# Configurar SSL AnyConnect Management VPN no FTD

## Contents



## Introduction

Este documento descreve como configurar um túnel de gerenciamento do Cisco AnyConnect em um Cisco Firepower Threat Defense (FTD) gerenciado pelo Cisco Firepower Management Center (FMC). No exemplo abaixo, a Secure Sockets Layer (SSL) é usada para criar a VPN (Virtual Private Network) entre o FTD e um cliente Windows 10.

Contribuído por Daniel Perez Vertti Vazquez, engenheiro do TAC da Cisco.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Editor de perfis do Cisco AnyConnect
- Configuração do AnyConnect SSL através do FMC.
- Autenticação de certificado de cliente

### Componentes Utilizados

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

- Cisco FTD versão 6.7.0 (Build 65)
- Cisco FMC versão 6.7.0 (Build 65)
- Cisco AnyConnect 4.9.01095 instalado na máquina Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

# Informações de Apoio

A partir da versão 6.7, o Cisco FTD suporta a configuração de túneis de gerenciamento do AnyConnect. Isso corrige a solicitação de aprimoramento aberta anteriormente CSCvs78215.

O recurso Gerenciamento do AnyConnect permite criar um túnel VPN imediatamente depois que o endpoint termina sua inicialização. Não há necessidade de que os usuários iniciem manualmente o aplicativo AnyConnect, assim que o sistema é ligado, o serviço do agente AnyConnect VPN detecta o recurso Management VPN e inicia uma sessão do AnyConnect usando a entrada do host definida na lista de servidores do perfil de gerenciamento do AnyConnect VPN.

## Limitações

- Somente a autenticação de certificado do cliente é suportada.
- Somente o Repositório de Certificados de Máquina é compatível com clientes Windows.
- Não suportado no Cisco Firepower Device Manager (FDM) CSCvx90058.
- Não suportado em clientes Linux.

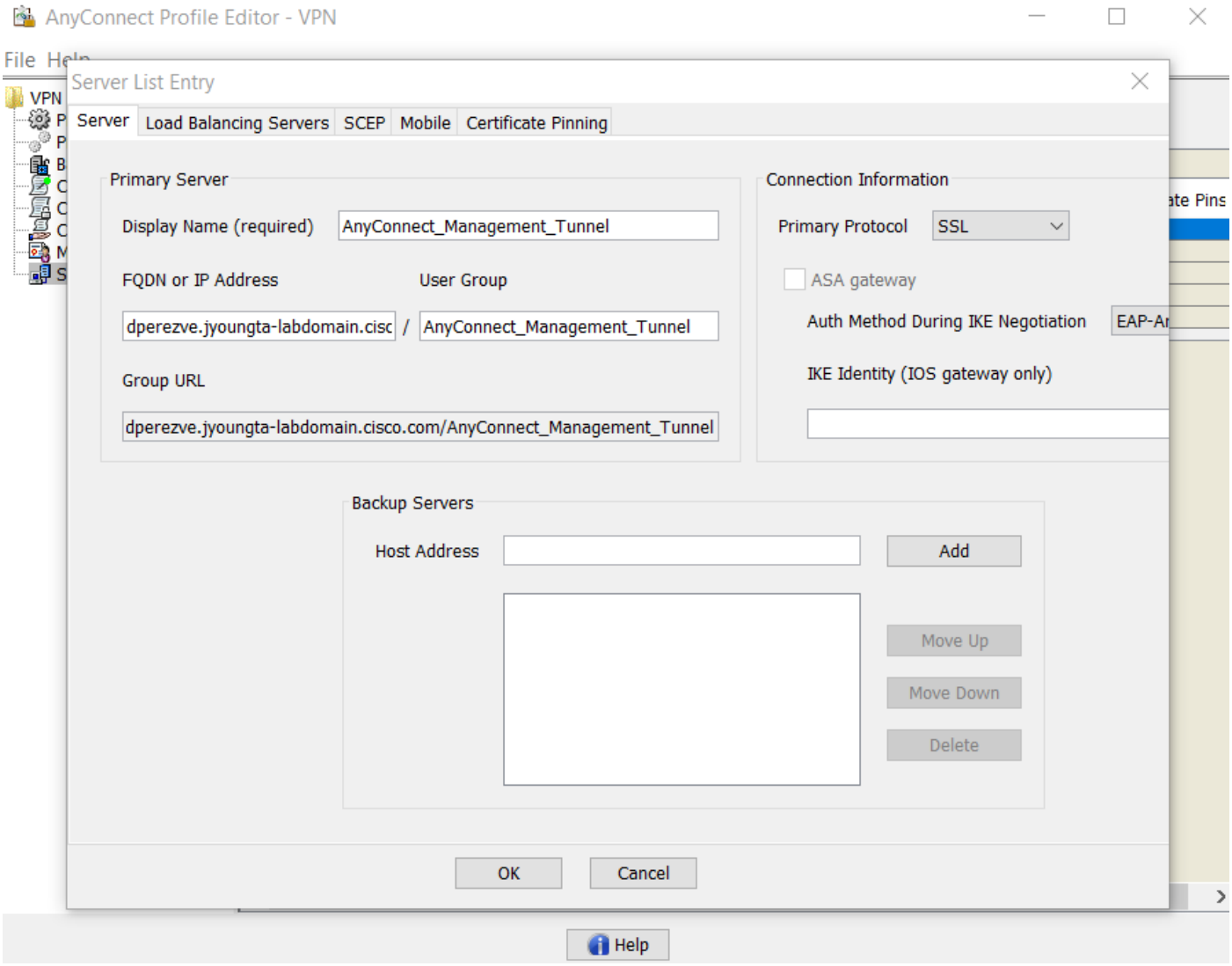
# Configurar

## Configurações

### Etapa 1. Criar perfil de VPN de gerenciamento do AnyConnect

Abra o Editor de perfis do AnyConnect para criar o perfil do AnyConnect Management VPN. O perfil de gerenciamento contém todas as configurações usadas para estabelecer o túnel VPN após a inicialização do ponto final.

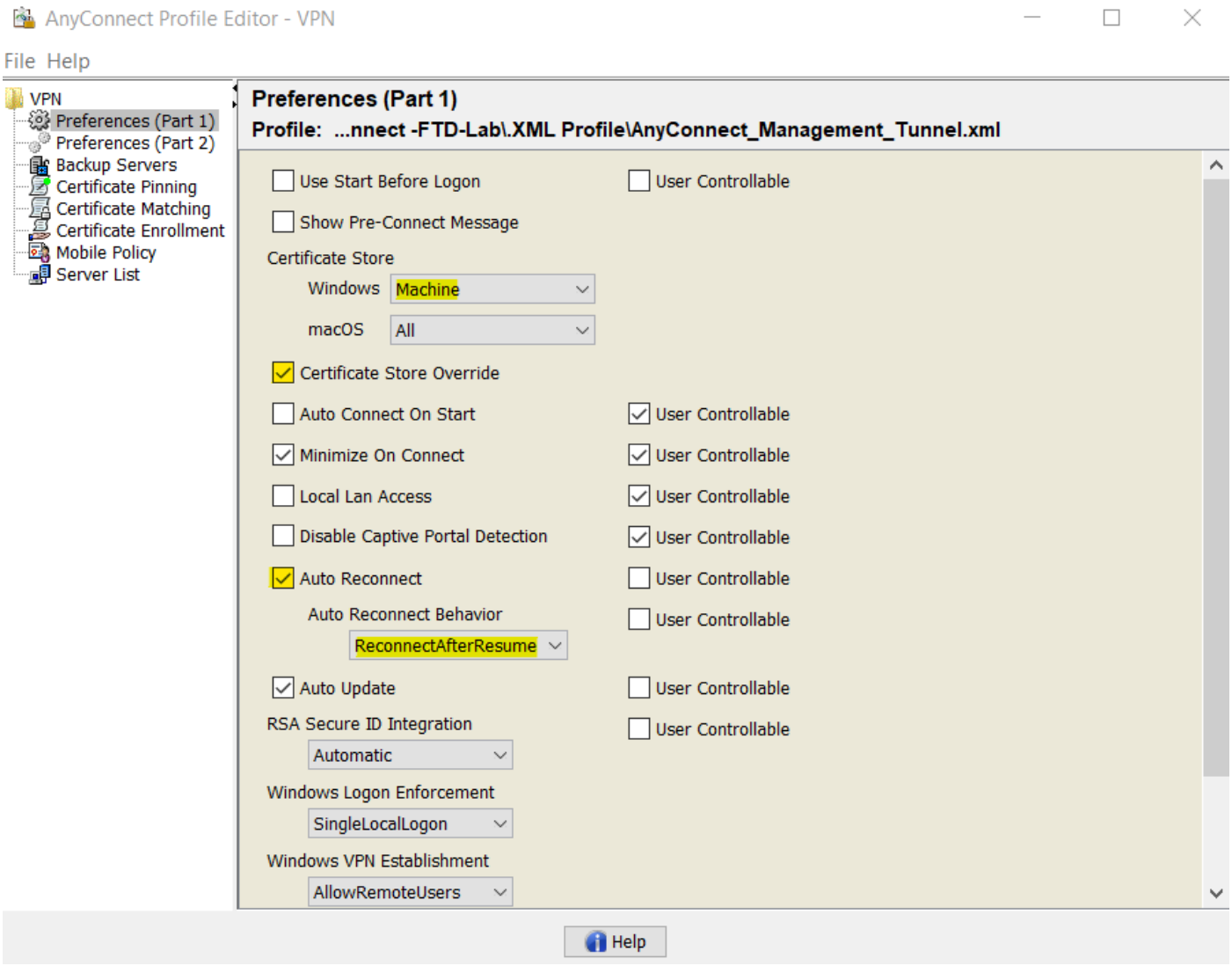
Neste exemplo, uma entrada da lista de servidores que aponta para Fully Qualified Domain Name (FQDN) dperezve.jyoung-labdomain.cisco.com é definida e SSL é selecionado como o protocolo principal. Para adicionar uma Lista de servidores, navegue até **Lista de servidores** e selecione o botão **Adicionar**, preencha os campos obrigatórios e salve as alterações.



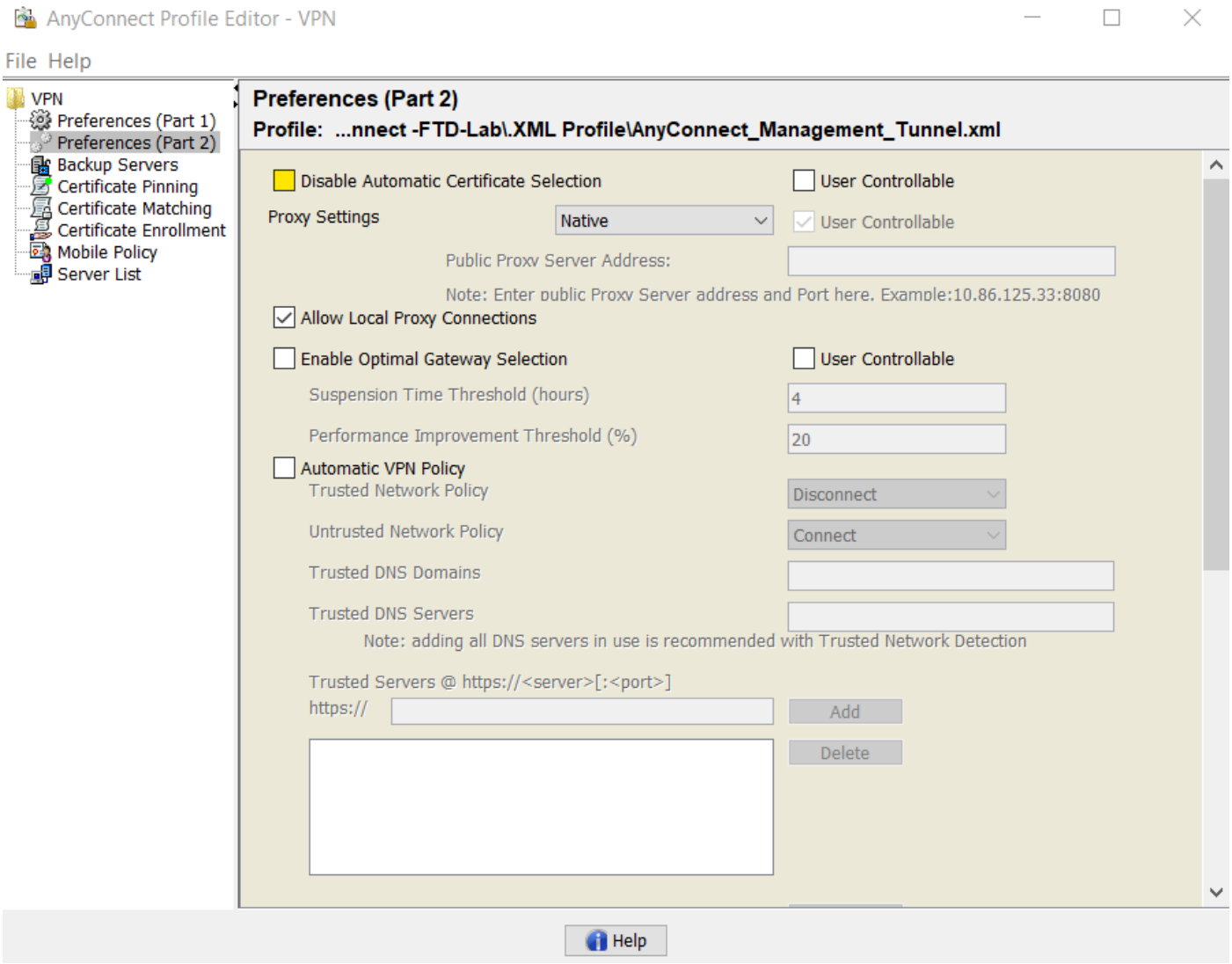

Além da lista de servidores, o perfil de gerenciamento VPN deve conter algumas preferências obrigatórias:

- **AutomaticCertSelection** deve ser definido como **true**.
- **AutoReconnect** deve ser definido como **verdadeiro**.
- **AutoReconnectBehavior** deve ser configurado para **ReconnectAfterResume**.
- **AutoUpdate** deve ser definido como **false**.
- **BlockUntrustServers** deve ser definido como **verdadeiro**.
- **CertificateStore** deve ser configurado para **MachineStore**.
- **CertificateStoreOverride** deve ser definido como **true**.
- **EnableAutomaticServerSelection** deve ser definido como **false**.
- **EnableScripting** deve ser definido como **false**.
- **RetainVPNOnLogoff** deve ser definido como **verdadeiro**.

No Editor de perfis do AnyConnect, navegue até **Preferences (Parte 1)** e ajuste as configurações da seguinte maneira:




Em seguida, navegue até **Preferences (Parte 2)** e desmarque a opção **Disable Automatic Certificate Selection (Desativar seleção automática de certificado)**.




## Etapa 2. Criar perfil de VPN do AnyConnect

Além do perfil de gerenciamento VPN, o perfil normal de AnyConnect VPN precisa ser configurado. O perfil de VPN do AnyConnect é usado na primeira tentativa de conexão, durante esta sessão, o perfil de VPN de gerenciamento é baixado do FTD.

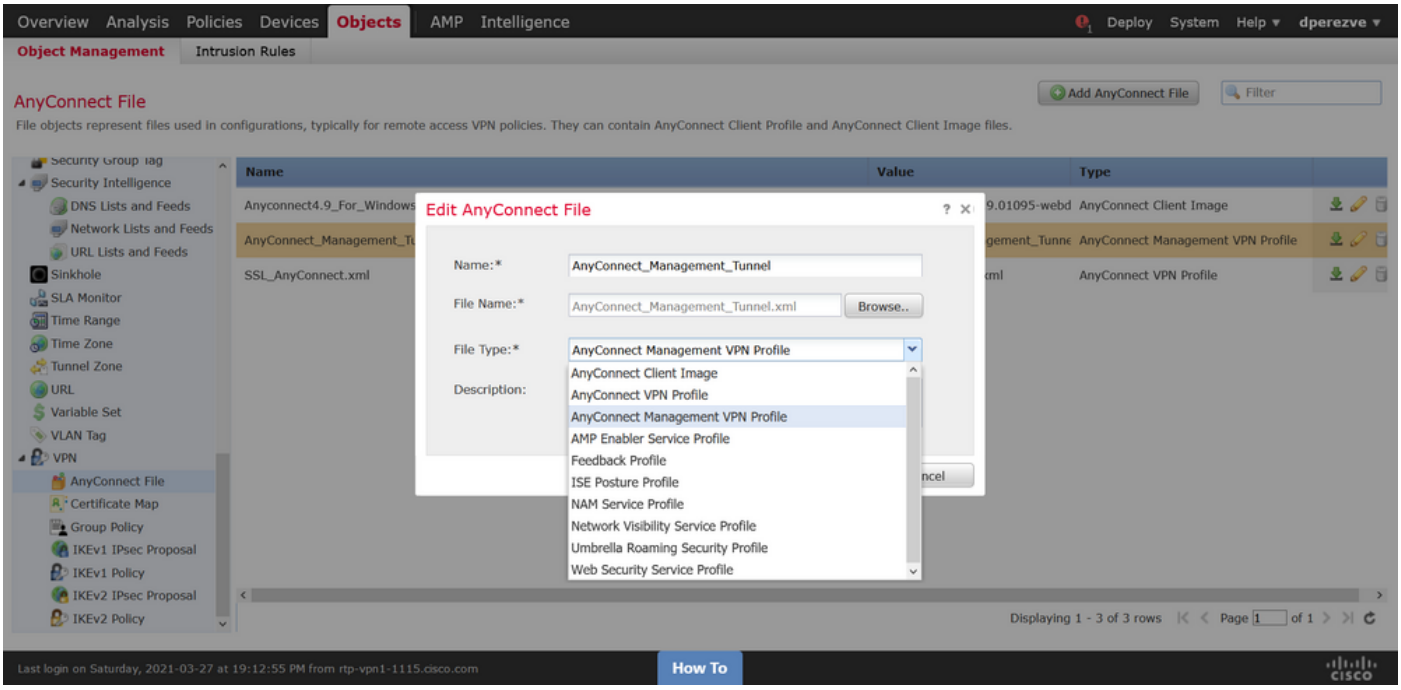
Use o Editor de perfis do AnyConnect para criar o perfil de VPN do AnyConnect. Nesse caso, ambos os arquivos contêm as mesmas configurações, de modo que o mesmo procedimento pode ser seguido.

## Etapa 3. Carregue o perfil de VPN de gerenciamento do AnyConnect e o perfil de VPN do AnyConnect para a FMC

Quando os perfis forem criados, a próxima etapa será carregá-los no FMC como objetos de arquivo do AnyConnect.

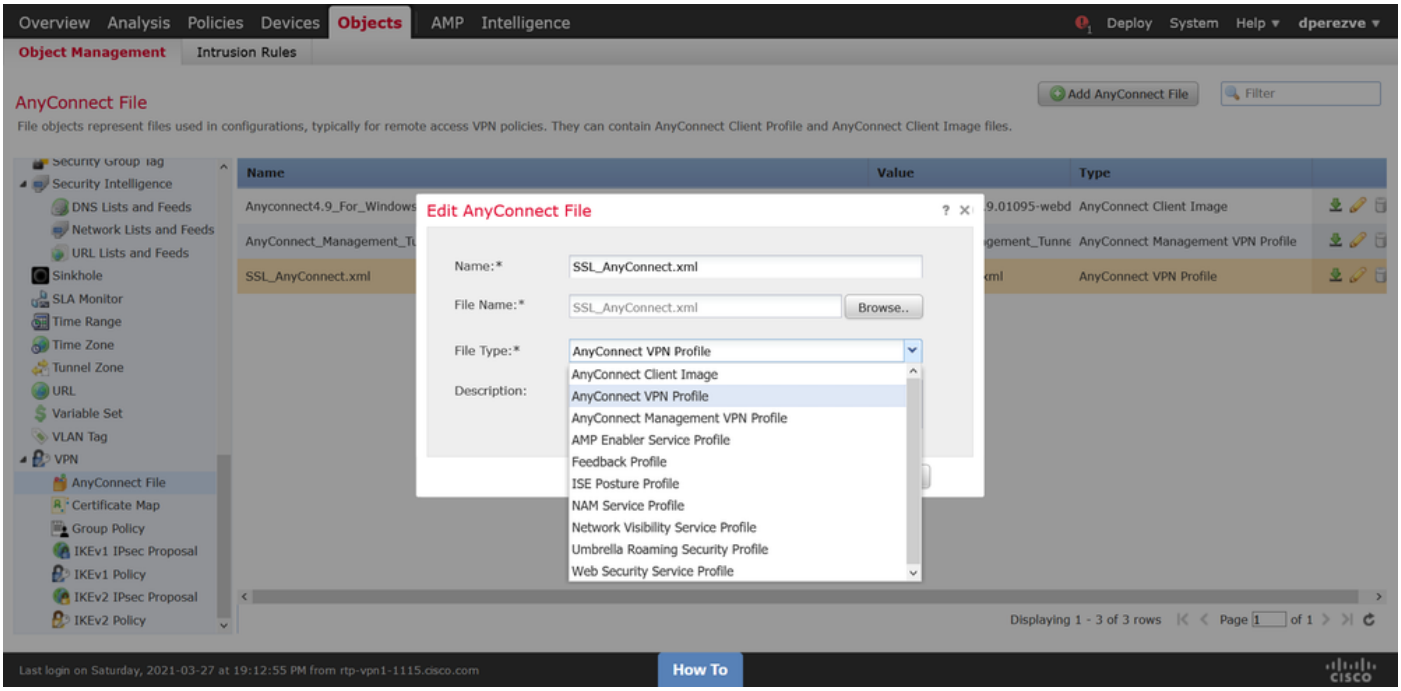
Para fazer o upload do novo perfil de VPN de gerenciamento do AnyConnect para o FMC, navegue para **Objects > Object Management** e escolha a opção **VPN** do sumário e selecione o botão **Add AnyConnect File**.

Forneça um nome para o arquivo, escolha **AnyConnect Management VPN Profile** como o tipo de arquivo e salve o objeto.

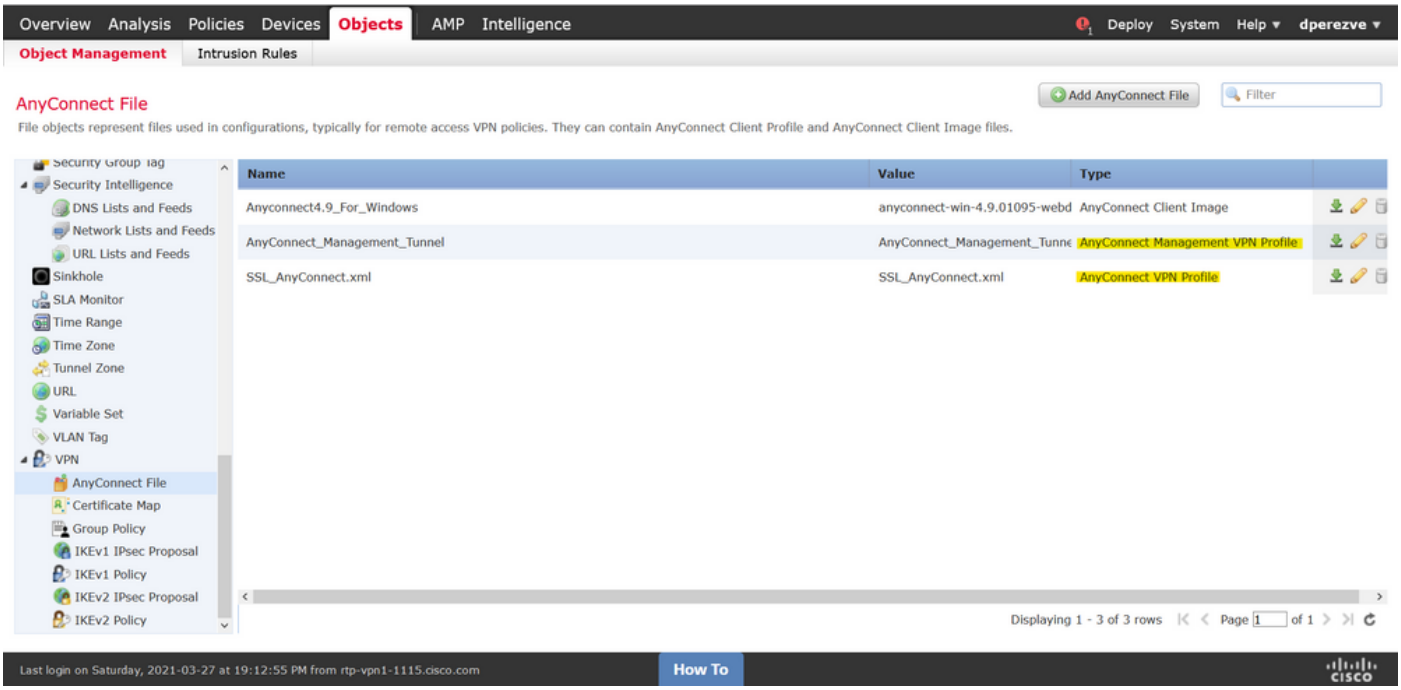



Agora, para fazer o upload do perfil de VPN do AnyConnect, navegue novamente para **Objects > Object Management** e escolha a opção **VPN** do índice e selecione o botão **Add AnyConnect File**.

Forneça um nome para o arquivo, mas desta vez escolha **AnyConnect VPN Profile** como o tipo de arquivo e salve o novo objeto.



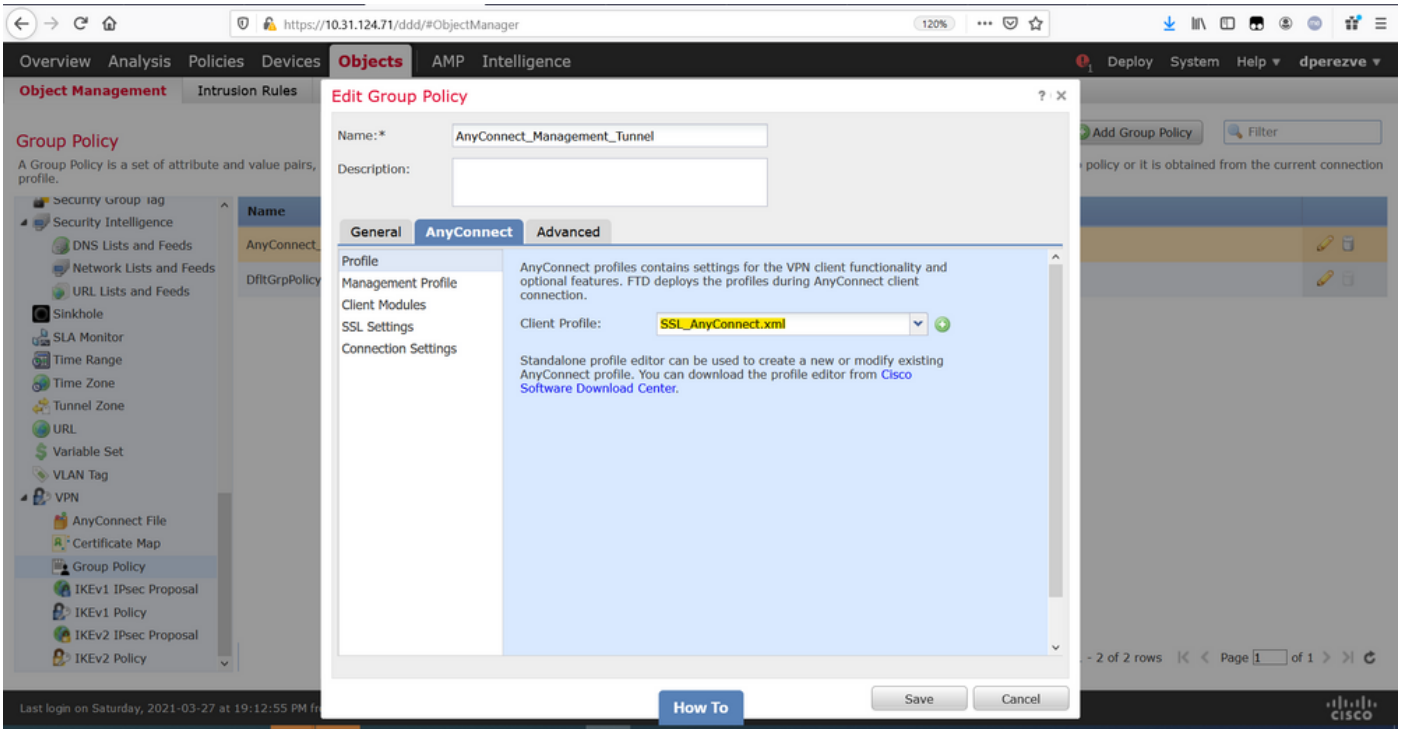

Os perfis devem ser adicionados à lista de objetos e marcados como **perfil de VPN de gerenciamento do AnyConnect** e **perfil de VPN do AnyConnect**, respectivamente.



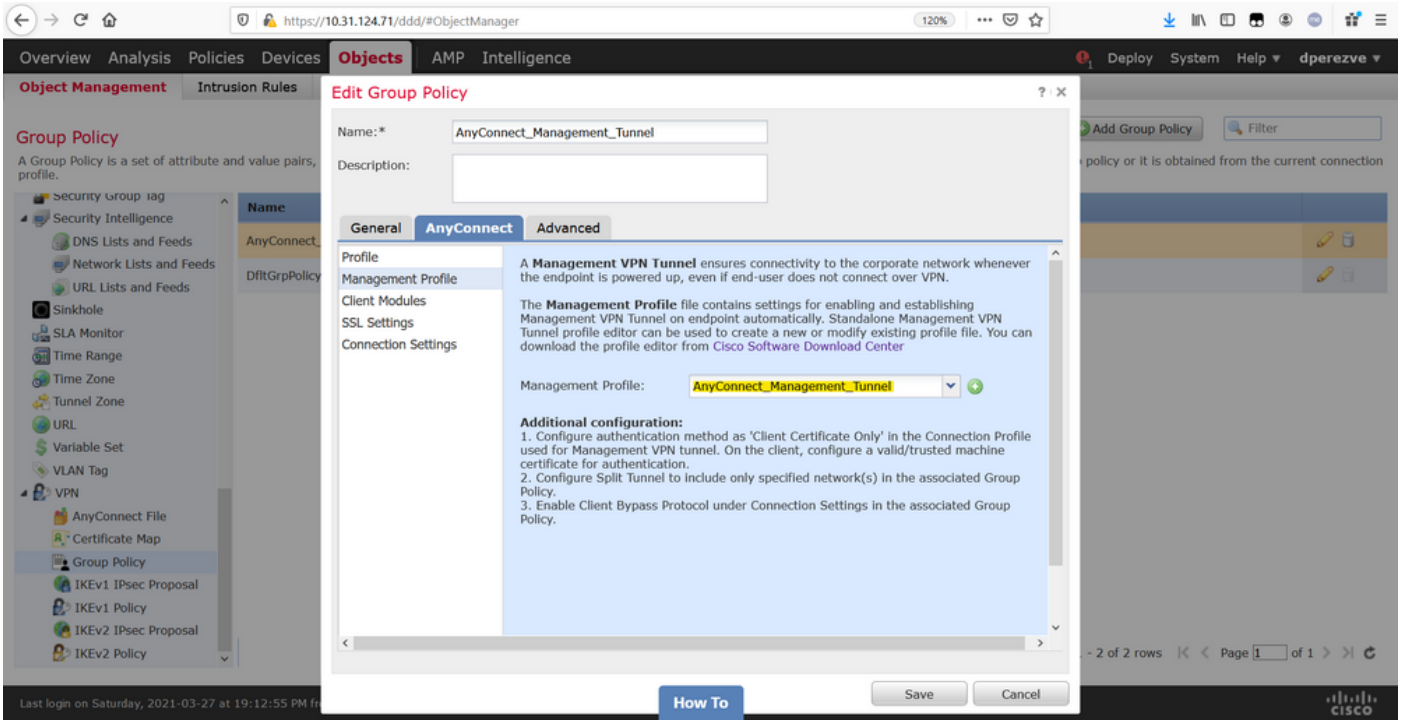

## Etapa 4. Criar política de grupo

Para criar uma nova Política de Grupo, navegue para **Objetos > Gerenciamento de Objeto** e escolha a opção **VPN** do índice e selecione **Política de Grupo** e clique no botão **Adicionar Política de Grupo**.

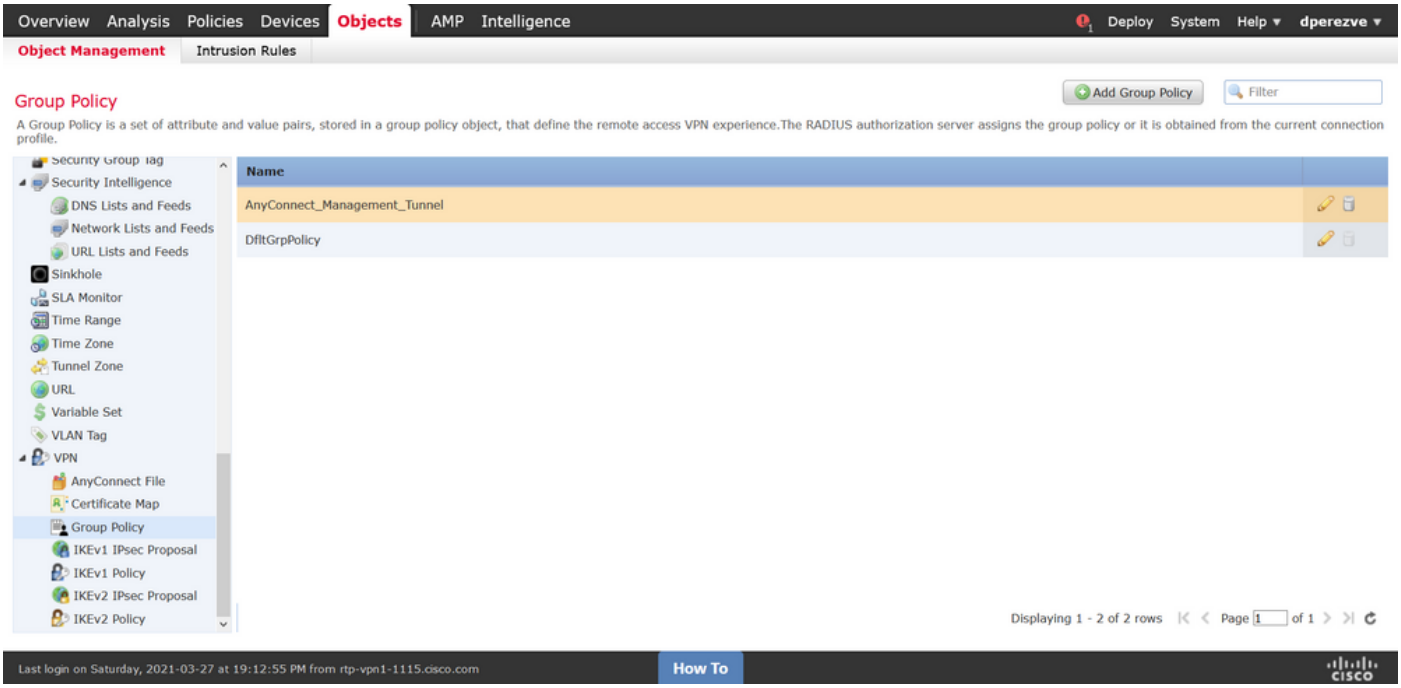
Quando a janela **Adicionar política de grupo** for aberta, atribua um nome, defina um pool do AnyConnect e abra a guia **AnyConnect**. Navegue até **Profile** e selecione o objeto que representa o perfil normal de AnyConnect VPN no menu suspenso **Client Profile**.




Em seguida, navegue até a guia **Management Profile** e selecione o objeto que contém o Management VPN Profile no menu suspenso **Management Profile**.



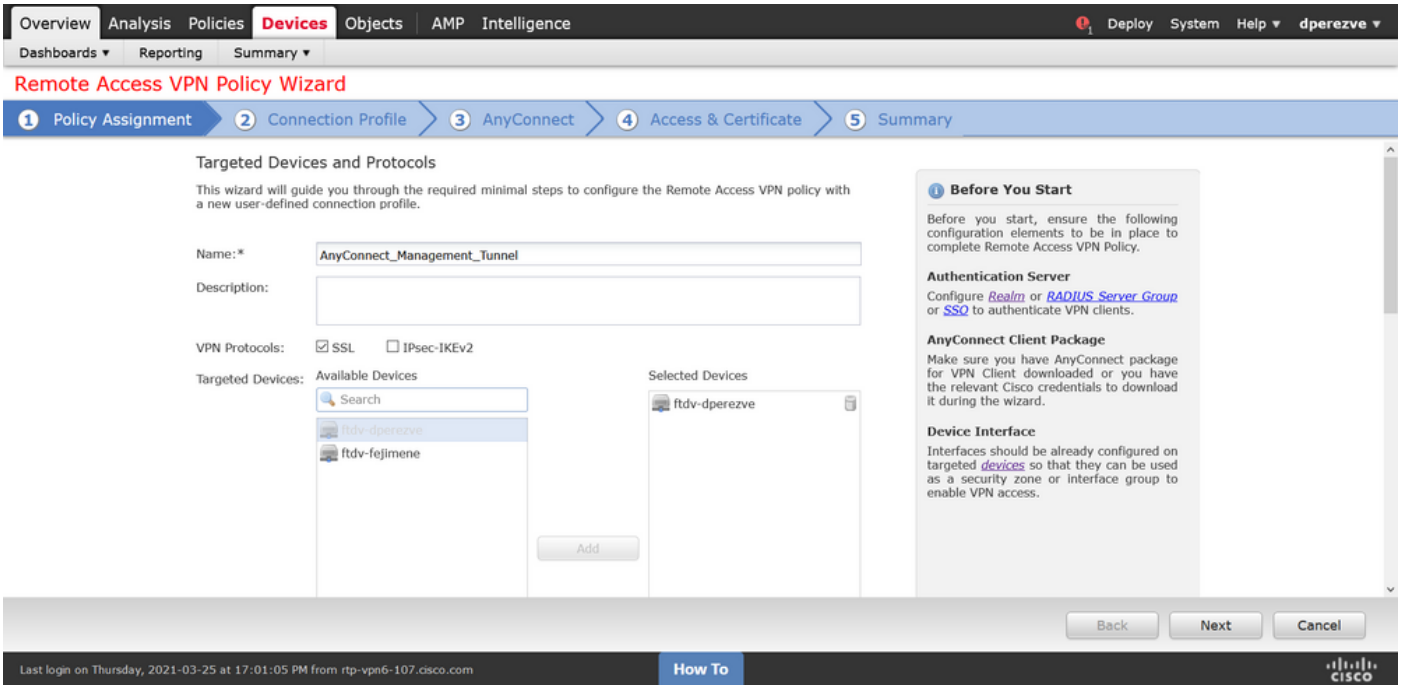

Salve as alterações para adicionar o novo objeto às Políticas de grupo existentes.



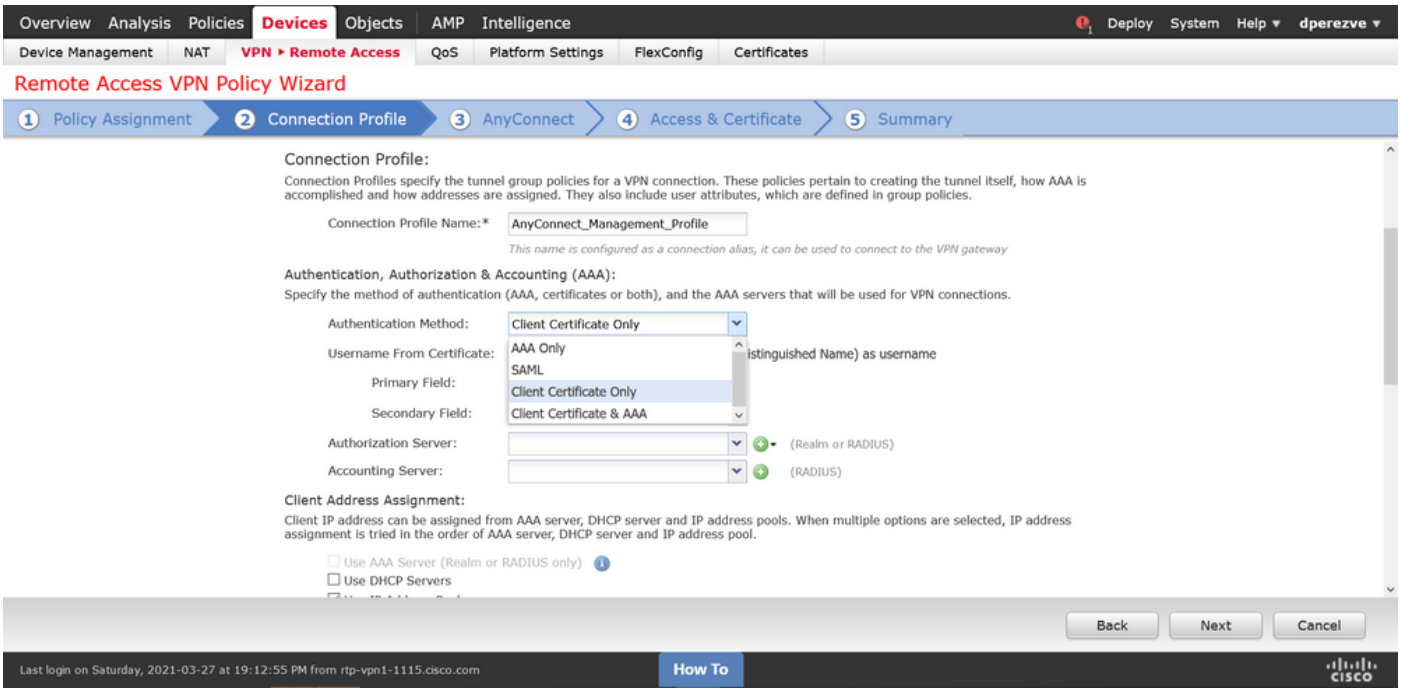

## Etapa 5. Criar nova configuração do AnyConnect

A configuração do AnyConnect SSL no FMC é composta de 4 etapas diferentes. Para configurar o AnyConnect, navegue para **Dispositivos > VPN > Acesso remoto** e selecione o botão **Adicionar**. Isso deve abrir o **Assistente de Política de VPN de Acesso Remoto**.

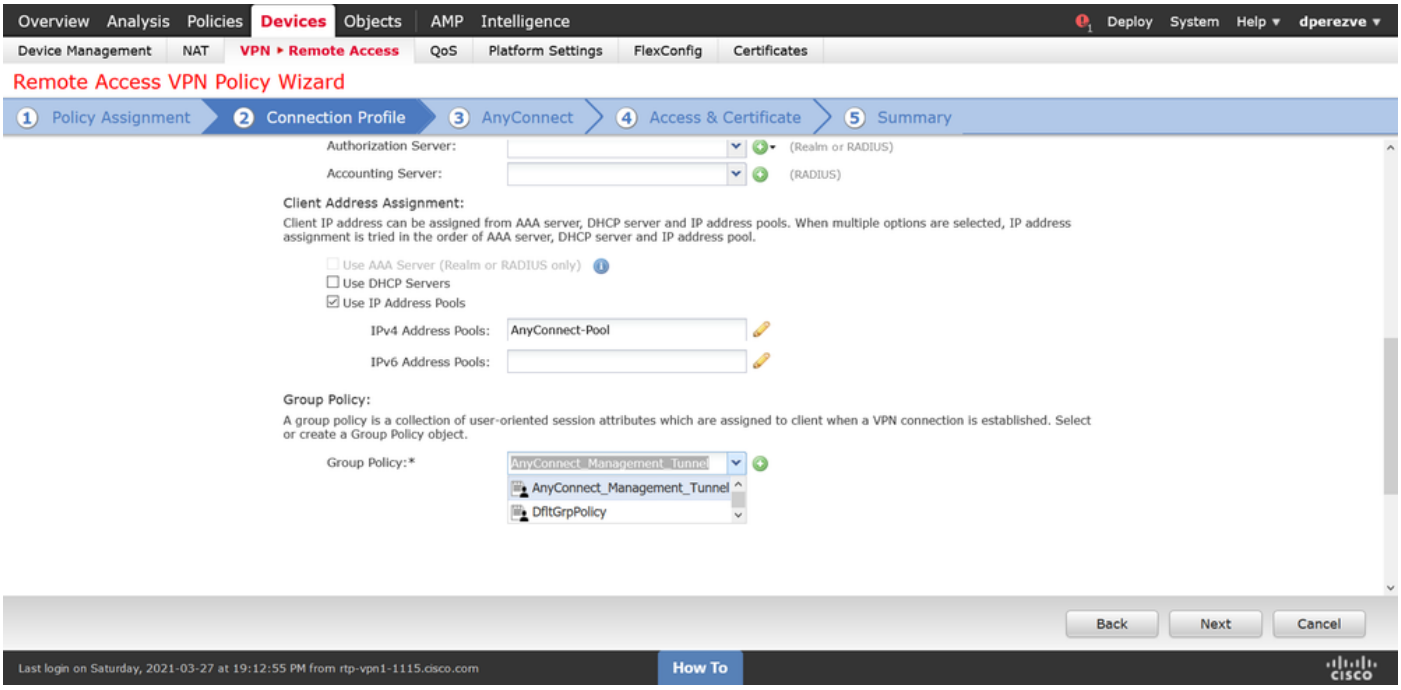
Na guia **Policy Assignment**, selecione o dispositivo FTD em mãos, defina um nome para o perfil de conexão e marque a caixa de seleção SSL.



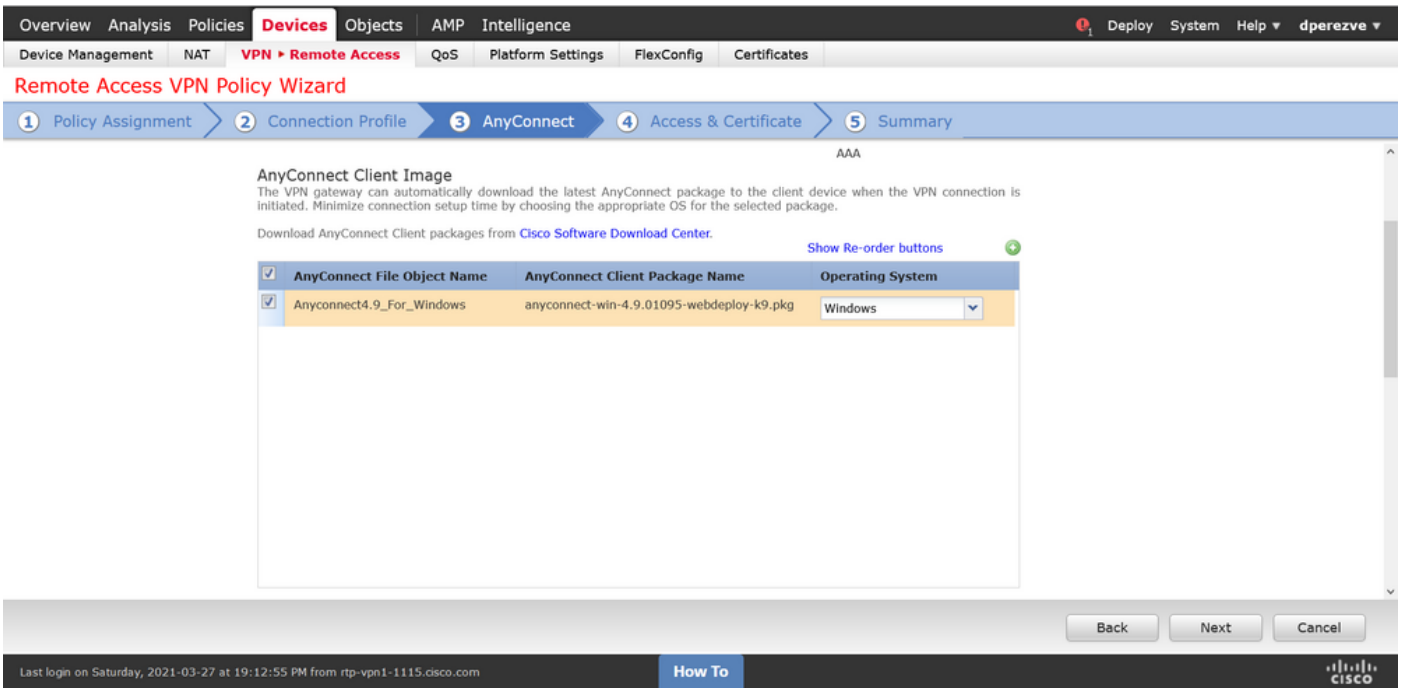

Em **Perfil de conexão,** selecione **Somente certificado do cliente** como o método de autenticação. Esta é a única autenticação suportada para a funcionalidade.




Em seguida, selecione o objeto Diretiva de grupo criado na etapa 3 no menu suspenso **Diretiva de grupo**.



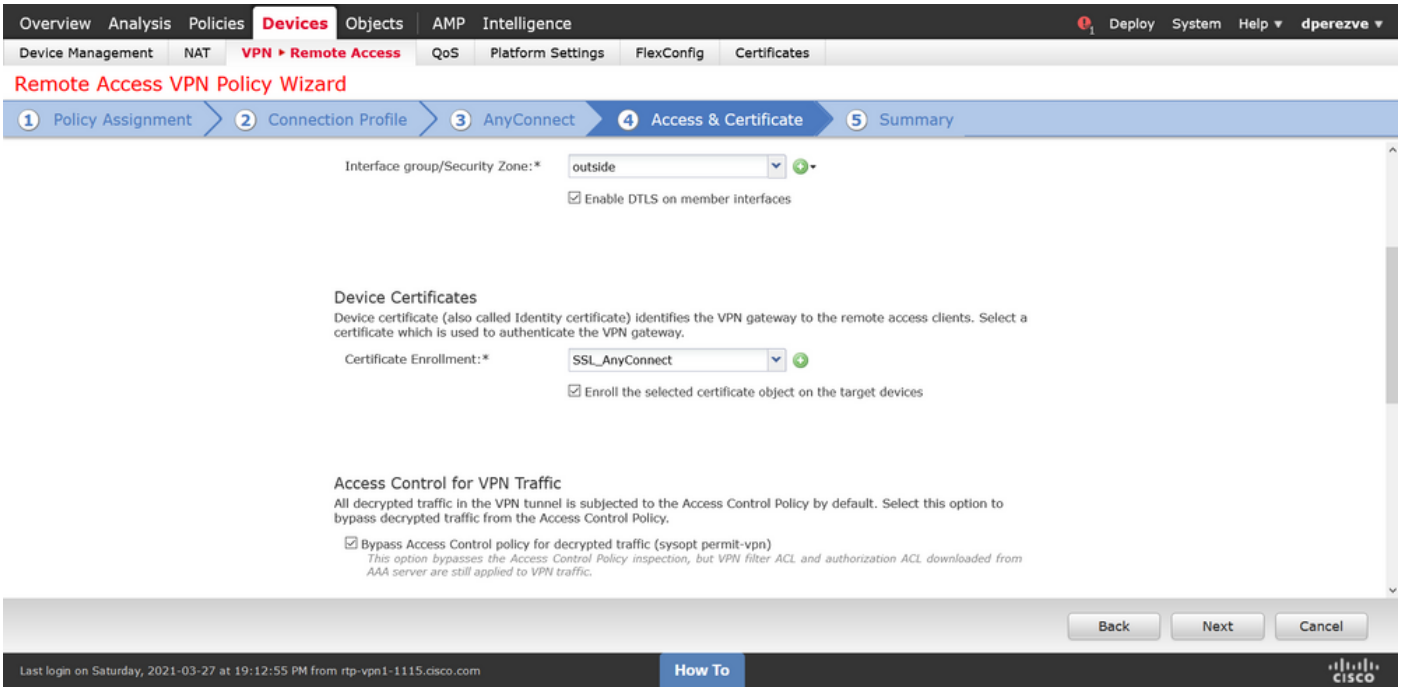

Na guia **AnyConnect** selecione o **AnyConnect File Object** de acordo com o OS (Operating System, sistema operacional) no endpoint.



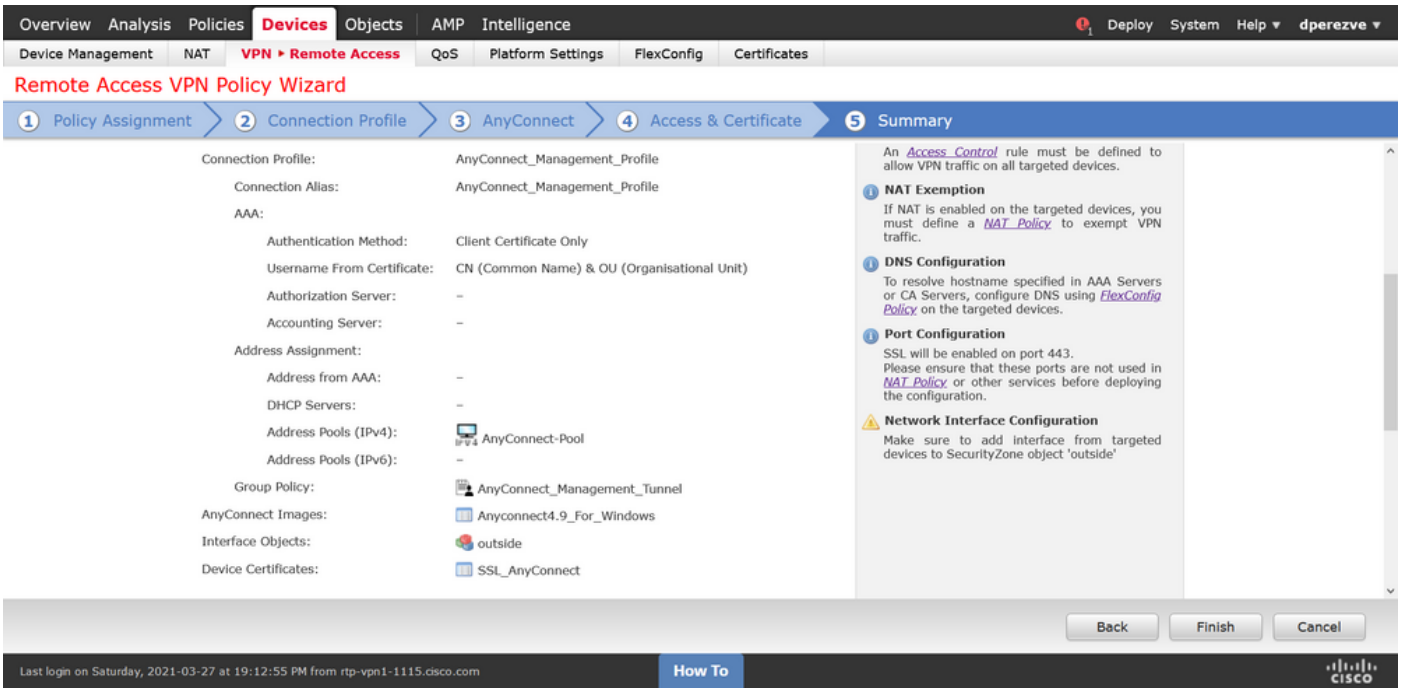

No **Access & Certificate,** especifique o certificado que deve ser usado pelo FTD para investigar sua identidade para o cliente Windows.

> **Note**: Como os usuários não devem interagir com o aplicativo AnyConnect ao usar o recurso Management VPN, o certificado precisa ser totalmente confiável e não deve imprimir nenhuma mensagem de aviso.

> **Note**: Para evitar erros de validação de certificado, o campo Nome Comum (CN) incluído no Nome do assunto do certificado deve corresponder ao FQDN definido na Lista de perfis XML do servidor (Etapa 1 e Etapa 2).



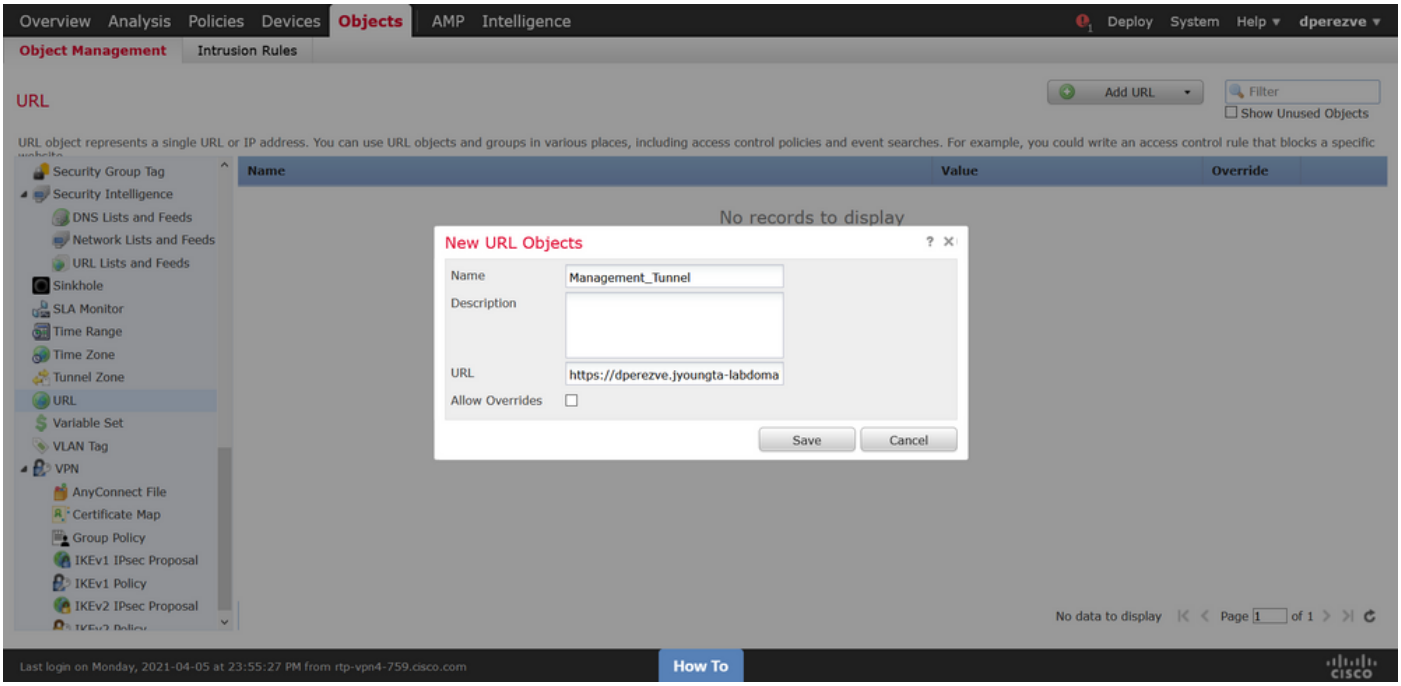

Finalmente, selecione o botão **Concluir** na guia **Resumo** para adicionar a nova configuração do AnyConnect.




## Etapa 6. Criar objeto de URL

Navegue até **Objects > Object Management** e selecione **URL** no índice. Em seguida, selecione **Add Object (Adicionar objeto)** na lista suspensa **Add URL (Adicionar URL)**.

Forneça um nome para o objeto e defina a URL usando o mesmo FQDN/Grupo de usuários especificado na Management VPN Profile Server List (Etapa 2). Neste exemplo, a URL deve ser dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnel.




Salve as alterações para adicionar o objeto à lista de objetos.

### Passo 7. Definir alias de URL

Para habilitar o URL Alias na configuração do AnyConnect, navegue até **Devices > VPN > Remote Access** e clique no ícone do lápis para editar.

Em seguida, na guia Perfil de conexão, selecione a configuração à mão, navegue até **Aliases**, clique no botão **Adicionar** e selecione o **Objeto de URL** na lista suspensa **Alias de URL** . Verifique se a caixa de seleção **Habilitado** está selecionada.


Salve as alterações e implante configurações no FTD.

## Verificar

Após a conclusão da implantação, uma primeira conexão manual do AnyConnect com o perfil de VPN do AnyConnect é necessária. Durante esta conexão, o Perfil de gerenciamento VPN é baixado do FTD e armazenado em **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**. A partir desse ponto, as conexões subsequentes devem ser iniciadas através do perfil de gerenciamento VPN sem nenhuma interação do usuário.

# Troubleshoot

Para erros de validação de certificado:

- Certifique-se de que o certificado raiz da autoridade de certificação (AC) está instalado no FTD.
- Verifique se um certificado de identidade assinado pela mesma AC está instalado no Windows Machine Store.
- Certifique-se de que o campo CN esteja incluído no certificado e seja o mesmo que o FQDN definido na Lista de servidores do Perfil de VPN de gerenciamento e FQDN definido no alias de URL.

Para túnel de gerenciamento não iniciado:

- Verifique se o perfil de gerenciamento VPN foi baixado e armazenado em **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**.
- Verifique se o nome do perfil de gerenciamento VPN é **VpnMgmtTunProfile.xml**.

Para problemas de conectividade, colete o pacote DART e entre em contato com o Cisco TAC para obter mais pesquisas.