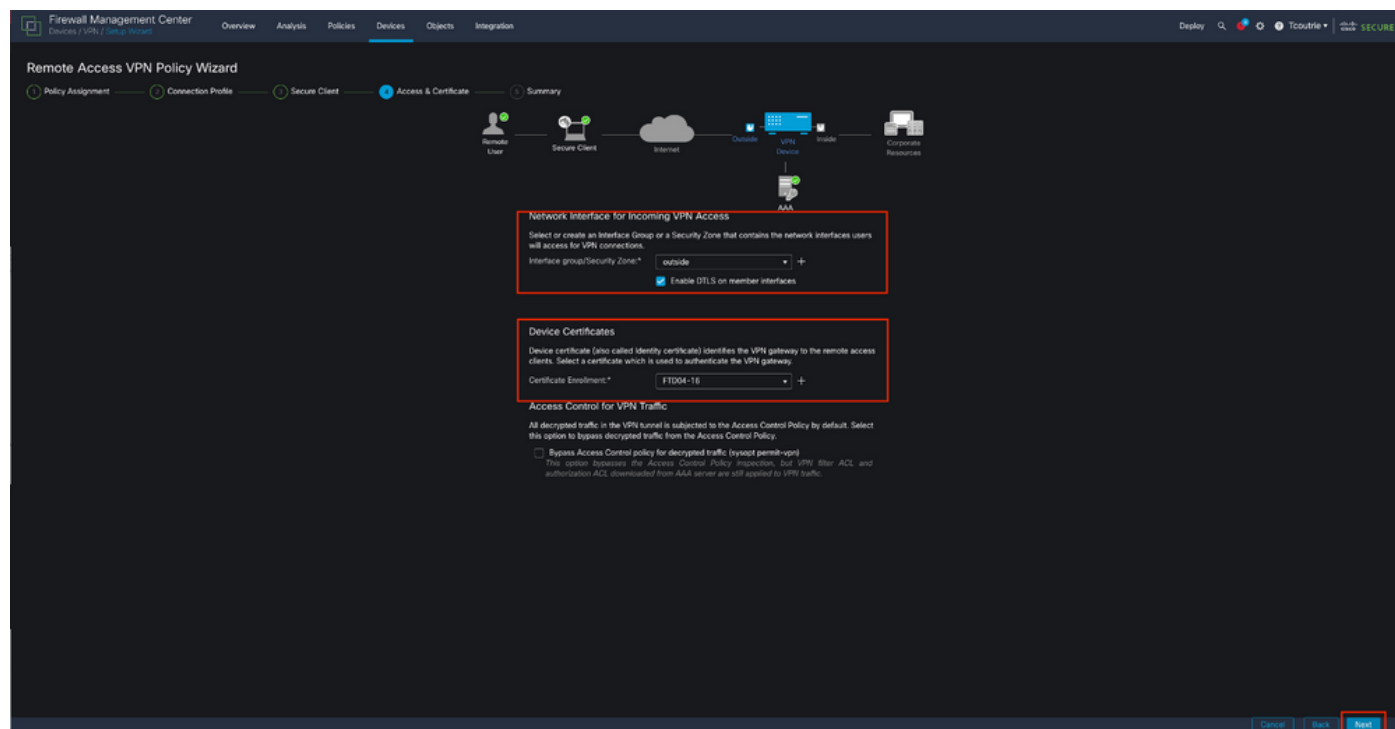
Cancel Back Next

Etapas 3 Assistente de RAVPN

Etapa 4. Definir esses objetos (conforme ilustrado na imagem): Selecione "Próximo" quando terminar.

Grupo de interface/Zona de segurança:*: Interface externa

"Registro de certificado:": Certificado de identidade criado durante a seção "Implantar certificado de identidade no FTD" deste guia



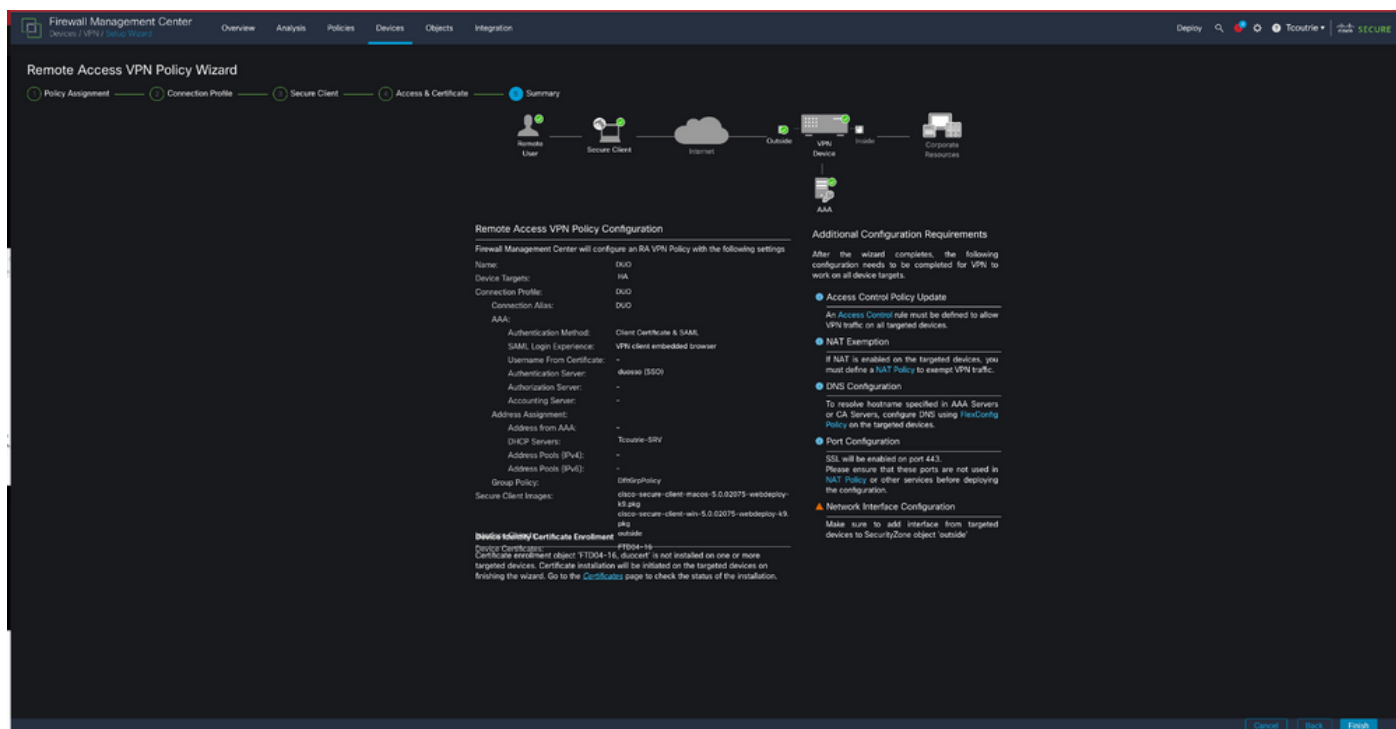
Etapa 4 do assistente de RAVPN



Tip: Se isso não tiver sido criado, adicione um novo objeto de registro de certificado selecionando "+".

Etapa 6. Resumo

Verifique todas as informações. Se tudo estiver correto, continue com "Concluir".



Página Resumo

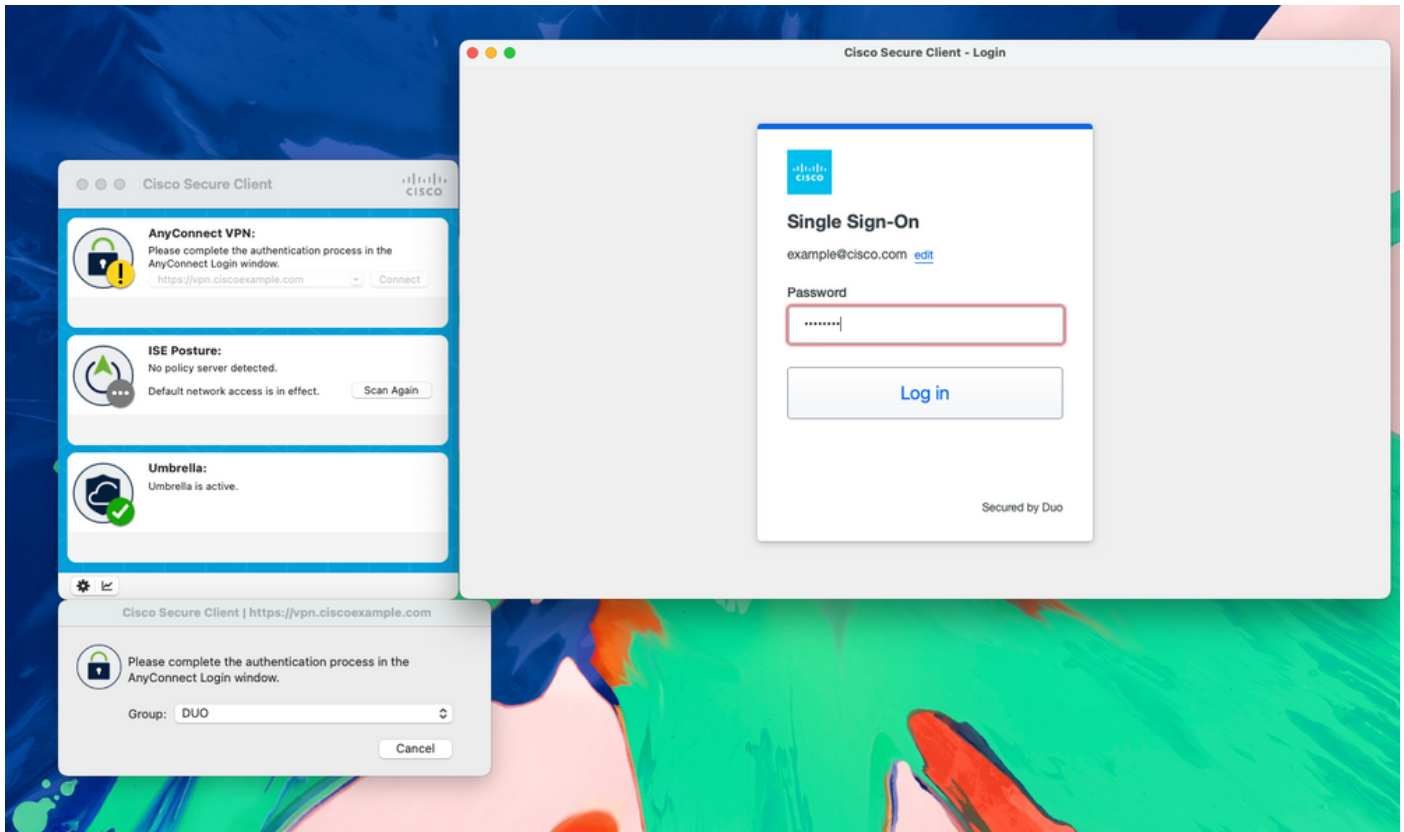
Etapa 7. Implantar as configurações recém-adicionadas.

Verificar

Esta seção descreve a verificação de uma tentativa de conexão bem-sucedida.

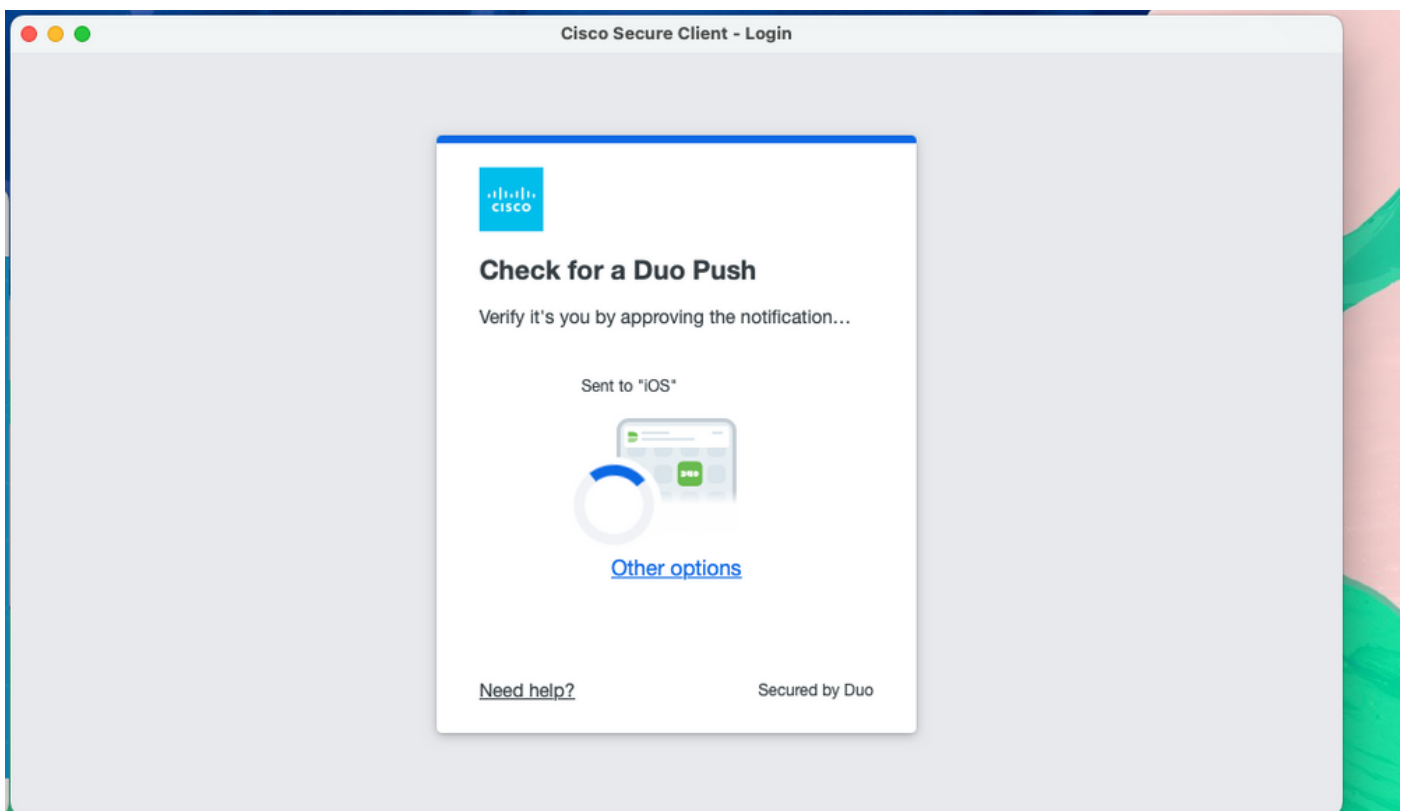
Abra o Cisco Secure Client, insira o FQDN do FTD e conecte-se.

Insira as credenciais na página SSO.



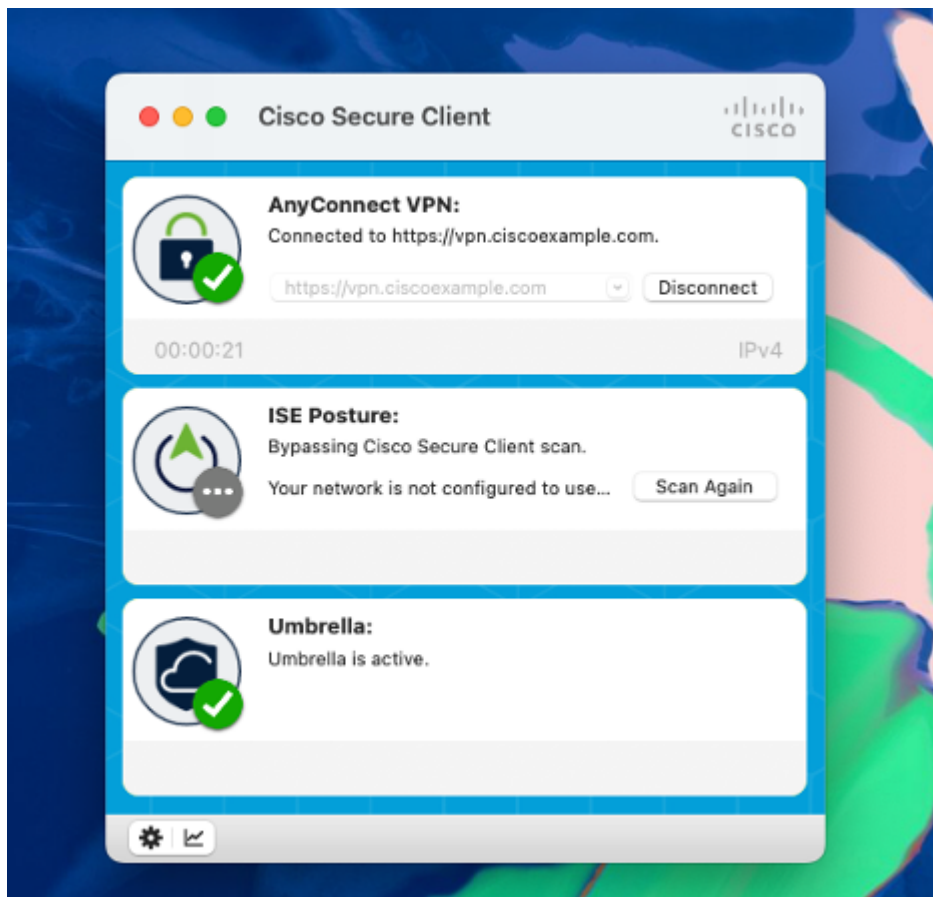
Página SSO via Cisco Secure Client

Aceite o envio DUO para o dispositivo registrado.



Push DUO

Conexão bem-sucedida.



Conectado ao FTD

Verifique a conexão no FTD com o comando: `show vpn-sessiondb detail anyconnect`

```

tcoutrie-ftd2# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username      :                               Index      : 1916
Assigned IP   :                               Public IP    :
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128  DTLS-Tunnel:
Hashing       : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SH
Bytes Tx      : 390964                        Bytes Rx     : 124114
Pkts Tx       : 1216                          Pkts Rx      : 1223
Pkts Tx Drop  : 0                            Pkts Rx Drop : 0
Group Policy  :                               Tunnel Group :
Login Time    : 23:54:41 UTC Tue Jul 18 2023
Duration      : 0h:11m:28s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                          VLAN         : none
Audt Sess ID  : 0a7aa95d0077c00064b72641
Security Grp  : none                        Tunnel Zone  : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID     : 1916.1
Public IP     :
Encryption    : none                        Hashing       : none
TCP Src Port  : 53859                      TCP Dst Port  : 443
Auth Mode     : Certificate and SAML
Idle Time Out: 30 Minutes                  Idle TO Left  : 18 Minutes
Client OS     : mac-intel

```

Algumas informações foram omitidas do exemplo de saída

Troubleshooting

Esses são possíveis problemas que surgem após a implementação.

Problema 1: Falha na autenticação do certificado.

Assegurar que o certificado raiz está instalado no FTD;

use estas depurações:

debug crypto ca 14

debug aaa shim 128

debug aaa common 128

problema 2: Falhas de SAML

Essas depurações podem ser ativadas para solucionar problemas:

debug aaa shim 128

debug aaa common 128

debug webvpn anyconnect 128

debug webvpn saml 255

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.