

Configurar SSL Secure Client com autenticação local no FTD

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurações](#)

[Etapa 1. Verificar licenciamento](#)

[Etapa 2. Carregar o Cisco Secure Client Package no FMC](#)

[Etapa 3. Gerar um certificado autoassinado](#)

[Etapa 4. Criar território local no FMC](#)

[Etapa 5. Configurar SSL Cisco Secure Client](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar o Cisco Secure Client (inclui o Anyconnect) com autenticação local no Cisco FTD gerenciado pelo Cisco FMC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do SSL Secure Client através do Firepower Management Center (FMC)
- Configuração de objetos do Firepower por meio do FMC
- Certificados SSL no Firepower

Componentes Utilizados

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

- Cisco Firepower Threat Defense (FTD) versão 7.0.0 (Build 94)
- Cisco FMC versão 7.0.0 (Build 94)
- Cisco Secure Mobility Client 4.10.01075

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

Neste exemplo, o Secure Sockets Layer (SSL) é usado para criar a Virtual Private Network (VPN) entre o FTD e um cliente Windows 10.

A partir da versão 7.0.0, o FTD gerenciado pelo FMC suporta autenticação local para Cisco Secure Clients. Isso pode ser definido como o método de autenticação principal ou como fallback, caso o método principal falhe. Neste exemplo, a autenticação local é configurada como a autenticação primária.

Antes desta versão de software, a autenticação local do Cisco Secure Client no FTD estava disponível apenas no Cisco Firepower Device Manager (FDM).

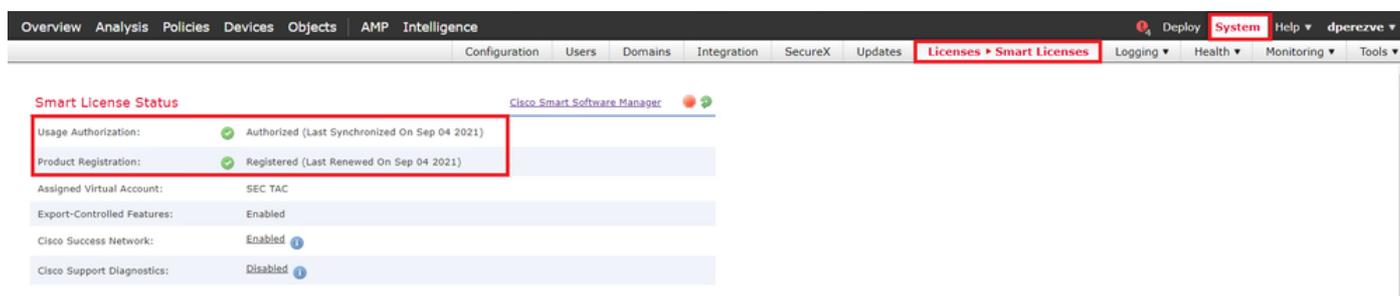
Configurar

Configurações

Etapa 1. Verificar licenciamento

Antes de configurar o Cisco Secure Client, o FMC deve ser registrado e estar em conformidade com o Smart Licensing Portal. Você não pode implantar o Cisco Secure Client se o FTD não tiver uma licença Plus, Apex ou VPN Only válida.

Navegue até System > Licenses > Smart Licenses para garantir que o FMC esteja registrado e em conformidade com o Smart Licensing Portal:



Role para baixo na mesma página. Na parte inferior do gráfico Smart Licenses, você pode ver os diferentes tipos de licenças do Cisco Secure Client (AnyConnect) disponíveis e os dispositivos assinados para cada um. Assegurar que o DTF em questão está registrado em qualquer uma destas categorias:

Smart Licenses

Filter Devices... Edit Performance Tier Edit Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
Firepower Management Center Virtual (2)	✓			
Base (2)	✓			
Malware (2)	✓			
Threat (2)	✓			
URL Filtering (2)	✓			
AnyConnect Apex (2)	✓			
ftdv-dperevze 192.168.13.8 - Cisco Firepower Threat Defense for VMWare - v6.7.0	✓	Cisco Firepower Threat Defense for VMWare	Global	N/A
ftdvha-dperevze (Performance Tier: FTDv50 - Tiered) 192.168.13.9 - Cisco Firepower Threat Defense for VMWare - v7.0.0	✓	Cisco Firepower Threat Defense for VMWare	Global	N/A
AnyConnect Plus (0)				
AnyConnect VPN Only (0)				

Note: Container Instances of same blade share feature licenses

Activate Windows
Go to System in Control Panel to activate Windows.

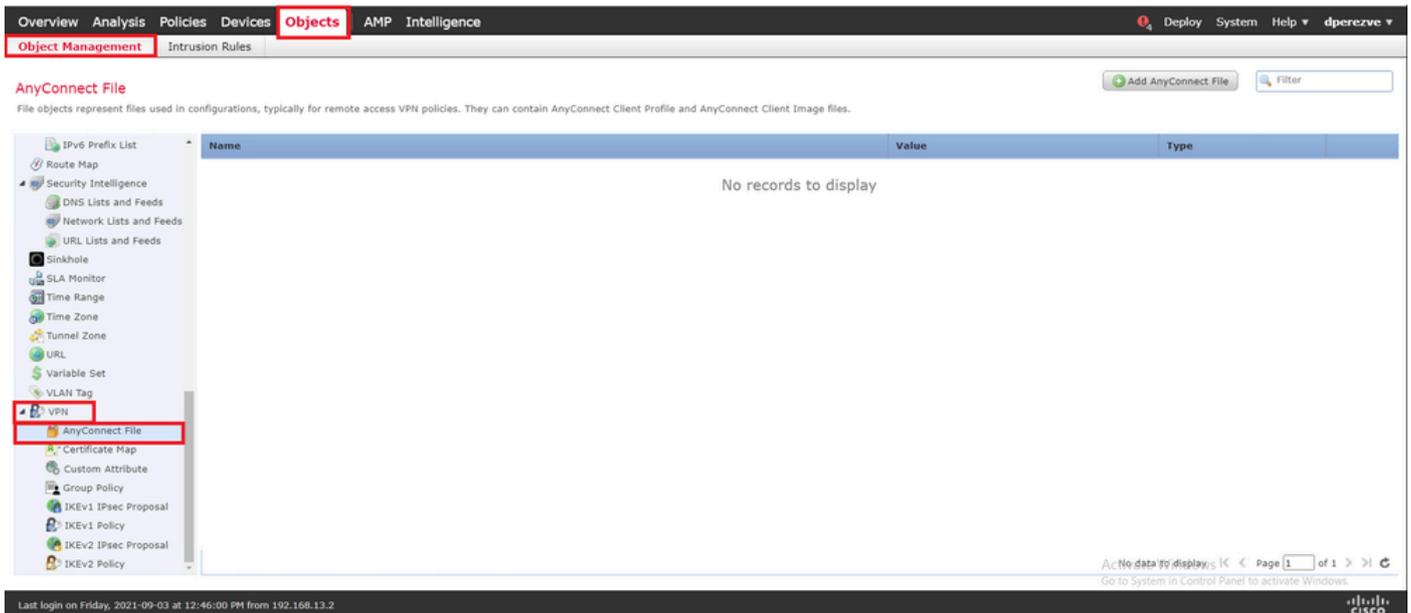
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

Etapa 2. Carregar o pacote Cisco Secure Client no FMC

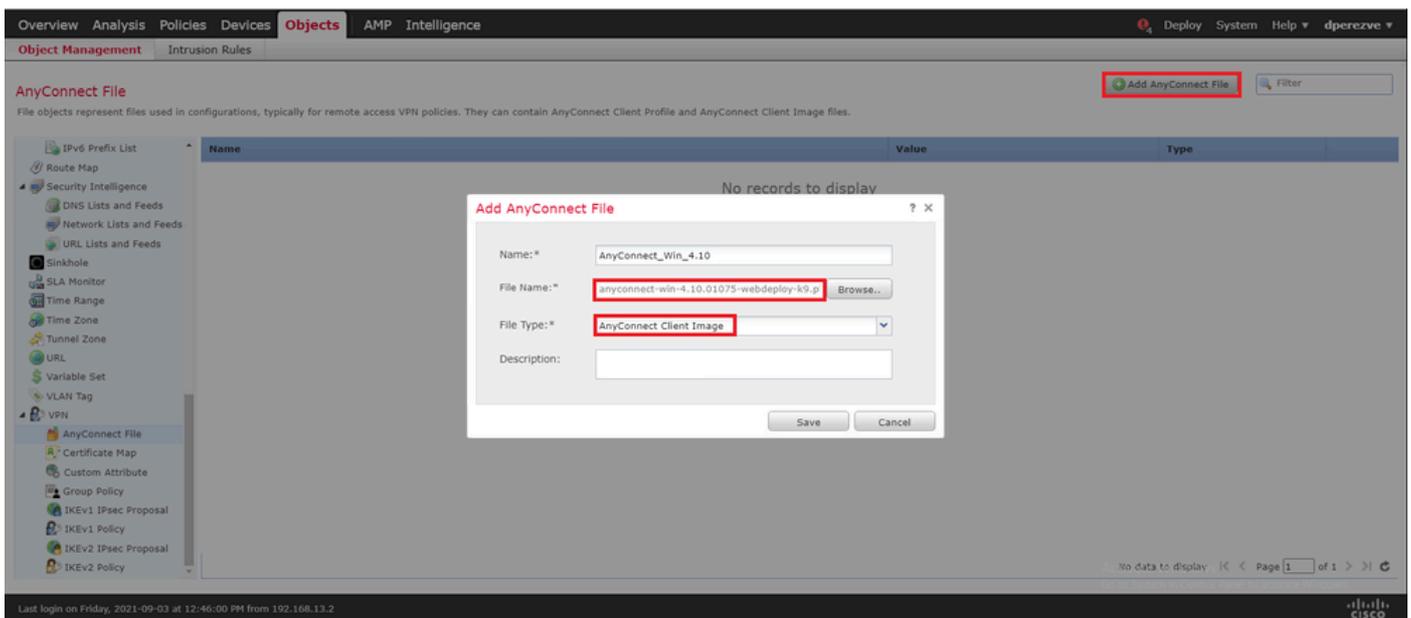
Faça o download do pacote de implantação de headend do Cisco Secure Client (AnyConnect) para Windows em cisco.com:

Application Programming Interface [API] (Windows)   anyconnect-win-4.10.01075-vpnapi.zip Advisories 	21-May-2021	141.72 MB	 
AnyConnect Headend Deployment Package (Windows)   anyconnect-win-4.10.01075-webdeploy-k9.pkg Advisories 	21-May-2021	77.81 MB	 
AnyConnect Pre-Deployment Package (Windows 10 ARM64) - includes individual MSI files   anyconnect-win-arm64-4.10.01075-predeploy-k9.zip Advisories 	21-May-2021	34.78 MB	 
AnyConnect Headend Deployment Package (Windows 10 ARM64)    anyconnect-win-arm64-4.10.01075-webdeploy-k9.pkg Advisories 	21-May-2021	44.76 MB	 
Profile Editor (Windows)   tools-anyconnect-win-4.10.01075-profileeditor-k9.msi Advisories 	21-May-2021	10.90 MB	 
AnyConnect Installer Transforms (Windows)   tools-anyconnect-win-4.10.01075-transforms.zip Advisories 	21-May-2021	0.05 MB	 

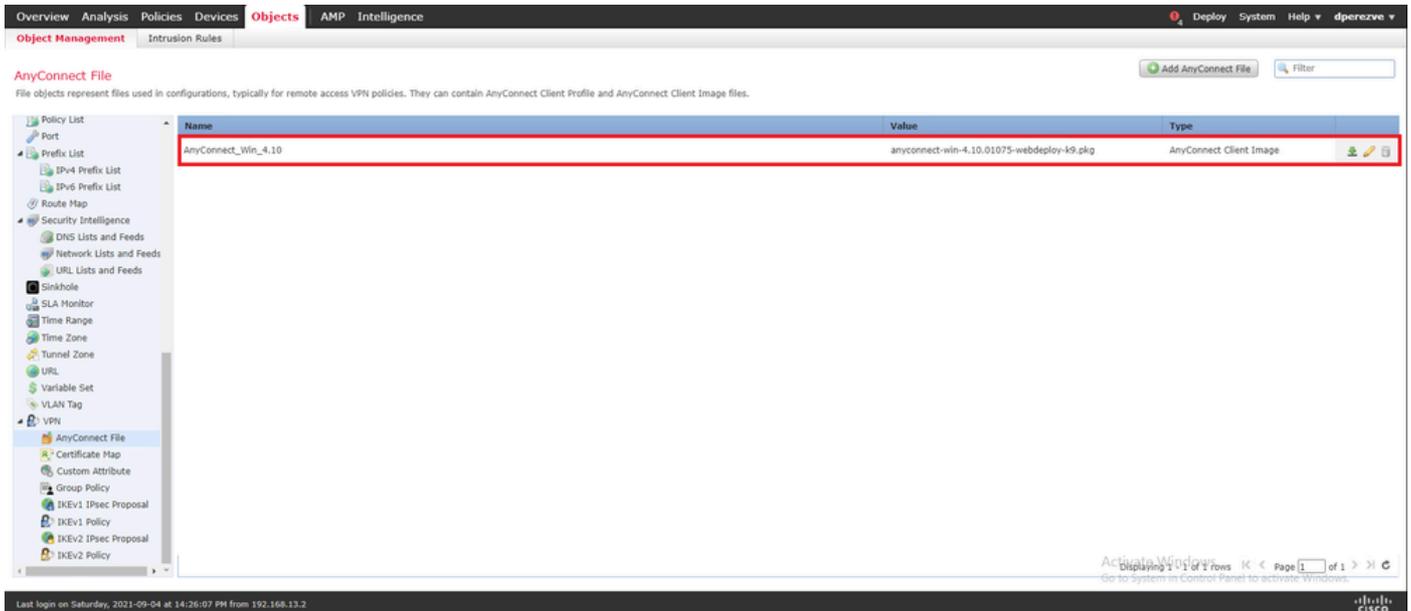
Para carregar a imagem do Cisco Secure Client, navegue para Objects > Object Management e escolha Cisco Secure Client File na categoria VPN no sumário:



Escolha o botão Add AnyConnect File. Na janela Add AnyConnect Secure Client File, atribua um nome para o objeto e escolha Browse... para selecionar o pacote do Cisco Secure Client. Finalmente, escolha AnyConnect Client Image como o tipo de arquivo no menu suspenso:



Escolha o botão Salvar. O objeto deve ser adicionado à lista de objetos:



Etapa 3. Gerar um certificado autoassinado

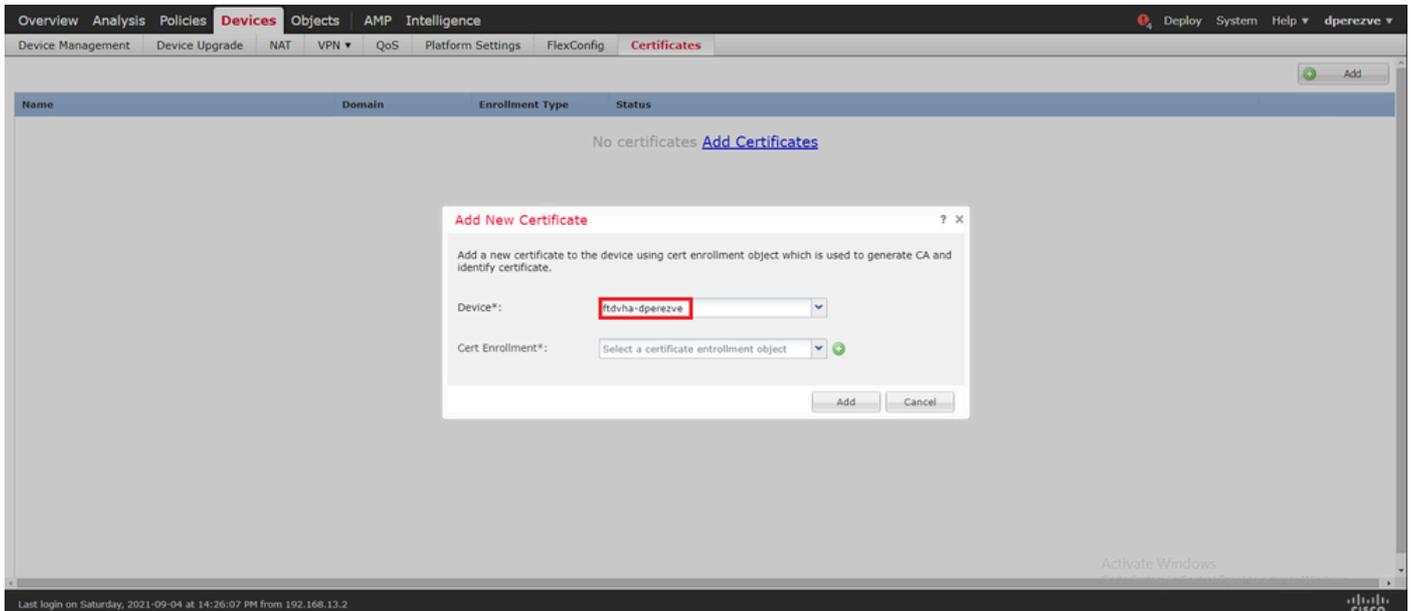
O SSL Cisco Secure Client (AnyConnect) requer um certificado válido para ser usado no handshake SSL entre o headend da VPN e o cliente.

 Observação: neste exemplo, um certificado autoassinado é gerado para essa finalidade. Além disso, além dos certificados autoassinados, é possível carregar um certificado assinado por uma CA (Certificate Authority, Autoridade de Certificação) interna ou também por uma CA conhecida.

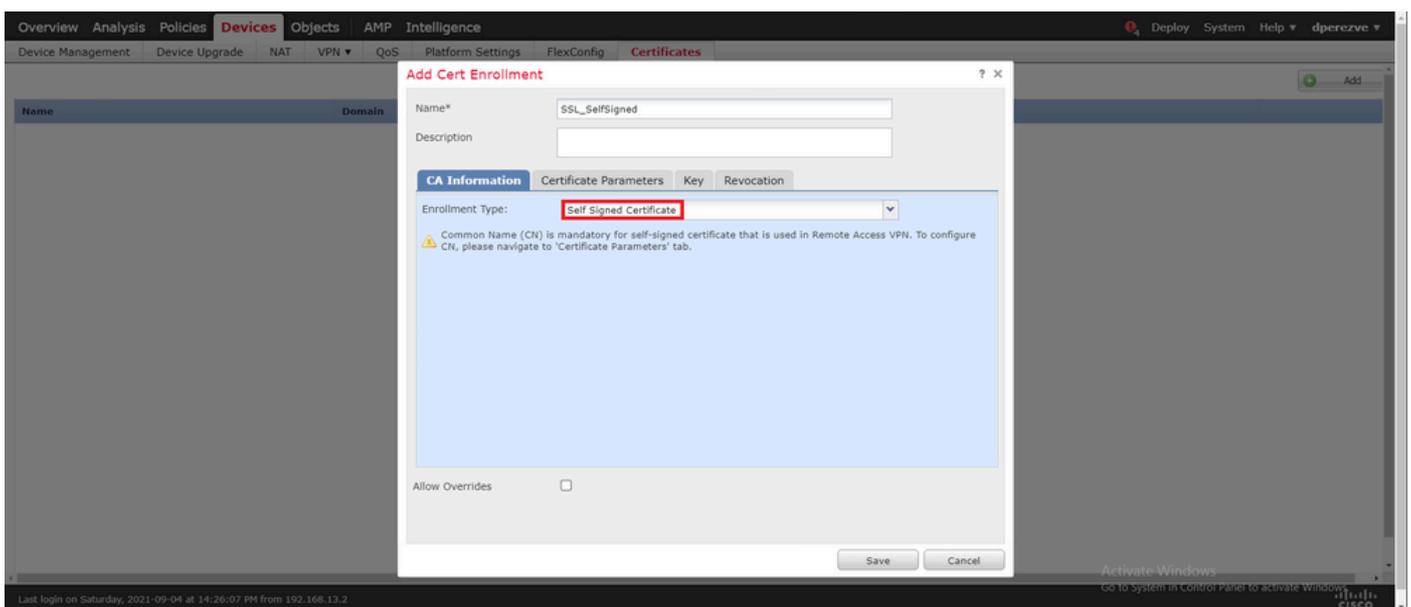
Para criar o certificado autoassinado, navegue para Dispositivos > Certificados.



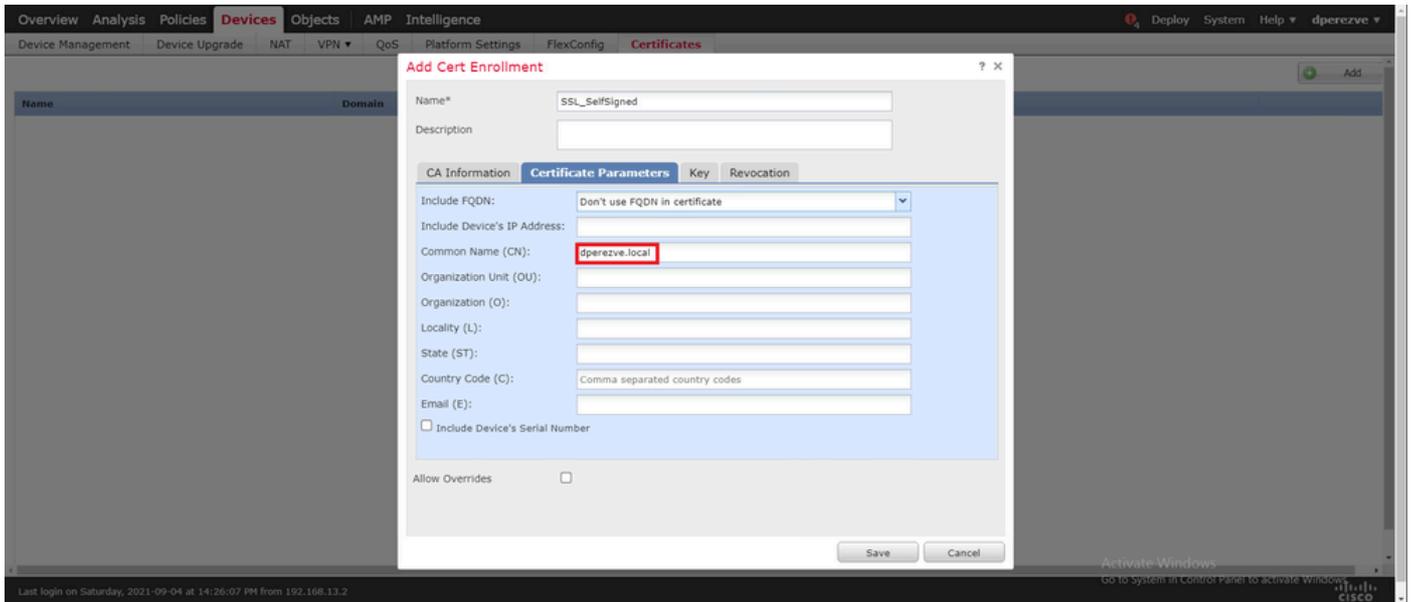
Escolha o botão Adicionar. Em seguida, escolha o FTD listado no menu suspenso Device na janela Add New Certificate.



Escolha o botão Add Cert Enrollment (verde + símbolo) para criar um novo objeto de inscrição. Agora, na janela Add Cert Enrollment, atribua um nome ao objeto e escolha Self Signed Certificate no menu suspenso Enrollment Type.



Por fim, para certificados autoassinados, é obrigatório ter um nome comum (CN). Navegue até a guia Parâmetros do Certificado para definir um CN:



Clique nos botões Salvar e Adicionar. Após alguns segundos, o novo certificado deve ser adicionado à lista de certificados:

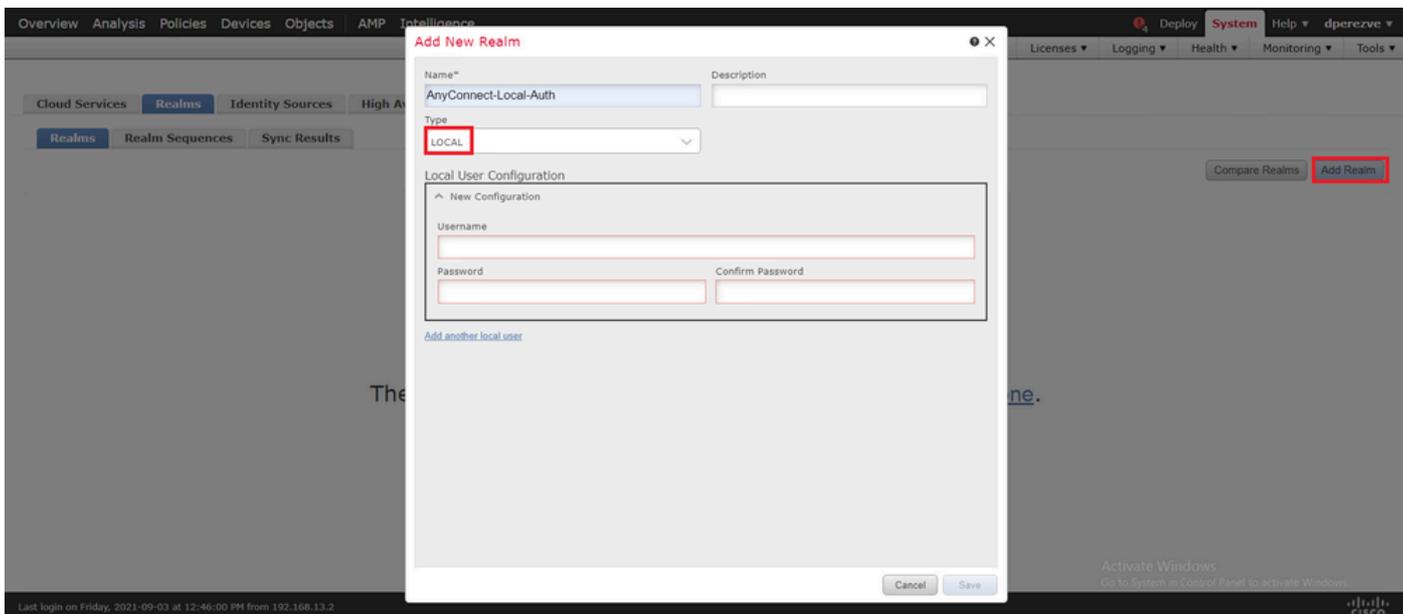


Etapa 4. Criar território local no FMC

O banco de dados de usuário local e as respectivas senhas são armazenados em um realm local. Para criar o território local, navegue para Sistema > Integração > Territórios:

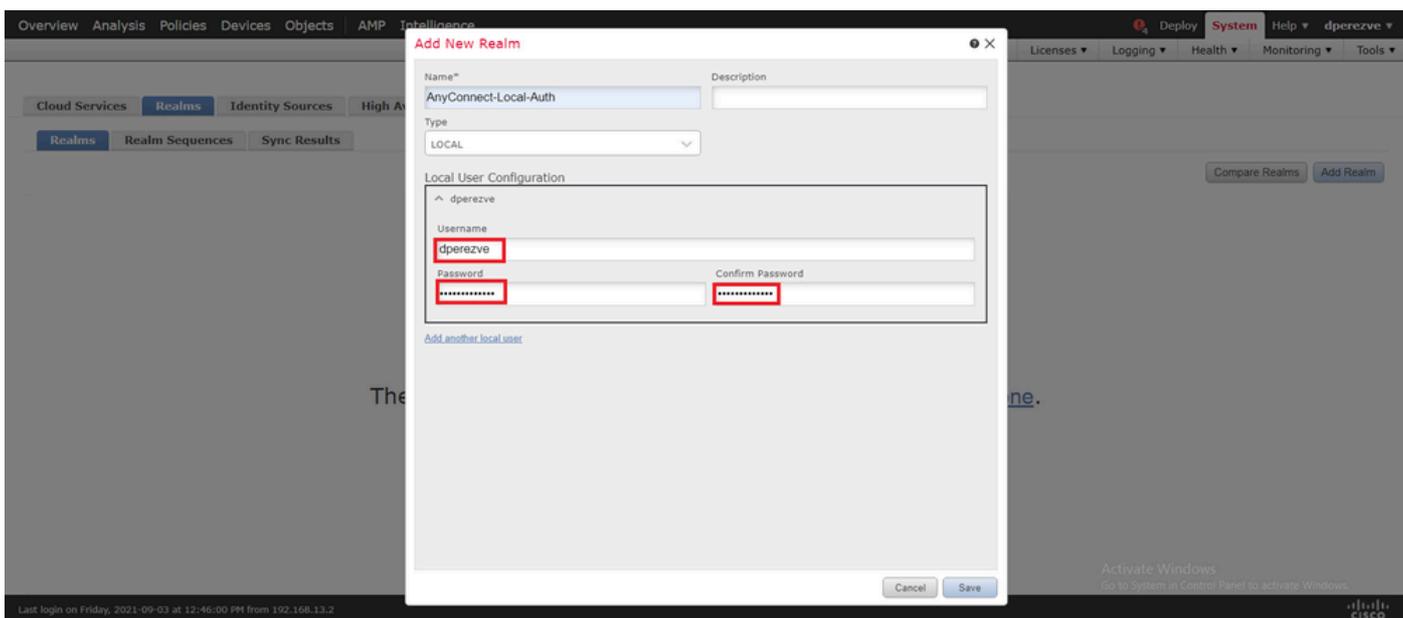


Escolha o botão Add Realm. Na janela Add New Realm, atribua um nome e escolha a opção LOCAL no menu suspenso Type:

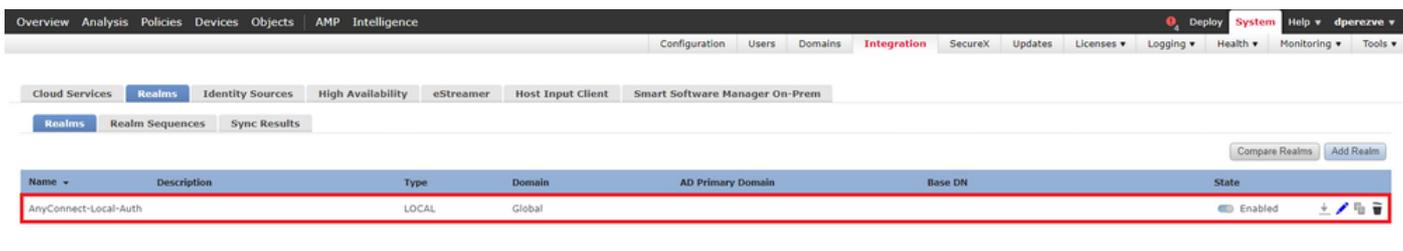


As contas de usuário e senhas são criadas na seção Configuração de usuário local.

 Observação: as senhas devem ter pelo menos uma letra maiúscula, uma letra minúscula, um número e um caractere especial.



Salve as alterações e clique em Adicionar território para adicionar um novo território à lista de territórios existente.

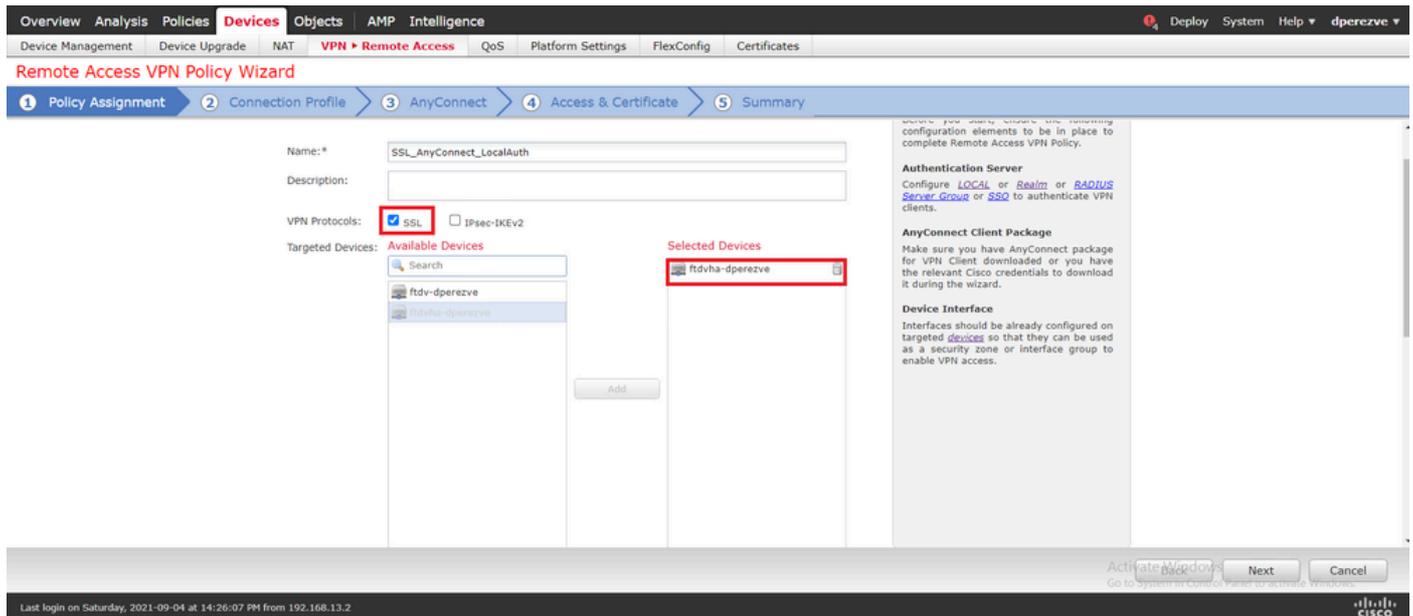


Etapa 5. Configurar SSL Cisco Secure Client

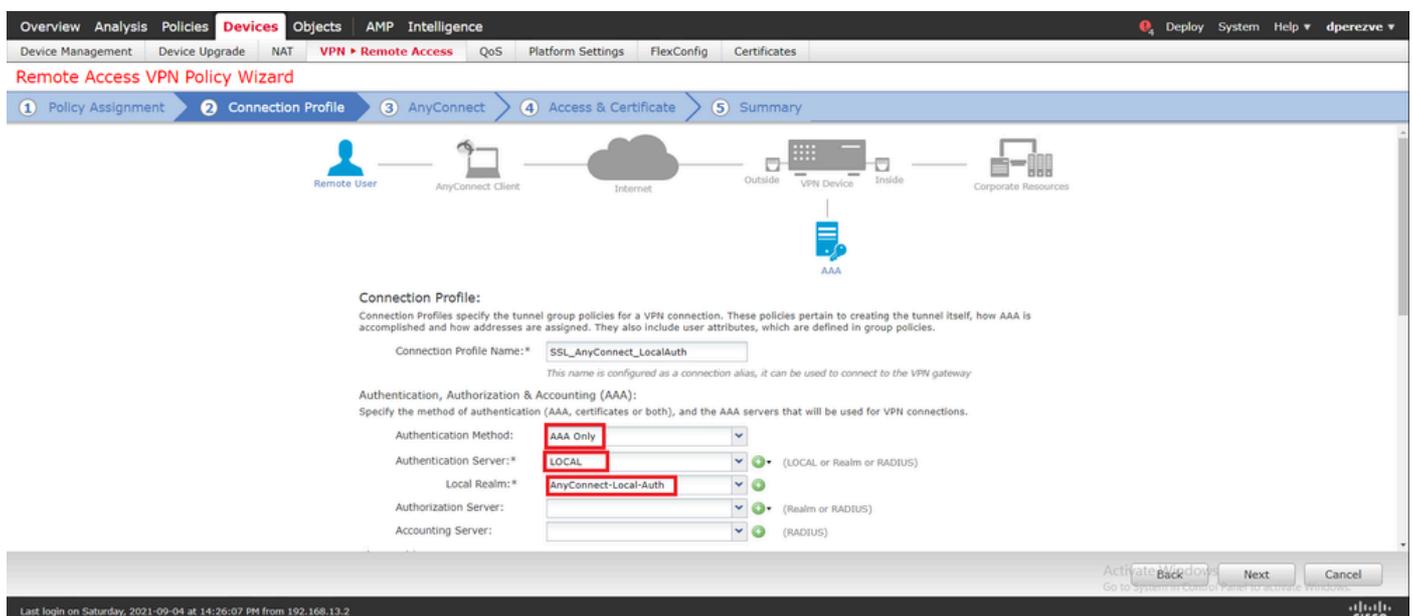
Para configurar o SSL Cisco Secure Client, navegue para Devices > VPN > Remote Access:



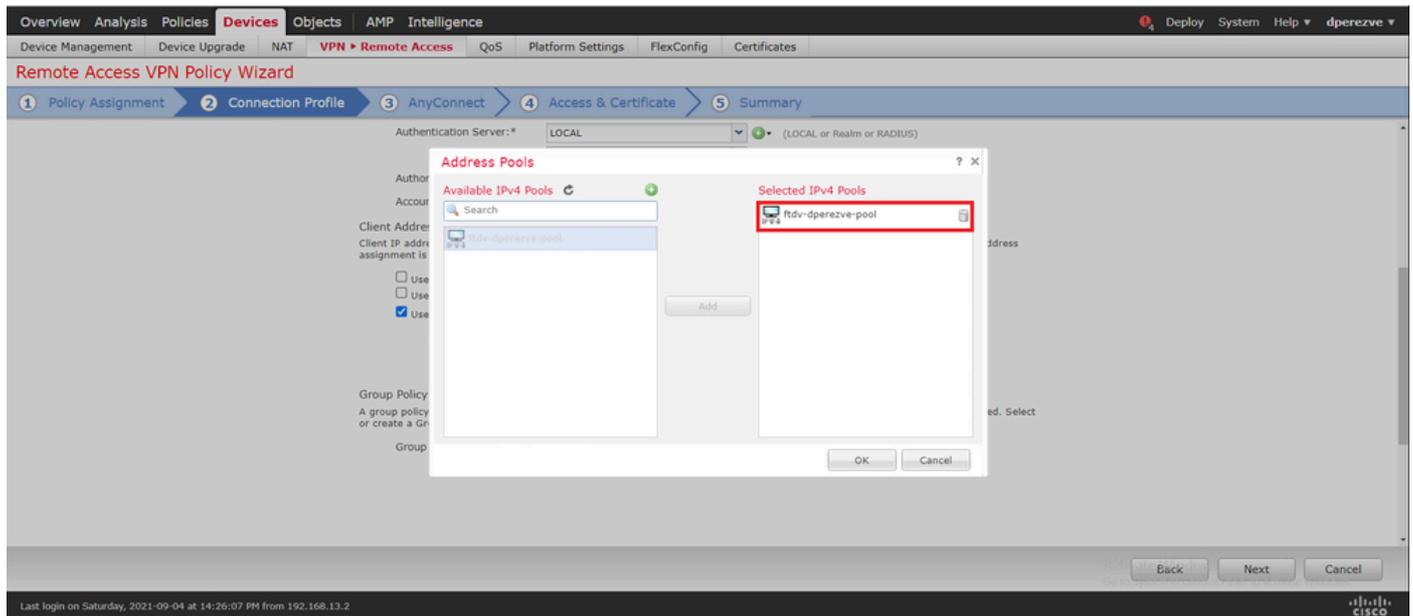
Clique no botão Add para criar uma nova política de VPN. Defina um nome para o perfil de conexão, marque a caixa de seleção SSL e escolha o FTD listado como o dispositivo de destino. Tudo deve ser configurado na seção Atribuição de política no Assistente de política de VPN de acesso remoto:



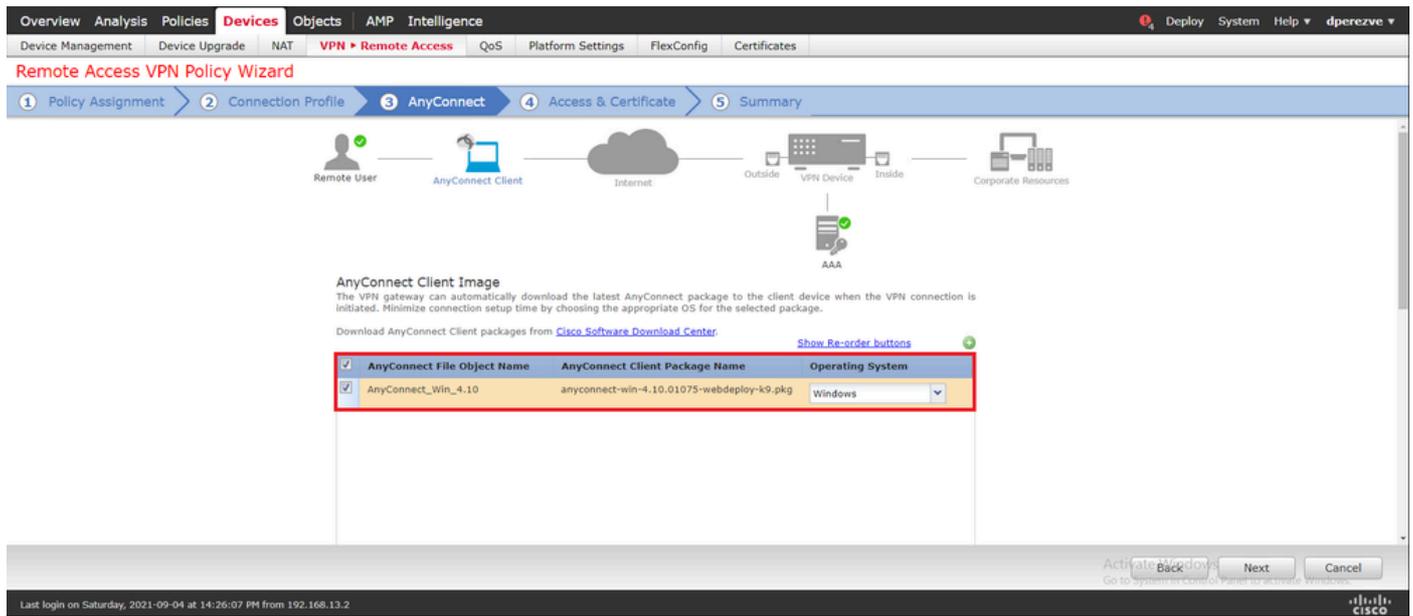
Escolha Next para ir para a configuração Connection Profile. Defina um nome para o perfil de conexão e escolha AAA Only como o método de autenticação. Em seguida, no menu suspenso Authentication Server, escolha LOCAL e, finalmente, escolha o território local criado na Etapa 4 no menu suspenso Território local:



Role para baixo na mesma página e clique no ícone do lápis na seção IPv4 Address Pool para definir o pool de IP usado pelos Cisco Secure Clients:



Clique em Next para ir para a seção AnyConnect . Agora, selecione a imagem do Cisco Secure Client carregada na Etapa 2:



Clique em Avançar para ir para a seção Acesso e certificado. No menu suspenso Interface group/Security Zone, escolha a interface em que o Cisco Secure Client (AnyConnect) precisa ser habilitado. Em seguida, no menu suspenso Certificate Enrollment, escolha o certificado criado na Etapa 3:

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management Device Upgrade NAT VPN Remote Access QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

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

Remote User AnyConnect Client Internet Outside VPN Device Inside Corporate Resources AAA

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:* **VLAN232**

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:* **SSL_SelfSigned**

Activate Windows Back Next Cancel

Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

Finalmente, clique em Avançar para ver um resumo da configuração do Cisco Secure Client:

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management Device Upgrade NAT VPN Remote Access QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

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

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

Name: SSL_AnyConnect_LocalAuth

Device Targets: ftd/va-dperezve

Connection Profile: SSL_AnyConnect_LocalAuth

Connection Alias: SSL_AnyConnect_LocalAuth

AAA:

- Authentication Method: AAA Only
- Authentication Server: AnyConnect-Local-Auth (Local)
- Authorization Server: -
- Accounting Server: -

Address Assignment:

- Address from AAA: -
- DHCP Servers: -
- Address Pools (IPv4): ftd/va-dperezve-pool
- Address Pools (IPv6): -

Group Policy: DfltGrpPolicy

AnyConnect Images: AnyConnect_Win_4.10

Interface Objects: VLAN232

Device Certificates: SSL_SelfSigned

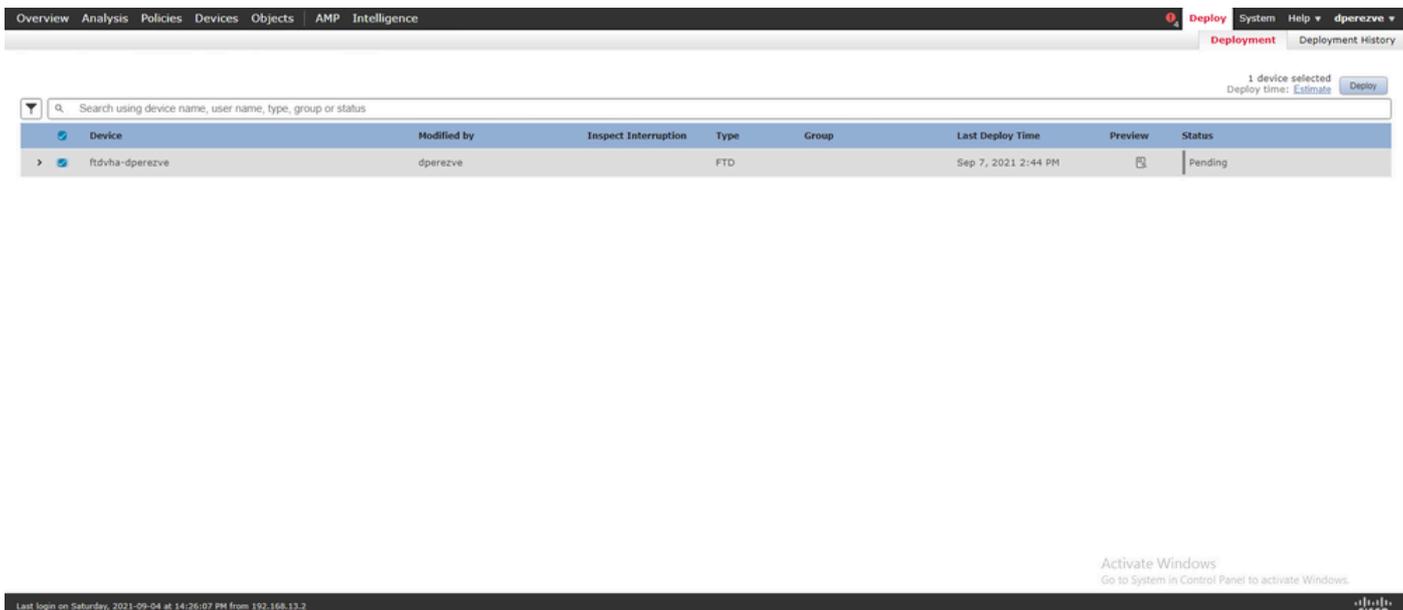
Additional Configuration Requirements
 After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- 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 devices to SecurityZone object 'VLAN232'

Activate Windows Back Finish Cancel

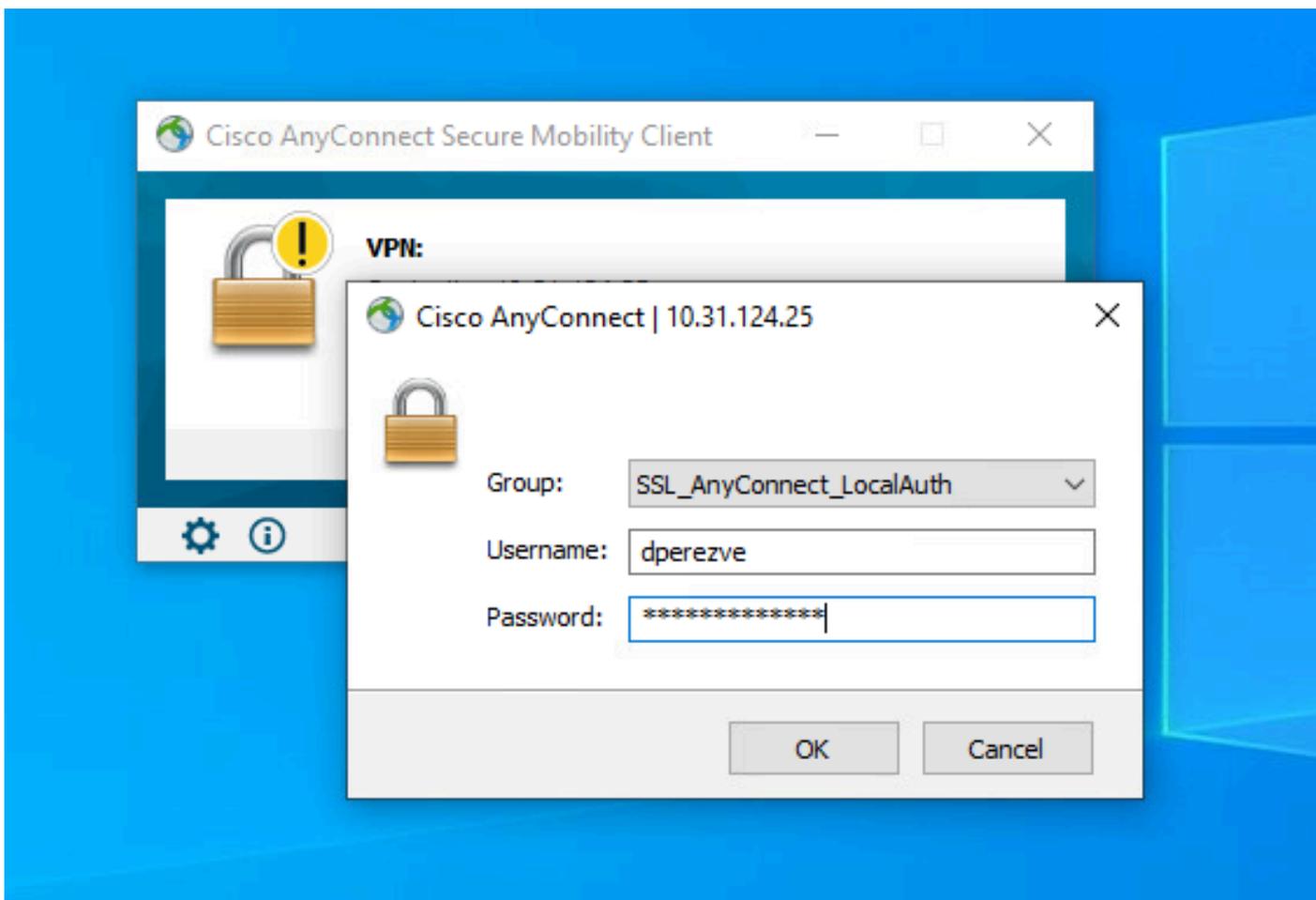
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

Se todas as configurações estiverem corretas, clique em Concluir e implante as alterações no FTD.



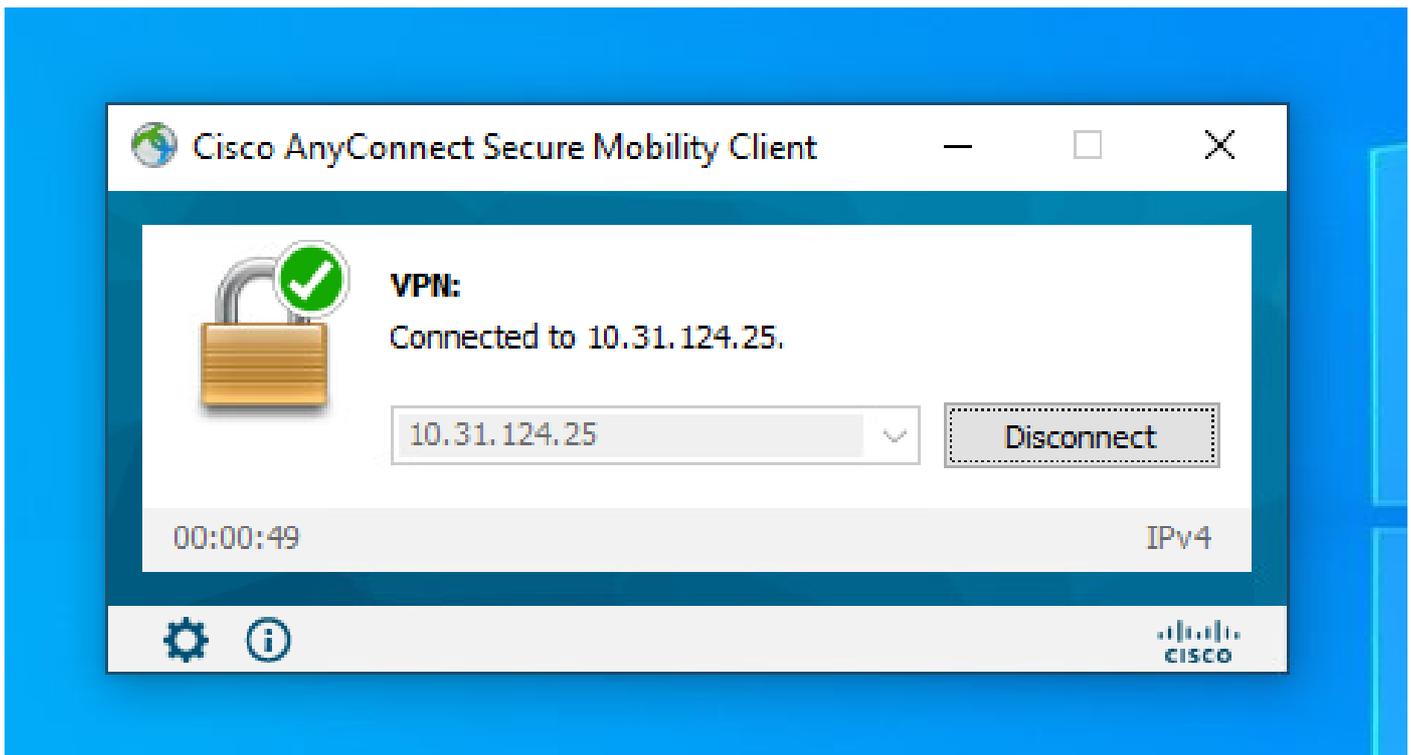
Verificar

Depois que a implantação tiver sido bem-sucedida, inicie uma conexão do Cisco AnyConnect Secure Mobility Client do cliente Windows para o FTD. O nome de usuário e a senha usados no prompt de autenticação devem ser iguais aos criados na Etapa 4:



Quando as credenciais forem aprovadas pelo FTD, o aplicativo Cisco AnyConnect Secure Mobility

Client deverá exibir o estado conectado:



No FTD, você pode executar o comando `show vpn-sessiondb anyconnect` para exibir as sessões do Cisco Secure Client atualmente ativas no Firewall:

```
firepower# show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

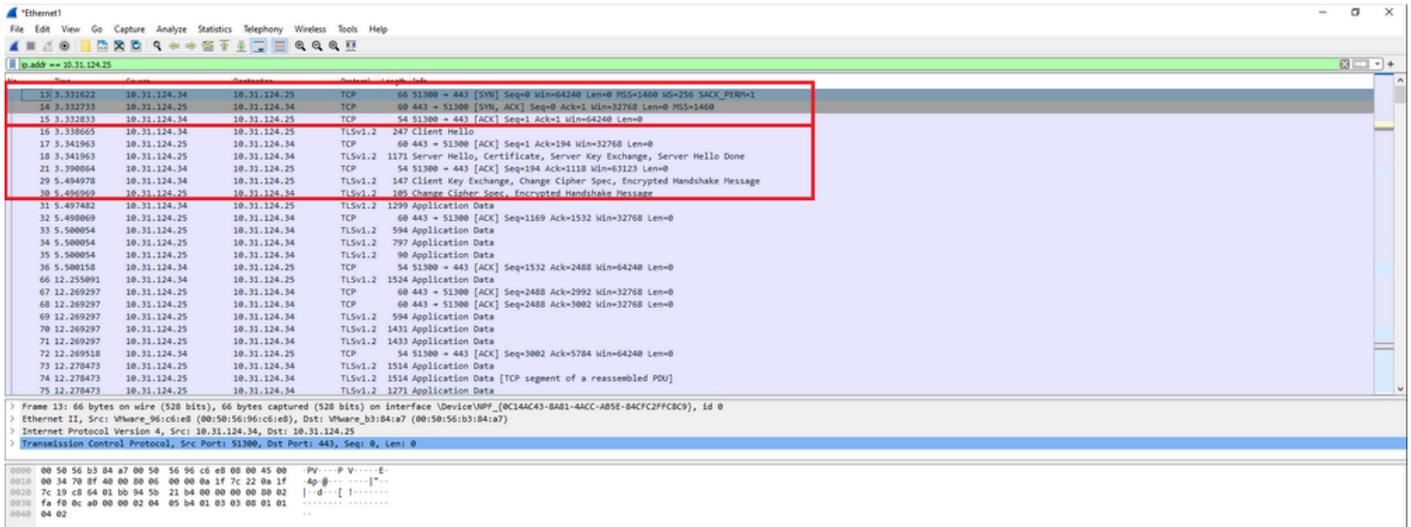
```
Username      : dperezve                Index      : 8
Assigned IP   : 172.16.13.1             Public IP  : 10.31.124.34
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx      : 15756                  Bytes Rx   : 14606
Group Policy  : DfltGrpPolicy
Tunnel Group  : SSL_AnyConnect_LocalAuth
Login Time    : 21:42:33 UTC Tue Sep 7 2021
Duration      : 0h:00m:30s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                    VLAN       : none
Audt Sess ID  : 00000000000080006137dcc9
Security Grp  : none                    Tunnel Zone : 0
```

Troubleshooting

Execute o comando `debug webvpn anyconnect 255` no FTD para ver o fluxo de conexão SSL no FTD:

firepower# debug webvpn anyconnect 255

Além das depurações do Cisco Secure Client, o fluxo de conexão também pode ser observado com capturas de pacotes TCP. Este é um exemplo de uma conexão bem-sucedida, um handshake triplo regular entre o cliente Windows e o FTD é concluído, seguido por um handshake SSL usado para concordar com cifras.



Após handshakes de protocolo, o FTD deve validar as credenciais com as informações armazenadas no território local.

Colete o pacote DART e entre em contato com o TAC da Cisco para pesquisa adicional.

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.