

Implante o módulo de segurança de roaming do guarda-chuva do AnyConnect com o FMC

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Instalação e download do módulo do AnyConnect Umbrella do FMC:](#)

[Opcional: Autenticação local de VPN \(FMC 7.0 ou posterior necessário\)](#)

[Informações adicionais](#)

Introdução

Este documento descreve como implantar o módulo de segurança de roaming Umbrella do AnyConnect usando o Cisco Firewall Management Console (FMC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso ao painel do Cisco Umbrella
- Acesso ao Cisco Firewall Management Console (FMC), versão 6.7 ou posterior, pois esta versão adiciona suporte para módulos adicionais do AnyConnect. Para versões anteriores à 6.7, o FlexConfig pode ser usado para implantar o módulo. Consulte a [documentação da Cisco](#) para obter detalhes.
- Perfil do módulo Umbrella do AnyConnect (orginfo.json)
- A configuração do AnyConnect VPN já está completa e funcional no FMC/FTD

Componentes Utilizados

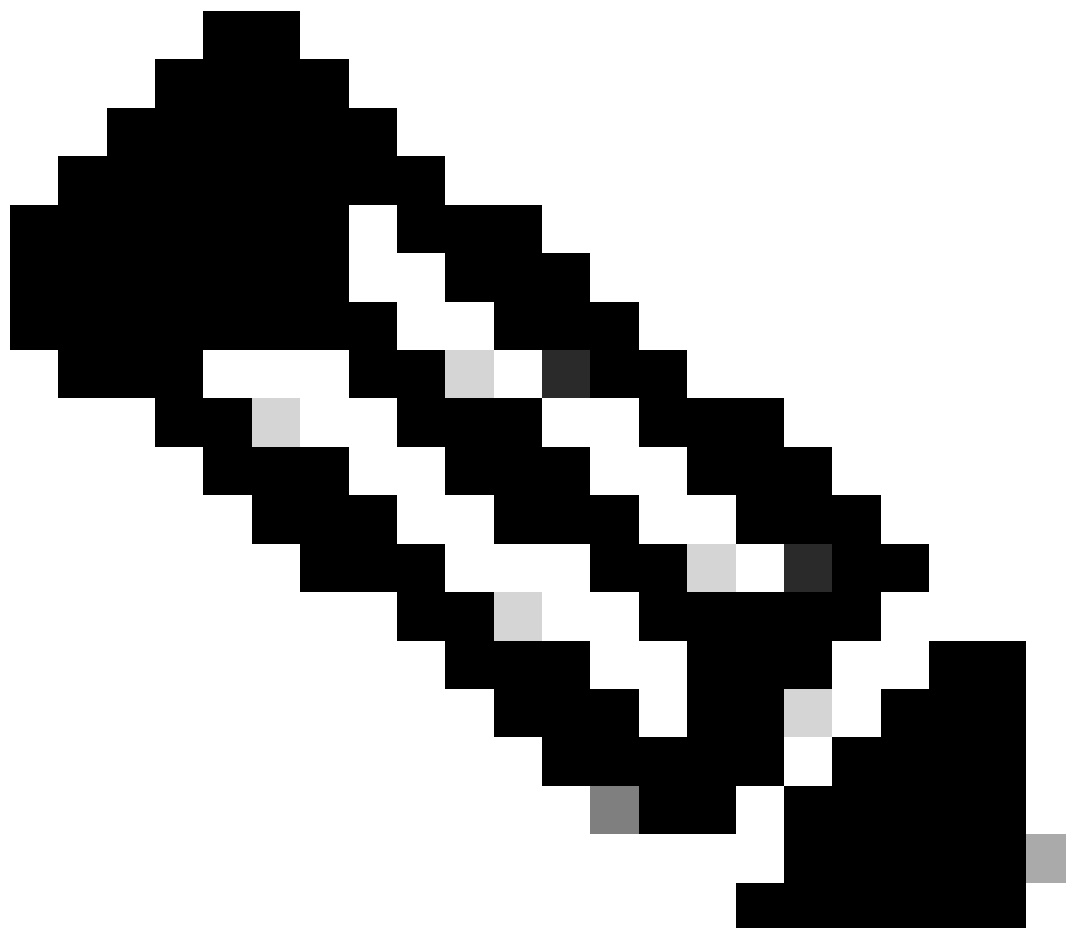
As informações neste documento são baseadas nestas versões de software e hardware:

- Módulo de segurança de roaming Umbrella do AnyConnect
- Cisco Firewall Management Console (FMC) para versões 6.7 ou posteriores

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.

Overview



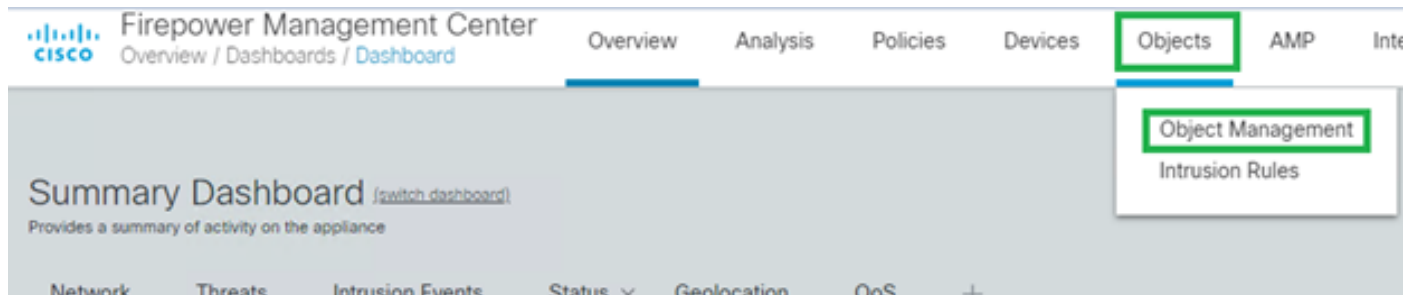
Note: A Cisco anunciou o fim da vida útil do Cisco AnyConnect em 2023. A Cisco anunciou o Fim da Vida Útil do Umbrella Roaming Client em 2 de abril de 2024, e a última data de suporte foi 2 de abril de 2025. Muitos clientes do Cisco Umbrella já estão se beneficiando da migração para o Cisco Secure Client, e você é encorajado a iniciar a migração o mais rápido possível para obter uma melhor experiência de roaming. Leia mais neste artigo da Base de conhecimento: [Como instalo o Cisco Secure Client com o Umbrella Module?](#)

Este guia de configuração aborda as etapas para provisionar o Módulo de segurança de roaming do AnyConnect Umbrella através do Cisco Firewall Management Console (FMC) para as versões 6.7 ou posteriores.

Instalação e download do módulo do AnyConnect Umbrella do FMC:

Conclua estas etapas para ativar a instalação/download do módulo do AnyConnect Umbrella a partir do FMC:

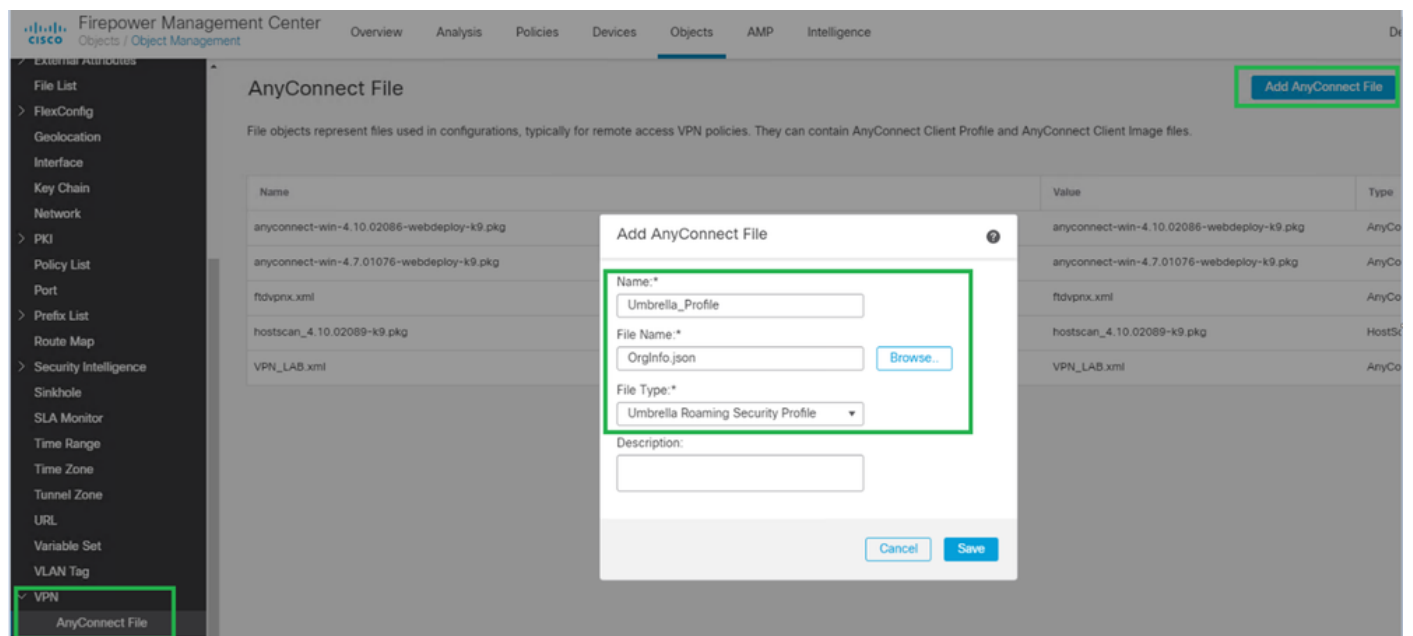
1. Vá para Objetos > Gerenciamento de Objetos:



8178144512532

2. Navegue até VPN > AnyConnect File > Add AnyConnect File. Defina um nome para o perfil (significativo localmente).

- Procure o JSON baixado do painel do Cisco Umbrella.
- Em File Type, selecione Umbrella Roaming Security Profile e depois Save.



8178144531860

3. Uma vez lá, selecione Group Policy, em seguida, selecione a política de grupo que você está usando para implantar Umbrella ("Umbrella_GP" neste caso):

Firepower Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects**

External Attributes

- File List
- FlexConfig
- Geolocation
- Interface
- Key Chain
- Network
- PKI
- Policy List
- Port
- Prefix List
- Route Map
- Security Intelligence
- Sinkhole
- SLA Monitor
- Time Range
- Time Zone
- Tunnel Zone
- URL
- Variable Set
- VLAN Tag
- VPN**
 - AnyConnect File
 - Certificate Map
 - Custom Attribute
 - Group Policy**

Group Policy

A Group Policy is a set of attribute and value pairs, stored in a group policy object, that

Name
DfltGrpPolicy
GP_Split
ISE_Posture
Umbrella_GP

8178147609492

4. Selecione AnyConnect > Módulos do cliente > Adicionar módulo do cliente.

- Em Client Module, selecione o Umbrella Roaming Client e, em seguida, Profile para baixar o perfil que definimos na etapa 2.
- Certifique-se de que o download do módulo Habilitado esteja selecionado para que os usuários que se conectam via AnyConnect possam baixar automaticamente o perfil JSON Umbrella.

Edit Group Policy ?

Name:*
Umbrella_GP

Description:

General **AnyConnect** Advanced

Profile
Management Profile
Client Modules
SSL Settings
Connection Settings
Custom Attributes

Download optional client modules to the endpoint. AnyConnect client requests download from the FTD of only the modules that are configured here.

Client Module	Profile	Download	
No records to display			

+

Add Client Module ?

Client Module
Umbrella Roaming Security ▼

Profile to download
Umbrella_Profile ▼ +

☒ Enable module download

Cancel Add

Cancel Save

8178147636628

Opcional: Autenticação local de VPN (FMC 7.0 ou posterior necessário)

Se quiser testar um perfil separado com Autenticação Local no FMC/FTD, você pode concluir estas etapas (FMC 7.0 ou posterior é necessário):

1. Crie um realm local.

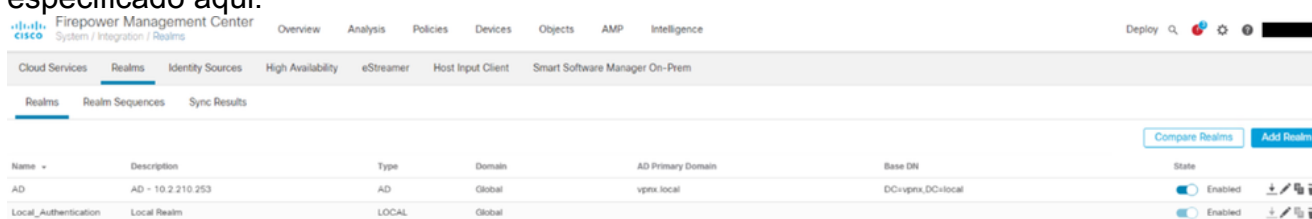
- Nomes de usuário e senhas locais são armazenados em territórios locais.
- Quando você cria um território (**Sistema > Integração > Territórios**) e seleciona o novo tipo de território **LOCAL**, o sistema solicita que você adicione um ou mais usuários locais.

2. Configure a VPN do RA para usar a autenticação local.

- Crie ou edite uma política de VPN RA (**Dispositivos > VPN > Acesso Remoto**).
- Crie um perfil de conexão dentro dessa política.
- Especifique **LOCAL** como o servidor de autenticação principal, secundário ou de fallback nesse perfil de conexão.

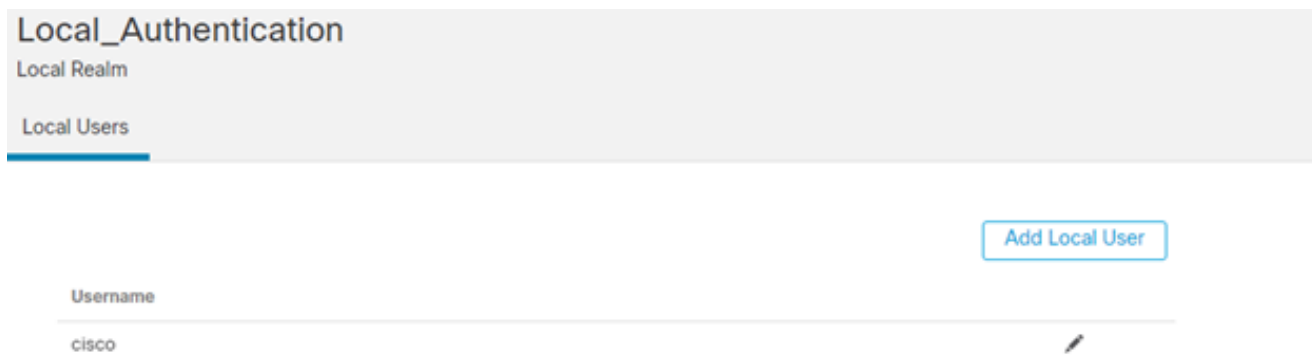
3. Associe o realm local que você criou a uma política VPN do RA.

- No editor de política de VPN do RA, use a nova configuração **Local Realm**. Cada perfil de conexão na política de VPN do RA que usa a autenticação local pode usar o território local especificado aqui.



Name	Description	Type	Domain	AD Primary Domain	Base DN	State
AD	AD - 10.2.210.253	AD	Global	vpn.local	DC=vpn,DC=local	Enabled
Local_Authentication	Local Realm	LOCAL	Global			Enabled

8178273923732



Local_Authentication
Local Realm

Local Users

Username
cisco

8178144714388

Informações adicionais

[Notas de versão do Cisco Firewall \(anteriormente Firepower\), versão 7.0.x](#)

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.