Configurar a autenticação de certificado & Autenticação SAML DUO

Contents

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.

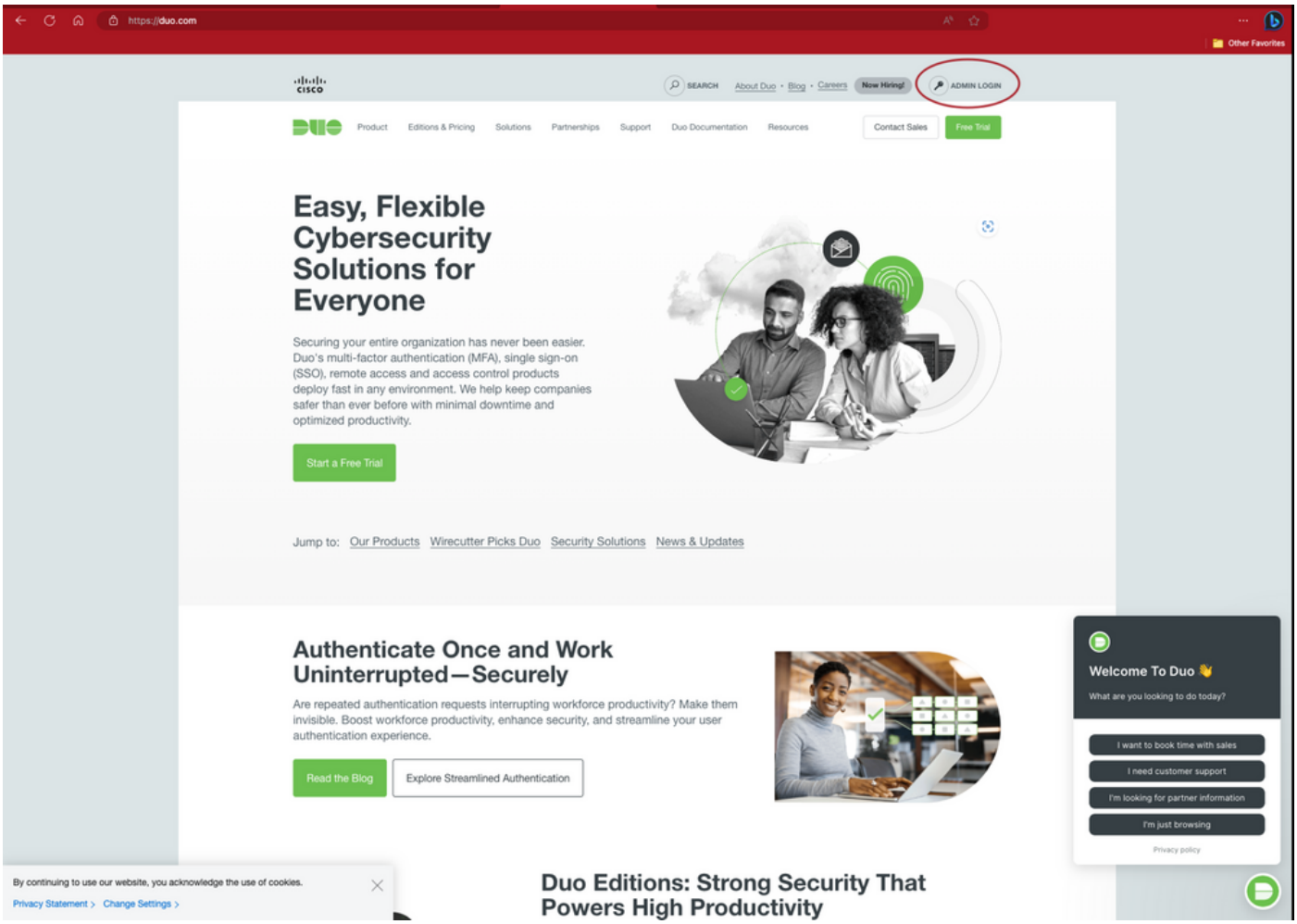
Configurar Etapas no DUO

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

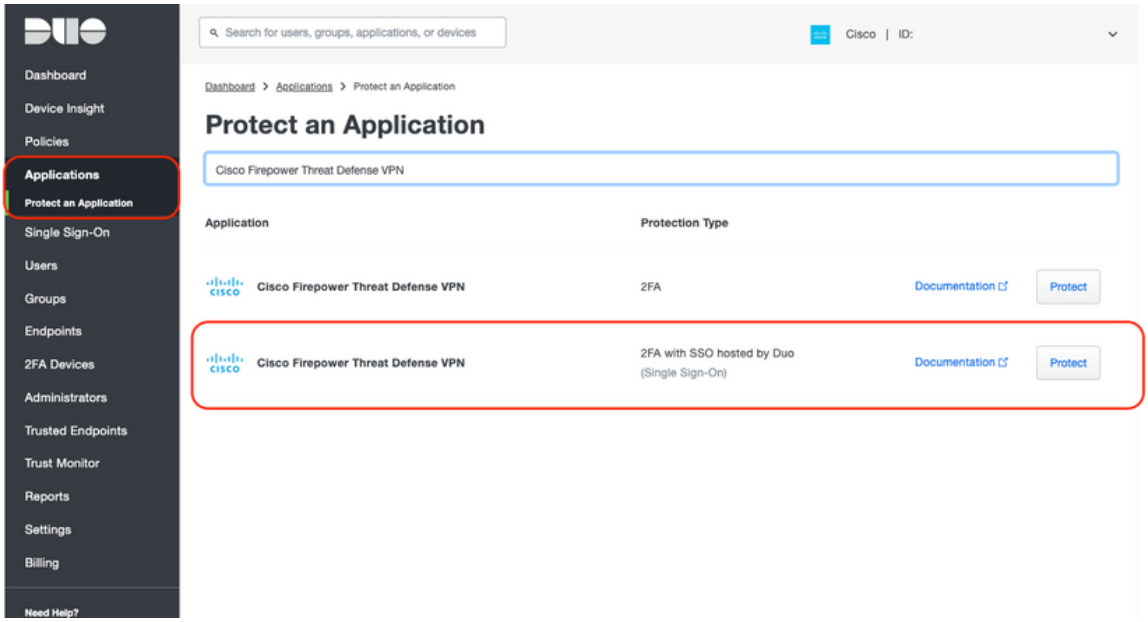
Etapa 1. Entre no painel de administração através deste link Cisco Duo



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

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.

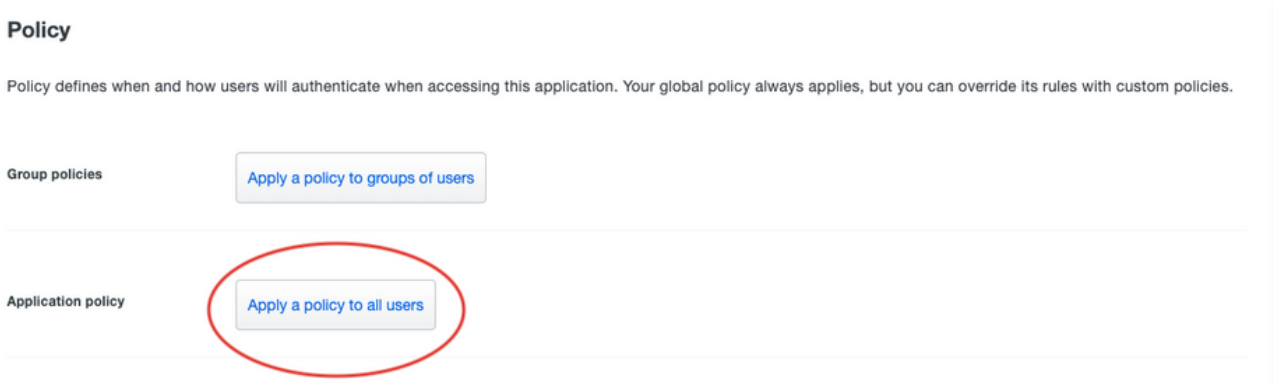
Etapa 5. Preencher as informações do provedor de serviços

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

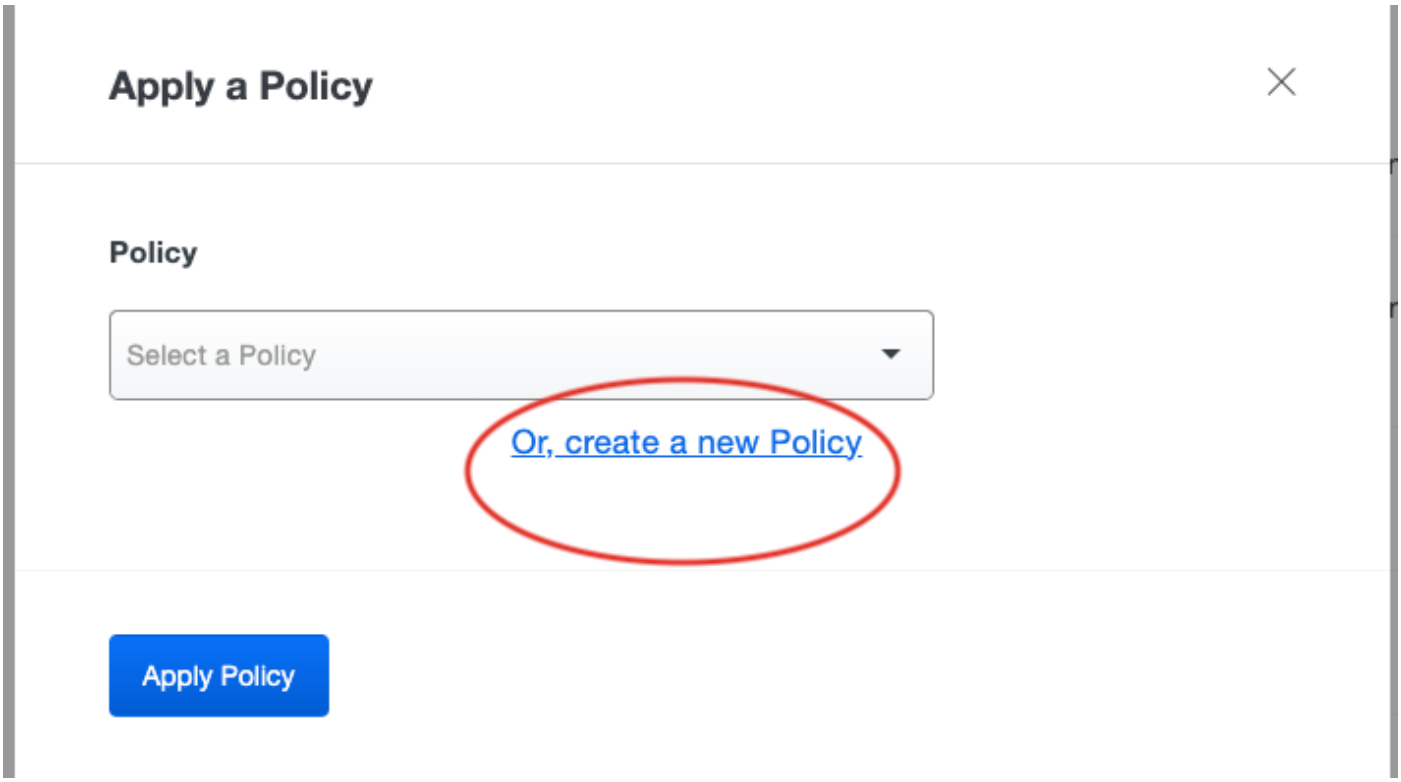
Nome Do Perfil De Conexão- O Nome Do Grupo De Túneis

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.

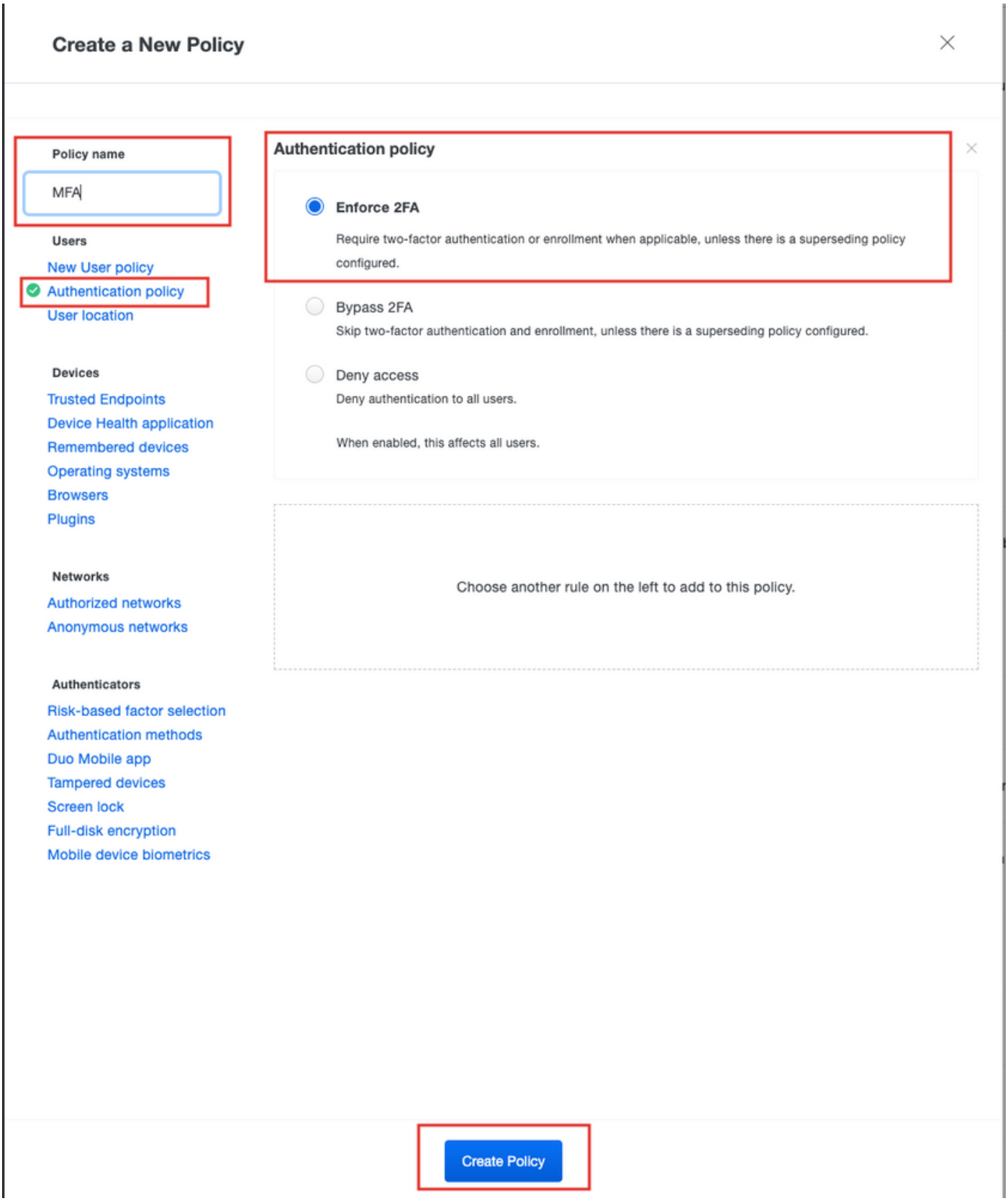


Exemplo de criação de uma política de aplicativo



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."



Exemplo de criação de uma política de aplicativo

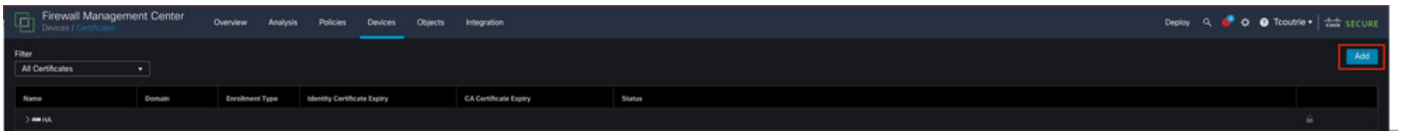
Etapa 3. Aplique a política com "Aplicar política" na próxima janela. em seguida, role até a parte inferior da página e selecione "Save" para concluir as configurações do DUO

Passos de configuração para o FMC

Implantar Certificado de Identidade no FTD

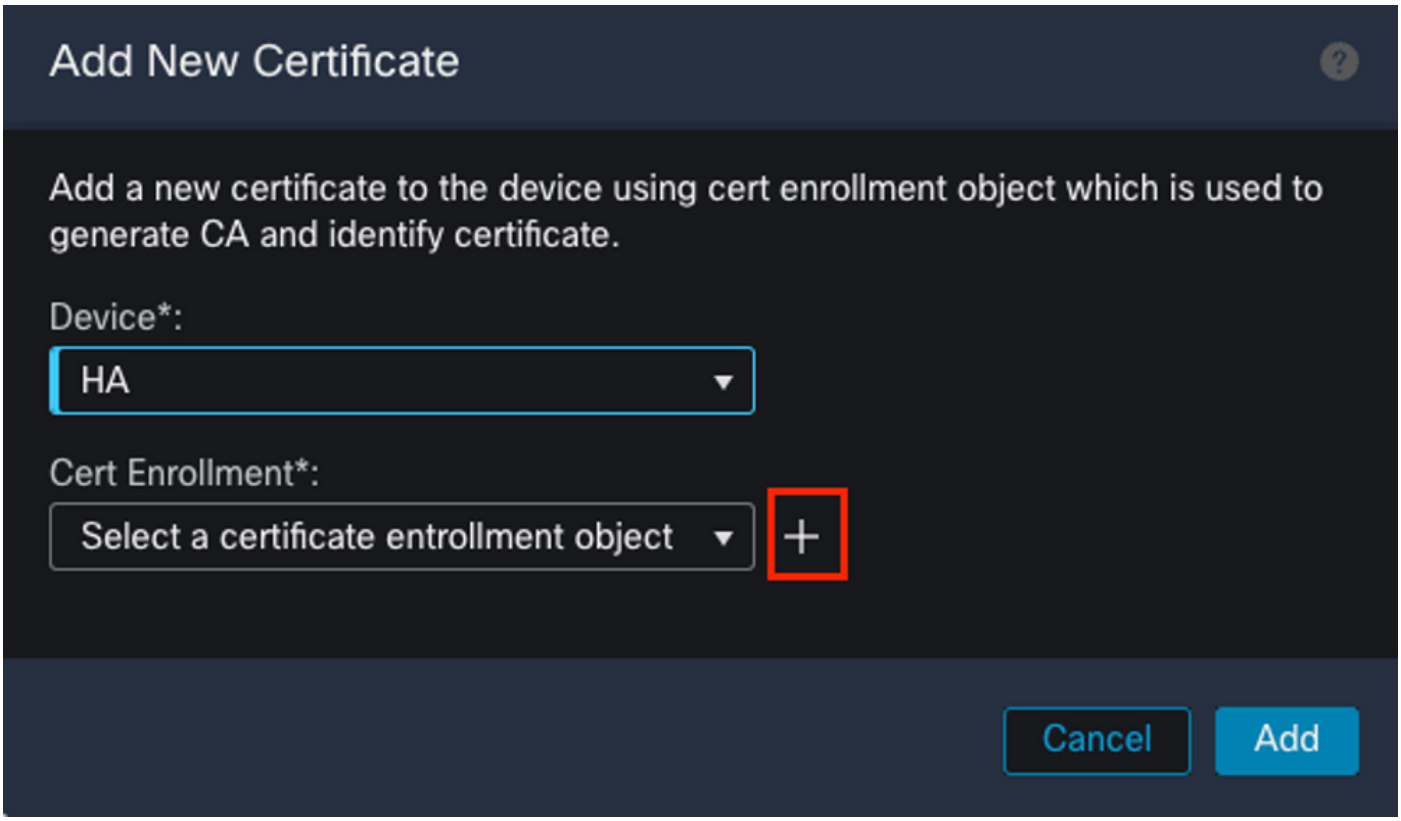
Esta seção descreve como configurar e implantar o certificado de identidade no FTD necessário para autenticação de certificado. Antes de começar, certifique-se de implantar todas as configurações.

Etapa 1. Navegue atéDevices > Certificatee escolhaAdd, conforme mostrado na imagem.



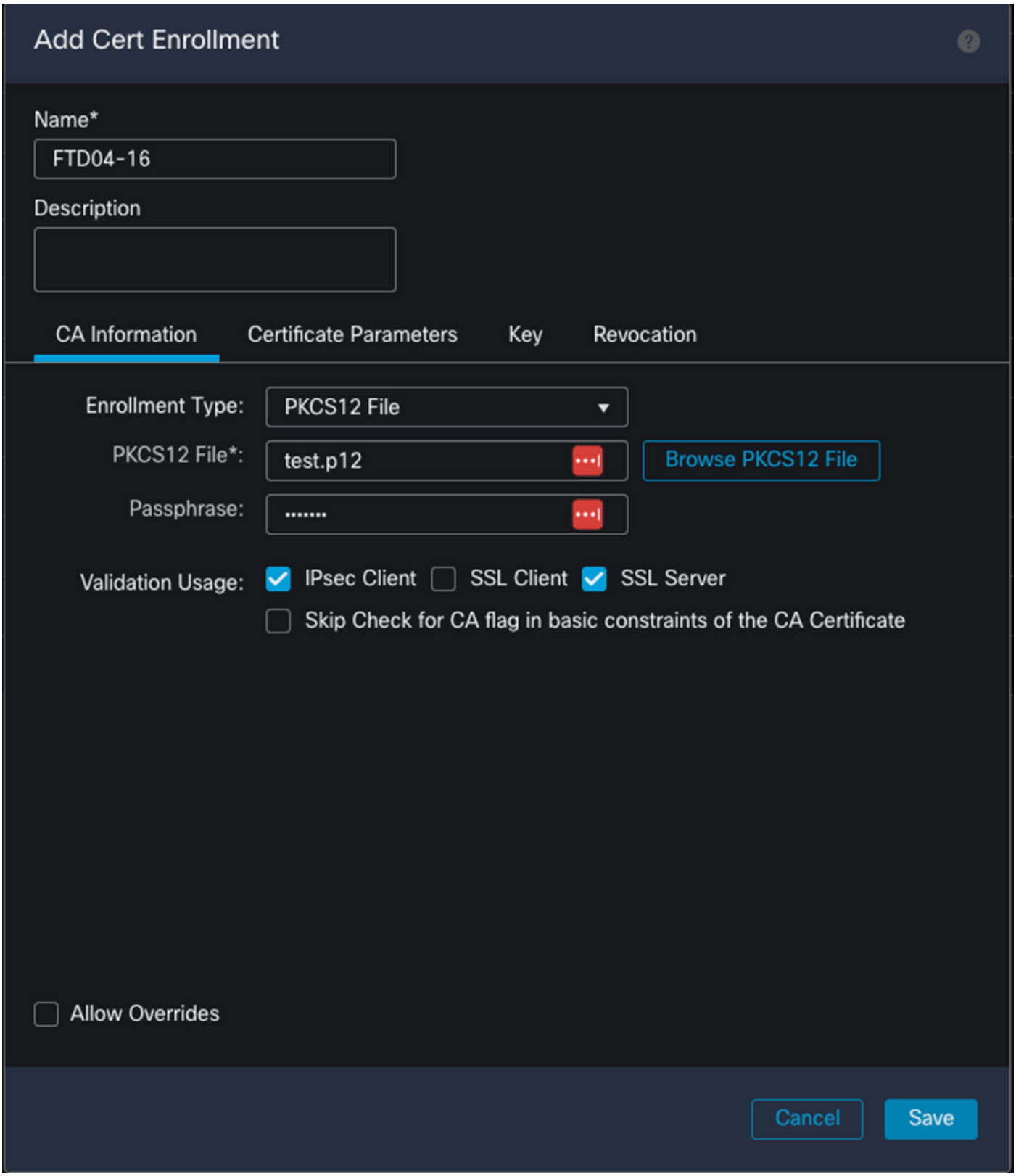
Captura de tela de dispositivos/certificados

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



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.



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

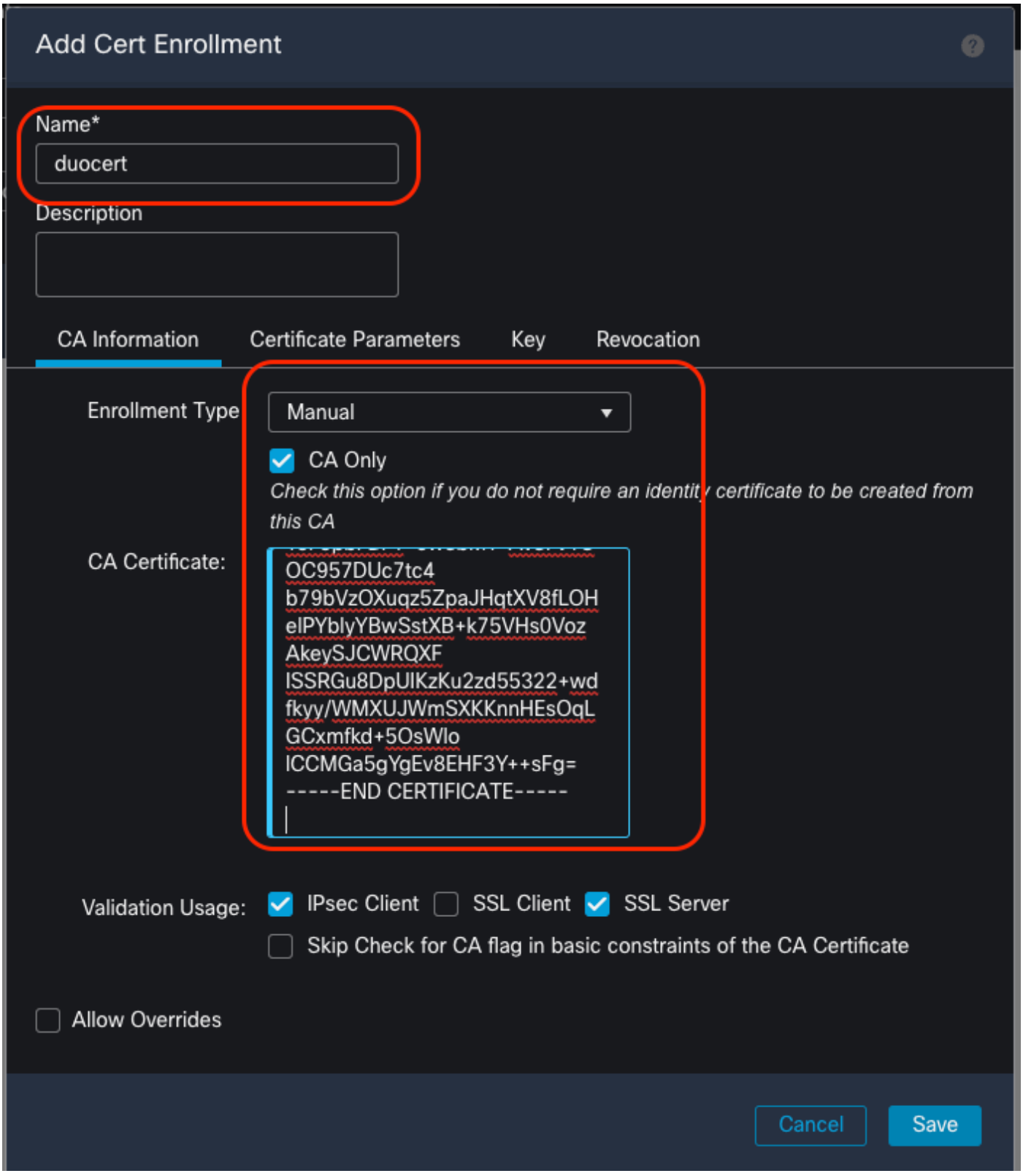
Esta seção descreve a configuração e a implantação do certificado IDP no FTD. Antes de começar, assegure-se de implantar todas as configurações.

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

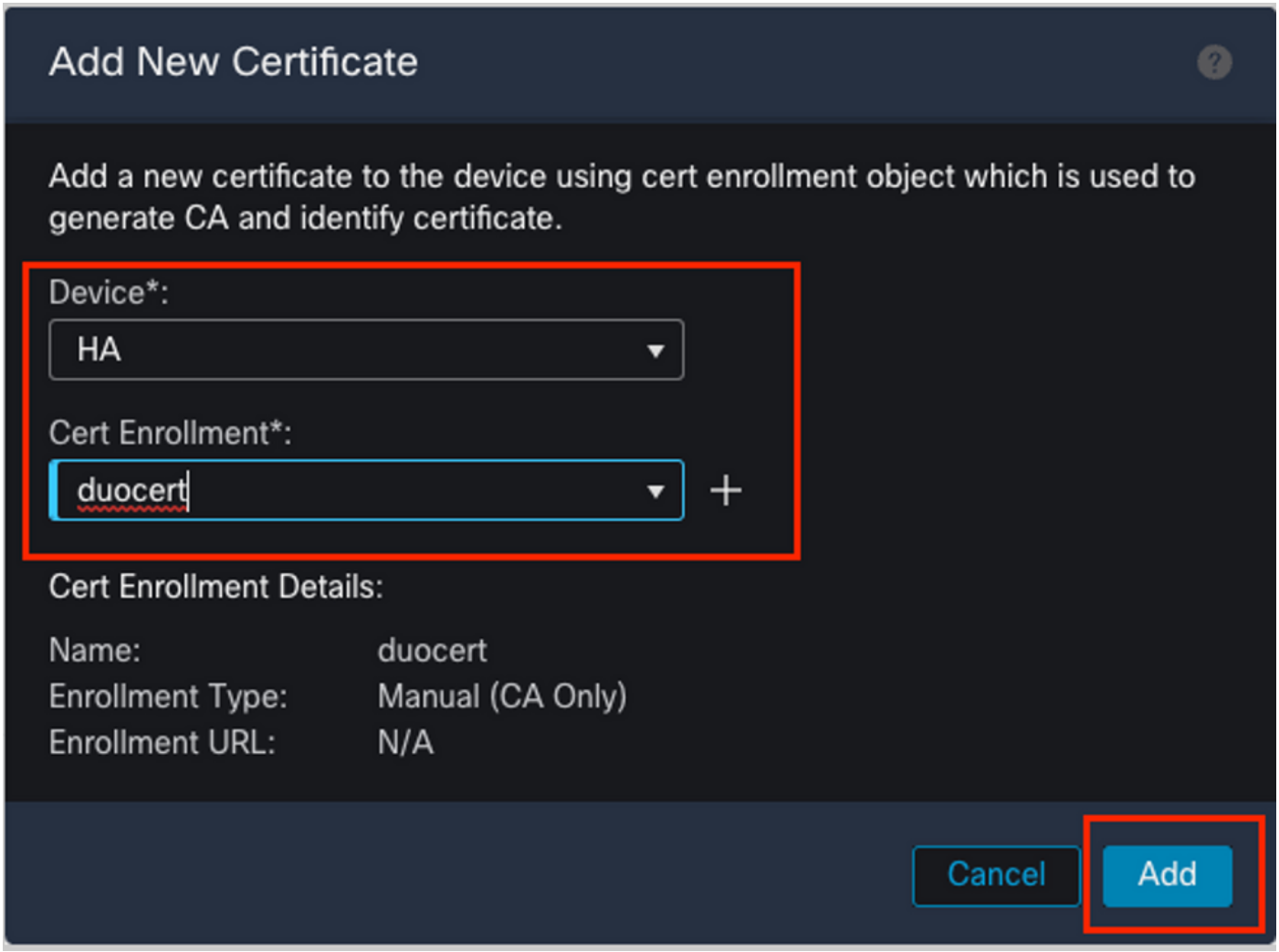


Exemplo de criação de um objeto de registro de certificado

⚠ 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.



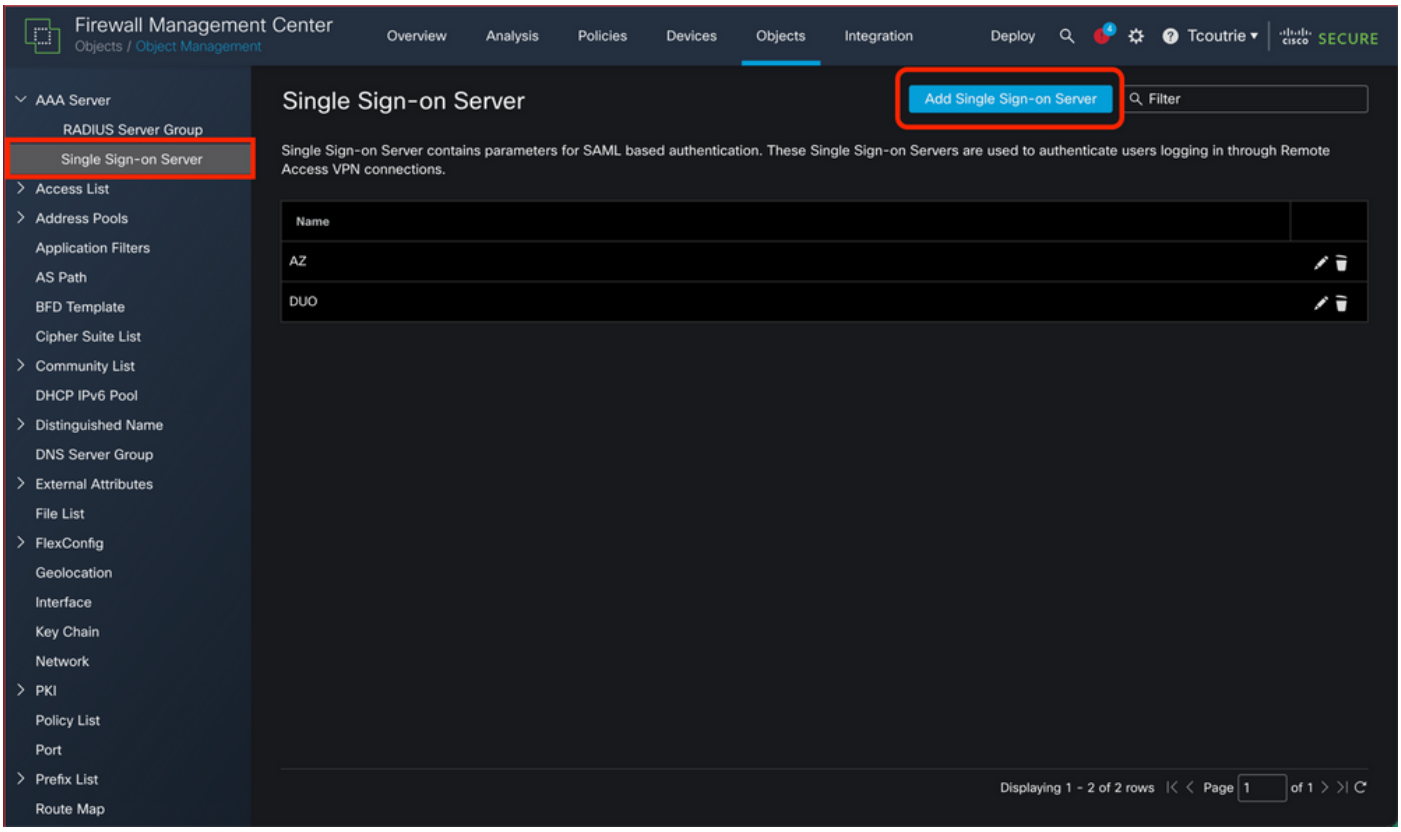
Captura de tela do objeto e dispositivo de registro de certificado adicionado

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".

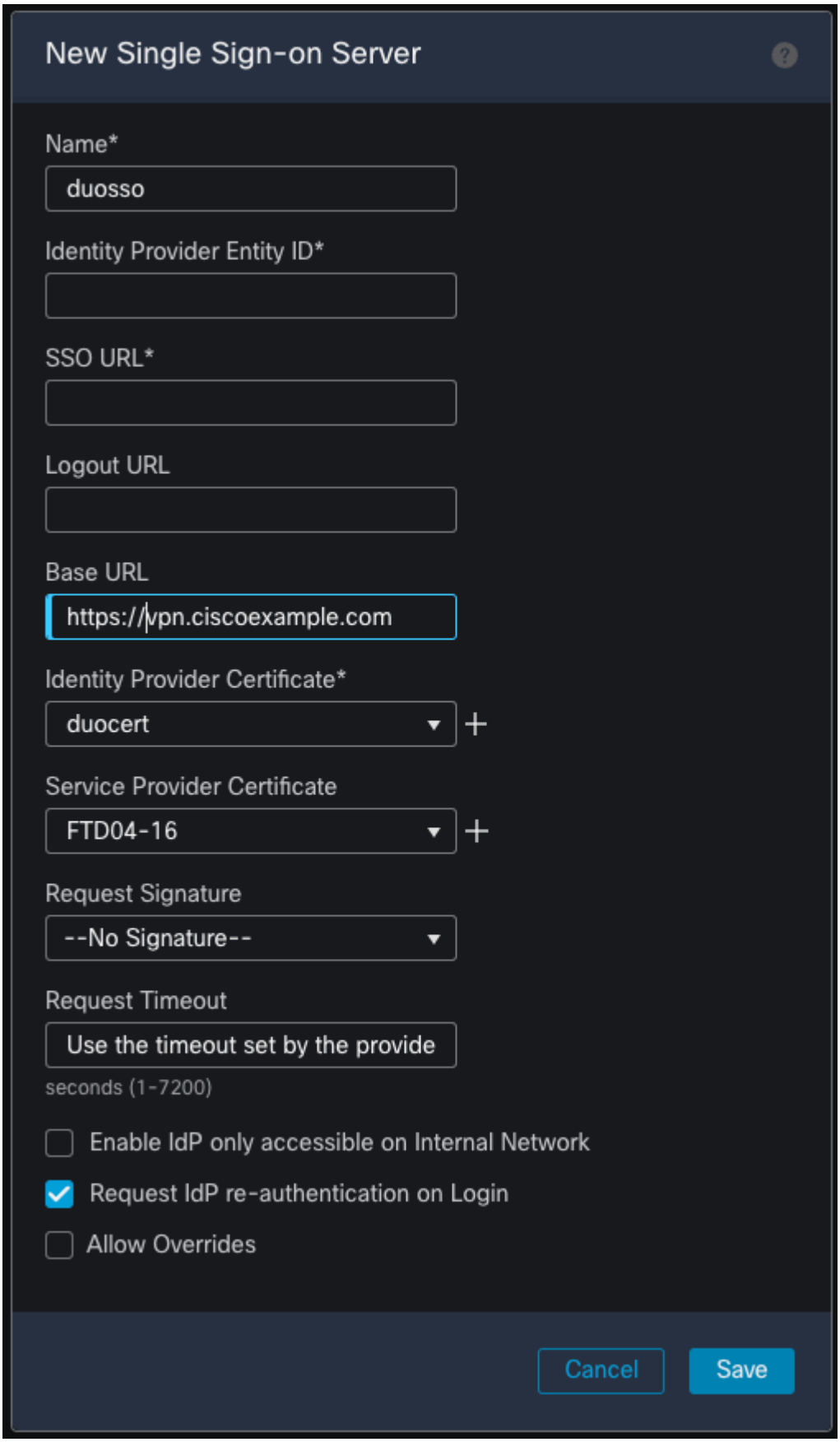


exemplo de criação de um novo objeto SSO

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



Exemplo do novo objeto SSO.

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

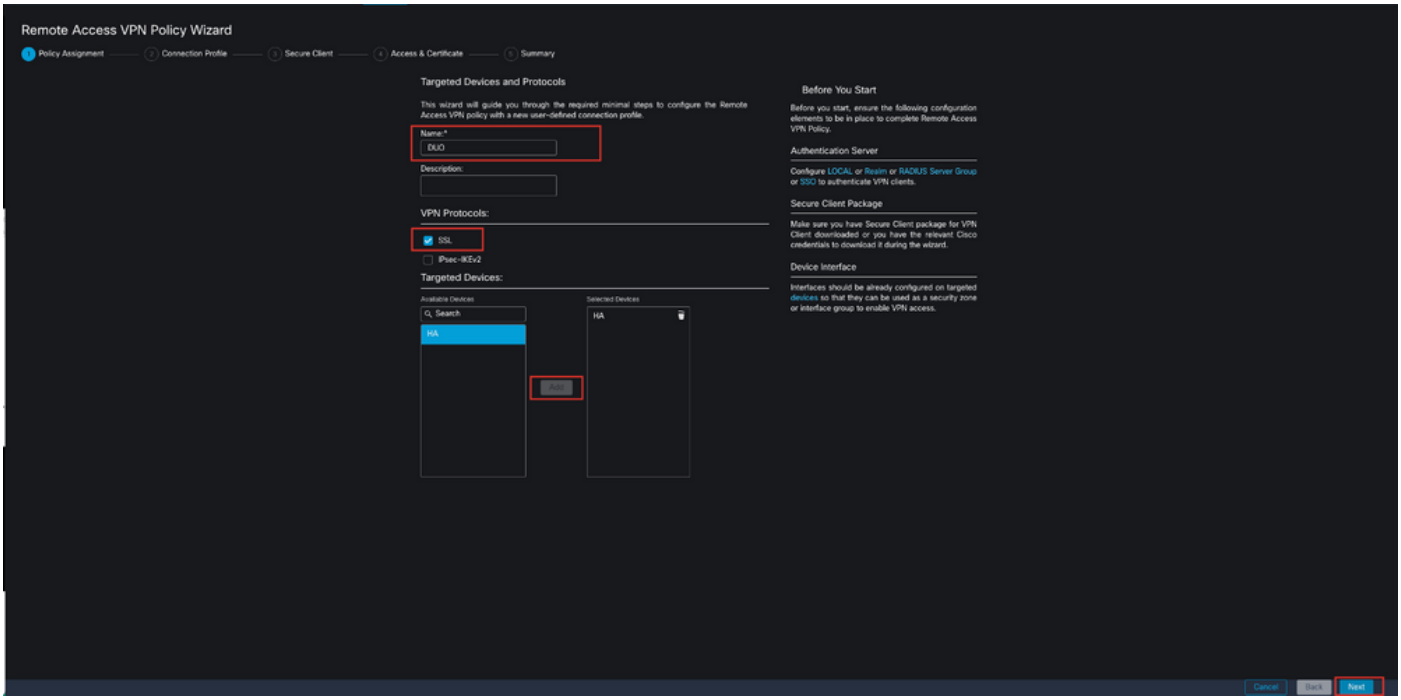
tela

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.



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".

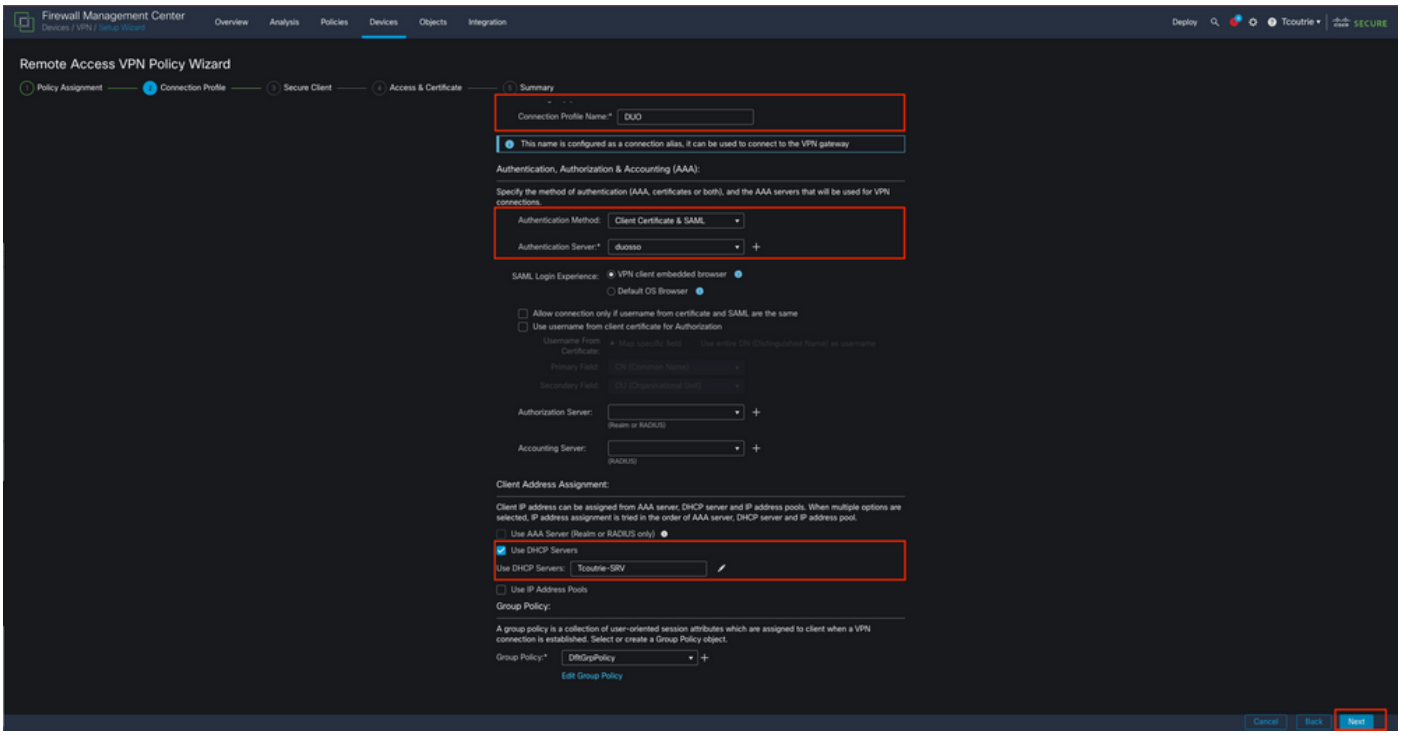
Autenticação, Autorização e Tarifação (AAA - Authentication, Authorization & Accounting):

- 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

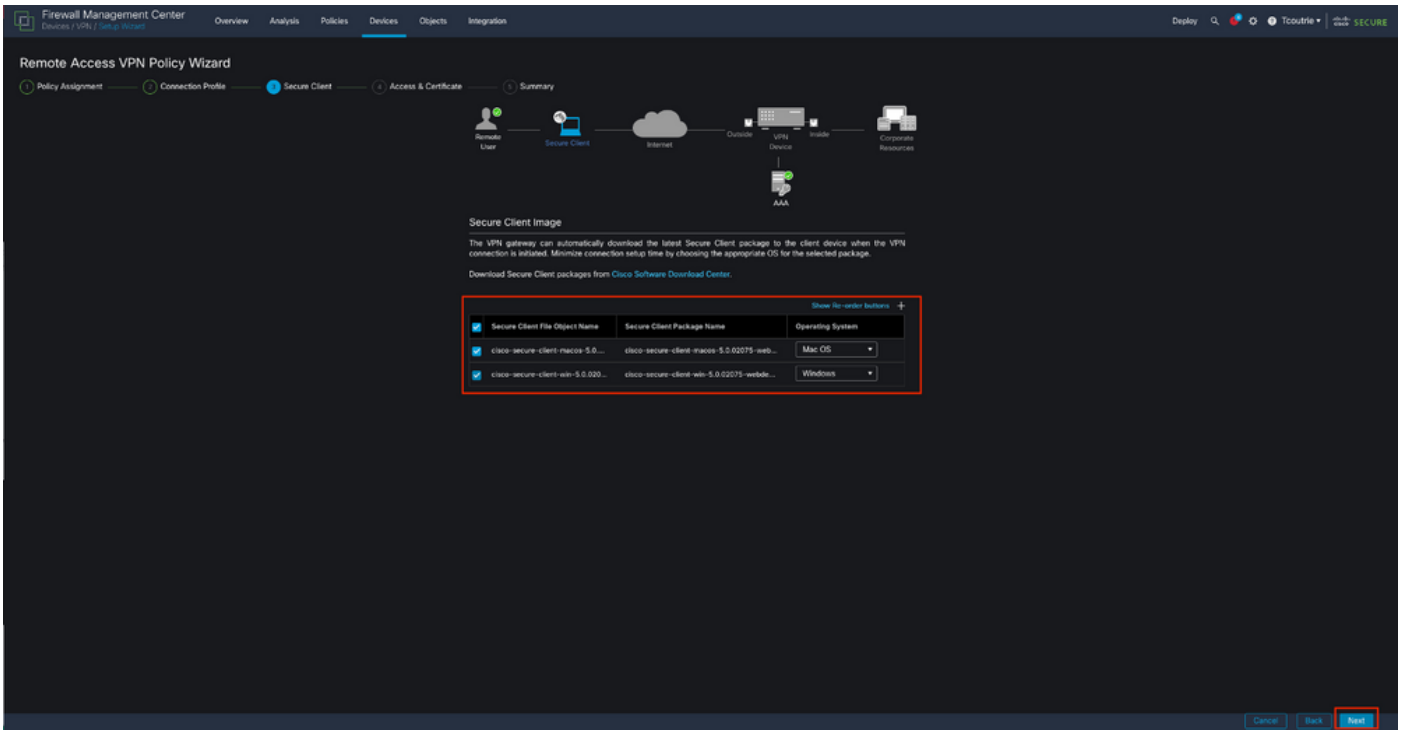
- Usar pools de endereços IP- pool local no FTD



Etapa 2 do assistente de RAVPN

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

Etapa 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.

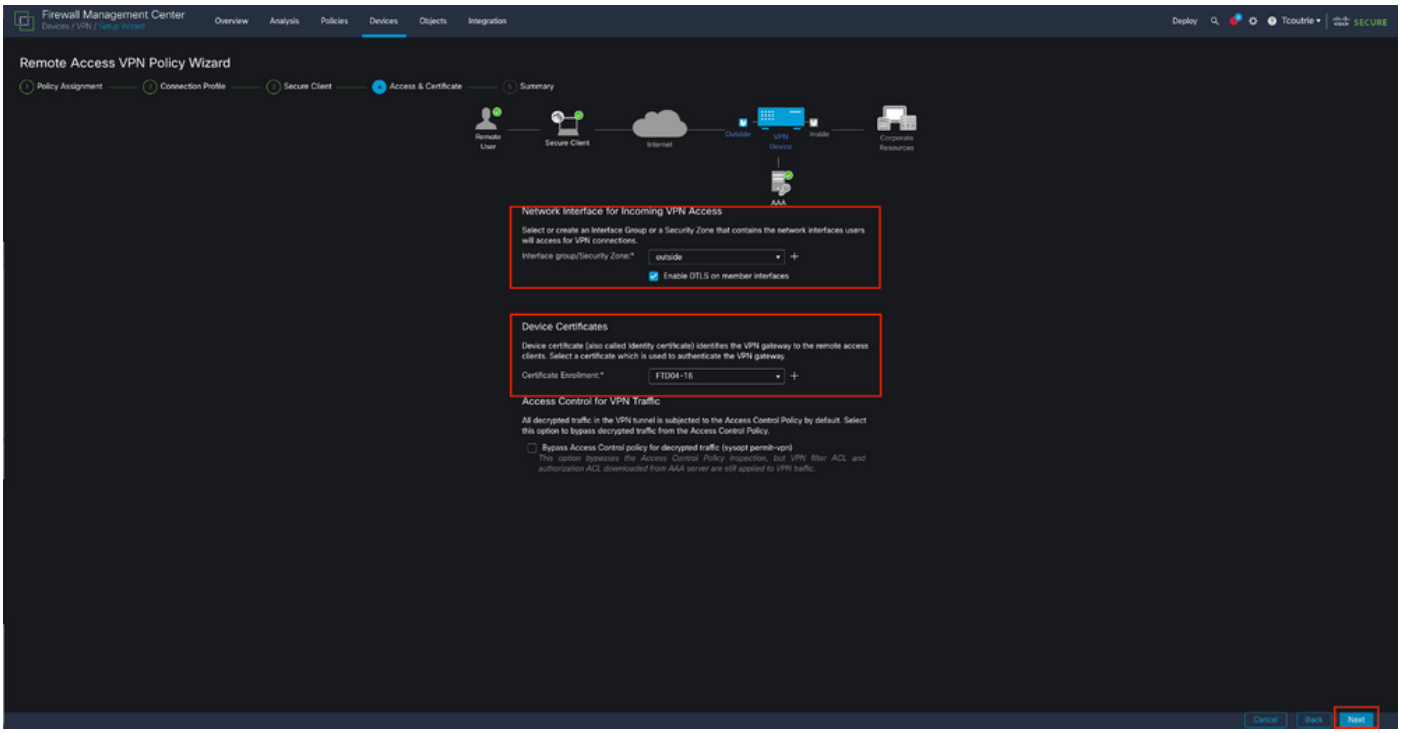


Etapa 3 Assistente de RAVPN

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

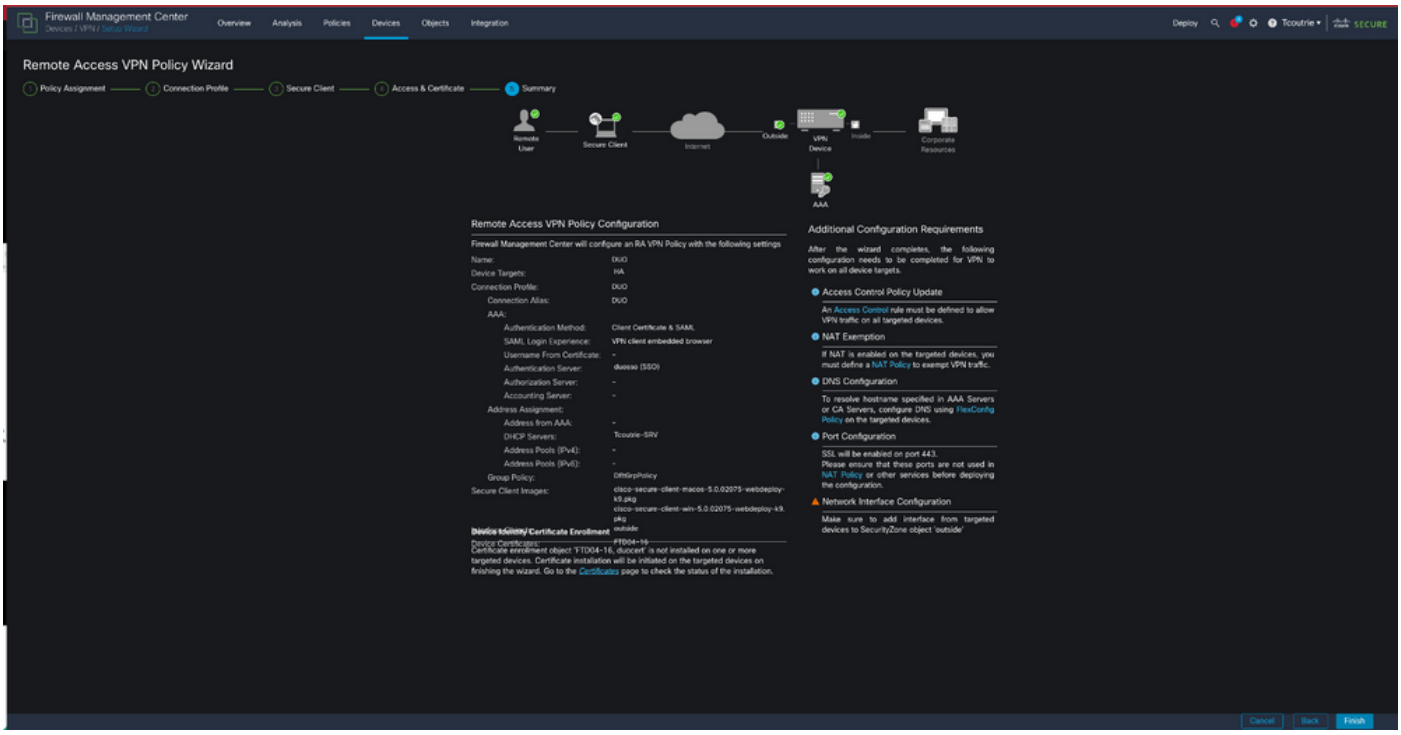


Etapa 4 do assistente de RAVPN

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

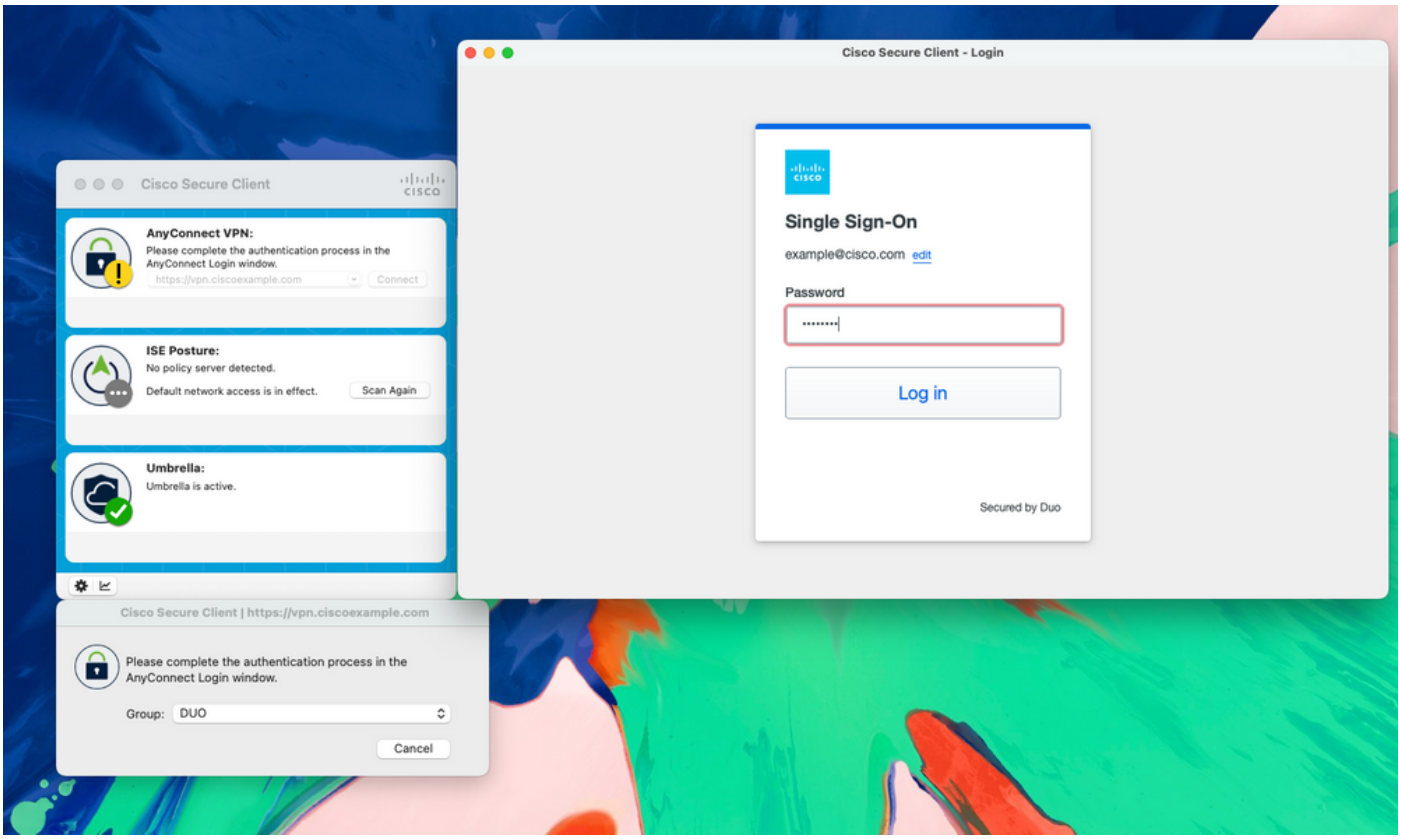
Etapa 7. Implantar as configurações recém-adicionadas.

Verificar

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

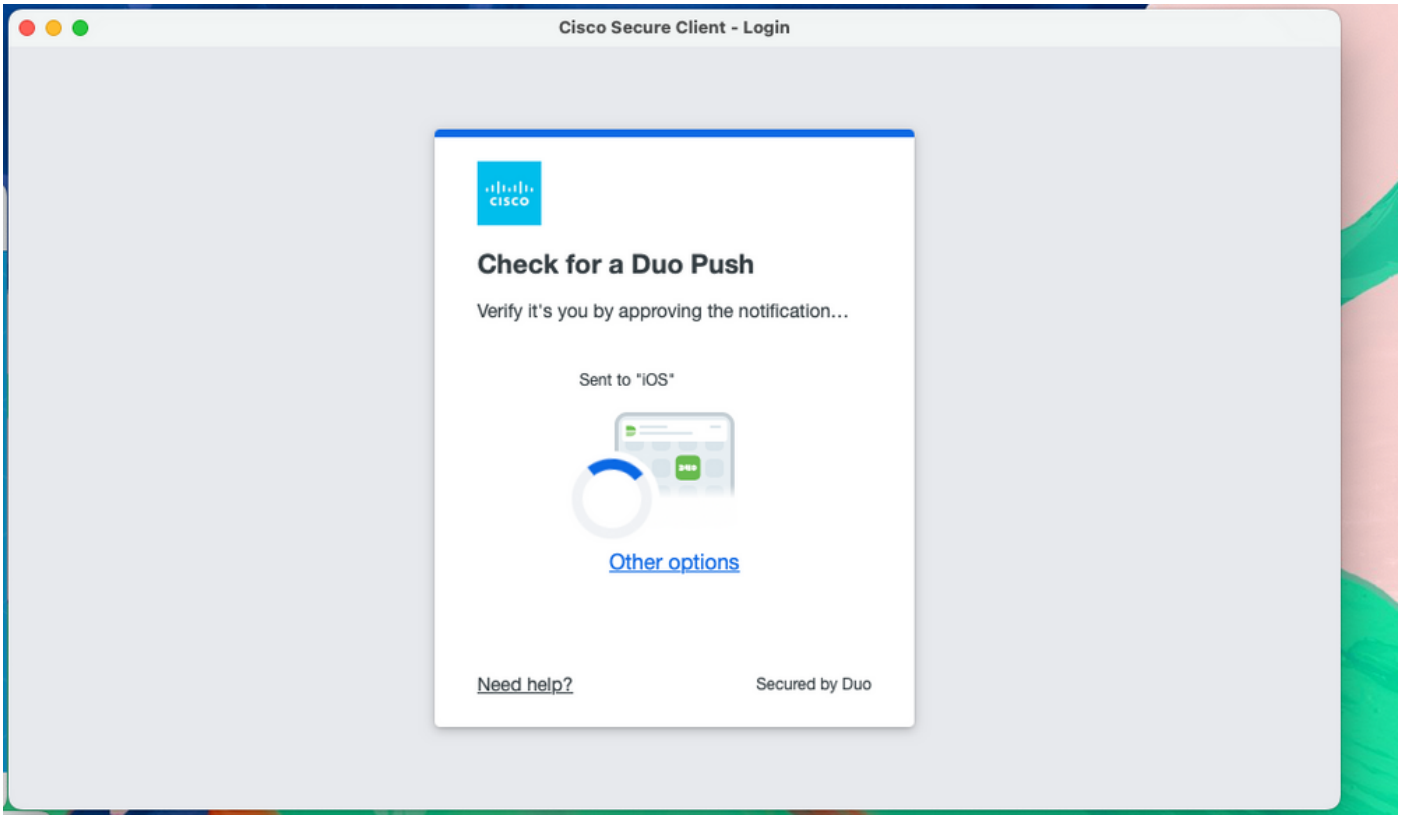
Abra o Cisco Secure Client, insira o FQDN do FTD e conecte-se.

Insira as credenciais na página SSO.



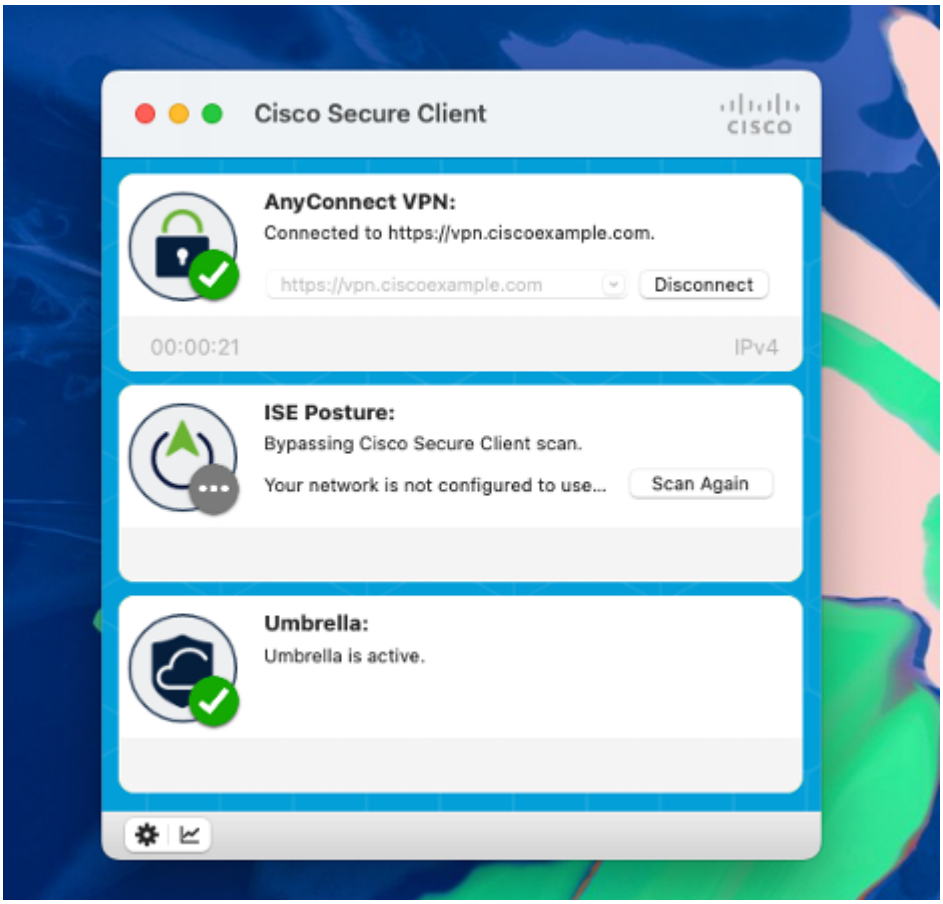
Página SSO via Cisco Secure Client

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.