# Configurar SSL AnyConnect Management VPN no FTD

## Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Informações de Apoio Limitações Configurar Configurações Etapa 1. Criar perfil de VPN de gerenciamento do AnyConnect Etapa 2. Criar perfil de VPN do AnyConnect Etapa 3. Carregue o perfil de VPN de gerenciamento do AnyConnect e o perfil de VPN do AnyConnect para a FMC Etapa 4. Criar política de grupo Etapa 5. Criar nova configuração do AnyConnect Etapa 6. Criar objeto de URL Passo 7. Definir alias de URL Verificar **Troubleshoot** 

## 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 <u>CSCvs78215</u>.

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.

- an	AnyConnect	Profile	Editor -	VPN
------	------------	---------	----------	-----

Server Load Balancing Se	ervers SCEP Mobile Certificate Pinning	
Primary Server		Connection Information
Display Name (requi	red) AnyConnect_Management_Tunnel	Primary Protocol SSL ~
FQDN or IP Address	User Group	ASA gateway
dperezve.jyoungta-l	abdomain.cisc / AnyConnect_Management_Tunnel	Auth Method During IKE Negotiation EAP-A
Group URL		IKE Identity (IOS gateway only)
dperezve.jyoungta-la	abdomain.cisco.com/AnyConnect_Management_Tunn	
	Backup Servers	
	Host Address	Add
		Move Up
		Move Down
		Delete
	OK Cancel	

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:

 $\times$ 

File Help

VPN Preferences (Part 1) Preferences (Part 2)	Preferences (Part 1) Profile:nnect -FTD-Lab\.XML Profile\AnyConnect_Management_Tunnel.xml										
Backup Servers Certificate Pinning Certificate Matching Certificate Enrollment Mobile Policy	□ Use Start Before Logon □ Show Pre-Connect Message Certificate Store Windows Machine macOS All ✓ Certificate Store Override □ Auto Connect On Start	User Controllable	^								
	Minimize On Connect	User Controllable									
	Disable Captive Portal Detection	User Controllable									
	Auto Reconnect Auto Reconnect Behavior ReconnectAfterResume	User Controllable									
	Auto Update RSA Secure ID Integration Automatic	User Controllable									
	Windows Logon Enforcement SingleLocalLogon V Windows VPN Establishment										
	AllowRemoteUsers		~								
	6	Help									

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

 $\Box$   $\times$ 

\_

File Help

VPN Preferences (Part 1) Preferences (Part 2) Backup Servers Certificate Pinning Certificate Matching Certificate Enrollment Mobile Policy Server List	Preferences (Part 2 Profile:nnect -FTI	) D-Lab\.XML Profile\AnyConnec	t Management Tunnel.xml										
	Disable Automatic (	Certificate Selection	User Controllable	^									
	Proxy Settings	Native	✓ Vser Controllable										
	I	Public Proxv Server Address:											
	Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080  Allow Local Proxy Connections												
	Enable Optimal Gat	eway Selection	User Controllable										
	Suspension Time	Threshold (hours)	4										
	Performance Impr	ovement Threshold (%)	20										
	Trusted Network F	Policy	Disconnect $\vee$										
	Untrusted Network	C Policy	Connect $\sim$										
	Trusted DNS Dom	ains											
	Trusted DNS Serv Note: addir	ers Ig all DNS servers in use is recomme	nded with Trusted Network Detection										
	Trusted Servers @	<pre>&gt; https://<server>[:<port>]</port></server></pre>											
	https://		Add										
			Delete										
				~									
		📢 Help											

 $\sim$ 

#### 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.

Overview Analysis Policie	s Devices Objects	AMP Intelligen	ce				. Peploy System Help ▼ d	perezve 🔻
Object Management Intrus	sion Rules							
AnyConnect File File objects represent files used in co	nfigurations, typically for remot	te access VPN policies.	They can contain AnyConnect Client Profile and Ar	nyConnect Clie	nt Image	e files.	Add AnyConnect File	
Security Group lag	Name			Value			Туре	
Security Intelligence     DNS Lists and Feeds	Anyconnect4.9_For_Windows	Edit AnyConnec	t File		? ×	9.01095-web	AnyConnect Client Image	205
Network Lists and Feeds     NPL Lists and Feeds	AnyConnect_Management_TL					gement_Tunn	AnyConnect Management VPN Profile	2 🖉 🖯
Sinkhole	SSL_AnyConnect.xml	Name:*	SSL_AnyConnect.xml			cml	AnyConnect VPN Profile	205
نظ SLA Monitor آلته Range آلته		File Name:*	SSL_AnyConnect.xml	Browse				
🗑 Time Zone		File Type:*	AnyConnect VPN Profile	~				
Tunnel Zone		Description	AnyConnect Client Image	^				
S Variable Set		Description.	AnyConnect VPN Profile					
📎 VLAN Tag			AMP Enabler Service Profile					
- 😰 VPN			Feedback Profile					
🍏 AnyConnect File			ISE Posture Profile	-	J			
R Certificate Map			NAM Service Profile					
Group Policy			Network Visibility Service Profile					
IKEv1 IPsec Proposal			Umbrella Roaming Security Profile					
IKEv1 Policy			Web Security Service Profile	~				
IKEv2 IPsec Proposal	<							>
1KEv2 Policy						Displaying	1 - 3 of 3 rows 🛛 🤇 Page 1 of	2 21 6
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115	5.cisco.com	How To					uluilu cisco

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.

Overview Analysis Policie	es Devices Objects AMP Intelligence			perezve 🔻
Object Management Intru	sion Rules			
AnyConnect File File objects represent files used in co	onfigurations, typically for remote access VPN policies. They can contain	AnyConnect Client Profile and AnyConnect Client Image files.	Add AnyConnect File	
Security Group lag	Name	Value	Туре	
Security Intelligence  DNS Lists and Feeds	Anyconnect4.9_For_Windows	anyconnect-win-4.9.01095	-webd AnyConnect Client Image	2 🥒 🖯
Network Lists and Feeds URL Lists and Feeds	AnyConnect_Management_Tunnel	AnyConnect_Management_	Tunne AnyConnect Management VPN Profile	2 🥒 🖯
Sinkhole SLA Monitor SLA Monitor Time Range Time Zone Time Zone Time Zone URL VRL VRL VLN Tag VNN	SSL_AnyConnect.xml	SSL_AnyConnect.xml	AnyConnect VPN Profile	ž 🥜 词
AnyConnect File  Arrow Certificate Map  Certificate Map	٢	Disp	ələying 1 - 3 of 3 rows 🌾 🗧 Page 1 of 3	, , > > , ¢
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115.cisco.com	How To		cisco

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.

Overview Analysis Policie	es Devices Objects AMP Intelligence Q Deploy System	n Help 🔻 dperezve 🔻
Object Management Intrus	sion Rules	
		Cilber
Group Policy	add Group Policy	Ser Filter
A Group Policy is a set of attribute ar profile.	id value pairs, stored in a group policy object, that define the remote access VPN experience. The RADIUS authorization server assigns the group policy or it is obtained	from the current connection
Security Group lag	Nama	
Security Intelligence	None	
DNS Lists and Feeds	AnyConnect_Management_Tunnel	Ø 🖥
Network Lists and Feeds	DftGraphicy	1 A A
URL Lists and Feeds		
Sinkhole		
SLA Monitor		
Time Range		
💮 Time Zone		
Tunnel Zone		
URL URL		
S Variable Set		
S VLAN Tag		
A DO VPN		
AnyConnect File		
R, Certificate Map		
Group Policy		
REVI IPSec Proposal		
IKEV1 Policy		
INEV2 IPSEC Proposal	Displaying 1 - 2 of 2 rows 1/ 4	Page 1 of 1 > > #
INEVZ POlicy	Uspagning 1 - 2 of 2 rows - N - N	rage [L] of 1 / / / U
		սիսիս
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115.casco.com HOW TO	cisco

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.

Overview Analysis Policies Devic	es Objects AMP Intellig	jence			$oldsymbol{\theta}_{1}$ Deploy Syst	em Help 🔻	dperezve 🔻
Remote Access VPN Policy Wiz	ard						
1 Policy Assignment 2 Conne	ection Profile 🔰 3 AnyCo	nnect 🔰 4	Access & Certificate > 🤅	5 Summary			
Targeted Devic This wizard will gui a new user-defined Name:* Description: VPN Protocols: Targeted Devices:	es and Protocols de you through the required minimal : connection profile. AnyConnect_Management_Tunnel SSL IPSec-IKEv2 Available Devices Search MovedDereover ftdv-fejimene	steps to configure th	e Remote Access VPN policy with Selected Devices	Before Y Before you s configuration complete Rem Authenticati Configure Res or SSQ to auti AnyConnect Make sure yo for VPN Cleft the relevant C it during the w Device Inter Interfaces sho targeted devia as a security enable VPN ac	You Start start, ensure the following elements to be in place to ote Access VPN Policy. on Server im or RADIUS Server Group henticate VPN clients. Client Package u have AnyConnect package ti downloaded or you have isco credentials to download vizard. face uld be already configured on cess of that they can be used zone or interface group to cess.		
Last loon on Thursday, 2021-03-25 at 12-01-05 DM	from the units 107 circo com		How To		Back	Next	Cancel

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

Overview Analysis Policies Devices Objects AMP Intelligence	€ Deploy	System	Help 🔻	dperezve 🔻
Device Management 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				
Connection Profile: Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AA accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies. Connection Profile Name:* AnyConnect_Management_Profile	\ is			,
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: Client Certificate Only V Username From Certificate: AAA Only istinguished Name) as username SAML				
Client Certificate Only       Secondary Field:     Client Certificate & AAA				
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 addres assignment is tried in the order of AAA server, DHCP server and IP address pool.				
Use AAA Server (Realm or RADIUS only)				
	Back	Nex	dt 🗌	Cancel
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com How To				uluiu cisco

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

Overview Analysis Policies Devices Objects AMP Intellige	ence	. Deploy	y System	Help 🔻	dperezve 🔻	
Device Management NAT VPN > Remote Access QoS Platform	n Settings FlexConfig Certificates					
Remote Access VPN Policy Wizard						
1 Policy Assignment 2 Connection Profile 3 AnyCor	nnect $>$ 4 Access & Certificate $>$ 5 Summary					
Authorization Server:	(Realm or RADIUS)					^
Accounting Server:	V (RADIUS)					
Client Address Assignment: Client IP address can be assigned from AAA assignment is tried in the order of AAA serv	A server, DHCP server and IP address pools. When multiple options are selected, IP address pool.	55				
Use AAA Server (Realm or RADIU Use DHCP Servers Use IP Address Pools	iS only) 🕕					
IPv4 Address Pools: Anyo	Connect-Pool 🖉					l
IPv6 Address Pools:	Ø					
Group Policy:						
A group policy is a collection of user-oriente or create a Group Policy object.	ed session attributes which are assigned to client when a VPN connection is established.	select				
Group Policy:* Anyt	Connect_Management_Tunnel 💙 🚱					
E /	AnyConnect_Management_Tunnel					
1 m	offtGrpPolicy v					
						ř
		Back	Nex	t 🗌	Cancel	
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com	How To				-ilialia cisco	ſ

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

Overview Analysis Policies		es Objects	AMP	Intelligence	ElexConfig	Cartificates				$m{0}_1$ Deplo	oy System	Help 🔻	dperezve 🔻
Remote Access VPN Pol	licy Wiz	zard	QUU	riadonii octango	Thexeoring	Continuation							
1 Policy Assignment	2) Conne	ection Profile	3	AnyConnect	4 Access 8	k Certificate	Summ	hary					
	AnyCor The VPN initiated.	nnect Client Im gateway can autor Minimize connectio	<b>age</b> natically d n setup tir	lownload the latest A ne by choosing the ap	nyConnect packa propriate OS for t	ge to the client of the selected pack	AAA device when the VI age.	PN connectio	on is				^
	Download	d AnyConnect Client	t packages	from Cisco Software	Download Center.	5	Show Re-order butt	ons	0				
	✓ An	nyConnect File Obj	ject Name	e AnyConnect (	Client Package N	lame	Operating Syste	m					
	An An	vconnect4.9_For_W	indows	anyconnect-wi	n-4.9.01095-web	deploy-k9.pkg	Windows	*					
													~
										Back	Ne	d	Cancel
Last login on Saturday, 2021-03-27 at 19	9:12:55 PM	from rtp-vpn1-1115.	.cisco.com		How	То							ll. cisco

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).

Overview Analysis Policies Devices Objects AMP Intelligence	. ● Deploy	System Help 🔻	dperezve 🔻
Device Management 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			
Interface group/Security Zone:* Outside V O-			
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_AnyConnect         Image: Certificate object on the target devices			
Access Control for VPN Traffic All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy. Bypass Access Control policy for decrypted traffic (sysopt permit-vpn) This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.			
	Back	Next	Cancel
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com How To			

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.

Overview Analysis Policie	ies Devices Objects AMP Intelligence						tem Help <del>v</del>	dperezve 🔻
Object Management Intrus	sion Rules							
URL URL object represents a single URL of	r IP address. You can use URL	objects and groups in vari	ous places, including access control p	olicies and event searches. Fi	or example, you	Add URL •	Filter	used Objects ocks a specific
Security Group Tag	Name			Va	alue		Override	
A Security Intelligence								
DNS Lists and Feeds			No reco	rds to display				
Network Lists and Feeds		New URL Object	ts	? X				
URL Lists and Feeds		Name						
Sinkhole		Name	Management_Tunnel					
SLA Monitor		Description						
🚮 Time Range								
🕣 Time Zone								
and Tunnel Zone		URL	https://dperezve.jyoungta-labdoma					
() URL		Allow Overrides						
\$ Variable Set				Cancel				
VLAN Tag				Save Cancer				
▲ ∰2 VPN								
AnyConnect File								
Certificate Map								
Group Policy								
IKEVI IPSec Proposal								
IVEN2 IDeas Proposal								
D TKEY2 Insec Proposal						No data to display	< Page 1	of 1 > >  C
	_				_			abab
			How To					cisco

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.

Overview Analysis Policies Device	Edit Connection Profile		? ×	🎙 Deploy System Help 🔻	dperezve 🔻	
Device Management NAT VPN + Rem AnyConnect_Management_ Enter Description		Save	Cancel			
Connection Profile Access Interfaces	Client Address Assignment AAA Aliase	s				
Name	Alias Names: Add URL Alias Incoming users can ch can be turned on or of Enabled	? Management_Tunnel	s configured on this device		0	
DefaultWEBVPNGroup	Name	OK Cancel			<i>I</i>	
AnyConnect_Management_Tunnel				inel	6	
	URL Alias: Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile.					
	URL	Status				
			Save Cancel			
Last login on Monday, 2021-04-05 at 23:55:27 PM from	n rtp-vpn4-759.cisco.com	How To			uluilu cisco	

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.